

AVG 7.5 Internet Security

User Manual

Document revision 75.3 (1.10.2006)

Copyright GRISOFT, s.r.o. All rights reserved.

This product contains Mailshell SpamCompiler, Copyright (c) 2006 Mailshell. 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 libbzip2, Copyright (c) 1996-2002 Julian R. Seward. This product uses compression library zlib, Copyright (c) 1995-2002 Jean-Ioup Gailly and Mark Adler. All other trademarks are the property of their respective owners.



Copyright (c) 1992-2006 GRISOFT, s.r.o. All rights reserved.



Contents

1. Introduction 5
1.1. Anti-Virus Detection Technologies and Levels of Protection
1.2. Firewall Principles
1.3. Anti-Spam Protection
1.4. Anti-Spyware Protection7
1.5. Operating Systems Supported7
2. Installation
2.1. Installation from the Internet
3. Installation Process
3.1. Installation – Welcome Dialog9
3.2. Installation – License Agreement
3.3. Installation – Select Installation Type10
3.4. Installation – Installation Summary14
3.5. Installation – Application Termination14
3.6. Installation – Installation Complete15
4. AVG First Run
4.1. First Run Wizard16
4.2. AVG Program Start18
5. After Installation 19
5.1. Running the Complete Test19
5.2. Setting up the On-Close Scan19
5.3. Eicar Test
5.4. Test and Update Scheduling19
6. Product Registration
6. Product Registration 21 7. AVG Basic Test Center Interface 22
6. Product Registration 21 7. AVG Basic Test Center Interface 22 7.1. Switch to Advanced 23
6. Product Registration 21 7. AVG Basic Test Center Interface 22 7.1. Switch to Advanced 23 7.2. Control Center 23
6. Product Registration 21 7. AVG Basic Test Center Interface 22 7.1. Switch to Advanced 23 7.2. Control Center 23 7.3. Virus Vault 23
6. Product Registration217. AVG Basic Test Center Interface227.1. Switch to Advanced237.2. Control Center237.3. Virus Vault237.4. Test Results23
6. Product Registration217. AVG Basic Test Center Interface227.1. Switch to Advanced237.2. Control Center237.3. Virus Vault237.4. Test Results237.5. Check for Updates28
6. Product Registration217. AVG Basic Test Center Interface227.1. Switch to Advanced237.2. Control Center237.3. Virus Vault237.4. Test Results237.5. Check for Updates287.6. Exit28
6. Product Registration217. AVG Basic Test Center Interface227.1. Switch to Advanced237.2. Control Center237.3. Virus Vault237.4. Test Results237.5. Check for Updates287.6. Exit287.7. Test Settings28





7.9. Program Settings	29
7.10. Rescue Disk	31
7.11. Update Scheduling	32
7.12. Event History Log	32
7.13. Language Selection	33
7.14. Potentially Unwanted Programs Exceptions	34
7.15. Information	35
8. AVG Advanced Test Center Interface	39
8.1. Test Manager	
8.2. Scheduled Tasks	40
8.3. Test Results	41
8.4. Program Settings	44
8.5. Update	48
8.6. Rescue Disk	49
8.7. Virus Encyclopedia	49
8.8. Information	50
8.9. Help	50
9. Control Center	52
9.1. Control Center Launch	52
9.2. Control Center Left Menu	53
9.3. Control Center Top Menu	55
9.4. AVG Components in Control Center	56
9.5. Control Center System Tray Icon	56
9.6. Control Center Components	56
9.7. Control Center - Anti-Virus	57
9.8. Control Center - Anti-Spyware	58
9.9. Control Center - Anti-Spam	58
9.10. Control Center - Firewall	59
9.11. Control Center - Scheduler	59
9.12. Control Center - Resident Shield	60
9.13. Control Center - Virus Vault	64
9.14. Control Center - Update Manager	65
9.15. Control Center - Shell Extension	70
9.16. Control Center - E-mail Scanner	74
9.17. Control Center - License	76
10. Firewall	78





10.1. Firewall Control Panel within the Control Center	
10.2. Firewall Deactivation	
10.3. Stopping All Traffic in Firewall	79
10.4. Firewall Actions	80
10.5. Firewall Logging	81
10.6. Firewall Configuration Wizard	84
10.7. Firewall Configuration	
10.8. Firewall Properties	110
11. Anti-Spam	113
12. Virus Vault	119
12.1. Moving Suspect Objects into the Virus Vault	
12.2. Virus Vault Environment	119
12.3. Virus Vault Administration	120
13. Tests Review	
13. Tests Review . 13.1. Complete Test.	122
13. Tests Review 13.1. Complete Test13.2. User Test	
13. Tests Review 13.1. Complete Test13.2. User Test13.3. Selected Areas Test	
13. Tests Review. 13.1. Complete Test.13.2. User Test .13.3. Selected Areas Test .13.4. Detailed Tests .	122 122 134 135 138
 13. Tests Review. 13.1. Complete Test. 13.2. User Test 13.3. Selected Areas Test 13.4. Detailed Tests. 13.5. E-mail Scanner 	122 122 134 135 138 138
 13. Tests Review. 13.1. Complete Test. 13.2. User Test 13.3. Selected Areas Test 13.4. Detailed Tests. 13.5. E-mail Scanner 13.6. Command Line Test Launch 	122 122 134 135 138 138 138 139
 13. Tests Review	
 13. Tests Review	
 13. Tests Review	
 13. Tests Review	122 122 134 135 135 138 138 139 140 140 140 140
 13. Tests Review	122 122 134 135 138 138 138 139 140 140 140 140 140





1. Introduction

The **AVG 7.5 Internet Security** User Manual offers a comprehensive overview of all tasks and detection technologies provided by AVG.

Compared to **AVG Anti-Virus**, the **AVG 7.5 Internet Security** edition offers extended protection to your personal computer due to the <u>Firewall</u>, <u>Anti-Spyware</u> and <u>Anti-Spam</u> components.

1.1. Anti-Virus Detection Technologies and Levels of Protection

The **Anti-Virus** component uses the following technologies to detect computer 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

Where just a single technology might fall short of detecting or identifying a virus, AVG combines several technologies to ensure that your computer is protected.

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* (PUP). Such a program could, for example, be some kind of spyware, adware etc. Upon the user's request, AVG is able to remove such programs or block access to them.

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.

There are many ways a virus can enter your computer. For example, a virus contained in an incoming e-mail message is, upon receipt of the message, activated and stored on your hard disk, from where it can subsequently spread. An antivirus application which concentrates only on a single level of detection might fail in isolating the virus. AVG allows you to perform antivirus checks on multiple levels – such as when you receive your electronic mail, as well as when you are working with files on your computer. You can also perform a check on demand. The following list outlines each level:

a) E-mail Scanner

Checks incoming and outgoing mail by using plug-ins designed for the most frequently used e-mail programs. The **E-mail Scanner** is an additional program for electronic mail monitoring; it can run in fully automatic mode or you can configure it according to your specific needs. The **E-mail Scanner** is designed for applications supporting the POP3/SMTP protocols. When detected, viruses are moved to the **Virus Vault** (where they are quarantined). Some e-mail clients may support messages with text certifying that sent and received e-mail has been scanned for viruses. Another component for an





increased level of security when working with electronic mail is the Attachment Filter, which can be set by defining undesirable or suspect files.

b) Resident Shield

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.

c) Tests

Scanning is a crucial part of AVG functionality. You can run on-demand tests or schedule them to run periodically at convenient times. Within AVG, you will find pre-defined tests, and you can create your own specific tests.

1.2. Firewall Principles

Computers that are not protected by a firewall are an easy target for computer hackers and all kinds of data thieves.

A firewall is a system that enforces an access control policy between two or more networks by blocking/permitting traffic. Every 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 the firewall recognizes any intrusion attempts, it "blocks" the attempt and does not let the intruder access to the computer.

The **Firewall** helps you maintain your privacy and protect your personallyidentifiable 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.

1.3. Anti-Spam Protection

Spam refers to unsolicited e-mail, mostly advertising a product or service that is mass mailed to 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. As spam is not only annoying, but also can often be a source of scams, viruses or offensive content, it is strongly advised to protect your mailbox with Anti-Spam protection.

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

To get more information about **Anti-Spam** features and settings, see chapter <u>11.</u> <u>Anti-Spam</u>.



1.4. Anti-Spyware Protection

AVG 7.5

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.

Ideally, you should prevent spyware and other malware from intruding onto your computer. 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, such as Grisoft's **Anti-Spyware** component 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 up-to-date with the latest database and program updates. For this reason, AVG allows you to fully scan your computer for malware/spyware using the scanning feature. It also detects *sleeping and non-dangerous* malware, i.e. malware that has been downloaded but not yet activated.

1.5. Operating Systems Supported

AVG 7.5 Internet Security is intended to protect workstations with the following operating systems: Windows NT/9x/Me/2000/XP including 64-bit versions.

Note: Some older operating systems like Windows 95/98/ME do not support onaccess scanning of opened files by Anti-Spyware component.





2. Installation

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

Before you start installing AVG, we strongly recommend that you visit the Grisoft website to check for a new installation file. This way you can be sure to install the latest available version of AVG.

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 license/sales number can be found on a registration card in the AVG package. If you have purchased your copy of AVG on-line, your license/sales number was delivered to you via e-mail.

2.1. Installation from the Internet

To install AVG from the Internet, follow these steps:

- Refer to the Grisoft website and download the latest version of the AVG 7.5 Internet Security installation package from the Grisoft website at <u>www.grisoft.com</u>, downloads section.
- b) Download the installation file and save it on your local disk.
- c) Start the installation by executing the downloaded file.





3. Installation Process

3.1. Installation – Welcome Dialog

In the installation welcome dialog you are invited to select the application language.

Note: By default, only two application languages will be installed. The one you select in this dialog and English (the default language). If you select English language, then only English will be installed. You can choose to install additional languages in the **Component selection** dialog (later on in the installation process).

Press the *Next* button to confirm your choice:

AVG 7.5	
	Welcome!
AVG	Welcome to the AVG Setup program. This will install AVG on your computer. Click Next to continue with the Setup, or click Exit to quit now. 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. Before you start the installation process please consult the special <u>FAQ section</u> , providing advice and recommendations that will help you install the program according to your needs and requirements.
	Choose setup language
	Next > Exit

3.2. Installation – License Agreement

The following dialog offers full wording of the license agreement. Read it carefully and approve by pressing the *Accept* button. Otherwise the installation process will be canceled.

Licensing Agreement This is an AVG 7.5 beta version intended for test testing progress and/or results must not be provided t persons that are not involved in this beta testing	ting purposes only. Any information about the
testing results, reviews or evaluations is only possible explicit permission of such actions from the GRIS	process. Any publication of AVG 7.5 beta with OFT company.
This is a Licensing Agreement between you	u, the end user of software, and GRISOFT,
s.r.o. (hereinafter "GRISOFT"). Please read this docu	ment carefully!
In case you do not agree with the said term	is and conditions, immediately stop using this
n order to continue with the installation of AVG you m	ust accept this License Agreement. Do you
cocept the terms of the preceeding License Agreemer	nt?



3.3. Installation – Select Installation Type

In this dialog window you have to select between two types of installation: *Standard installation* and *Custom installation*.

a) Standard Installation

Standard installation will automatically install AVG with the predefined configuration of all its components. If you do not have any specific requirements on configuration of some part of AVG, we strongly recommend that you select this option (you will be able to configure all AVG components setting even after the standard installation is performed).

AVG 7.5	$\overline{\mathbf{X}}$
	Select Installation Type
AVG	Standard Installation (recommended) Installs the product in the standard configuration, which is recommended for most users.
	Custom Installation With options to customize certain parameters during the installation process.
	< Back Next > Exit

Confirm the *Standard installation* option with the *Next* button to enter the *Personalize AVG* dialog where you need to specify your name/company name and your license number:

AVG 7.5	-	$\overline{\mathbf{X}}$
	Personaliz	e AVG
📕 📲 AVG	User Name:	Grisoft
	Company Name:	
	License/Sales Number:	
	You will find your L - in the e-mail sent - on the product re - on the retail pack	icense/Sales Number: to your e-mail address, or gistration card, or age label
		< Back Next > Exit

Confirm the entered license data by pressing the *Next* button to continue to the <u>Installation Summary</u> dialog.

b) Custom Installation





Custom installation is recommended only to experienced users who have specific requirements for AVG components' configuration, and who want to define the configuration settings already during the installation process. However, you will always have the possibility of configuring the AVG components' settings later.



Confirm your choice by pressing the *Next* button to continue to the following dialog of the Custom installation branch:

• Personalize AVG

In the *Personalize AVG* dialog you need to enter your name/company name, and your valid license number:

AVG 7.5	-	X
	Personaliz	e AVG
📕 📲 AVG	User Name:	Grisoft
	Company Name:	
	License/Sales Number:	
	You will find your L - in the e-mail sent - on the product re - on the retail pact	icense/Sales Number: to your e-mail address, or egistration card, or kage label
		< Back Next > Exit

o Destination Folder

In the *Destination folder* dialog you can specify the path to the directory where you want to install AVG. If not specified otherwise, the program will be installed into the predefined directory (see picture). The directory path can either be typed in, or you can select the location from your local disk navigation tree using the *Browse* button.





AVG 7.5	
	Destination folder
avg 📲	Changing the destination folder is not allowed because the AVG has been installed in the folder shown below.
	If you would like to change the destination folder anyway, it will be necessary to uninstall AVG and then reinstall.
	- Destination folder
	Browse
	C:\Program Files\Grisoft\AVG7
	<back next=""> Exit</back>

• Component Selection

In the *Component selection* dialog you can define what AVG components should be installed. By default, all available components are selected and will be installed. We recommend that you keep these settings unless you have an actual reason to change it. If no component is selected, the program will be uninstalled.

Note the *Additional installed languages* item, where you can select one or more additional language packs. By default, only English language and the language selected at the beginning of the installation process are installed.



• E-mail Scanning

In the *E-mail Scanning* dialog you can select one of two options for your electronic mail monitoring:

- Recommended Configuration

AVG allows you to scan your electronic mail using the program plugin for the most frequently used e-mail programs: MS Outlook, MS





Exchange, The BAT!, Qualcomm Eudora. If you use any of these email programs the setup will automatically detect it, and recommend you to install a direct plugin for your e-mail client (see picture).

AVG 7.5	
	E-mail Scanning
AVG	The installer has detected that Microsoft Outlook is set as your default e-mail application. Select Microsoft Outlook to install e-mail scanning for this e-mail application, or select Advanced Configuration to set up e-mail scanning manually.
P	 Microsoft Outlook (recommended) Installs the antivirus plugin for the e-mail application Microsoft Outlook.
	 Advanced Configuration Manually configure e-mail scanning.
	< Back Next > Exit

For other e-mail programs, AVG will provide comprehensive e-mail scanning using the **E-mail Scanner** component. In that case the setup dialog offers the recommended option of **Personal E-mail Scanner**.

Confirm the configuration by pressing the *Next* button, and continue to the Installation Summary dialog.

• Advanced Configuration

If you want to configure the e-mail scanning manually, select the *Advanced configuration* option. This option is recommended to experienced users only!

The configuration itself can be performed within the following dialog:



You can select a plugin for the specific e-mail program you use. If your





e-mail program is not directly supported, select the *Personal E-Mail Scanner* option.

Note: E-mail Scanner will be installed and run in fully automatic mode. Its configuration can be set up manually– for a detailed description refer to the E-mail Scanner supplementary documentation, to be downloaded from the downloads section of the Grisoft website at <u>www.grisoft.com</u>.

Press the *Next* button to confirm your choice, and to continue to the <u>Installation</u> <u>Summary</u> dialog.

3.4. Installation – Installation Summary

The *Installation summary* dialog offers an overview of all installation parameters.

AVG 7.5		
	Installation Summary	
AVG 📲	Please review the information below to confirm that it is correc Click Finish to complete the installation, or click Back to modify settings.	t. yany
	Destination folder for AVG files: C:\Program Files\Grisoft\AVG7	
	License: Licensed user: Grisoft	
	Company name:	ш
	License type: full	~
	< Back Finish Exit	

3.5. Installation – Application Termination

Some of the programs that are currently running on your PC may conflict with the AVG installation process.

AVG 7.5	$\overline{\mathbf{X}}$
	Applications Termination
AVG	The following applications must be terminated prior to installation. Press Next to terminate these applications, and begin installation.
	The Bat
	< Back Next > Exit





In that case, another *Application Termination* window opens providing a list of programs that must be closed in order to finalize the installation. You can close the listed programs manually, or they will be closed automatically by the setup after pressing the *Next* button:

3.6. Installation – Installation Complete

WG 7.5

The installation process is finalized with the *Installation complete* dialog. By default, the *Restart the computer now* option is marked, and we highly recommend keeping it marked. Confirm your choice by clicking the *OK* button.

Before your PC restart, the <u>Firewall Configuration Wizard (Chapter 10.6)</u> will be launched – although the possibility of **Firewall** configuration editing is available at any time during your work with AVG, we highly recommend that you take the configuration wizard's tour and define the Firewall settings in an easy way.



Note: Should the installation process fail for some reason, the last dialog window will also provide the Details button. Press the button to see the diagnostic data overview. The diagnostic data, and the AVG7INST.LOG installation logging file information (saved in the TEMP system directory) will help you solve the problem.

Once the installation process is over, the *Firewall Configuration Wizard* will open automatically and offer you the option of setting up the default Firewall configuration in an easy way. You can decide to omit the wizard's services but it is strongly recommended to use this option. For detailed description please refer to chapter <u>10.6 – Firewall Configuration Wizard</u>.





4. AVG First Run

4.1. First Run Wizard

When you first install AVG on your computer, the **AVG First Run Wizard** pops up to help you with initial program 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:

4.1.1. First Run Wizard – Welcome Screen

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:

📕 AVG - First Run	Wizard
	CONGRATULATIONS!
AVG	AVG has been successfully installed. A few simple steps remain to ensure your maximum protection. This First Run Wizard will guide you through the following recommended steps:
	- Perform AVG update - Create Rescue Disk - Scan your computer for viruses
	Clicking "Next" at any of the following steps will allow you to skip it. Of course, you can perform any step at a later time.
2	Next 2>

Note: From Windows XP onwards the rescue disk feature is not supported any more.

4.1.2. First Run Wizard - AVG Update

The **AVG Update** window will automatically check and download the latest AVG updates. Click on the **Check for Updates** button to download the latest update files and perform the update:





4.1.3. First Run Wizard - Daily Scanning

The *Daily Scanning* window invites you to decide what priority level should be assigned to the daily scheduled complete test of your computer. It is recommended that you keep the default settings. Confirm your selection by simply pressing the *Next* button:

🛃 AVG - First Run Wizard	? 🗙			
Daily Scanning Set the priority level for the scheduled daily scan	ġ.			
For maximum security and simplicity a full computer scan is scheduled daily. Here you can change the priority level of the scan.				
Contraction of the second s				
C High Priority - faster, but may slow down computer during scan				
☑ Enable Scheduled Daily scan (recommended)				
Image: Second secon	(t <u>></u> >			

4.1.4. First Run Wizard - Virus Scan

The *Virus Scan* window will launch a complete test, and treat any viruses that may be found. Click on the *Scan computer!* button to start scanning:

📕 AVG - First Run Wizard	? 🗙
Virus Scan Would you like to scan your computer, now?	ġ:
The virus scan tests your computer for viruses. All system areas, a as all files on your hard drives will be checked. If a virus is found, AVG will attempt to automatically heal the infect or move the file to the Virus Vault, where it is quarantined to be de at a later time.	s well ed file alt with
Scan computer!	ext <u>>></u>

4.1.5. First Run Wizard - Your Computer Is Protected

Now your computer has been scanned, and your AVG is configured properly. Press the *Continue* button to start working with AVG:







4.2. AVG Program Start

Next time you want to open the program you can do so:

- by double clicking on the AVG icon created on your desktop
- from the Start menu:

Start/All programs/AVG 7.5/AVG Control Center

from the context menu of the Control Center system tray icon





5. After Installation

To secure the maximum anti-virus protection level we recommend that you perform the following steps after AVG installation:

5.1. Running the Complete Test

There is a potential risk that a computer virus has been transmitted to your computer prior to AVG installation. For this reason you should run the *Complete Test* to scan the whole of your computer for possible infections. If you have gone through the *First Run Wizard* recommended actions, your computer has been already scanned automatically, and you may as well skip this paragraph.

For further information on the Complete Test refer to chapter 13.1 - Complete Test.

5.2. Setting up the On-Close Scan

It is recommended to activate the *On-Close Scan* in the **Resident Shield** component. The on-close scanning ensures that AVG will scan active objects (e.g. applications, documents ...) when they are being opened, and also when they are being closed. This component helps you prevent your computer from some kind of sophisticated virus.

You can activate the on-close scanning within the **Resident Shield** panel in the **Control Center**.

For further information about the on-close scanning option refer to the chapter <u>9.12</u> <u>Components controlled from Control Center/Resident Shield</u>.

5.3. Eicar Test

To check whether AVG has been installed properly 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 the testing file, the *Resident Shield* will react to it with a warning. This Resident Shield notice demonstrates that AVG is properly installed on your computer.

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

5.4. Test and Update Scheduling

To ensure your computer is virus-free, it is crucial to set up the regular AVG test/updates schedules.

• **Test** - a Complete Test should be scheduled on a workstation at least once a week; for instructions on test scheduling refer to the <u>13. Test Review</u> chapter





• **Update** – AVG installed on a workstation should have the update scheduled approximately once a day; for instruction on update types and scheduling refer to the chapter <u>14. Program Update</u>



Copyright (c) 1992-2006 GRISOFT, s.r.o. All rights reserved.



6. Product Registration

Once you have completed AVG installation, you should register your product to be able to gain full access to AVG Technical Support, the AVG Update newsletter, and other services provided by Grisoft exclusively for registered users.

Note: Customers who have purchased their AVG in the Grisoft online shop have been registered automatically and do not need to register again.

To register your AVG:

• You can go directly to the Grisoft website at <u>www.grisoft.com</u> and follow the *Register AVG* link

or

• In your AVG user interface select from the main menu:

Information/Register online - to get to the Grisoft registration web page.

- Enter your Sales/License number into the empty field (make sure you keep to the exact form of the license number (upper/lower case, spaces, etc.)
- Press the *Submit* button to confirm your registration





7. AVG Basic Test Center Interface

After you have successfully installed AVG on your computer, the AVG icon will appear on your Windows desktop. Double-click the icon to launch the **Test Center**. AVG provides two variations of the **Test Center** interface – *Basic* and *Advanced*.

The **Basic Test Interface** provides access to most AVG protection features: updating, scanning, task scheduling, and basic program configuration. The features provided by both interfaces are similar, with the major difference being in the range of available settings and the availability of advanced features, such as the creation of test and update schedules. If you like simplicity, choose the **Basic Test Interface**.

The Basic Test Interface is recommended for less experienced users who want to take advantage of maximum virus protection with limited need for user intervention.



Additionally you can check the *Security status* of AVG in the Test Center top section. There are three possible signs:

- Your computer is fully protected, up to date and all installed components are working properly
- One or more components are incorrectly configured and you should pay attention to their properties/settings. The problem components will be listed in the status error message.

Indicates, that you have decided to ignore the reported faulty status of one of the components.





Note: To quickly open the Control Center, simply double click the Security status section.

To switch to the Advanced Test Interface you can use the shortcut Switch to Advanced button in the left menu. Or select from the top menu Program/Switch to Advanced Test Interface.

By default, in the *Basic Test Interface* you will find shortcut links (left menu) - see their descriptions in the following chapters.

Note: However, the menu items list can be modified, for details refer to chapter <u>8.4</u> <u>*Program Settings/Customize*</u>.

7.1. Switch to Advanced

The *Switch to Advanced* shortcut button allows you to switch between the *Basic/Advanced Test Center* interface of AVG.

For further description of the *Advanced Test Center* interface, refer to chapter<u>8</u>. <u>AVG Advanced Test Interface</u>.

7.2. Control Center

The *Control Center* shortcut button launches the Control Center – a central controlling application of AVG; from the Control Center you can review, configure, and fully administer the whole AVG program.

For further description of the **Control Center** refer to the <u>9. Control Center</u>.

7.3. Virus Vault

The *Virus Vault* shortcut button launches the Virus Vault – a safe environment for storing and further treatment of infected objects.

