AVG 7.5 File Server Edition

User Manual

Document revision 75.3 (1.10.2006)

Contents

1. Introduction

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

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. Anti-Spyware Protection

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.

1.3. Operating Systems Supported

AVG 7.5 File Server is intended to protect servers with the following operating systems:

- Windows 2003 server
- Windows 2000 server
- Windows NT 4.0 server

including 64-bit Windows versions.

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

-

1.4. Reasons to Install AVG 7.5 File Server

You should install **AVG 7.5 File Server** on your server under the following circumstances:

- **The server is used for network files storage**

  AVG 7.5 File Server is able to scan all files as soon as they are stored on the server drive, and detect viruses or possible malicious software that could harm the stored files. All files are also scanned as the clients approach the server, and either open the files, or copy them to their workstations.

- **The server is used as a "terminal server"**

  If your server allows users to access the server remotely, and work directly on the server (i.e. the server is used as a "terminal server"), your server is also exposed to possible harm and virus attack. In this case you should definitely install **AVG File Server**.

- **The server requires AVG 7.5 File Server for further antivirus/anti-malware scanning functionality**

  For example, to provide protection for Microsoft Share Point Portal Server 2003 using AVG for Microsoft Share Point Portal Server 2003, it is necessary to install **AVG 7.5 File Server** first.

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 www.grisoft.com.

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:

a) Refer to the Grisoft website and download the latest version of the **AVG 7.5 File Server** installation package from the Grisoft website at www.grisoft.com, downloads section.

b) Download the installation file and save it on your local disk.

c) Start the installation by executing the downloaded file.

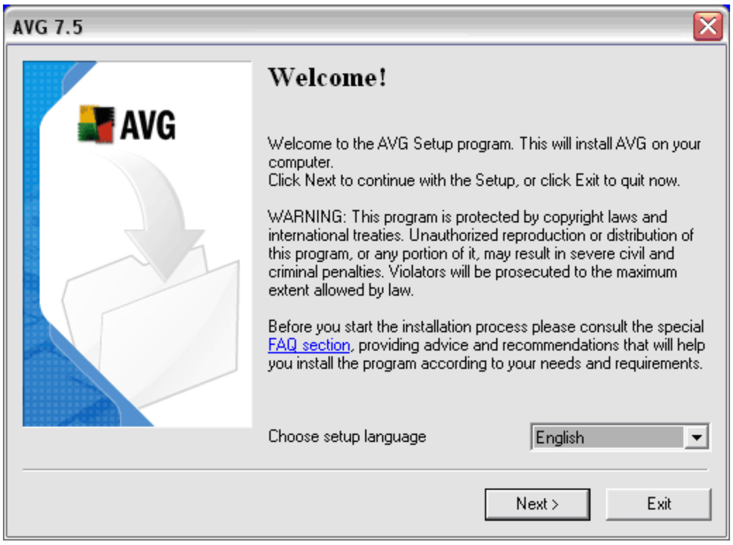
3. Installation Process

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:



Welcome!

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.

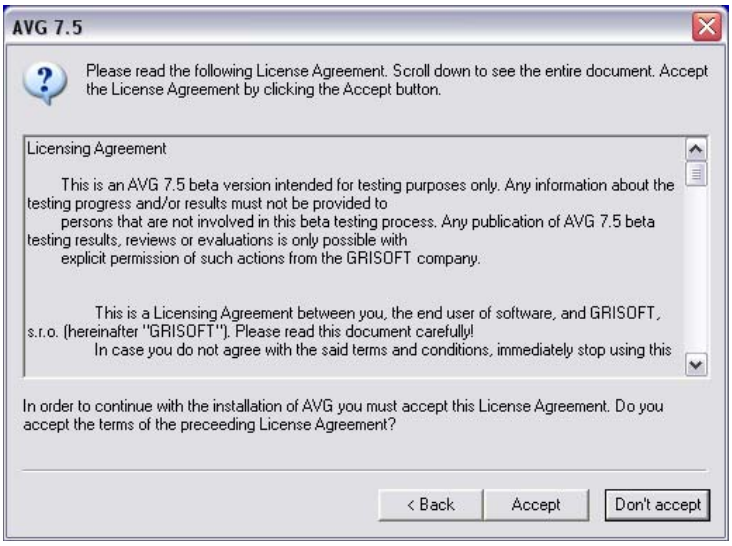
WARNING: This program is protected by copyright laws and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties. Violators will be prosecuted to the maximum extent allowed by law.

Before you start the installation process please consult the special FAQ section, providing advice and recommendations that will help you install the program according to your needs and requirements.

Choose setup language: English

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.



Please read the following License Agreement. Scroll down to see the entire document. Accept the License Agreement by clicking the Accept button.

Licensing Agreement

This is an AVG 7.5 beta version intended for testing purposes only. Any information about the testing progress and/or results must not be provided to persons that are not involved in this beta testing process. Any publication of AVG 7.5 beta testing results, reviews or evaluations is only possible with explicit permission of such actions from the GRISOFT company.

This is a Licensing Agreement between you, the end user of software, and GRISOFT, s.r.o. (hereinafter "GRISOFT"). Please read this document carefully!
In case you do not agree with the said terms and conditions, immediately stop using this

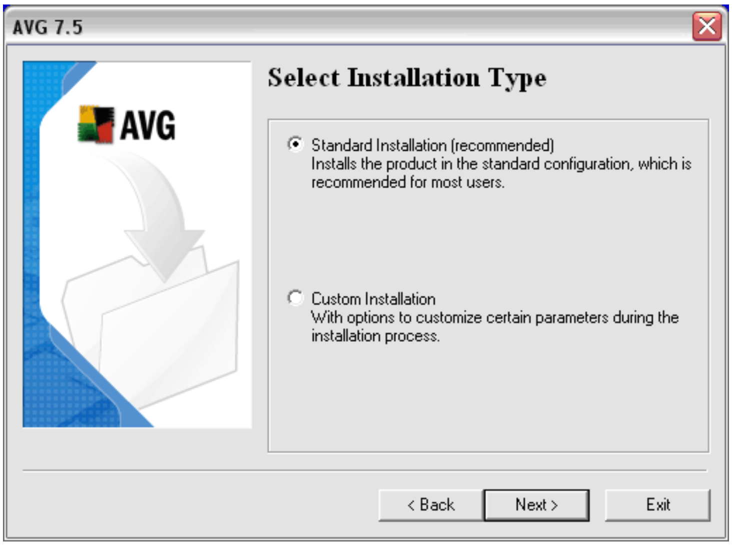
In order to continue with the installation of AVG you must accept this License Agreement. Do you accept the terms of the preceeding License Agreement?

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).

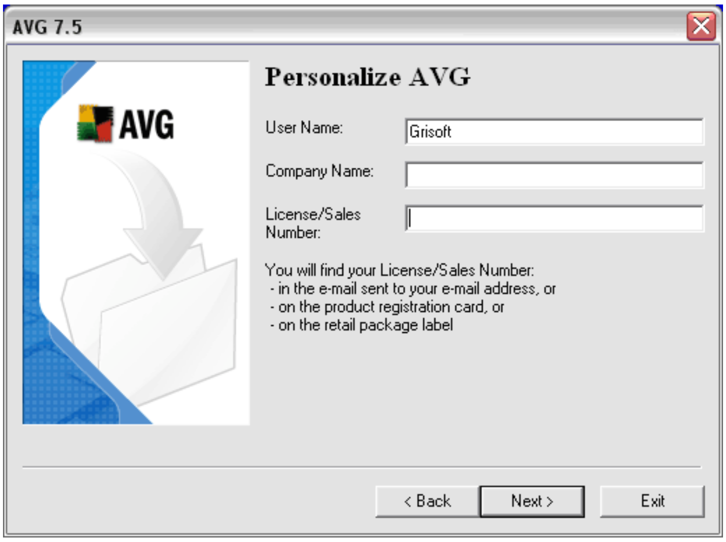


Select Installation Type

● 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.

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:



Personalize AVG

User Name: Grisoft

Company Name:

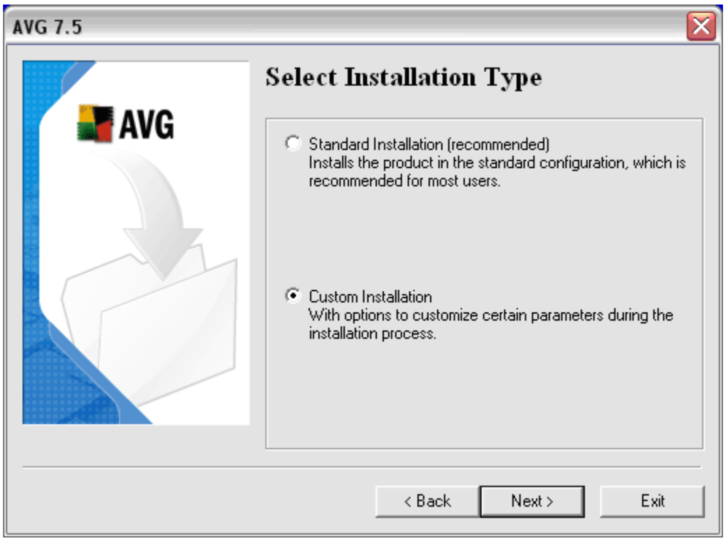
License/Sales Number:

You will find your License/Sales Number:
- in the e-mail sent to your e-mail address, or
- on the product registration card, or
- on the retail package label

Confirm the entered license data by pressing the ***Next*** button to continue to the Installation Summary 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.



AVG 7.5

Select Installation Type

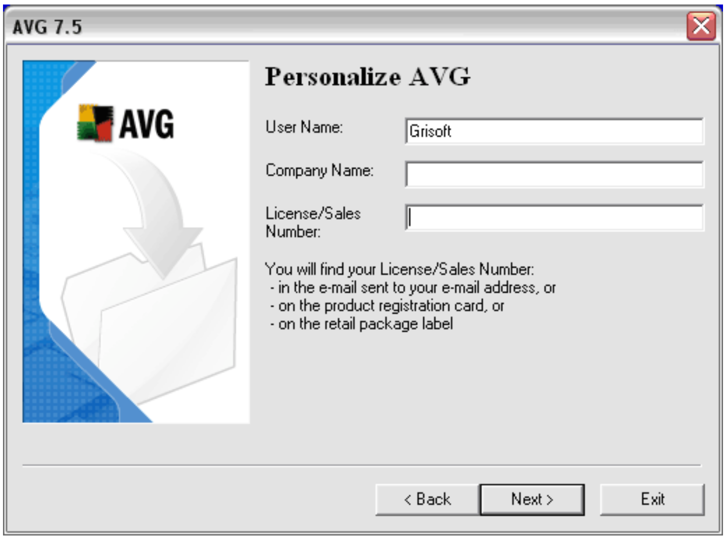
○ Standard Installation (recommended)
Installs the product in the standard configuration, which is recommended for most users.

● Custom Installation
With options to customize certain parameters during the installation process.

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

o ***Personalize AVG***

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



AVG 7.5

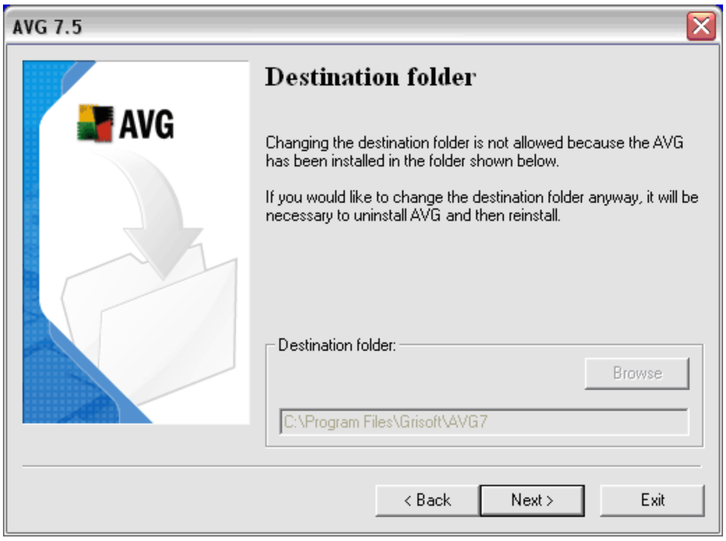
Personalize AVG

User Name: Grisoft
Company Name:
License/Sales Number:

You will find your License/Sales Number:
- in the e-mail sent to your e-mail address, or
- on the product registration card, or
- on the retail package label

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

Changing the destination folder is not allowed because the AVG has been installed in the folder shown below.

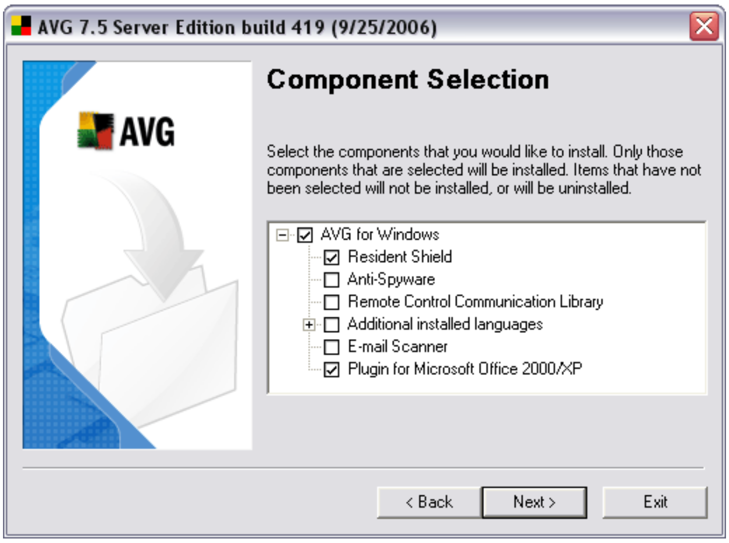
If you would like to change the destination folder anyway, it will be necessary to uninstall AVG and then reinstall.

Destination folder: C:\Program Files\Grisoft\AVG7

- ***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.


AVG 7.5 Server Edition build 419 (9/25/2006)

Component Selection

Select the components that you would like to install. Only those components that are selected will be installed. Items that have not been selected will not be installed, or will be uninstalled.

- ☑ AVG for Windows
  - ☑ Resident Shield
  - ☐ Anti-Spyware
  - ☐ Remote Control Communication Library
  - ☐ Additional installed languages
  - ☐ E-mail Scanner
  - ☑ Plugin for Microsoft Office 2000/XP

- ***E-mail Scanning***

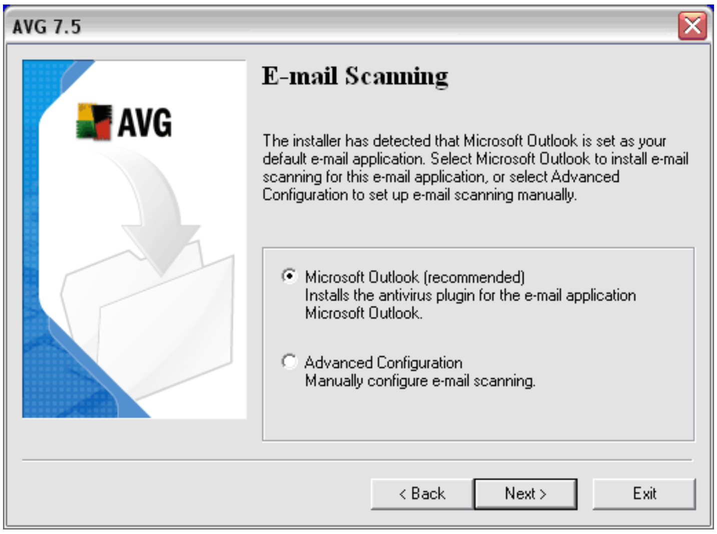
  E-mail scanning provided by **AVG 7.5 File Server** is only suitable for protecting your e-mail client on the fileserver itself. As it is not normal practice to run an e-mail client on a fileserver, by default the ***E-mail***

Scanner is not installed. If you selected to install the e-mail scanner (in the previous dialog), then follow the steps below, else go directly to 3.4 Installation Summary.

Note: The ***E-mail Scanner*** is not for scanning all mail on a mail server. For scanning all mail on a mail server, please refer to **AVG 7.5 Email Server** Edition.

- ***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 e-mail programs the setup will automatically detect it, and recommend you to install a direct plugin for your e-mail client (see picture).



E-mail Scanning

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.

● Microsoft Outlook (recommended)
Installs the antivirus plugin for the e-mail application Microsoft Outlook.

○ Advanced Configuration
Manually configure e-mail scanning.

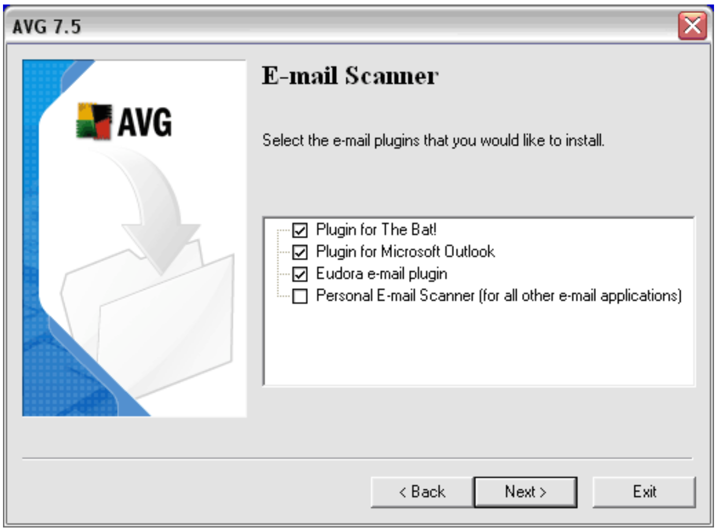
For other e-mail programs, AVG will provide comprehensive e-mail scanning using the **E-mail Scanner** component. In that case the setup dialog offers the recommended option of **Personal E-mail Scanner**.

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

o ***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:



E-mail Scanner

Select the e-mail plugins that you would like to install.

- ☑ Plugin for The Bat!
- ☑ Plugin for Microsoft Outlook
- ☑ Eudora e-mail plugin
- □ Personal E-mail Scanner (for all other e-mail applications)

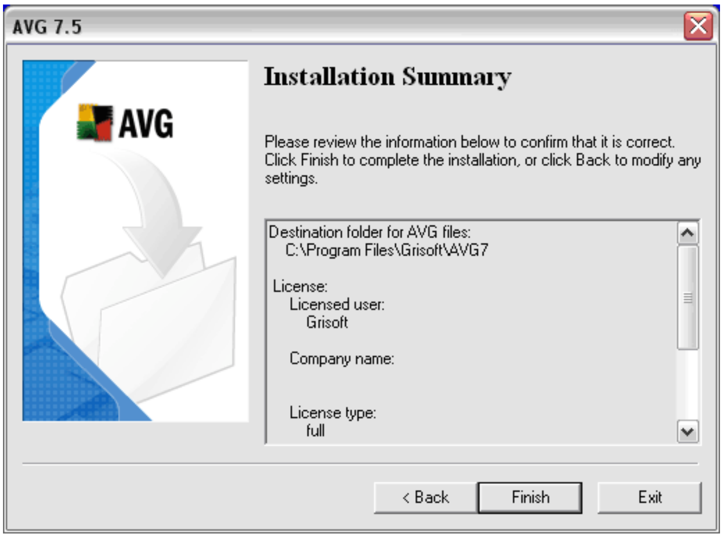
You can select a plugin for the specific e-mail program you use. If your e-mail program is not directly supported, select the ***Personal E-Mail Scanner*** option.

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 www.grisoft.com*.

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

3.4. Installation – Installation Summary

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



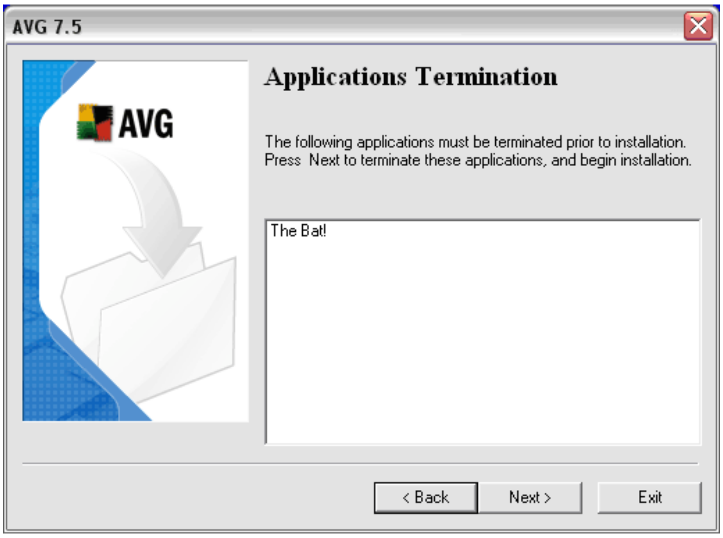
Installation Summary

Please review the information below to confirm that it is correct. Click Finish to complete the installation, or click Back to modify any settings.

```
Destination folder for AVG files:
   C:\Program Files\Grisoft\AVG7

 License:
    Licensed user:
       Grisoft

    Company name:


    License type:
       full
```

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

Applications Termination

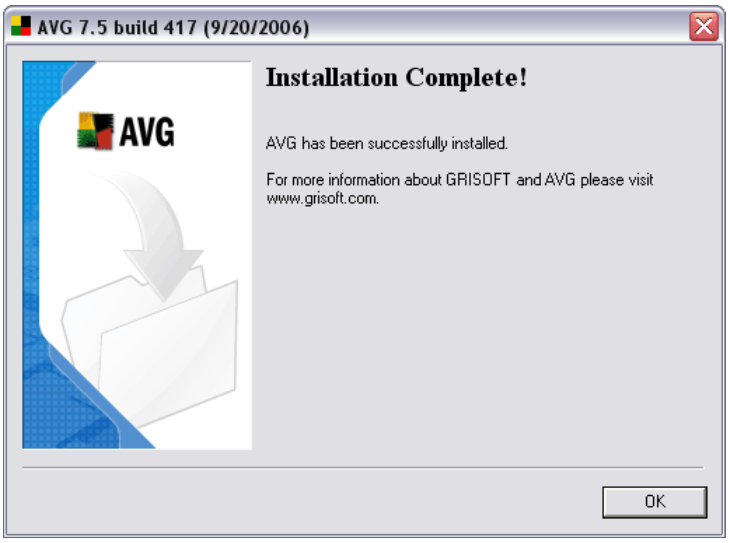
The following applications must be terminated prior to installation. Press Next to terminate these applications, and begin installation.

The Bat!

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

The installation process is finalized with the ***Installation complete*** dialog. Click on the ***OK*** button to complete the installation (on some operating systems the computer may have to restart).



AVG 7.5 build 417 (9/20/2006)

Installation Complete!

AVG has been successfully installed.

For more information about GRISOFT and AVG please visit www.grisoft.com.

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.*

4. AVG First Run

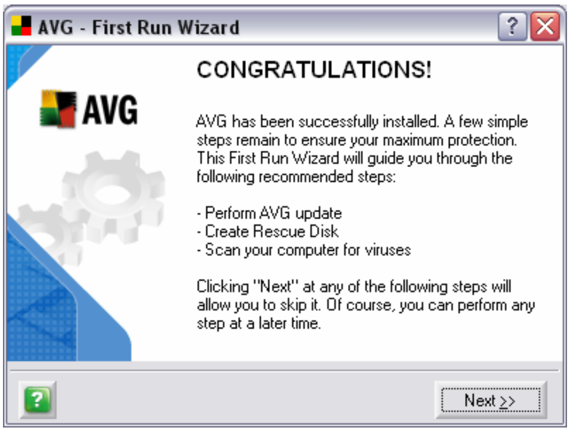
4.1. First Run Wizard

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:



CONGRATULATIONS!

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:

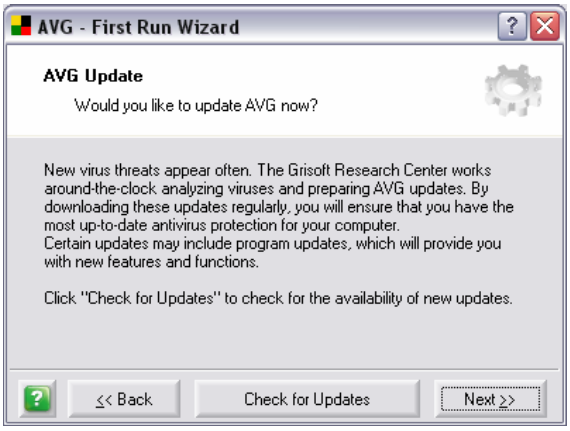
- Perform AVG update
- Create Rescue Disk
- Scan your computer for viruses

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.

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:



AVG Update

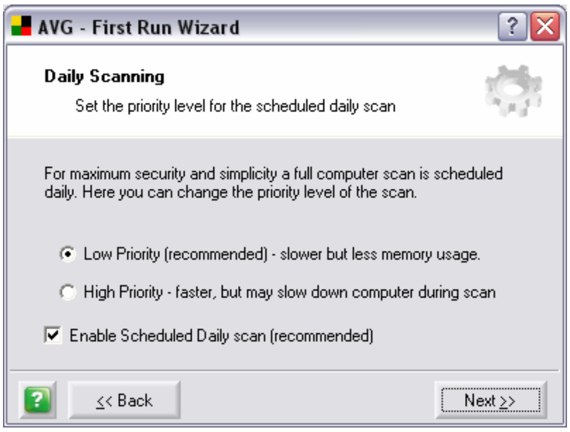
Would you like to update AVG now?

New virus threats appear often. The Grisoft Research Center works around-the-clock analyzing viruses and preparing AVG updates. By downloading these updates regularly, you will ensure that you have the most up-to-date antivirus protection for your computer.
Certain updates may include program updates, which will provide you with new features and functions.

Click "Check for Updates" to check for the availability of new updates.

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

For maximum security and simplicity a full computer scan is scheduled daily. Here you can change the priority level of the scan.

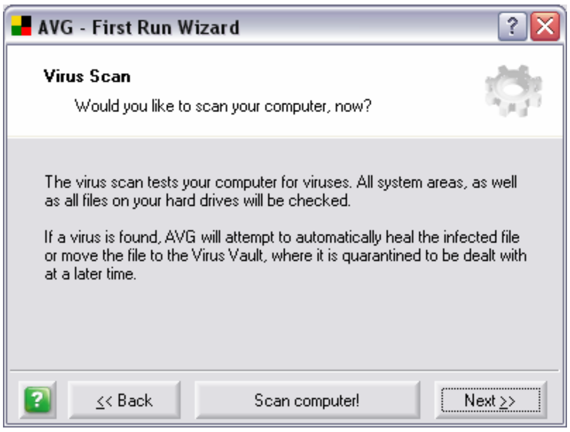
● Low Priority (recommended) - slower but less memory usage.

○ High Priority - faster, but may slow down computer during scan

☑ Enable Scheduled Daily scan (recommended)

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

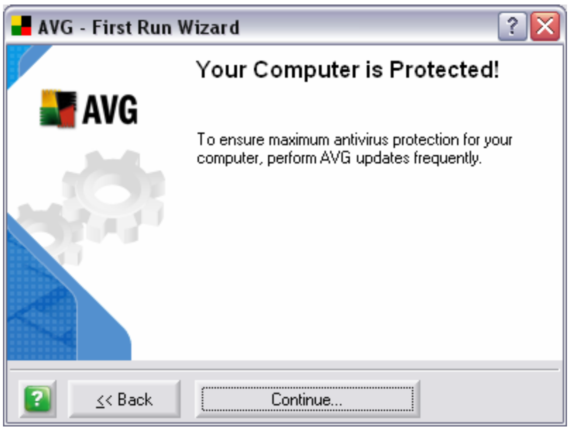
Would you like to scan your computer, now?

The virus scan tests your computer for viruses. All system areas, as well as all files on your hard drives will be checked.

If a virus is found, AVG will attempt to automatically heal the infected file or move the file to the Virus Vault, where it is quarantined to be dealt with at a later time.

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:



Your Computer is Protected!

To ensure maximum antivirus protection for your computer, perform AVG updates frequently.

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 11.1 - 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 9.10 Components controlled from Control Center/Resident Shield.

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 www.eicar.com, 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 11. Test Review 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 12. Program Update

Note: *For* **AVG 7.5 File Server,** *installed on a terminal server, it is highly recommended to set up all essential scheduled tests and updates for all users (Scheduled task properties configuration window / Task tab / Schedule for all users option. This ensures the plans are launched even if nobody is logged in. Also, this way it is guaranteed that no plan will run simultaneously in multiple instances (for example when a user has more concurrent sessions open), which minimizes system resource usage.*

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 www.grisoft.com 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.)

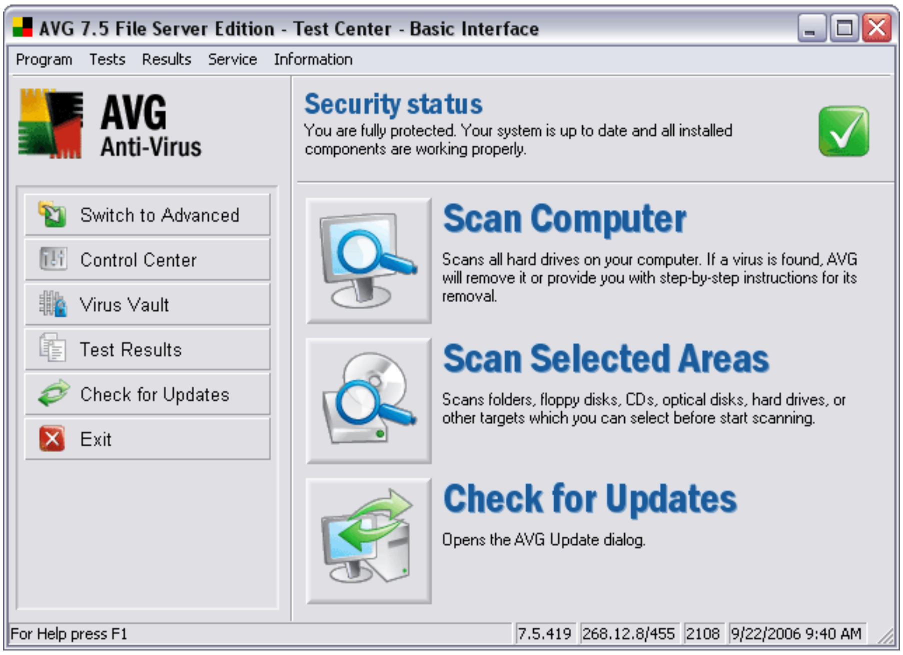
- Press the ***Submit*** button to confirm your registration

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.



Security status

You are fully protected. Your system is up to date and all installed components are working properly.

Scan Computer

Scans all hard drives on your computer. If a virus is found, AVG will remove it or provide you with step-by-step instructions for its removal.

Scan Selected Areas

Scans folders, floppy disks, CDs, optical disks, hard drives, or other targets which you can select before start scanning.

Check for Updates

Opens the AVG Update dialog.

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 8.4 Program Settings/Customize.*

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 8. AVG Advanced Test Interface.

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 9. Control Center.

7.3. Virus Vault

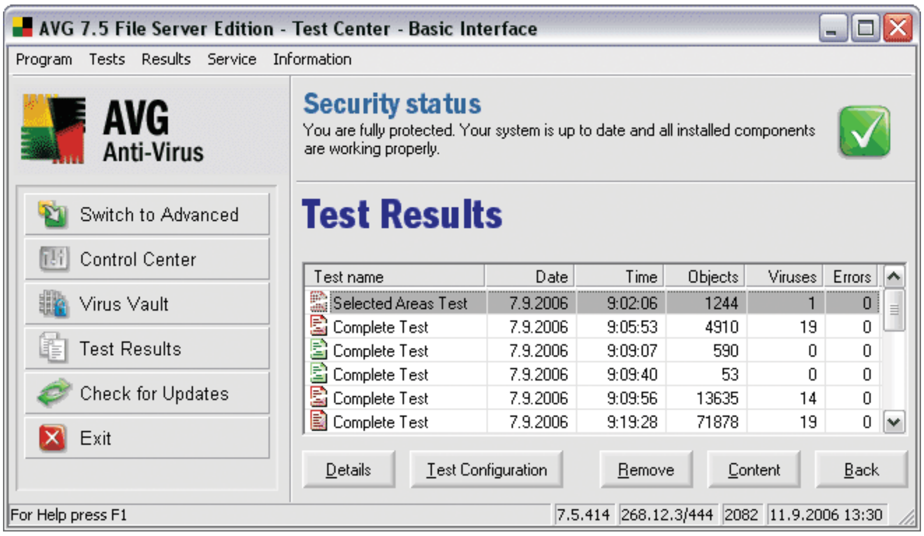
The ***Virus Vault*** shortcut button launches the **Virus Vault** – a safe environment for storing and further treatment of infected objects.

