# AVG 9.0 File Server

## User Manual

**Document revision 90.2 (23.10.2009)**

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

This product uses RSA Data Security, Inc. MD5 Message-Digest Algorithm, Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991.
This product uses code from C-SaCzech library, Copyright (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).
This product uses compression library zlib, Copyright (c) 1995-2002 Jean-loup Gailly and Mark Adler.
This product uses compression library libbzip2, Copyright (c) 1996-2002 Julian R. Seward.

# Contents


**1. Introduction ..... 6**

**2. Installation Requirements ..... 7**

2.1 Operation Systems Supported ..... 7
2.2 Hardware Requirements ..... 7

**3. AVG Installation Options ..... 8**

**4. AVG Download Manager ..... 9**

4.1 Language Selection ..... 9
4.2 Connectivity Check ..... 10
4.3 Proxy Settings ..... 11
4.4 Select License Type ..... 12
4.5 Download Files to Install ..... 13

**5. AVG Installation Process ..... 14**

5.1 Installation Launch ..... 14
5.2 License Agreement ..... 15
5.3 Checking System Status ..... 16
5.4 Select Installation Type ..... 17
5.5 Activate your AVG License ..... 17
5.6 Custom Installation - Destination Folder ..... 19
5.7 Custom Installation - Component Selection ..... 20
5.8 Installing AVG ..... 21
5.9 Schedule regular scans and updates ..... 22
5.10 AVG protection configuration is complete ..... 22

**6. After Installation ..... 24**

6.1 Product Registration ..... 24
6.2 Access to User Interface ..... 24
6.3 Scanning of the whole computer ..... 24
6.4 Eicar Test ..... 24
6.5 AVG Default Configuration ..... 25

**7. AVG User Interface ..... 26**

7.1 System Menu ..... 27
*7.1.1 File ..... 27*


AVG 9.0 File Server © 2009 Copyright AVG Technologies CZ, s.r.o. All rights reserved. 

*7.1.2 Components* ..... *27*
*7.1.3 History* ..... *27*
*7.1.4 Tools* ..... *27*
*7.1.5 Help* ..... *27*
7.2 Security Status Info ..... 29
7.3 Quick Links ..... 30
7.4 Components Overview ..... 31
7.5 Statistics ..... 32
7.6 System Tray Icon ..... 33

**8. AVG Components ..... 34**

8.1 Anti-Virus ..... 34
*8.1.1 Anti-Virus Principles* ..... *34*
*8.1.2 Anti-Virus Interface* ..... *34*
8.2 Anti-Spyware ..... 36
*8.2.1 Anti-Spyware Principles* ..... *36*
*8.2.2 Anti-Spyware Interface* ..... *36*
8.3 License ..... 38
8.4 Resident Shield ..... 39
*8.4.1 Resident Shield Principles* ..... *39*
*8.4.2 Resident Shield Interface* ..... *39*
*8.4.3 Resident Shield Detection* ..... *39*
8.5 Update Manager ..... 44
*8.5.1 Update Manager Principles* ..... *44*
*8.5.2 Update Manager Interface* ..... *44*

**9. AVG for SharePoint Portal Server ..... 47**

9.1 Program Maintenance ..... 47
9.2 AVG for SPPS Configuration - SharePoint 2007 ..... 48
9.3 AVG for SPPS Configuration - SharePoint 2003 ..... 50
9.4 AVG for SPPS Edition Diagnostics ..... 52

**10. AVG Advanced Settings ..... 54**

10.1 Appearance ..... 54
10.2 Sounds ..... 56
10.3 Ignore Faulty Conditions ..... 58
10.4 Virus Vault ..... 59
10.5 PUP Exceptions ..... 60
10.6 Scans ..... 62

*10.6.1 Scan Whole Computer* ..... *62*
*10.6.2 Shell Extension Scan* ..... *62*
*10.6.3 Scan Specific Files or Folders* ..... *62*
*10.6.4 Removable Device Scan* ..... *62*
10.7 Schedules ..... 69
*10.7.1 Scheduled Scan* ..... *69*
*10.7.2 Virus Database Update Schedule* ..... *69*
*10.7.3 Program Update Schedule* ..... *69*
10.8 Resident Shield ..... 79
*10.8.1 Advanced Settings* ..... *79*
*10.8.2 Directory Exludes* ..... *79*
*10.8.3 Excluded Files* ..... *79*
10.9 Update ..... 84
*10.9.1 Proxy* ..... *84*
*10.9.2 Dial-up* ..... *84*
*10.9.3 URL* ..... *84*
*10.9.4 Manage* ..... *84*

**11. AVG Scanning ..... 91**

11.1 Scanning Interface ..... 91
11.2 Predefined Scans ..... 92
*11.2.1 Scan Whole Computer* ..... *92*
*11.2.2 Scan Specific Files or Folders* ..... *92*
11.3 Scanning in Windows Explorer ..... 100
11.4 Command Line Scanning ..... 101
*11.4.1 CMD Scan Parameters* ..... *101*
11.5 Scan Scheduling ..... 103
*11.5.1 Schedule Settings* ..... *103*
*11.5.2 How to Scan* ..... *103*
*11.5.3 What to Scan* ..... *103*
11.6 Scan Results Overview ..... 113
11.7 Scan Results Details ..... 114
*11.7.1 Results Overview Tab* ..... *114*
*11.7.2 Infections Tab* ..... *114*
*11.7.3 Spyware Tab* ..... *114*
*11.7.4 Warnings Tab* ..... *114*
*11.7.5 Information Tab* ..... *114*
11.8 Virus Vault ..... 123

**12. AVG Updates ..... 125**

12.1 Update Levels ..... 125
12.2 Update Types ..... 125
12.3 Update Process ..... 125

**13. Event History ..... 127**

**14. FAQ and Technical Support ..... 129**

# 1. Introduction

This user manual provides comprehensive documentation for **AVG 9.0 File Server**.

**Congratulations on your purchase of AVG 9.0 File Server!**

**AVG 9.0 File Server** is one of a range of award winning AVG products designed to provide you with peace of mind and total security for your PC. As with all AVG products **AVG 9.0 File Server** has been completely re-designed, from the ground up, to deliver AVG's renowned and accredited security protection in a new, more user friendly and efficient way.

Your new **AVG 9.0 File Server** product has a streamlined interface combined with more aggressive and faster scanning. More security features have been automated for your convenience, and new 'intelligent' user options have been included so that you can fit our security features to your way of life. No more compromising usability over security!

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

AVG 9.0 File Server © 2009 Copyright AVG Technologies CZ, s.r.o. All rights reserved.

# 2. Installation Requirements

## 2.1. Operation Systems Supported

**AVG 9.0 File Server** is intended to protect workstations with the following operating systems:

- Windows 2000
- Windows XP and Windows XP Pro x64 Edition
- Windows Vista and Windows Vista x64 Edition
- Windows 2000 Server
- Windows 2003 Server and Windows 2003 Server x64 Edition
- Windows 2008 Server and Windows 2008 Server x64 Edition

(and possibly higher service packs for specific operating systems)

## 2.2. Hardware Requirements

Minimum hardware requirements for **AVG 9.0 File Server**:

- Intel Pentium CPU 1,5 GHz
- 470 MB of free hard drive space (for installation purposes)
- 512 MB of RAM memory

Recommended hardware requirements for **AVG 9.0 File Server**:

- Intel Pentium CPU 1,8 GHz
- 600 MB of free hard drive space (for installation purposes)
- 512 MB of RAM memory

AVG 9.0 File Server © 2009 Copyright AVG Technologies CZ, s.r.o. All rights reserved.

# 3. AVG Installation Options

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

**Before you start installing AVG, we strongly recommend that you visit AVG website (http://www.avg.com) to check for a new installation file. This way you can be sure to install the latest available version of AVG 9.0 File Server.**

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

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

# 4. AVG Download Manager

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

***Warning:*** *Please note that AVG Download Manager is not suitable for downloading of network and SBS editions and only the following operating systems are supported: Windows 2000 (SP4 + SRP roll-up), Windows XP (SP2 and higher), Windows Vista (all editions).*

**AVG Download Manager** is available for download at AVG website (http://www.avg.com). Following please find a brief description of each single step you need to take within the **AVG Download Manager**:

## 4.1. Language Selection

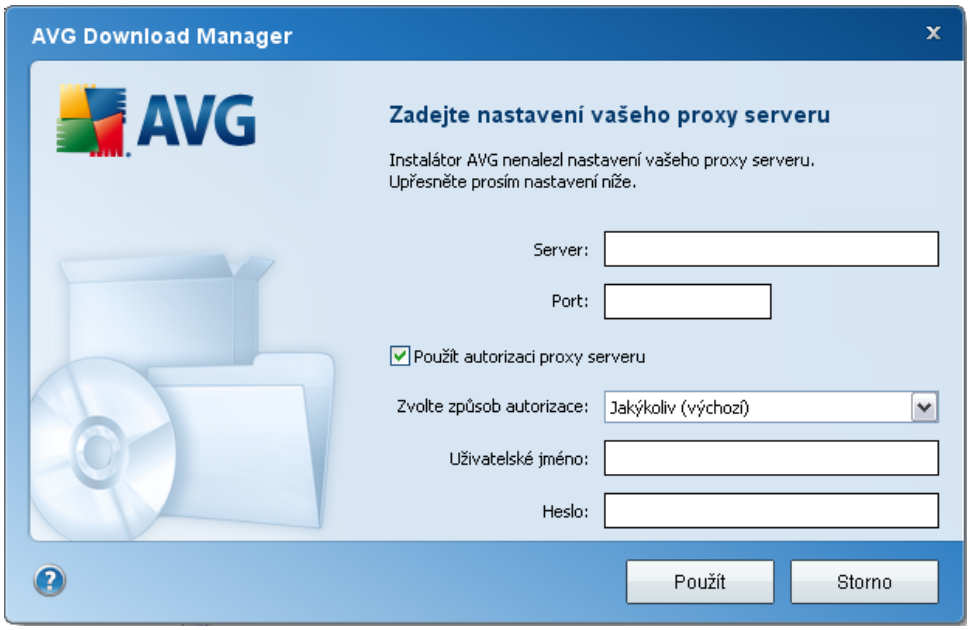
In this first step of **AVG Download Manager** select the installation language from the roll-down menu. Note, that your language selection applies only to the installation process; after the installation you will be able to change the language directly from program settings. Then press the ***Next***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

## 4.2. Connectivity Check

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

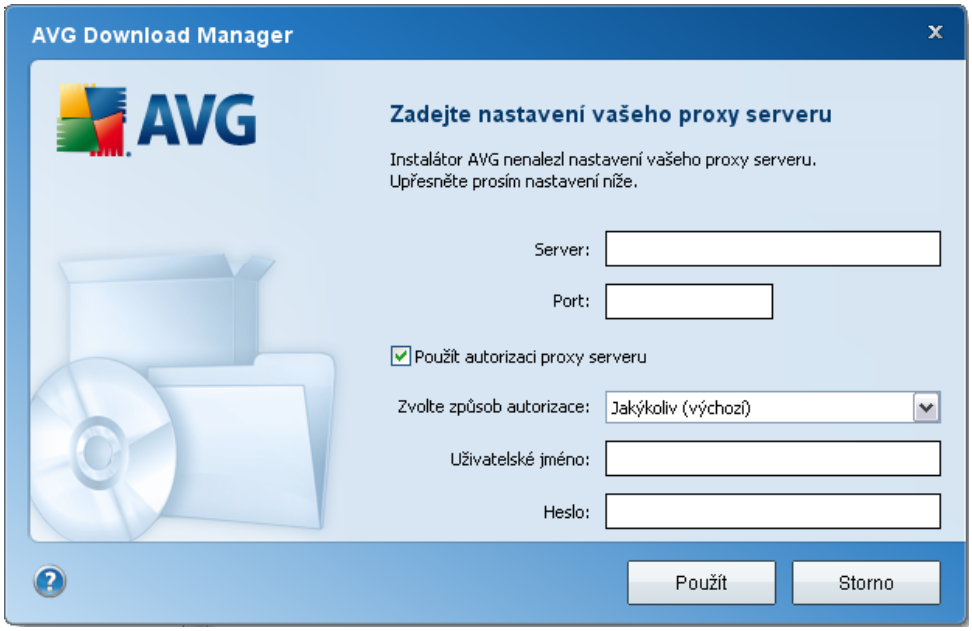
- If the test shows no connectivity, make sure you are really connected to Internet. Then click the ***Retry*** button