For further description of Virus Vault refer to chapter <u>12. Virus Vault</u>.

7.4. Test Results

The *Test Results* shortcut button provides an overview of recently run tests and their results:

- Test name full name of the run test
- Date date of the test launch
- Time exact time of the test launch
- Objects total number of objects scanned
- Viruses total number of viruses detected
- Errors total number of errors occurring







You can further review detailed test result information for any listed test using the operating buttons in the bottom section of the **Test result** dialog window:

a) Details

The **Details** button opens a new dialog window with detailed information about the selected test and its results. The data are divided into two sections: **General properties** (test parameters and test results) and **Object summary** (scanned objects and findings statistics):

General propertie:	8	Object summary	
Report name:	Selected Areas Test	Scanned:	1244
Start time:	7.9.2006 9:02:06	Infected:	1
End time:	7.9.2006 9:03:57 (total: 1:50.7 Min)	Cleaned:	0
Launch method:	Scanning launched manually	Moved to vault:	0
Scanning result:	Viral infection found	Deleted:	1
Report status:	Scanning stopped manually	Errors:	0

This dialog window operation buttons are:

Test configuration – opens a new dialog window with the test settings overview (For detailed information on specific test settings options please refer to 11. Test Review chapter)

www.grisoft.com

• Close – closes the Test report – more details dialog window



b) Test Configuration

The *Test configuration* button provides a new dialog window with information on the test set parameters used: test name and description, scanned files information, scanning properties, and other scanning parameters:

📕 Used Test configu	ration - "Complete Test"		? 🗙
Test name and description	n Complete Test		
Scanning parameters: —			
Local hard drives			-
Jex -		<u></u>	elect
Scan files without int	erruption al infected files		
Scanning properties Scan System Areas I Detect Potentially Ur Use heuristic Analysi Scan inside archives	efore the test starts wanted Programs and Spyware s		
 File extensions C Scan all files S Scan all infectable file 	25	S	elect
2			Close

c) Remove

The *Remove* button will delete the highlighted test result from the list.

d) Content

The *Content* button opens an overview of detailed test result information for the selected test: location of the infected scanned file, result (finding specification), and status of the infected file:







This dialog window is divided into several tabs.

• *Results overview*

In this tab, you will find detailed testing statistics and summaries.

• Virus results

This tab is only displayed if there is a virus infection found during the testing process. The tab lists all viruses found .

Selected Areas Test (9/7/2006 10:40:10 AM)			
Result overview Virus results Spyware found			
Object	Result	Status	
C.\Documents and Settings\dolejsekm\My Documents\		Deleted	
	1	B	ack



The dialog's operation buttons are:

- *Heal* allows you to heal the infected object if the cure for this kind of infection is available.
- Move to Vault moves the selected infected object into the Virus Vault.
- **Details** opens the Virus Encyclopedia to provide information on the detected virus.
- **Back** closes the detailed **Test result** dialog.

Note: Buttons will only be displayed for operations that are possible on the virus selected in the list. I.e. If the selected virus has already been automatically deleted during the scan, (as shown above) then it cannot be healed or moved.

• Spyware found

VG 7.5

This tab is only displayed if there is a spyware/malware infection or an Internet tracking cookie is found during the testing process. The tab lists all such threats found.

Test Result Selected Areas Test (9/7/20	006 10:40:10 AM)	
Result overview Virus results Spyware found		
Object	Result	^
Not-A-Virus. Test. Trojan Simulator Family	Not-A-Virus. Test. Troja	
C:\Documents and Settings\dolejsekm\My Documen	Not-A-Virus.Test.Troja	_
TrackingCookie.Myaffiliateprogram Family	TrackingCookie.Myafl	
C:\Documents and Settings\dolejsekm\Cookies\dolej	TrackingCookie.Myafl	
C:\Documents and Settings\dolejsekm\Cookies\dolej	TrackingCookie.Myafl	
C:\Documents and Settings\dolejsekm\Cookies\dolej	TrackingCookie.Myafl	
👔 C:\Documents and Settings\dolejsekm\Cookies\dolej	TrackingCookie.Myafl	
👔 C:\Documents and Settings\dolejsekm\Cookies\dolej	TrackingCookie.Myafl	_
C:\Documents and Sattings\dolaisekm\Cookies\dolai	TrackingCookie Muafl	×
Move to Vault Add to exceptions	<u>D</u> etails <u>B</u> ack	

The Dialog's operation buttons are:

- Move to Vault moves the selected infected object into the Virus Vault.
- Add to exceptions adds the selected Potentially Unwanted Programs (or spyware/malware) to the list of Exceptions. Then the selected program(s) will again be fully working and AVG will ignore them in future scans. More information on this topic can be found in the <u>Potentially Unwanted Programs Exceptions (Chapter 7.14)</u> section.
- Details opens the Virus Encyclopedia to provide information on the detected infection.
- **Back** closes the detailed **Test result** dialog.

Note: Buttons will only be displayed for operations that are possible on the malware selected in the list.

e) Close





The *Close* button terminates the *Test results* window.

7.5. Check for Updates

The *Update* shortcut button launches a window offering an immediate update of AVG.

For further information on the update possibilities refer to the chapter <u>14. Program</u> <u>Updates</u>.



The dialog operating buttons are:

- Internet launches AVG update from the Internet
- **Folder** opens a dialog window where you need to specify the update source directory (either local or network); press the **OK** button to confirm selection and launch the AVG update
- Cancel closes the Update dialog window

If you want to use the same update files source repeatedly select the **Do not ask** for the update source next time option. Within the next update you will not be asked for the update source specification any more, and the update will be performed automatically from the source you have specified.

In the future, if you wish to restore the update source specification in the **Update** dialog, you can do so within the **Update Manager** component in the Control Center – for a detailed settings description please refer to chapter <u>9.14 – Control Center – Update Manager</u>, **Properties** section.

7.6. Exit

The *Exit Program* shortcut button closes the **Test Center** application.

Besides the shortcut links, the upper menu of the Basic Test Interface further offers the following options:

7.7. Test Settings

Tests/System Areas Test settings (alternatively other test settings)

Within this section you specify your own parameters for the AVG tests by default preset by the vendor.





For a detailed test settings description refer to the <u>13. Test Review</u>.

7.8. Test Scheduling

Tests/Schedule a Test

In the *Basic Test Interface* the test scheduling options are rather limited. You can only schedule the test (Complete Test or User Test) launch once a day. You can specify the exact time of the test launch, and decide whether the test should be run after the user logs on if missed at the scheduled time:

📕 Schedule Daily T	est	? 🗙
Scheduled time	heduled antivirus test	
Start daily at	08:00	
🔽 If missed, start imme	ediately when user logs on	
Schedule		
Complete Test		
C User Test		
2	ок с	Cancel

We recommend using the *Advanced Test Interface* for further test scheduling.

For detailed Advanced Test Interface test scheduling options please refer to chapter <u>8.2 Scheduled Tasks</u>.

7.9. Program Settings

Service/Program settings

The *Program settings* section allows you to specify some general AVG options on separate tabs. However, the Basic Test Interface possibilities are also rather limited:

a) Program

• For how long you want to store the test results, and how many of them

- How many recent test results shall be displayed in the *Basic Test Interface* menu
- What test results time sorting you prefer





Program Settings				? >
Program Keyboard Customize				
Test Results Maintenance				
Delete Test Results after:		60 ÷	days	
Store last:		1000 🕂	Test Results	
Test Results displayed in Results menu				
Show last:		20 🕂	Test Results	
Sort Test Results:				
C descending				
• ascending				
Display a notification balloon when component status changes				
2	OK	Cance	A	eply

b) Keyboard

The *Keyboard* tab allows you to define your own keyboard shortcuts to be used in the AVG environment:

Program Settings			? 🗙
Program Keyboard Customize			
Program		Shortout key:	
Switch to Advanced Interface Launch AVG Virus Vault		None	
Launch AVG Control Center Export List to File	Ctrl+S	≣ <u>A</u> ssign short	cut key
Print Exit	Ctrl+P Alt+F4	Bemove shore	tcut kev
Start System Areas Test	F3	1 ======	
Scan Computer - Complete Test Scan Selected Areas Scan User Defined Path - User Test	F4 F5		
System Areas Test settings	Ctrl+F3		
Complete Test Settings Selected Areas Test Settings User Test Settings	Ctrl+F4 Ctrl+F5	Export key de	efinitions
		Import key de	efinitions
		4.1	
?	OK	Cancel	Apply

c) Customize

The *Customize* tab allows you to define what AVG functionality you want to have available in **Test Center/Control Center** via the shortcut links:





Program Settings Program Keyboard Customize AVG Test Center Available buttons		Selected buttons	2 × -
Available buttons AVG Help Language Selection Program Settings Rescue Disk Wizard Scheduler Test Manager	Add -> <- <u>R</u> emove	Switch to Advanced Control Center Virus Vault Test Results Check for Updates Exit	
If you click on the button list, its description	Move <u>Up</u> Move <u>D</u> own n appears here. Ho OK	wever no button has been selected yet	t.

We recommend using the *Advanced Test Interface* options for further program configuration.

For detailed program configuration options available in the AVG Advanced Test Interface please refer to chapter <u>8.4 Program Settings</u>.

7.10. Rescue Disk

Service/Rescue Disk

From Windows XP onwards the rescue disk feature is not supported any more.

The **Rescue disk** will help you scan and clean files on your computer and restore system areas in MS-DOS mode (from the command prompt) but it is basically only intended for the OS Windows 9x/Me.

This function is useful when you need to remove viruses from a computer:

- that has a sharing violations problem
- to which you do not have sufficient access rights
- that has its system areas infected

The **Rescue Disk** menu item launches a wizard that will lead you through the process of creating a rescue disc. To create the Rescue Disk follow the wizard's instructions:





7.11. Update Scheduling

Service/Schedule an Update

In the *Basic Test Interface* the update scheduling options are rather limited. The update can only be scheduled once a day. You can specify the exact update time, and decide whether an update should be launched after the Internet connection is restored (if missed at its scheduled time):

📕 Schedule Daily Update		? 🗙
Scheduled download time Periodically check for Internet upo	lates	
Check daily betwe	een 8:00 AM and 9:5	59 AM 💌
✓ If Internet connection is not available	ble, check when it g	joes on-line
?	ОК	Cancel

For further update scheduling configuration we recommend using the *Advanced Test Interface* options.

For detailed Advanced Test Interface update scheduling options please refer to <u>8.2</u> <u>Scheduled Tasks</u>.

7.12. Event History Log

Service/Event History Log

Within this section you can find a summary of important events that occurred during AVG operation.

Event History Log records the following types of events:

- Information about updates of the AVG application
- Test start, end or stop (including automatically performed tests)
- Events connected with virus detection (by Resident Shield or scanning) including occurrence location





• Other important events

Pressing the Export history button will allow you to save the history log in XML format. All records can be deleted by clicking the Delete history button.

📕 AVG 7.5 Internet Security - T	est Center - Basic Interf	ace						
Program Tests Results Service In	formation							
AVG Internet Security	Security status You are fully protected. Your system is up to date and all installed components are working properly.							
🖄 Switch to Advanced	Event His	tory	Log					
11 Control Center		- T						
III Virue Vault	Date and time	Source	User	Event description				
	8 2006/09/12 08:01:14	Virus	SYSTEM	In C:\Documents and Setting				
Test Results	8 2006/09/12 08:01:14	Virus	SYSTEM	In C:\Documents and Settin				
	12006/09/12 08:03:23	General	SYSTEM	Complete Test stopped. Fou 👝				
🥏 Check for Updates	👷 2006/09/12 10:03:37	Update	SYSTEM	Update successfully done. (i 💌				
X Exit	Export Log Delete L	.og		<u>C</u> lose				
For Help press F1 7.5.414 268.12.3/445 2082 11.9.2006 20:45								

7.13. Language Selection

Service/Language selection

This option allows you to select the language you want to use; and if desired set the selected language as the application's default language:

Note: By default only English language and the language you selected during the installation process are installed. You can run the <u>installation process (Chapter 3)</u> again at any time and choose additional languages in the Component selection dialog.







7.14. Potentially Unwanted Programs Exceptions

Service/Potentially Unwanted Programs Exceptions

This item activates the dialog window for defining exceptions for *Potentially Unwanted Programs (PUP)*.

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*:

- AVG 7.5 Internet Security - Test Center - Basic Interface					
Program Tests Results Service In	formation				
AVG Internet Security	Security status You are fully protected. Your system is up to date and all installed components are working properly.				
Switch to Advanced	Potentia	lly Un	wanted Programs Exceptions		
I Vinue Mault	File	File Path	Checksum		
	C:\KLARA\		73b78ea08982ad3e721a347d453fdd7c		
Test Results					
Theck for Updates					
🛛 Exit			ini ini		
	Edit	<u>R</u> emove	<u>N</u> ew	<u>C</u> lose	
For Help press F1			7.5.414 268.12.3/445 2082 11.9.	2006 20:45 🏑	

All already defined and currently valid exceptions are listed within this dialog. You can add a new exception by clicking the New button. You can also change existing exceptions, by using the Edit button. By clicking the Remove button, you will delete the currently selected exception.

a) Defining a new exception for Potentially Unwanted Program

By pressing the *New* button, you can manually define a new exception:

📕 Excepti	n Definition 🔹 👔 🔀					
File:	C:\Documents and Settings\dolejsekm\My Documents\avg75f_4130798.exe					
	Any location - do not use full path					
File Info:	Extended file information not available.					
	Cause: File does not contain version information.					
Checksum:	/					
CHECKSUIII.	[Kundenned/					
2	Add Cancel					

In the *File* field, type the full path to the file that you want to mark as an exception. If you want to define this file as an exception only for the specific





location, then leave the checkbox *Any location – do not use full path* unchecked.

If you tick the checkbox, then the selected file (and any copies of the file) will be defined as an exception, no matter where they are actually located. You still need to fill in the full path to the specific file, since this will be used as the sample file (just in case more than one 'different' file with the same filename exists on your computer).

You can alternatively click this button ... to open a standard explorer dialog for easier location of the desired file.

If there is any additional information available about the file (license/version information etc.), it will be displayed within the *File info* section.

The *Checksum* field 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.

To confirm and save the new exception, click the Add button.

b) Editing an existing Potentially Unwanted Program exception

By pressing the *Edit* button, you can manually edit an existing exception:

📕 Excepti	on Definition 🔹 👔 🔀				
File:	C:\Documents and Settings\dolejsekm\My Documents\avg75f_413a798.exe				
	I▼ Any location - do not use full path				
File Info:	Extended file information not available.				
	Cause: File does not contain version information.				
Checksum:	c1a1ba827717706d8f35165ac37d572e - MODIFIED				
2	Re-Validate Cancel				

During editing of the existing exception, the <u>Checksum</u> field might appear as MODIFIED. It means, that the file has been changed since its addition and does not correspond to the originally generated checksum. If you want to mark the edited file as a exception, press the *Re-Validate* button.

7.15. Information

Information/...

Within this section you can find general AVG product and support related information:

a) About AVG, Contacts

Both these options launch a new window with five tabs providing AVG information:



- Program provides information about the AVG Basic Test Interface
- *Version* provides AVG version information and AVI database version information
- **System** provides information on the current status of the operating system
- License Agreements provides full wording of the AVG License agreement
- *Contacts* provides an overview of the AVG vendor and AVG business partners contact information

Information	? 🗙
Program Version System License Agreement Contacts	i
Test Center - Basic Interface	
File version: 7.5.0.414	
The Basic Interface provides access to the most used features of AVG. This includes updating, testing, scheduling and ba configuration options. Its ease of use makes it ideal for users who need maximum virus protection with limited user intervent necessary.	isic tion
	ose

b) Virus Encyclopedia

The Virus Encyclopedia option opens an online encyclopedia of known viruses with the possibility of searching for an information on specific viruses.

The Virus Encyclopedia is available online only; you must be connected to the Internet to be able to use it.



GRISOFT




c) Technical support by e-mail

AVG Diagnostics is a supportive diagnostic utility distributed by AVG Technical Support. Its main purpose is to obtain information from the host computer. This information helps the Technical Support team to solve your problem with AVG by analyzing the collected logs, error reports, system information, suspicious files, your own comments and other data.

To learn more about **AVG Diagnostics** utility proceed to chapter <u>15.1 AVG</u> <u>Diagnostics utility</u>.

Note: Under no circumstances does the AVG Diagnostics utility send any personal or other sensitive data from your computer without the user's explicit permission. The user is able to check the content of all collected files and to prevent any of them from being sent to AVG Technical Support.

d) Register on the web

This option opens the AVG registration web page.

e) Activate AVG

This option launches a window asking you to type in your license number to active your AVG.

📕 Activate AV	G ? 🔀
	Enter your AVG License Number and personal/company information.
License Number:	XXXXXX-XXXXX-XXXXXXXXXXXXXXXXXXXXXXXXX
User Name:	GRISOFT, s.r.o.
Company:	GRISOFT, s.r.o.
License Number:	
2	<u>A</u> ctivate <u>B</u> ack

f) Help topics

This option launches an overview of help structure, help topics, and enables quick search within the help themes.





Help Topics: AVG 7.5	? 🗙
Contents Index Find	
Click a book, and then click Open. Or click another tab, such as Index.	
📚 Basic Information	_
🔷 🔷 AVG System Menu	
AVG for Windows Selected Features	
🔷 AVG Control Center	
🔷 AVG Virus Vault	
1	
Open Print Ca	ancel
Open Princ	meer

g) AVG Help

This option launches a new window with brief topic-related help.





8. AVG Advanced Test Center Interface

The *Advanced Test Interface* offers all AVG functions (scanning, updating, task planning, full configuration), and at the same time gives you greater control over all parts of AVG.

The *Advanced Test Interface* use is recommended to experienced computer users.



Additionally you can check the *Security status* of AVG in the Test Center top section. There are three possible signs:

- Your computer is fully protected, up to date and all installed components are working properly
- One or more components are incorrectly configured and you should pay attention to their properties/settings. The problem components will be listed in the status error message.

~

Indicates, that you have decided to ignore the reported faulty status of one of the components.

Note: To quickly open the Control Center, simply double click the Security status section. To switch to the Basic Test Interface, select from the top menu Program/Switch to Basic Test Interface.

In the Advanced Test Interface menu you will find the following items:

8.1. Test Manager

The *Test manager* menu branch contains a list of pre-defined tests that can be run using AVG. You can launch any of these tests from here.

www.grisoft.com

For further information on test types refer to chapter 13. Tests Review.



8.2. Scheduled Tasks

AVG 7.5

The *Scheduled tasks* menu branch contains a list of planned AVG tests/AVG updates.

Double click the menu item to open a new *Scheduled tasks* dialog window:

Scheduled	Task	S	P
Name	Туре	Last start	Next start
💑 Test plan in basic mode	Test	7.9.2006 8:00:00	8.9.2006 8:00:00
🐻 Update plan in Basic mode	Update	7.9.2006 8:52:00	8.9.2006 between 8:00 and
🖲 Anti-Spam rules update	Anti-Spam	7.9.2006 9:58:00	7.9.2006 11:58:00
<	III.		>
			0

This dialog window provides a more in-depth description of each of the planned tasks:

- Name the full name of the planned task
- Type type of the planned task (update/test/Antispam)
- Last start when the task was performed last time (date and time)
- Next start when the task will be performed next time (date and time)
- Status indicates the task settings status
- Scheduled for for whom is the task scheduled

The bottom section of the window offers buttons you can use to add/edit the planned tasks:

a) New Schedule

The *New schedule* button opens a *Scheduled task properties* dialog window where you can define a new task and its parameters on four tabs:

Scheduled task	properties			? 🔀
ask Perform task	Action to take If	missed		
N	l la data alau			
Comment	jopuale plan			
	,			
Schedule	Update			-
Schedule options	Optional update			•
C Schedule for al	users			
Schedule for ci	irrent user only			
Disable this task				
		- 1		
4	OK	·	Cancel	Apply





Task – specify the task *Name* and *Comment* (optional description), task type - *Schedule* (Test/Update/Anti-Spam rules update) and if available also *Schedule options* (priority for Updates and type of test for Tests).

You can also decide whether the task is scheduled for all users or the current user only.

Note: To schedule the task for the current user only means the task will be launched from the Control Center after the respective user logs in. If you want to make sure the task will be launched even if nobody is currently logged in on the PC, it is recommended to schedule the task for a station; the task is then launched by the Alert Manager component and does not rely on the Control Center running.

Tasks that use the network drives (e.g. update run from within the network drive, or network drives test) must be planned for the current user only, and not for the station. The reason is that the Alert Manager runs under the Local System account and is not able to see the network drives. (This problem only applies to the Win NT system, i.e. Windows 2000, Windows 2003, Windows XP PRO etc..; it does not apply for Windows 95, Windows 98, Windows ME a Windows XP Home.)

You can tick *Disable this task* checkbox to disable the task processing.

- **Perform task** define the task periodicity, exact timing, and start/end date
- **Action to take** decide whether you want to be notified before the task starts
- *If missed* select what action shall be taken if the task launch has been missed

b) Edit Schedule

The *Edit schedule* button opens the same dialog window for a defined task, i.e. the task name and necessary parameters are defined already, and you have a chance to edit them.

c) Delete

The *Delete* button will remove the selected (highlighted) task from the list of tasks in the *Scheduled tasks* dialog window.

d) Close

The *Close* button quits the *Schedule tasks* dialog window.

8.3. Test Results

The *Test Results* menu branch contains a list of recently run tests, their parameters, and results.

Double click on the *Test Results* menu item to open a new window *Test Results* dialog window:





Test Results					
Test name	Date	Time	Objects	Viruses	Errors
Selected Areas Test	7.9.2006	9:02:06	1244	1	0
Complete Test	7.9.2006	9:05:53	4910	19	0
🖹 Complete Test	7.9.2006	9:09:07	590	0	0
🖹 Complete Test	7.9.2006	9:09:40	53	0	0
🗟 Complete Test	7.9.2006	9:09:56	13635	14	0
📓 Complete Test	7.9.2006	9:19:28	71878	19	0
? <u>D</u> etails	<u>I</u> est Config	uration	<u>R</u> emove	<u>C</u> onten	t <u>C</u> lose

This dialog window provides more in-depth information on the run tests:

- Test name the full name of the test performed
- **Date** the date when the test was performed
- *Time* the exact time when the test was performed
- Objects number of objects scanned
- *Viruses* number of viruses found (if there is a virus found, the test's icon in the list of tests appears red; if the scanning is interrupted, the test's icon appears as though torn apart)
- *Errors* number of errors occurring during scanning

Note: For further information on the test results please consult chapter <u>13.1</u> <u>d) – Complete Test - Results</u>. This chapter describes warning messages informing of suspect object detection during the test run, detection of infected archives, and the embedded file treatment possibilities, and displayed test results filtering possibilities.

The bottom section of the window offers the following operating buttons:

a) Details

The **Details** button opens a new window with detailed report of the selected test:

General propertie:	8	Object summary	
Report name:	Selected Areas Test	Scanned:	1244
Start time:	7.9.2006 9:02:06	Infected:	1
End time:	7.9.2006 9:03:57 (total: 1:50.7 Min)	Cleaned:	0
Launch method:	Scanning launched manually	Moved to vault:	0
Scanning result:	Viral infection found	Deleted:	1
Report status:	Scanning stopped manually	Errors:	0

b) Test Configuration

The *Test configuration* button opens a window with a report of the performed test configuration settings. Within this window you can specify





various parameters of the test divided into groups represented by the left menu branches:

- Test properties general description of the test
- Objects to scan define what object should be scanned during the test run
- **Scan details** define use of scanning methods; by the file extension you can specify objects that should/should not be scanned; and also you can decide whether archives should be scanned
- *Report* select which specific situations occurring during scanning should be reported
- Action to take define what should be done if a virus is found/if a warning is displayed
- Advanced settings specify parameters of the scanning message windows; decide whether the Control Center should be closed once scanning is finished; specify test priority and define gaps during scanning

📕 Used Test configuration - "Se	elected Areas Test"		? 🔀
Test properties Scan details — Report — Action to take — Advanced settings	Test properties Name: Description: Based on:	Selected Areas Test Predefined test	
	When finished, displa with test result with test statistics	y dialog sult when no virus was detected	
		ОК	Cancel

c) Remove

The *Remove* button deletes the selected (highlighted) test results from the list in the *Test Results* window.

d) Content

The *Content* button opens an overview of detailed test result information for the selected test. For more information on the dialog, consult chapter <u>7.4 Test</u> <u>Results, section d</u>).

www.grisoft.com

e) Close

The *Close* button quits the *List of Test Results* dialog window.