For further description of **Virus Vault** refer to chapter *10. Virus Vault*.

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



Security status

You are fully protected. Your system is up to date and all installed components are working properly.

Test Results

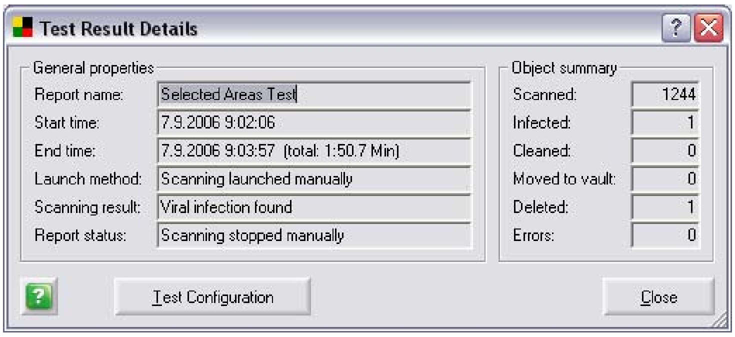
Test name	Date	Time	Objects	Viruses	Errors
Selected Areas Test	7.9.2006	9:02:06	1244	1	0
Complete Test	7.9.2006	9:05:53	4910	19	0
Complete Test	7.9.2006	9:09:07	590	0	0
Complete Test	7.9.2006	9:09:40	53	0	0
Complete Test	7.9.2006	9:09:56	13635	14	0
Complete Test	7.9.2006	9:19:28	71878	19	0

For Help press F1 | 7.5.414 | 268.12.3/444 | 2082 | 11.9.2006 13:30

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 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
Scanning result:	Viral infection found
Report status:	Scanning stopped manually

Object summary

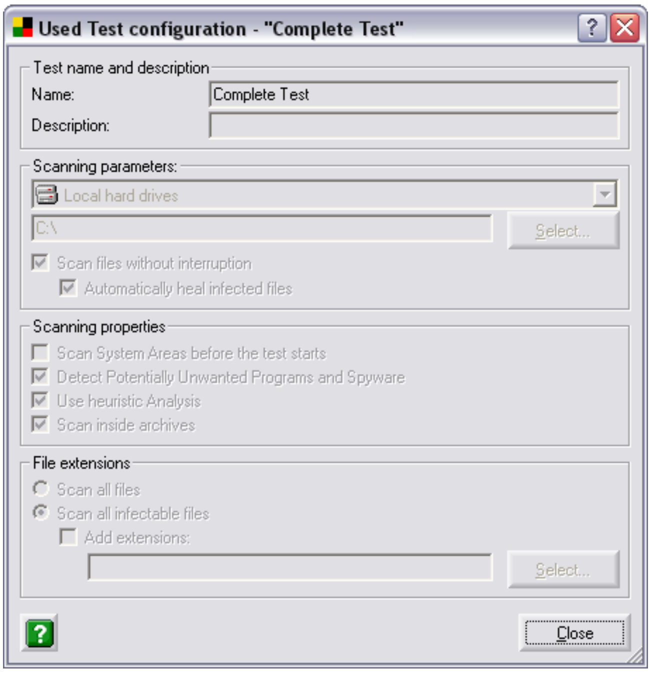
Scanned:	1244
Infected:	1
Cleaned:	0
Moved to vault:	0
Deleted:	1
Errors:	0

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)
- ***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 configuration - "Complete Test"

Test name and description

Name: Complete Test

Description:

Scanning parameters:

Local hard drives

C:\

☑ Scan files without interruption

☑ Automatically heal infected files

Scanning properties

☐ Scan System Areas before the test starts

☑ Detect Potentially Unwanted Programs and Spyware

☑ Use heuristic Analysis

☑ Scan inside archives

File extensions

○ Scan all files

● Scan all infectable files

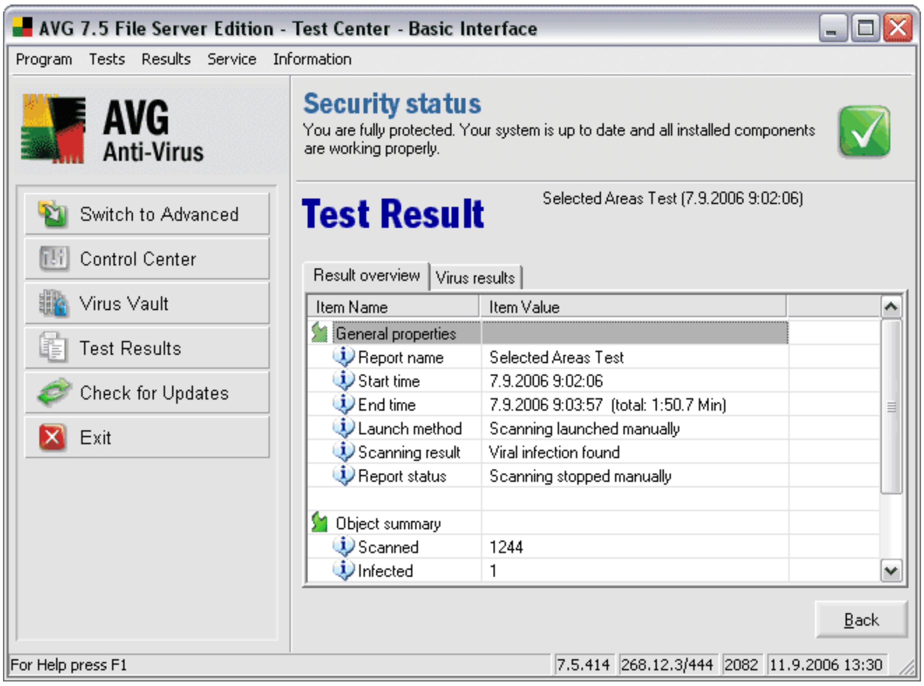
☐ Add extensions:

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:



Security status

You are fully protected. Your system is up to date and all installed components are working properly.

Test Result

Selected Areas Test (7.9.2006 9:02:06)

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
Scanning result	Viral infection found
Report status	Scanning stopped manually
Object summary	
Scanned	1244
Infected	1

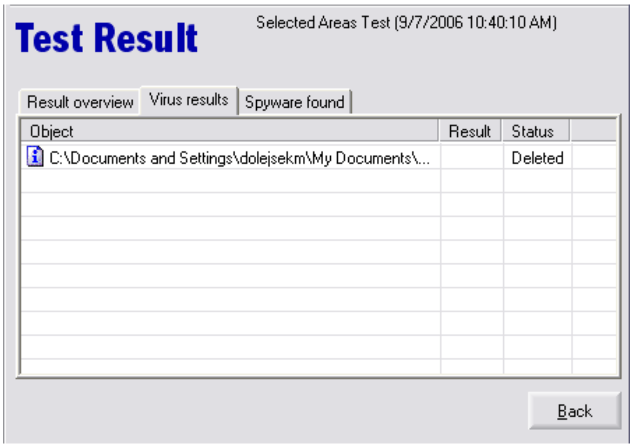
This dialog window is divided into several tabs.

- ***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 .



Test Result

Selected Areas Test (9/7/2006 10:40:10 AM)

Object	Result	Status
C:\Documents and Settings\dolejsekm\My Documents\...		Deleted

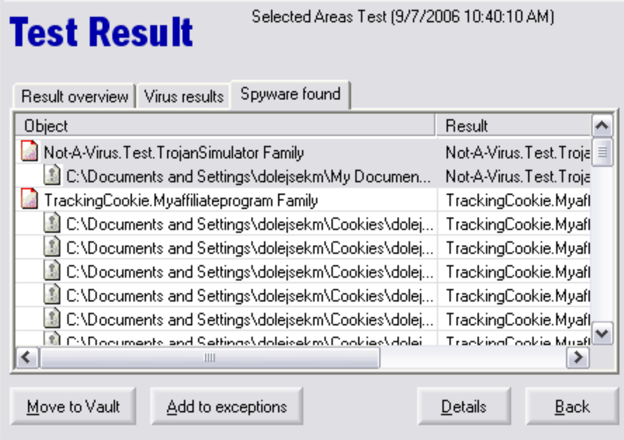
The dialog's operation buttons are:

- ***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.*

o ***Spyware found***

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 (9/7/2006 10:40:10 AM)

Object	Result
Not-A-Virus.Test.TrojanSimulator 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 Settings\dolejsekm\Cookies\dolej...	TrackingCookie.Myafl

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 Potentially Unwanted Programs Exceptions (Chapter 7.14) 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.*

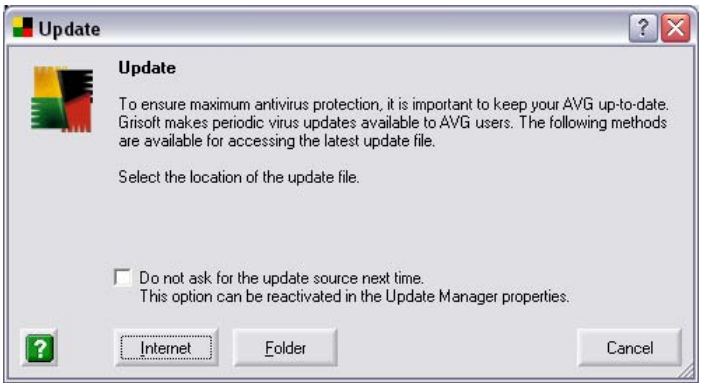
e) Close

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 12. Program Updates.



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.

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 9.12 – Control Center – Update Manager, ***Propertie***s 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)

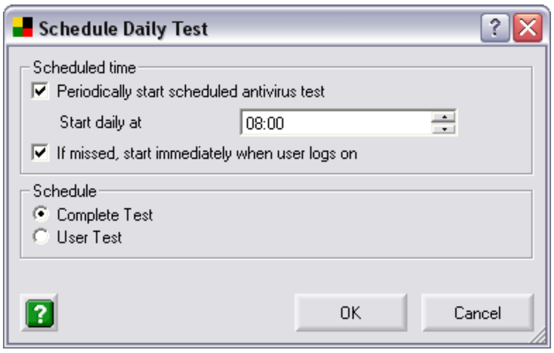
Within this section you specify your own parameters for the AVG tests by default preset by the vendor.

For a detailed test settings description refer to the 11. Test Review.

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 Test

Scheduled time
☑ Periodically start scheduled antivirus test
Start daily at 08:00
☑ If missed, start immediately when user logs on

Schedule
● Complete Test
○ User Test

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

For detailed Advanced Test Interface test scheduling options please refer to chapter 8.2 Scheduled Tasks**.**

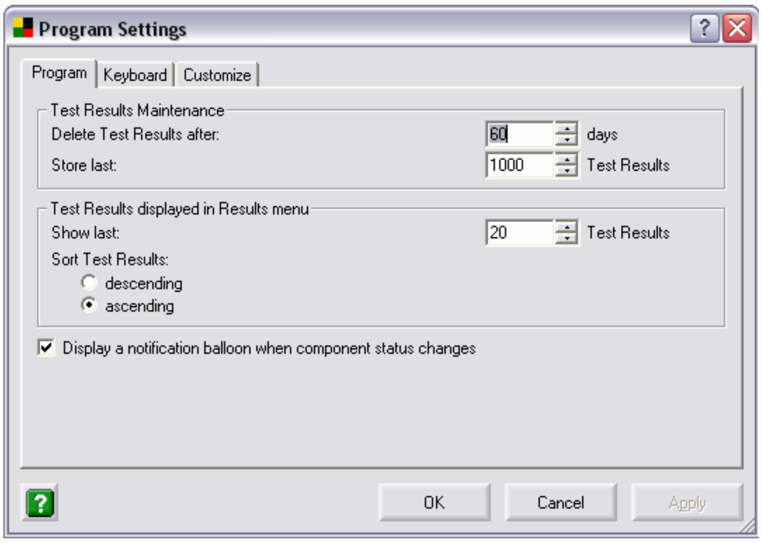
7.9. Program Settings

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



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:

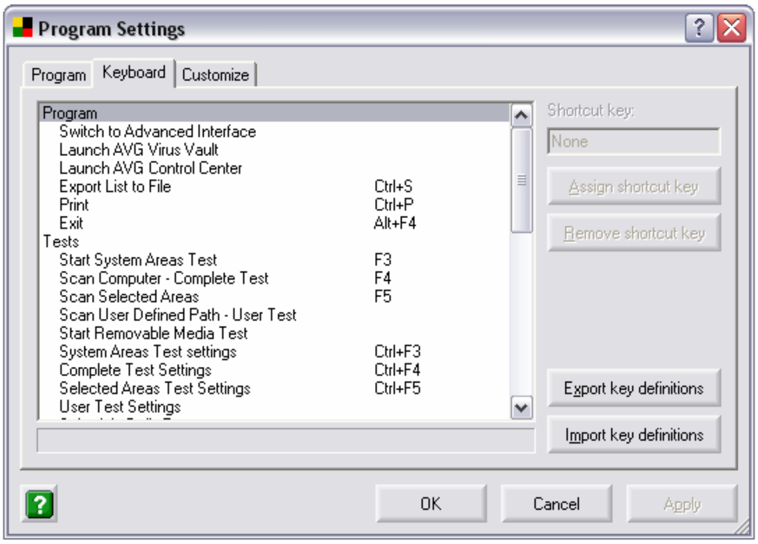
○ descending

● ascending

☑ Display a notification balloon when component status changes

b) Keyboard

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

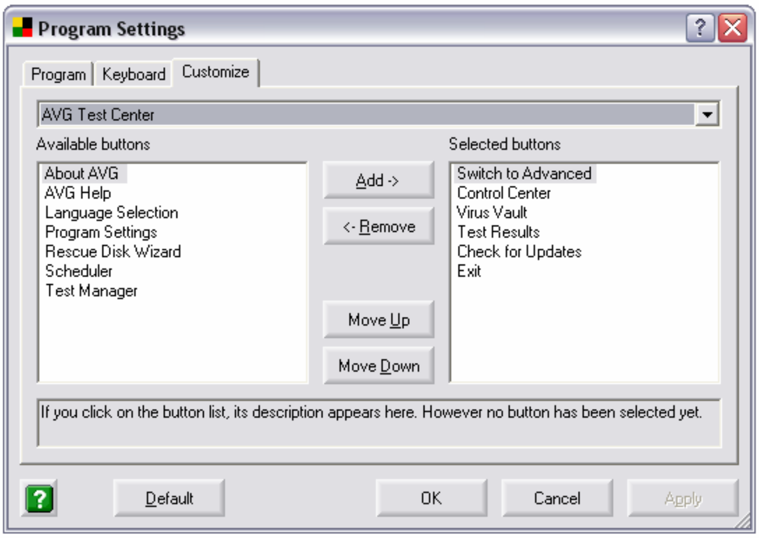


```
Program
   Switch to Advanced Interface
   Launch AVG Virus Vault
   Launch AVG Control Center
   Export List to File                    Ctrl+S
   Print                                  Ctrl+P
   Exit                                   Alt+F4
Tests
   Start System Areas Test                F3
   Scan Computer - Complete Test          F4
   Scan Selected Areas                    F5
   Scan User Defined Path - User Test
   Start Removable Media Test
   System Areas Test settings             Ctrl+F3
   Complete Test Settings                 Ctrl+F4
   Selected Areas Test Settings           Ctrl+F5
   User Test Settings
```

Shortcut key: None

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:



If you click on the button list, its description appears here. However no button has been selected yet.

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 8.4 Program Settings***.***

7.10. Rescue Disk

Service/Rescue Disk

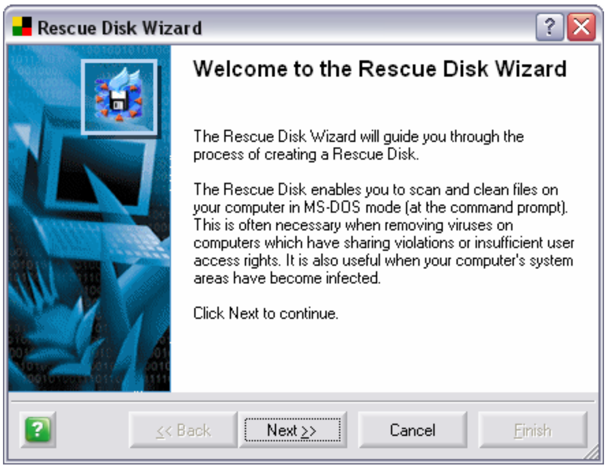
From Windows XP onwards the rescue disk feature is not supported any more.

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:



Rescue Disk Wizard

Welcome to the Rescue Disk Wizard

The Rescue Disk Wizard will guide you through the process of creating a Rescue Disk.

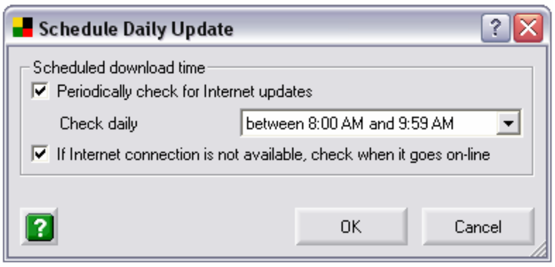
The Rescue Disk enables you to scan and clean files on your computer in MS-DOS mode (at the command prompt). This is often necessary when removing viruses on computers which have sharing violations or insufficient user access rights. It is also useful when your computer's system areas have become infected.

Click Next to continue.

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 updates

Check daily: between 8:00 AM and 9:59 AM

☑ If Internet connection is not available, check when it goes on-line

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

For detailed Advanced Test Interface update scheduling options please refer to 8.2 Scheduled Tasks.

7.12. Event History Log

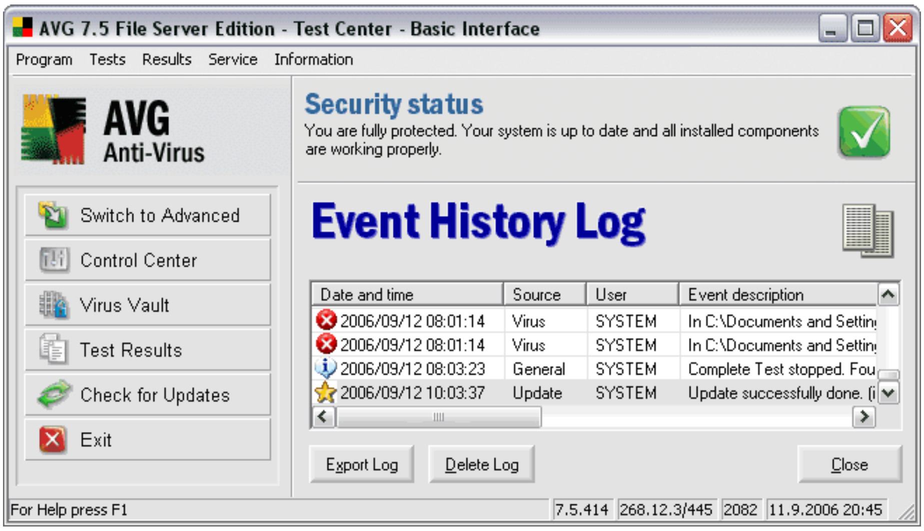
Service/Event History Log

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.



Security status

You are fully protected. Your system is up to date and all installed components are working properly.

Event History Log

Date and time	Source	User	Event description
2006/09/12 08:01:14	Virus	SYSTEM	In C:\Documents and Settin
2006/09/12 08:01:14	Virus	SYSTEM	In C:\Documents and Settin
2006/09/12 08:03:23	General	SYSTEM	Complete Test stopped. Fou
2006/09/12 10:03:37	Update	SYSTEM	Update successfully done. (i

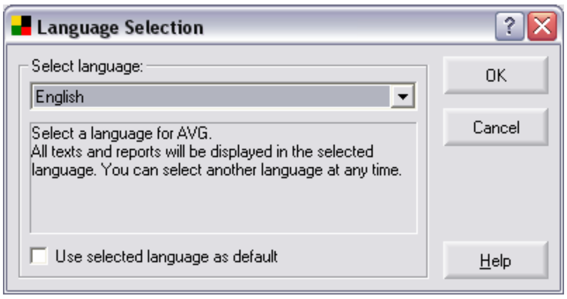
For Help press F1 | 7.5.414 | 268.12.3/445 | 2082 | 11.9.2006 20:45

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 installation process (Chapter 3) again at any time and choose additional languages in the Component selection dialog.*



Select language: English

Select a language for AVG.
All texts and reports will be displayed in the selected language. You can select another language at any time.

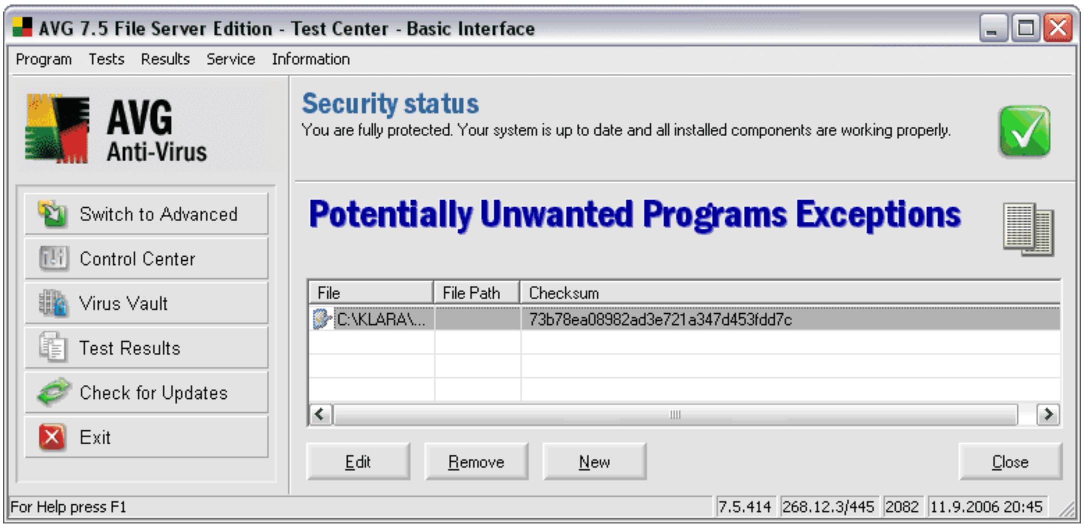
□ Use selected language as default

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***:



Security status

You are fully protected. Your system is up to date and all installed components are working properly.

Potentially Unwanted Programs Exceptions

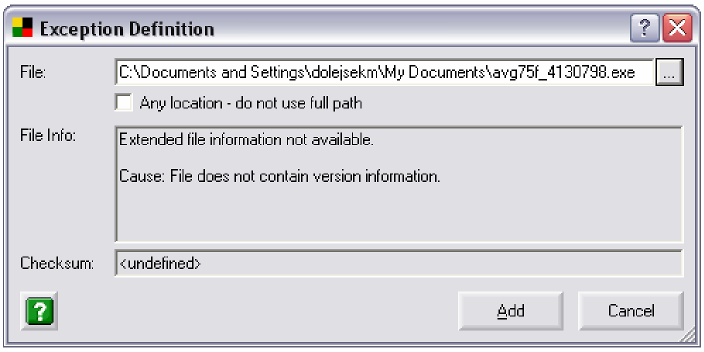
File	File Path	Checksum
C:\KLARA\...		73b78ea08982ad3e721a347d453fdd7c

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:



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: <undefined>

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.

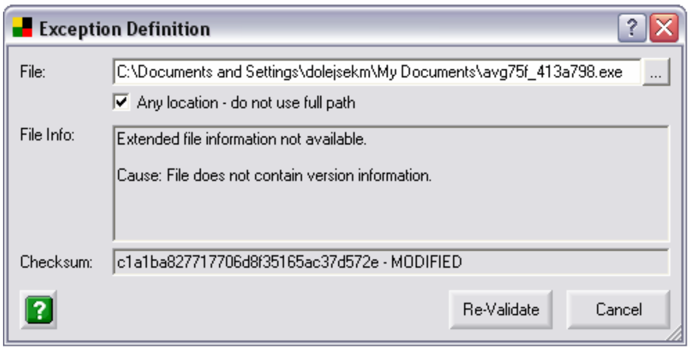
If there is any additional information available about the file (license/version information etc.), it will be displayed within the ***File info*** section.

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:



File: C:\Documents and Settings\dolejsekm\My Documents\avg75f_413a798.exe

☑ Any location - do not use full path

File Info: Extended file information not available.

Cause: File does not contain version information.

Checksum: c1a1ba827717706d8f35165ac37d572e - MODIFIED

During editing of the existing exception, the Checksum 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

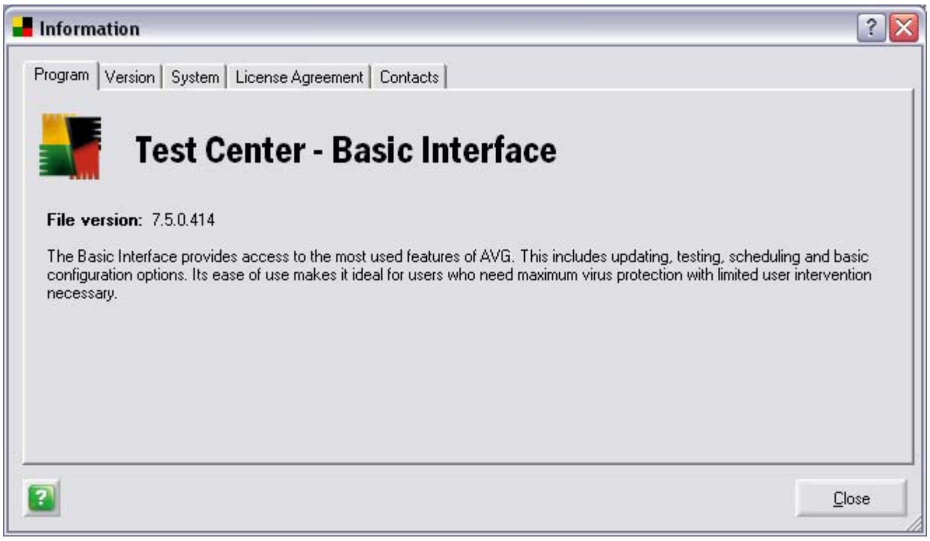
Information/...

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



Test Center - Basic Interface

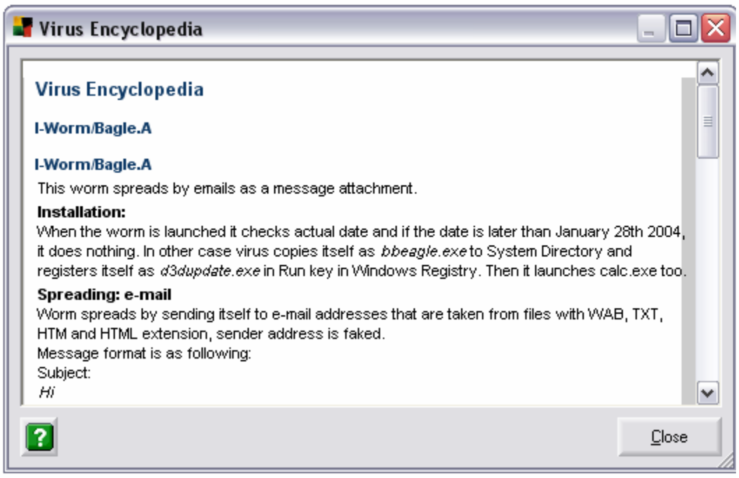
File version: 7.5.0.414

The Basic Interface provides access to the most used features of AVG. This includes updating, testing, scheduling and basic configuration options. Its ease of use makes it ideal for users who need maximum virus protection with limited user intervention necessary.

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.



Virus Encyclopedia

I-Worm/Bagle.A

I-Worm/Bagle.A

This worm spreads by emails as a message attachment.

Installation:
When the worm is launched it checks actual date and if the date is later than January 28th 2004, it does nothing. In other case virus copies itself as *bbeagle.exe* to System Directory and registers itself as *d3dupdate.exe* in Run key in Windows Registry. Then it launches calc.exe too.

Spreading: e-mail
Worm spreads by sending itself to e-mail addresses that are taken from files with WAB, TXT, HTM and HTML extension, sender address is faked.
Message format is as following:
Subject:
Hi

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 15.1 AVG Diagnostics utility.

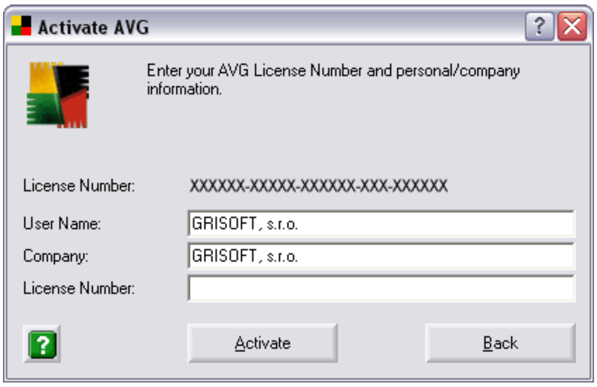
Note: *Under no circumstances does the AVG Diagnostics utility send any personal or other sensitive data from your computer without the user's explicit permission. The user is able to check the content of all collected files and to prevent any of them from being sent to AVG Technical Support.*

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.



Enter your AVG License Number and personal/company information.

License Number: XXXXXX-XXXXX-XXXXXX-XXX-XXXXXX

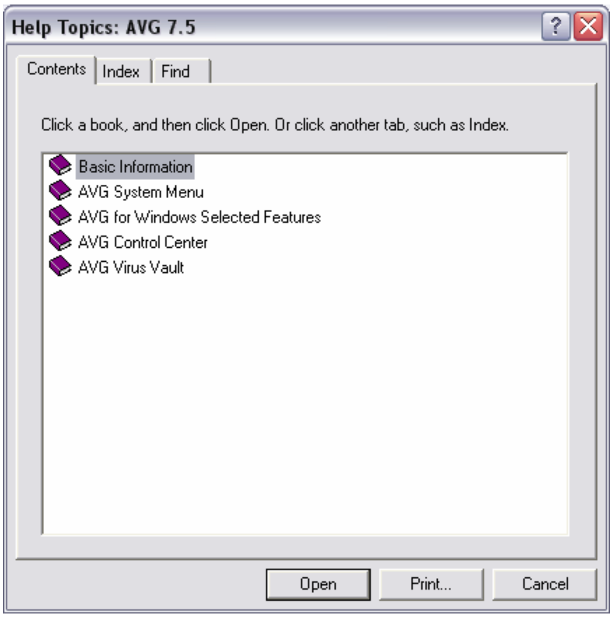
User Name: GRISOFT, s.r.o.

Company: GRISOFT, s.r.o.