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




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

## 4.3. Proxy Settings



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

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

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

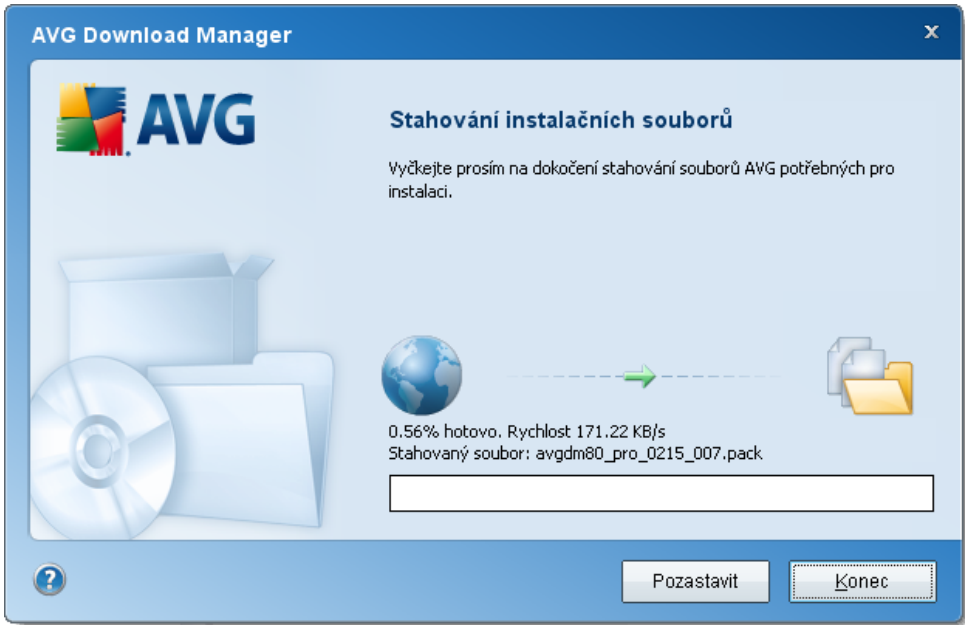
## 4.4. Select License Type

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

most:

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

## 4.5. Download Files to Install



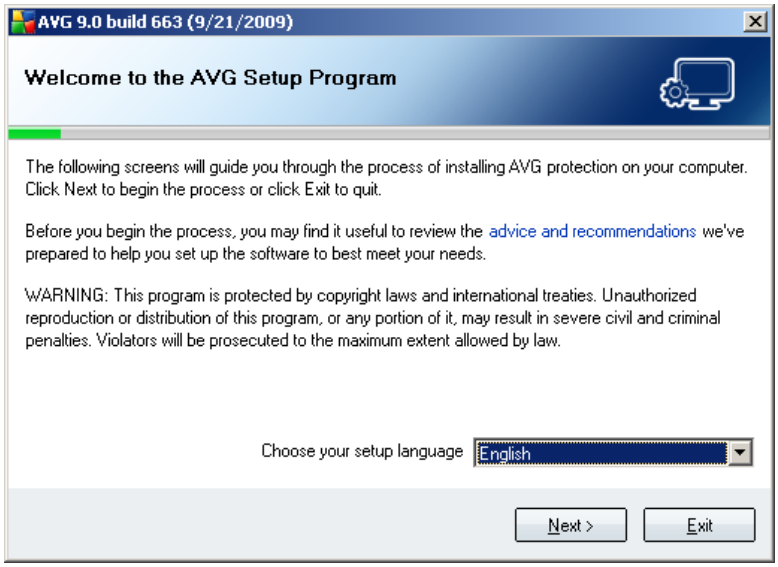

Now, you have provided all information needed for the **AVG Download Manager** to start the installation package download, and launch the installation process. Further, advance to the AVG Installation Process.

# 5. AVG Installation Process

To install **AVG 9.0 File Server** on your computer, you need to get the latest installation file. You can use the installation file from the CD that is a part of your box edition but this file might be out-of-date. Therefore we recommended getting the latest installation file online. You can download the file from AVG website (http://www.avg.com), ***Downloads*** section. Or, you can make use of our new ***AVG Download Manager*** tool that helps you create and download the installation package you need, and launch the installation process.

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

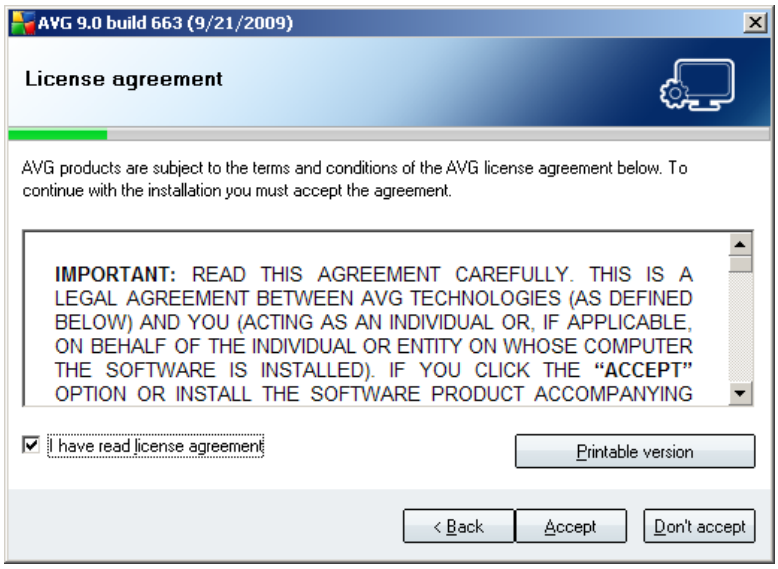
## 5.1. Installation Launch




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

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

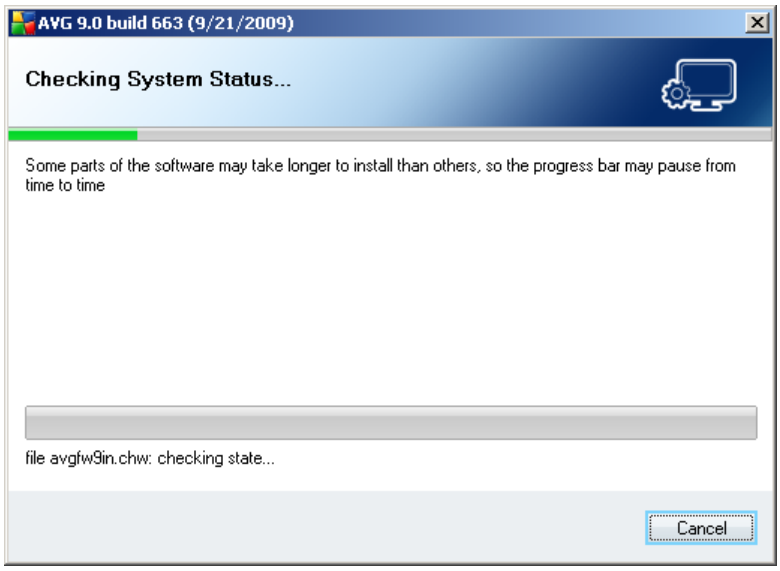
## 5.2. License Agreement




The ***License Agreement*** dialog provides the full wording of the AVG license agreement. Please read it carefully and confirm that you have read, understood and accept the agreement by marking the ***I have read license agreement*** check box and pressing the ***Accept*** button.

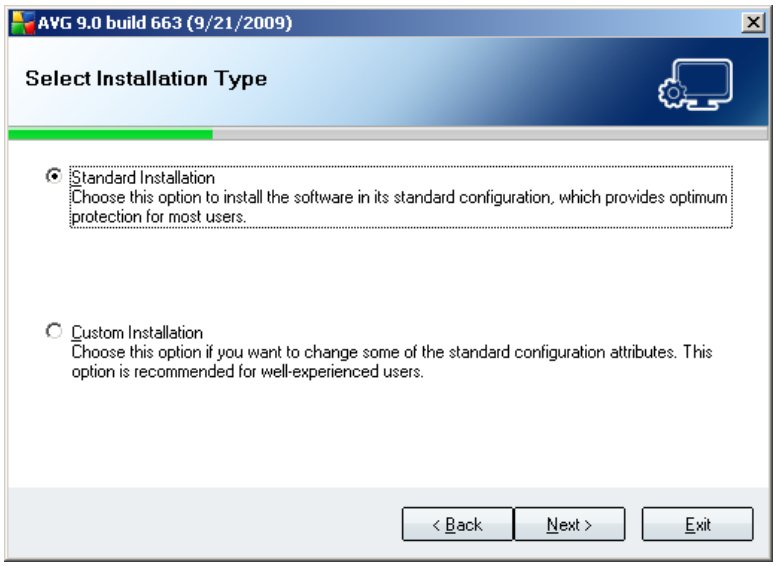
If you do not agree with the license agreement press the ***Don't accept*** button, and the installation process will be terminated immediately.

## 5.3. Checking System Status




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

## 5.4. Select Installation Type




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

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

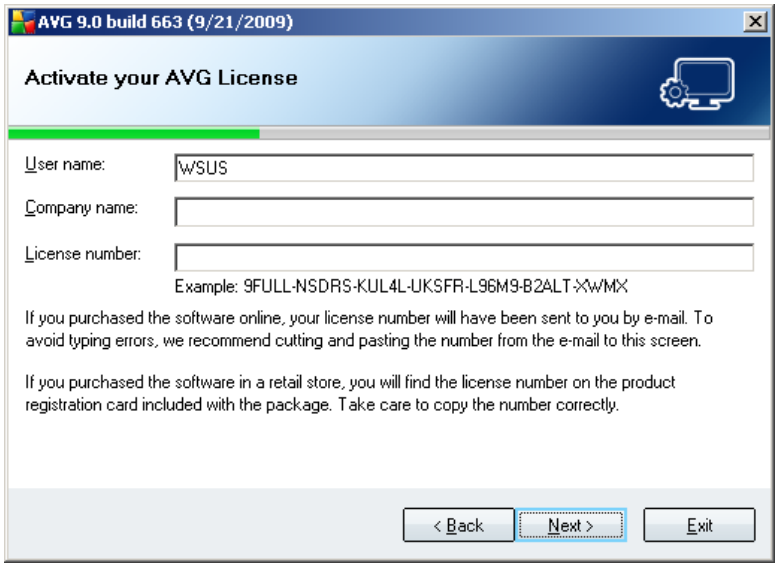
***Custom installation*** should only be used by experienced users who have a valid reason to install AVG with non-standard settings. E.g. to fit specific system requirements.

## 5.5. Activate your AVG License

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

Then enter your license/sales number into the ***License Number*** text field. The sales number can be found on the CD packaging in your **AVG 9.0 File Server** box. The license number will be in the confirmation email that you received after purchasing your **AVG 9.0 File Server** on-line. You must type in the number exactly as shown. If the digital form of the license number is available (*in the email*), it is recommended to

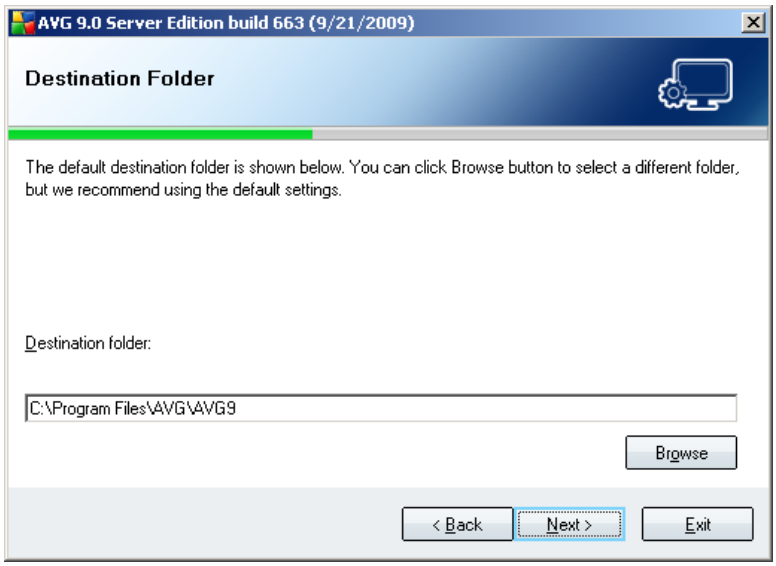
use the copy and paste method to insert it.




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

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

## 5.6. Custom Installation - Destination Folder

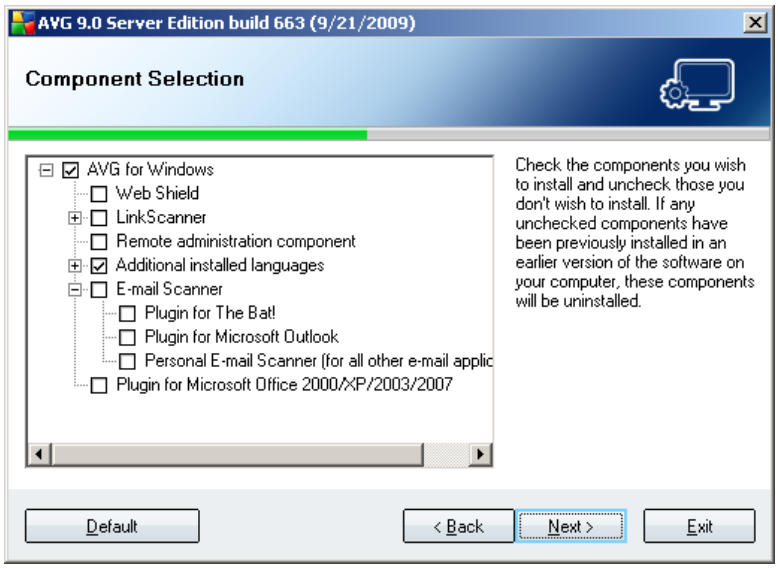



The ***Destination Folder*** dialog allows you to specify the location where **AVG 9.0 File Server** should be installed. By default, AVG will be installed to the program files folder located on drive C:. In case the folder does not exist yet, you will be asked in a new dialog to confirm you agree AVG creates this folder now.