Note: For further information on the test results please refer also to chapter <u>13.1</u> <u>Complete Test - d) Complete Test - Results</u>.

8.4. Program Settings

The *Program settings* branch opens a dialog with several tabs where you can define specific program parameters:

- a) Program
 - o Test Results Maintenance section
 - Delete Test Results after specify for how long you want to store the test results
 - Store Last specify how many last test results you want to store
 - o Test Results Displayed in Menu section
 - Show last specify how many recent test results are displayed in the Test results branch of the Advanced Test Interface menu
 - Sort test Results define what test results sorting you prefer

You can also select the option *Display a notification balloon when component status changes*.

elete Test Results after:	60 🕂 days
tore last:	1000 🕂 Test Results
est Results displayed in Results menu	
how last:	20 🕂 Test Results
ort Test Results:	
G descending	
• ascending	
Display a notification balloon when co	mponent status changes

b) Tests

System Areas Test section – specify the name and location of the System Areas Test results database





Program Sett	ings			1
Program Tests	Startup Date and	time Control Tree	Keyboard Customize	
System Areas T	l est			
Database cont	aining the status of sc	anned files		
C:VAVG7QT.D	AT			
0. 7.				

c) Startup

Scan System Areas – decide whether you want to run the System Areas Test at AVG launch

Program Sett	ings			? 🗙
Program Tests	Startup Date and g AVG m Areas	I time Control Tree	Keyboard Customiz	

d) Date and Time

- o Date and Time Format section
 - **Date and Time** select the preferred way of date and time display (when the date and time values are being displayed together)
- Single Value Format section
 - Date select the preferred way of date display
 - Time select the preferred way of time display





rogram Setti	ngs		?
ogram Tests	Startup Date and time Cor	trol Tree Keyboard Customize	
Date & time form	at		
Date and time:	<date> <time></time></date>	▼ 7.9.2006 13:40:01	<u>[</u>]
Single value form			
Date:		- 7.9 2006	
0.0.0	pregional system settings	11.3.2000	
Time:	regional system settings	▼ 13:40:01	
1	0	K Cancel	Applu
	U	Cancer	ABbill

e) Control Tree

st Manager branch Display date on which the last Tes			
Display date on which the last Tes	A		
	st was run		
heduled Tasks branch			
Display date on which the last sch	eduled task wa	as launched	
Sort tasks by launch date			
st Results branch			
Display number of infected files			
Display test name with test results			
Sort Test Results by date and time			
🙆 ascending			
C descending			
ow last	20	📑 Test F	lesults
	Ø		

- o Test Manager Branch section
 - Display Date on Which the Last Test Was Run in the Advanced Test Interface menu enable/disable displaying of the date when the last test was launched
- Scheduled Tasks Branch section
 - Display Date on Which the Last Scheduled Task Was Launched
 enable/disable displaying the scheduled task launch date together with the task's name
 - **Sort Tasks by Launch Date** specify whether the scheduled tasks should be sorted chronologically according to the launch dates
- o Test Results Branch section
 - **Display Number of Infected Files** in the menu enable/disable displaying the number of infected objects found during scanning
 - Display Test Name with Test Results enable/disable displaying the test name together with the test results information





- Sort Test results by Date and Time specify whether the test results should be ascending /descending when sorted out by the test launch date
- Show Last (Test Results) specify the maximum number of test results to be displayed in the menu

f) Keyboard

The *Keyboard* tab allows you to define your own keyboard shortcuts using the following operating buttons:

- **Assign Shortcut Key** define a new keyboard shortcut for the selected function
- **Remove Shortcut Key** remove the current keyboard shortcut assigned to a specific function
- **Export Key Definitions** select directory where to which you want to export the current settings of the keyboard shortcuts
- **Import Key Definitions** select directory from where you want to import the new settings of the keyboard shortcuts



g) Customize

The *Customize* tab allows you to define what AVG functions you want to have available in **Test Center/Control Center**:





Available buttons		Selected buttons	
About AVG AVG Help	<u>A</u> dd ->	Switch to Advanced Control Center Virus Vault Test Results Check for Updates Exit	
Language Selection Program Settings	<- <u>R</u> emove		
Rescue Disk Wizard Scheduler Test Manager			
	Move <u>U</u> p		
	Move <u>D</u> own		

Separate tabs provide the following operating buttons:

- **Default** change the customized configuration settings, and return to the default settings
- **OK** apply all changes of the program parameters and close the dialog window
- *Cancel* cancel all changes of program parameters, and close the dialog window
- Apply apply all changes of the program parameters and leave the dialog window open

8.5. Update

The *Update* menu item launches a dialog window offering the immediate AVG update. The update can be performed either from the Internet or from the selected network directory. To cancel the update, press the *Cancel* button.

For further information on update possibilities refer to the chapter <u>14. Program</u> <u>Updates</u>.



The dialog operating buttons are:

• Internet – launches the AVG update from the Internet





- **Folde**r opens a dialog window where you need to specify the update source directory (either local or network); press the **OK** button to confirm selection and launch the AVG update
- **Cancel** closes the Update dialog window

If you want to use the same update files source repeatedly select the **Do not ask** for the update source next time option. Within the next update you will not be asked for the update source specification any more, and the update will be performed automatically from the source you have specified.

In the future, if you wish to restore the update source specification in the **Update** dialog, you can do so within the **Update Manager** component in the Control Center – for detailed settings description please refer to chapter <u>9.14 – Control Center –</u> <u>Update Manager</u>, the **Properties** section.

8.6. Rescue Disk

From Windows XP onwards the rescue disk feature is not supported any more.

This functionality is useful when you need to remove viruses from a computer:

- that has sharing violations problem
- to which you do not have sufficient access rights
- that has infected its system areas

The **Rescue Disk** menu item launches a wizard that will lead you through the process of creating a rescue disc. To create the **Rescue Disk** follow the wizard's instructions.



8.7. Virus Encyclopedia

The *Virus Encyclopedia* menu item launches a window with the possibility of searching for a virus by its name within the known viruses' database. *Virus Encyclopedia* is available online only!







8.8. Information

The *Information* menu item contains a list of sub-items corresponding to separate tabs of the newly opened dialog window with AVG information:

- Program installed AVG version
- *Version* license number used, user related data, program version, virus base version, and Anti-Spyware version
- System operating system data
- License Agreement full wording of AVG License Agreement
- Contacts overview of AVG vendor and partners contact information

8.9. Help

The *Help* menu item launches a new window with structured quick help for AVG:

- *Contents* topic related AVG information
- **Index** detailed description of AVG themes with help provided
- Find quick keyword search within the help information database











9. Control Center

The **Control Center** is the main controlling application of **AVG**. Within the **Control Center** environment, you can find items representing the separate installed components of **AVG 7.5 Internet Security**, and their respective control buttons that allow you to configure and maintain each component.

By default, the **Control Center** is started in reduced mode, where each item is listed in text format. You can switch to the extended mode at any time via the *View* menu <u>Chapter 9.3. Control Center Top Menu - b) View</u>.

The full color (yellow, black, red, and green) of the **Control Center** system tray icon on your Windows Taskbar indicates that all **AVG** components are active and fully functional. Gray icon coloring indicates a problem (inactive component, error status, old virus database, etc.). Double-click the system tray icon to open the main **Control Center** screen to edit a component.

Additionally you can check the *Security status* of AVG in the Control Center top section. There are three possible signs:

- Your computer is fully protected, up to date and all installed components are working properly
- One or more components are incorrectly configured and you should pay attention to their properties/settings. The problem components will be listed in the status error message.

 \checkmark

Indicates, that you have decided to ignore the reported faulty status of one of the components.

9.1. Control Center Launch

To launch the Control Center you can either:

 press the *Control Center* button in the *Test Center Basic Test Interface's* left menu

www.grisoft.com

- select *Program/Launch Control Center* from the top menu of either the *Basic* or *Advanced Test Center Interface*
- double click on the AVG system tray icon in the windows taskbar

The Control Center opens in this environment:





📕 AVG 7.5 Internet Security - Control Center 📃 🔲 🔀				
Program View Service Information				
AVG Internet Security	Security status You are fully protected. Your system is up to date and all installed components are working properly.			
🛐 Test Center	Component	Status	Description	
AVG Help	Manti-Virus Anti-Spyware	Internal Virus Datab Anti-Spyware is inst	Information about status and releas Protection against spyware, adware	
🛷 Check for Updates	V Anti-Spam	Anti-Spam is installe Firewall is running Next scheduled task	Protection against spam, i.e. unsolici Protection against undesired access	
👂 Language Selection	Resident Shield	Resident Shield is lo The Virus Vault cont	Provides on-access scanning of exec Virus guarantine, safe storage for in	
💽 Rescue Disk Wizard	Update Manager Shell Extension E-mail Scanner License	Last update on 11.9 AVG is active in Win E-mail Scanner is full Your license will expi	Automatic AVG update from the Inte Antivirus scanning in the Windows E Scans incoming and outgoing e-mail Information about the AVG license.	
	Anti-Vi Internal 11.9.20	irus Virus Database version is 06 (1 day ago). Last Test	268.12.3/444 and was released on was run on 7.9.2006 at 15:12:16.	
For Help press F1		7.5.414	268.12.3/444 2082 11.9.2006 13:30	

Note: The list of components displayed in the Control Center panel may differ according to the Control Center configuration, and also according to the components installed.

9.2. Control Center Left Menu

The Control Center's left navigation offers by default the following menu items:

However, the menu items list can be modified, for details refer to chapter <u>8.4</u> <u>Program Settings d) Keyboard</u>

a) Test Center

The *Test Center* menu item launches the **Test Center** application.

For details on the Test Center Basic/Advanced Test Interface refer to chapters <u>7. AVG Basic Test Center Interface</u> and <u>8. AVG Advanced Test Center</u> <u>Interface</u>.

b) AVG Help

The *AVG Help* menu item shows the help window with the description of **Control Center** items.

c) Check for Updates

The Check for Updates menu item opens the Update dialog window:



Copyright (c) 1992-2006 GRISOFT, s.r.o. All rights reserved.



Update	2
	Update
	To ensure maximum antivirus protection, it is important to keep your AVG up-to-date, Grisoft makes periodic virus updates available to AVG users. The following methods are available for accessing the latest update file.
	Select the location of the update file.
	Do not ask for the update source next time. This option can be reactivated in the Update Manager properties.
?	Internet Eolder Cancel

The dialog operating buttons are:

- *Internet* launches AVG update to download the latest updates from the Internet
- Folder opens a dialog window where you can specify an update source directory (either local or network); press the OK button to confirm selection and launch AVG update
- Cancel closes the Update dialog window

For details on update types and possibilities please refer to chapter <u>14.</u> <u>Program Updates</u>.

d) Rescue Disk Wizard

The *Rescue Disk Wizard* menu item launches the initial *Rescue Disk Wizard* dialog window:



For details on Rescue Disk creation and use please refer to chapter <u>8.6 Rescue</u> <u>Disk</u>.





e) Language Selection

The *language Selection* menu item launches the *Language Selection* dialog window. Here you can select the interface language from all installed languages.:

Language Selection	? 🗙
Select language:	ОК
Select a language for AVG. All texts and reports will be displayed in the selected language. You can select another language at any time.	Cancel
Use selected language as default	Help

Note: If you only installed English, then this button will not be available.

9.3. Control Center Top Menu

In addition to the standard menu items (common for all **AVG** environments), the **Control Center** top menu provides the following options:

a) Service/Administrator options

This option opens a new dialog where you can configure (enable/disable) accessibility of specific **AVG** functions.

📕 Administrator Options	? 🗙
Settings	
User interface	
Access to Advanced Interface	
Access to Basic Interface	
Access to Test Manager	=
Access to Scheduled Tasks	
🗌 🖂 Create a Rescue Disk	
🗌 🖂 On-Line registration of AVG	
Change AVG licence number	
🛛 🗁 🗹 Submit Bug Report	
- Zanguage Selection	
Potentially unwanted programs exceptions list editing	
Access to Administrator Options dialog	
Program configuration	
Access to Program Tab	
Access to lests lab	
Access to Startup Tab	~
Password Protection Default OK Canc	el

The dialog window provides the following operating buttons:

- **Password protection** allows you to define and confirm a password that will secure access to the **Administrator Options** dialog.
- **Default** returns the administrator options settings to default
- OK accepts all performed changes, and closes the dialog
- *Cancel* closes the dialog without accepting the performed changes
- b) View





Here you can select which components should be displayed in the main *Control Center* area, and whether these are displayed in reduced or extended mode.

c) Service/Program settings

This option opens the **Program Settings** dialog windows where you can find five tabs with all possibilities for full **AVG** configuration. For a detailed description of specific tabs please refer to chapter <u>8.4 Program Settings</u>.

Program Settings	? 🔀			
Program Startup Date and time Keyboard				
Store last:	1000 🕂 Test Results			
Test Results displayed in Results menu Show last: Sort Test Results: C descending C ascending	20 + Test Results			
Display a notification balloon when component status changes				
С.	Cancel Apply			

9.4. AVG Components in Control Center

In the main box of the **Control Center** you can see a list of all installed AVG components (in reduced mode), or panels representing the AVG components (in extended mode). To edit a component, just click the respective panel (or item in the list), and use the operating buttons in the bottom section of the **Control Center** window.

Whenever a component's state is erroneous, (e.g. the virus database has not been updated recently and is out-of-date), the component will be listed with a red "warning" icon, and the program system tray icon will turn gray. In the extended mode the component's panel will be highlighted in red. It is recommended that you pay close attention to such highlighted components, and keep the state of all components optimal in order to ensure correct functioning of AVG.

9.5. Control Center System Tray Icon

The **Control Center** icon appears on the system tray, and helps you to monitor AVG's current status. If all AVG components are fully functional, the icon is depicted in color. However, if the icon turns gray, at least one AVG component needs your attention! In that case double click the system tray icon to open the **Control Center**, and review the separate components status.

9.6. Control Center Components

The Control Center allows management of these AVG components:

- Anti-Virus
- Anti-Spyware





- <u>Anti-Spam</u>
- <u>Firewall</u>
- <u>Scheduler</u>
- Resident Shield
- Virus Vault
- Update Manager
- Shell Extension
- <u>E-mail Scanner</u>
- <u>License</u>

9.7. Control Center - Anti-Virus

The Anti-Virus component contains information on all currently known viruses.

*	Anti-Virus Internal Virus Database version is 268.12.3/445 and was released on 11.9.2006 (1 day ago). Last Test was run on 12.9.2006 at 10:55:11.		
		Update	Properties

Important: If the virus database is older than 7 days, it is considered to be outdated. To signal this, the component changes its internal state to error and turns red. Please remember that reliable antivirus protection can be achieved only if you update your antivirus system regularly and frequently. You can find more details on updates in chapter <u>14. Program Updates</u>.

The Anti-Virus panel's operating buttons are:

a) Update

The *Update* button opens the manual update dialog window. If not updated, the **Anti-Virus** database becomes out-of-date after 7 days!

Update		? 🔰
	Update	
	To ensure maximum antivirus protection, it is imp Grisoft makes periodic virus updates available to are available for accessing the latest update file.	ortant to keep your AVG up-to-date. AVG users. The following methods
	Select the location of the update file.	
	Do not ask for the update source next time. This option can be reactivated in the Update	Manager properties.
?	Internet Eolder	Cancel

For details on update types and possibilities please refer to chapter <u>14.</u> <u>Program updates</u>.

b) Properties





The *Properties* button provides a brief overview of the **Update** component's information. Also you have a chance to define how the component will be displayed in the **Control Center**:

Anti-Virus			? 🗙
General			
Component Information at Virus Databas	oout status and :e.	I release date of th	e AVG
Internal Virus	Database is up	o-to-date.	
Display comp	onent		
🔽 Display co	omponent		
🗖 Only v	vhen a faulty c	ondition exists	
🗌 🔲 Ignore fau	Ity condition of	the component	
ОК	Cancel	Apply	Help

9.8. Control Center - Anti-Spyware

t	Anti-Spyware Anti-Spyware version 4.2.11 is installed and is using datat	base version 2082.
		Properties

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

The *Anti-Spyware* component in **AVG 7.5 Internet Security** allows you to fully scan your computer for malware/spyware. It also detects *sleeping and non-dangerous* malware, i.e. malware that has been downloaded but not yet activated.

9.9. Control Center - Anti-Spam

Anti-Spam Anti-Spam version Spamcatcher 4.0.9 is installed and it is using the database released 12.9.2006 10:05:01.		s using the database
	Update	Properties

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

It requires very little maintenance, whilst allowing the user to customize several anti-spam options. To get more information about *Anti-Spam* features and settings, see chapter <u>11. Anti-Spam</u>.





9.10. Control Center - Firewall



The *Firewall* component controls all traffic on every single 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 network (local network or the Internet), or applications that approach your computer from outside trying to connect to your PC. For each of these applications the **Firewall** either allows or forbids their communication on the network ports.

To get more information about **Firewall** features and settings, please refer to chapter <u>10. Firewall</u>.

9.11. Control Center - Scheduler

The *Scheduler* controls scheduled events, such as updating and scanning.

 Scheduler Next scheduled task: 12.9.2006 12:04 Anti-Spam rules update.		
	Scheduled Tasks	Properties

The *Scheduler* panel's operating buttons are:

a) Scheduled Tasks

The *Scheduled Tasks* button launches the *Scheduled Tasks* window: the dialog and task scheduling options are described in detail in chapter <u>8.2</u> <u>Scheduled Tasks</u>

Scheduled 1	Fask s	5	P
Name	Туре	Last start	Next start
💑 Test plan in basic mode	Test	7.9.2006 8:00:00	8.9.2006 8:00:00
Update plan in Basic mode	Update	7.9.2006 8:52:00	8.9.2006 between 8:00 and 9:
💍 Anti-Spam rules update	Anti-Spam	7.9.2006 11:58:00	7.9.2006 13:58:00
<]	III		

b) Properties

The *Properties* button shows the *Scheduler* component's general info and allows you to specify the component's display options:





Scheduler 🔹 👔
General
Component Automatic (scheduled) triggering of Tests and Updates. Next scheduled task: 7.9.2006 13:58 Anti-Spam rules update.
Display component Display component Duly when a faulty condition exists Ignore faulty condition of the component
OK Cancel Apply Help

9.12. Control Center - Resident Shield

a) Resident Shield Properties

The *Resident Shield* component performs live protection of files and folders against viruses, spyware and other malware. This feature has to be activated first in the Resident Shield **Properties** dialog.

Resident Shield Resident Shield is loaded and all important functions are activated. Heuri Analysis is active. Scan floppy disks is active. On-close scan is not active	
	Properties

Use the *Properties* control button to open a new dialog window for *Resident Shield* configuration. The dialog opens with three tabs:

• **Properties** – The tab offers a range of possible **Resident Shield** scanning options to select from:

Resident Shield	? 🗙
Properties Excludes Ger	neral
✓ Turn on AVG Reside C Scan all files Scan infectable fil List of files to be s are available in the	ent Shield protection les canned and advanced settings e Advanced Settings dialog.
	Advanced Settings
- Additional options	
Scan floppy drives	
Use Heuristic Analys	sis
☐ On-close scanning ☑ Scan Potentially Unit	wanted Programs
OK Cance	el Apply Help

 Advanced Settings – opens the dialog window Resident Shield advanced settings, where it is possible to configure which files will be scanned (all or only infectable files). You can further define which





types of file (by specific extensions) will/will not be scanned. According to these settings the **Resident Shield** will skip or include the chosen extension during the scanning process.

📕 AVG Resident Shield - Advanced Settings 🛛 🔹 💽
Files scanned by AVG Resident Shield
C 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:
✓ Also scan files without extension
The AVG Resident Shield will scan:
Resident Shield scans files with extensions 386, ASP, BAT, BIN, BMP, BOD, CHM, CLA, CLASS, CMD, CNM, COM, CPL, DEV, DLL, DO*, DRV, EML, EXE, GIF, HLP, HT*, INI, JPEG, JPG, JS*, LNK, MD*, MSG, NWS, OCX, OV*, PCX, PGM, PHP*, PIF, PL*, PNG, POT, PP*, SCR, SHS, SMM, SYS, TIF, VBE, VBS, VBX, VXD, WMF, XL*, XML, ZL*. Checking files without extension is turned on.
OK Cancel

Excludes – The Excludes tab offers the possibility of defining folders that should be excluded from the Resident Shield scanning. If this is not a must, we strongly recommend not excluding any directories! If you decide to exclude a folder from Resident Shield scanning, mark the Use excludes in Resident Shield check box. The new settings will manifest only after the computer restart!

Please note: Exceptions for Potentially Unwanted Programs should be defined in a different dialog. See chapter <u>7.14 Potentially Unwanted</u> <u>Programs Exceptions</u>.

Resident Shiel	d		? 🗙
Properties Exc	udes General		
Directories exclu Resident Shield	ided from AVG scanning:	E dit E	xcludes
Computer restar	is needed for cha	nges to take eff	ect.
ОК	Cancel	Apply	Help

Use the *Edit Excludes* button to open a new dialog where you can directly specify the folders to be excluded from scanning:







This dialog provides the following control buttons:

- Add path offers you to 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 the whole list of directories to be excluded from the Resident Shield 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
- Check names verifies that the provided paths are valid paths leading to existing folders on the local disk, and removes all possible mistaken paths
- OK accepts all new settings, and closes the dialog window
- *Cancel* closes the dialog window without accepting the changes
- **General** The **General** tab offers an overview of general information on the **Resident Shield** component, and allows you to define whether the component should be displayed always, or only when a faulty condition exists, or whether the component's faulty condition should be ignored:







b) Resident Shield Findings

According to the set-up configuration, the Resident Shield continuously examines folders and files as these are being opened, closed, and saved. If a suspect object is detected, you will be immediately informed about the finding with this warning dialog:

📕 AVG Residen	t Shield 🔹 ? 🔀
()	Virus Detected!
While opening \Temporary Interr Virus identified EII	file: C:\Documents and Settings\klara\Local Settings et Files\Content.IE5\YXGNYHC9\eicar[1].com CAR_Test
	Info

The **Resident Shield – Virus Detected** dialog informs you about the process during which the suspect file was detected, it also provides information on the detected object location, and may even identify the infection type (if it is a known infection). The dialog also offers several operating buttons you can use for further treatment of the infected object:

- *Ignore* ignores the Virus Detected warning, and allows you to continue working (and also forbids access to the threat)
- **Info** open the on-line virus encyclopedia where you can look up detailed information on the identified virus
- *Hea*I allows you to heal the infected object if the cure for this kind of infection is available
- Move to Vault moves the infected object into the Virus Vault (and also removes it from its current location)

AVG is able to analyze and detect executable applications and DLL libraries that could be potentially unwanted within the system. Generally known as **Potentially Unwanted Programs** (for example spyware, adware).

If a **Potentially Unwanted Program** is found during a continuous system check by the Resident Shield, you will be notified by the following dialog:



Copyright (c) 1992-2006 GRISOFT, s.r.o. All rights reserved.





The dialog informs you about the detected Potentially Unwanted Program location and offers several operating buttons you can use for further treatment of the suspicious file:

- **Ignore** ignores the Resident Shield warning, and allows you to continue working (and also forbids access to the threat)
- **Info** opens the on-line virus encyclopedia where you can look up detailed information on the identified threat
- *Move to Vault* moves the potentially unwanted object into the Virus Vault (and also removes it from its current location)
- Add to exceptions allows to keep the Potentially Unwanted Program in the system and define it as a <u>Potentially Unwanted Programs</u> <u>Exception. (Chapter 7.14)</u>. A confirmation dialog will be displayed.

9.13. Control Center - Virus Vault

The *Virus Vault* works as a storage of suspect/infected object, and provides options for their further treatment or healing.