License Number:

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

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

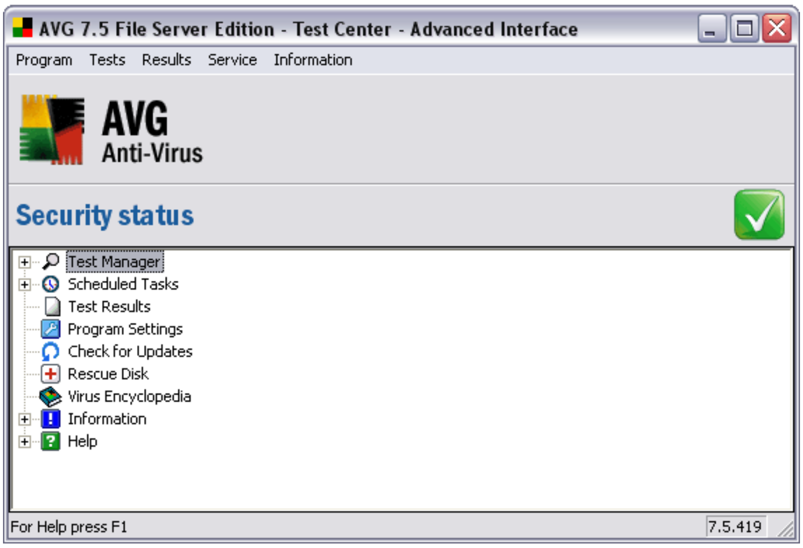
g) AVG Help

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

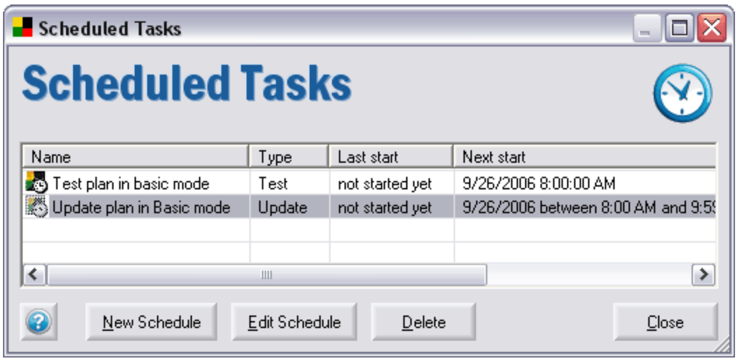
The ***Test manager*** menu branch contains a list of pre-defined tests that can be run using AVG. You can launch any of these tests from here.

For further information on test types refer to chapter 11. Tests Review**.**

8.2. Scheduled Tasks

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 Tasks

Name	Type	Last start	Next start
Test plan in basic mode	Test	not started yet	9/26/2006 8:00:00 AM
Update plan in Basic mode	Update	not started yet	9/26/2006 between 8:00 AM and 9:5

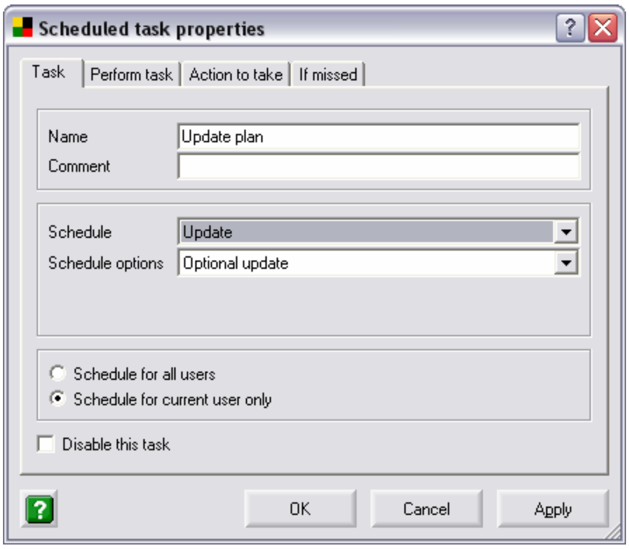
This dialog window provides a more in-depth description of each of the planned tasks:

- 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:



Name: Update plan

Comment:

Schedule: Update

Schedule options: Optional update

○ Schedule for all users

● Schedule for current user only

□ Disable this task

- ***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.

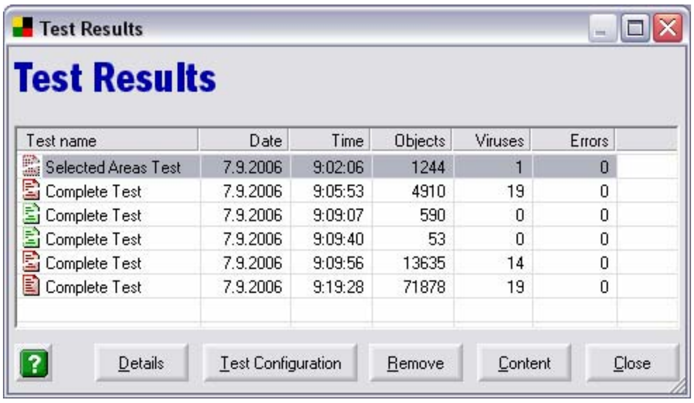
d) Close

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

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

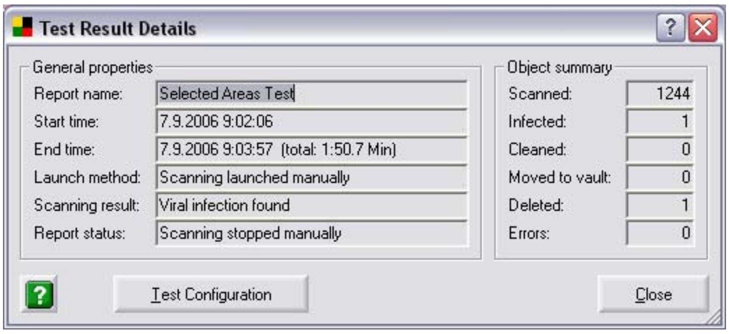
- ***Test name*** – the full name of the test performed
- ***Date*** – the date when the test was performed
- ***Time*** – the exact time when the test was performed
- ***Objects*** – number of objects scanned
- ***Viruses*** – number of viruses found (if there is a virus found, the test's icon in the 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 11.1 d) – Complete Test - Results. 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:



Test Result Details

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
Scanning result: Viral infection found
Report status: Scanning stopped manually

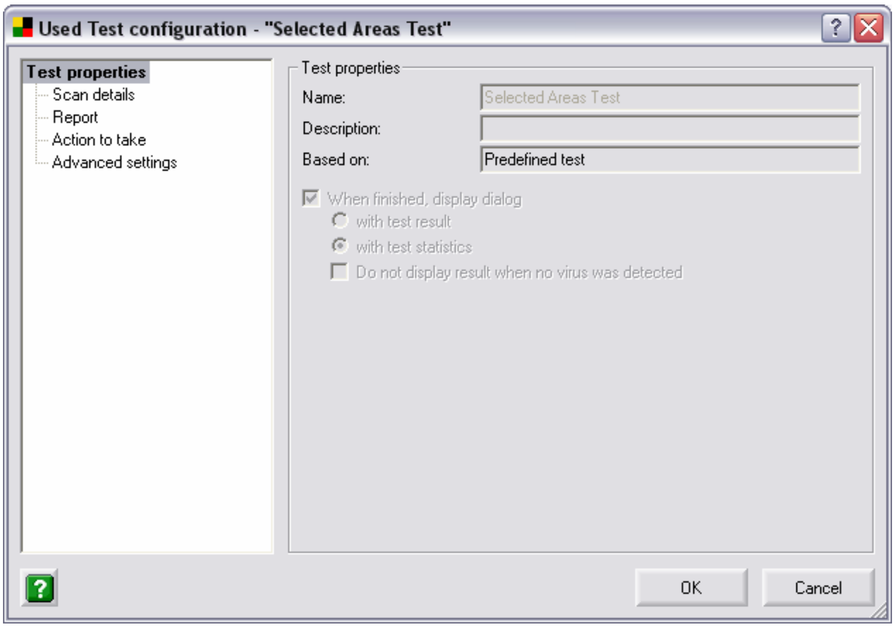
Object summary

Scanned: 1244
Infected: 1
Cleaned: 0
Moved to vault: 0
Deleted: 1
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 - "Selected Areas Test"

Test properties
Name: Selected Areas Test
Description:
Based on: Predefined test
☑ When finished, display dialog
○ with test result
● with test statistics
□ Do not display result when no virus was detected

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 7.4 Test Results, section d)**.**

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 11.1 Complete Test - d) Complete Test - Results.*

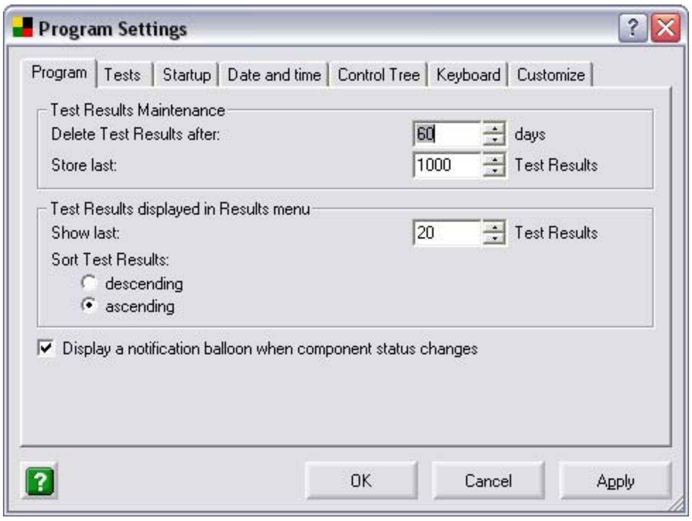
8.4. Program Settings

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

a) Program

- ***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
- ***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***.



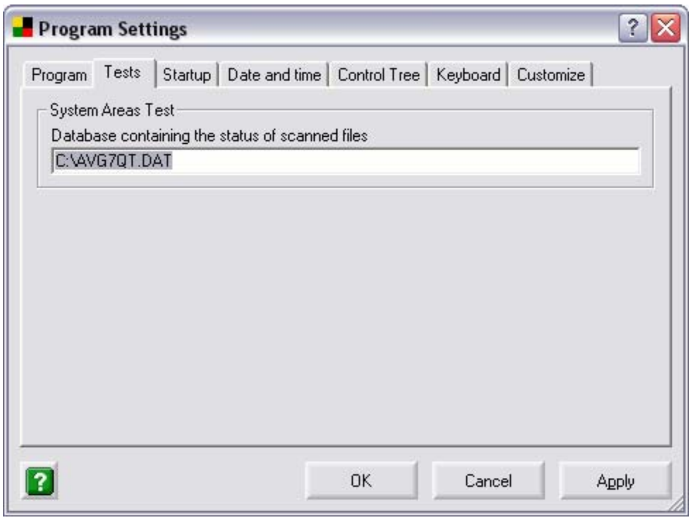
Test Results Maintenance
Delete Test Results after: 60 days
Store last: 1000 Test Results

Test Results displayed in Results menu
Show last: 20 Test Results
Sort Test Results:
○ descending
● ascending

☑ Display a notification balloon when component status changes

b) Tests

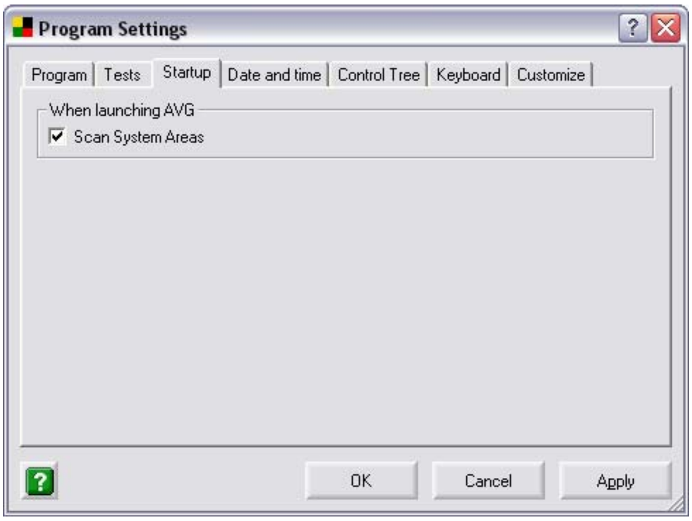
System Areas Test section – specify the name and location of the System Areas Test results database



System Areas Test
Database containing the status of scanned files
C:\AVG7QT.DAT

c) **_Startup_**

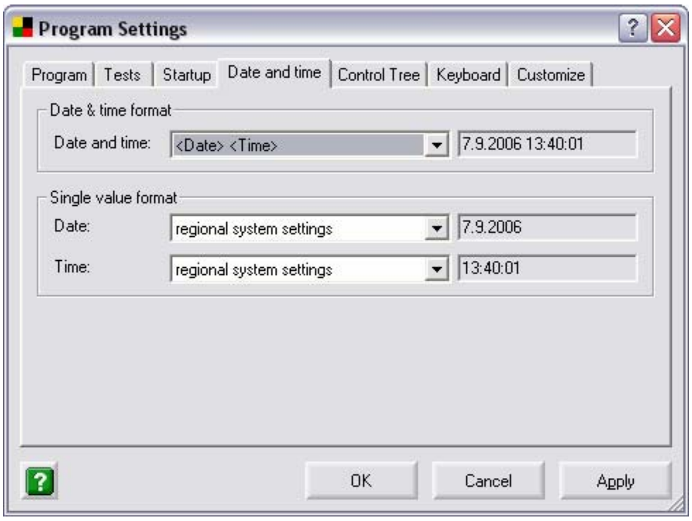
Scan System Areas – decide whether you want to run the System Areas Test at AVG launch



When launching AVG
☑ Scan System Areas

d) **_Date and Time_**

- **_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



Program Settings

Program | Tests | Startup | Date and time | Control Tree | Keyboard | Customize

Date & time format

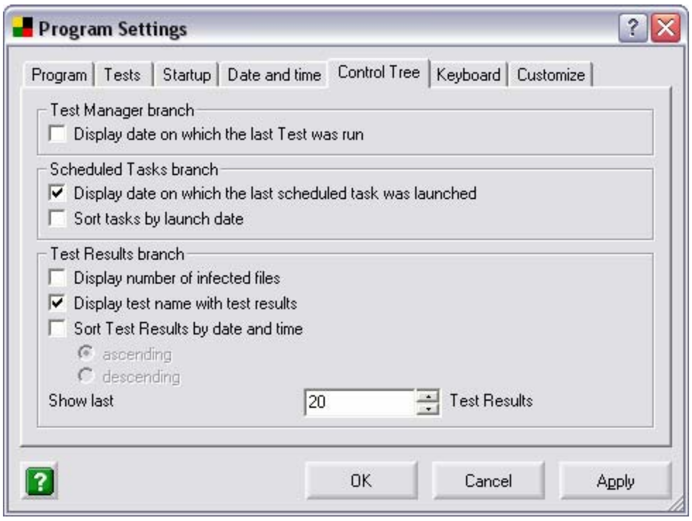
Date and time: <Date> <Time> | 7.9.2006 13:40:01

Single value format

Date: regional system settings | 7.9.2006

Time: regional system settings | 13:40:01

e) Control Tree



Program Settings

Program | Tests | Startup | Date and time | Control Tree | Keyboard | Customize

Test Manager branch

□ Display date on which the last Test was run

Scheduled Tasks branch

☑ Display date on which the last scheduled task was launched

□ Sort tasks by launch date

Test Results branch

□ Display number of infected files

☑ Display test name with test results

□ Sort Test Results by date and time

● ascending

○ descending

Show last 20 Test Results

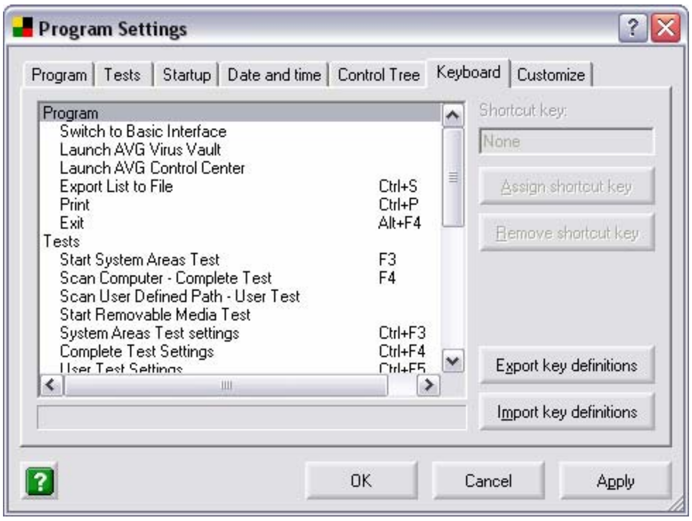
- ***Test Manager Branch*** section
  - ***Display Date on Which the Last Test Was Run*** – in the ***Advanced Test Interface*** menu enable/disable displaying of the date when the last test was launched
- ***Scheduled Tasks Branch*** section
  - ***Display Date on Which the Last Scheduled Task Was Launched*** – 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
- ***Tes*t *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

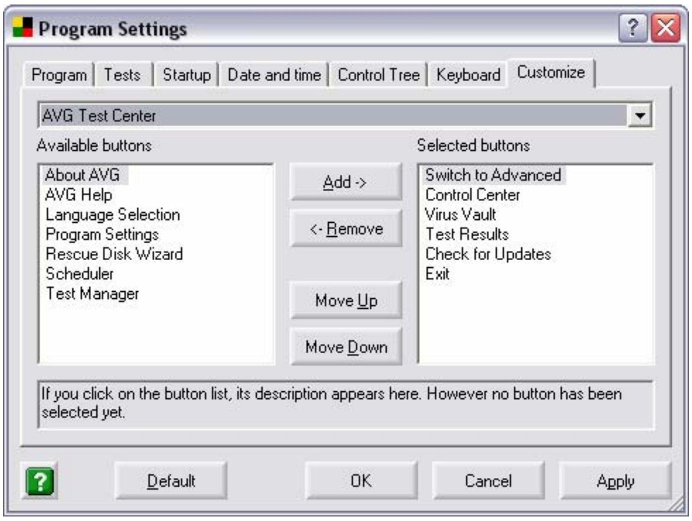


Program	
Switch to Basic Interface	
Launch AVG Virus Vault	
Launch AVG Control Center	
Export List to File	Ctrl+S
Print	Ctrl+P
Exit	Alt+F4
Tests	
Start System Areas Test	F3
Scan Computer - Complete Test	F4
Scan User Defined Path - User Test	
Start Removable Media Test	
System Areas Test settings	Ctrl+F3
Complete Test Settings	Ctrl+F4
User Test Settings	Ctrl+F5

Shortcut key: None

g) Customize

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



AVG Test Center

Available buttons: About AVG, AVG Help, Language Selection, Program Settings, Rescue Disk Wizard, Scheduler, Test Manager

Selected buttons: Switch to Advanced, Control Center, Virus Vault, Test Results, Check for Updates, Exit

If you click on the button list, its description appears here. However no button has been selected yet.

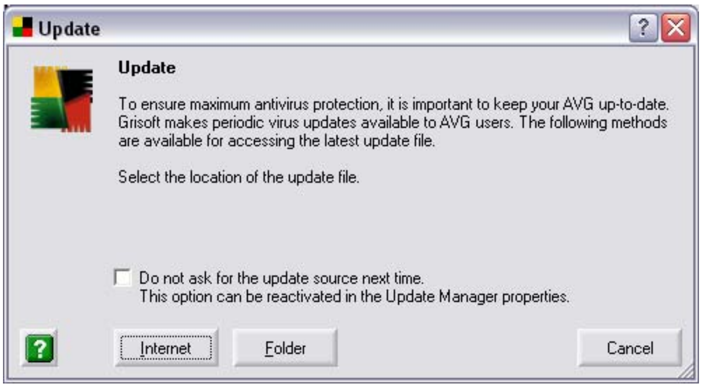
Separate tabs provide the following operating buttons:

- ***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 12. Program Updates.



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.

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 9.12 – Control Center – Update Manager, the ***Properties*** section**.**

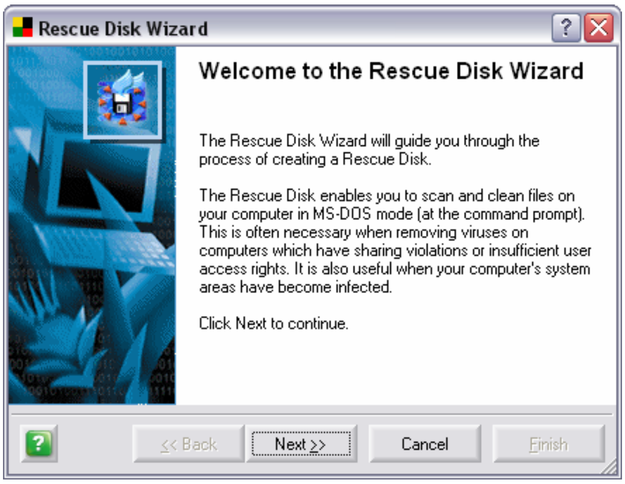
8.6. Rescue Disk

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.



Rescue Disk Wizard

Welcome to the Rescue Disk Wizard

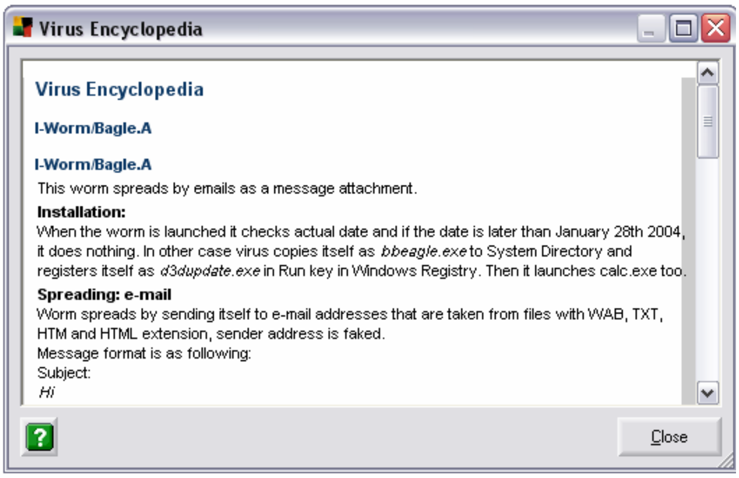
The Rescue Disk Wizard will guide you through the process of creating a Rescue Disk.

The Rescue Disk enables you to scan and clean files on your computer in MS-DOS mode (at the command prompt). This is often necessary when removing viruses on computers which have sharing violations or insufficient user access rights. It is also useful when your computer's system areas have become infected.

Click Next to continue.

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!



Virus Encyclopedia

I-Worm/Bagle.A

I-Worm/Bagle.A

This worm spreads by emails as a message attachment.

Installation:

When the worm is launched it checks actual date and if the date is later than January 28th 2004, it does nothing. In other case virus copies itself as *bbeagle.exe* to System Directory and registers itself as *d3dupdate.exe* in Run key in Windows Registry. Then it launches calc.exe too.

Spreading: e-mail

Worm spreads by sending itself to e-mail addresses that are taken from files with WAB, TXT, HTM and HTML extension, sender address is faked.

Message format is as following:

Subject:

Hi

8.8. Information

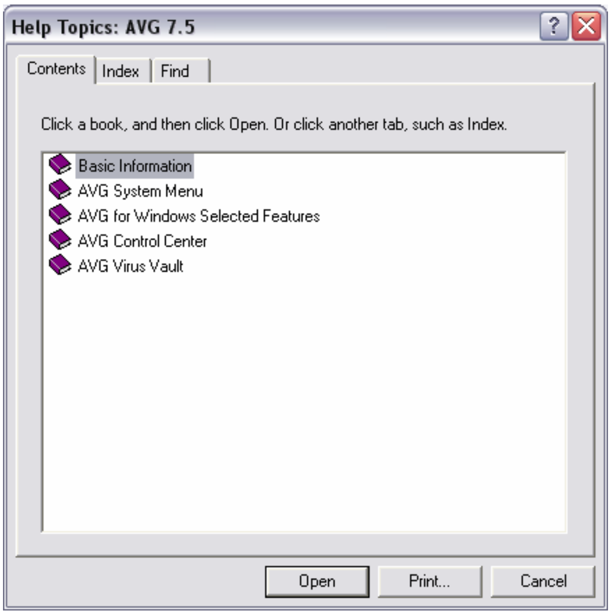
The ***Information*** menu item contains a list of sub-items corresponding to separate tabs of the newly opened dialog window with AVG information:

- ***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



Help Topics: AVG 7.5

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

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 Anti-Malware**, 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 Chapter 9.3. Control Center Top Menu - b) View.

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:

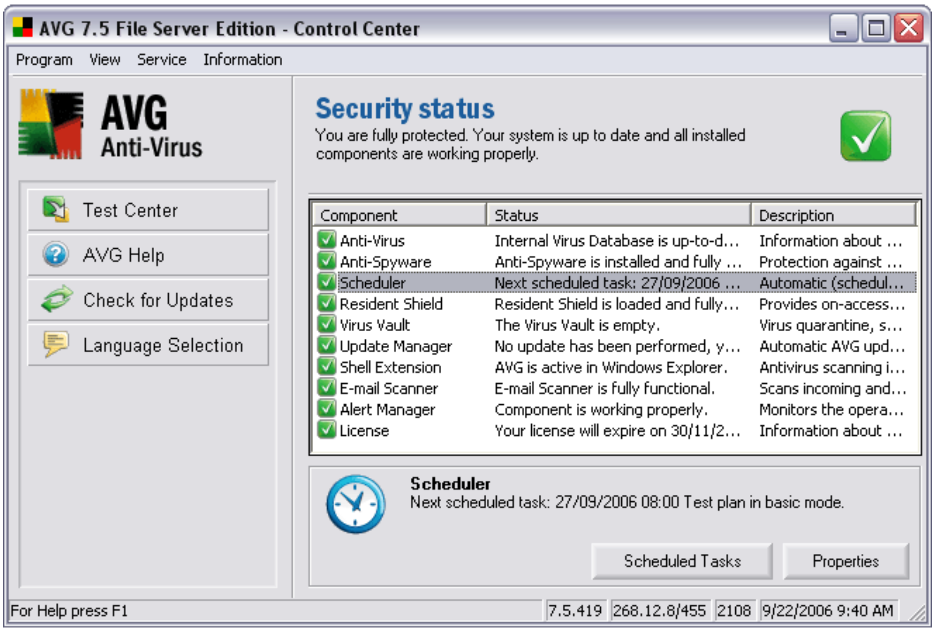
- ✓ Your computer is fully protected, up to date and all installed components are working properly
- ! One or more components are incorrectly configured and you should pay attention to their properties/settings. The problem components will be listed in the status error message.
- ✓ Indicates, that you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



Security status

You are fully protected. Your system is up to date and all installed components are working properly.

Component	Status	Description
✓ Anti-Virus	Internal Virus Database is up-to-d...	Information about ...
✓ Anti-Spyware	Anti-Spyware is installed and fully ...	Protection against ...
✓ Scheduler	Next scheduled task: 27/09/2006 ...	Automatic (schedul...
✓ Resident Shield	Resident Shield is loaded and fully...	Provides on-access...
✓ Virus Vault	The Virus Vault is empty.	Virus quarantine, s...
✓ Update Manager	No update has been performed, y...	Automatic AVG upd...
✓ Shell Extension	AVG is active in Windows Explorer.	Antivirus scanning i...
✓ E-mail Scanner	E-mail Scanner is fully functional.	Scans incoming and...
✓ Alert Manager	Component is working properly.	Monitors the opera...
✓ License	Your license will expire on 30/11/2...	Information about ...

Scheduler
Next scheduled task: 27/09/2006 08:00 Test plan in basic mode.

For Help press F1 | 7.5.419 | 268.12.8/455 | 2108 | 9/22/2006 9:40 AM

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 8.4 Program Settings d) Keyboard

a) Test Center

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

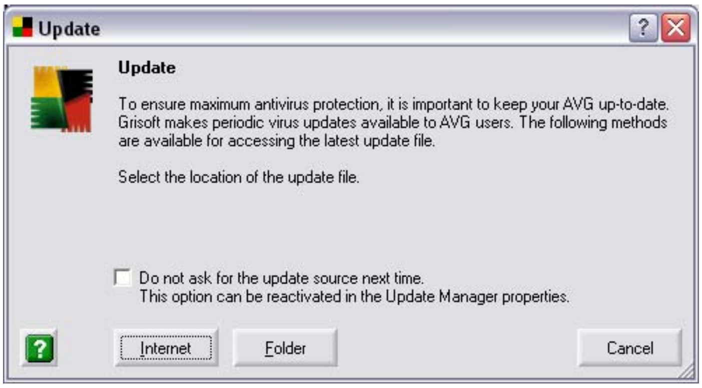
For details on the Test Center Basic/Advanced Test Interface refer to chapters 7. AVG Basic Test Center Interface and 8. AVG Advanced Test Center Interface.

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:



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.

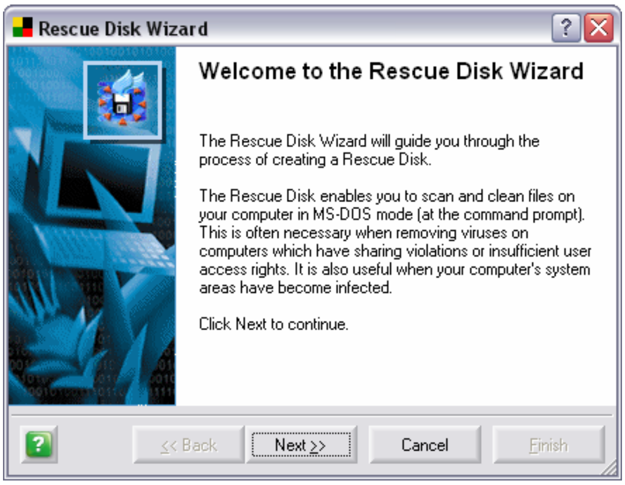
The dialog operating buttons are:

- ***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 12. Program Updates.

d) Rescue Disk Wizard

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



Rescue Disk Wizard

Welcome to the Rescue Disk Wizard

The Rescue Disk Wizard will guide you through the process of creating a Rescue Disk.

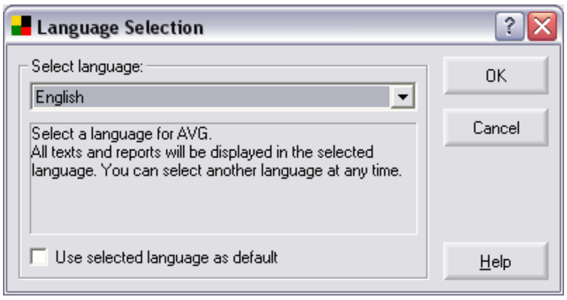
The Rescue Disk enables you to scan and clean files on your computer in MS-DOS mode (at the command prompt). This is often necessary when removing viruses on computers which have sharing violations or insufficient user access rights. It is also useful when your computer's system areas have become infected.

Click Next to continue.

For details on Rescue Disk creation and use please refer to chapter 8.6 Rescue Disk.

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: English

Select a language for AVG.
All texts and reports will be displayed in the selected language. You can select another language at any time.

□ Use selected language as default

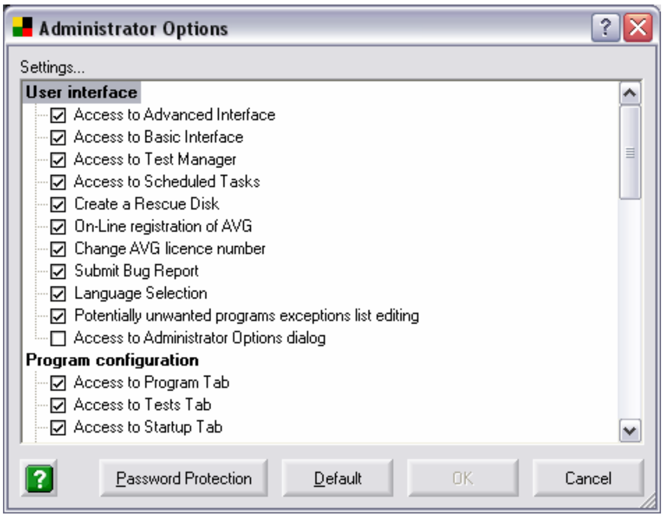
Note: If you only installed English, then this button will not be available.