If you want to change this location, use the ***Browse*** button to display the drive structure, and select the respective folder.

Press the ***Next*** button to confirm.

## 5.7. Custom Installation - Component Selection




The ***Component Selection*** dialog displays an overview of all **AVG 9.0 File Server** components that can be installed. If the default settings do not suit you, you can remove/add specific components.

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

- ***Language selection***

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

- ***E-mail Scanner plug-ins***

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

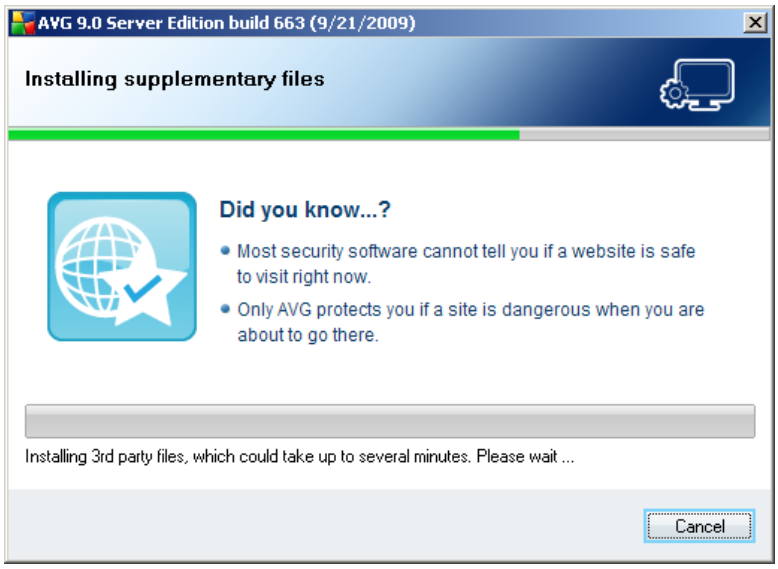
- ***Remote Administration***

If you plan to connect your computer to the AVG Remote Administration later, please mark the respective item to be installed as well.

Continue by pressing the ***Next*** button.

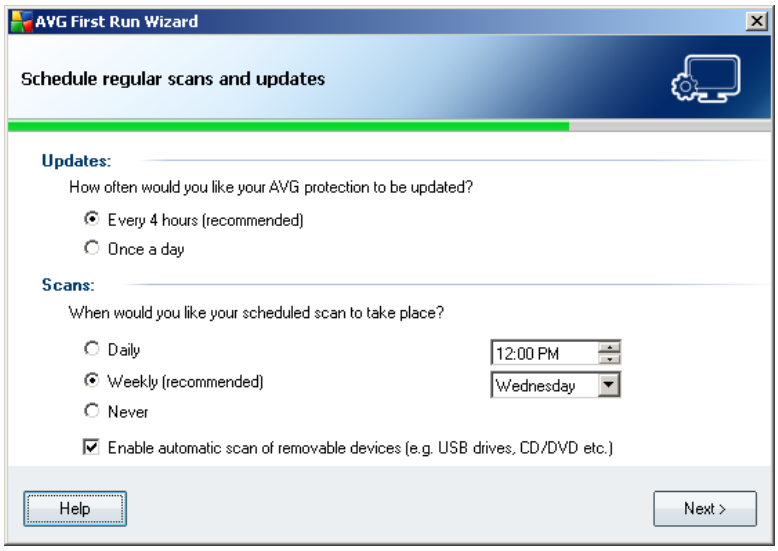
## 5.8. Installing AVG

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



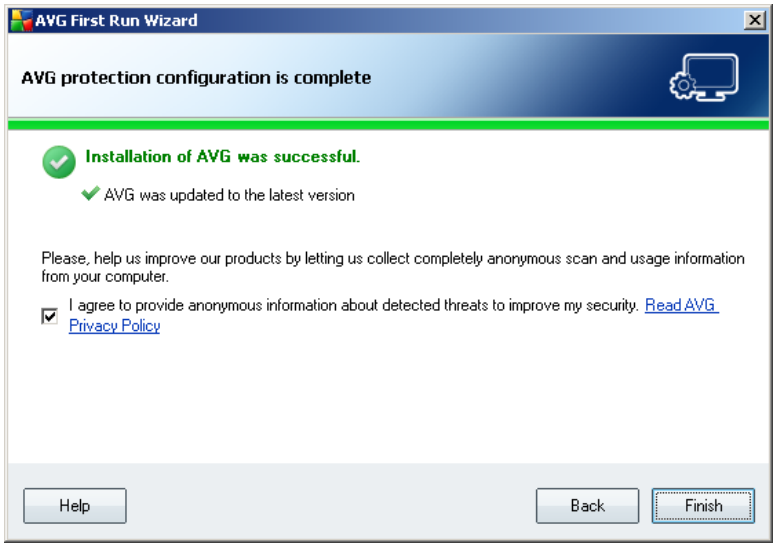

After the installation process is finished, you will be redirected to the next dialog automatically.

## 5.9. Schedule regular scans and updates




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

## 5.10. AVG protection configuration is complete



Now your **AVG 9.0 File Server** has been configured.

In this dialog you decide whether you want to activate the option of anonymous reporting of exploits and bad sites to AVG virus lab. If so, please mark the ***I agree to provide ANONYMOUS information about detected threats to improve my security*** option.

Finally, press the ***Finish*** button. Your computer restart may be required so that you can start working with AVG.

AVG 9.0 File Server © 2009 Copyright AVG Technologies CZ, s.r.o. All rights reserved.

# 6. After Installation

## 6.1. Product Registration

Having finished the **AVG 9.0 File Server** installation, please register you product online on AVG website (http://www.avg.com), ***Registration*** page (*follow the instruction provided directly in the page*). After the registration you will be able to gain full access to your AVG User account, the AVG Update newsletter, and other services provided exclusively for registered users.

## 6.2. Access to User Interface

The ***AVG User Interface*** is accessible in several ways:

- double-click the AVG icon on the system tray
- double-click the AVG icon on the desktop
- from the menu ***Start/Programs/AVG 9.0/AVG User Interface***

## 6.3. Scanning of the whole computer

There is a potential risk that a computer virus has been transmitted to your computer prior to **AVG 9.0 File Server** installation. For this reason you should run a ***Scan of the whole computer*** to make sure there are no infections on your PC.

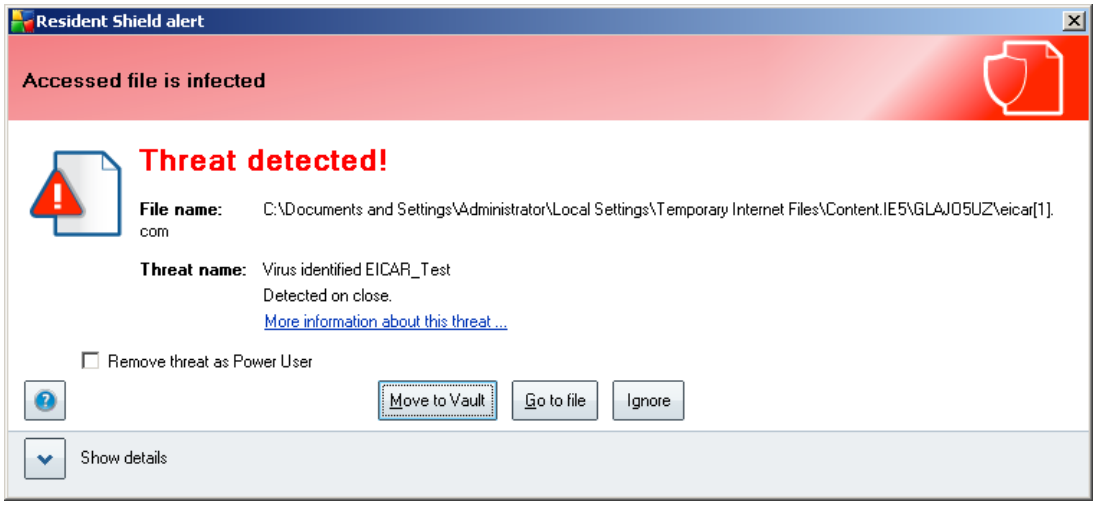
For instructions on running a ***Scan of the whole computer*** please consult the chapter ***AVG Scanning***.

## 6.4. Eicar Test

To confirm that **AVG 9.0 File Server** has been installed correctly you can perform the EICAR test.

The EICAR test is a standard and absolutely safe method used to test antivirus system functioning. It is safe to pass around, because it is not an actual virus, and does not include any fragments of viral code. Most products react to it as if it were a virus ( *though they typically report it with an obvious name, such as "EICAR-AV-Test"*). You can download the EICAR virus from the EICAR website at 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 of the test file, the ***Resident Shield*** will react to it with a warning. This ***Resident Shield*** notice demonstrates that AVG is correctly installed on your computer.




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

## 6.5. AVG Default Configuration

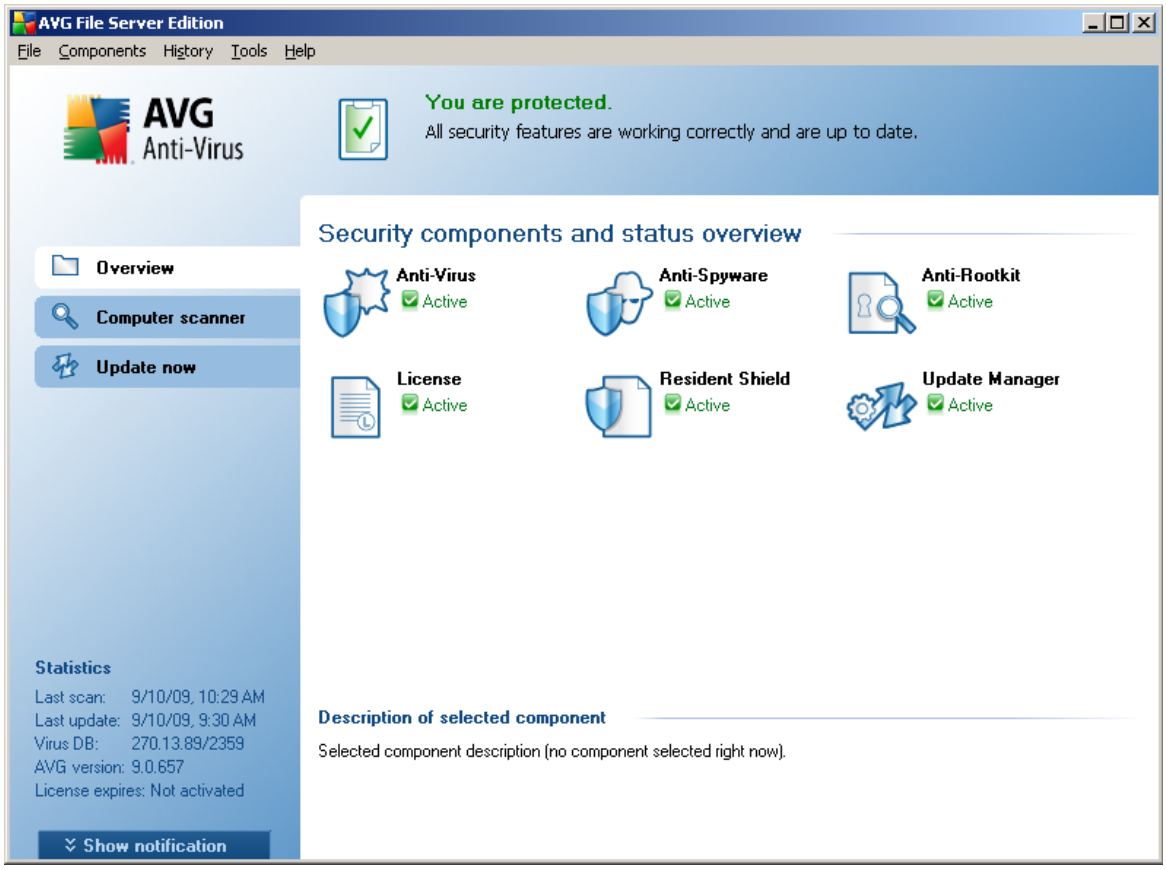
The default configuration (*i.e. how the application is set up right after installation*) of **AVG 9.0 File Server** is set up by the software vendor so that all components and functions are tuned up to achieve optimum performance.

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

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

# 7. AVG User Interface

**AVG 9.0 File Server** open with the main window:




The main window is divided into several sections:

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

- ***Statistics*** *(left bottom section of the window)* provide you with all statistical data regarding the programs operation - details >>

- ***System Tray Icon*** *(bottom right corner of the monitor, on the system tray)* indicates the AVG current status - details >>

## 7.1. System Menu

The ***System menu*** is the standard navigation used in all Windows applications. It is located horizontally in the very top part of the **AVG 9.0 File Server** main window. Use the system menu to access specific AVG components, feature, and services.