Virus Vault The Virus Vaul GB (20 % of th	irus Vault he Virus Vault contains 13 files with a total size of 377,7 kB. Size limit is B (20 % of the disk volume).				
	Empty vault	Open	Properties		

The Virus Vault panel's operating buttons are:

a) Empty vault

Deletes all objects stored in the Virus Vault.

b) Open

Opens the Virus Vault application:







For further details on the Virus Vault environment and possibilities of use please refer to chapter <u>12. Virus Vault</u>.

c) Properties

Offers a brief overview of the **Virus Vault** component information and allows you to define the required display options for the component:

Virus Vault 🔹 👔 🛛
General
Component Virus quarantine, safe storage for infected files. The Virus Vault contains 5 files with a total size of 376,5 kB.
Display component Display component Display component Duly when a faulty condition exists Ignore faulty condition of the component
OK Cancel Apply Help

9.14. Control Center - Update Manager

The Update Manager controls the AVG updates.

Ø	Update Mana Last update on 12.9.2006 21:38	l anager e on 12.9.2006 10:06 (today). Next update check scheduled on 21:38 from update.grisoft.cz, backup.grisoft.com.			
		Update	Settings	Properties	

The Update Manager panel's operating buttons are:

a) Update





The *Update* button opens a new dialog window offering an immediate update of AVG. The update can be performed by selecting the respective operating button:

- Internet downloads the update files directly from the Internet
- *Folder* performs the update from a directory where you have previously downloaded the update files from the Grisoft server

📕 Update	? 🛛
	Update
	To ensure maximum antivirus protection, it is important to keep your AVG up-to-date. Grisoft makes periodic virus updates available to AVG users. The following methods are available for accessing the latest update file.
	Select the location of the update file.
	Do not ask for the update source next time. This option can be reactivated in the Update Manager properties.
?	[Internet] Eolder Cancel

For further information on update types and possibilities please refer to chapter <u>14. Program Updates</u>.

b) Settings

The *Settings* button opens the *AVG Inet* dialog window with four tabs where you can configure your Internet connection parameters and define the update source:

o Proxy

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.

On the *Proxy* tab - based on the rules specified for your network – you should then specify whether you want to connect to the Internet via proxy server. Unfold the combo box list to select from these options:

- Do not use proxy server
- Use proxy server
- Use proxy server, if it fails try direct connection

If you use the *Use proxy server, if it fails try direct connection* or the *Use proxy server* option, you need to further 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 8080 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 *Proxy Authentication* option to verify that your user name and password are valid for connecting to the Internet via proxy server (within this dialog, the options of *Ask for password*, *User name*, *Password* will activate).

If the *Ask for password* option is marked, the specified password will not be saved and used automatically; instead you will be asked for the password every time you access the proxy server to connect to the Internet. Otherwise you can specify your user name (*User name*) and your password (*Password*) in this dialog; with the next update launch these data will automatically be used to connect to the proxy server.

📲 AVG Inet	? 🗙
Proxy Dial-Up URL Advanced	
Use proxy server	⊡│
Server: Port: 8080	-
✓ Proxy authentication	
Username:	
Password:	
OK Cancel Apply He	elp

o Dial-Up

All parameters optionally defined on the *Dial-Up* tab refer to the dial-up connection to the Internet. The tab's fields are inactive until you mark up the *Use Dial-Up connections* option that activates the fields.

Specify whether you want to connect to the Internet automatically (*Automa*tically open this connection) or you wish to confirm the connection manually every time (*Ask before connection*). For the automatic connection, select from the list of set-up connection the one that should be used (*Connection*), or define a new one (*New Connection*).

Then you can decide whether the connection should be closed after the update is finished (*Close Dial-Up connection when finished*).





The second secon	? 🗙
Proxy Dial-Up URL Advanced	
✓ Use dial-up connections	
 Automatically open this connection 	
☐ If another connection is established, use it	
Connection :	-
New Connection Properties	
Close dial-up connection when finished	
C Ask before connection	
OK Cancel Apply H	elp

• **URL**

The *URL* tab offers a list of Internet addresses from where 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

📲 AVG Inet			? 🔀
Proxy Dial-Up URL A	dvanced		
Name	LIBI		Add
update.grisoft.cz	http://update.gr	isoft.cz	
☑ backup.grisoft.com	http://backup.g	risoft.c	Edit
			Delete
			Default
			Move Up
			Move Down
ОК	Cancel	Apply	Help

o Advanced

The *Advanced* tab offers a possibility to delete all update temporary files that AVG may have created during the update process. To clear all such temporary files, simply click the *Delete update temporary files* button.





If you prefer to log all delete actions, keep the *Save to Log file* check box ticked.

📲 AVG Inet	? 🗙
Proxy Dial-Up URL Advanced	
Delete update temporary files	
Save to Log file	
OK Cancel Apply	Help

c) Properties

The *Properties* button opens the Update Manager dialog window with two tabs:

- *Properties* on this tab you can specify whether the update should be performed after your computer restart (Update upon next computer restart) or immediately (Update immediately) – for this option you can further define the behavior of AVG if the computer needs to restart.
- The *Do not ask for the update source* item allows you to enable/disable the option of selection of the update files source in the Update dialog.
- Next, specify rules for the update process information display (*Display information about update process*) and for AVG behavior toward other running applications that may collide with the update process.

Update Manager 🔹 🕄		
Properties General		
 Update upon next computer restart. (Updated files will be prepared and update finished after computer restart). 		
© Update immediately		
If computer restart is required:		
 Require confirmation from the user 		
C Restart immediately		
Complete at next computer restart		
✓ Do not ask for the update source		
Display information about update process		
Require confirmation to close running applications. AVG may require the closing of some running applications (for example MS Outlook)		
OK Cancel Apply Help		

 General – this tab provides a brief overview of the Update Manager component information, and you can define the component's display parameters:







9.15. Control Center - Shell Extension

The *Shell extension* activates the AVG functions in the Windows Explorer application so that you can test locations and objects within the Windows Explorer file browser by clicking the right mouse button and selecting the *Scan with AVG* option.

Shell Extension AVG is active in	on Windows Explorer.		
	Deactivate	Settings	Properties

The *Shell Extension* panel's operating buttons are:

a) Deactivate

The *Deactivate* button switches the *Shell Extension* component off

b) Settings

The *Settings* button opens a *Test Properties "Shell Extension Test"* dialog window. In the left part of this dialog you can see the navigation tree with branches responding to the "tabs" of a dialog window. The following configuration dialogs are offered within the navigation tree:

Test properties – in this dialog you can define the test name (Name), optionally also a detailed test description (Description). In the Based on section it is specified that the test was pre-defined by the AVG vendor. Further you can specify in what format and extent the test results should be displayed (When finished, display dialog).

GRISOFT

Copyright (c) 1992-2006 GRISOFT, s.r.o. All rights reserved.



Test properties	Test properties	
- Scan details - Report - Action to take - Advanced settings	Name: Description: Based on: When finished With test n with test s Do not dis detected	Shell Extension Test Predefined test d, display dialog esult tatistics splay result when no virus was
Iest Defaults	Page Defaults	OK Cancel

0

Scan details – in this dialog you can define whether the system areas should be scanned and what methods should be used for scanning (*General*). If you prefer not to *Scan NTFS Alternate Data Streams*, uncheck this check box.

Note: NTFS Alternate Data Streams is a Windows feature that can be misused by attackers (hackers mostly) for hiding data, especially rootkits, viruses, trojans, etc. Therefore it is recommended to keep this default settings checked.

You can also scan all active operating system's processes by ticking the *Scan active processes for viruses* check box. An Active process is basically a running application, that may be a regular software or also a virus/spyware/malware or different type of danger.

Further, decide whether the scanning should be performed on all files or only on 'infectable' files (*File extensions*), and you may also define extensions of files that will be excluded from scanning (*Exclusions*). You can also select the option of scanning files inside archives (*Archives*).

In the *Anti-Spyware* section you can disable/enable scanning for spyware/malware with the Anti-Spyware engine (*Enable Anti-Spyware engine(s)* check box).





Test properties - "Shell Exter Scan details - Scan details - Report - Action to take - Advanced settings	Image: Second details Scan details General Scan System Areas before the test starts Scan active processes for viruses Use heuristic Analysis Scan NTFS Alternate Data Streams File extensions Scan all files (except those defined below in "Exceptions") Scan all files (except those defined below in "Exceptions") Scan all infectable files Add extensions: Use Smart scan Exceptions Exclude extensions: Archives Scan inside archives Anti-Spyware Enable Anti-Spyware engine
Iest Defaults	Page Defaults OK Cancel

• *Report* – the *Report* dialog offers a list of situations that may be encountered during scanning. Select those that you want to be informed about:

 Test properties - "Shell Exte Scan details Report Action to take Advanced settings 	nsion Test"
Iest Defaults	Page Defaults OK Cancel

• **Action to take** – in the next dialog define actions that should be taken if a virus is detected (**When a virus is detected**) and while the warning (with parameters specified on the previous tab) is being displayed (**When warning is displayed**).




📕 Test properties - "Shell Ext	tension Test"
Test properties Scan details Report Action to take Advanced settings	Action to take When a virus is detected Automatically heal infected files Prompt user (display virus detection dialog) Continue testing Activate scanning window Only when the first virus is detected When warning is displayed Continue scanning Activate scanning window Only when the first varies is detected Only when the first warning is displayed Only when the first warning is displayed Display warning information dialog
I est Defaults	Page Defaults OK Cancel

Advanced settings – this dialog allows you to specify for how long the AVG warning message should be displayed (*Test message windows*) and whether the **Test Center** should be closed once the test is finished (*Close Test Center*). In the *Test priority* section you can select what priority the test should be assigned and how long the gaps between scanning separate files should be (the bigger the gaps, the longer the whole test takes but at the same time the overall system load decreases; this setting might be useful for older and slower computers).

Test properties - "Shell Extension Test"				
Test properties Scan details Report Action to take Advanced settings	Advanced settings Test message windows Automatic timeout during test Do not display other windows when the Close Test Center Close AVG upon completion of the test Close AVG only if no virus was found Test priority Set priority of the test when scanning Enable gaps during file scan	30		
<u>I</u> est Defaults	Page Defaults	OK Cance		

For all tabs of the *Test Properties "Shell Extension Test"* dialog window the accessible operating buttons are:

- *Test Defaults* returns the parameters edited on all dialog window tabs back to default values
- Page Defaults returns the parameters edited on a specific dialog tab back to default values
- **OK** accepts changes, and closes the dialog window
- **Cancel** closes the dialog window without accepting the changes
- c) Properties

0

The button *Properties* shows the *Shell extension* component's general info and allows you to specify the component's display options:







9.16. Control Center - E-mail Scanner

The E-mail scanner scans incoming and outgoing e-mail messages.

E-mail Scanner E-mail Scanner is fully functional.		
		Properties

Use the *Properties* control button on the *E-mail Scanner* panel to open the editing dialog window with two tabs:

 Plugins – This tab allows you to configure behavior parameters for all installed AVG plugins for specific e-mail clients:

E-mail Scanner				
Plugins General				
Select the e-mail plugin that you wish to modify, then select from among the available options.				
Installed plugins				
AVG MS Outlook Extension				
Options 「Ignore plugin status				
Use the shared test configuration				
C Use the personal test configuration				
Configure				
Properties Disable Plugin				
OK Cancel Apply Help				

In the **Options** Section you can set up the following parameters:

 Ignore plugin status – select this option if you do not want the Control Center to display information on the installed plugin current status





0

- *Test configuration* if you wish to set your own e-mail scanning configuration, you can select whether the test parameters should be specified as common for all installed plugins (*Use the shared test configuration*) or for each plugin individually (*Use the personal test configuration*). In both cases use the *Configure* button to open a similar dialog for test configuration editing. In the newly-opened dialog specify the following parameters:
 - Test name and description provide test name and description (optional)
 - *E-mail scanning* in this section select whether you want to scan the incoming/outgoing e-mail messages and whether the e-mail should be certified (always or only e-mails with attachments).

Note: Email virus-free certification is not supported in HTML/RTF format.

Additionally you can choose if you want AVG to modify subject for messages that contain potential viruses. Tick the *Modify subject for messages marked as virus* check box and optionally change the text (default value is ***VIRUS***).

- Scanning properties specify whether the heuristic analysis method should be used during scanning (Use heuristic analysis), whether you want to check incoming / outgoing e-mail for spyware/malware (Enable Anti-Spyware engine), and whether the archives should be scanned too (Scan inside archives).
- Attachment filter from the list of possibilities select parameters of the e-mail messages attachments scanning

📕 Test Options - "E-mail Scanr	ner"		? 🗙
Test name and description Name: E-mail Sca Description:	anner		
E-mail scanning Check incoming mail Certify mail With attachments only Modify subject for messages mark wwwJRUS***	Check Ce ed as virus	outgoing mail ertify mail With attachment	s only
Scanning properties ✓ Use heuristic Analysis ✓ Enable Anti-Spyware engine ✓ Scan inside archives ✓ Automatically move password	protected archives	to the Virus Vault	
Attachment filter Use heuristic e-mail message filter Remove attachments Remove all executable files Remove all documents Remove files with these extension	18;		
Pefault	<u>D</u> etails	ОК	Cancel

• **General** – This tab offers a brief overview of general information on the **E**mail Scanner component, and allows you to define required display options of the component:





E-mail Scanner	? 🗙
Plugins General	
Component Scans incoming and outgoing e-mail messages. E-mail Scanner is fully functional.	
Display component Display component Duly when a faulty condition exists Ignore faulty condition of the component	
OK Cancel Apply	Help

9.17. Control Center - License

The *License* panel has the full wording of the AVG License Agreement.

License AVG has been i -SA-PDZ, Coun	installed with Licens t of licenses is 10, s	e Number XXXX-X tandard license lengt	xxxx-xxxx-xxxx-xxx h 2 years. Your <u></u>
	Сору	Re-activate	Properties

The *License* panel's operating buttons are:

a) Copy

The *Copy* button automatically copies your license number into the clipboard, so you can paste it where needed (this can be useful when registering your AVG online).

b) Re-activate

The *Copy* button launches the *Activate AVG* dialog window: enter the license data to activate your **AVG**.

📕 Activate AVG 🛛 🔹 👔				
	Enter your AVG License Number and personal/company information.			
License Number:	XXXXXXX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX			
User Name:	GRISOFT, s.r.o.			
Company:	GRISOFT, s.r.o.			
License Number:				
2	Activate Back			





c) Properties

The *Properties* button shows the *License* component's general info and allows you to specify the display possibilities of this component:

License			? 🔀
General Component Information a Your license due, please v renewal at a	bout the AVG lic will expire on 30. risit www.girsoft. discounted price	ense. 11.2006. When n com to purchase y	enewal is vour license
Display comp Display c Display c Display c Display c Display comp	onent omponent when a faulty co ulty condition of I	ndition exists the component	
ОК	Cancel	Apply	Help



10. Firewall

AVG 7.5

The *Firewall* component controls all traffic on every single 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 their communication on the network ports.

10.1. Firewall Control Panel within the Control Center

Firewall Firewall is runnir	unning and fully function	al. Current profile is ''(Computer in domain
	Stop All Traffic	Configure	Properties

The operating buttons accessible directly from the *Firewall* control panel are the following:

- <u>Stop All Traffic</u> the Firewall will stop all traffic in both directions
- <u>Configure</u> opens the Firewall configuration dialog
- <u>Properties</u> opens the Firewall properties dialog

However, right-click your mouse over the *Firewall* component's panel to open the context menu with the following options:

Component		Status	
🗹 Anti-Virus		Internal Virus Database is	
🗹 Anti-Spywa	are	Anti-Spyware is installe	ed a
🗹 Anti-Spam		Anti-Spam is installed a	ind
Firew "		II· · -	en
🗹 Schei 🛛 🎽	ropercies		9.
🗹 Resid 🛛 🤇	onfigure		đa,
🔽 Virus 🔰 Sl	how Log		3
🗹 Upda 🛛 SI	top All Traf	ffic	68
🗹 Shell 🛛 D	eactivate f	Firewall	s E
🗹 E-ma 🛛 🗛	utomatic C	onfiguration Wizard	JDC
🗹 Licenso		Tour recense will expire	Jn

- <u>Properties</u> opens the Firewall properties dialog
- <u>Configure</u> opens the Firewall configuration dialog
- <u>Show Log</u> opens the list of logged Firewall actions and events within the Firewall configuration dialog
- <u>Stop All Traffic</u> Firewall will stop all traffic in both directions
- <u>Deactivate Firewall</u> stops Firewall
- <u>Automatic Configuration Wizard</u> launches the Firewall Automatic Configuration Wizard



10.2. Firewall Deactivation

VG 7.5

The **Firewall** can be deactivated via the **Deactivate Firewall** option from the context menu opened by right clicking over the **Firewall** panel in the **Control Center**.

The *Deactivate Firewall* button allows you to immediately switch the **Firewall** component off within the **Control Center** environment if the need arises. If you decide to deactivate the **Firewall** for any reason please keep in mind that right after the deactivation your PC's protection against both inner/outer network attacks is stopped, and your computer is exposed to the risk of invasion.

Having pressed the *Deactivate Firewall* button you will be warned about the possible risks with the following warning:



When the **Firewall** is inactive, its control panel within the **Control Center** displays the following three operating buttons:

Firewall Firewall is stopp	ed.		
	Activate	Show Log	Properties

• Activate – use the Activate button to restart the previously stopped Firewall, and to restore all its functions. You will be notified about Firewall activation by the following announcement:



- Show Log opens the list of logged Firewall actions and events
- **Properties** this button is always displayed in the **Firewall**'s control panel within the **Control Center** environment, and you can find detailed information on the **Firewall** properties and current status within the <u>Firewall Properties</u> chapter.

10.3. Stopping All Traffic in Firewall

The **Firewall** can stop all network traffic using the **Stop All Traffic** button within the **Firewall** control panel in the **Control Center**.

The *Stop All Traffic* button works as another hot key that allows you to quickly control the **Firewall** within the **Control Center** environment; and it is not necessary to change the component's configuration. If needed, by selecting this option you can block all traffic on every single network port: the **Firewall** is still running but all network traffic is stopped.





Having pressed the *Stop All Traffic* button, the new **Firewall** status will be announced by this warning message:



Once all traffic is stopped, the **Firewall** control panel displayed in the **Control Center** will provide a new **Allow Traffic** button that can be used to again allow communication for all applications that are assigned as "allowed" in the set of rules defined within the **Firewall** component:



Then, if you select the *Allow Traffic* option, the **Firewall** will again inform you about the status change.

10.4. Firewall Actions

The **Firewall** controls traffic on network ports by assigning rules to applications trying to communicate over the network. Rules are assigned to specific applications in the <u>Firewall – Configuration</u> dialog. Each rule is defined by one of the following actions:

a) Allowed

The rule specifies that all communication for this application is allowed.

b) Blocked

The rule specifies that all communication for this application is forbidden.

c) Ask

No rule has been specified for this application, and you will be asked what to do every time the application tries to communicate. When the application attempts to communicate on any network port, the *Firewall – Confirmation* dialog will pop up:







The *Firewall – Confirmation* dialog offers the following options:

- **Allow** allowing all of the application's communication (on this occasion only).
- *Deny* forbidding the application's communication (on this occasion only).
- Save the answer as a permanent rule creating a new rule based on your current choice (Allow/Deny) for the specific application; the rule will be saved into the Firewall configuration
- Show Details (Hide Details) displaying detailed information about the application and its parameters (application name, full path to the application's location, address, connection type, direction of the communication)

(WWV)	Applica addres <u>More ir</u>	ation 'Internet Ex Is 192.168.104.10 Information	xplorer' is trying to establish 1.	TCP connection with remote IP
	Do you	u want to allow this	communication?	
?		Allow	Deny	Hide Details
	IF U	iou select this ontic	on a new rule will be created	l lf such a rule alreadu eviste, ite
	lf y set	ou select this optic tings will be overw	on, a new rule will be created rritten.	I. If such a rule already exists, its

d) Advanced

If you assign the *Advanced* action to an application, you can then further define detailed rules for specific application services and for specific networks that the application communicates with. To assign the respective action to an application you need to go to the **Firewall – Configuration** dialog that is described in detail in the <u>Firewall Configuration</u> chapter.

10.5. Firewall Logging

You can view the **Firewall** log file information via the **Show Log** option from the context menu opened by right clicking over the **Firewall** panel in the **Control Center**. While the **Firewall** is deactivated, the list of logged actions and events is accessible directly from the **Firewall** control panel using the **Show Log** button.

The *Show Log* button opens a new *Firewall Configuration* dialog window opened on the *Log* tab. Within this tab you will be able to review the list of all logged **Firewall** actions and events with a detailed description of relevant parameters.



Copyright (c) 1992-2006 GRISOFT, s.r.o. All rights reserved.



Firewall Configuration	n - Comp	uter in domain	?
Logged Firewall actions and	itch Appli events:	cations System Networks	
Date and time	Action	Application	Add/Edit
2006-09-07 10:59:23	Block	C:\Program Files\lot	Application
2006-09-07 11:29:02	Block	C:\httpd\Apache2\	
2006-09-07 11:29:02	Block	C:\Program Files\0	Show Details
2006-09-07 11:29:02	Block	C:\Program Files\lol	
2006-09-07 11:29:02	Block	C:\Program Files\lol =	
8 2006-09-07 11:29:02	Block	C:\Program Files\lol	
2006-09-07 11:29:02	Ask	C:\httpd\Apache2\	
		▼	
<		>	
Information:			
Date and time: 2006	-09-07 10-9	i9·23	
Action: Block	<		
Application: C:\Pr	ogram File	s\lotus\notes\nInotes.	
Direction: TLP			Emphylica
Local address: local	host:1175		Emply Log
Remote address: 10.21	10.100.37:1	1352	Petresh
		<u> </u>	Tienesu
2		OK Cancel	Annly
		Canoor	

The main part of the *Log* tab is divided into two sections:

a) Logged Firewall Actions and Events Section

This section offers an overview of all actions and events that were performed by the **Firewall** with their parameters recorded within the log file.

By default, the *Log* tab opens in the standard mode with the following parameters provided for each of the logged actions:

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

If you find the provided parameters insufficient, and want to see more, use the *Show Details* button to switch to the advanced log file overview:



Date and time	Action	Application	User	Direction	Protocol	Local address	Remote address	~	Add/E dit
2006-09-07 10:59:23	Block	C:\Program Files\lot	klara	Out	TCP	localhost:1175	10.210.100.37:1352		Application
2006-09-07 11:29:02	Block	C:\httpd\Apache2\b	SYSTEM	In	TCP	localhost:80	0.0.0.0:0		-
2006-09-07 11:29:02	Block	C:\Program Files\Op	SYSTEM	In	TCP	localhost:22	0.0.0.0:0		Hide Details
2006-09-07 11:29:02	Block	C:\Program Files\lot	klara	Out	TCP	localhost:1175	10.210.100.37:1352	1.1	
2006-09-07 11:29:02	Block	C:\Program Files\lot	klara	Out	TCP	localhost:1175	10.210.100.37:1352	=	
3 2006-09-07 11:29:02	Block	C:\Program Files\lot	klara	Out	TCP	localhost:1175	10.210.100.37:1352		
2006-09-07 11:29:02	Ask	C:\httpd\Apache2\b	SYSTEM	In	TCP	localhost:80	0.0.0.0:0		
()			.1111				>		
formation:									
late and time: 200 lotion: Bloc lopplication: C:\F rotocol: TCF	6-09-07 1 :k Program F '	0:59:23 "iles\lotus\notes\ninotes.	exe					4	
virection: Out ocal address: loca	lhost:117	5							Empty Log
lemote address: 10.2	10.100.3	17:1352							

Then you will be able to review the following parameters:

- Date and Time exact date and time when the event was encountered
- Action type of action performed
- **Application** name of the process to which the logged event refers
- User name of the user of the application
- Direction the application's communication direction (in/out, or both ways)
- Protocol type of protocol used
- Local Address the local address of the connection related to the logged event
- *Remote Address* the remote address of the connection related to the logged event

In both the standard/advance *Log* tab mode you can always use the option of sorting the logged parameters according to a selected attribute: you can sort the data chronologically (press the header of the *Date and Time* column), by type of action (press the *Action* column header), etc.

b) Information Section

The *Information* section provides a comfortable and easy to view list of parameters logged for a specific event that is currently highlighted in the above *Logged Firewall Actions and Events* section.

c) Log Tab Operating Buttons

The *Log* tab offers three operating buttons:

 Add/Edit Application – add or edit an application to be covered by the logging mechanism





- **Show/Hide Details** switch between the standard/advanced mode of the log file display (as described above)
- *Empty Log* delete all information on the logged events from the overview
- *Refresh* update the currently displayed information

10.6. Firewall Configuration Wizard

The initial **Firewall** configuration can be set up using the *Firewall Configuration Wizard*. Though you can configure the component's parameters later on (see chapter <u>10.7. Firewall Configuration</u>), it is recommended that you take the wizard's tour to ensure the **Firewall** works properly.