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
- ☑ Language Selection
- ☑ Potentially unwanted programs exceptions list editing
- □ Access to Administrator Options dialog

Program configuration
- ☑ Access to Program Tab
- ☑ Access to Tests Tab
- ☑ Access to Startup Tab

The dialog window provides the following operating buttons:

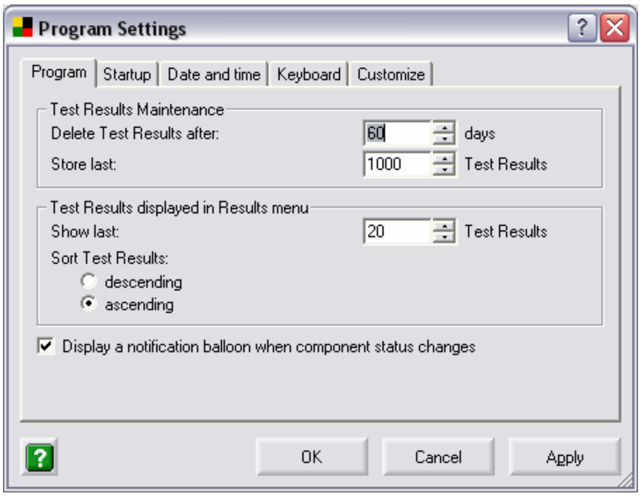
- ***Password protection*** – allows you to define and confirm a password that will secure access to the **Administrator Options** dialog.
- ***Default*** – returns the administrator options settings to default
- ***OK*** – accepts all performed changes, and closes the dialog
- ***Cancel*** – closes 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 8.4 Program Settings.



Program Settings

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:
○ descending
● ascending

☑ Display a notification balloon when component status changes

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

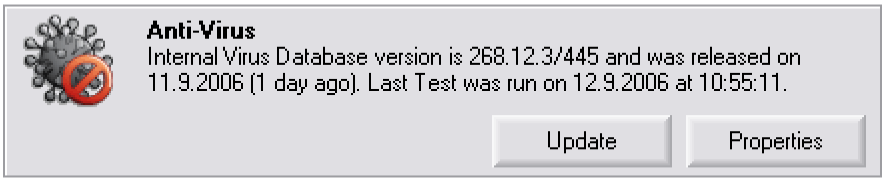
The **Control Center** allows management of these AVG components:

- Anti-Virus
- Anti-Spyware

- Scheduler
- Resident Shield
- Virus Vault
- Update Manager
- Shell Extension
- E-mail Scanner
- Alert Manager
- License

9.7. Control Center - Anti-Virus

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



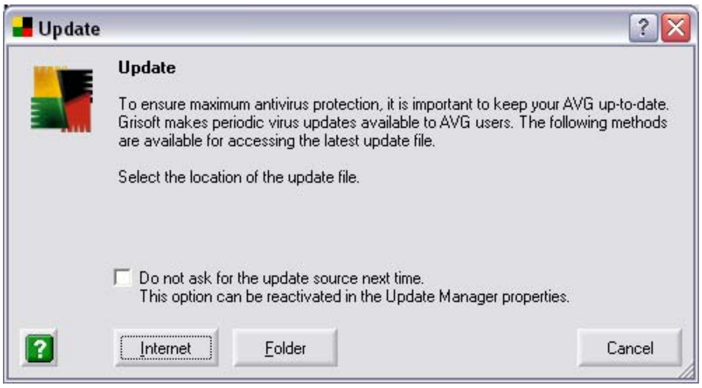
Anti-Virus
Internal Virus Database version is 268.12.3/445 and was released on 11.9.2006 (1 day ago). Last Test was run on 12.9.2006 at 10:55:11.

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 12. Program Updates.*

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

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.

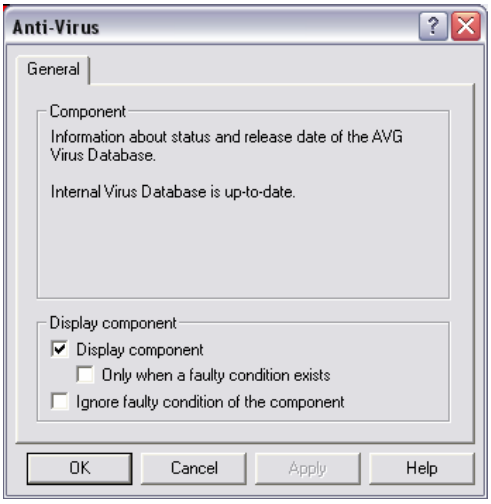
Select the location of the update file.

□ Do not ask for the update source next time.
This option can be reactivated in the Update Manager properties.

For details on update types and possibilities please refer to chapter 12. Program updates.

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 about status and release date of the AVG Virus Database.

Internal Virus Database is up-to-date.

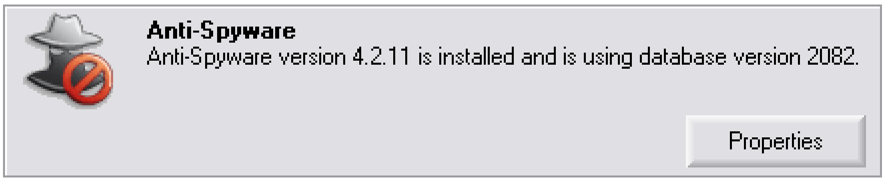
Display component

☑ Display component

□ Only when a faulty condition exists

□ Ignore faulty condition of the component

9.8. Control Center - Anti-Spyware


Anti-Spyware

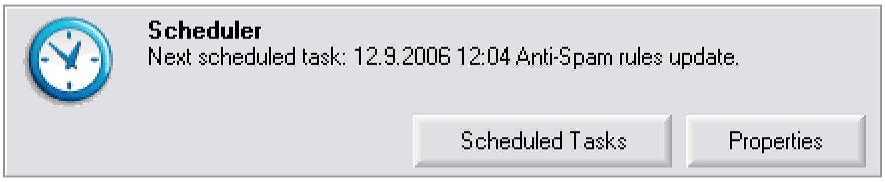
Anti-Spyware version 4.2.11 is installed and is using database version 2082.

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 File Server** 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 - Scheduler

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

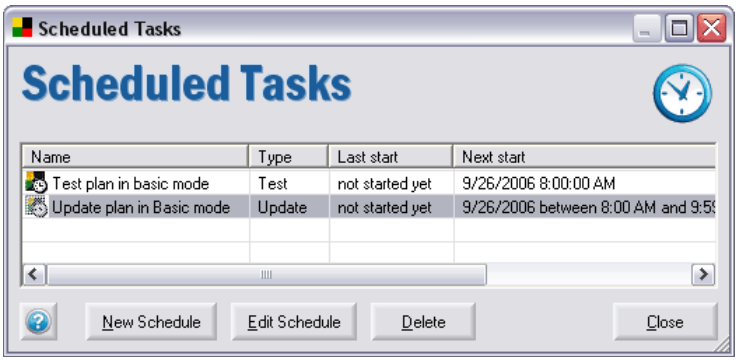

Scheduler

Next scheduled task: 12.9.2006 12:04 Anti-Spam rules update.

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 8.2 Scheduled Tasks

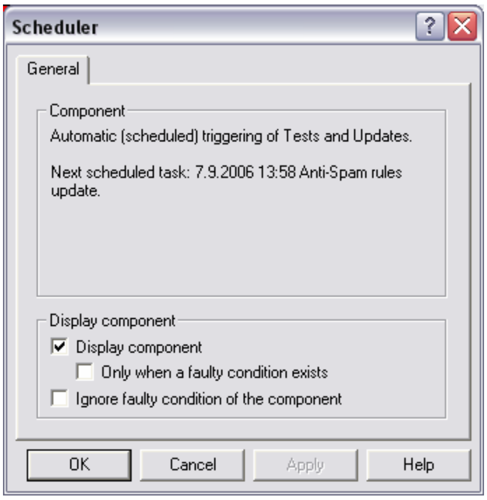


Scheduled Tasks

Name	Type	Last start	Next start
Test plan in basic mode	Test	not started yet	9/26/2006 8:00:00 AM
Update plan in Basic mode	Update	not started yet	9/26/2006 between 8:00 AM and 9:5

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.

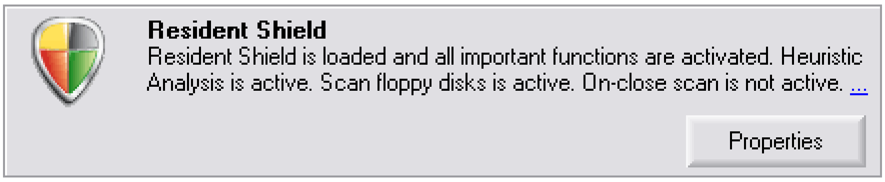
Next scheduled task: 7.9.2006 13:58 Anti-Spam rules update.

Display component
☑ Display component
☐ Only when a faulty condition exists
☐ Ignore faulty condition of the component

9.10. Control Center - Resident Shield

a) *Resident Shield Properties*

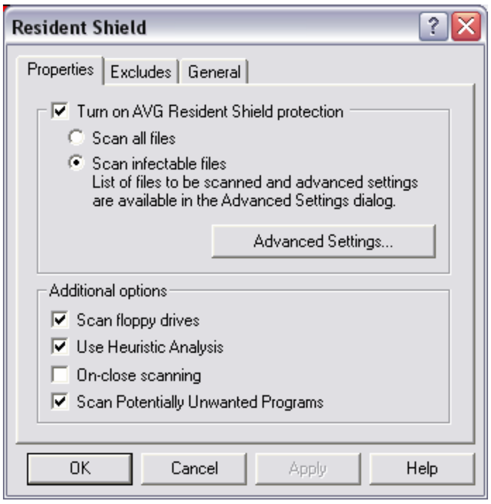
The ***Resident Shield*** component performs live protection of files and folders against viruses, spyware and other malware. This feature has to be activated first in the Resident Shield **Properties** dialog.



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

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

☑ Turn on AVG Resident Shield protection

○ Scan all files

● Scan infectable files
List of files to be scanned and advanced settings are available in the Advanced Settings dialog.

Additional options

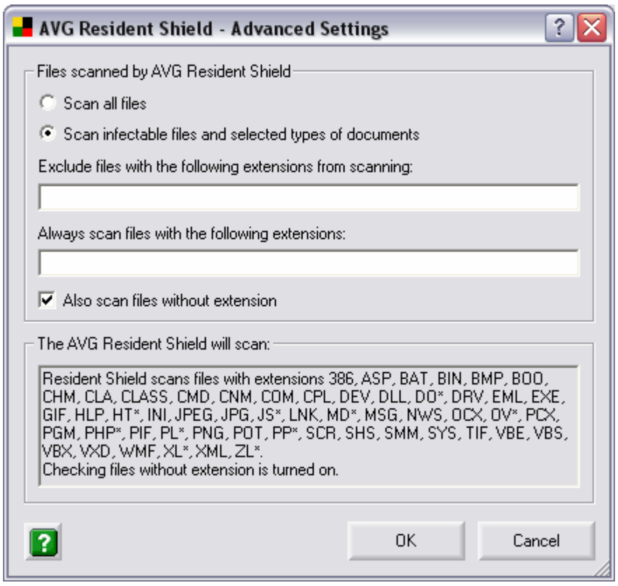
☑ Scan floppy drives

☑ Use Heuristic Analysis

□ On-close scanning

☑ Scan Potentially Unwanted Programs

- ***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

○ 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:

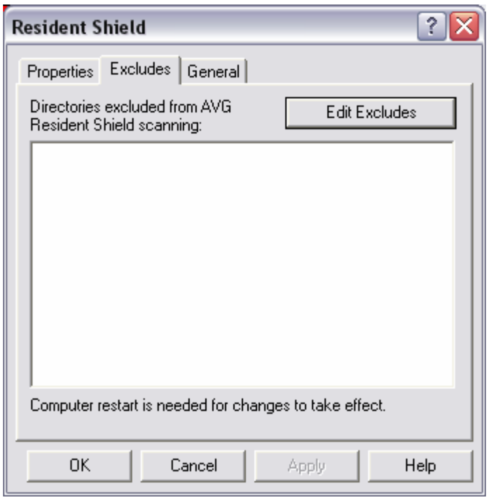
☑ Also scan files without extension

The AVG Resident Shield will scan:

Resident Shield scans files with extensions 386, ASP, BAT, BIN, BMP, BOO, 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.

o ***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!

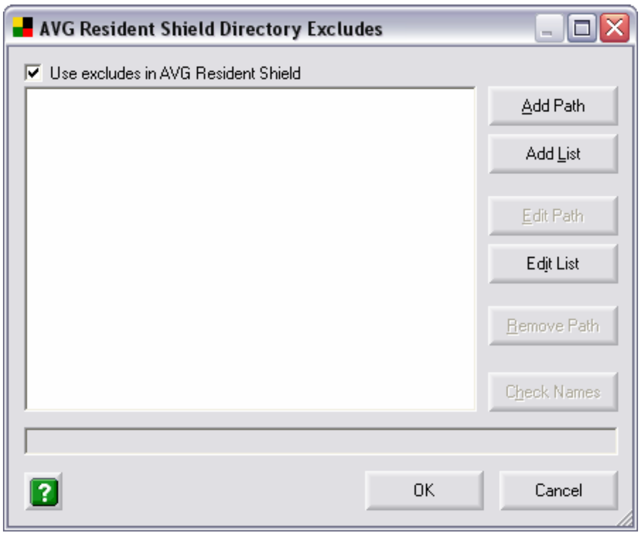
Please note: *Exceptions for Potentially Unwanted Programs should be defined in a different dialog. See chapter 7.14 Potentially Unwanted Programs Exceptions.*



Directories excluded from AVG Resident Shield scanning:

Computer restart is needed for changes to take effect.

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



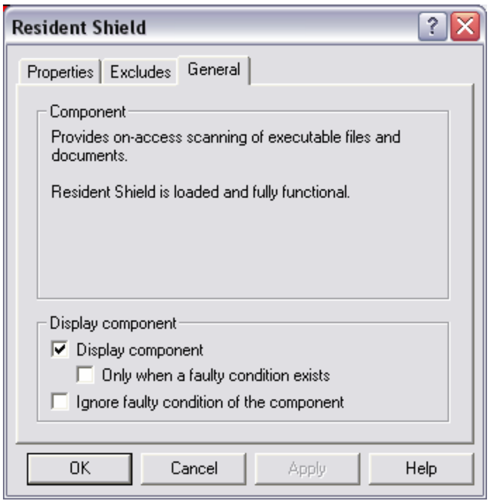
☑ Use excludes in AVG Resident Shield

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

o ***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:



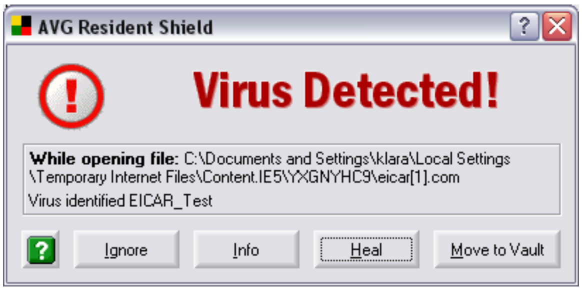
Provides on-access scanning of executable files and documents.

Resident Shield is loaded and fully functional.

☑ Display component
□ Only when a faulty condition exists
□ Ignore faulty condition of the component

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:



While opening file: C:\Documents and Settings\klara\Local Settings\Temporary Internet Files\Content.IE5\YXGNYHC9\eicar[1].com
Virus identified EICAR_Test

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:

o ***Ignore*** – ignores the Virus Detected warning, and allows you to continue working (and also forbids access to the threat)

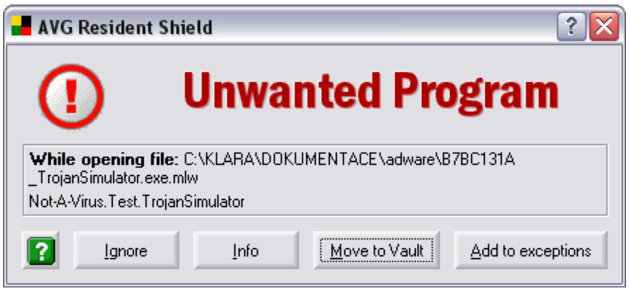
o ***Info*** – open the on-line virus encyclopedia where you can look up detailed information on the identified virus

o ***Heal*** – allows you to heal the infected object if the cure for this kind of infection is available

o ***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:



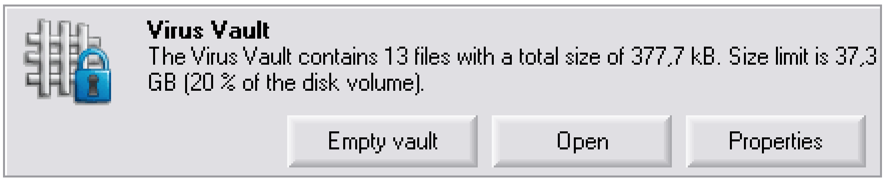
While opening file: C:\KLARA\DOKUMENTACE\adware\B7BC131A _TrojanSimulator.exe.mlw
Not-A-Virus.Test.TrojanSimulator

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 Potentially Unwanted Programs Exception. (Chapter 7.14). A confirmation dialog will be displayed.

9.11. 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 Vault contains 13 files with a total size of 377,7 kB. Size limit is 37,3 GB (20 % of the disk volume).

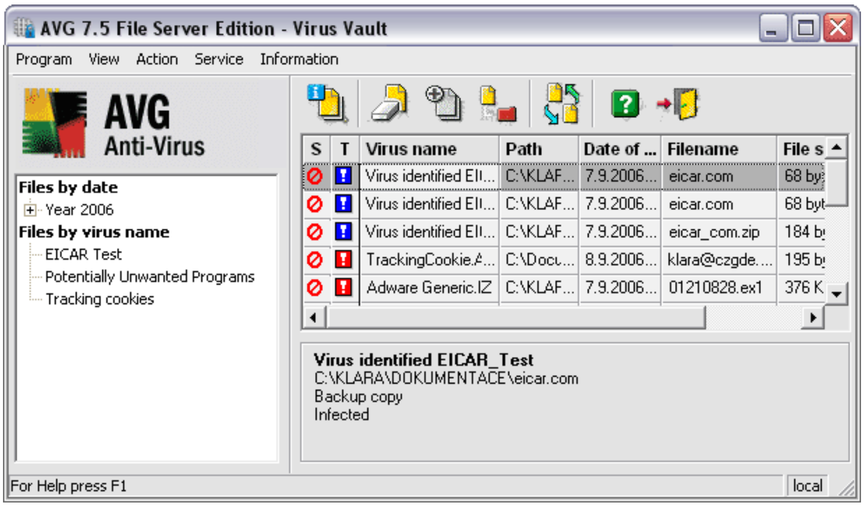
The ***Virus Vault*** panel's operating buttons are:

a) Empty vault

Deletes all objects stored in the ***Virus Vault***.

b) Open

Opens the ***Virus Vault*** application:


AVG 7.5 File Server Edition - Virus Vault
Program View Action Service Information
AVG Anti-Virus
For Help press F1
local

Files by date
- Year 2006

Files by virus name
- EICAR Test
- Potentially Unwanted Programs
- Tracking cookies

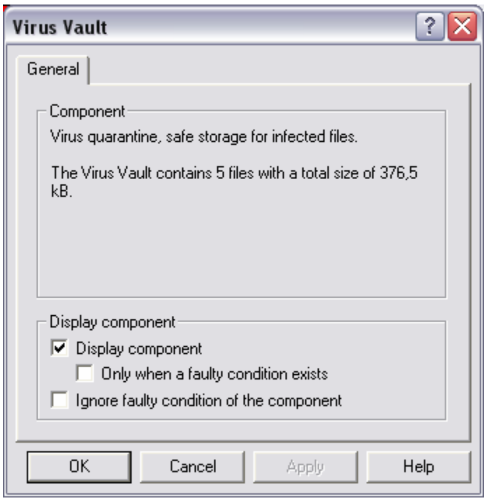
S	T	Virus name	Path	Date of ...	Filename	File s
⊘	!	Virus identified EI...	C:\KLAF...	7.9.2006...	eicar.com	68 by
⊘	!	Virus identified EI...	C:\KLAF...	7.9.2006...	eicar.com	68 byt
⊘	!	Virus identified EI...	C:\KLAF...	7.9.2006...	eicar_com.zip	184 b
⊘	!	TrackingCookie.A...	C:\Docu...	8.9.2006...	klara@czgde....	195 b
⊘	!	Adware Generic.IZ	C:\KLAF...	7.9.2006...	01210828.ex1	376 K

Virus identified EICAR_Test
C:\KLARA\DOKUMENTACE\eicar.com
Backup copy
Infected

For further details on the Virus Vault environment and possibilities of use please refer to chapter 10. Virus Vault.

c) Properties

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



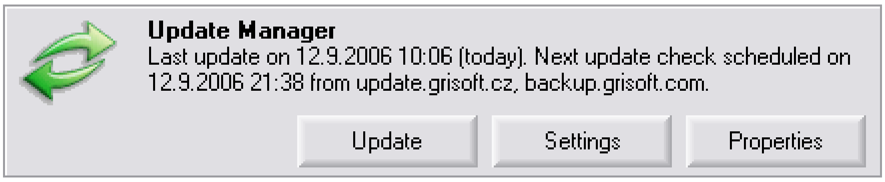
Component
Virus quarantine, safe storage for infected files.

The Virus Vault contains 5 files with a total size of 376,5 kB.

Display component
☑ Display component
☐ Only when a faulty condition exists
☐ Ignore faulty condition of the component

9.12. Control Center - Update Manager

The ***Update Manager*** controls the AVG updates.



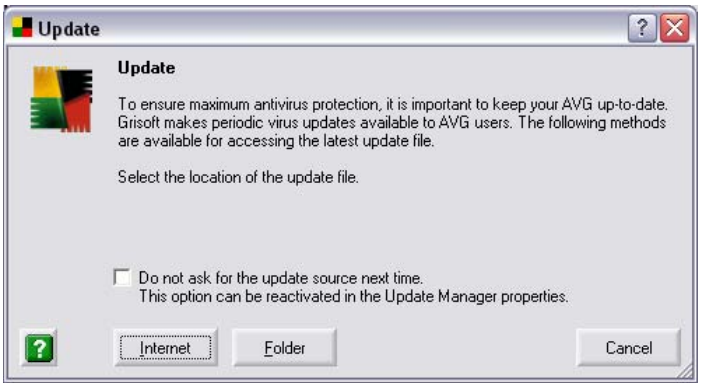
Update Manager
Last update on 12.9.2006 10:06 (today). Next update check scheduled on 12.9.2006 21:38 from update.grisoft.cz, backup.grisoft.com.

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.

For further information on update types and possibilities please refer to chapter 12. Program Updates.

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:

- ***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:

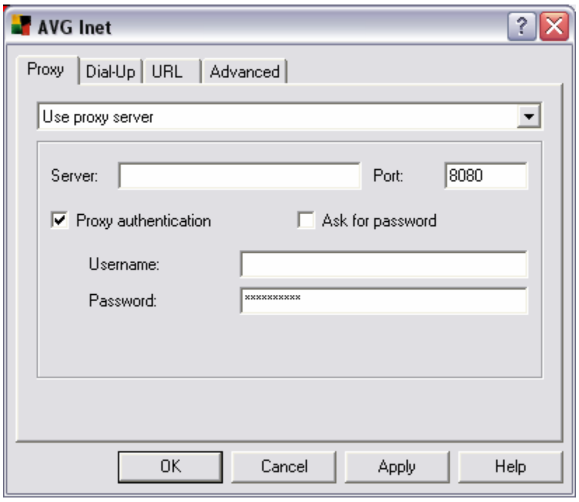
  - Do not use proxy server
  - Use proxy server
  - Use proxy server, if it fails try direct connection

  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.



Use proxy server

Server:

Port: 8080

☑ Proxy authentication

□ Ask for password

Username:

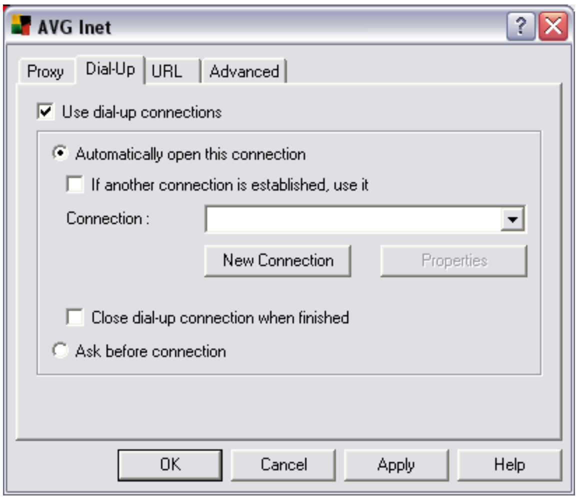
Password: **********

- 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***).



☑ Use dial-up connections

● Automatically open this connection

□ If another connection is established, use it

Connection :

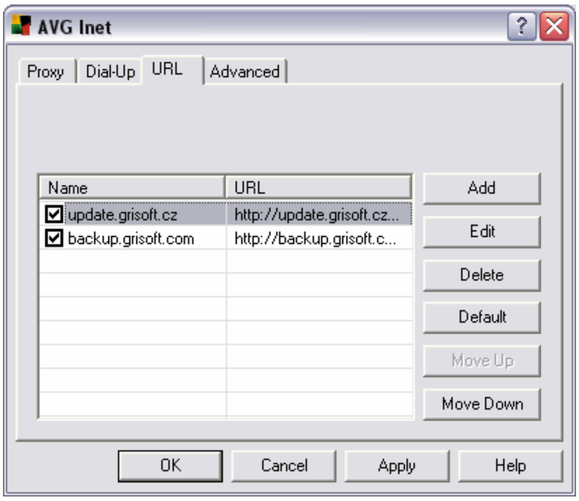
□ Close dial-up connection when finished

○ Ask before connection

- **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

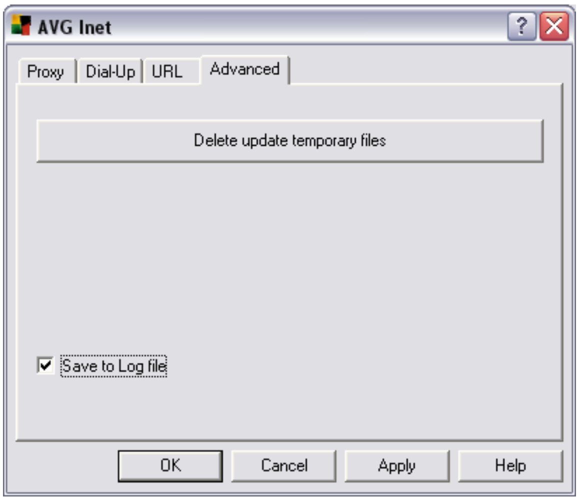


Name	URL
☑ update.grisoft.cz	http://update.grisoft.cz...
☑ backup.grisoft.com	http://backup.grisoft.c...

- ***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.

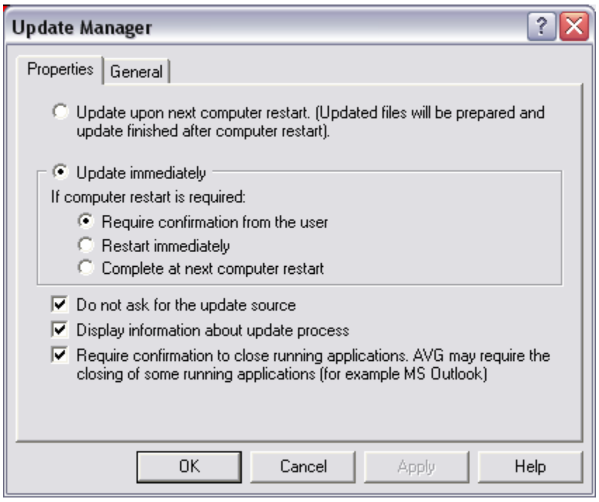


☑ Save to Log file

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 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

○ Restart immediately

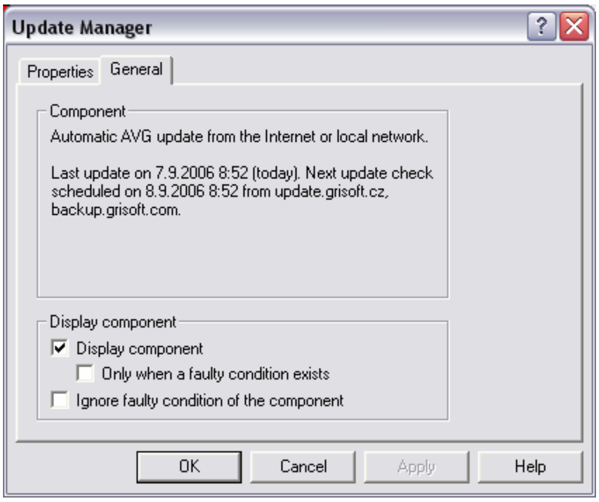
○ Complete at next computer restart

☑ 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)

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



Update Manager

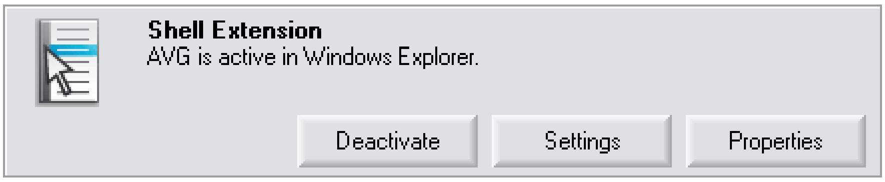
Component
Automatic AVG update from the Internet or local network.

Last update on 7.9.2006 8:52 (today). Next update check scheduled on 8.9.2006 8:52 from update.grisoft.cz, backup.grisoft.com.

Display component
☑ Display component
☐ Only when a faulty condition exists
☐ Ignore faulty condition of the component

9.13. 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 Windows Explorer.

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

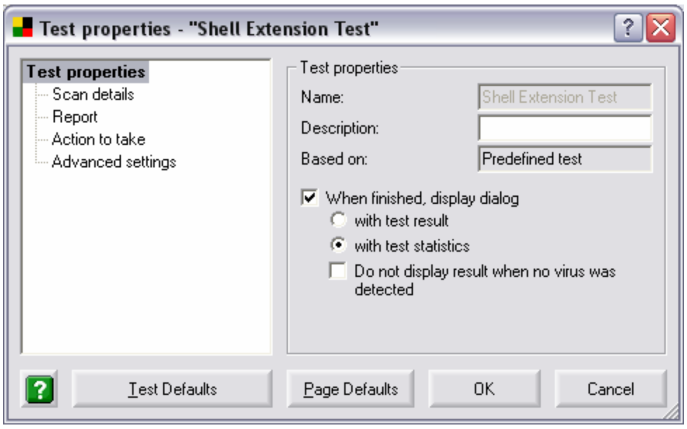
a) Deactivate

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***).



Test properties - "Shell Extension Test"

Test properties

Name: Shell Extension Test

Description:

Based on: Predefined test

☑ When finished, display dialog

○ with test result

● with test statistics

□ Do not display result when no virus was detected

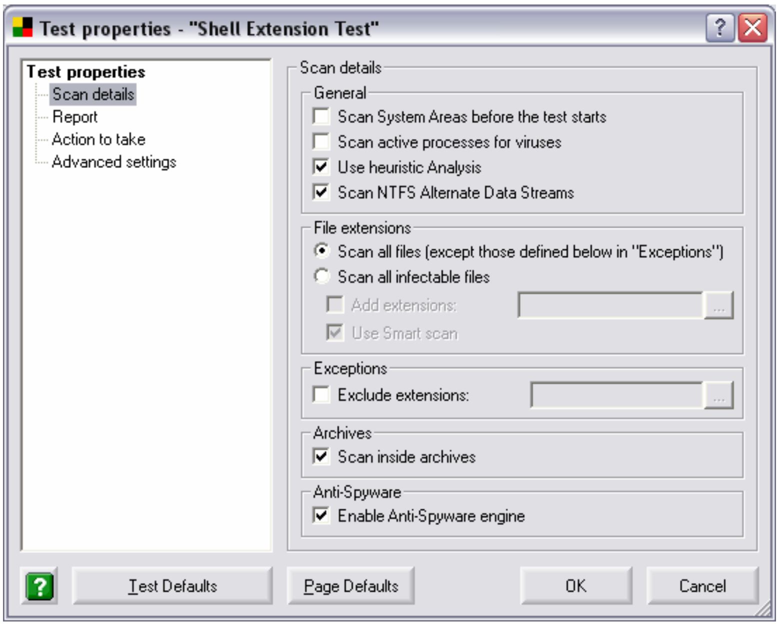
- ***Scan details*** – in this dialog you can define whether the system areas should be scanned and what methods should be used for scanning (***General***). If you prefer not to ***Scan NTFS Alternate Data Streams***, uncheck this check box.

  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*** check box).