The system menu is divided into five main sections:

### 7.1.1. File

- ***Exit*** - closes the **AVG 9.0 File Server**'s user interface. However, the AVG application will continue running in the background and your computer will still be protected!

### 7.1.2. Components

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

- ***System overview*** - switch to the default user interface dialog with the overview of all installed components and their status

- ***Anti-Virus*** - opens the default page of the ***Anti-Virus*** component

- ***Anti-Rootkit*** - opens the default page of the ***Anti-Rootkit*** component

- ***Anti-Spyware*** - opens the default page of the ***Anti-Spyware*** component

- ***License*** - opens the default page of the ***License*** component

- ***Resident Shield*** - opens the default page of the ***Resident Shield*** component

- ***Update Manager*** - opens the default page of the ***Update Manager*** component

### 7.1.3. History

- ***Scan results*** - switches to the AVG testing interface, specifically to the ***Scan Results Overview*** dialog

- ***Resident Shield Detection*** - open a dialog with an overview of threats detected by ***Resident Shield***

- ***Virus Vault*** - opens the interface of the quarantine space (***Virus Vault***) to where AVG removes all detected infections that cannot be healed automatically for some reason. Inside this quarantine the infected files are isolated and your computer's security is guaranteed, and at the same time the infected files are stored for possible future repair.

- ***Event History Log*** - opens the history log interface with an overview of all logged **AVG 9.0 File Server** actions.

### 7.1.4. Tools

- ***Scan computer*** - switches to the AVG scanning interface and launches a scan of the whole computer

- ***Scan selected folder*** - switches to the AVG scanning interface and allows you to define within the tree structure of your computer which files and folders should be scanned

- ***Scan file*** - allows you to run an on-demand test over a single file selected from the tree structure of your disk

- ***Update*** - automatically launches the update process of **AVG 9.0 File Server**

- ***Update from directory*** - runs the update process from the update files located in a specified folder on your local disk. However, this option is only recommended as an emergency, e.g. in situations where there is no connection to the Internet (*for example, your computer is infected and disconnected from the Internet; your computer is connected to a network with no access to the Internet, etc.*). In the newly opened window select the folder where you have previously placed the update file, and launch the update process.

- ***Advanced settings*** - opens the ***AVG advanced settings*** dialog where you can edit the **AVG 9.0 File Server** configuration. Generally, it is recommended to keep the default settings of the application as defined by the software vendor.

### 7.1.5. Help

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

## 7.2. Security Status Info

The ***Security Status Info*** section is located in the upper part of the AVG main window. Within this section you will always find information on the current security status of your **AVG 9.0 File Server**. Please see an overview of icons possibly depicted in this section, and their meaning:

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

The orange icon warns that one or more components are incorrectly configured and you should pay attention to their properties/settings. There is no critical problem in AVG and you have probably decided to switch some component off for some reason. You are still protected by AVG. However, please

pay attention to the problem component's settings! Its name will be provided in the ***Security Status Info*** section.

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

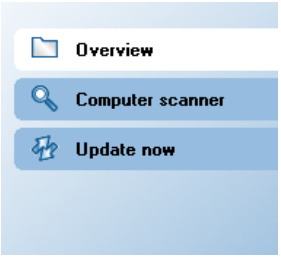
The red icon indicates that AVG is in critical status! One or more components does not work properly and AVG cannot protect your computer. Please pay immediate attention to fixing the reported problem. If you are not able to fix the error yourself, contact the AVG technical support team.

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

***Note:*** *AVG status information can also be obtained at any moment from the system tray icon.*

## 7.3. Quick Links

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




- ***Overview*** - use this link to switch from any currently opened AVG interface to the default one with an overview of all installed components - see chapter ***Components Overview >>***
- ***Computer scanner*** - use this link to open the AVG scanning interface where you can run tests directly, schedule scans, or edit their parameters - see chapter ***AVG Tests >>***

- ***Update now*** - this link open the updating interface, and launches the AVG update process immediately - see chapter ***AVG Updates*** >>

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

## 7.4. Components Overview

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

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

Within the **AVG 9.0 File Server** the ***Components Overview*** section contains information on the following components:

- ***Anti-Virus*** ensures that your computer is protected from viruses trying to enter your computer - details >>
- ***Anti-Spyware*** scans your applications in the background as you run them - details >>
- ***Anti-Rootkit*** detects programs and technologies trying to camouflage malware - details >>
- ***License*** provides full wording of the AVG License Agreement - details >>
- ***Resident Shield*** runs in the background and scans files as they are copied, opened or saved - details >>
- ***Update Manager*** controls all AVG updates - details >>

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

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

## 7.5. Statistics

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

- ***Last scan*** - provides the date when the last scan was performed
- ***Last update*** - provides the date when the last update was launched
- ***Virus DB*** - informs you about the currently installed version of the virus database
- ***AVG version*** - informs you about the AVG version installed *(the number is in the form of 8.0.xx, where 8.0 is the product line version, and xx stands for*

*the number of the build)*

- ***License expires*** - provides the date of your AVG license expiration

## 7.6. System Tray Icon

***System Tray Icon*** (*on your Windows taskbar*) indicates the current status of your **AVG 9.0 File Server**. It is visible at all times on your system tray, no matter whether your AVG main window is opened or closed.

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

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

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

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

- ***Open AVG User Interface*** - click to open the AVG User Interface
- ***Update*** - launches an immediate update

# 8. AVG Components

## 8.1. Anti-Virus

### 8.1.1. Anti-Virus Principles

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

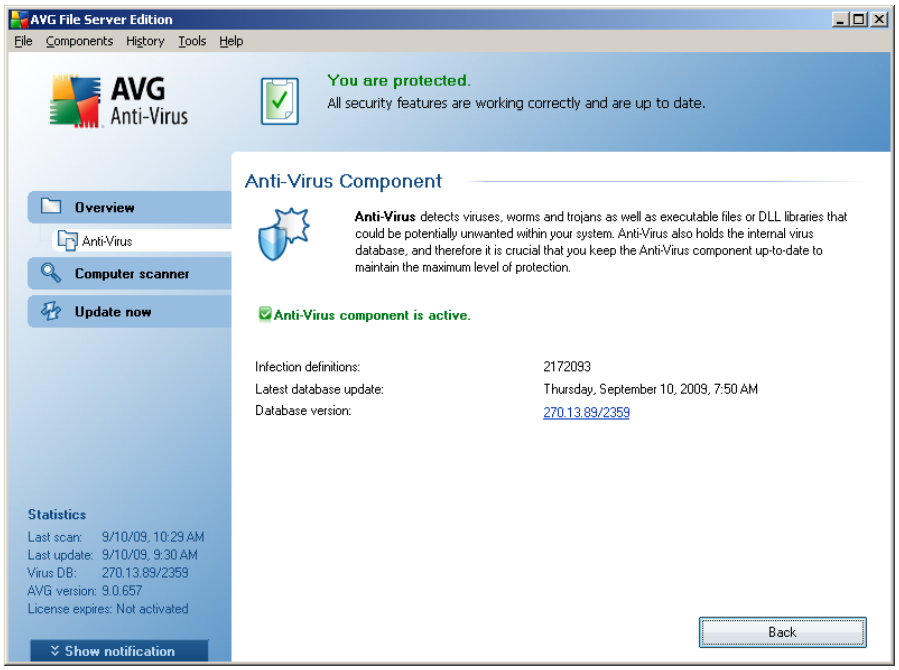
***The important feature of antivirus protection is that no known virus can run on the computer!***

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

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

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

## 8.1.2. Anti-Virus Interface




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

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

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

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

*Advanced Settings dialog.*

## 8.2. Anti-Spyware

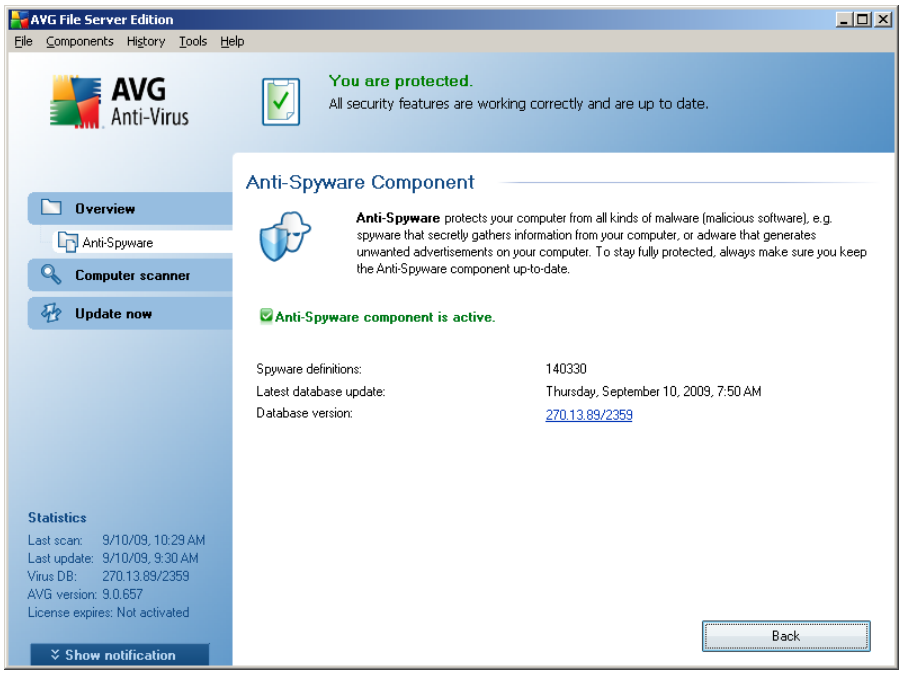
### 8.2.1. Anti-Spyware Principles

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

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

There is also the potential risk that malware has been transmitted to your computer prior to AVG installation, or that you have neglected to keep your **AVG 9.0 File Server** 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-active malware, i.e. malware that has been downloaded but not yet activated.

## 8.2.2. Anti-Spyware Interface




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

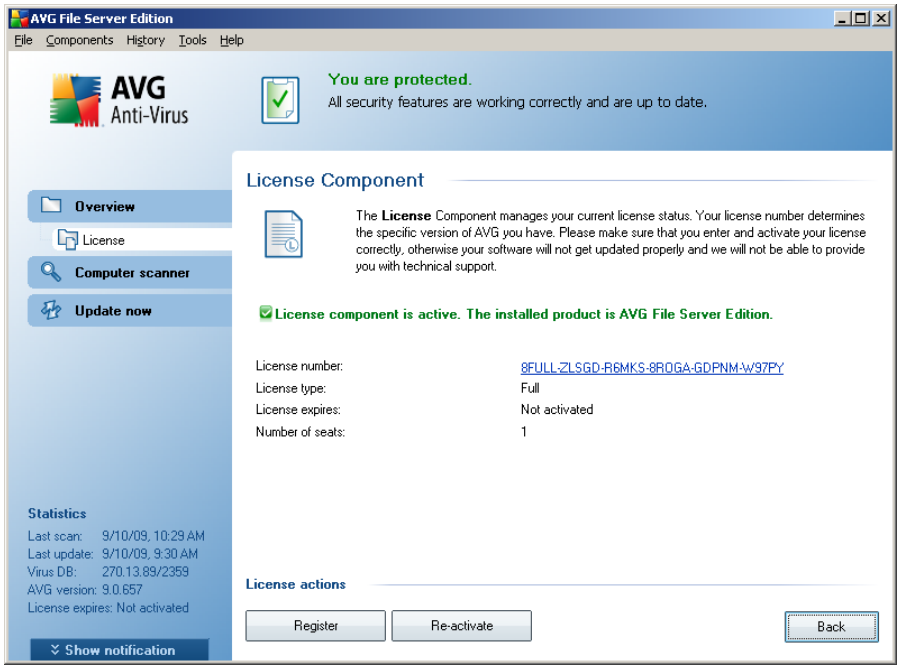
- ***Spyware definitions*** - number provides the count of spyware samples defined in the latest spyware database version
- ***Latest database update*** - specifies when and at what time the spyware database was updated
- ***Database version*** - defines the number of the latest spyware database version;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

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

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

*Advanced Settings dialog.*

## 8.3. License




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

- ***License number*** - provides the exact form of your license number. When entering your license number, you have to be absolutely precise and type it exactly as shown. Therefore we strongly recommend to always use "copy & paste" method for any manipulation with the license number.
- ***License type*** - specifies the product type installed.
- ***License expires*** - this date determines the period of validity of your license. If you want to go on using **AVG 9.0 File Server** after this date you have to renew your license. The license renewal can be performed online on AVG website (http://www.avg.com).
- ***Number of seats*** - how many workstations on which you are entitled to install your **AVG 9.0 File Server**.

**Control buttons**

- ***Register*** - connects to the registration page of AVG website (http://www.avg.com). Please fill in your registration data; only customers who register their AVG product can receive free technical support.

- ***Re-activate*** - opens the ***Activate AVG*** dialog with the data you have entered in the ***Personalize AVG*** dialog of the installation process. Within this dialog you can enter your license number to either replace the sales number (*the number you have installed AVG with*), or to replace the old license number (*e.g. when upgrading to a new AVG product*).