The *Automatic Firewall Configuration Wizard* can be launched from the Start menu:

Start / All Programs / AVG 7.5 / Firewall – Configuration Wizard

or via the *Automatic Configuration Wizard* option from the context menu opened on right mouse click over the **Firewall** panel in **Control Center**.

Once you run the *Automatic Configuration Wizard*, it will check for an existing configuration and start in two possible modes:

- <u>Network connection options (a)</u> dialog appears if no existing configuration is found
- <u>Existing configuration (b)</u> dialog pops up when an already existing configuration is found

a) Computer networking connection options (new configuration)

If there is no existing configuration found, the *Automatic Firewall Configuration Wizard* opens with this dialog:

AVG Firewall Automatic Configuration Wizard	? 🔀
Network Connection Options How is your computer connected to the Internet?	þ
For maximum security, without disturbing the current network services that you access, it necessary to select ALL connection types that you use to connect to the Internet.	is
Select at least one option Standalone computer - directly connected to the Internet. Computer in domain - connected to company network. Computer on the move - when travelling	
Cancel Enish	

In this dialog the *Firewall Automatic 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

www.grisoft.com



Copyright (c) 1992-2006 GRISOFT, s.r.o. All rights reserved.



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:

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

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, *Scan your computer*.

Once you select corresponding choice(s), please proceed to the next step: <u>Scan your computer (c)</u>.

b) Existing configuration found

To avoid configuration conflicts, the *Firewall Automatic Configuration Wizard* detects your existing settings. If some existing configuration settings are found, the AVG Configuration Wizard will start with the following screen:

Firewall Automatic Configuration Wizard	X
Existing configuration Firewall configuration already exists	
The settings already exist. Do you want to update your current configuration or generate new settings and completely replace your current configuration? WARNING! All your custom settings will be lost if you confirm creating a new configuration.	
Required operation:	
Cancel Einish Cancel	

You can choose to **Update current settings** or <u>Create a new configuration</u>. If you select to update your current settings, the following dialog will be displayed:

• Update current settings





📕 Firewall Automatic Configuration Wizard 🔹 👔 🔀
Scan for Internet Applications
Which areas of your computer should be scanned?
To make sure your computer works correctly it is necessary to allow network communication for some programs. The Firewall Automatic Configuration Wizard will now scan your computer and try to find applications that should be allowed to communicate over the network. Select scanning option:
 Quick search (take advantage of current settings for update).
C Complete scan (scans all local hard drives of your computer)
Selected areas scan (scans selected hard drives)
Drive Drive size Free size Drive label
☑
Cancel Einish

Within this dialog you have to decide whether you want to scan all local hard drives of your computer (*Complete scan*) or you want to specify selected hard drives to be scanned (*Selected areas scan*), or proceed only with the *Quick search*.

Note: If you select Complete Scan or Selected areas scan options, 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.

To avoid repeating the scanning process again, we recommend to select the *Quick Search* option in this case. *Quick search* does not search the drives but only works with applications that are currently saved within the existing FW configuration and applies the rules defined in the new default configuration to their existing rules.

That means that using the *Quick search* option no new applications will be detected. All applications that are installed in the respective PC and have not been detected so far (i.e. no FW configuration rule has been created for them yet) have never attempted to communicate over the network. Therefore it is highly probable that these do not have to be taken into account.

If you choose the *Quick search* option, the *Configuration update conflicts* dialog will be displayed.

Note: In some cases, this error message may come up as well:

📲 AVG Fii	rewall 🛛 🕅
	An error occurred while creating AVG Firewall automatic configuration. The AVG Firewall settings are being edited by another process or thread.

This happens rarely when the Firewall configuration has been changed meanwhile you run the Firewall Configuration Wizard or the Firewall





configuration is currently opened in Control Center. To solve this problem, simply close the Configuration Wizard and start it again from the Start menu or by right-clicking the Firewall item in the Control Center and selecting the Automatic Configuration Wizard menu item from the list.

• Configuration update conflicts

Configu F	uration updat lease solve co	te conflicts nfiguration conflicts here	
	No conflicts	were found	
	Conflicts	Use settings	User settings
			Default settings
	<		

This dialog provides an overview of conflicts that have appeared while merging the existing FW configuration with the recommended default configuration. Usually, the list in this dialog is empty - that means both configuration sets were merged with no problem, and can be saved and used.

However, if the user manually changed the rule for a specific application/service in the past, and the default rule for this application/service has also been changed, a conflict in merging occurs. This conflict cannot be solved automatically and the user has to decide which configuration shall be used.

This is an example of the list of configuration merge conflicts:

AVG Firewall Automatic Configuration W	/izard	? 2
Configuration update conflicts		
Please solve configuration conflicts here		
One or more conflict has been found. Pleas here. If you have had problems with functio application or service in past, we recommen default settings. If you have modified function	e solve them nality of conflict nd you to choose onality of	
Conflicts	Use settings	User settings
See Computer in domain		
Application: Internet Explorer	X Unresolve	Default settings
Application: Windows Messenger	X Unresolve	
(>	
	(
C . Dark Martin	Carred	Calab

The user has to decide whether *User settings* or *Default settings* will be applied before the configuration can be saved. The user can choose to:





- Solve all items at once by clicking the User settings or Default settings buttons. The wizard will assign the selected choice to all items in the list.
- Solve individual items by clicking the Unresolved row in the Use settings column for each item and choosing User or Default settings.

Note: Default settings means that all customized changes to the previously saved Firewall configuration related to the conflicting application will be overruled by the Grisoft default rule. This option is recommended for less computer experienced users.

Also, if you have experienced any problems with the conflicting application in the past, we recommend that you select the Default settings for this application. Otherwise, you might keep the existing settings.

By selecting the User configuration, the conflicting application rule will be kept as it is and no settings recommended by AVG will apply to it.

In case you decide for the default settings to be applied to an application that has some very specific parameters defined (specific networks, adapters, etc.) a confirmation dialog may appear. In that case it is recommended to keep the customized configuration settings so that you do not lose your specific configuration parameters that would be lost otherwise.

Press the *Finish* button to finalize and save the configuration process.

c) Scan your computer

If no existing **Firewall** configuration was detected, the **Firewall Automatic Configuration Wizard** will start by scanning of your computer for applications that connect to the network:

📕 AVG Firev	vall Automatic Configuration Wizard	? 🔀
Scan for Inte	ernet Applications	
Which	areas of your computer should be scanned?	5
To mak commun now sca over the Select	e sure your computer works correctly it is necessary to allow network isoation for some programs. The AVG Firewall Automatic Configuration Wizar an your computer and try to find applications that should be allowed to comm network.	rd will sunicate
Cont	scanning option:	
G Corr	sk search (rake auvantage of current settings for update).	
C Sele	nplete scan (scans all local nard drives of your composer)	
D	rive Drive size Free size Drive label	
	□C\ 186.3 GB 167 GB	
2	Cancel	sh

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.



AVG 7.5

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 your computer* dialog you have to decide whether you want to scan all local hard drives of your computer (*Complete scan*) or you want to specify selected hard drives to be scanned (*Selected areas scan*). Press the *Next* button to confirm your selection, and continue to the following dialog:

d) System services

The *System services* dialog offers a list of services and protocols found on your computer that may need to communicate over the network. In the list, mark with a "green tick" any services/protocols that you want to use.

Recommendation: Make sure that only services that you really need are marked as allowed in the list. A new Firewall rule will be created for each of these services enabling them to communicate over the network.

Access rules will be created for all items listed below, accordi The rule specifies if the service or protocol can communicate	on to the onlines allow black
Click on the item's icon to change its access options.	over the network.
Joseph Content Joseph C	<u>Expand all</u>
	

e) Programs and applications

The *Programs and applications* dialog offers a list of all programs and applications found on your computer that may need to communicate over the network. In the list, select the required network connection option for each application, as follows:



- 洋 ... block
- ? ... ask user

In do not create rule for this application







f) Completing the Automatic AVG Configuration Wizard

The last dialog informs you about the **Firewall** configuration set up in the previous dialogs.

Before closing the Firewall Automatic 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 of this wizard. You can then later on switch between the predefined Firewall profiles according to the current state of your computer.

This option refers to the specific defined *Firewall profile* – for details please see chapter <u>10.7 – Firewall Configuration - b) Profile</u>.

A۷	G Firewall Automatic Configuration Wizard
Se	elect Current Profile
	Automatic AVG Firewall configuration has finished successfully
	The AVG Firewall Automatic 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.
	Select the profile you would like to activate after completing the wizard:
	Standalone computer - directly connected to the Internet.
	Press the Finish button to save all settings.
	r less the r maar buttor to save at severys.
2	<kback next="">> Cancel Einish</kback>

Press the *Finish* button to save the specified configuration and to close the wizard.

10.7. Firewall Configuration

To reach the **Firewall** configuration environment use the **Configure** button within the **Firewall** control panel in **Control Center**.

The *Configure* button opens a new *Firewall Configuration* dialog window with following tabs:





- <u>General</u>
- Profile
- Profile switch
- <u>Applications</u>
- <u>System</u>
- <u>Networks</u>
- <u>Log</u>

a) General

Firewall Configuration - Cor	nputer in do	nain	? 🗙
General Profile Profile switch A	pplications Sys	tem Networks Lo	g
Settings on this page apply to all pro	ofiles!		
Statistics			
Firewall up-time: Blocked packets: Total packets:			36:38 649 19 770
- Global Settings			
Export Settings Exports m backup f	ules and configu iles (e.g. for trans	ation from all profiles ferring them to anoth	into the er computer).
Import Settings Imports ru	Imports rules and configuration for all profiles from a backup file.		
Settings archive Restore s	settings from auto	omatically managed a	irchive.
Firewall security			
Permit settings modification to:		Administrators and	Power U: 🔻
Show confirmation dialogs for:		All Users	
Firewall information messages:		Show only errors a	nd warnin 💌
?	OK	Cancel	Apply

The *General* tab offers an overview of the **Firewall** settings parameters that apply to all profiles. The tab is divided into three sections:

- Statistics contains a brief overview of the Firewall component's current status:
 - Information on the time since Firewall's last restart
 - Information on the number of blocked communication attempts
 - Information on the total number of communication attempts
- Global settings using the Export settings / Import settings buttons you can export the defined Firewall rules and settings to the back-up files, or on the other hand to import the entire back up file.
- Settings 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 Settings archive is empty it means that no change has been done since the Firewall was installed.

As soon as settings are changed and confirmed, the dialog window will look like this:

Settings archive		?
Settings write time	Status	Restore settings
7.9.2006 10:57:38	Active	Thestore settings
7.9.2006 10:56:34		
7.9.2006 10:54:43		
7.9.2006 10:53:08		
7.9.2006 10:52:32		
7.9.2006 10:51:45		
6.9.2006 17:21:58		
		Cancel

The column Settings write time, contains the exact time when the configuration change occurred. The Status column displays which configuration is active.

The current Firewall configuration is marked as *Active*. Records are always sorted chronologically, where the settings indicated on the top are the very last saved.

The Settings archive tracks every Firewall configuration change except profile changes (i.e. switching from the profile Computer in domain to the profile Computer on the move will not be tracked). Changes are archived as soon as you confirm the desired configuration by pressing the OK or Apply button.

The Maximum number of stored records is 10. If you try to save more records, the oldest records will be over-written.

Activation of any of the stored settings can be done by clicking the Restore settings button. The chosen configuration will become active immediately.

- Firewall Security in this section you can define rules for the Firewall configuration rights. Specify who should be allowed to modify the Firewall settings, and to whom the <u>confirmation dialogs</u> and Firewall information messages should be shown. You can select from the following three categories with a different authority level:
 - 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

- All Users other users not assigned into any specific group
- b) Profile





📕 Firewall Configura	ntion - Computer in domain 🛛 🔹 👔
General Profile Profi	e switch Applications System Networks Log
Computer in domain	Computer in domain - connected to company network.
Manage Profiles	Activate Profile
Export Profile	Exports rules and configuration from the current profile into a backup file (e.g. for transferring it to another computer).
Import Profile	Imports rules and configuration from a backup file. If a profile with the same name already exists then the profile will be
Profile currently in us The current profile us	e ed by the Firewall engine is "Computer in domain".
	OK Cancel Apply

On the **Profile** tab you can select the desired **Firewall** profile (profile specification option is available on the following operating systems only: Windows NT/Win2K/WinXP). The main principle of **Profile** selection is the possibility to set different **Firewall** security levels.

For example, consider the two following profiles – *Computer on the move* and *Computer in domain*. During a business trip, you may wish to connect your notebook to the Internet from a hotel or at the airport. Here the risk to your computer will be significantly higher than while connecting to the company network. For this reason, we recommend that you define, and set up, a specific *Computer on the move* profile - with parameters that will ensure a higher protection level. However, the *Computer in domain* profile could be defined with a lower security level. In addition, the *Computer in domain* profile could allow some services that would not be required or desired while you are on a business trip (e.g. file sharing).

Typically you can select among the following profile options:

- o Allow All
- Block All
- o Computer in domain
- o Computer on the move
- o Standalone computer

By default, the profile generated based on parameters that you have specified within the Firewall Automatic Configuration Wizard will be used. Each profile covers specific settings of your PC, and an adequate **Firewall** security level is assigned to each of the profiles. The proper profile option can be selected from the drop-down menu; then confirm your choice using the **Set active profile** button.

Setting the **Firewall** profile you can use the following two operating buttons:





0

Manage profiles – opens a new *Manage profiles* dialog where you can edit each specified profile and add new custom profiles.

Allow all	
Block all	Rename Profile
Computer in domain	
	Delete Profile
	<u>C</u> lose

The following buttons can be used:

- Copy profile makes creating a new profile easier and more comfortable for you: To use this option, highlight a profile in the list of profiles and press the Copy profile button. A new profile will be created with predefined parameters taken from the definition of the cloned profile. Then you can easily edit the parameters for the new profile.
- Rename Profile press this button to enable editing of the selected profile name
- Delete Profile press this button to delete the selected profile from the list (unless the profile is currently used)
- Close closes the Manage profile dialog
- **Activate profile** use this button to confirm the profile selection, or any changes made to the profile settings

In the bottom part of the *Profile* tab you will find the *Export profile*/*Import profile* buttons that allow you to export the defined **Firewall** profiles into the back-up files, or on the other hand import the entire back-up profiles.

c) Profile switch

On the *Profile switch* tab you can manage network areas and local network interfaces. You can assign specific profiles to local interfaces and network areas.

The Firewall is able to automatically switch the active profile according to the currently used type of network connection. This feature is useful especially for:

- **Users with laptops** using the same network interface for connecting to various networks on different places (business travel, home vs. work environment, etc.).
- **Users using more than one network connection type** for example xDSL connection vs. some backup connection (e.g. Dial-up, wireless, ...)
- Users with more than one network interface





Whenever you connect to a new (unrecognized) connection, the *New area* dialog will appear. Here you should select the most appropriate profile for the current network connection, then click on *Assign Profile*.

New area	? 🔀
New or unassigned area was detected. Choose profil each time this area detected.	e, which will be activated
Detected area:	
A Local network	
Choose profile:	
🐳 Allow all	
😥 Block all	
Secomputer in domain	
Disable area detection and profile switch	
Disable dialog for assigning new area	
Without profile	Assign profile

- **Detected area** indicates the type of network connection that has been detected. You can rename the area, by clicking the text field to make it more convenient for remembering if you are using more connections on a regular basis.
- **Choose profile** contains a list of available profiles. Choose the most suitable profile.
- **Disable area detection and profile switch** tick this checkbox to disable the whole Profile detection feature.
- Disable dialog for assigning new area tick this checkbox if you prefer not to display the New area dialog anymore. The default profile will then be automatically assigned.

Control buttons are as follows:

- Assign profile Once you have clicked on this button, the selected profile will always be automatically associated with this connection, and in the future, this dialog will not be displayed when connecting to this connection.
- Without profile press this button to keep the connection type without a profile. The Firewall will ask you again, each time when this connection type is found. To disable this window, (before confirming your choice) tick either Disable area detection and profile switch checkbox to disable the entire area detection system, or Disable dialog for assigning new area checkbox to disable the confirmation dialog (profile will be assigned automatically).

GRISOFT



📕 Firewall Configuration - Computer in domain	? 🔀
General Profile Profile switch Applications Sustem Networks	
	109
Disable area detection and profile switch	
The following list contains areas and assigned profiles	
Areas Assigned pr	Edit Area
III All Local Interfaces	
🕮 Intel(R) PRO/100 VE Network Conn 🗙 Unassign	Delete Area
All network areas	
	Assign active
Advanced settings	
Default profile Allow all	
Disable dialog for assigning new area	
Disable displaying information about areas and profile cha	
This setting enables selection of profiles to various network	
connections. The assigned profile is switched in accordance with the detected connection (area)	
with the detected connection (area).	Show details
· · · · · · · · · · · · · · · · · · ·	
	1 0h
	Арру

Users can setup separate profiles for each connection type and/or network interface and then assign them as preferred.

To disable this feature, simply tick the *Disable area detection and profile switch* checkbox.

To view more details about selected network area, click the *Show details* button.

The main list contains areas and assigned profiles. By clicking on the requested row in the *Assigned profile* column, a list of profiles that can be currently assigned will be displayed:

Areas	Assigned profile
🕮 All Local Interfaces	
🕮 VMware Virtual Ethernet Ad	Mallow all
B VMware Virtual Ethernet Ad	Block all
📑 🎟 Marvell Yukon 88E8001/80	Somputer in domain
💑 All network areas	
🛃 Local network	
<	>

If you do not want to specify a profile for a specific interface or area, simply leave the option as *Unassigned*.

- To change the network area name, select the area you want to rename and click the *Rename* button.
- To delete the network area, select the desired area and click the **Delete** button.

Please note: If you delete all network areas, or when there is no network area present in the list, a new button Assign active will appear. By clicking this button, you will simply assign the currently active network area.





📕 Firewall Configuration - Computer in domain	? 🔀
General Profile Profile Switch Applications System Networks	
deneral Frome Frome official Applications System (Networks)	
Disable area detection and profile switch	
The following list contains areas and assigned profiles	
Areas Assigned profile	Edit Area
All Local Interfaces	
Intel(R) PRO/100 VE Netwo X Unassigned	Delete Area
Rel network areas	
	Assign active
Advanced settings	
Default profile Computer in domain 💌	
Disable dialog for assigning new area	
Disable displaying information about areas and profile chan-	
Area activated count: 1	
Last time activated: 2006-09-13 15:29:35	
IF address of net gateway. 132,166,133,1	Hide details
	Applu

• **Default profile** - this profile will be automatically activated when:

- A new area is detected.
- An error occurs during new area detection (for example when there is no active connection type).
- An area with no assigned profile is active.
- Disable dialog for assigning new area tick this checkbox if you prefer not to display the New area dialog. The default profile will then be automatically used.
- Disable displaying information about areas and profiles changes tick this check box to manifest you do not wish to have displayed any warning messages.

Please note:

- (i) Assigning a profile to a network interface has a higher priority than to a network area. This means that once you assign a profile to your network interface, it will be always used regardless of the network area.
- (ii) When in safe mode, automatic profiles will be disabled.
- d) Applications Basic Settings





Firewall applications and rules overview:	Actic	
Application	Alleu	Add Application
		Edit Application
Ave Alert Manager	Allow	EakApplication
Application Layer Clateway service	Allow	Delete Application
V AVG Control Center	Allow	
AVG Undate Downloader	Allow	
V AVG S-Tool	Allow	
V AVG Test Interface Module	Allow	
😃 🗖 Dr. Watson Windows Error Reporting Tool	Adva	
Vindows Explorer	Allow	
<	>	
If there is no rule for an application: C Block C Allow • Ask This option will be used when an application is trying communicate and no appropriate rule can be found) to for such	
types of communication.		Show Details

In the main section of the *Applications* tab you can see the list of all applications, and the list of rules that have been created for each application. In the list of applications, there is always one of the following signs displayed left to the icon and the name of the respective application:

- o **√** Allow
- o 🎽 Block
- o **?** Ask
- Advanced settings

For detailed information on specific actions please refer to chapter <u>10.4 -</u> <i>Firewall Actions

Click this sign to change the rule assigned to the currently highlighted application by selecting another action from the newly opened context menu:



Press the *Enter* key to confirm your choice, or the *Esc* key to cancel it.

The *Applications* tab offers the following operating buttons:

Add/Edit Application – these buttons open a new Application
 Properties dialog window where you can create (edit) a new rule for a specific application. Within the dialog you need to provide the application's name, the path to the application's current location on your hard disk, and you must assign the relevant action to the application



(e.g. an action to be taken when the application attempts to communicate on any network port).

Application Properties	? 🗙
Application name:	
	OK
Application path:	
	Cancel
Action:	
Allow	

- Delete Application this button deletes the rule defined for a specific application, and removes the application and its relevant action from the list within the Applications tab of the Firewall Configuration dialog window.
- Show/Hide Details in the same dialog window, this button provides a brief overview of detailed information referring to the application currently highlighted in the list of applications:
 - Application name of the application
 - File path current location of the respective application
 - Action action assigned to the respective application

Firewall Configuration - Computer in dom	nain	? 🔀
General Profile Profile switch Applications System	em Network	<s log<="" th=""></s>
Firewall applications and rules overview:		
Application	Actic 🔨	Add Application
🖌 🛅 Personal E-mail Scanner	Allow	
🖌 📩 AVG Alert Manager	Allow	Edit Application
🖌 🗂 Application Layer Gateway service	Allow	
🖌 🗂 AVG Agent	Allow	Delete Application
🖌 🚽 AVG Control Center	Allov	
🖌 🚽 AVG Update Downloader	Allow	
VG S-Tool	Allow	
🖌 🚽 AVG Test Interface Module	Allow	
🏶 🛅 Dr. Watson Windows Error Reporting Tool	Adva	
Vindows Explorer	Allov	
	>	
If there is no rule for an application:		
C Block C Allow @ Ask		
This option will be used when an application is trying communicate and no appropriate rule can be found types of communication.) to for such	
		Show Details
ОК	Cancel	Apply

On the *Application* tab you can also find a section named *If there is no rule for an application*; here you should specify what action should be performed in case a new application attempts to communicate over the network and there is no rule specified for this application in the **Firewall** yet.

www.grisoft.com

e) Applications – Advanced Settings

Caution! Use of the Advanced Settings can be recommended to savvy and experienced users only!



Copyright (c) 1992-2006 GRISOFT, s.r.o. All rights reserved.



The *Applications* tab also allows you to configure advanced settings for specific application. For a new application, use the *Add Application* button and in the newly opened *Application Properties* dialog select the *Advanced configuration* option within the *Action* section.

If you have already selected an application with the advanced settings from the list of applications in the *Applications* tab, the *Application Properties* dialog opens with the following extended interface:

Applic	ation Properti	es		? 🔀
Applicatio	n name:			
Mozilla				OK
Application	n path:			
C:\Progra	m Files\mozilla.org	\Mozilla\mozilla.	exe	Cancel
Action:				
Advance	d configuration		•	
List of rule	s - advanced confi	iguration:		
Action	Services	Networks	Log	Create Rule
Allow	FTP, HTTP,	All networks	No	
				Edit Rule
				Edit Rule Delete Rule
				Edit Rule Delete Rule Move Up

The following control buttons are available in the extended *Application Properties* dialog:

- Create Rule/Edit Rule opens the same Application Rule dialog where you can define parameters for a new application rule, or edit parameters of an existing application rule.
- **Delete Rule** removes the currently selected rule from the list of rules.
- *Move Up* moves the rule one position up in the list of rules.
- *Move Down* moves the rule one position down in the list of rules.