Test properties - "Shell Extension Test"

Test properties
- 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

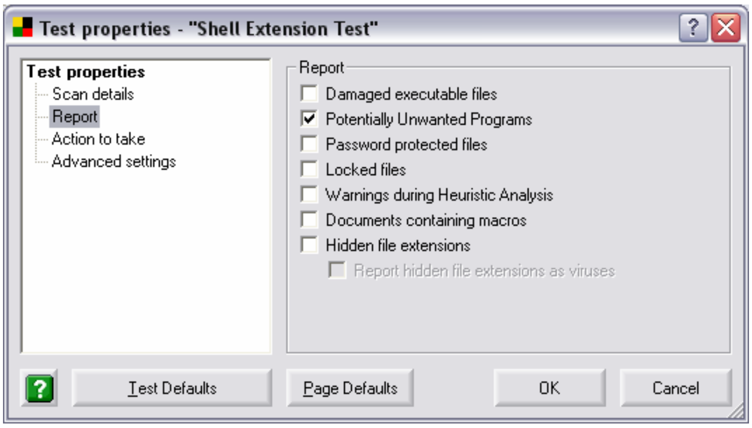
File extensions
- ● Scan all files (except those defined below in "Exceptions")
- ○ Scan all infectable files
- □ Add extensions:
- ☑ Use Smart scan

Exceptions
- □ Exclude extensions:

Archives
- ☑ Scan inside archives

Anti-Spyware
- ☑ Enable Anti-Spyware engine

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

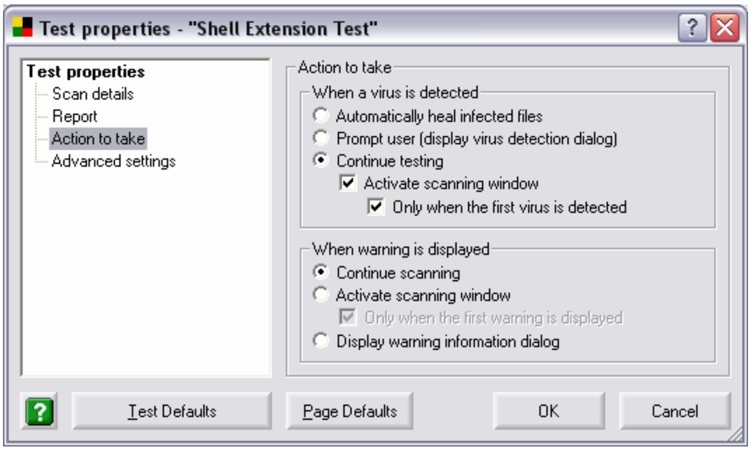


Test properties - "Shell Extension Test"

Test properties
- Scan details
- Report
- Action to take
- Advanced settings

Report
- □ Damaged executable files
- ☑ Potentially Unwanted Programs
- □ Password protected files
- □ Locked files
- □ Warnings during Heuristic Analysis
- □ Documents containing macros
- □ Hidden file extensions
- □ Report hidden file extensions as viruses

- o **_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 Extension Test"

- Test properties
  - Scan details
  - Report
  - Action to take
  - Advanced settings

Action to take

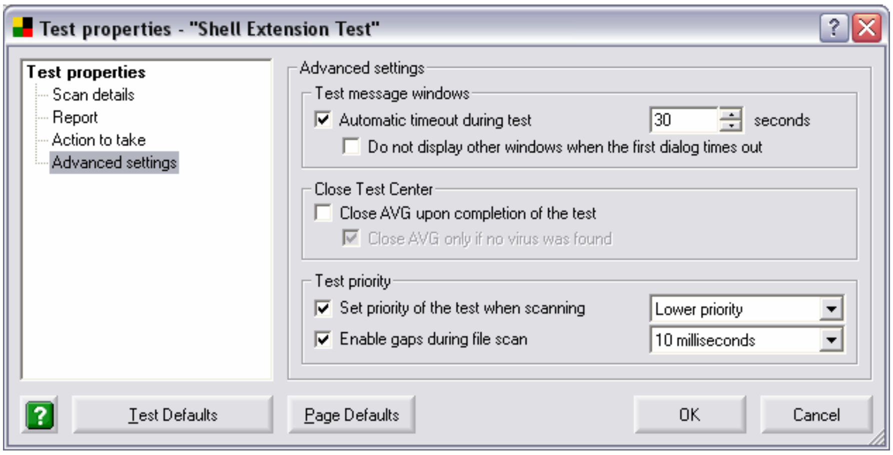
When a virus is detected

○ 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 warning is displayed
○ Display warning information dialog

o **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 30 seconds
☐ Do not display other windows when the first dialog times out

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

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

o ***Test Defaults*** – returns the parameters edited on all dialog window tabs back to default values

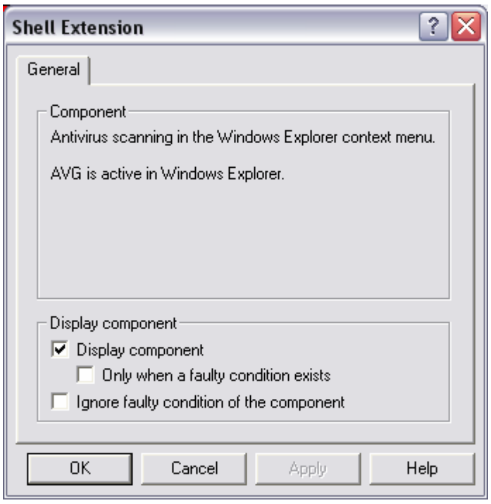
o ***Page Defaults*** – returns the parameters edited on a specific dialog tab back to default values

o ***OK*** – accepts changes, and closes the dialog window

o ***Cancel*** – closes the dialog window without accepting the changes

c) Properties

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

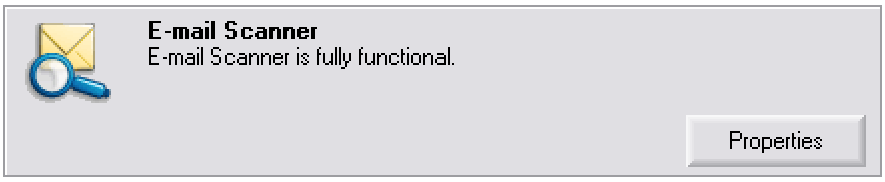


Component
Antivirus scanning in the Windows Explorer context menu.
AVG is active in Windows Explorer.

Display component
☑ Display component
□ Only when a faulty condition exists
□ Ignore faulty condition of the component

9.14. Control Center - E-mail Scanner

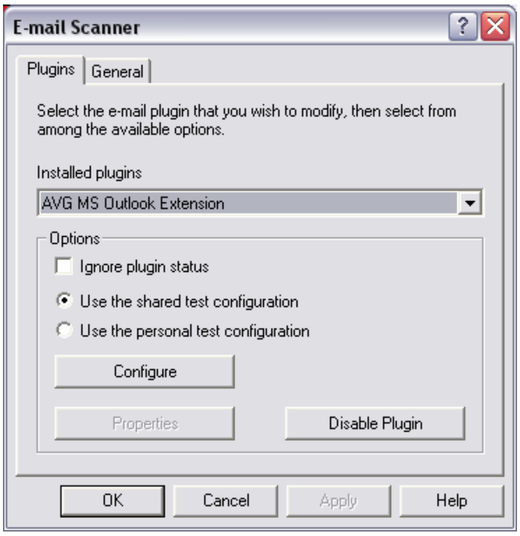
The **E-mail scanner** scans incoming and outgoing e-mail messages.



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

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:



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
○ Use the personal test configuration

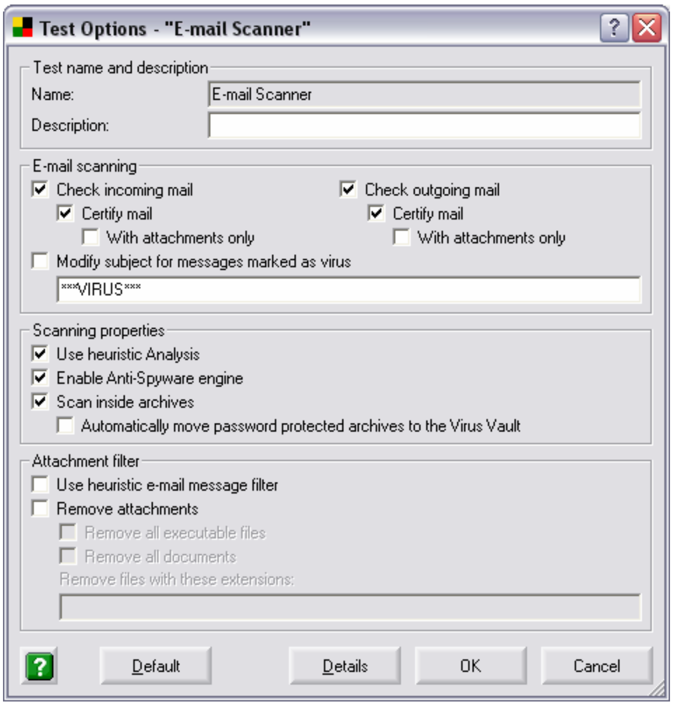
In the ***Options*** Section you can set up the following parameters:

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

- ***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 Scanner"

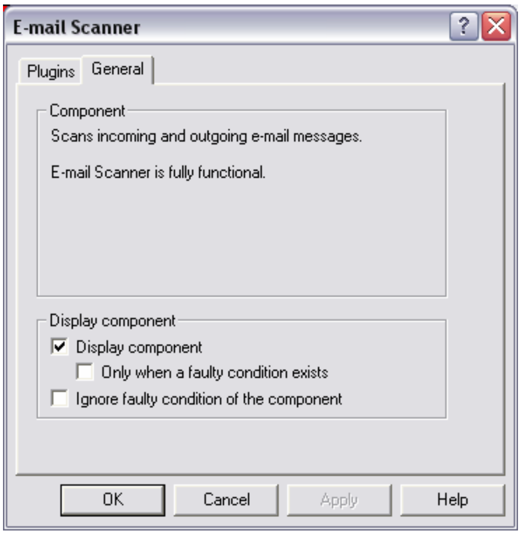
Test name and description
Name: E-mail Scanner
Description:

E-mail scanning
☑ Check incoming mail
☑ Certify mail
□ With attachments only
☑ Check outgoing mail
☑ Certify mail
□ With attachments only
□ Modify subject for messages marked as virus
VIRUS

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 extensions:

- ***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

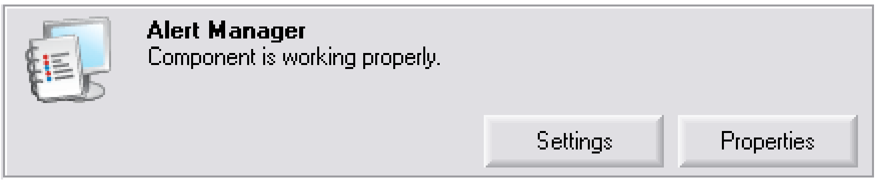
Component
Scans incoming and outgoing e-mail messages.

E-mail Scanner is fully functional.

Display component
☑ Display component
☐ Only when a faulty condition exists
☐ Ignore faulty condition of the component

9.15. Control Center – Alert Manager

The **Alert Manager** component controls form, which the program uses to report whenever a specific event occurs.

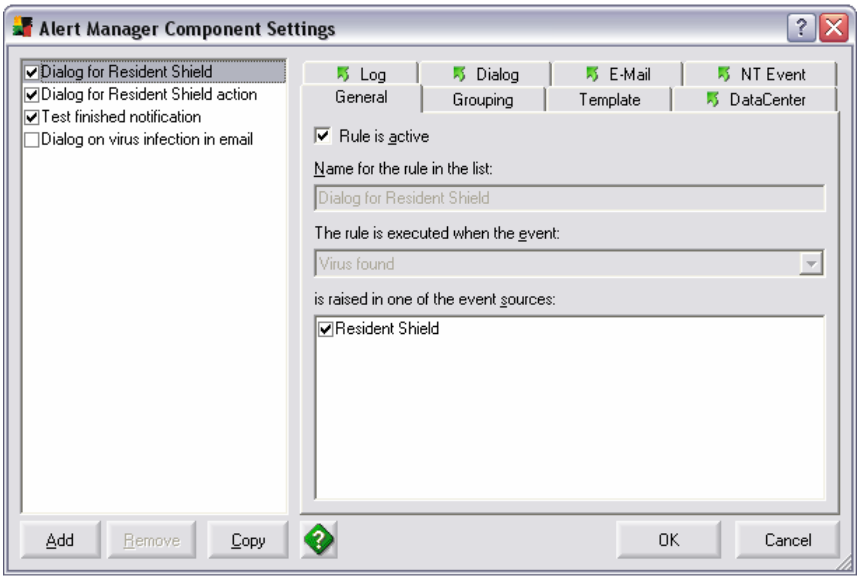


Alert Manager
Component is working properly.

Controlling elements of the **Alert Manager** component control panel are as follows:

a) Settings

The ***Settings*** button opens a dialog window ***Alert Manager Component Settings*** with seven tabs, which offer a possibility to configure parameters of a program behavior in certain situations as well as to define form of a report, which the program uses to inform a user:



Alert Manager Component Settings

☑ Dialog for Resident Shield
☑ Dialog for Resident Shield action
☑ Test finished notification
☐ Dialog on virus infection in email

☑ Rule is active

Name for the rule in the list: Dialog for Resident Shield

The rule is executed when the event: Virus found

is raised in one of the event sources:
☑ Resident Shield

The left part of the dialog window offers by default a section with four defined rules. This section is available from each tab in the ***Alert Manager Component Settings*** dialog window. Marking desired issues (rules) you will find out that parameters configured at individual tabs will be valid for reports related to chosen events. The default setting will display these rules:

- Dialog for Resident Shield
- Dialog for Resident shield action
- Test finished notification
- Dialog on virus infection in email

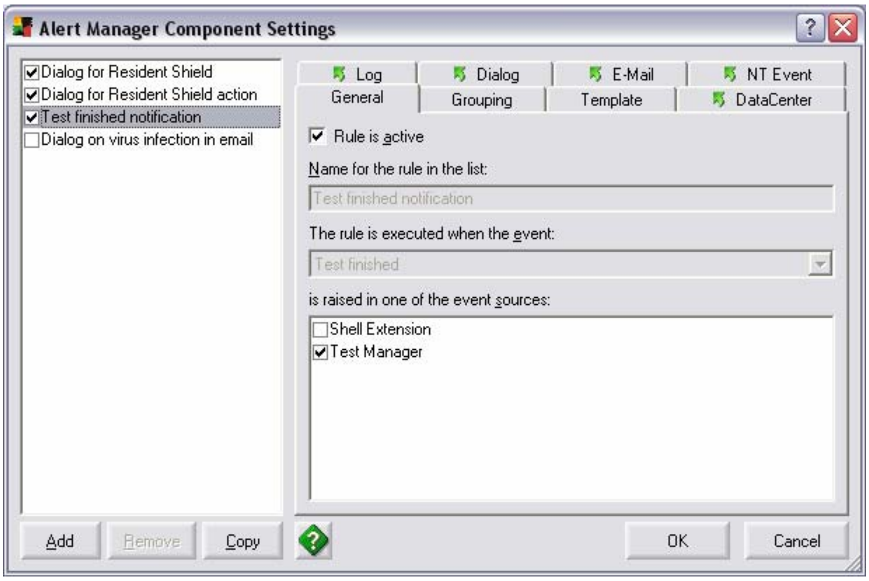
The list of rules can be extended (edited) using corresponding buttons placed in the dialog window ***Alert Manager Component Settings*** directly under the rules section:

- ***Add*** – using this button a new rule can be created, whose parameters can be defined in the right section of the dialog window in the ***General*** tab.
- ***Remove*** – chosen rules will be deleted and removed from the list. Rules adjusted as default cannot be deleted; so if the list contains just four default rules, the button is displayed as inactive.
- ***Copy*** – enables one to create a copy of a chosen rule, whose parameters can be edited afterwards as needed and afterwards a new rule can be created.

The tabs of the ***Alert Manager Component Settings*** dialog window are either without graphical marking (***General, Grouping, Template –*** tabs for adjustment of general parameters of a rule) or are marked with a green arrow (***Log, Dialog, E-Mail, NT Event -*** tabs which determine a report output, i.e. how and where an event should be displayed).

Individual tabs of the ***Alert Manager Component Settings*** dialog window are:

- ***General***


Alert Manager Component Settings

☑ Dialog for Resident Shield
☑ Dialog for Resident Shield action
☑ Test finished notification
□ Dialog on virus infection in email

☑ Rule is active

Name for the rule in the list: Test finished notification

The rule is executed when the event: Test finished

is raised in one of the event sources:

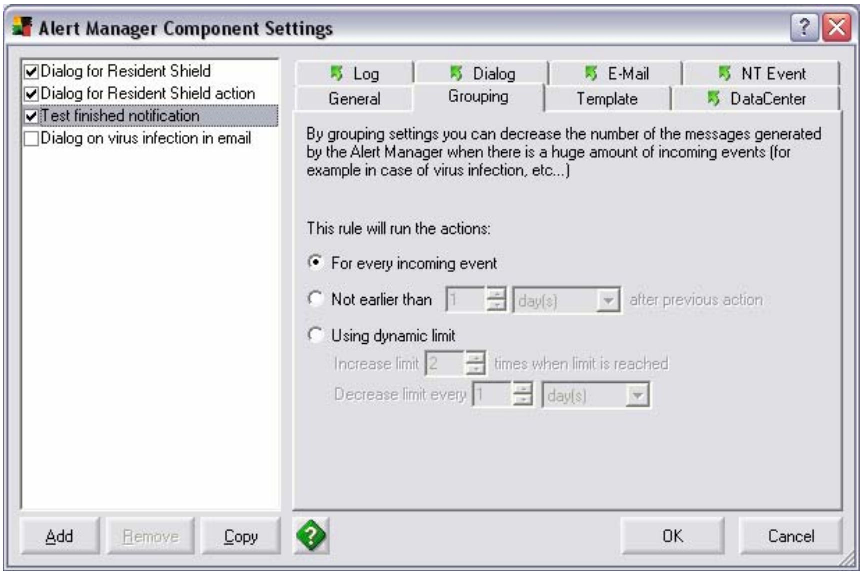
□ Shell Extension
☑ Test Manager

The ***General*** tab enables one to define general parameters of individual rules shown in the list in the left part of the dialog window. These following parameters can be edited:

- ***Rule is active –*** marking a checkbox at this issue you can decide whether the defined parameters will be asserted (Rule is active) or not (Rule is inactive).
- ***Name for the rule in the list –*** shows the name of a rule in a shape, in which it is stated in the list of rules in the left part of the dialog. If one of four default rules in the list is marked, you do not have a possibility to edit its name (the text field is defined), it is possible to edit just names of newly created rules.
- ***Rule is executed when the event -*** please, choose a type of an event from a drop down menu which the rule is related to. Type of an event with automatic settings for four rules cannot be changed; so if the list on of the default rules is chosen, the issue is deactivated.
- ***Is raised in one of the event sources –*** there are presented these AVG components in the list of event source at which a defined event might occur (the list can contain even one issue). Please, choose these components to which you wish to assign the rule.

o ***Grouping***

The ***Grouping*** tab enables managing a number of reports generated by the ***Alert Manager*** component. In case of a huge virus epidemic, the event frequency reported by the ***Alert Manager*** component can be very high. In such a case a user would be overloaded with individual reports. To prevent an excessive number of shown events you can define event grouping conditions for each rule.



Alert Manager Component Settings

☑ Dialog for Resident Shield
☑ Dialog for Resident Shield action
☑ Test finished notification
☐ Dialog on virus infection in email

By grouping settings you can decrease the number of the messages generated by the Alert Manager when there is a huge amount of incoming events (for example in case of virus infection, etc...)

This rule will run the actions:

● For every incoming event
○ Not earlier than 1 day(s) after previous action
○ Using dynamic limit
Increase limit 2 times when limit is reached
Decrease limit every 1 day(s)

The action can be executed:

- ***For every incoming event –*** if you mark this option, a user will be informed about every individual event.
- ***Not earlier than ... after previous action -*** It is possible to delay the next action launch by setting a minimum time interval for which

the same event is ignored. After the minimum time interval passes, a user will be informed about the total number of actions, which occurred in this time interval.

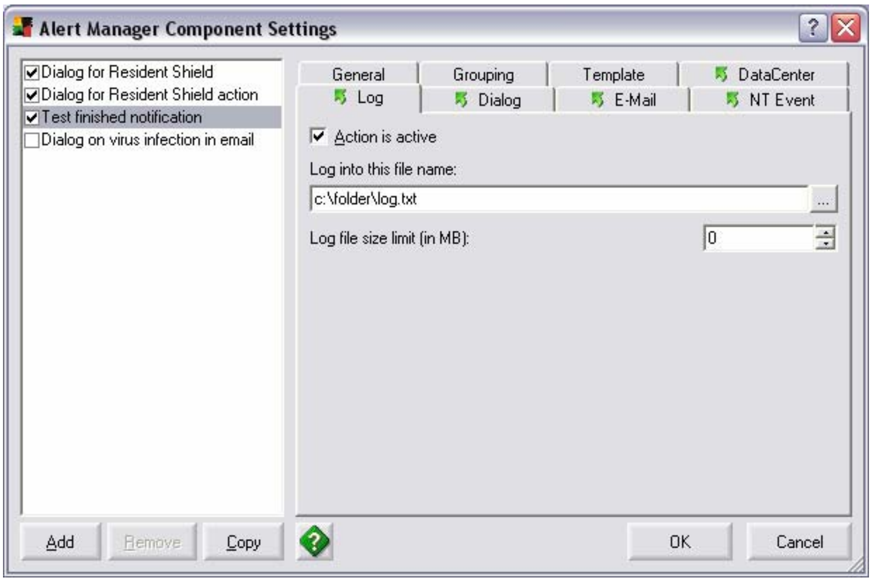
- ***Using dynamic limit*** **–** it is possible to set up a frequency of generated reports on an event on the basis of a starting limit, which is given implicitly on a value of one report. When an event to be reported occurs and a report on this event is sent, the limit increases automatically n-times according a value you have set up. Thus, afterwards you will not be informed about each following event, but the report will be shown only after the number of events reaches the defined n-multiple of the starting limit.

  At continuous occurrence of reported events (e.g. at virus epidemic) the limit will be dynamically increased up the moment the number of events starts to decrease. The set up limit will afterwards go to the starting value after a defined time interval.

o ***Template***

The ***Template*** enables one to change a text which will be displayed when a certain event occurs. For four default rules the text is set as automatic and you can edit it. For newly defined rules you can set your own text, which is to be displayed.

o ***Log***



Alert Manager Component Settings

☑ Dialog for Resident Shield
☑ Dialog for Resident Shield action
☑ Test finished notification
□ Dialog on virus infection in email

☑ Action is active

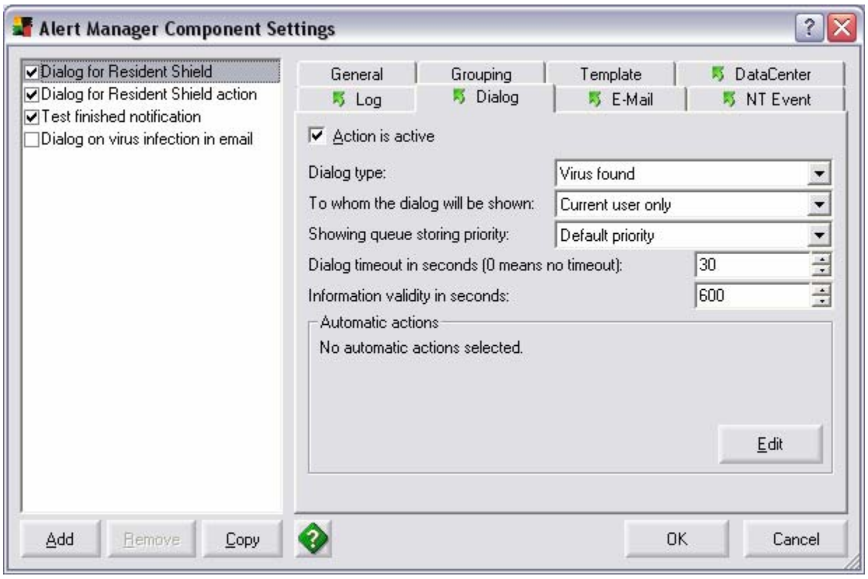
Log into this file name: c:\folder\log.txt

Log file size limit (in MB): 0

Using the ***Log*** tab you can define, whether the actions assigned to individual rules will be recorded. If you wish to check all reports related to individual events, please mark the issue ***Action is active.***

o ***Dialog***

Using the ***Dialog*** tab you can define parameters for displaying information on an event in a form of a dialog:


Alert Manager Component Settings

☑ Dialog for Resident Shield
☑ Dialog for Resident Shield action
☑ Test finished notification
□ Dialog on virus infection in email

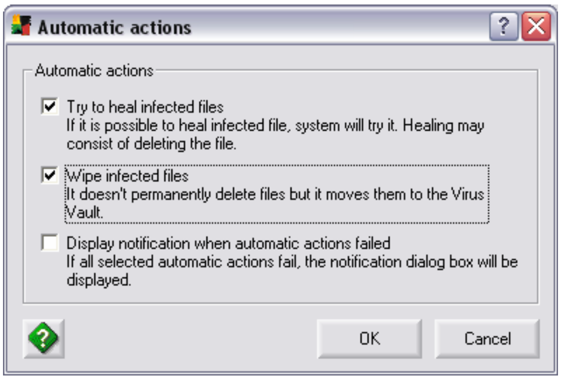
☑ Action is active

Dialog type: Virus found
To whom the dialog will be shown: Current user only
Showing queue storing priority: Default priority
Dialog timeout in seconds (0 means no timeout): 30
Information validity in seconds: 600

Automatic actions
No automatic actions selected.

- ***Dialog type*** – please choose, whether a dialog will be displayed in a form of a text report or as a virus report
- ***To whom the dialog will be shown –*** please choose, whether a dialog will be displayed just for a user at whose workstation an event occurred or to all currently logged users
- ***Showing queue storing priority –*** please determine the priority of a running process. In case several events which should be reported happen contemporarily, individual reports will be displayed in an order according a predefined priority of a reported process.
- ***Dialog timeout in seconds –*** please determine for how long an information dialog will be displayed for a user.
- ***Information validity in seconds –*** you will be able to determine a longest time interval after which you wish to be informed the event occurred – if the information was not possible, for any reason, to be delivered immediately after the event occurred.

If there is an option ***Virus found*** chosen in the ***Dialog*** tab, the ***Edit*** button in the lower part of the dialog is activated; it opens an ***Automatic actions*** dialog**,** in which it is possible to define a procedure in case a virus is found:


Automatic actions

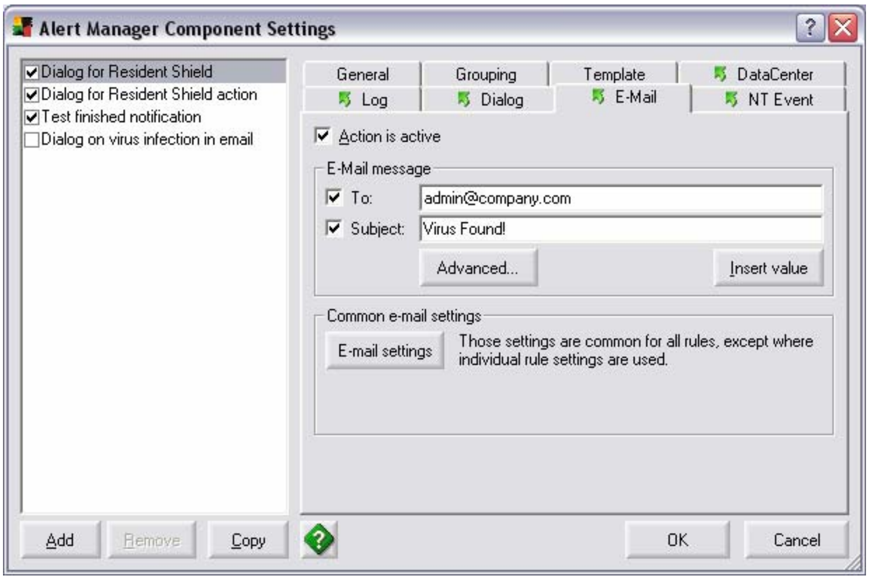
Automatic actions

☑ Try to heal infected files
If it is possible to heal infected file, system will try it. Healing may consist of deleting the file.

☑ Wipe infected files
It doesn't permanently delete files but it moves them to the Virus Vault.

□ Display notification when automatic actions failed
If all selected automatic actions fail, the notification dialog box will be displayed.

- ***E-mail***



Alert Manager Component Settings

- ☑ Dialog for Resident Shield
- ☑ Dialog for Resident Shield action
- ☑ Test finished notification
- □ Dialog on virus infection in email

☑ Action is active

E-Mail message
☑ To: admin@company.com
☑ Subject: Virus Found!

Common e-mail settings

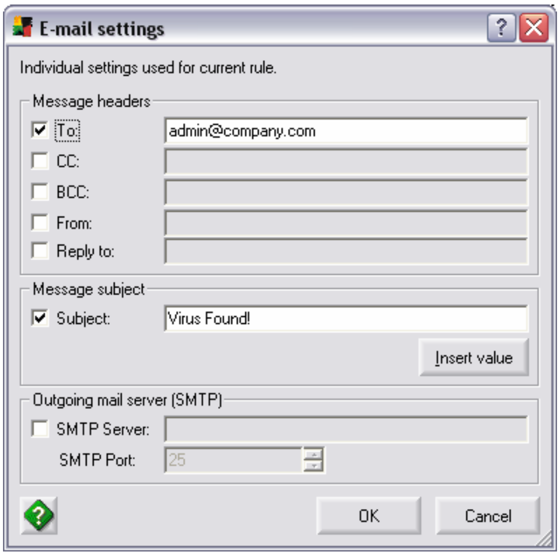
Those settings are common for all rules, except where individual rule settings are used.

Using the ***E-mail*** tab it is possible to set parameters for displaying information about an event in a form an e-mail message. The dialog is divided into two sections:

- ***E-mail message –*** please provide an e-mail address ***(To)*** and define text, which will be displayed as a subject of the e-mail message ***(Subject)***

  This section contains two buttons:

  - ***Advanced value –*** the button opens an ***E-mail settings*** dialog, using which it is possible to edit all parameters of an e-mail message: you can define contents of the Message headers, insert a text displayed as a subject of a message or choose this text from a menu dropped after pressing the ***Insert value*** button as well as to set a value of the SMTP server and a number of a respective port:



E-mail settings

Individual settings used for current rule.

Message headers
☑ To: admin@company.com
□ CC:
□ BCC:
□ From:
□ Reply to:

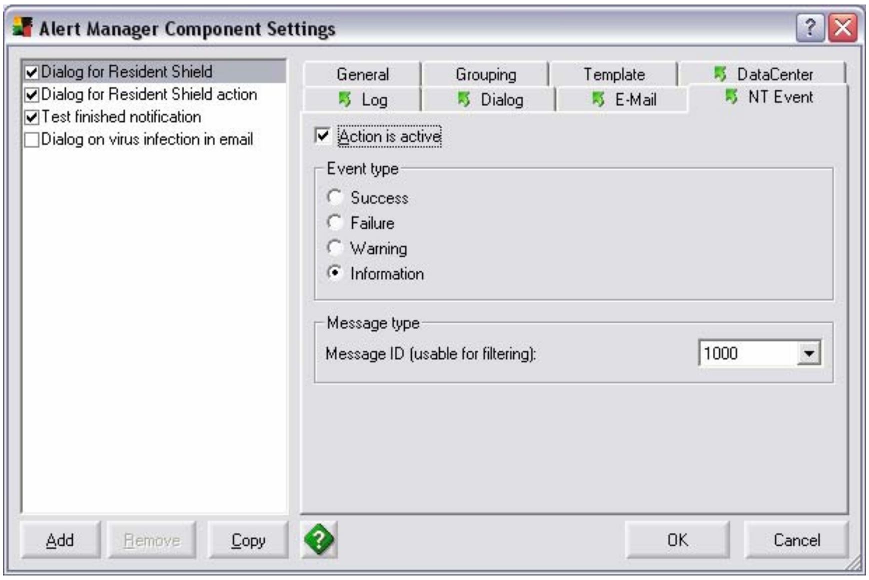
Message subject
☑ Subject: Virus Found!