- ***Back*** - press this button to return to the default AVG user interface (components overview).

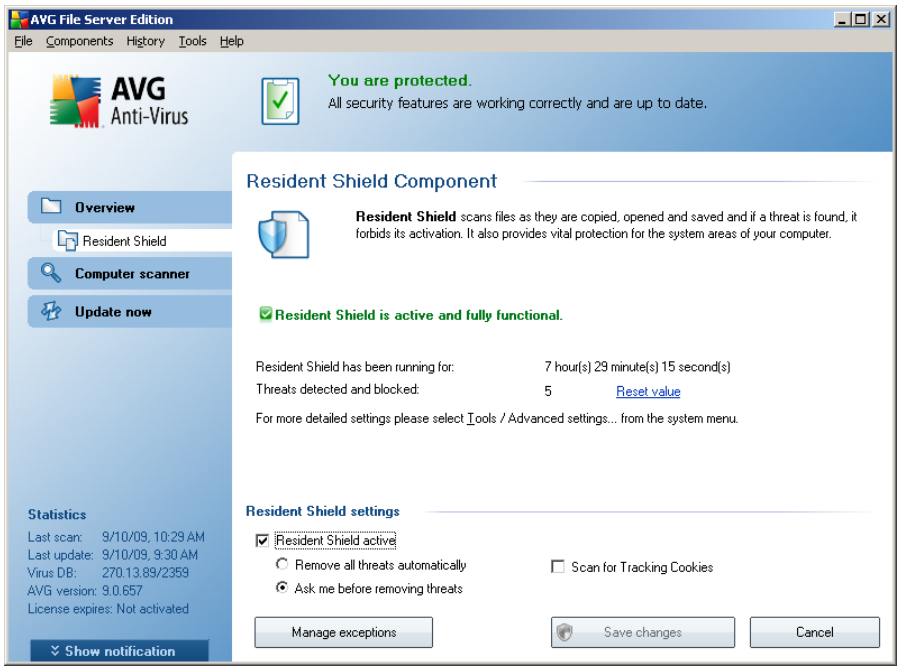
## 8.4. Resident Shield

### 8.4.1. Resident Shield Principles

The ***Resident Shield*** component gives your computer continuous protection. It scans every single file that is being opened, saved, or copied, and guards the system areas of the computer. When ***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. Normally, you do not even notice the process, as it runs "in the background", and you only get notified when threats are found; at the same time, ***Resident Shield*** blocks activation of the threat and removes it. ***Resident Shield*** is being loaded in the memory of your computer during system startup.

***Warning: Resident Shield is loaded in the memory of your computer during startup, and it is vital that you keep it switched on at all times!***

## 8.4.2. Resident Shield Interface




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

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

### Basic component configuration

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

The ***Resident Shield is active*** option allows you to easily switch on/off resident

protection. By default, the function is on. With resident protection on you can further decide how the possibly detected infections should be treated (removed):

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

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

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

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

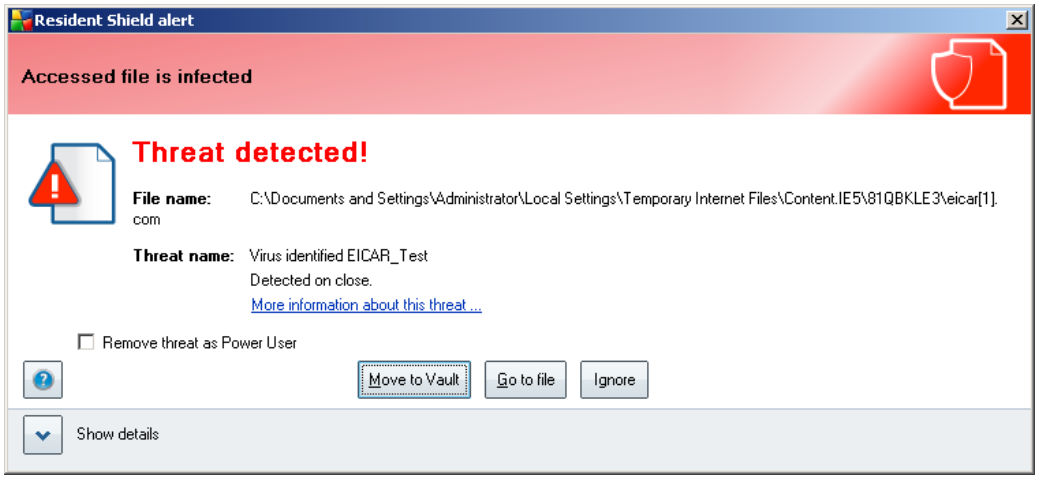
## Control buttons

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

- ***Manage exceptions*** - opens the ***Resident Shield - Directory Excludes*** dialog where you can define folders that should be left out from the ***Resident Shield*** scanning
- ***Save changes*** - press this button to save and apply any changes made in this dialog
- ***Cancel*** - press this button to return to the default ***AVG user interface*** (components overview)

### 8.4.3. Resident Shield Detection

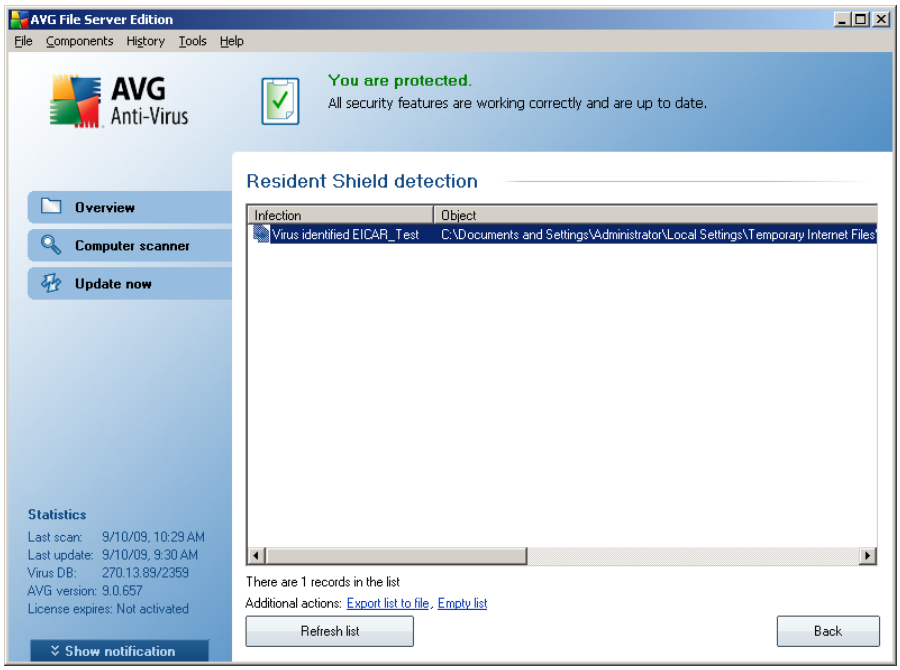
***Resident Shield*** scans files as they are copied, opened or saved. When a virus or any kind of threat is detected, you will be warned immediately via the following dialog:




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

- ***Heal*** - if a cure is available, AVG will heal the infected file automatically; this option is the recommended action to be taken
- ***Move to Vault*** - the virus will be moved to AVG ***Virus Vault***
- ***Go to file*** - this option redirects you to the exact location of the suspicious object ( *opens new Windows Explorer window*)
- ***Ignore*** - we strictly recommend NOT TO use this option unless you have a very good reason to do so!

The entire overview of all threats detected by ***Resident Shield*** can be found in the ***Resident Shield detection*** dialog accessible from via system menu option ***History / Resident Shield findings***:




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

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

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

## 8.5. Update Manager

### 8.5.1. Update Manager Principles

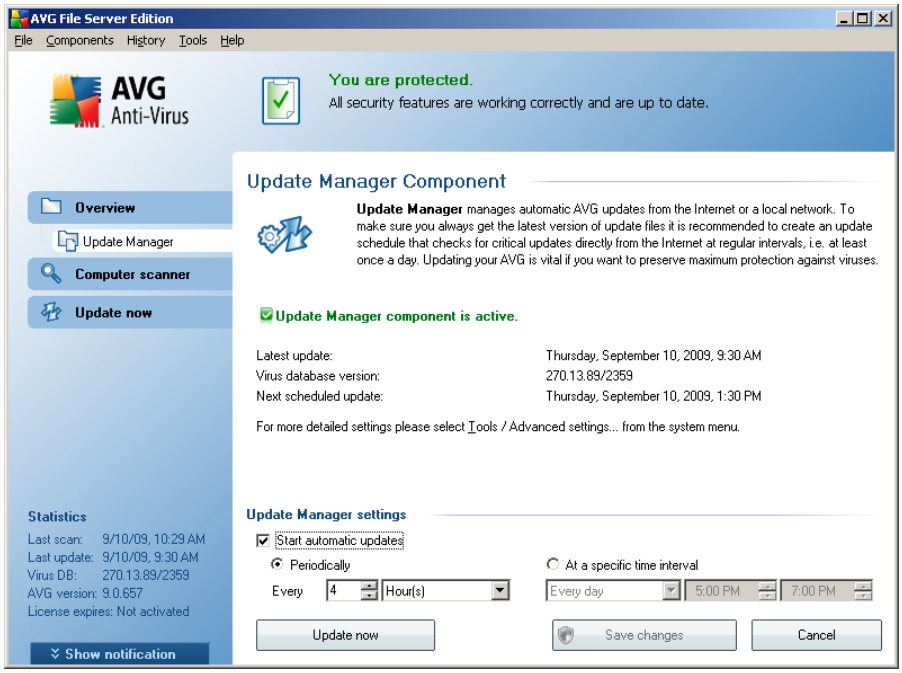
No security software can guarantee true protection from various types of threats unless it is regularly updated! Virus writers are always looking for new flaws that they can exploit in both software and operating systems. New viruses, new malware, new hacking attacks appear daily. For this reason, software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

***It is crucial to update your AVG regularly!***

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

***Note:*** *Please pay attention to the AVG Updates chapter for more information on update types and levels!*

### 8.5.2. Update Manager Interface



The ***Update Manager***'s interface displays information about the component's functionality and its current status (*Update manager is active.*), and provides the relevant statistical data:

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

## Basic component configuration

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

Further you can define when the update should be launched:

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

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

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

## Control buttons

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

- ***Update now*** - launches an immediate update on demand

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

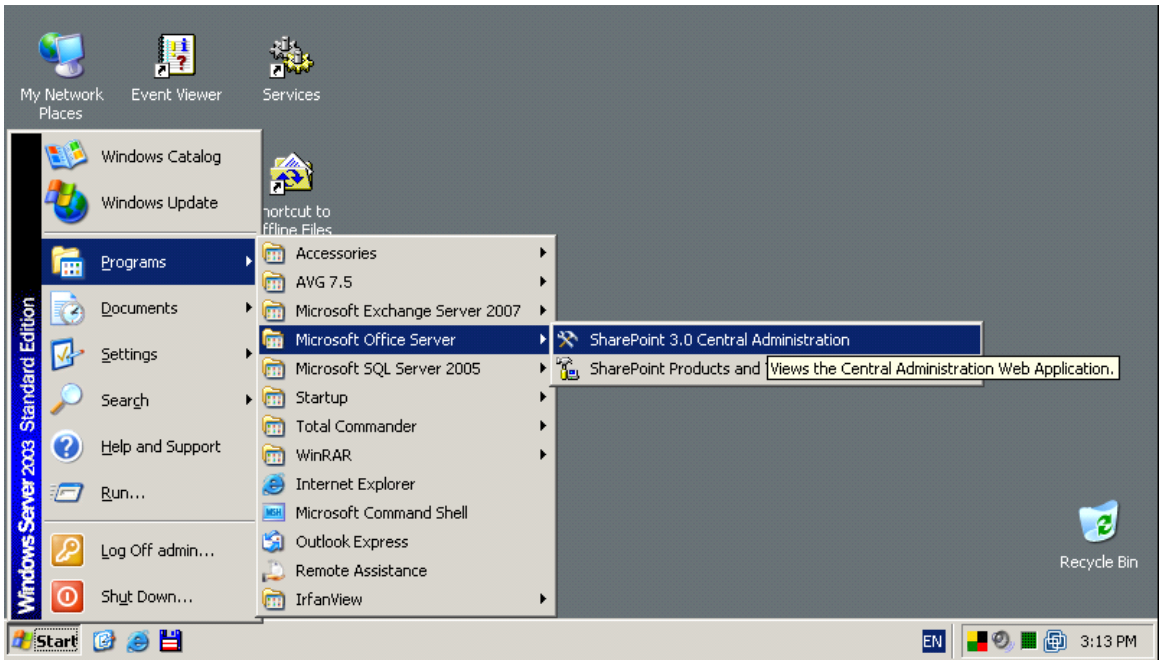
# 9. AVG for SharePoint Portal Server

This chapter deals with AVG maintenance on ***MS SharePoint Portal Server*** that can be considered a special type of a file server.