In the bottom part of this dialog you can see a new section named *List of Rules – Advanced Configuration*. This section contains information divided into four columns:

- **Action** brings information on an action type assigned to the selected application
- **Services** brings information on a network service assigned to which the application rule relates
- **Networks** brings information on a network to which the application rule relates
- **Log** provides information about whether the selected application events are being recorded into the log file

The following control buttons are available:

• **Create Rule** – opens a new **Application Rule** dialog where you can define a new rule for the selected application:





Allow		=	
411077) white to Log	
ervices			Networks
vailable services:		Applied services:	Available networks:
ILS_DUT Ident SMTP SMTPS IMAPS POPS POPS NNTP DNS DNS_Server DHCP SMD_Microsoft Drin		POP	All Networks All Local Interfaces All Local Interfaces All Remote Networks All Remote Networks Internet
New Service	$\overline{\mathbf{b}}$	<- Edit Service	New Network Edit Network

The dialog is divided into three sections:

 Actions – from the drop-down menu select an action that should be performed in case all network communication conditions (as defined I the bottom part of this dialog) are met. The available action types are Block / Allow / Ask (see the action types description in chapter <u>10.4</u> <u>Firewall Actions</u>)

The *Actions* section also contains the *Write to Log* item – mark this option if you want the application's communication to be recorded in the **Firewall** log file.

- **Services** this section offers two lists of services:
 - Available Services list of services defined for the application in the default configuration, and services that have already been defined by the user
 - Applied Services list of services covered by the defined application rule. This list is a subset of the Available Services list.

You can move items between both of the lists using the -> or <buttons respectively. Moving an item from the list of **Available Services** to the **Applied Services** list means the service will be considered for the respective application when applying this rule.

There are two control buttons in the *Services* section:

- New Service/Edit Service – opens a new Service Properties dialog where you can specify the new service parameters/edit parameters of already defined service:

Service	Properties			? 🔀
Service name	B:			
FTP				OK
Service items				Cancel
Direction	Protocol	Local ports	Remote ports	Add Item
Out In	TCP TCP	all ports 20	21 all ports	<u>E</u> dit Item
				Delete Item
				<u>C</u> opy Service Items

In the *Service Properties* dialog specify the service name in the *Service Name* field. The dialog contains the following control buttons:

- Add Item/Edit Item - opens a new Service Item dialog where you can define (edit) parameters of specific service items (Protocol, Direction of communication, Local Ports, and Remote Ports):

Service Item	? 🔀
Protocol	Direction
TCP	⊖ In
Custom Protocol Number:	🖲 Out
6	O Both ways
Local ports (comma separated list of val	ues or ranges [23,45-50,11]):
×	
Remote ports (comma separated list of v	values or ranges [23,45-50,11]):
25	
2	OK Cancel

- Protocol select a predefined protocol from a drop down menu, or select the option of *Custom protocol* and then provide the standard protocol number in the *Custom Protocol Number* field (the "0" value stands for all protocols).
 - Direction define the service direction
 - Local Ports list all local ports or define a range
 - Remote Ports list all local ports or define a range
- Delete Item removes the selected item from the Service Items list.
- Copy Service Items makes it easier to create a new service item record using the possibility of copying the already defined parameters of an existing item. The button opens a new Select Service dialog where you are offered a list of services; select a service whose items you want to copy:

📕 Select Se	rvice		? 🔀
Available Serv	ices:		
Service			^
ICS_IN ICS_OUT Ident SMTP IMAP POP SMTPS IMAPS POPS NNTP DNS SNS C			
?	OK	Cance	

• **Networks** – this section offers a control tree providing a list of available networks. Mark the check box for each network to which the respective application rule should be assigned.

There are two control buttons in the *Networks* section:

 New Network / Edit Network – opens a new Network Properties dialog where you can define (edit) new network parameters: Network Name and Network Addresses (specified by the IP address range):

Network name: network_name		_
Network addresses		
O IP address range	From: 0.0.0.0	
	To: 0 . 0 . 0 . 0	
IP address/mask	Address:	
	Mask:	
One IP address	Address: 123. 25 . 45 . 255	
C Whole network (all IP addre	esses)	
You are only able to add, edit, or on network definitions depend on you be changed.	delete remote network definitions. Local ur PC hardware configuration, and canno	ot
2	OK Cancel	

f) System

Any editing of the *System* tab parameters is recommended to experienced users only!

Firewall Configuration - C	omputer in	domain		? 🔀
General Profile Profile switch	Applications	System	Vetwork	s Log
System services and protocols rul	es overview:			
System Service or Protocol			<u> </u>	Add Rule
🔀 🐨 Internet Connection Sha	ring			
🗴 🐨 Windows RPC Service				Edit Rule
🗸 🐨 DHCP Protocol Client				
🖌 🐨 DNS Protocol Client			=	Delete Rule
🖌 🗸 🐨 ICMP network diagnostic	cs			
🖌 🗸 🐨 Microsoft file sharing and	l printing			
🗸 🐨 Replies on ICMP networ	k diagnostics			
🕺 🎾 🔭 Remote Desktop Server				
💢 🔭 Web Server Apache2				
🖌 🖌 🐨 Destination Unreachable	•		_	
💢 🐨 Ident service			*	
Log blocked system communica	ation			
🗌 Incoming 🔤 🖸	Dutgoing			
Adding and/or modification of sys recommend only for advanced us	tem communic ers with a goo	ation rules i d knowledg	is le of	
networks and communications.				Show Details
?	ОК		Cancel	

The **System** tab opens an overview of rules specified for system services that need to communicate over the network. Compared to the applications, there are only two kinds of actions that can be assigned to a system service:

- Allow signed by the green check mark before the system service's name
- **Block** signed by the red cross mark before the system service's name

If you want to change the rule assigned to a specific system service, click the color sign (green check mark / red cross mark) displayed in the list of services and the sign switches to the opposite one automatically (the rule is changed).

In the *Log blocked system communication* section you can specify whether you want to log the incoming / outgoing blocked communication, or communication in both ways.

The *System* tab further offers the following operating buttons:

• **Add/Edit Rule** – opens a new dialog where you can add a new system service rule, or edit the current one:

Systen	n Service F	Rule Properti	es		? 🔀
System se	rvice name:				
DHCP Pro	otocol Clienț				OK
Application	n type:				
SYSTEM					Cancel
Action:					
Advance	d configuratio	n		-	
List of rule	s - advanced	configuration:			
Action	Services	Networks	Log		Create Rule
Allow	DHCP	All networks	No		Edb Dula
					Luithuie
					Delete Rule
					Move Up
					Move Down
					move blown

- **Delete Rule** deletes the rule defined for the selected system service
- Show Details in the bottom section of the dialog window, this button displays an information overview referring to the system service currently selected in the list of system services and protocols:
 - Service name of the system service (or protocol)
 - Rule rule assigned to the respective system service (or protocol)

Having selected the *Show Details* option, a new button labeled *Services* appears in the *System* tab:

Firewall Configuration - Computer in domain	? 🔀
General Profile Profile switch Applications System Network	s Log
System services and protocols rules overview:	
System Service or Protocol	Add Rule
🗶 🐨 Internet Connection Sharing	
🗶 🐨 Windows RPC Service	Edit Rule
✓ 🐨 DHCP Protocol Client	
✓ TF DNS Protocol Client	Delete Rule
✓ TFICMP network diagnostics	
✓ 🐨 Microsoft file sharing and printing	
✓ 🐨 Replies on ICMP network diagnostics	
🗶 🐨 Remote Desktop Server	
🗶 🐨 Web Server Apache2	
🗸 🐨 Destination Unreachable	
🗶 🐨 Ident service 🗠 🗠	Services
Log blocked system communication	
☐ Incoming	
Service: DHCP Protocol Client	
Action: Allow	
	Hide Details
	Δροίμ

The *Services* button opens a new *Services* dialog that displays a detailed overview of system services and brings the option of editing parameters of respective system services:

s Overview:		
Details	~	Add Service
All protocols In/Out all ports		
TCP In all ports, UDP In/Out all ports	=	Edit Service
TCP Out all ports	<u> </u>	
TCP In on local port 113		agana ang agang
TCP Out on remote port 25		<u>D</u> elete Service
TCP Out on remote port 143		
TCP Out on remote port 110		Copy Service
TCP Out on remote port 465		-10,
TCP Out on remote port 993		
TCP Out on remote port 995		
TCP Out on remote port 119		
UDP In/Out on remote port 53	~	
	Details All protocols In/Dut all ports TCP In all ports, UDP In/Dut all ports TCP out all ports TCP Out on remote port 113 TCP Out on remote port 143 TCP Out on remote port 143 TCP Out on remote port 143 TCP Out on remote port 465 TCP Out on remote port 993 TCP Out on remote port 199 TCP Out on remote port 119 UDP In/Dut on remote port 53	Details All protocols In/Dut all ports TCP In all ports, UDP In/Dut all ports TCP Out all ports, UDP In/Out all ports TCP Out on remote port 113 TCP Out on remote port 143 TCP Out on remote port 143 TCP Out on remote port 465 TCP Out on remote port 993 TCP Out on remote port 119 UDP In/Out on remote port 119 UDP In/Out on remote port 53

The *Services* dialog window provides the following operating buttons:

 Add Service – opens a new Service Properties dialog where you can define the new service name and set specific parameters for this service (direction, protocol, local ports, remote ports)

Service	Properties	ŝ		?
Service nam	e:			
ICS_IN				OK
Service item:	s:			Cancel
Direction	Protocol	Local ports	Remote ports	<u>A</u> dd Item
In In/Out	TCP UDP	all ports all ports	all ports all ports	<u>E</u> dit Item
				<u>D</u> elete Item

- *Edit Service* opens the *Service Properties* dialog window where you can edit the existing parameters defined for a specific service.
- Delete Service deletes the defined service (and removes the information about the service from the list of services)
- Clone Service makes creating a new service record easier and more comfortable for you: To use this option, highlight a service in the list of services (Services dialog) and press the Clone Service button. A new service record will be created with predefined parameters taken from the definition of the cloned service. Then you can easily edit the parameters for the new service.

g) Networks

The *Networks* tab offers a list of networks that the application communicates with. You can add new networks, edit parameters of the currently defined networks, and delete a defined network:

irewall Configuration - Computer in domain eneral Profile Profile switch Applications System Networks	2 Log
Name	Add Matwork
All Remote Networks	Addinetwork
🛸 Internet	<u>E</u> dit Network
■#All Local Interfaces All Local Interfaces All Amount of the second	<u>D</u> elete Network
	C <u>o</u> py Network
You are only able to add, edit, or delete remote network definitions.	Local network
definitions depend on your PC hardware configuration, and cannot t	Apply

One or more network interfaces may be listed within the Defined networks list. If you wish Firewall to stop filtering traffic coming through one of the interfaces, simply uncheck the required check box located to the left of the network interface's name.

Stopping traffic filtering for a particular network interface can be useful in the following situation: If your computer is connected to the Internet by one network interface and to the Local Area Network (LAN) by another interface, it is possible to select traffic filtering for the Internet interface and leave the LAN connection unfiltered, (as the LAN has a lower risk of potential threats).

The dialog window additionally provides the following operating buttons:

• **Add Network** – opens a new **Network Properties** dialog where you can define the new network name and set its parameters:

From: To: Address: Mask:	0.0.0.0
To: Address: Mask:	0.0.0.0
Address: Mask:	· · · ·
Mask:	
Address:	123. 25 . 45 . 255
emote netwo ardware conf	rk definitions. Local iguration, and cannot
	Address: mote netwo rdware conf

- *Edit Network* opens the *Network Properties* dialog window with parameters already set for a specific network, and allows you to edit them
- o **Delete Network** deletes the defined network from the list of networks
- Copy Network makes creating a new network record easier and more comfortable for you: To use this option, highlight a network in the list of networks (Networks dialog) and press the Copy Network button. A new network record will be created with predefined parameters taken from the definition of the cloned network. Then you can easily edit the parameters for the new network.
- h) Log

📕 Firewall Configuration - Computer in domain 🛛 🔹 👔				
General Profile Profile switch Applications System Networks Log				
Date and time	Action	Application	~	Add/Edit
2006-09-07 10:59:23	Block	C:\Program Files\lot	_	Application
2006-09-07 11:29:02	Block	C:\httpd\Apache2\b		
2006-09-07 11:29:02	Block	C:\Program Files\Op		Hide Details
2006-09-07 11:29:02	Block	C:\Program Files\lot		
2006-09-07 11:29:02	Block	C:\Program Files\lot		
2006-09-07 11:29:02	Block	C:\Program Files\lot		
2006-09-07 11:29:02	Ask	C:\httpd\Apache2\b		
		1	~	
<		>		
Information:				
Date and time: 200	6-09-07 1	0:59:23	~	
Action: Block				
Application: C:\Program Files\lotus\notes\nInotes.				
Direction: Out				Emptuling
Local address: localhost:1175				Empty cog
Remote address: 10.2	210.100.3	37:1352		Befrech
J				Liencen
2		OK Ca	ncel	Apply
-	_		_	

Within the *Log* tab you are able to review the list of all logged **Firewall** actions and events with a detailed description of relevant parameters.



The main part of the *Log* tab is divided into two sections:

• Logged Firewall Actions and Events Section

This section offers an overview of all actions and events that were performed by **Firewall** with their parameters recorded within the log file.

By default, the *Log* tab opens in the standard mode with the following parameters provided for each of the logged actions:

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

If you find the provided parameters insufficient, and want to see more, use the *Show Details* button to switch to the advanced log file overview:

ogged Firewall actions an	d events:								
Date and time	Action	Application	User	Directi	Protocol	Local address	Remote address	^	Add/Edit
2006-09-07 10:59:23	Block	C:\Program Files\I	klara	Out	TCP	localhost:1175	10.210.100.37:1352		Application
2006-09-07 10:59:23	Block	C:\Program Files\L	klara	Out	TCP	localhost:1175	10.210.100.37:1352		
2006-09-07 11:29:02	Block	C:\httpd\Apache2	SYST	In	TCP	localhost:80	0.0.0.0:0		Hide Details
2006-09-07 11:29:02	Block	C:\Program Files\	SYST	ln	TCP	localhost:22	0.0.0.0:0	1	
2006-09-07 11:29:02	Block	C:\Program Files\I	klara	Out	TCP	localhost:1175	10.210.100.37:1352	=	
2006-09-07 11:29:02	Block	C:\Program Files\I	klara	Out	TCP	localhost:1175	10.210.100.37:1352	-	
2006-09-07 11:29:02	Block	C:\Program Files\L	klara	Out	TCP	localhost:1175	10.210.100.37:1352		
2006-09-07 11:29:02	Ask	C:\httpd\Apache2	SYST	In	TCP	localhost:80	0.0.0.0:0		
								~	
formation:									
Date and time: 200 Action: Bloc Application: C:\P Votocol: TCE	6-09-07 1 :k ^P rogram F	0:59:23 "iles\lotus\notes\nlnote	s.exe						
Direction: Out	lhost 117	75 1959							Empty Log
remote address: 10.2	10.100.3	17:1352							Defrech

Then you will be able to review the following parameters:

- **Date and Time** exact date and time when the event was encountered
- Action type of action performed
- Application name of the process to which the logged event refers
- User name of the user of the application
- Direction the application's communication direction (in/out, or both ways)
- Protocol type of protocol used
- Local Address the local address of the connection related to the logged event
- Remote Address the remote address of the connection related to the logged event





In both the standard/advance *Log* tab mode you can always use the option of sorting the logged parameters according to a selected attribute: you can sort the data chronologically (press the header of the *Date and Time* column), by type of action (press the *Action* column header), etc.

o Information Section

The *Information* section provides a comfortable and easy to view list of parameters logged for a specific event that is currently highlighted in the above *Logged Firewall Actions and Events* section.

• Log Tab Operating Buttons

The *Log* tab offers three operating buttons:

- Add/Edit Application add or edit an application to be covered by the logging mechanism
- Show/Hide Details switch between the standard/advanced mode of the log file display (as described above)
- *Empty Log* erases information logged for a specific event removing all existing entries
- **Refresh** update the currently displayed information

10.8. Firewall Properties

To display the **Firewall** properties overview use the **Properties** button within the **Firewall** control panel in **Control Center**.

The *Properties* operating button opens a new dialog window with two tabs:

<u>Settings</u>

AVG 7.5

<u>General</u>

a) Settings Tab







The *Settings* tab offers the *Firewall Status* section providing brief information on the *Firewall* state:

- **Firewall**'s status information (running/stopped)
- **Firewall**'s configuration information

Information on the time since **Firewall**'s last restart; on the number of blocked communication attempts and the total number of communication attempts

Further you can select the desired <u>Firewall profile</u>. There are profile options predefined that you can usually select from: *Allow all, Block all, Computer in domain, Computer on the move, Standalone computer.* Typically, each profile covers specific settings of your PC, and an adequate **Firewall** security level is assigned to each of the profiles.

The proper profile option can be selected from the drop-down menu; then confirm your choice using the *Use profile* button.

Within the *Firewall Status* section you can also find the *Configure* operating button that launches the *Firewall Configuration* dialog window – for detailed description of the configuration options please refer to chapter <u>Firewall</u> <u>Configuration</u>.

The bottom part of the *Settings* tab offers two emergency buttons:

- Deactivate Firewall this button allows you to immediately switch the Firewall component off if the need arises. This option is described in detail in the <u>Firewall Deactivation</u> chapter.
- Stop All Traffic this button allows you to block all traffic on every single network port. This option is described in detail in the <u>Stopping All</u> <u>Traffic in Firewall</u> chapter.

Firewall			? 🔀
Settings Genera	al		
Component Protection ag computer. Firewall is run Current area	ainst undesired ning. Current pr is ''Local netwo	access attempts to ofile is "Computer i rk".	o your n domain''.
Display compo Display co Display co Only v	onent omponent when a faulty co ilty condition of	ondition exists the component	
ОК	Cancel	Apply	Help

The *General* tab is divided into two main sections:

Component – the *Component* section provides brief description of the Firewall component main purpose, and brings information on the



b) General Tab

Firewall component version number and release date. It also defines the component's current state.

- Display component in the Display component section you have a chance to adjust the Firewall component's display parameters; you can check/uncheck the following options:
 - Display component this option is marked by default, and the Firewall component's panel is therefore visible in the Control Center.

Uncheck this option if you do not want the **Firewall** component to be shown in the **Control Center**.

Once the component's parameters are set to "not to display", you can always make the component visible in the **Control Center** again via the **Control Center** main menu, selecting the *View/Components/Firewall* option.

Under the *Display component* option you can also select the *Only when a faulty condition exists* option. Then, the **Firewall** component will be shown in the **Control Center** only if the component's state is not OK.

- Ignore faulty condition of the component – having marked this option, the Firewall component will not provide the standard information on the component's current state. Typically, if there is something wrong with any AVG component, the Control Center icon displayed on the system tray turns gray, and the respective component's panel in the Control Center gets highlighted in red.



AVG 7.5



11. Anti-Spam

The **Anti-Spam** component checks all incoming e-mail messages and marks unwanted e-mails as SPAM. It uses several analyzing methods to process each email message, offering maximum possible protection against unwanted e-mail messages. Requires very little maintenance, whilst allowing the user to customize several **Anti-Spam** options.

To keep the **Anti-Spam** component up to date, the **Scheduler** contains a predefined **Anti-Spam rules update** task, which will regularly update all Anti-spam rules, so that protection remains optimal.

• **Note:** If you are using The Bat! as your e-mail client, the Anti-Spam component will be automatically installed as an Anti-Spam plugin into the The Bat! application. The AVG Anti-Spam component settings will then be also available from the The Bat! interface. To change the Anti-Spam component settings directly from The Bat!, navigate via menu Options to Preferences/Protection/Anti-Spam, select AVG Plugin for The Bat!, click Configure button and the settings dialog will come up.

You can access Anti Spam configuration settings directly via the **Control Center** panel buttons:

Anti-Spam Anti-Spam version Spamcatcher 4.0.3 released 12.9.2006 10:05:01.	9 is installed and it is	s using the database
	Update	Properties

The Update button immediately updates the anti-spam rules.

Use the *Properties* control button to open a new dialog window for **Anti-Spam** configuration. The dialog opens with the following tabs:

• Settings



The tab offers general settings for protection against SPAM.



• General settings

VG 7.5

Allows you to 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 (50-90).

Generally we recommended to set 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 SPAM). The most easily identified SPAM will be filtered out, but a significant amount of SPAM may still be allowed through.
- *Value 80-89* E-mail messages likely to be SPAM will be filtered out. Some non-spam messages may be incorrectly filtered as well.
- Value 60-79 Considered as a quite aggressive configuration. Email messages that are possibly SPAM 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 SPAM messages. This threshold range is not recommended for normal use.
- Value O In this mode, you will only receive e-mail messages from senders in your Whitelist. Any other e-mail messages will be considered as SPAM. This threshold range is not recommended for normal use.
- Modify subject for messages marked as spam tick this check box if you would like all messages detected as SPAM to be marked with a specific word or character in the subject field.
- o **Default** returns all changed settings back to default values.

Blacklist

Anti-Spam 🔹 🕄 🔀
Settings Blacklist Whitelist Performance RBL General
spammer@spammingcompany.com
, Edit Export <u>I</u> mport
Lancei Apply Help





The *Blacklist* tab represents a global list of blocked sender e-mail addresses and domain names whose messages will always be marked as SPAM.

You can compile a list of senders that you expect to send you unwanted messages (SPAM). You can also compile a list of full domain names (like *spammingcompany.com* for example), that you expect or receive SPAM messages from. All e-mail addresses from the listed domains will be identified as spam.

Once you have such a list of senders and/or domain names prepared, you can enter them by two different ways:

- **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 e-mail 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.

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

Whitelist

Anti-Spam				? 🗙
Settings Blacklis	t Whitelist	Performa	ince RBL	. General
sender@grisoft.o	:om			
Edit		vport	1	mport
		Vpor		
OK	Cancel	A	pply	Help

The *Whitelist* tab represents a global list of approved sender e-mail addresses and domain names whose messages will never be marked as a SPAM.

You can compile a list of senders that you do not expect to send you any unwanted messages (SPAM). You can also compile a list of full domain names (like *grisoft.com* for example), from that you do not expect any SPAM messages as well.

Once you have such a list of senders and/or domain names prepared, you can enter them by two different ways:





- **Edit** press this button to open a dialog, where you can manually insert 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 with e-mail addresses or 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.

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

• Performance

Anti-Spam		? 🔀		
Settings Blacklist Whi	telist Performa	ance RBL General		
Engine performance set	ttings			
1 1		·		
Low memory		High performance		
To identify spam: Use advanced rules ar Basic and advanced ru identify spam. All messa recommended setting.	nd the on-line ch Iles and training ages are checke	neck. I data are used to ed on-line. This is		
Advanced Settings				
Advanced settings are available by editing the configuration file. We do not				
OK Can	icel Aj	pply Help		

The tab offers performance settings.

- **Engine performance settings** move the slider left or right to change the level of scanning performance. There are four possible stages:
 - Use rules and spam database cache (highest performance)

This mode will consume large amount of memory. During the scanning process to identify spam, the following features will be used: Rules and SPAM database cache, basic and advanced rules, spammer IP addresses and spammer databases.

- Use advanced rules

During the scanning process to identify spam, only basic and advanced rules and training data will be used. *This mode is recommended to all newer computers.*

- Use basic rules only

During the scanning process to identify spam, only basic rules and training data will be used. This settings allows the Anti-Spam engine to run very fast and consume a small amount of memory, but SPAM detection is not as reliable as if Advanced rules are selected.

Do not use rules (lowest memory usage)

During the scanning process to identify spam, 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.

 Advanced settings - Press the Edit button to view the Anti-Spam configuration file, where all advanced settings are available for editing.

Note: We strongly recommend not to change the content of this file, unless you are fully familiar with all advanced settings of Spamcatcher (Mailshell Inc.). Any inappropriate change to the file may result in bad performance or component incorrect functionality/failure.

• RBL



The *RBL* tab offers the *Query RBL servers* option. RBL (Realtime Blackhole List) server is a DNS server with an extensive database of known spammer senders. When this feature is switched on, all e-mail messages will be verified against the RBL server database and if marked as spam if identical to any of the database entries.

The *RBL servers list* allows you to define specific RBL servers locations. By default, two RBL servers addresses are specified. We recommend to keep the default settings unless you are an experienced user and really need to change this settings.

The RBL servers databases contain the latest up-to-the-minute spam fingerprints, to provide the very best and most accurate spam detection. This feature is especially useful for users who receive large amounts of spam that is not being normally detected by the **Anti-Spam** engine.