Outgoing mail server (SMTP)
□ SMTP Server:
SMTP Port: 25

- ***Insert value –*** the button opens a menu with a list of issues which can be used as a text in the subject of a message.

o ***Common setting used within all rules –*** using this section you will be able to define parameters of e-mail commonly for all rules set by a component ***Alert Manager.*** Pressing the ***E-mail settings*** button you will open a dialog ***E-mail settings,*** using which you can define all parameters of an e-mail message – see description in the previous paragraph.

o ***NT Event***



☑ Dialog for Resident Shield
☑ Dialog for Resident Shield action
☑ Test finished notification
☐ Dialog on virus infection in email

☑ Action is active

Event type
○ Success
○ Failure
○ Warning
● Information

Message type
Message ID (usable for filtering): 1000

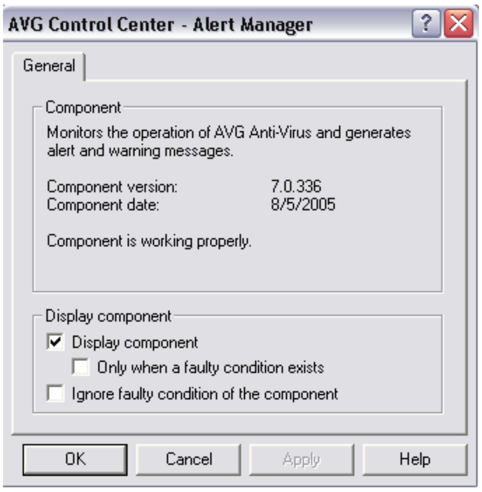
Using the ***NT Event*** tab it is possible to set parameters of information record in the operating system protocol (valid only for OS at the Windows NT platform):

- ***Event type –*** please choose, what events should be recorded (we recommend to record just errors in order to keep the protocol size reasonable)

- ***Message type –*** please choose an identifier, which you wish to assign to a message (it serves for easier finding a record in the OS protocol)

b) Properties

Offers listed information about the ***Alert Manager*** component and enables one to define how the component will be displayed:



Component

Monitors the operation of AVG Anti-Virus and generates alert and warning messages.

Component version: 7.0.336
Component date: 8/5/2005

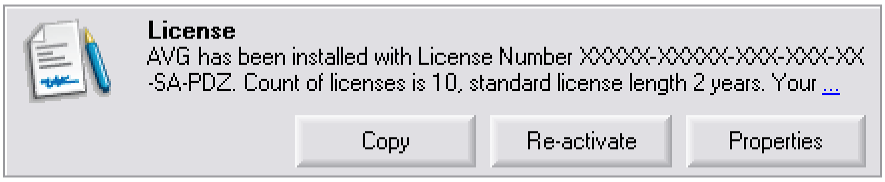
Component is working properly.

Display component

☑ Display component
□ Only when a faulty condition exists
□ Ignore faulty condition of the component

9.16. Control Center - License

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



License

AVG has been installed with License Number XXXXX-XXXXX-XXX-XXX-XX -SA-PDZ. Count of licenses is 10, standard license length 2 years. Your ...

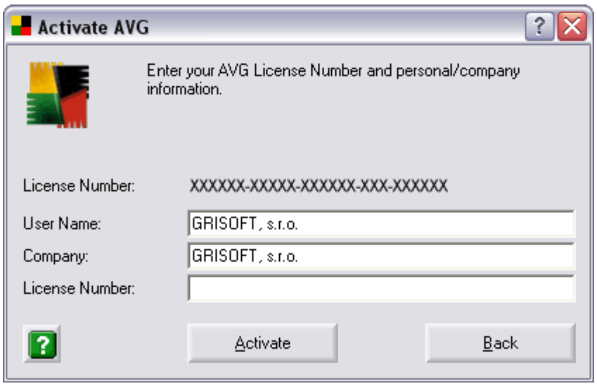
The ***License*** panel's operating buttons are:

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**.

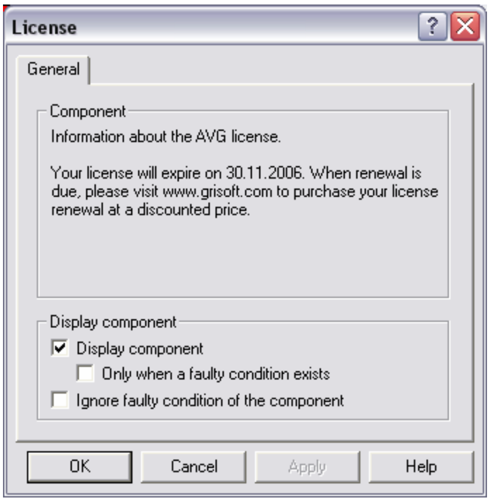


Enter your AVG License Number and personal/company information.

License Number: XXXXXX-XXXXX-XXXXXX-XXX-XXXXXX
User Name: GRISOFT, s.r.o.
Company: GRISOFT, s.r.o.
License Number:

c) Properties

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



Component

Information about the AVG license.

Your license will expire on 30.11.2006. When renewal is due, please visit www.grisoft.com to purchase your license renewal at a discounted price.

Display component

☑ Display component

☐ Only when a faulty condition exists

☐ Ignore faulty condition of the component

10. Virus Vault

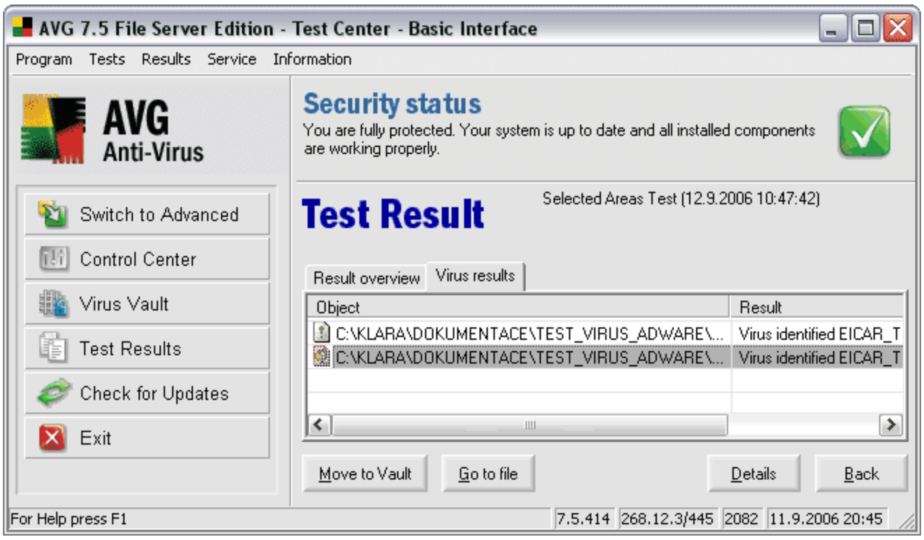
The ***Virus Vault*** application is a safe environment for the management of suspect/infected objects detected during AVG tests.

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.

10.1. 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



Security status

You are fully protected. Your system is up to date and all installed components are working properly.

Test Result

Selected Areas Test (12.9.2006 10:47:42)

Object	Result
C:\KLARA\DOKUMENTACE\TEST_VIRUS_ADWARE\...	Virus identified EICAR_T
C:\KLARA\DOKUMENTACE\TEST_VIRUS_ADWARE\...	Virus identified EICAR_T

For Help press F1 | 7.5.414 | 268.12.3/445 | 2082 | 11.9.2006 20:45

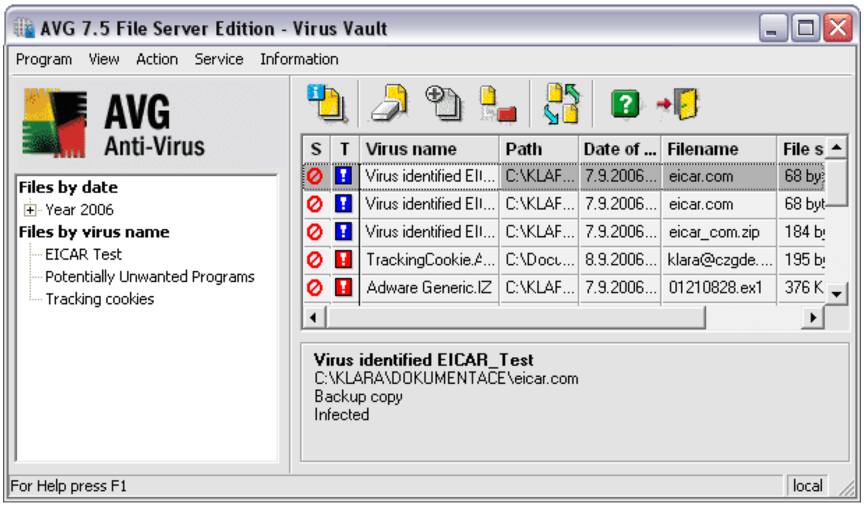
Within the **Virus Vault** you can then examine the object, delete it, and even heal and restore the object when a new cure for this kind of infection is implemented.

10.2. 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



AVG 7.5 File Server Edition - Virus Vault
Program View Action Service Information
AVG Anti-Virus
For Help press F1
local

Files by date
- Year 2006

Files by virus name
- EICAR Test
- Potentially Unwanted Programs
- Tracking cookies

S	T	Virus name	Path	Date of ...	Filename	File s
⊘	!	Virus identified EI...	C:\KLAF...	7.9.2006...	eicar.com	68 by
⊘	!	Virus identified EI...	C:\KLAF...	7.9.2006...	eicar.com	68 byt
⊘	!	Virus identified EI...	C:\KLAF...	7.9.2006...	eicar_com.zip	184 b
⊘	!	TrackingCookie.A...	C:\Docu...	8.9.2006...	klara@czgde....	195 b
⊘	!	Adware Generic.IZ	C:\KLAF...	7.9.2006...	01210828.ex1	376 K

Virus identified EICAR_Test
C:\KLARA\DOKUMENTACE\eicar.com
Backup copy
Infected

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:

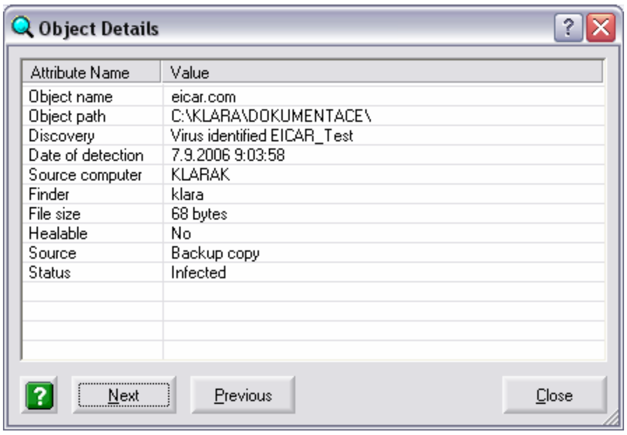
- ***S*** – object status:
  - infected/suspect object (red crossed circle)
  - cured object (red cross)
- ***T*** – object type
  - ***object moved to the Virus Vault*** (exclamation mark in the red field)
  - ***object's backup created in Virus Vault before healing*** (exclamation mark in the blue 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

10.3. 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 7. AVG Basic Test Center Interface.

11. 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 7.8 Test Scheduling or 8.2 Scheduled Tasks 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.

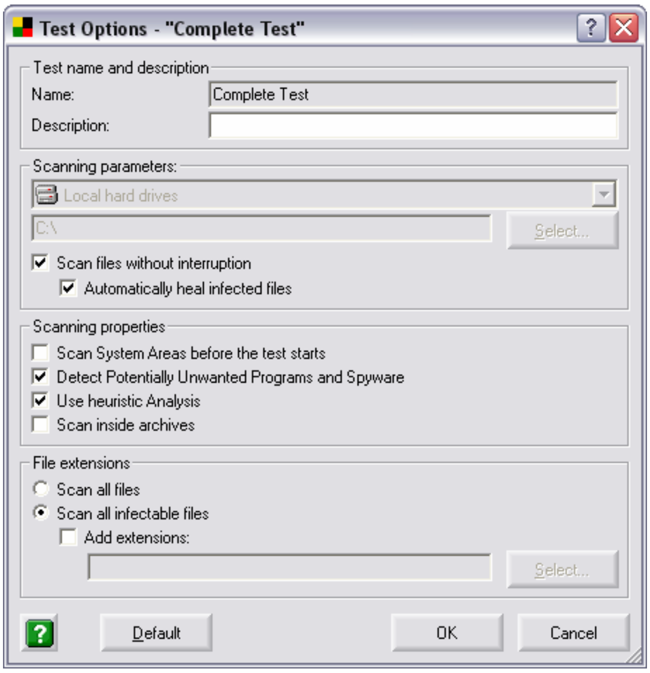
11.1. Complete Test

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 - "Complete Test"

Test name and description
Name: Complete Test
Description:

Scanning parameters:
Local hard drives
C:\
☑ Scan files without interruption
☑ Automatically heal infected files

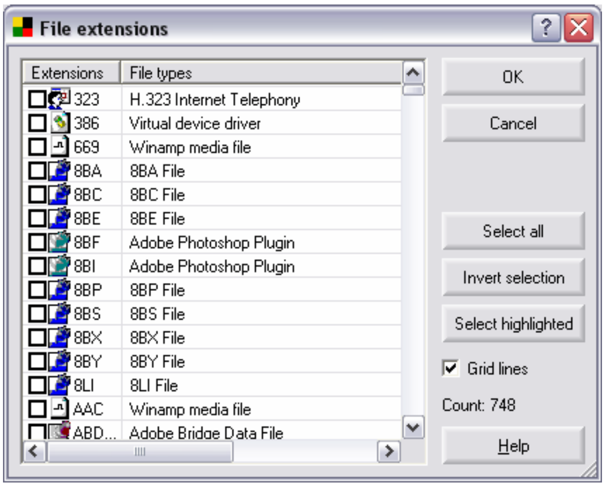
Scanning properties
□ Scan System Areas before the test starts
☑ Detect Potentially Unwanted Programs and Spyware
☑ Use heuristic Analysis
□ Scan inside archives

File extensions
○ Scan all files
● Scan all infectable files
□ Add extensions:

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 chapter 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:



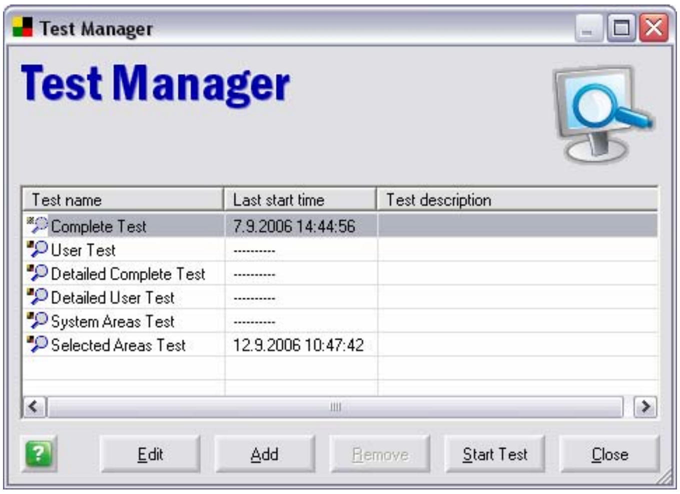
File extensions

Extensions	File types
□ 323	H.323 Internet Telephony
□ 386	Virtual device driver
□ 669	Winamp media file
□ 8BA	8BA File
□ 8BC	8BC File
□ 8BE	8BE File
□ 8BF	Adobe Photoshop Plugin
□ 8BI	Adobe Photoshop Plugin
□ 8BP	8BP File
□ 8BS	8BS File
□ 8BX	8BX File
□ 8BY	8BY File
□ 8LI	8LI File
□ AAC	Winamp media file
□ ABD...	Adobe Bridge Data File

☑ Grid lines

Count: 748

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

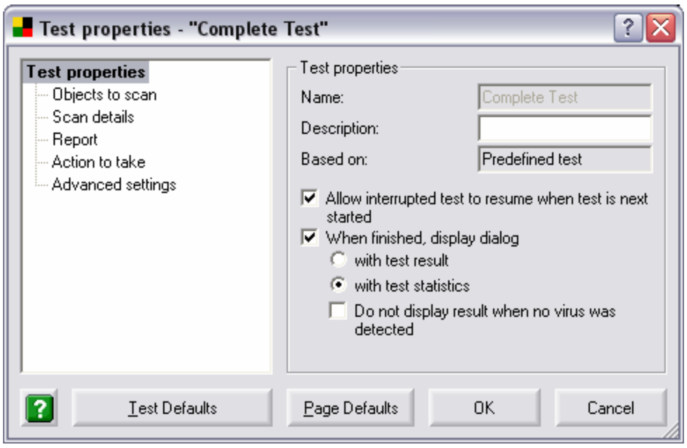


Test Manager

Test name	Last start time	Test description
Complete Test	7.9.2006 14:44:56	
User Test	---------	
Detailed Complete Test	---------	
Detailed User Test	---------	
System Areas Test	---------	
Selected Areas Test	12.9.2006 10:47:42	

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***



Test properties - "Complete Test"

Test properties
- Objects to scan
- Scan details
- Report
- Action to take
- Advanced settings

Test properties

Name: Complete Test

Description:

Based on: Predefined test

☑ Allow interrupted test to resume when test is next started

☑ When finished, display dialog

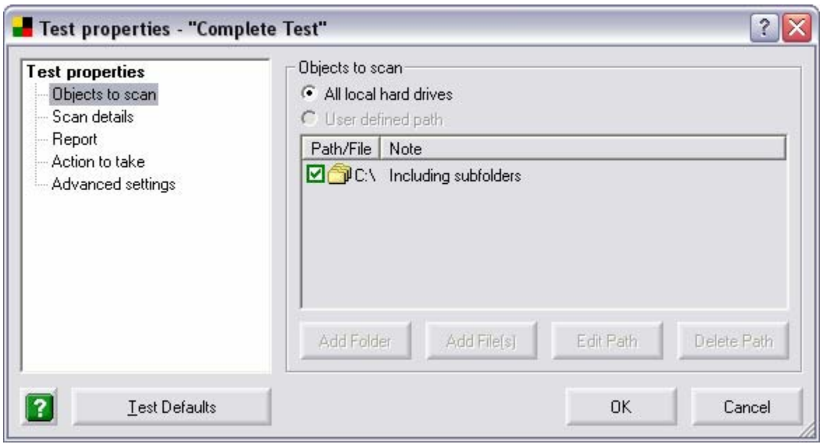
○ with test result

● with test statistics

□ Do not display result when no virus was detected

- ***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

o ***Objects to scan***



Objects to scan

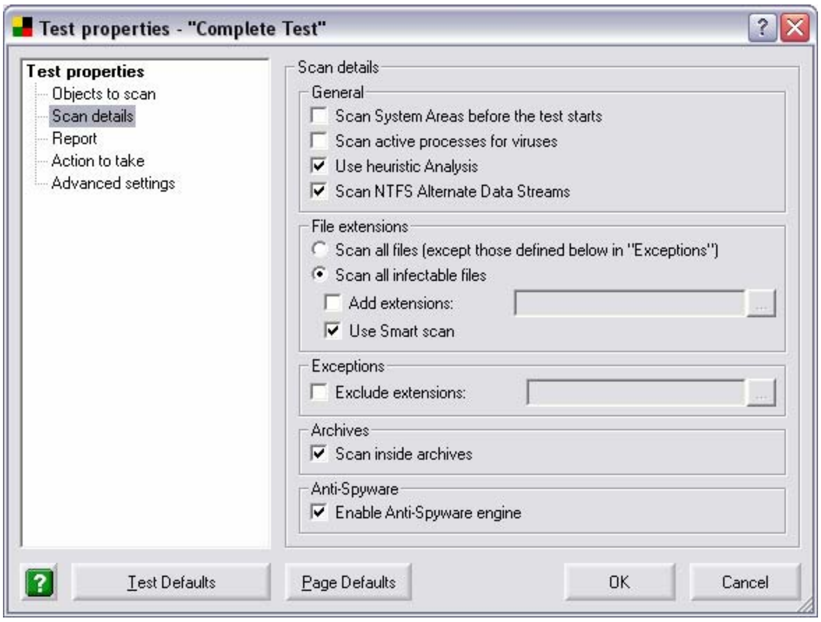
● All local hard drives

○ User defined path

Path/File	Note
☑ C:\	Including subfolders

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***.

o ***Scan 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 infectable files

□ Add extensions:

☑ Use Smart scan

Exceptions

□ Exclude extensions:

Archives

☑ Scan inside archives

Anti-Spyware

☑ Enable Anti-Spyware engine

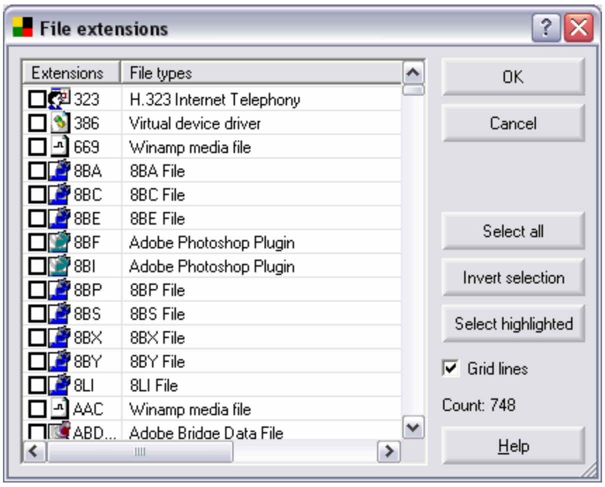
- ***General*** – in this dialog you can define whether the system areas should be scanned and if heuristic analysis should be used for scanning. You can also scan all active operating system processes by ticking the ***Scan active processes for viruses*** check box. An active process is basically a 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:



Extensions	File types
□ 323	H.323 Internet Telephony
□ 386	Virtual device driver
□ 669	Winamp media file
□ 8BA	8BA File
□ 8BC	8BC File
□ 8BE	8BE File
□ 8BF	Adobe Photoshop Plugin
□ 8BI	Adobe Photoshop Plugin
□ 8BP	8BP File
□ 8BS	8BS File
□ 8BX	8BX File
□ 8BY	8BY File
□ 8LI	8LI File
□ AAC	Winamp media file
□ ABD...	Adobe Bridge Data File

☑ Grid lines

Count: 748

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:

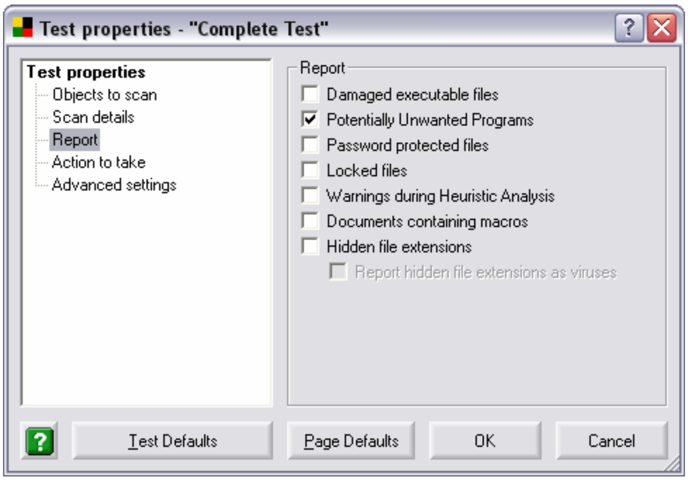
- ***OK*** – accepts all selected extensions, includes all files with the specified extension into scanning by the ***Complete Test*** and closes the ***File extensions*** dialog window

- ***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 ***Shif***t 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***

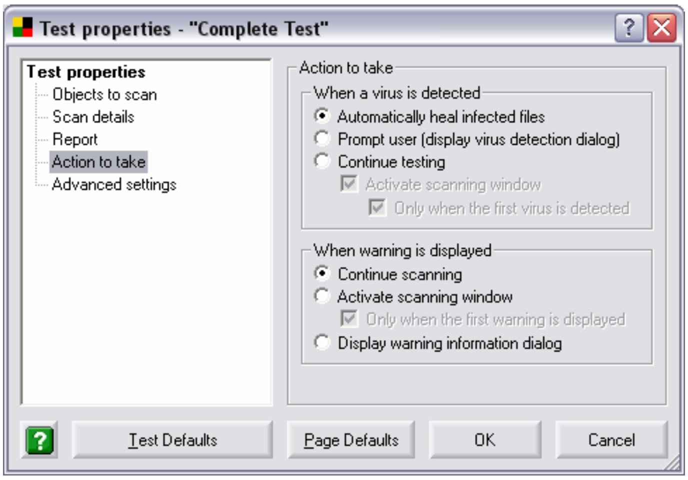

Test properties - "Complete Test"

Test properties
- Objects to scan
- Scan details
- Report
- Action to take
- Advanced settings

Report
□ Damaged executable files
☑ Potentially Unwanted Programs
□ Password protected files
□ Locked files
□ Warnings during Heuristic Analysis
□ Documents containing macros
□ Hidden file extensions
□ Report hidden file extensions as viruses

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.

o ***Action to take***



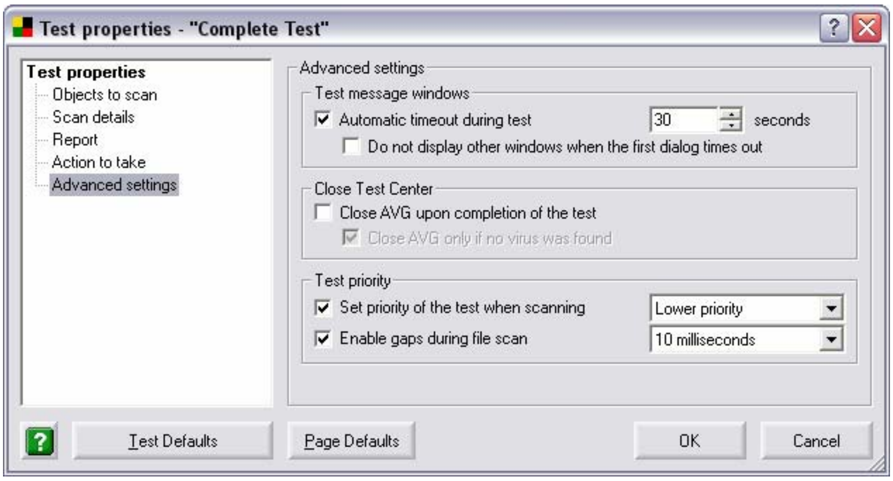
Action to take

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 warning is displayed
○ Display 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).

o ***Advanced settings***



Advanced settings

Test message windows
☑ Automatic timeout during test 30 seconds
☐ Do not display other windows when the first dialog times out

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:

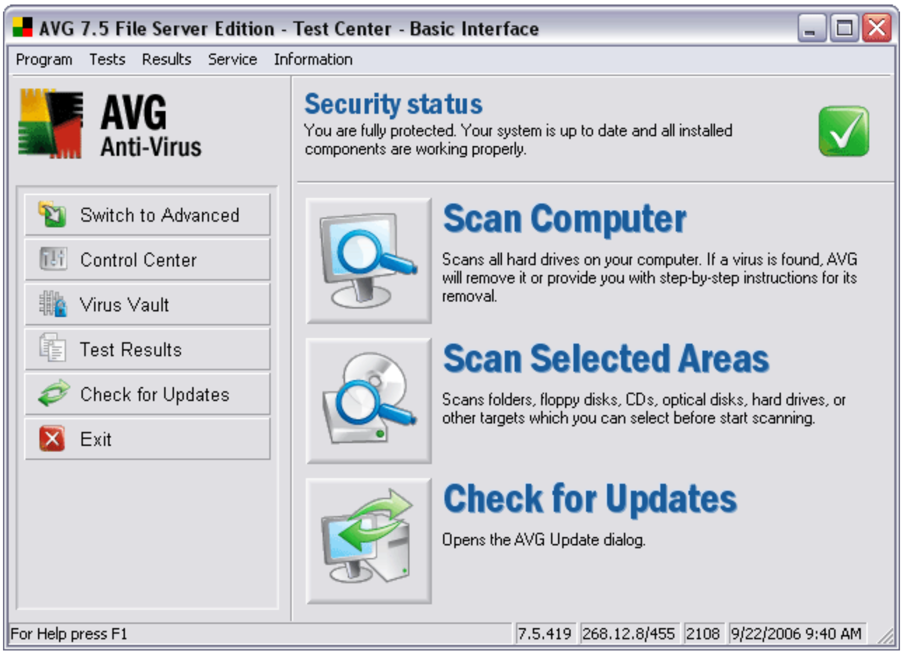
- ***Test message windows*** – specify for how long the warning messages should be displayed

- ***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***:


AVG 7.5 File Server Edition - Test Center - Basic Interface

Security status

You are fully protected. Your system is up to date and all installed components are working properly.

Scan Computer

Scans all hard drives on your computer. If a virus is found, AVG will remove it or provide you with step-by-step instructions for its removal.

Scan Selected Areas

Scans folders, floppy disks, CDs, optical disks, hard drives, or other targets which you can select before start scanning.

Check for Updates

Opens the AVG Update dialog.

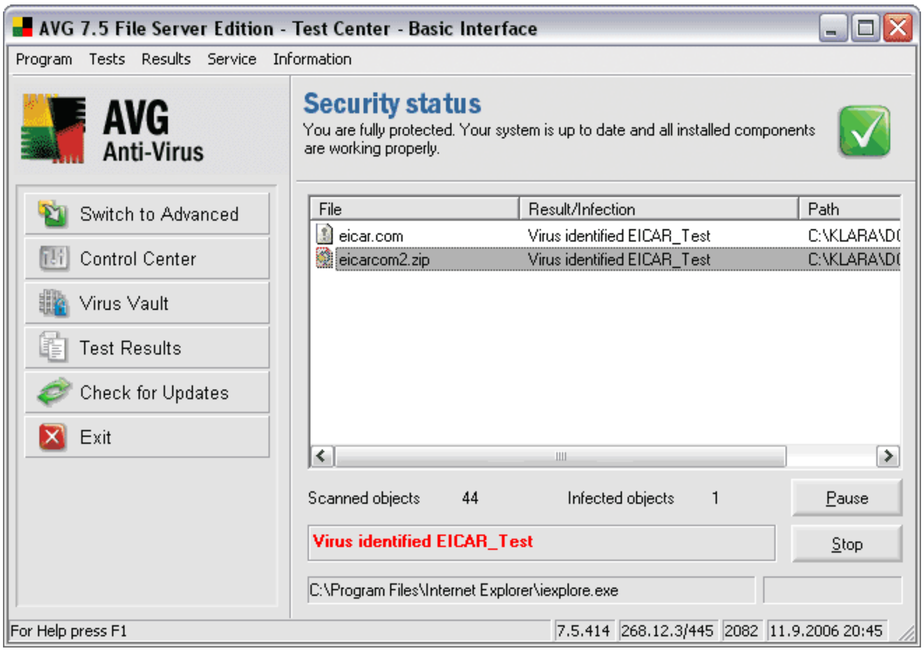
For Help press F1 | 7.5.419 | 268.12.8/455 | 2108 | 9/22/2006 9:40 AM

Also, you can run the ***Complete Test***:

- o in the ***Basic Test Interface*** select from the top menu: ***Tests/Start Complete Test***
- o 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 File Server Edition - Test Center - Basic Interface

Security status

You are fully protected. Your system is up to date and all installed components are working properly.