## 9.1. Program Maintenance

**AVG for SharePoint Portal Server** uses the Microsoft SP VSAPI 1.4 virus-scanning interface for the protection of your server against possible virus infection. The objects on the server are tested for the presence of malware when they are downloaded and/ or uploaded from or on the server by your users. The configuration of the anti-virus protection can be set up using the ***Central Administration*** interface of your SharePoint Portal Server. Within the ***Central Administration*** you can also view and manage the **AVG for SharePoint Portal Server** log file.

You can launch the ***SharePoint Portal Server Central Administration*** when you are logged in on the computer that your server is running on. The administration interface is web-based (*as well as the user interface of the SharePoint Portal Server*) and you can open it using the ***SharePoint (3.0) Central Administration*** option in the ***Programs/Microsoft Office Server*** folder (***or SharePoint Portal Server***) of the Windows ***Start*** menu:



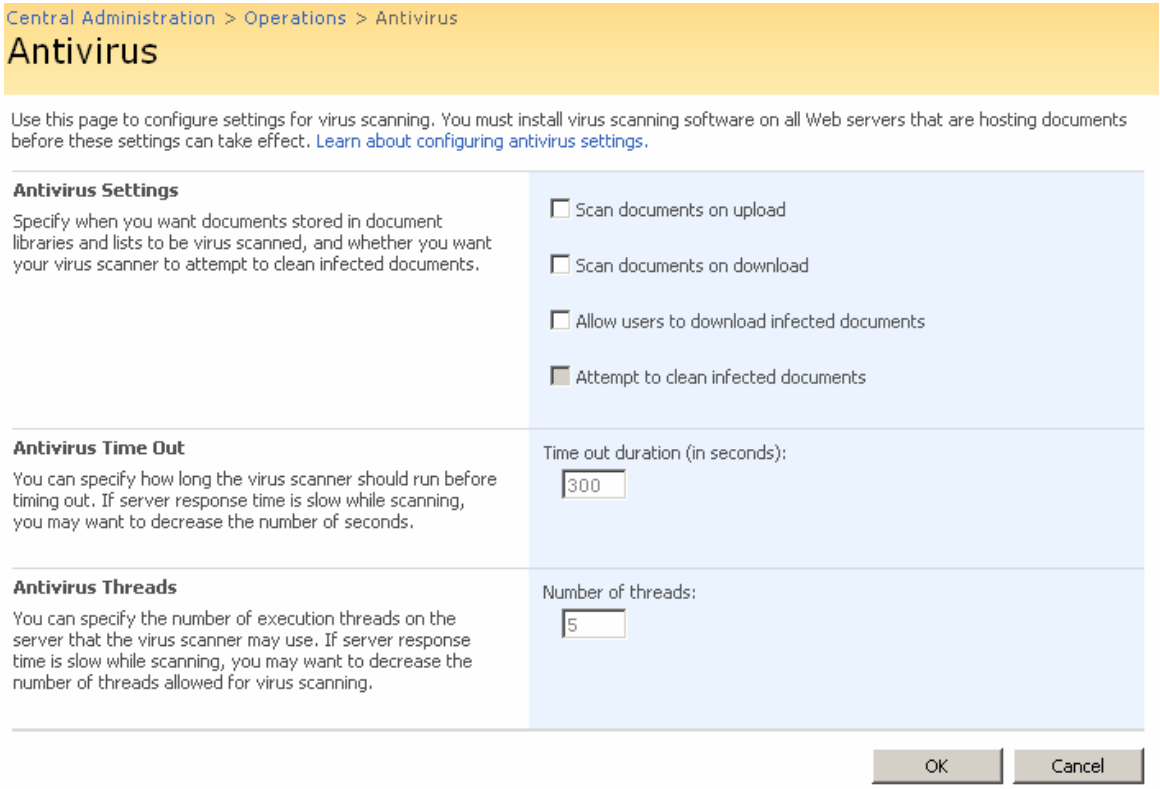

You can also enter the ***SharePoint Portal Server Central Administration*** web page

remotely using the proper access rights and URL.

## 9.2. AVG for SPPS Configuration - SharePoint 2007

In the ***SharePoint 3.0 Central Administration*** interface you can easily configure the performance parameters and actions of the **AVG for SharePoint Portal Server** scanner. Choose the ***Operations*** option in the ***Central Administration*** section. A new dialog will appear. Select ***Antivirus*** item in the ***Security Configuration*** part.

The following window will then be displayed:



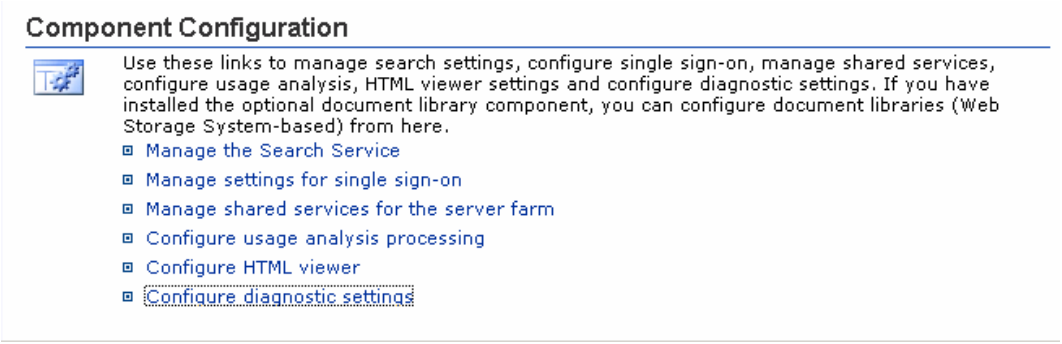

You can configure various **AVG for SharePoint Portal Server** anti-virus scanning actions and performance features here:

- ***Scan documents on upload*** – enable/disable the scanning of documents being uploaded
- ***Scan documents on download*** – enable/disable the scanning of documents being downloaded
- ***Allow users to download infected documents*** – allow/disallow users to download infected documents
- ***Clean infected documents*** – enable/disable automatic erasing of infected documents
- ***Time out duration*** (*in seconds*) – the maximum number of seconds the virus scanning process will run after single launch (decrease the value when the server's response seems to be slow when scanning the documents)

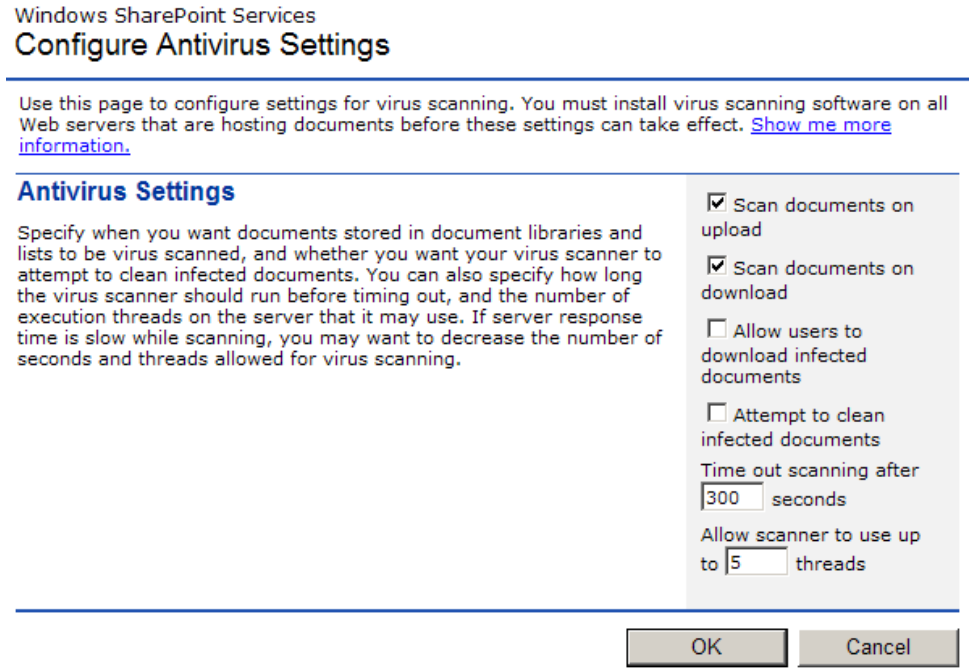
- ***Number of threads*** – you can specify the number of virus scanning threads that can run simultaneously; increasing the number may speed up the scanning due to the higher level of parallelism, but it can increase the server's response time on the other hand

## 9.3. AVG for SPPS Configuration - SharePoint 2003

In the ***SharePoint Portal Server Central Administration*** interface you can easily configure the performance parameters and actions of the **AVG for SharePoint Portal Server** scanner. Choose the ***Antivirus Actions Configuration*** option in the ***Security Configuration*** section:




The following window will then be displayed:



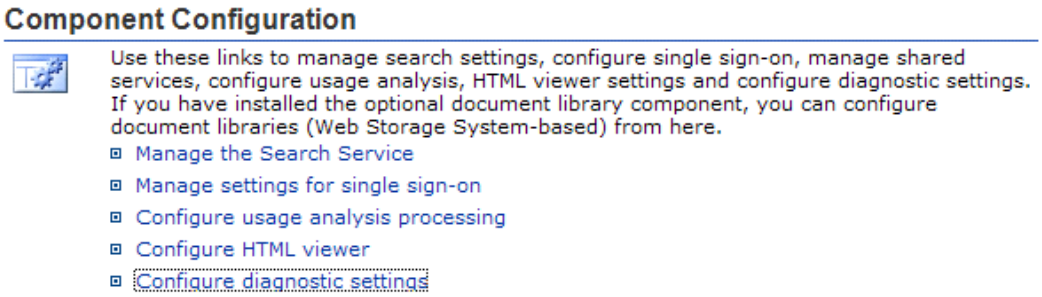

You can configure various **AVG for SharePoint Portal Server** anti-virus scanning actions and performance features here:

- ***Scan documents on upload*** – enable/disable the scanning of documents being uploaded
- ***Scan documents on download*** – enable/disable the scanning of documents being downloaded
- ***Allow users to download infected documents*** – allow/disallow users to download infected documents
- ***Clean infected documents*** – enable/disable automatic erasing of infected documents
- ***Time limit of scanning*** – the maximum number of seconds the virus scanning process will run after single launch (*decrease the value when the server's response seems to be slow when scanning the documents*)
- ***Use max. X sub-processes when scanning documents*** – the X specifies the number of virus scanning threads that can run simultaneously; increasing the number may speed up the scanning due to the higher level of parallelism, but it

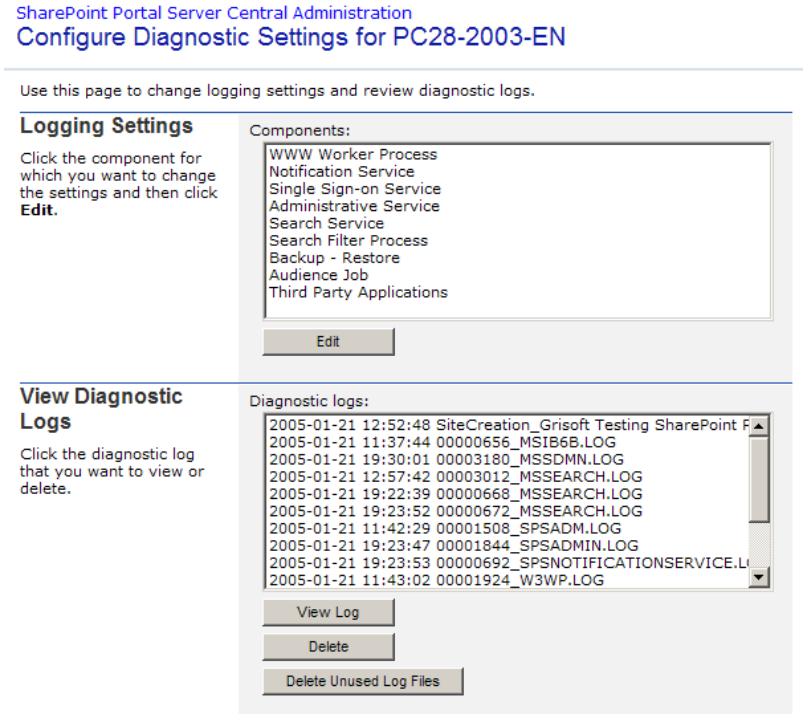
can increase the server's response time on the other hand

## 9.4. AVG for SPPS Edition Diagnostics

The diagnostics messages of **AVG for SharePoint Portal Server** can be viewed after choosing the ***Diagnostics Settings Configuration*** in the ***SharePoint Central Administration's Component Configuration*** section:




All diagnostics information related to **AVG for SharePoint Portal Server** performance are stored in the *_AVG4SPS.LOG file. The contents of this file can be viewed after choosing it in the ***Display diagnostics protocols*** section of the ***Diagnostics Settings Configuration*** window:



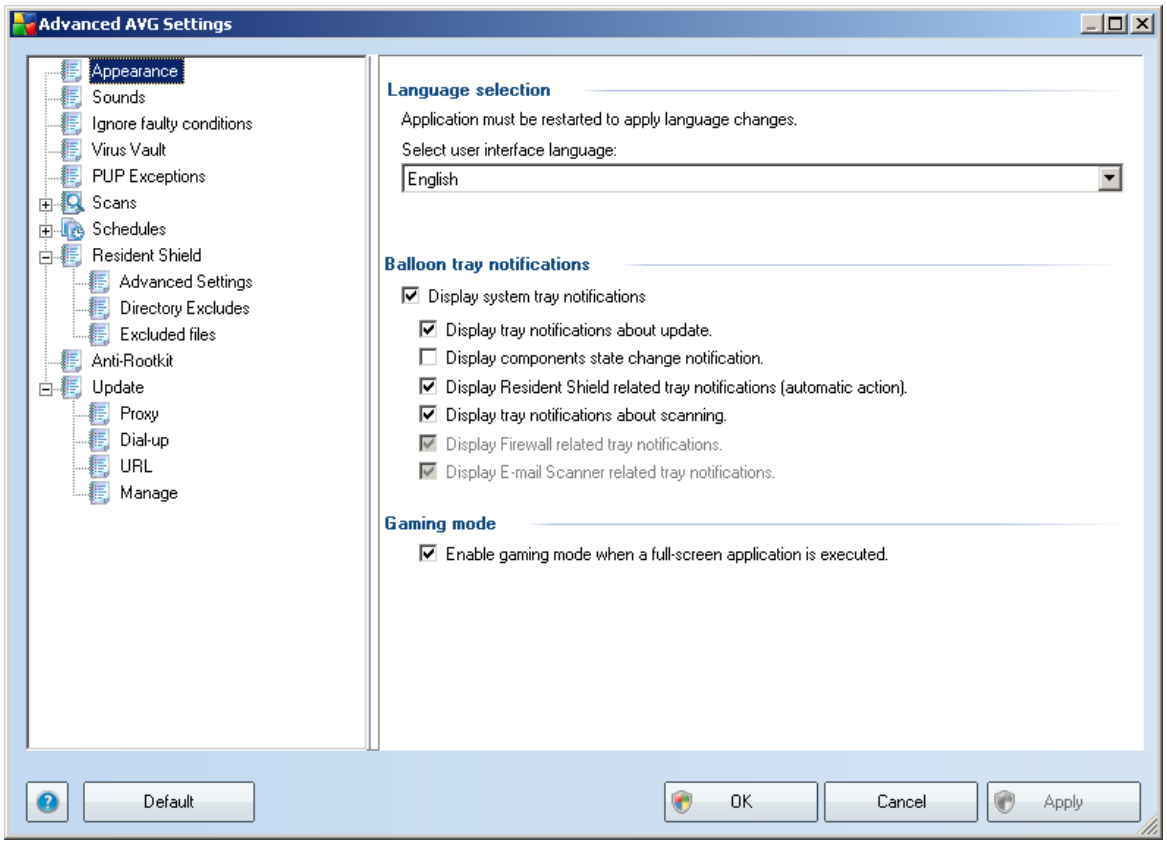

Press the ***View log*** button to view the log file of **AVG for SharePoint Portal Server**.

# 10. AVG Advanced Settings

The advanced configuration dialog of **AVG 9.0 File Server** opens in a new window named ***Advanced AVG Settings***. The window is divided into two sections: the left part offers a tree-arranged navigation to the program configuration options. Select the component you want to change the configuration of (*or its specific part*) to open the editing dialog in the right-hand section of the window.

## 10.1. Appearance

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

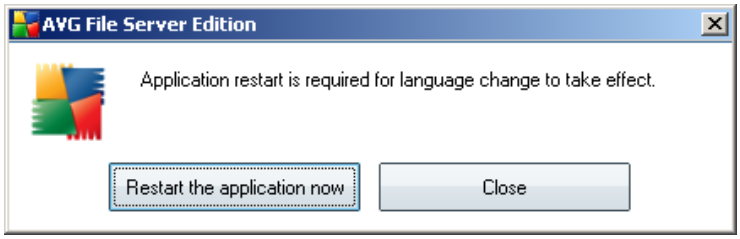



### Language selection

In the ***Language selection*** section you can chose your desired language from the

drop-down menu; the language will then be used for the entire AVG user interface. The drop-down menu only offers those languages you have previously selected to be installed during the installation process (see chapter Custom Installation - Component Selection). However, to finish switching the application to another language you have to restart the user interface; follow these steps:

- Select the desired language of the application and confirm your selection by pressing the ***Apply*** button (right-hand bottom corner)
- Press the ***OK*** button confirm
- New dialog window pops-up informing you the language change of AVG user interface requires the application restart:




## Balloon tray notifications

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

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

- ***Display system tray notifications*** - by default, this item is checked ( *switched on*), and notifications are displayed. Uncheck this item to completely turn off the display of all balloon notifications. When turned on, you can further select what specific notifications should be displayed:
  - ***Display tray notifications about update*** - decide whether information regarding AVG update process launch, progress, and finalization should be displayed;

- ***Display components state change notifications*** - decide whether information regarding component's activity/inactivity or its possible problem should be displayed. When reporting a component's fault status, this option equals to the informative function of the system tray icon (color changing) reporting a problem in any AVG component;

- ***Display Resident Shield related tray notifications*** - decide whether information regarding file saving, copying, and opening processes should be displayed or suppressed;

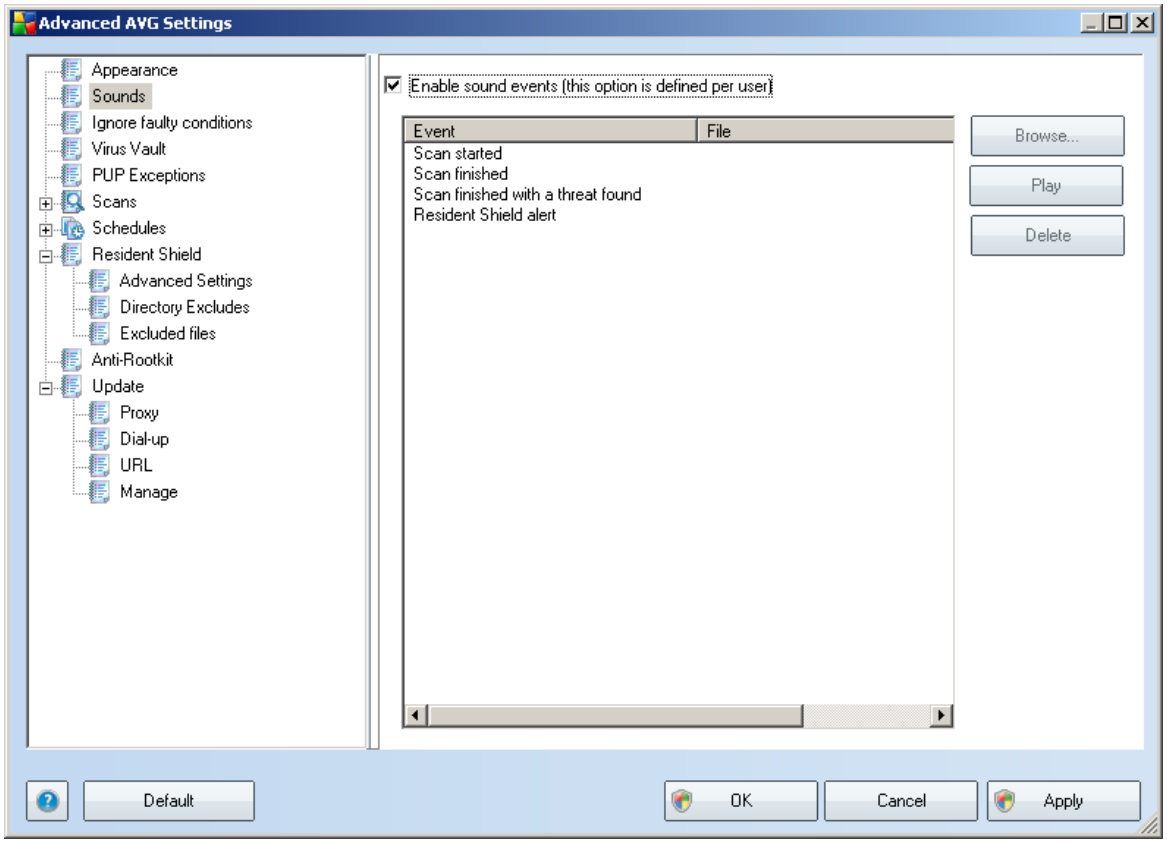
- ***Display tray notifications about scanning*** - decide whether information upon automatic launch of the scheduled scan, its progress and results should be displayed.

### Gaming mode

This AVG function is designed for full-screen applications that need to communicate over Internet and possible AVG ask dialogs would affect the application (*minimize it or corrupt its graphics*). To avoid this situation, keep the check box for the ***Enable gaming mode when a full-screen application is executed*** option marked (*default setting*).

## 10.2. Sounds

Within the ***Sounds*** dialog you can specify whether you want to be informed about specific AVG actions by a sound notification. If so, check the ***Enable sound events*** option (*off by default*) to activate the list of AVG actions:

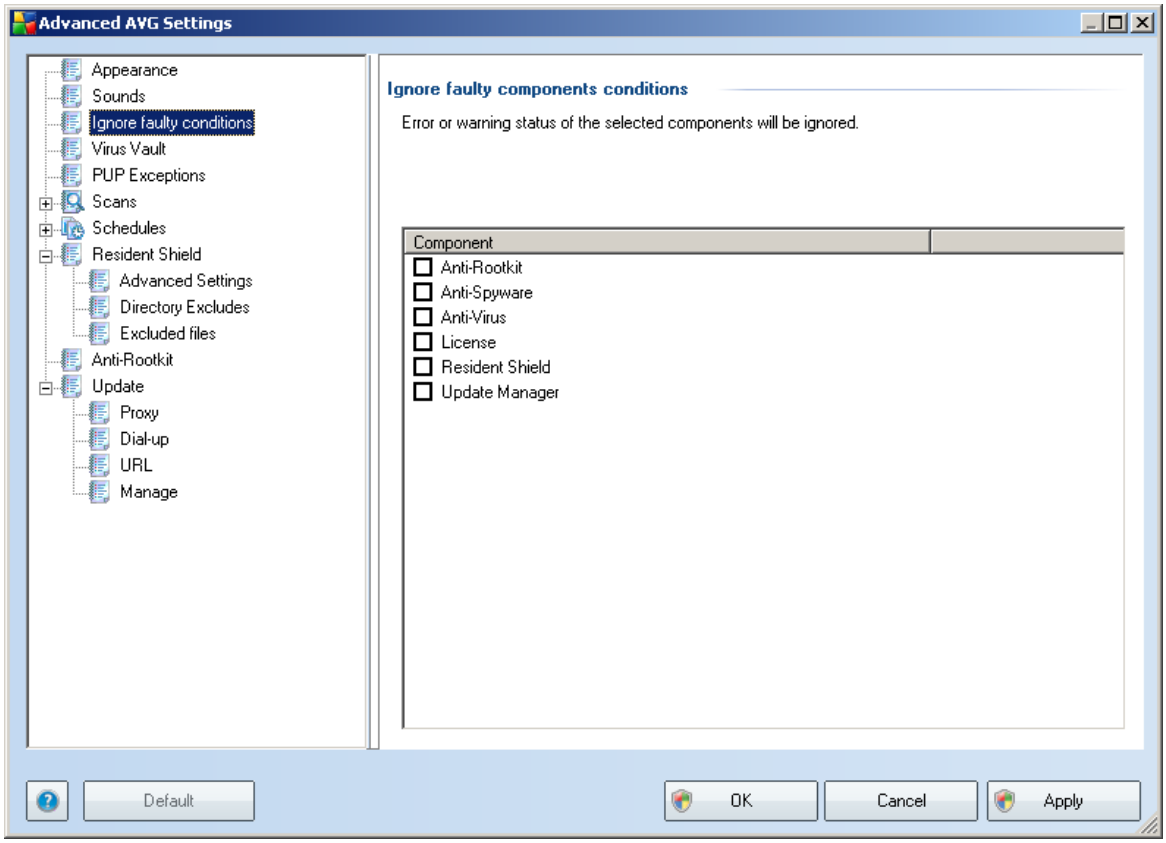



Then, select the respective event from the list and browse (***Browse***) your disk for an appropriate sound you want to assign to this event. To listen to the selected sound, highlight the event in the list and push the ***Play*** button. Use the ***Delete*** button to remove the sound assigned to a specific event.