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 over to the server!





• General



The *General* tab offers an overview of general information on the **Anti-Spam** component, and allows you to define whether the component should be displayed always, or only when a faulty condition exists, or whether the component's faulty condition should be ignored.





12. Virus Vault

The *Virus Vault* application 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.

12.1. Moving Suspect Objects into the Virus Vault

If a suspect/infected object is detected during scanning, and reported in the test results, you should move the object into the **Virus Vault**:

- In the *Test Result* screen (in the relevant tab- *Virus results* or *Spyware found*) select the infected file (virus, registry entry, tracking cookie, etc.) you want to move to the Virus Vault
- Press the *Move to Vault* button to move the object to the vault

📕 AVG 7.5 Internet Security - T	est Center - Basic Interface	_ 🗆 🖂
Program Tests Results Service Inf	formation	
AVG Internet Security	Security status You are fully protected. Your system is up to date and all installed are working properly.	components
🛐 Switch to Advanced	Test Result Selected Areas Test (12.9.2	006 10:47:42)
Control Center	Result overview Virus results	
🏢 Virus Vault	Object	Result
Test Results	C:\KLARA\DOKUMENTACE\TEST_VIRUS_ADWARE\ C:\KLARA\DOKUMENTACE\TEST_VIRUS_ADWARE\	Virus identified EICAR_T Virus identified EICAR_T
🥏 Check for Updates		
🔀 Exit		>
	Move to Vault <u>G</u> o to file	<u>D</u> etails <u>B</u> ack
For Help press F1	7.5.414 268.12.3/445 2	2082 11.9.2006 20:45

Within the **Virus Vault** you can then examine the object, delete it, and even heal and restore the object when a new cure for this kind of infection is implemented.

12.2. Virus Vault Environment

To open the Virus Vault:

- In the Basic Test Center Interface select the Virus Vault left menu item
- In the *Advanced Test Center Interface* select from the top menu *Program/Launch Virus Vault*
- In the Control Center select from the top menu *Program/Launch Virus Vault*
- From the Windows Start menu:

Start/All programs/AVG 7.5/AVG Virus Vault







The navigation tree in the left section of the **Virus Vault** environment allows you to review infected objects by:

- Files by date
- Files by virus name

All infected objects stored in the **Virus Vault** are displayed in a list in the main box; and for each object the following information is presented:

- **S** object status:
 - infected/suspect object (red crossed circle)
 - o cured object (red cross)
- T object type
 - o *object moved to the Virus Vault* (exclamation mark in the red field)
 - **object's backup created in Virus Vault before healing** (exclamation mark in the blue field)
- Virus name suggested name of the infection
- **Path** the complete path to the suspect object's previous location
- Date of detection time and date when the suspected object was identified
- Filename exact name of the suspect/infected file
- *File size* exact size of the suspect/infected file

12.3. Virus Vault Administration

To administer the **Virus Vault** environment you may use the top menu category *Action* and its options:

Action/Display File Details

to see a review of detailed information on the infected object





Attribute Name	Value	
Object name	eicar.com	
Object path	C:\KLARA\DOKUMENTACE\	
Discovery	Virus identified EICAR_Test	
Date of detection	7.9.2006 9:03:58	
Source computer	KLARAK	
Finder	klara	
File size	68 bytes	
Healable	No	
Source	Backup copy	
Status	Infected	

• Action/Empty the Virus Vault

to delete all contents of the Virus Vault

• Action/Heal file

to heal the selected file if the cure is available; once the file is healed, its status changes to *healed object*.

• Action/Delete file

to remove the selected object from the Virus Vault.

• Action/Restore file (Restore file as)

to restore the suspected object moved to the Virus Vault in its original location; you will be asked to specify the restored file name and location.

Corresponding to the top menu options are the shortcut buttons of the **toolbar navigation** in the upper part of the screen. To show/hide the toolbar select from the top menu **View/Toolbar**.

The rest of the top menu items are similar to those described in other AVG applications. For detailed information please refer to chapter <u>7. AVG Basic Test</u> <u>Center Interface</u>.





13. Tests Review

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. The recommended period for complete system scanning is approximately 1 week.

All the on-demand tests are run from the **Test Center** environment. Tests can be also planned and run according to the preset schedule.

For more information on test scheduling see <u>7.9 Test Scheduling</u> or <u>8.2 Scheduled</u> <u>Tasks</u> sections.

Different test types are available with vendor pre-set parameters, by default.

- Complete Test
- User Test
- Selected Areas Test
- Detailed Test
- Detailed User Test (accessible from Test Manager in the Advance Test Interface)
- System Areas Test (accessible from Test Manager in the Advance Test Interface)

You can change the test configuration according to your own needs. However, for less experienced computer users it is recommended to use the default test configuration.

13.1. Complete Test

The *Complete Test* will scan all hard drives of your computer, and will detect and possibly heal or remove any virus found.

a) Complete Test – Settings

The *Complete Test* can be used either with the default configuration pre-set by the AVG vendor or you can also define your own test settings (however, this is only recommended to experienced users). To edit the *Complete Test* settings follow these steps:

 In the *Basic Test Interface* select from the top menu *Tests/Complete Test settings* to open the dialog window for elementary configuration of the *Complete Test*:





Test Options - "Com	plete Test"		?
 Lest name and description: 	o		
Name:	Complete Lest		
Description:			
Scanning parameters:			
📑 Local hard drives			7
C:V			<u>S</u> elect
Scan files without interr	uption		
🔽 Automatically heal i	infected files		
Scanning properties			
🔲 Scan System Areas bef	ore the test starts		
Detect Potentially Unwa	anted Programs and Spywa	are	
🔽 Use heuristic Analysis			
🔲 Scan inside archives			
File extensions			
C Scan all files			
Scan all infectable files			
Add extensions:			
			<u>S</u> elect
Default	1	οκ	Cancel
			Cancel

This dialog allows you to configure some of the test parameters:

- Test name and description in the Name field the Complete Test text is pre-set by default; and you can enter additional information about the test into the Description field.
- Scan files in the complete test scans the hard disks of your PC and within the AVG Basic Test Interface environment you cannot change these settings.
- Scanning properties in this section you can define the desired scanning methods and functions to be applied during scanning by selecting them from a list. If you prefer not to *Detect Potentially Unwanted Programs and Spyware*, deselect this option. To learn more about *Potentially Unwanted Programs*, navigate to <u>chapter</u> 7.14.
- File extensions specify whether the test should scan all files (Scan all files) or only all 'infectable' files (Scan all infectable files).

If you decide to scan all 'infectable' files you can also define the specific file extensions. Mark the *Add extensions* check box to activate the *Select* button that opens a new dialog. Within this dialog you can see the list of file extensions and corresponding file types; select those that should be scanned:





• In the *Advanced Test Interface* select from the top menu *Tests/Test Manager/Complete Test*:

rest mana		
Test name	Last start time	Test description
Complete Test	7.9.2006 14:44:56	
Duser Test		
Detailed Complete Test		
🞾 Detailed User Test		
🎾 System Areas Test		
P Selected Areas Test	12.9.2006 10:47:42	
2		

Press the *Edit* button to open a dialog window of the *Complete Test* extended configuration with six tabs (to be opened one by one from the navigation tree in the left section of the window):

• Test properties







- *Name* the test name is specified by default as *Complete Test* and cannot be changed
- Description in this field you can specify your own additional information describing the test (specific settings, ...)
- Based on this field contains information about the fact the test is predefined by the program vendor
- Allow interrupted test to resume when test is next started mark this option to allow the test that has been interrupted during its run to resume scanning (at the second start of the test only locations that have not been scanned previously will be examined)
- When finished, display dialog select what information should be displayed when the test is finished

• Objects to scan

Fest properties Dbjects to scan Scan details Report Action to take Advanced settings	Objects to scan All local hard drives User defined path Path/File Note Of C:\ Including subfolders		
	Add Folder Add File(s)	Edit Path	Delete Path
I est Defaults		OK	Cancel

By default, the *Complete Test* scans all hard drives of your computer and you cannot define only a specific location as is possible e.g. with the *Test Target*.

	0	Scan	details
--	---	------	---------

Test properties Dijects to scan Scan details Report Action to take Advanced settings	Scan details General Scan System Areas before the test starts Scan active processes for viruses Use heuristic Analysis Scan NTFS Alternate Data Streams File extensions Scan all files (except those defined below in "Exceptions")
	Scan all intectable files Add extensions: Use Smart scan Exceptions Exclude extensions:
	Archives Scan inside archives Anti-Spyware
? <u>I</u> est Defaults	Enable Anti-Spyware engine Bage Defaults OK Cancel





General – in this dialog you can define whether the system areas should be scanned and if heuristic analysis should be used for scanning. You can also scan all active operating system processes by ticking the Scan active processes for viruses check box. An active process is basically a running application, that may be a regular software program or could be a virus/spyware/malware or different type of danger. Here you can also select not to scan NTFS Alternate Data Streams.

Note: NTFS Alternate Data Streams is a Windows feature that can be misused by attackers (hackers mostly) for hiding data, especially rootkits, viruses, trojans, etc. Therefore it is recommended to keep this settings checked (as by default).

You can also scan all active operating system's processes by ticking the *Scan active processes for viruses* check box. An Active process is basically a running application, that may be a regular software or also a virus/spyware/malware or different type of danger.

- Further, decide whether the scanning should be performed on all files or only on 'infectable' files (*File extensions*), and you may also define extensions of files that will be excluded from scanning (*Exclusions*). You can also select the option of scanning files inside archives (*Archives*).
- In the *Anti-Spyware* section you can disable/enable scanning for spyware/malware with the Anti-Spyware engine (*Enable Anti-Spyware engine* check box).

If you decide to scan only all 'infectable' files, you can also define specific extensions determining files that should be scanned. Select the *Add extensions* option to activate the *Select* (...) to open a new *File extension* dialog:

File exte	nsions		? 🔀
Extensions	File types		ок
123	H.323 Internet Telephony		
🗖 👏 386	Virtual device driver		Cancel
🗖 🗗 669	Winamp media file		
🗖 🎑 🖉 88A	8BA File		
🗖 🎑 88 C	8BC File		
🗖 🎑 88E	8BE File		Colorad
🗖 💇 88F	Adobe Photoshop Plugin		Select all
🗖 🖾 881	Adobe Photoshop Plugin		Invert selection
🗖 🎑 88 P	8BP File		Inveit selection
🗖 🌁 88 S	8BS File		Select bigblighted
🗖 🏹 88×	8BX File		Select highlighted
🗖 🏹 88 Y	8BY File		Grid lines
🗖 🚰 8LI	8LI File		
🗖 🗗 🗖 AAC	Winamp media file	_	Count: 748
ABD	Adobe Bridge Data File	~	<u>H</u> elp

In this dialog you are invited to select from the list of extensions and corresponding files those that should be scanned. The *File extensions* dialog window offers the following control buttons:

 OK – accepts all selected extensions, includes all files with the specified extension into scanning by the Complete Test and closes the File extensions dialog window





- *Cancel* closes the *File extensions* dialog window without applying any changes
- Select all marks all extensions in the list as selected
- Invert selection when selecting a large amount of extensions it might be easier to define extension of file that should not be scanned, and then to invert the selection
- Select highlighted files with a specific extension can be selected directly in the list by clicking the file's name (for multiple selection press the Shift key at the same time) and then marked as selected at once using the Select highlighted button
- Help opens a new window with the dialog related help information

In the *File extension* section you can also apply the *Use Smart scan* option. This option can only be used if you have previously selected that you want to scan only all 'infectable' files. The *Smart scan* function can recognize the file type from its content regardless of the file extension, i.e. it scans 'infectable' files even if these are not defined by their extension as to be scanned but that can still be infected (*e.g. exe files that have been renamed*).

- Exceptions in this section you can on the other hand define extensions of files that should be excluded from scanning by the *Complete Test*. Use the *Select* (...) button to open the *File extensions* dialog again and specify your own definition of files intended for scanning. For a detailed description of this dialog please refer to the previous paragraph.
- Archives this section offers the Scan inside archives option. If the option is allowed, the Complete Test opens and scans also all files saved in common archive types.

o **Report**



The dialog provides a list of situations that can be encountered during the test run. Mark up those situations that you want to be informed about if they occur.

• Action to take





F 4 + i	- Action to take
i est properties	
 Objects to scan 	When a virus is detected
- Scan details	Automatically heal infected files
- Report	 Prompt user (display virus detection dialog)
Action to take	C Continue testing
Advanced settings	Activate scanning window
-	Only when the first virus is detected
	When warning is displayed
	Continue scanning
	C Activate scapping window
	Only when the first warning is displayed
	In only when the first warring is displayed
	Uisplay warning information dialog

- When a virus is detected if a virus is detected during scanning, it can be healed if a cure is available (*Automatically heal infected file* option). If the virus cannot be healed automatically, you can decide about its further treatment based on information about the virus detection (*Prompt user* option) or you can keep on scanning without interrupting the test (*Continue testing* option). Should you decide not to interrupt the test and continue scanning, you can use the following options (*Activate scanning window*, *Only when the first warning is displayed*) to configure the program behavior and specify which way (if at all) you want to be informed about virus detection.
- When warning is displayed similarly, in this section you can define the program behavior in a situation when a warning message pops up (as defined on the previous *Report* tab).
- Advanced settings

est properties	Advanced settings		
Ubjects to scan	Test message windows	20	.a.
- Report - Action to take	Do not display other windows when the	e first dialog times out	nus
Advanced settings	Close Test Center		
	Close AVG upon completion of the test		
	Close AVG only if no virus was found		
	Test priority		
	Set priority of the test when scanning	Lower priority	-
	✓ Enable gaps during file scan	10 milliseconds	-

The dialog allows the setting of the specific test parameters determining the **Test Center** interface behavior:

Test message windows – specify for how long the warning messages should be displayed





- Close Test Center select whether the Test Center should be closed after the test is finished or it should be closed only if the test finishes with negative results
- Test priority in this section you can set/edit the test priority (compared to other running applications) and also define the length of time gaps during scanning (within one test).

Generally it is true: the lower the test priority and the longer the time gap, the longer the whole test takes but at the same time the lower the overall system load. This configuration can be used for instance when you need to decrease system load on older/slower computers.

b) Complete Test - Start

The easiest way to run the *Complete Test* is to press the *Scan Computer* button in the *Basic Test Interface*:



Also, you can run the Complete Test:

- in the *Basic Test Interface* select from the top menu: *Tests/Start Complete Test*
- in the Advanced Test Interface select from main menu: Test manager/Complete Test
- o in the **Test Center** environment just press the F4 key

c) Complete Test – Progress

When the *Complete Test* starts, a new screen is displayed showing the progress and results of the test. If suspect files are found, you will see them in the main box of the screen:





📕 AVG 7.5 Internet Security - T	est Center - Basic	Interface		
Program Tests Results Service Inf	formation			
AVG Internet Security	Security sta You are fully protecte are working properly.	tus d. Your system is up to c	late and all installed	components
Switch to Advanced	File	Result/Infe	ction	Path
	🔝 eicar.com	Virus identi	ied EICAR_Test	C:\KLARA\D(
🔠 Control Center	🕺 eicarcom2.zip	Virus identi	ied EICAR_Test	C:\KLARA\D(
🚻 Virus Vault				
📳 Test Results				
🛷 Check for Updates				
🔀 Exit	<	Ш		
	Scanned objects	44 Infec	ted objects 1	Pause
	Virus identified E	ICAR_Test		Stop
	C:\Program Files\Int	ernet Explorer\iexplore.e	xe	
For Help press F1		7.5.41	4 268.12.3/445 2	2082 11.9.2006 20:45

In the new window you will be able to see for each possible virus found:

- File full name of the infected file
- *Result/Infection* short information on the suspected infection
- Path location of the infected file

In the window's bottom section you can continuously watch the test progress, and review information on:

- Number of scanned objects
- Number of infected objects
- Number of identified viruses
- o Currently scanned file location
- Test status

You can also *Pause/Continue*, or *Stop* the test here by pressing the corresponding buttons.

d) Complete Test – Results

If a virus was identified during scanning you will be immediately informed about it with the following announcement:

📕 AVG Resident Shield 🔹 👔 🔀				
()	Virus Detected!			
While opening file: C:\Documents and Settings\klara\Local Settings \Temporary Internet Files\Content.IE5\YXGNYHC9\eicar[1].com Virus identified EICAR_Test				
	Info			





The Virus Detected dialog informs you about the detected infected file and its location. Selecting the *Do not show this dialog again (scan files without interruption)* option you confirm you do not wish to be informed about the scanning results before the test is completed.

The Virus Detected dialog provides the following control buttons:

- *Ignore* press to ignore the "virus detected" announcement and continue scanning
- **Info** opens the on-line virus encyclopedia where you can find information on the detected virus
- *Heal* allows you to heal the infected object if the cure for this kind of infection is available
- *Move to Vault* moves the infected file into the Virus Vault (and deletes it from its current location)
- **Stop** interrupts the currently run test

AVG is able to analyze and detect executable applications and DLL libraries that could be potentially unwanted within the system. Generally known as Potentially Unwanted Programs (for example spyware, adware).

If a Potentially Unwanted Program is found during the testing, you will be notified by the following dialog:

📕 AVG I	Resident Shie	ld		? 🔀
0		Jnwa	nted Pro	gram
While opening file: C:\KLARA\DOKUMENTACE\adware\B7BC131A TrojanSimulator.exe.mlw				
Not-A-Vi	irus. Test. TrojanS	imulator		
?	<u>I</u> gnore	<u>I</u> nfo	Move to Vault	Add to exceptions

The dialog informs you about the detected Potentially Unwanted Program location. Selecting the *Do not show this dialog again (scan files without interruption)* option you confirm you do not wish to be informed about the scanning results before the test is completed.

The dialog offers several operating buttons you can use for further treatment of the suspicious file:

- *Ignore* ignores the **Resident Shield** warning, and allows you to continue working (and also forbids access to the threat)
- **Info** opens the on-line virus encyclopedia where you can look up detailed information on the identified threat
- *Move to Vault* moves the potentially unwanted object into the Virus Vault (and also removes it from its current location)
- Add to exceptions allows to keep the Potentially Unwanted Program in the system and define it as a Potentially Unwanted Programs Exception. A confirmation dialog will be displayed.
- **Stop** interrupts the currently run test





The test also scans the content of archive files. If there is a suspect object detected inside the scanned archive, you will be informed with the exact dialog as in case of a regular findings. The dialog refers to the whole archive, not to the specific infected file inside it, e.g. you will only be informed about the suspect archive's name and location.

The *Move to Vault* button will transfer the whole archive to the Virus Vault.

However, in the *Test result* overview you can also display detailed information on specific infected files inside the archive. To do so, navigate to the *Virus results* tab, or *Spyware found* tab (will be displayed only if any spyware/malware was found).

In the following screenshot, only the detected archives with infected content are displayed in the test result overview:

📕 AVG 7.5 Internet Security - T	est Center - Basic Inte	erface		_ 🗆 🛛
Program Tests Results Service In	formation			
AVG Internet Security	Security status You are fully protected. Yo working properly.	bur system is up to date and	all installed components a	e 🔽
Switch to Advanced	Test Resul	Complete Test (7. Filter list by result 1	9,2006 9:09:56) type: Hide viruses inside a	rchives
🏨 Virus Vault	Result overview Virus I Object		Result	Status
Test Results	Rootkit.Agent.x Fa	 Display item details	Pootkit.Agent.x	Spyware Family Infected Archive
🔊 Check for Updates	C:\KLARA\DOKUI	Filter list by result type	✓ Display all items	
Exit			Display viruses only Display messages or Display warnings on V Hide viruses inside a	ily rchives
For Help press F1		7.5.4	14 268.12.3/445 2082	11.9.2006 20:45

Right-click your mouse in the grid of the *Test Result* dialog (and its appropriate tab) to open the context menu: in the context menu then uncheck the *Hide viruses inside archives* option to reach the complete display of all objects embedded in the detected archives (in the overview, an archive/embedded object are also distinguished graphically by different icons):







Next to the information on the test type and its launch date in the upper righthand section of this dialog, you can find here the information about the test result list filtering used.

e) Complete Test – Statistics

Once the test is completed, you will be informed about the test results by the *Scanning statistics* dialog that provides comprehensive information on the test progress and results:

Scanning Statist	ics ?	
Ē	Virus Found!	
- Scanning Information	n	
Started:	Manually 12.9.2006 10:12:20	
Ended:	12.9.2006 10:12:22	
Objects scanned:	: 56	
Errors:	0	
	1	
	Display Test <u>c</u> onfiguration	
Virus statistics —		
Infected:	1	
Healed:	0	
Moved to Virus V	ault: 0	
Deleted:	0	
?	<u>S</u> can again <u>C</u> lose	
		-

Whenever infection is detected, AVG tries to heal it automatically. If there is any problem healing the infected file, you will be asked for further instructions. Sometimes, you have to treat the infected files manually. The recommended solution for this case is to move the infected file into the **Virus**





Vault for further treatment with minimum risk of affecting the clean area of your computer.

For more information on Virus Vault refer to <u>12. Virus Vault</u>.

A detailed overview of the *Complete Test* results is available in the *Test report – more details* dialog. To open this dialog:

- o Click the *Display Result* button in the *Virus found* window
- In the *Basic/Advanced Test Interface* select the *Test Results* option from the left menu and choose the appropriate test in the window main section; then press the *Content* button

lest Resul	Selected Areas Test (7.9.2006 9:02:06)	
Result overview Virus	results	
Item Name	Item Value	^
🕍 General properties 👘		
🔍 Report name	Selected Areas Test	
🕠 Start time	7.9.2006 9:02:06	_
🔍 End time	7.9.2006 9:03:57 (total: 1:50.7 Min)	=
🔍 Launch method	Scanning launched manually	
i) Scanning result	Viral infection found	
🔱 Report status	Scanning stopped manually	_
🕍 Object summary		
🔍 Scanned	1244	
المتعادية المتعادية المتعادية	4	Y

13.2. User Test

The **User Test** allows you to use the default settings of the preset test and to configure the parameters according to your own needs at the same time. The test configuration interface, the test launch and progress, and the test results display are basically the same as with the **Complete Test**.

To edit the User Test settings you may do one of the following:

- In the *Basic Test Interface* select from the top menu *Tests/User Test settings*
- In the *Advanced Test Interface* select from the to menu *Tests/Test Manager/User Test* and click the *Edit* button
- In the **Test Center** environment use the *Ctrl* + *F5* keyboard shortcut

For further User Test settings options refer to the <u>Complete test settings</u> related section of this chapter.



Copyright (c) 1992-2006 GRISOFT, s.r.o. All rights reserved.





To run the User Test you can:

- In the *Basic Test Interface* select from the top menu *Tests/Start User Test*
- In the Advanced Test Interface select from the top menu Tests/Test Manager/User Test and click the Start Test button
- In the **Test Center** environment use the **F5** keyboard shortcut

For a detailed description of specific dialogs please refer to chapter <u>13.1 Complete</u> test.

13.3. Selected Areas Test

The *Selected Areas Test* examines only those areas of your computer that you have defined as to be scanned (selected folders, hard disks, floppy discs, CDs, etc.) Further test progress in case of virus detection and its treatment is the same as with the *Complete Test*.

a) Selected Areas Test – configuration and launch

The configuration dialog of the *Selected Areas Test* can be opened:

- o from the Basic Test Interface by the Selected Areas Test quick link
- from the Advanced Test Interface selecting the Test Manager/Selected Areas Test option in the left menu

📕 Test properties - "Selected Areas Test"				
Test properties Scan details Report Action to take Advanced settings	Test properties Name: Selected Areas Test Description: Based on: Predefined test ✓ When finished, display dialog			
Iest Defaults	Page Defaults OK Cancel			

In the left section of the newly-opened dialog you can select from several test configuration sections – the test configuration itself is very similar to the *Complete Test* configuration, see chapter 11.1 a) – Complete Test - Settings.

b) Selected Areas Test – Launch and Progress

The Selected Areas Test can be launched:

from the *Basic Testing Interface* via the *Selected Areas Test* quick link

www.grisoft.com

from the Advanced Testing Interface selecting the Test
 Manager/Selected Areas/Start Test option in the left menu





This choice opens a new *Selected Areas* dialog with the navigation tree representing your local disk and network neighborhood; within this tree you can specify the locations that should be scanned:

Selected Areas	? 🗙
Scan Selected Areas	
<doc>;</doc>	-
Desktop My Computer My Network Places My Docal hard drives My Documents folder My Documents My Documents Other settings Other settings Scan System Areas before the test starts	
Scan Selected Areas	

Once the locations to be scanned are defined, the *Scan Selected Areas* button activates and you can press it to confirm your selection and start the test.