File	Result/Infection	Path
eicar.com	Virus identified EICAR_Test	C:\KLARA\D(
eicarcom2.zip	Virus identified EICAR_Test	C:\KLARA\D(

Scanned objects 44 Infected objects 1

Virus identified EICAR_Test

C:\Program Files\Internet Explorer\iexplore.exe

For Help press F1 7.5.414 268.12.3/445 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

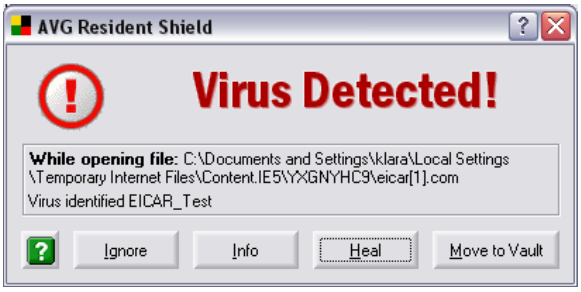
In the window's bottom section you can continuously watch the test progress, and review information on:

- Number of scanned objects
- Number of infected objects
- Number of identified viruses
- 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

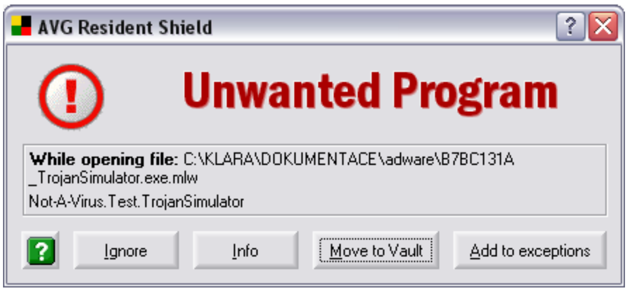
The Virus Detected dialog informs you about the detected infected file and its location. Selecting the ***Do not show this dialog again (scan files without interruption)*** option you confirm you do not wish to be informed about the scanning results before the test is completed.

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:



While opening file: C:\KLARA\DOKUMENTACE\adware\B7BC131A _TrojanSimulator.exe.mlw
Not-A-Virus.Test.TrojanSimulator

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:

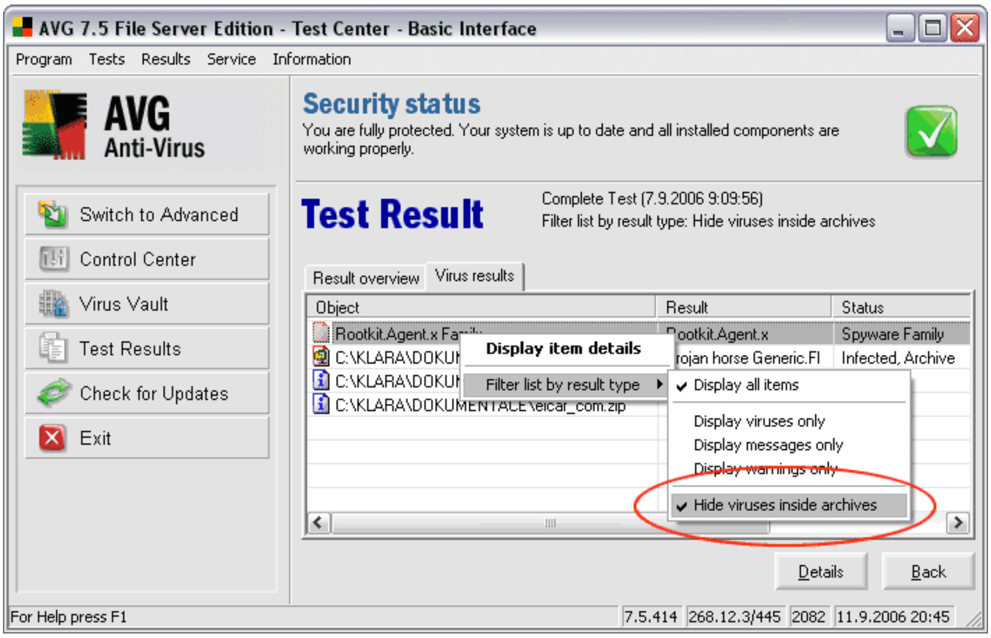
- ***Ignore*** – ignores the **Resident Shield** warning, and allows you to continue working (and also forbids access to the threat)
- ***Info*** – opens the on-line virus encyclopedia where you can look up detailed information on the identified threat
- ***Move to Vault*** – moves the potentially unwanted 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:



Security status

You are fully protected. Your system is up to date and all installed components are working properly.

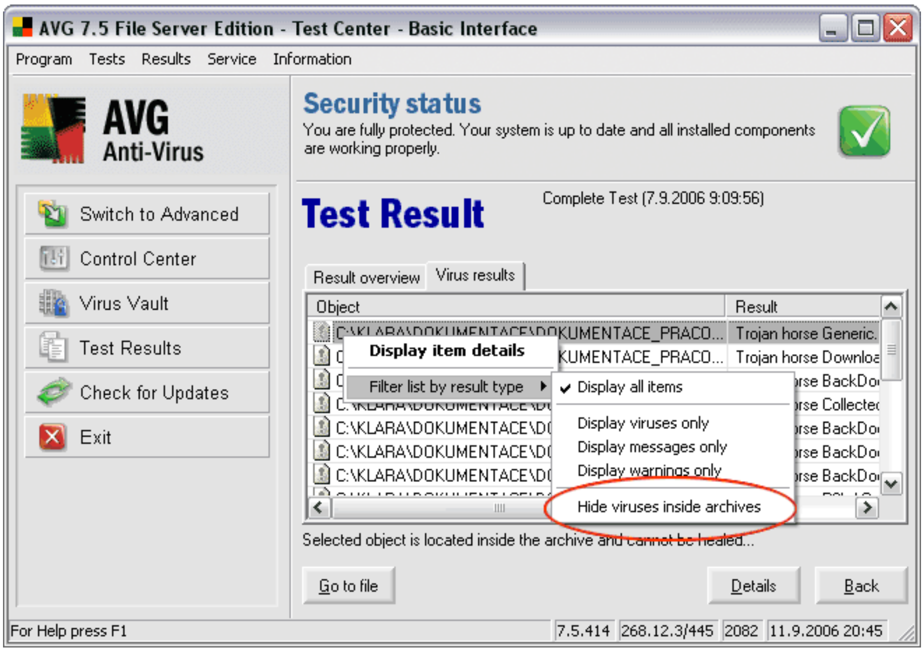
Test Result

Complete Test (7.9.2006 9:09:56)
Filter list by result type: Hide viruses inside archives

Object	Result	Status
Rootkit.Agent.x Fa	ootkit.Agent.x	Spyware Family
C:\KLARA\DOKUI	rojan horse Generic.FI	Infected, Archive
C:\KLARA\DOKUI		
C:\KLARA\DOKUMENTACE\eicar_com.zip		

✓ Display all items
Display viruses only
Display messages only
Display warnings only
✓ Hide viruses inside archives

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):



Security status

You are fully protected. Your system is up to date and all installed components are working properly.

Test Result

Complete Test (7.9.2006 9:09:56)

Object	Result
C:\KLARA\DOKUMENTACE\DOKUMENTACE_PRACO...	Trojan horse Generic.
C KUMENTACE_PRACO...	Trojan horse Downloa
C	rse BackDo
C:\KLARA\DOKUMENTACE\D	rse Collecte
C:\KLARA\DOKUMENTACE\D	rse BackDo
C:\KLARA\DOKUMENTACE\D	rse BackDo
C:\KLARA\DOKUMENTACE\D	rse BackDo

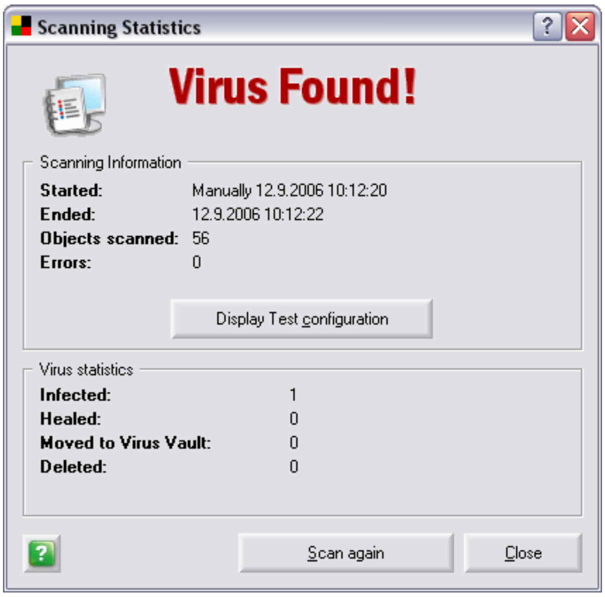
Selected object is located inside the archive and cannot be healed...

For Help press F1 | 7.5.414 | 268.12.3/445 | 2082 | 11.9.2006 20:45

Next to the information on the test type and its launch date in the upper right-hand 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:



Virus Found!

Scanning Information

Started: Manually 12.9.2006 10:12:20
Ended: 12.9.2006 10:12:22
Objects scanned: 56
Errors: 0

Virus statistics

Infected: 1
Healed: 0
Moved to Virus Vault: 0
Deleted: 0

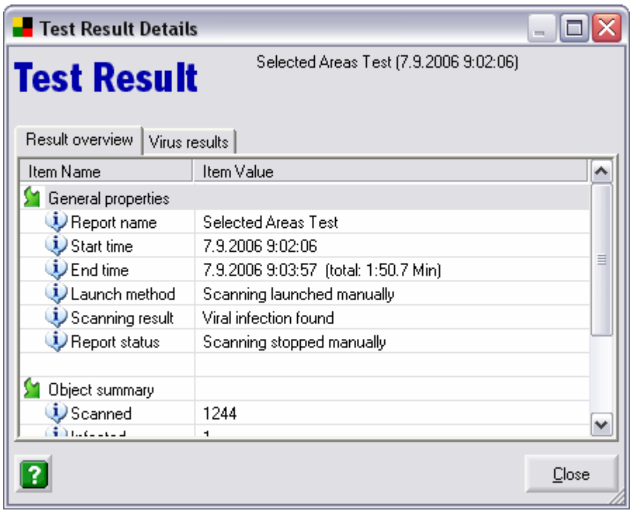
Whenever infection is detected, AVG tries to heal it automatically. If there is any problem healing the infected file, you will be asked for further instructions. Sometimes, you have to treat the infected files manually. The recommended solution for this case is to move the infected file into the **Virus**

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

*For more information on Virus Vault refer to [10. Virus Vault](#)**.***

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

- 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



Test Result Details

Test Result

Selected Areas Test (7.9.2006 9:02:06)

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
Scanning result	Viral infection found
Report status	Scanning stopped manually
Object summary	
Scanned	1244
Infected	1

11.2. 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 [Complete test settings](#) *related section of this chapter*.

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 11.1 Complete test.

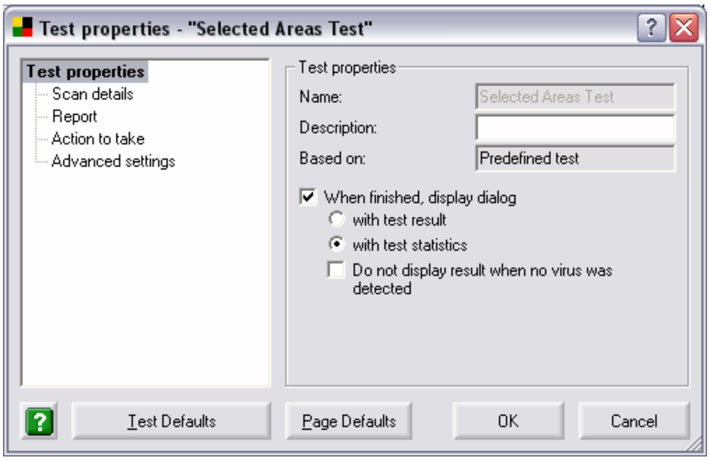
11.3. Selected Areas Test

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:

- 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
○ with test result
● with test statistics
□ Do not display result when no virus was detected

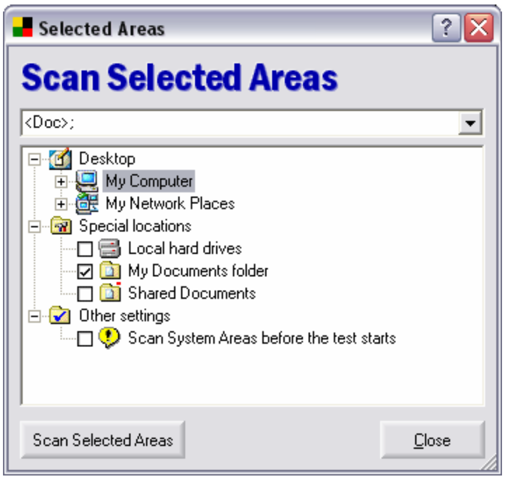
In the left section of the newly-opened dialog you can select from several test configuration sections – the test configuration itself is very similar to the ***Complete Test*** configuration, see chapter 11.1 a) – Complete Test - Settings.

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
- 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

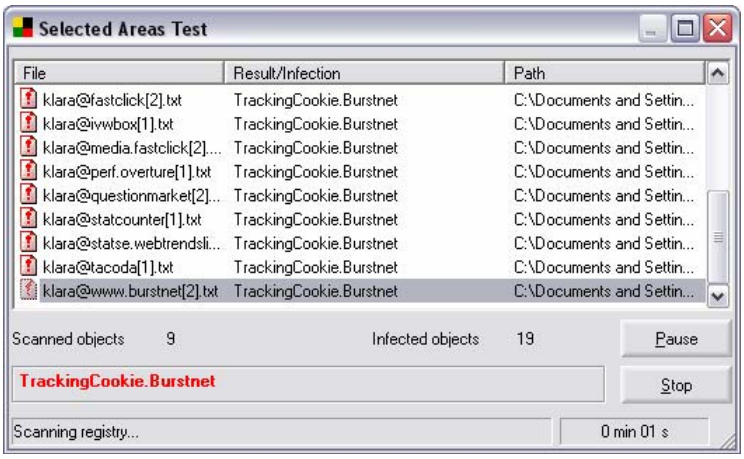
Scan Selected Areas

<Doc>;

- Desktop
  - My Computer
  - My Network Places
- Special locations
  - □ Local hard drives
  - ☑ My Documents folder
  - □ Shared Documents
- Other settings
  - □ Scan System Areas before the test starts

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 Areas Test

File	Result/Infection	Path
klara@fastclick[2].txt	TrackingCookie.Burstnet	C:\Documents and Settin...
klara@ivwbox[1].txt	TrackingCookie.Burstnet	C:\Documents and Settin...
klara@media.fastclick[2]....	TrackingCookie.Burstnet	C:\Documents and Settin...
klara@perf.overture[1].txt	TrackingCookie.Burstnet	C:\Documents and Settin...
klara@questionmarket[2]...	TrackingCookie.Burstnet	C:\Documents and Settin...
klara@statcounter[1].txt	TrackingCookie.Burstnet	C:\Documents and Settin...
klara@statse.webtrendsli...	TrackingCookie.Burstnet	C:\Documents and Settin...
klara@tacoda[1].txt	TrackingCookie.Burstnet	C:\Documents and Settin...
klara@www.burstnet[2].txt	TrackingCookie.Burstnet	C:\Documents and Settin...

Scanned objects 9 Infected objects 19

TrackingCookie.Burstnet

Scanning registry... 0 min 01 s

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:

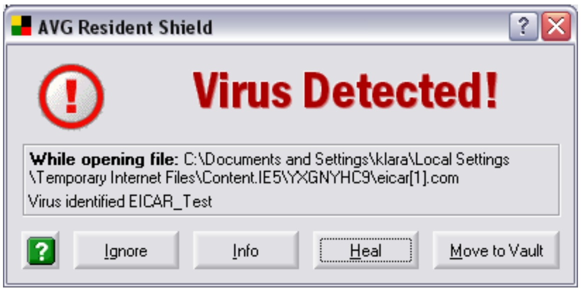
- Number of scanned objects
- Number of infected objects
- Number of identified viruses
- Currently scanned file location

- Test status

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

c) *Selected Areas Test – Results*

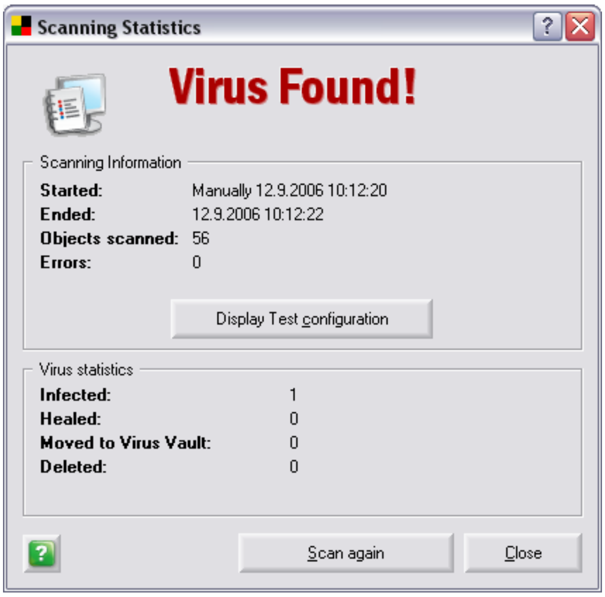
If a suspect file is detected during the test run, you will be informed about it with this warning. *For a detailed description of the warning message please refer to chapter 11.1 d) – Complete Test – Results*:



While opening file: C:\Documents and Settings\klara\Local Settings\Temporary Internet Files\Content.IE5\YXGNYHC9\eicar[1].com
Virus identified EICAR_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 Information

Started:	Manually 12.9.2006 10:12:20
Ended:	12.9.2006 10:12:22
Objects scanned:	56
Errors:	0

Virus statistics

Infected:	1
Healed:	0
Moved to Virus Vault:	0
Deleted:	0

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...***

11.4. 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.

11.5. 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:

- MS Outlook 97/98/2000/2003 (part of the Microsoft Office installation)
- MS Exchange client 4.0, and higher
- The BAT! 1.61, and higher
- 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:

- MS Outlook Express 4.0, and higher
- Netscape mail
- Incredimail
- 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.

11.6. 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 */

12. 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.

12.1. Update Levels

AVG offers three update levels to select from:

- ***Priority update***

  Priority update contains changes necessary for reliable anti-virus and anti-malware protection. Typically, it does not include any changes to the code and updates only the definition database. This update should be applied as soon as it is available.

- ***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.

12.2. 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***

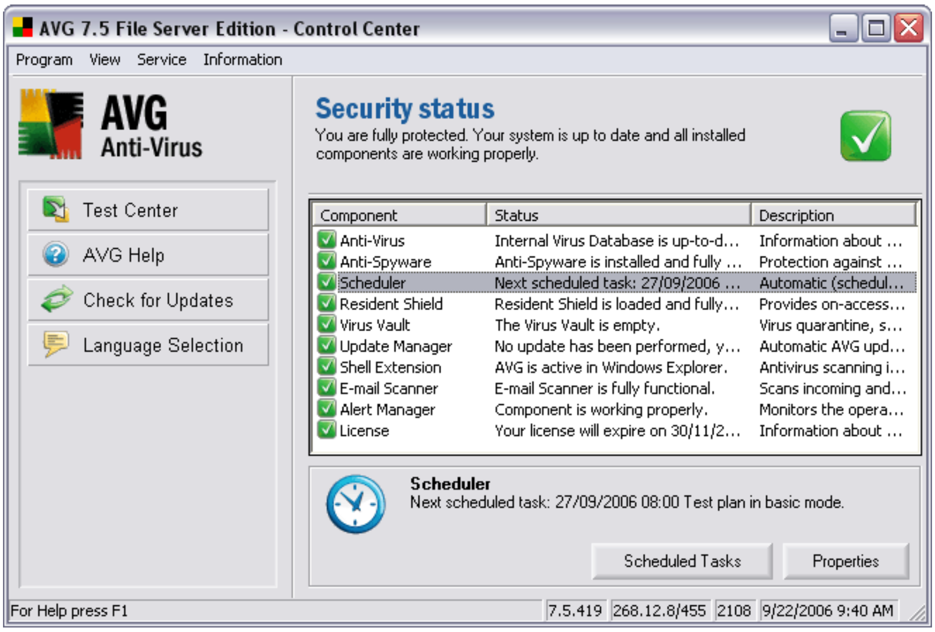
  Within AVG it is also possible to pre-set an update plan. The planned update is then performed periodically according to the setup configuration. Whenever new update files are present on the specified location, they are downloaded either directly from the Internet, or from the network directory. When no newer updates are available, nothing happens.

12.3. 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 File Server Edition - Control Center
Program View Service Information
AVG Anti-Virus
Test Center
AVG Help
Check for Updates
Language Selection

Security status

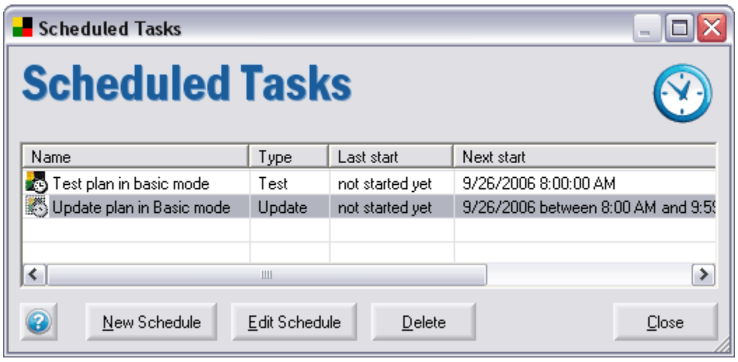
You are fully protected. Your system is up to date and all installed components are working properly.

Component	Status	Description
✓ Anti-Virus	Internal Virus Database is up-to-d...	Information about ...
✓ Anti-Spyware	Anti-Spyware is installed and fully ...	Protection against ...
✓ Scheduler	Next scheduled task: 27/09/2006 ...	Automatic (schedul...
✓ Resident Shield	Resident Shield is loaded and fully...	Provides on-access...
✓ Virus Vault	The Virus Vault is empty.	Virus quarantine, s...
✓ Update Manager	No update has been performed, y...	Automatic AVG upd...
✓ Shell Extension	AVG is active in Windows Explorer.	Antivirus scanning i...
✓ E-mail Scanner	E-mail Scanner is fully functional.	Scans incoming and...
✓ Alert Manager	Component is working properly.	Monitors the opera...
✓ License	Your license will expire on 30/11/2...	Information about ...

Scheduler

Next scheduled task: 27/09/2006 08:00 Test plan in basic mode.

The button opens a new ***Scheduled Tasks*** dialog window with an overview of the currently configured tasks:



Name	Type	Last start	Next start
Test plan in basic mode	Test	not started yet	9/26/2006 8:00:00 AM
Update plan in Basic mode	Update	not started yet	9/26/2006 between 8:00 AM and 9:5

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***

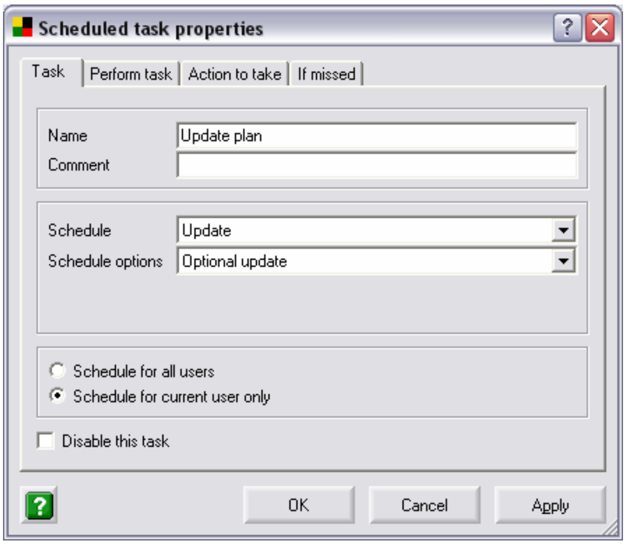
  For a detailed description of specific update types please refer to chapter 12.1 Update Levels.

  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 11. Test Review.

- ***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

Name: Update plan
Comment:

Schedule: Update
Schedule options: Optional update

○ Schedule for all users
● Schedule for current user only

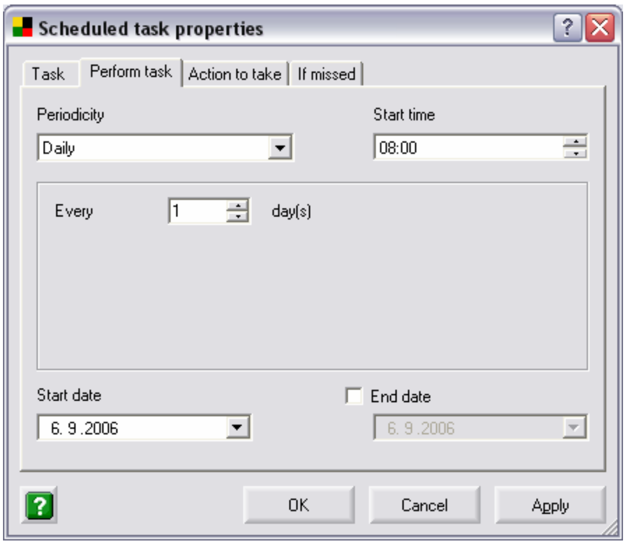
□ Disable this task

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 properties

Task | Perform task | Action to take | If missed

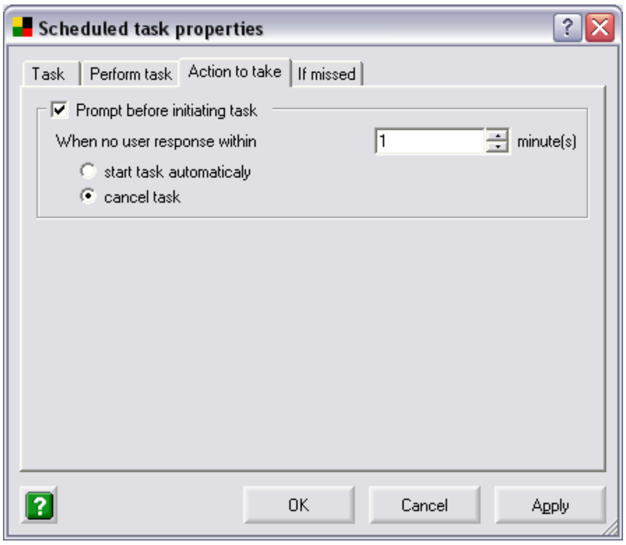
Periodicity: Daily
Start time: 08:00

Every 1 day(s)

Start date: 6. 9 .2006
□ End date: 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 properties

Task | Perform task | Action to take | If missed

☑ Prompt before initiating task

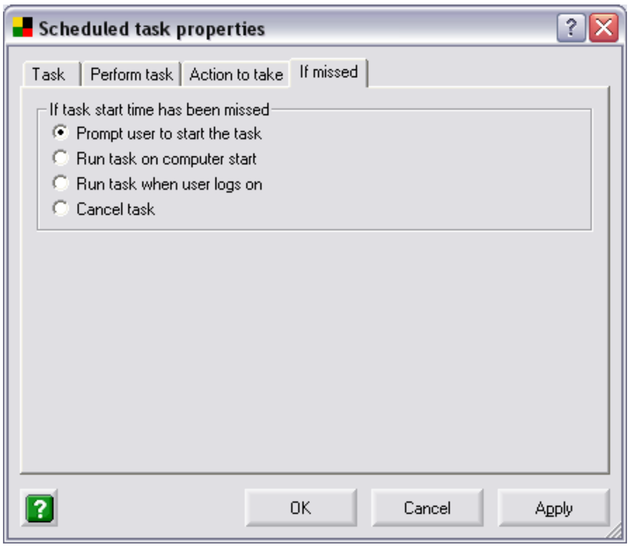
When no user response within 1 minute(s)

○ start task automaticaly

● cancel task

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

13. Terminal Services Server Mode

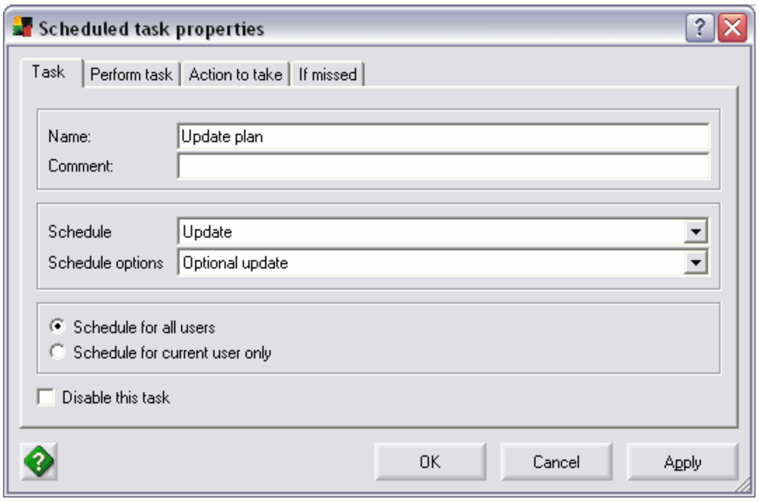
13.1. Installation Remarks

If you plan to use the server in a terminal services mode (either using the Microsoft Windows Terminal Services, Citrix WinFrames, or another similar product), to minimize system resource usage it is recommended that **AVG Control Center** is not run automatically for each user. In such cases, the installation should be run from the command line (using the ***setup.exe*** or ***avgsetup.exe*** command from the **AVG Anti-Virus** installation directory) with a command-line parameter ***/NO_CC_STARTUP*** or you can define this option within the setup process...

However, we recommend that you add the **AVG Control Center** component to the startup folder exclusively for the Administrator's account (profile), preferably with the ***/STARTUP*** parameter. This way the administrator will still be able to configure **AVG Anti-Virus**. **AVG Control Center** is then displayed as a minimized system tray icon.

13.2. Scheduled Tasks

For **AVG 7.5 File Server** installations on a terminal server it is highly recommended to set up all essential scheduled tests and updates for all users (***Scheduled task properties*** configuration window/**Task** tab/***Schedule for all users*** option:


Scheduled task properties

Name: Update plan
Comment:
Schedule: Update
Schedule options: Optional update
● Schedule for all users
○ Schedule for current user only
□ Disable this task

This ensures the plans are launched even if nobody is logged in. This way you also guarantee that no plan will run simultaneously in multiple instances (e.g. when a user has opened more concurrent sessions), which minimizes **AVG** resource usage.

It is recommended to restrict the **AVG Control Center** automatic launch for each user. Instead, **AVG Control Center** should be launched at startup only for the Administrator's account to manage all the essential tasks centrally, saving the system resources as much as possible.

You should launch scheduled updates ***for all users***, not for ***each user*** separately This will reduce the system resource usage and also ensure the essential scheduled updates will be performed even if nobody is logged in.

14. Alert Manager

14.1. Events and Actions

Anytime the **Resident Shield** has detected a virus, when a scheduled test has ended, when an update has been finished, and on many other occasions, an **event** is shown by **AVG**. The event is processed by the **Alert Manager** component that executes an **action** according to defined **rules**. An event message can be displayed to the user, or the information can be sent to the **DataCenter**.

All **AVG** installations implement this event management system. All users can **change the default rules** and **define new rules** as well. In addition to that, if **Remote Administration** is also installed, **DataCenter** tab will become visible. In this tab, specialized messages can be configured for sending to **DataCenter**. Users with workstations running Windows NT or later will additionally have **NT Event** tab available, where they can choose to record events to system log.

They can also use additional types of action that are not included in the default settings. It is possible to write event messages into the operating system Event Log, to send a special message to the **DataCenter**, and even to write an e-mail message to the specified address. All standard actions can be also edited. A typical example is the **automatic action** option in the dialog with information on the finding of a virus by **Resident Shield** - moving the infected file into **Virus Vault**, etc.

14.2. AVG Alert Manager Rules

The rules define relations between an action and the corresponding event. Every rule defines:

- An event to which it responds.
- The source component of the event; some of the events can be reported by more than one component, a rule can include restrictions to the selected ones.
- An action to be executed; within each rule more actions can be specified (e.g. Event Log recording, and sending a message to the **DataCenter** simultaneously).

After **AVG** installation there are a few default rules defined without the possibility of editing the event and source component definition. But you can edit actions as needed. In case of a new user defined rules, it is possible to change both the event and source component definitions, as well as the actions.

Besides these default rules there are some internal system rules which are hidden from the user.

The default settings of the rules are as follows:

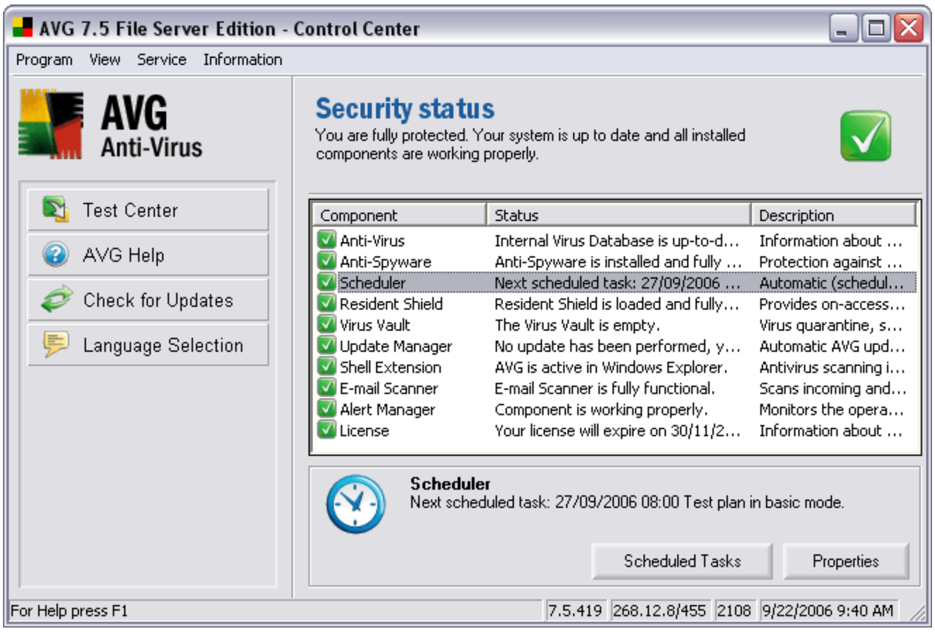
Event	**Shown**	**Action**
Virus detection by Resident Shield	When Resident Shield detects a virus	Opens a virus detected message dialog, the user must choose an action. It is possible to configure automatic behavior of the dialog (infected file movement into Virus Vault and so on)
Resident Shield dialog action	In the moment a user selects an action in the Resident Shield dialog (see the previous rule)	Sending detection information and action selected to AVG DataCenter. It is possible to define, for example, a record to be written into Event Log

	or when the action is executed automatically	
Finished test notification	After a scheduled or manually launched test has been finished	Sending information on the test results to the AVG DataCenter

14.3. Rules Configuration

a) AVG Client Rules Configuration

Within the client part of **AVG**, the event management configuration window is accessed from the **Control Center / Alert Manager** component:



AVG 7.5 File Server Edition - Control Center
Program View Service Information
AVG Anti-Virus
Test Center
AVG Help
Check for Updates
Language Selection

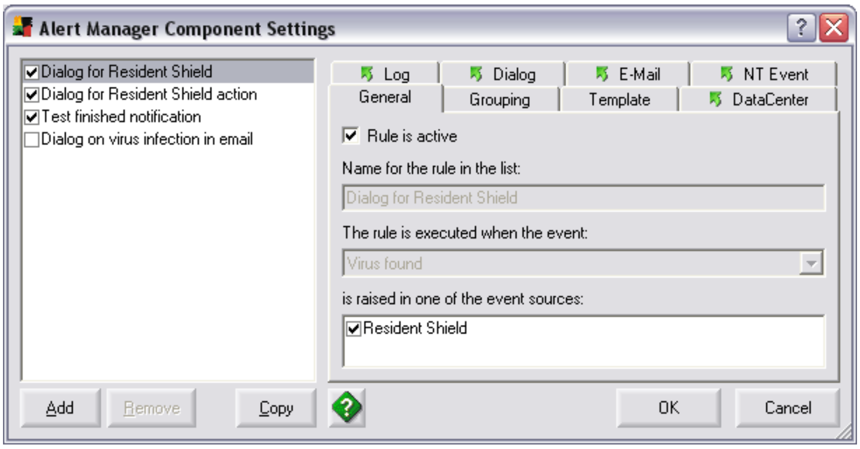
Security status

You are fully protected. Your system is up to date and all installed components are working properly.

Component	Status	Description
☑ Anti-Virus	Internal Virus Database is up-to-d...	Information about ...
☑ Anti-Spyware	Anti-Spyware is installed and fully ...	Protection against ...
☑ Scheduler	Next scheduled task: 27/09/2006 ...	Automatic (schedul...
☑ Resident Shield	Resident Shield is loaded and fully...	Provides on-access...
☑ Virus Vault	The Virus Vault is empty.	Virus quarantine, s...
☑ Update Manager	No update has been performed, y...	Automatic AVG upd...
☑ Shell Extension	AVG is active in Windows Explorer.	Antivirus scanning i...
☑ E-mail Scanner	E-mail Scanner is fully functional.	Scans incoming and...
☑ Alert Manager	Component is working properly.	Monitors the opera...
☑ License	Your license will expire on 30/11/2...	Information about ...

Scheduler
Next scheduled task: 27/09/2006 08:00 Test plan in basic mode.

Press the ***Settings*** button to open the ***Alert Manager Component Settings*** dialog:



☑ Dialog for Resident Shield
☑ Dialog for Resident Shield action
☑ Test finished notification
☐ Dialog on virus infection in email

☑ Rule is active

Name for the rule in the list: Dialog for Resident Shield

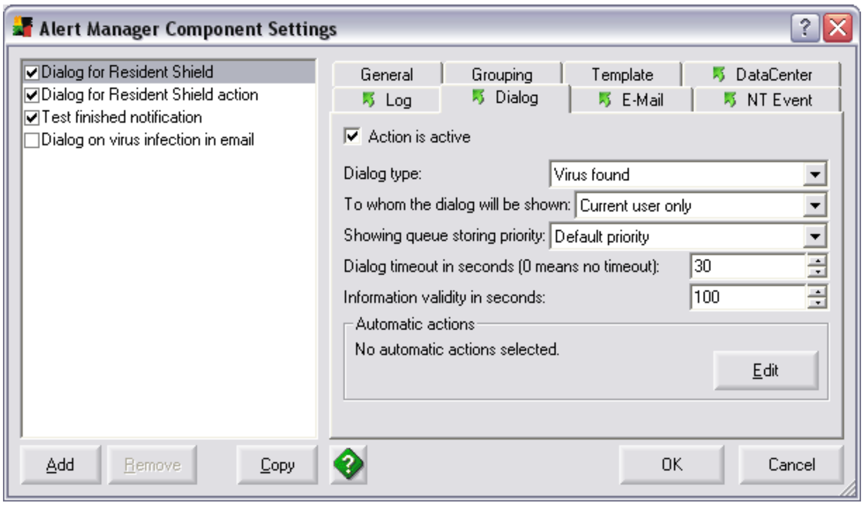
The rule is executed when the event: Virus found

is raised in one of the event sources: ☑ Resident Shield

On the left side of the window, there is a list of rules with active rules being marked. On the right side you can manage the selected rule settings. Default rules with automatic settings cannot be changed (neither the rule nor the respective action).

On the *General*, *Grouping* and *Template* tab you can define properties for the chosen rule (the rule name, event to which the rule relates etc.). In the tabs marked with green arrow you can define actions that you wish to assign to the rule. For each rule it is possible to define more actions.

The next screenshot shows an example of ***Display dialog to user*** action definition for the ***Dialog for Resident Shield*** rule. This rule is launched if the **Resident Shield** detects a virus.



Alert Manager Component Settings

☑ Dialog for Resident Shield
☑ Dialog for Resident Shield action
☑ Test finished notification
□ Dialog on virus infection in email

☑ Action is active

Dialog type: Virus found
To whom the dialog will be shown: Current user only
Showing queue storing priority: Default priority
Dialog timeout in seconds (0 means no timeout): 30
Information validity in seconds: 100

Automatic actions
No automatic actions selected.

In the menu **Dialog Type** choose, which dialog you wish to be displayed:

- ***Message Box*** – general text dialog displaying information about the event according to the template defined on the *Template* tab.
- ***Virus found*** – standard dialog for reporting viruses found by AVG Resident Shield.

In the menu **To whom the dialog will be shown** you can choose, if the dialog will be shown only to the user by whom the event occurred (***Current user only***) or to all the logged users (***All users***).

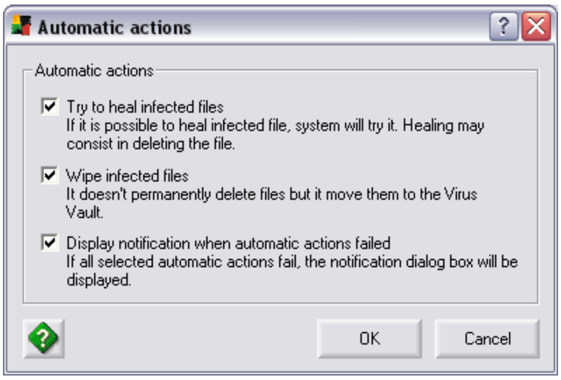
In the menu **Showing queue storing priority** you can define priority (low, default, high).

The item **Dialog timeout in seconds** determines, if the dialog will close itself (you can set the expiration period), or if closing of the dialog must be confirmed by the user (this option can be set by entering “0” in the appropriate field).

In the field next to **Information validity in seconds** you can enter a value, for how long will be the displayed information/dialog valid. In other words, the exact elapsed time needed before AVG will “drop” the information and stop dealing with it. This value can be set for a period longer than the default is. For example in case of a massive virus infection, the default period could expire before the user will have a chance to select an action for the previously displayed. In such case user would not be warned about every possible threat just because of the short expiration period.

Mind the ***Edit*** button within the screenshot. Using this button you can define automatic actions to be taken. As an example, all of the available actions are selected on the next screenshot:

- ***Try to heal infected files*** – **AVG** will try to heal and recover the infected files
- ***Wipe infected files*** – **AVG** will delete the infected files
- ***Display notification when automatic actions failed*** – a notification message will be displayed to the user if the automatic action failed


Automatic actions

Automatic actions

☑ Try to heal infected files
If it is possible to heal infected file, system will try it. Healing may consist in deleting the file.

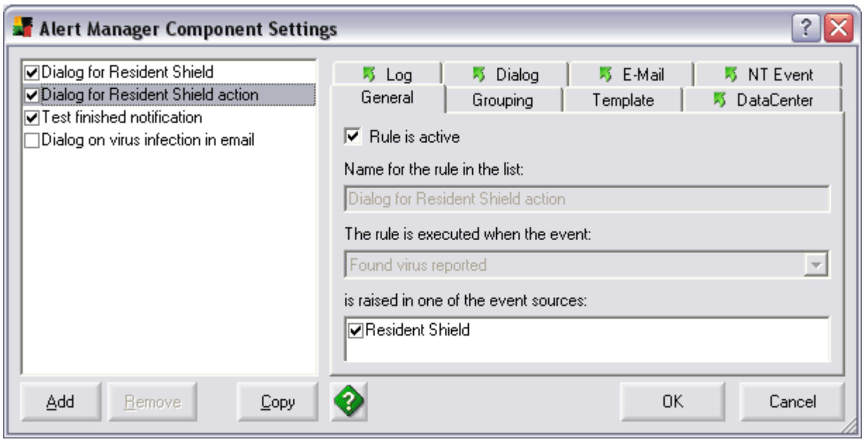
☑ Wipe infected files
It doesn't permanently delete files but it move them to the Virus Vault.

☑ Display notification when automatic actions failed
If all selected automatic actions fail, the notification dialog box will be displayed.

Based on the defined actions, **AVG** first tries to heal the infected file. If the healing is not successful, **AVG** tries to delete the file: of course, if the infected file is about to be deleted, it is always moved to the **Virus Vault** first. Then in case even deletion has failed, **AVG** eventually displays the appropriate notification to the user.

If you enable automatic actions, no notification window will be displayed. You can only get optional notification about automatic actions failure by ticking the **Display notification when automatic actions failed**.

After any of the automatic actions mentioned above have been performed, a ***Found virus reported*** event is generated. This event is passed to another default rule – ***Dialog for Resident Shield action***:


Alert Manager Component Settings

☑ Dialog for Resident Shield
☑ Dialog for Resident Shield action
☑ Test finished notification
□ Dialog on virus infection in email

☑ Rule is active

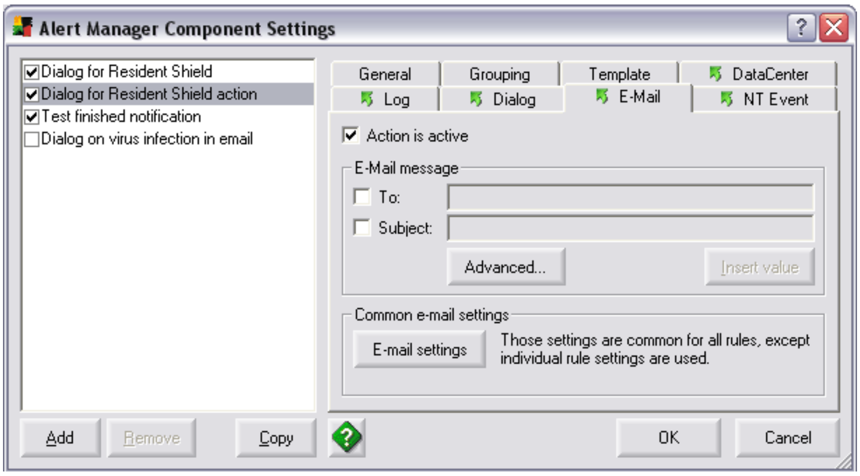
Name for the rule in the list: Dialog for Resident Shield action

The rule is executed when the event: Found virus reported

is raised in one of the event sources:
☑ Resident Shield

The ***Dialog for Resident Shield action*** rule has the default configuration set up to take the ***Send Message to AVG DataCenter*** action.

For some exceptional situations it may be appropriate to send an e-mail message as well – you can specify this option on the ***E-mail*** tab:



☑ Dialog for Resident Shield
☑ Dialog for Resident Shield action
☑ Test finished notification
☐ Dialog on virus infection in email

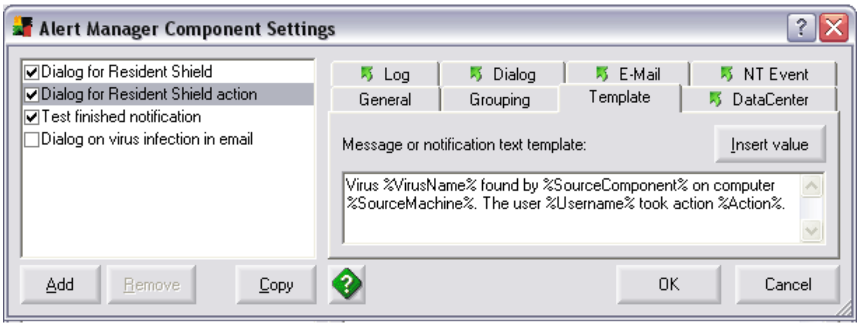
☑ Action is active

☐ To:
☐ Subject:

Those settings are common for all rules, except individual rule settings are used.

The ***E-mail Settings*** button open a new dialog where you can edit the common e-mail settings shared by all other rules (sender's name, address of mail server, etc.).

Text to be used after an action has been triggered (e.g. the e-mail body text) is predefined on the ***Template*** tab. The message text can be supplemented by special values related to the event properties. Those values are typed inside ***%*** characters for further internal processing. To add a new value, press the ***Insert value*** button:



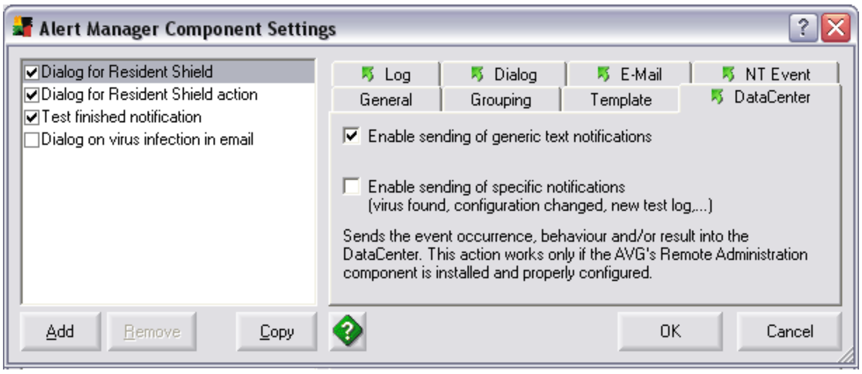
☑ Dialog for Resident Shield
☑ Dialog for Resident Shield action
☑ Test finished notification
☐ Dialog on virus infection in email

Message or notification text template:

Virus %VirusName% found by %SourceComponent% on computer %SourceMachine%. The user %Username% took action %Action%.

Default rules specify sending messages on selected important issues to the **DataCenter**. These messages project to their respective overviews. For example, a test result report is further processed according to the conditions specified in the **DataCenter** mode (enable/disable negative test results passing). Besides that you can send a general event message to the **DataCenter**. These messages are recorded in the event overview.

Only generic text message sending is enabled on the screenshot below:



Alert Manager Component Settings

☑ Dialog for Resident Shield
☑ Dialog for Resident Shield action
☑ Test finished notification
□ Dialog on virus infection in email

☑ Enable sending of generic text notifications

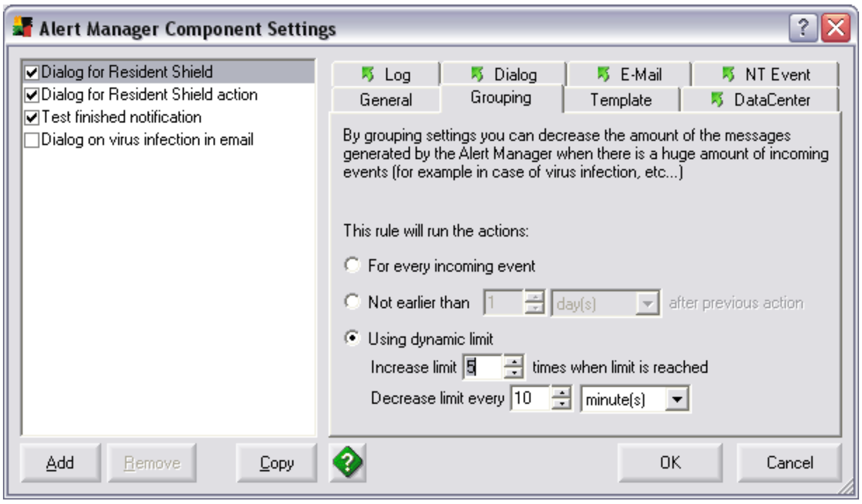
□ Enable sending of specific notifications
(virus found, configuration changed, new test log,...)

Sends the event occurrence, behaviour and/or result into the DataCenter. This action works only if the AVG's Remote Administration component is installed and properly configured.

Attention! *For proper AVG Remote Administration functioning it is recommended to keep the* ***Enable sending of specific notifications*** *option specified for the default rules! You are encouraged to disable this action only if you have an actual reason to do so! For sending a generic text notification we recommend creating a new rule!*

b) Events Grouping

In case of a huge virus epidemic, the e-mail messaging frequency can be very high. If the ***E-mail message sending*** action had been activated for a virus found event, the addressee mailbox and mail server may be overloaded very quickly. To prevent an excessive number of shown events you can define event grouping conditions for each rule.



Alert Manager Component Settings

☑ Dialog for Resident Shield
☑ Dialog for Resident Shield action
☑ Test finished notification
□ Dialog on virus infection in email

By grouping settings you can decrease the amount of the messages generated by the Alert Manager when there is a huge amount of incoming events (for example in case of virus infection, etc...)

This rule will run the actions:

○ For every incoming event

○ Not earlier than 1 day(s) after previous action

● Using dynamic limit

Increase limit 5 times when limit is reached

Decrease limit every 10 minute(s)

- ***For every incoming event*** - By default, an action is triggered for each event occurrence.
- ***Not earlier than ... after previous action*** - It is possible to delay the next action launch by setting a minimum time interval for which the same event is ignored. All the events shown in this interval will then be joined into a group. The next action (e. g. the next e-mail message) will cover an overview of all the grouped events.
- ***Using dynamic limit*** - In this mode, any triggered action will increase the limit of grouped events n-times. The first virus detection will trigger an action. The same following event will execute no action, it will be grouped instead. On the screenshot above the limit is set to 5, so the next action will be triggered after five successive virus detections. In

case of a sixth detection, the limit would be increased 5-times again. After the specified period of time the limit will decrease automatically.

This feature allows flexible adaptation to the current situation. It helps to ensure that the administrator is warned immediately in case of a single event; on the other hand it minimizes the chance of network overload in case of an epidemic.

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 www.grisoft.com.

If you do not succeed in finding help this way, contact the technical support department at technicalsupport@grisoft.com. Be sure to include your AVG License number in the body of the e-mail.

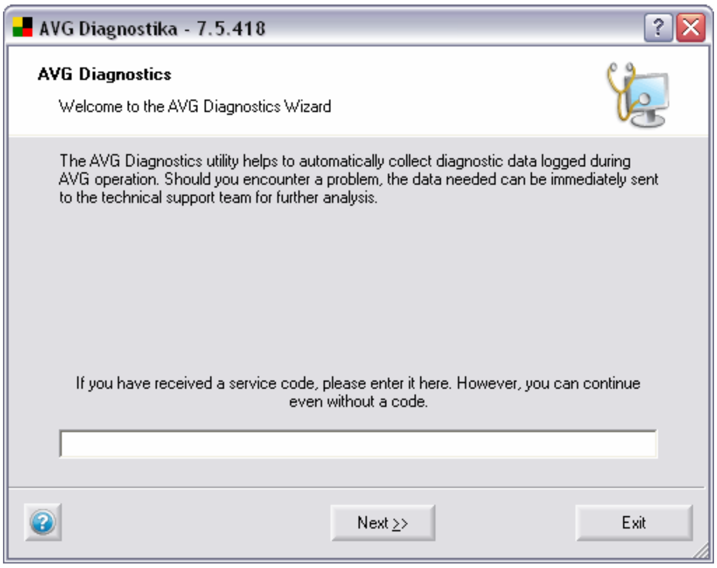
However, we recommended contacting the Grisoft technical support from the dialog window accessible from all AVG applications (e.g. **Test Center**, **Control Center** ...). To open this dialog, select ***Technical support by e-mail*** option from the ***Information*** folder of the application main menu. Then proceed to chapter 15.1 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

The AVG Diagnostics utility helps to automatically collect diagnostic data logged during AVG operation. Should you encounter a problem, the data needed can be immediately sent to the technical support team for further analysis.

If you have received a service code, please enter it here. However, you can continue even without a code.

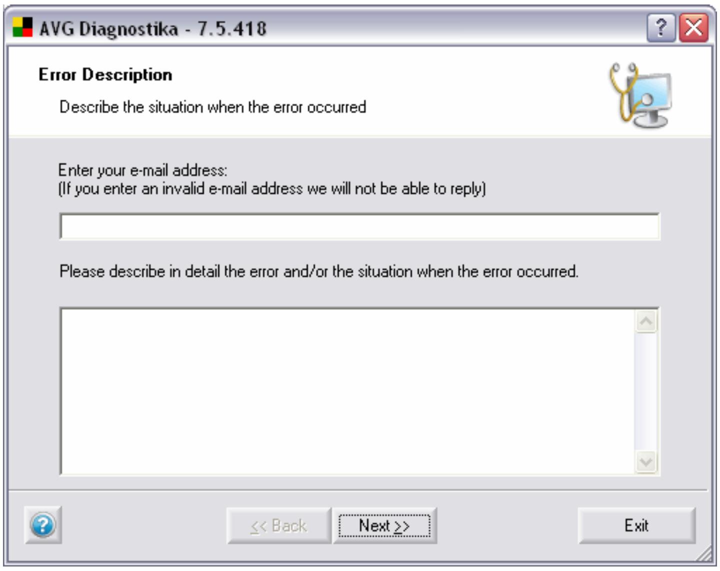
If you have received a service code, please type it into the text field, or use the copy/paste method. The code will automatically set up the correct AVG diagnostics mode which ensures that only the required (and no redundant) data is collected during the **AVG Diagnostics** session.

If you do not have a service code, you can choose any of the following options:

- Contact AVG Technical Support 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 b - Error description.
- If you are well experienced computer user you can shut down **AVG Diagnostics** and follow instructions in step d) 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

Enter your e-mail address:
(If you enter an invalid e-mail address we will not be able to reply)

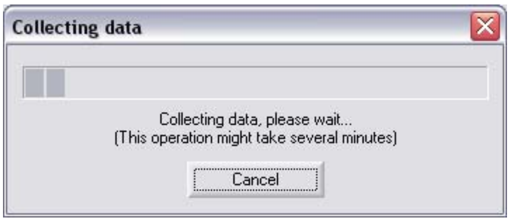
Please describe in detail the error and/or the situation when the error occurred.

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.

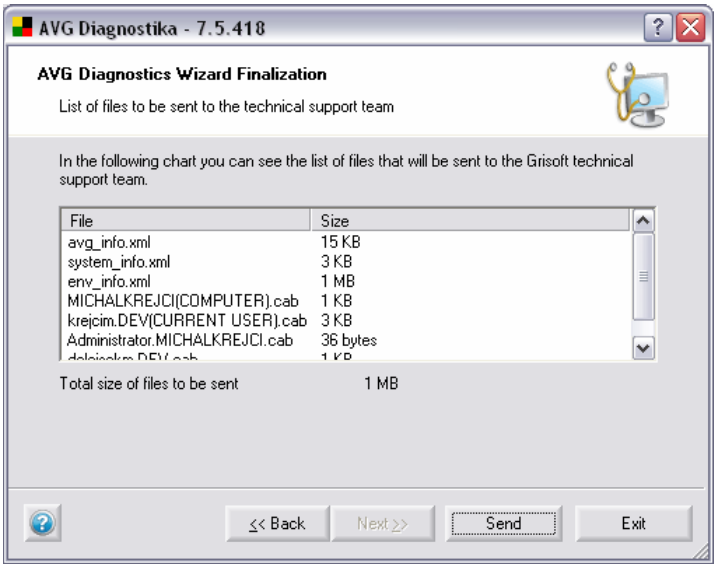


Collecting data

Collecting data, please wait...
(This operation might take several minutes)

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

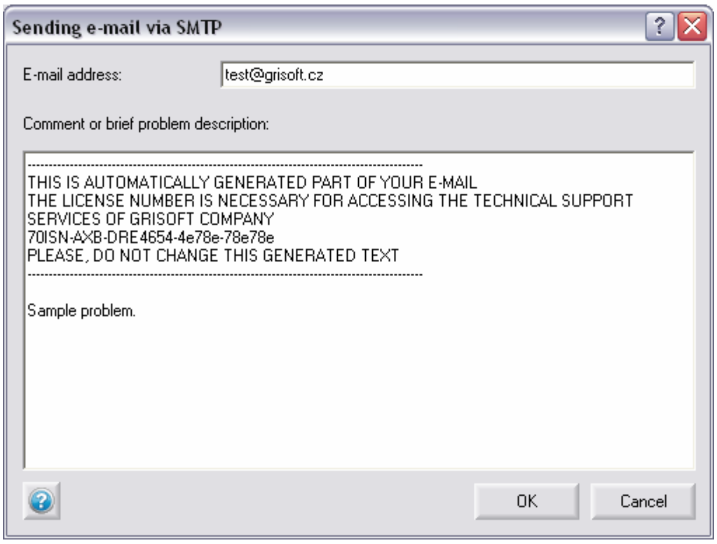
In the following chart you can see the list of files that will be sent to the Grisoft technical support team.

File	Size
avg_info.xml	15 KB
system_info.xml	3 KB
env_info.xml	1 MB
MICHALKREJCI(COMPUTER).cab	1 KB
krejcim.DEV(CURRENT USER).cab	3 KB
Administrator.MICHALKREJCI.cab	36 bytes

Total size of files to be sent 1 MB

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 SMTP

E-mail address: test@grisoft.cz

Comment or brief problem description:

```
------------------------------------------------------------------------
THIS IS AUTOMATICALLY GENERATED PART OF YOUR E-MAIL
THE LICENSE NUMBER IS NECESSARY FOR ACCESSING THE TECHNICAL SUPPORT
SERVICES OF GRISOFT COMPANY
70ISN-AXB-DRE4654-4e78e-78e78e
PLEASE, DO NOT CHANGE THIS GENERATED TEXT
------------------------------------------------------------------------

Sample problem.
```

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 e) AVG Diagnostics - Complete Parameter Overview.

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***

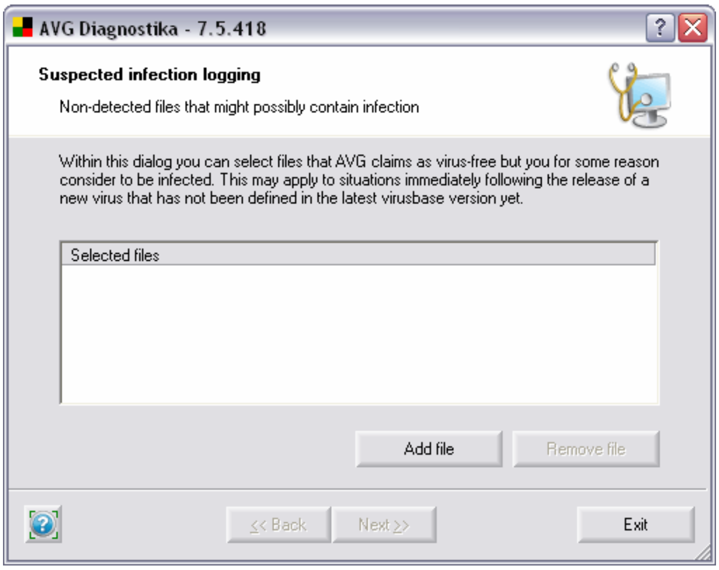
  This ***AVG Diagnostics Mode*** allows you to send a suspect file (or more files) for analysis to the Grisoft technical support team.

  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 logging

Non-detected files that might possibly contain infection

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.

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.

o ***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.

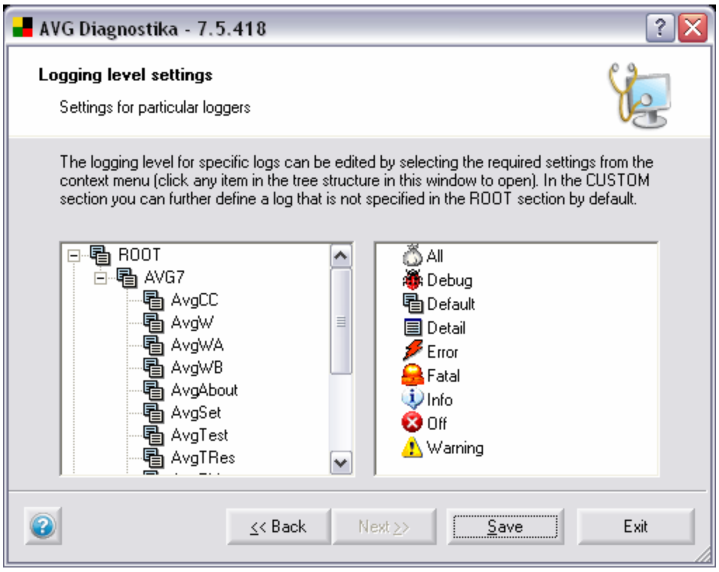
Parameter: /MODE=FEEDBACK

o ***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 - 7.5.418

Logging level settings

Settings for particular loggers

The logging level for specific logs can be edited by selecting the required settings from the context menu (click any item in the tree structure in this window to open). In the CUSTOM section you can further define a log that is not specified in the ROOT section by default.

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.

o ***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>	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 *false alarm* 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>	Automatically sets up the Log Level Setting mode and allows you to directly select logging level.
/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.

<table>
<tr>
<td><em>/LNG=&lt;lng&gt;</em></td>
<td>Allows you to switch the AVG Diagnostics interface to another language.

Available languages and their codes:
<table>
<tr><td>CZ=0x0405</td><td>GE=0x0407</td><td>PB=0x0416</td></tr>
<tr><td>SK=0x041b</td><td>FR=0x040c</td><td>PL=0x0415</td></tr>
<tr><td>US=0x0409</td><td>SP=0x040a</td><td>SC=0x081a</td></tr>
<tr><td>IT=0x0410</td><td>HU=0x040e</td><td>NL=0x0413</td></tr>
</table>
</td>
</tr>
</table>