The test progress can be observed in the Selected Areas Test dialog:

Selected Hieds Test				
File	Result/Infection	Path		^
🚺 klara@fastclick[2].txt	TrackingCookie.Burstnet	C:\Document	s and Settin	
🚺 klara@ivwbox[1].txt	TrackingCookie.Burstnet	C:\Document	s and Settin	
🚺 klara@media.fastclick[2]	TrackingCookie.Burstnet	C:\Document	s and Settin	
🚺 klara@perf.overture[1].txt	TrackingCookie.Burstnet	C:\Document	s and Settin	
🚺 klara@questionmarket[2]	TrackingCookie.Burstnet	C:\Documents and Settin		'n
🚺 klara@statcounter[1].txt	TrackingCookie.Burstnet	C:\Document	s and Settin	
🚺 klara@statse.webtrendsli	i TrackingCookie.Burstnet C:\Documents and		s and Settin	=
🚺 klara@tacoda[1].txt	TrackingCookie.Burstnet	C:\Document	s and Settin	
klara@www.burstnet[2].txt	TrackingCookie.Burstnet	C:\Document	s and Settin	
Scanned objects 9	Infected objects	19	Pause	
TrackingCookie.Burstnet		1	<u>S</u> top	
Scanning registry) min 01 s	-

In the new window you will be able to see for each possible virus found:

- o File full name of the infected file
- **Result/Infection** short information on the suspected infection
- Path location of the infected file

In the window's bottom section you can continuously watch the test progress, and review information on:

- Number of scanned objects
- o Number of infected objects
- Number of identified viruses
- o Currently scanned file location





o Test status

You can also *Pause/Continue*, or *Stop* the test here by pressing the corresponding buttons.

c) Selected Areas Test – Results

If a suspect file is detected during the test run, you will be informed about it with this warning. For a detailed description of the warning message please refer to chapter 13.1 d) – Complete Test – Results:

AVG Resident	Shield 🔹 👔
\square	Virus Detected!
$\mathbf{\overline{\mathbf{O}}}$	
While opening f \Temporary Interne Virus identified EIC	Ite: U:\Documents and Settings\klara\Local Settings tFiles\Content.IE5\YXGNYHC9\eicar[1].com \B_Test

d) Selected Areas Test – Scanning Statistics

When the test is completed, the test results will be presented to you in the form of a *Scanning statistics* dialog that offers information on the test run and results:

Scanning Statisti	cs		? 🗙
	/iru	is Found!	
 Scanning Information 			
Started:	Manua	lly 12.9.2006 10:12:20	
Ended:	12.9.20	006 10:12:22	
Objects scanned:	56		
Errors:	0		
	Dis	olay Test <u>c</u> onfiguration	
Virus statistics —			
Infected:		1	
Healed:		0	
Moved to Virus Va	ault:	0	
Deleted:		0	
2		<u>S</u> can again	Close

Detailed test results information can also be found in the *Test Result Details* dialog that can be reached:

- from the *Basic Testing Interface* selecting the *Test Results/...specific test.../Details* button in the left menu
- from the *Advanced Testing Interface* vial the left menu option of *Test Results/...specific test...*





13.4. Detailed Tests

The AVG offers detailed alternatives of the *Complete/User Test*. Detailed tests are available within the *Advanced Test Interface* only. The detailed version of each test performs scanning similar to the standard test setting but while each standard test scans the scope of all infectable files, the detailed test version scans all files.

13.5. E-mail Scanner

EMS stands for the *E-mail Scanner*, and it is the AVG application component used to check incoming/outgoing e-mail messages. **E-mail Scanner** can be controlled from **Control Center** – see the component **E-mail Scanner**.

EMS is an alternative solution for checking e-mail messages in e-mail clients that are not directly supported by the AVG application (in the form of a program plugin).

EMS works as a filter between the e-mail program you use (e.g. Outlook Express, Incredimail, Netscape, etc.) and your Internet/e-mail communication provider. AVG collects both incoming and outgoing messages, saves them in a temporary directory for virus scanning, and then actually receives/sends them.

E-mail Scanner Use

You need to know your e-mail program name and version to be able to state whether you should install EMS or not. If you are not sure which e-mail program you use, run the e-mail communication program and find the *Program Information* menu item (or a corresponding menu item).

- a) **You do not need to install EMS** if you use one of the listed e-mail programs:
 - o MS Outlook 97/98/2000/2003 (part of the Microsoft Office installation)
 - o MS Exchange client 4.0, and higher
 - o The BAT! 1.61, and higher
 - o Qualcomm Eudora (32 bit)

In this case, AVG guarantees to protect your e-mail communication with a plugin implemented directly in the AVG installation.

- b) You need to install EMS if you use one of the listed e-mail programs:
 - o MS Outlook Express 4.0, and higher

Copyright (c) 1992-2006 GRISOFT, s.r.o. All rights reserved.

- o Netscape mail
- o Incredimail
- o any other e-mail program

In this case, you need to use the **E-mail Scanner** for monitoring of your electronic mail. By default, **E-mail Scanner** will be installed and run in fully automatic mode. We strongly recommend that you keep to these default settings unless you have an actual reason to change it.

Of course, it is possible to set the **E-mail Scanner** configuration manually according to your needs.





13.6. Command Line Test Launch

In case you need to launch the test from the command line, use the AVGSCAN.EXE file run from the folder where AVG is installed. The command should be in this form:

AVGSCAN.EXE C: /parameter

If you want to test a specific file/folder, in the above mentioned example provide the path to this file/folder instead of C:

The following parameters can be used:

- ERRORLEVEL == 0 /* everything is o.k. */
- ERRORLEVEL == 1 /* user cancelled/interrupted test */
- ERRORLEVEL == 2 /* any error during the test cannot open file etc. */
- ERRORLEVEL == 3 /* change identified */
- ERRORLEVEL == 4 /* suspicion detected by heuristic analysis */
- ERRORLEVEL == 5 /* virus found by heuristic analysis */
- ERRORLEVEL == 6 /* specific virus detected */
- ERRORLEVEL == 7 /* active virus in memory detected */
- ERRORLEVEL == 8 /* AVG corrupted */
- ERRORLEVEL == 9 /* double extension */
- ERRORLEVEL == 10 /* archiv contains password protected files */





14. Program Updates

Any security system can only guarantee reliable protection if it is updated regularly. AVG provides a reliable and fast update service with quick response times. Modern viruses spread very quickly and infect huge numbers of workstations in a very short time period. Therefore, it is necessary that servers especially get updated as soon as possible so that the threat is stopped before end-user machines can be infected.

14.1. Update Levels

AVG offers three update levels to select from:

• Priority update

Priority update contains changes necessary for reliable anti-virus and antimalware 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.

• Recommended update

Recommended update contains various program changes, fixes and improvements.

• Optional update

Optional update reflects changes that are not necessary for program functionality – texts, updates of the setup component, etc. Optional updates can be downloaded and applied together with recommended updates but their importance is rather low.

When scheduling an update, it is possible to select which priority level should be downloaded and applied. Higher update levels automatically include more critical ones.

14.2. Update Types

You can distinguish between two types of update:

• On demand 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 pre-set an update plan. 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.

www.grisoft.com

14.3. Update Schedule

The update files can be downloaded directly from the Internet. To make sure you always get the latest version of update files it is recommended to create an update





schedule that checks for critical updates directly from the Internet at regular intervals.

In both cases, to set up update schedules follow these steps:

In the **Control Center** select the **Scheduler** component from the component list and then, in the bottom part of the window, press the **Scheduled Tasks** button:

📕 AVG 7.5 Internet Security - C	ontrol Center		
Program View Service Information			
AVG Internet Security	Security star You are fully protected components are work	tu s d. Your system is up to dal ing properly.	te and all installed
🛐 Test Center	Component	Status	Description
AVG Help	Anti-Virus Anti-Spyware	Internal Virus Datab Anti-Spyware is inst	Information about status and releas Protection against spyware, adware
🥏 Check for Updates	Si Firewall	Anti-Spam is installe Firewall is running	Protection against spam, i.e. unsolici Protection against undesired access
嫴 Language Selection	Scheduler Resident Shield	Next scheduled task Resident Shield is lo The Virus Vault cont	Automatic (scheduled) triggering of Provides on-access scanning of exec Virus guarantine, safe storage for in
🛨 Rescue Disk Wizard	Update Manager	Last update on 11.9 AVG is active in Win E-mail Scapper is full	Automatic AVG update from the Inte Antivirus scanning in the Windows E Scans incoming and outgoing e-mail
		Your license will expi	Information about the AVG license.
	Sched Next sc	luler heduled task: 12.9.2006	10:04 Anti-Spam rules update. Scheduled Tasks Properties
For Help press F1		7.5.414	268.12.3/444 2082 11.9.2006 13:30

The button opens a new *Scheduled Tasks* dialog window with an overview of the currently configured tasks:

Scheduled '	Task	5	
Name	Туре	Last start	Next start
🛃 Test plan in basic mode	Test	not started yet	12.9.2006 23:00:00
🛃 Update plan in Basic mode	Update	not started yet	12.9.2006 between 20:00 and
📕 Anti-Spam rules update	Anti-Spam	not started yet	12.9.2006 10:04:00
<]	1111		
	20000000000	11 200	

To create a new update plan press the *New schedule* button that opens the *Scheduled task properties* dialog window with four tabs:

- Task
- Perform task
- Action to take
- If missed





a) Update plan configuration/Task tab

The *Task* tab allows you to set the following parameters:

- *Name* this field's default text is set to the *Update plan* but you can change it as needed and specify your own task name
- **Comment** into the **Comment** field you can type in your own additional information describing the scheduled task in detail
- Schedule in a combo box, this item offers a choice of scheduled task types; you can select between Update, Test and Anti-Spam rules update options.
- Schedule options in a combo box, this item offers a choice of preset options.

For an update (specified in the *Schedule* item) you can select the desired update type selecting from:

- Priority update
- Recommended update
- Optional update

For a detailed description of specific update types please refer to chapter <u>14.1 Update Levels.</u>

For a test (specified in the *Schedule* item) you can select the desired test type selecting from:

- Complete Test
- User Test
- Detailed Complete Test
- Detailed User Test

For a detailed description of specific test please refer to chapter <u>13. Test</u> <u><i>Review</u>.

- **Schedule for all users/Schedule for current user only** select whether the newly scheduled task is valid only for the current user, or whether it should hold good for all users on the station
- **Disable this task** confirm this option if you wish to temporarily disable the scheduled task





Scheduled task	properties	? 🗙	
Task Perform task	Action to take If missed		
Marra	II. data alaa		
Name	jupdate plan		
Comment			
Schedule	Update	•	
Schedule options	Optional update		
C Schedule for all	users		
Schedule for c	urrent user only		
Diaphla this took			
Disable (fils (dsk			
-			
?	OK Cancel	Apply	

b) Update plan configuration/Perform task tab

The *Perform task tab* allows you to specify the following parameters:

- *Periodicity* from the list of options in the *Periodicity* section select whether you want to run the update only once or it should be launched regularly. In that case specify the time interval of the task launch.
- Start time if you have previously defined that the update should be performed Only once or if you have selected a specific time interval (Daily, Weekly, Monthly), now you need to define the regular launch time, or the specific day in a week/month.

If you have specified the *Interval* option in the *Periodicity section*, you need to further set up the time interval in hours/minutes.

- **Start date** assign the date when this scheduled task should be considered active
- **End date** optionally you can specify the date till when this scheduled task should be valid

Scheduled	task propertie	s		?
Task Perfor	m task Action to t	ake If mis	sed	
Periodicity Daily		•	Start time 08:00	<u> </u>
Every	1 .	day(s)		
Start date			End date	
6.9.2006	•		6, 9,2006	~





c) Update plan configuration/Action to take tab

On the *Action to take* tab confirm the *Prompt before initiating task* option if you want to be informed about the task being ready to start, and you want to confirm it manually every time. If you decide to activate this option, you can further specify for how long the program should wait for manual confirmation of the task launch, and what should be done if the user does not respond to the prompt within the specified time limit.

📕 Scheduled task propertie	es		? 🗙
Task Perform task Action to	take If missed	1	
Prompt before initiating tas	k		
When no user response withi	n	1	🛨 minute(s)
Start task automaticaly			
cancel task			
?	ОК	Cancel	Apply

d) Update plan configuration/If missed tab

The *If missed* tab allows you to define what the program should do if for some reason the scheduled task is not started at the assigned time:

Scheduled task properties
Task Perform task Action to take If missed If task start time has been missed Prompt user to start the task Run task on computer start Run task when user logs on Cancel task
OK Cancel Apply




15. FAQ and Technical Support

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

If you do not succeed in finding help this way, contact the technical support department at <u>technicalsupport@grisoft.com</u>. Be sure to include your AVG License number in the body of the e-mail.

However, we recommended contacting the Grisoft technical support from the dialog window accessible from all AVG applications (e.g. **Test Center**, **Control Center** ...). To open this dialog, select *Technical support by e-mail* option from the *Information* folder of the application main menu. Then proceed to chapter <u>15.1</u> AVG Diagnostics utility for more information how to process the technical support request.

15.1. AVG Diagnostics utility

AVG Diagnostics is a supportive diagnostic utility distributed by AVG Technical Support. Its main purpose is to obtain information from the host computer. This information helps the Technical Support team to solve your problem with AVG by analyzing the collected logs, error reports, system information, suspicious files, your own comments and other data.

Note: Under no circumstances does the AVG Diagnostics utility send any personal or other sensitive data from your computer without the user's explicit permission. The user is able to check the content of all collected files and to prevent any of them from being sent to AVG Technical Support.

a) **AVG Diagnostics** starts with the following screen asking for a service code:

📕 AVG Diagnostika - 7.5.418	? 🔀
AVG Diagnostics Welcome to the AVG Diagnostics Wizard	Y.
The AVG Diagnostics utility helps to automatically collect diagnostic data logged d AVG operation. Should you encounter a problem, the data needed can be immedia to the technical support team for further analysis.	uring ately sent
If you have received a service code, please enter it here. However, you can co even without a code.	intinue
Next 2>	Exit

If you have received a service code, please type it into the text field, or use the copy/paste method. The code will automatically set up the correct AVG diagnostics mode which ensures that only the required (and no redundant) data is collected during the **AVG Diagnostics** session.





If you do not have a service code, you can choose any of the following options:

- Contact <u>AVG Technical Support</u> and ask for an *AVG Diagnostics* service code. We strongly recommend this option if you are an inexperienced user.
- Click *Next* and run the AVG Diagnostics utility in full (default) mode.
 In this case continue to step <u>b Error description</u>.
- If you are well experienced computer user you can shut down AVG
 Diagnostics and follow instructions in step <u>d</u>) Advanced settings AVG
 Diagnostics Modes.

b) Error description

This dialog allows you to add your comments and contact information to the data that will be sent to Grisoft technical support team.

📕 AVG Diagnostika - 7.5.418	? 🔀
Error Description Describe the situation when the error occurred	Ye.
Enter your e-mail address: (If you enter an invalid e-mail address we will not be able to reply)	
J Please describe in detail the error and/or the situation when the error occurred.	
	Exit

Try your best to describe in detail what the problem with your AVG installation is, and in what circumstances it occurs; you are welcome to provide any information that might help the technical support team solve the problem.

Above, you can also enter your e-mail address where the technical support team can contact you.

Note: In this dialog, the Back button is disabled; if you want to enter a different AVG Diagnostics Service code, you have to shut down the current AVG Diagnostics session and run AVG Diagnostics again.

When done with selecting, click *Next* button. **AVG Diagnostics** utility will start collecting data. This process may take some time to process.





AVG Internet Security

Collecting data		X
(This o	Collecting data, please wait peration might take several minute	s)

c) AVG Diagnostics Wizard Finalization

This dialog displays an overview of the data (file name and size) that is going to be sent to Grisoft technical support team. Below this, the total size of the data is given.

📕 AVG Diagnostika - 7.5.418		? 🔀	
AVG Diagnostics Wizard Finalization List of files to be sent to the technical support team			
In the following chart you can see the support team.	list of files that will be sent to the Grisoft techr	nical	
File	Size	^	
avg_info.xml system_info.xml env_info.xml MICHALKREJCI(COMPUTER).cab krejcim.DEV(CUPRENT USER).cab Administrator.MICHALKREJCI.cab	15 KB 3 KB 1 MB 1 KB 3 KB 36 bytes 1 V D		
Total size of files to be sent	1 MB		
≤< Back	Next >> Send	Exit	

Confirm the process by clicking the *Send* button. A new dialog will appear with previously entered data and your license number.

Note: If you change the automatically generated part of the e-mail body containing your license number, you might not receive an answer from the Grisoft technical support team!

Sending e-mail via	бмтр		? 🗙
E-mail address:	test@grisoft.cz		
Comment or brief proble	m description:		
THIS IS AUTOMATICA THE LICENSE NUMBE SERVICES OF GRISO 70ISN-AXB-DRE4654- PLEASE, DO NOT CH	LLY GENERATED PART OF YO IS IS NECESSARY FOR ACCES FT COMPANY 4e78e-78e78e ANGE THIS GENERATED TEXT	 DUR E-MAIL SSING THE TECHNICAL SUPPO T	DRT
Sample problem.			
		ОК	Cancel





To send the data to the Grisoft technical support team, click the **OK** button. AVG Diagnostics will then try to automatically send the collected data.

Note: If you are not able to dispatch the report, please make sure that your firewall is not blocking the transmission.

d) Advanced settings - AVG diagnostics modes

Note: Follow these instructions only if you are fully familiar with AVG Diagnostics advanced features.

If **AVG Diagnostics** is already running, shut it down and launch it again from the command line with the respective AVG diagnostics mode parameter.

The AVG diagnostics modes serve to collect only the required and no redundant diagnostic data. Each mode affects the utility behavior so that it only performs the necessary actions, and only displays the necessary dialog boxes to the user, which also speeds up the whole process considerably.

The AVG diagnostics mode can be set:

- automatically by an *AVG Diagnostics Service code* (supplied by AVG Technical Support along with the AVG Diagnostics utility),
- by running **AVG Diagnostics** from the command line with the respective parameter.

For running **AVG Diagnostics** from a command line, see also step <u>e) AVG</u> <u>Diagnostics - Complete Parameter Overview</u>.

For parameters and more info on each individual AVG Diagnostics mode, see the respective topic:

• Full Diagnostics

This is the basic AVG Diagnostics mode.

AVG Diagnostics in full mode creates a complete set of information about the PC: logs, system info, configuration, license, network environment, and other important information that might be useful for solving a problem with AVG.

Parameter: /MODE=FULL, or no parameter

• Sending a suspect file for analysis

This *AVG Diagnostics Mode* allows you to send a suspect file (or more files) for analysis to the Grisoft technical support team.

A *suspect* is typically a file that is not being detected by AVG but you think, for some reason, that it could be infected, or an unwanted program.

Parameter: /MODE=VIRUS

To locate the suspect file directly: /FILE=<file>



The following dialog *Suspected Infection Logging* will appear:

📲 AVG Diagnostika -	7.5.418		? 🔀		
Suspected infection Non-detected files th	a logging Nat might possibly contai	in infection	1		
Within this dialog you consider to be infect new virus that has no	Within this dialog you can select files that AVG claims as virus-free but you for some reason consider to be infected. This may apply to situations immediately following the release of a new virus that has not been defined in the latest virusbase version yet.				
Selected files					
		Add file	Remove file		
	<u>≼</u> < Back	Next ≥>	Exit		

This dialog allows you to add a file to the report which will be sent to Grisoft technical support team.

You can add a file that you believe is infected but has not been detected by AVG.

Click *Add file* to open the browse dialog and locate the file you want to attach. You can repeat this step as many times as needed.

Click *Remove file* to remove the highlighted file from the list.

When done, click *Next* button.

• Sending a false alarm file for analysis

This *AVG Diagnostics Mode* allows you to send a *false alarm* file (or more files) for analysis to Grisoft technical support team.

A false alarm means a file that has been detected by AVG but you believe that it does not contain any viruses.

Parameter: /MODE=FALSE

To locate the false alarm file directly: /FILE=<file>

o Customer Feedback

This *AVG Diagnostics Mode* allows you to send your comments to Grisoft technical support team.

AVG settings and system info will be attached to your message.

Parameter: /MODE=FEEDBACK

• Log Level Setting





Basically, this *AVG Diagnostics Mode* allows you to set the required logging level for the AVG software, so that only the required information is logged when working with AVG and Grisoft technical support team will be able to deal with it effectively.

Parameter: /MODE=LOGLEVEL

Recommended to experienced users only!

📕 AVG Diagnostika - 7.5.41	18		? 🗙
Logging level settings Settings for particular loggers	:		Y.
The logging level for specific context menu (click any item section you can further define 다 아이지	logs can be edite in the tree structu e a log that is not	d by selecting the required se re in this window to open). In specified in the ROOT section All Debug Default Detail Fron Fratal Info Off Warning	ttings from the the CUSTOM n by default.
	K Back N	lext≥>	Exit

The left section displays an expanded logger tree. The AVG7 branch contains all default AVG loggers; the CUSTOM branch allows you to define a new logger (double-click <new item>). To specify a path for the logger, use dots, e.g. AVG7.AvgWB.MyLogger.

To remove a user-defined logger, right-click it and select *Remove logger*.

You can set a specific logging level for any item in the tree - available logging levels are shown in the right section of the dialog. Right-click an item and select the desired logging level from the context menu. If you want to apply your selection to all subordinate loggers, select *Apply to all* first.

When finished, click *Save* button to confirm and save the settings. (The *Next* button is disabled in this dialog.)

Then click *Exit* to shut down the *AVG Diagnostics* application.

• AVG Failure Detection

This **AVG Diagnostics Mode** allows you to detect and send for analysis any ERR and DMP files (only present if your AVG installation has previously broken down). Absence of these files indicates that there has been no AVG failure.





If an AVG failure is detected, a confirmation dialog with the error files overview appears and you are asked whether you wish to send them for analysis.

When running **AVG Diagnostics** in the *Failure Detection Mode* next time, only newly detected error files will be reported.

Parameter: /MODE=ERRDUMP

e) AVG Diagnostics - Complete Parameter Overview

In the list below you will find complete overview of all **AVG Diagnostics** parameters.

Parameter	Description
No parameter	Launches AVG Diagnostics in the full (default) mode.
/CODE= <code></code>	Allows you to enter the AVG Diagnostics Service code you obtained from AVG Technical Support. The code automatically sets up the required AVG Diagnostics mode.
/MODE=FULL	Launches AVG Diagnostics in the full (default) mode.
/MODE=VIRUS	Launches AVG Diagnostics in the Sending a suspect file for analysis mode.
/MODE=FALSE	Launches AVG Diagnostics in the Sending a <i>false alarm</i> file for analysis mode.
/MODE=FEEDBACK	Launches AVG Diagnostics in the Customer Feedback mode.
/MODE=LOGLEVEL	Launches AVG Diagnostics in the Log Level Setting mode.
/MODE=ERRDUMP	Launches AVG Diagnostics in the AVG Failure Detection mode.
/LOGROOT= <level></level>	Automatically sets up the Log Level Setting mode and allows you to directly select logging level.
/FILE= <file></file>	In the Sending a suspect file for analysis and Sending a "false alarm" file for analysis modes, it allows you to locate the respective file(s) directly.
	In the full (default) mode, it allows you to attach an additional file to the report.
/CLEARUPD	Deletes any obsolete update and temporary files.
/NOUI	Minimizes the number of displayed dialog windows.





AVG Internet Security

/LNG= <ing></ing>	Allows you to switch the AVG Diagnostics interface to another language. Available languages and their codes:		
	CZ=0x0405	GE=0x0407	PB=0x0416
	SK=0x041b	FR=0x040c	PL=0x0415
	US=0x0409	SP=0x040a	SC=0x081a
	IT=0x0410	HU=0x040e	NL=0x0413



Copyright (c) 1992-2006 GRISOFT, s.r.o. All rights reserved.