***Note:*** *Only *.wav sounds are supported!*

## 10.3. Ignore Faulty Conditions

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




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

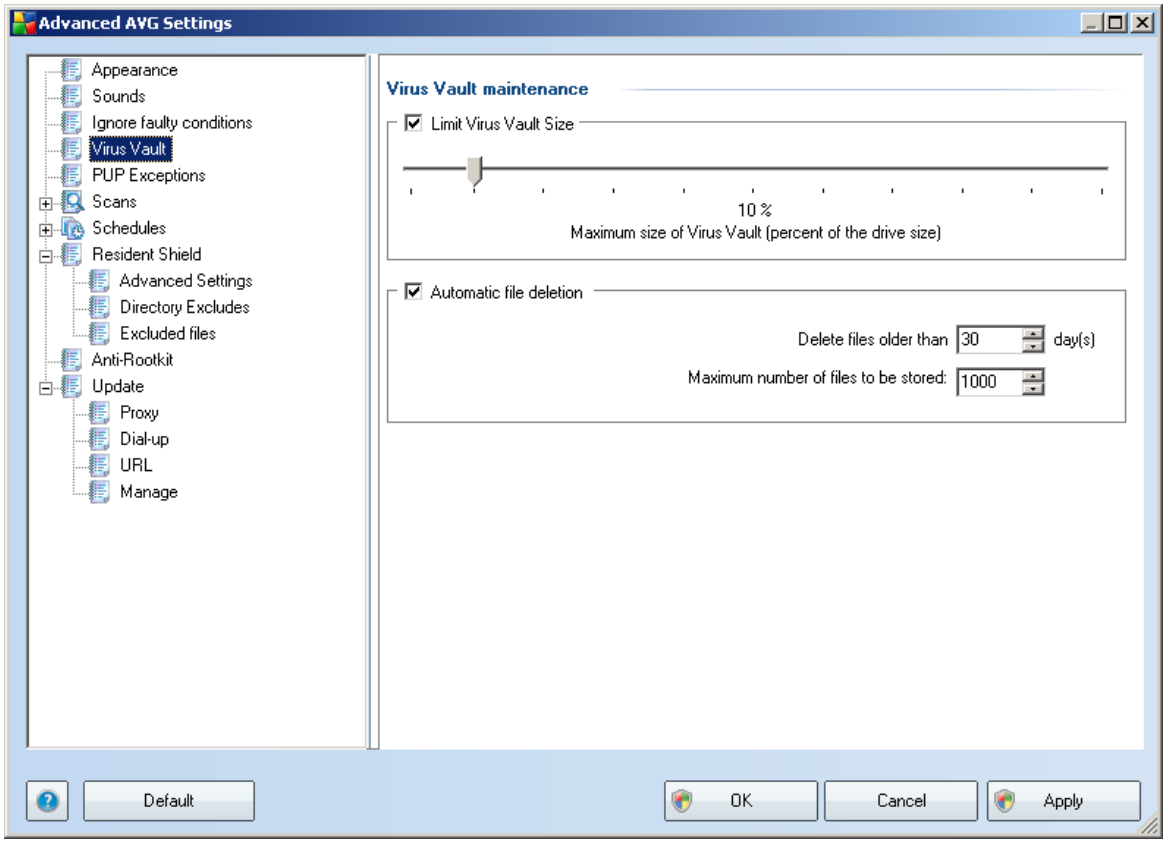
- ***system tray icon*** - while all parts of AVG are working properly, the icon is displayed in four colors; however, if an error occurs, the icon appears with a yellow exclamation mark,
- text description of the existing problem in the ***Security Status Info*** section of the AVG main window

There might be a situation that for some reason you need to switch a component off temporarily (*this is not recommended, you should try to keep all components*

*permanently on and in default configuration, but it may be happen*). In that case the system tray icon automatically reports the component's error status. However, in this very case we cannot talk about an actual error since you have deliberately induced it yourself, and you are aware of the potential risk. At the same time, once being displayed in grey color, the icon cannot actually report any possible further error that might appear.

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

## 10.4. Virus Vault



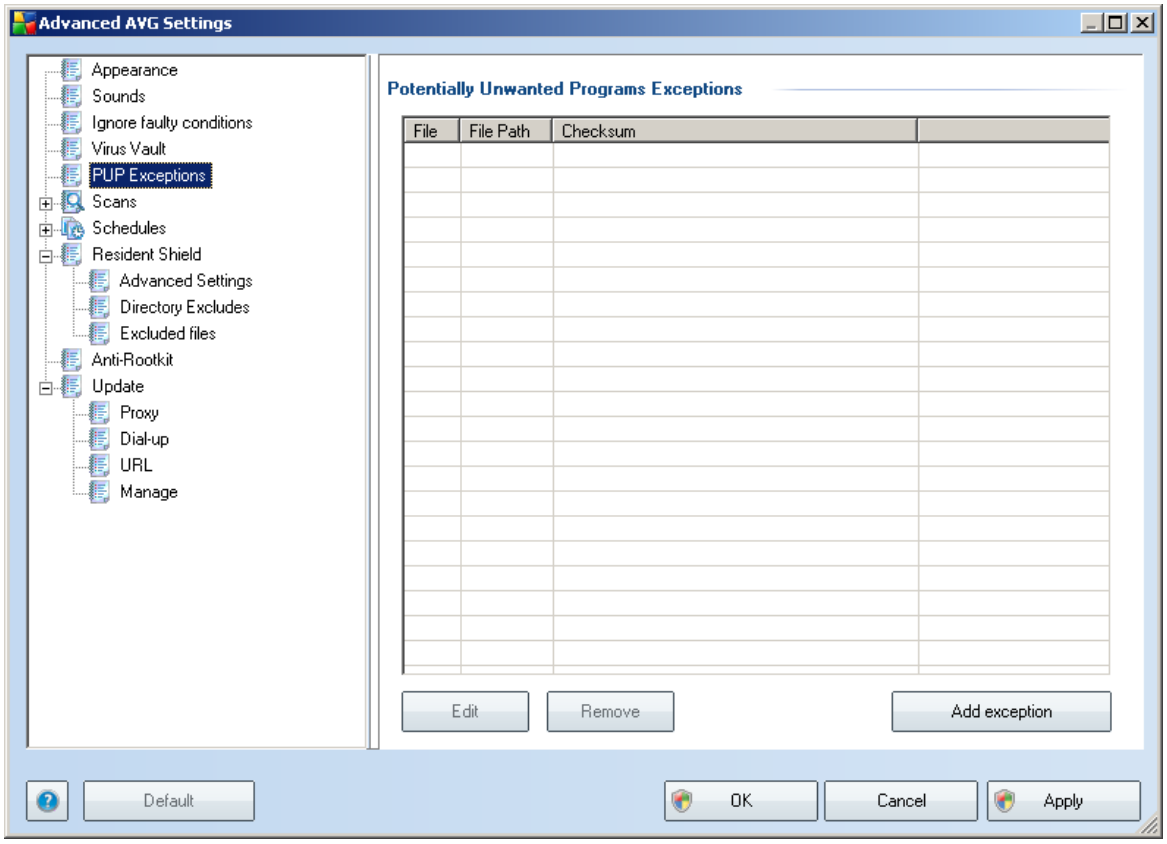

The ***Virus Vault maintenance*** dialog allows you to define several parameters regarding the administration of objects stored in the ***Virus Vault***:

- ***Limit Virus Vault size*** - use the slider to set up the maximum size of the ***Virus Vault***. The size is specified proportionally compared to the size of your local disk.

- ***Automatic file deletion*** - in this section define the maximum length of time that objects should be stored in the ***Virus Vault*** (***Delete files older than ... days***), and the maximum number of files to be stored in the ***Virus Vault*** (***Maximum number of files to be stored***)

## 10.5. PUP Exceptions

**AVG 9.0 File Server** 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:




The ***Potentially Unwanted Programs Exceptions*** dialog displays a list of already defined and currently valid exceptions from potentially unwanted programs. You can edit the list, delete existing items, or add new exceptions. The following information can be found in the list for every single exception:

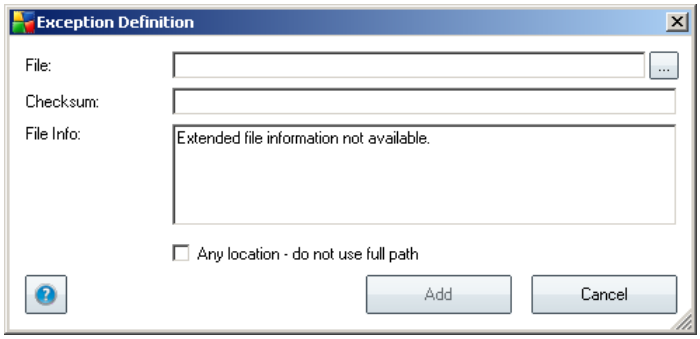
- ***File*** - provides the name of the respective application
- ***File Path*** - shows the way to the application's location
- ***Checksum*** - displays the unique 'signature' of the chosen file. This checksum is an automatically generated string of characters, which allows AVG to unequivocally distinguish the chosen file from other files. The checksum is generated and displayed after successful addition of the file.

## Control buttons

- ***Edit*** - opens an editing dialog (*identical with the dialog for a new exception definition, see below*) of an already defined exception where you can change the exception's parameters

- ***Remove*** - deletes the selected item from the list of exceptions

- ***Add exception*** - open an editing dialog where you can define parameters of the new exception to be created:




  - ***File*** - type the full path to the file that you want to mark as an exception

  - ***Checksum*** - displays the unique 'signature' of the chosen file. This checksum is an automatically generated string of characters, which allows AVG to unequivocally distinguish the chosen file from other files. The checksum is generated and displayed after successful addition of the file.

  - ***File Info*** - displays any additional information available about the file ( *license/version information etc.*)

  - ***Any location - do not use full path*** - if you want to define this file as an exception only for the specific location, then leave this checkbox unchecked

## 10.6. Scans

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

- ***Scan Whole Computer*** - standard predefined scan of the entire computer

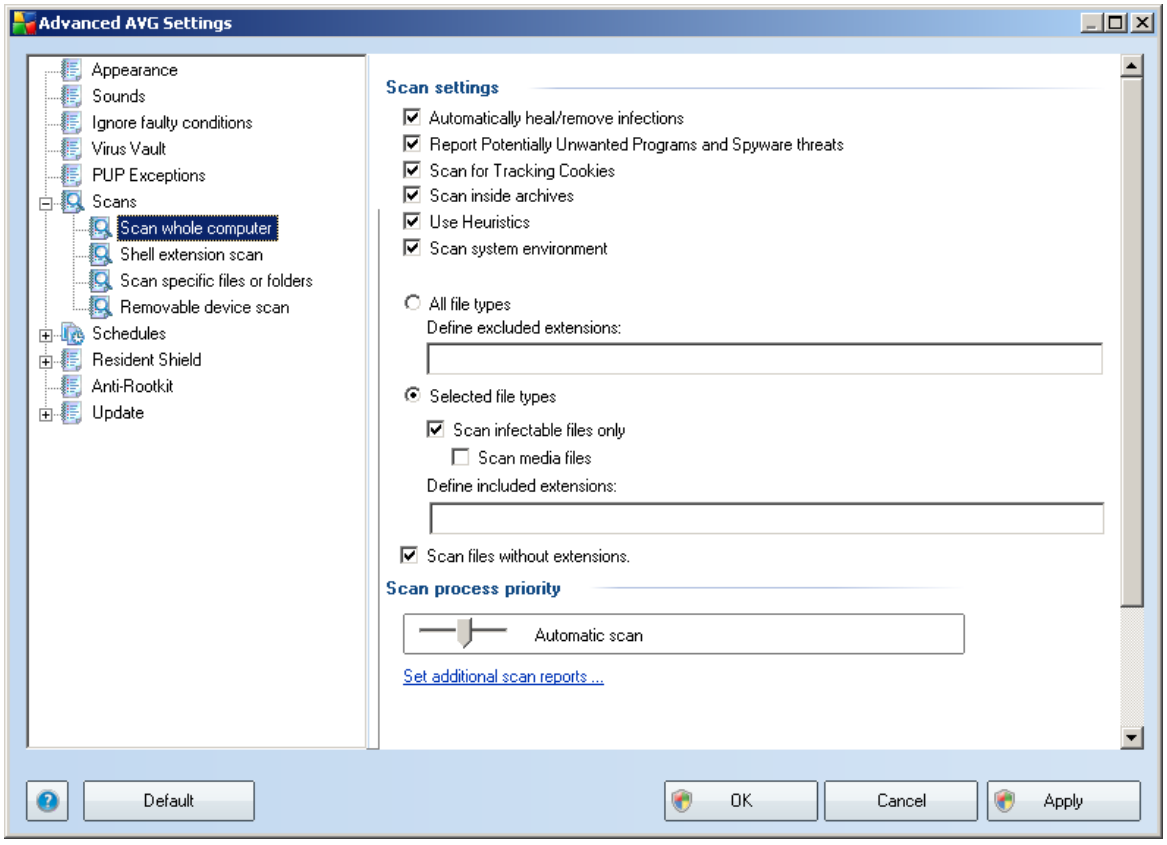
- ***Shell Extension Scan*** - specific scanning of a selected object directly from the

Windows Explorer environment

- ***Scan Specific Files or Folders*** - standard predefined scan of selected areas of your computer
- ***Removable Device Scan*** - specific scanning of removable devices attached to your computer

### 10.6.1. Scan Whole Computer

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




#### Scan settings

The ***Scan settings*** section offers a list of scanning parameters that can be optionally

switched on/off:

- ***Automatically heal/remove infection*** - if a virus is identified during scanning it can be healed automatically if a cure is available. If the infected file cannot be healed automatically, or if you decide to switch off this option, you will be notified upon a virus detection and will have to decide what to do with the detected infection. The recommended method is to remove the infected file to the Virus Vault.

- ***Report Potentially Unwanted Programs and Spyware Threats*** - this parameter controls the ***Anti-Virus*** functionality that allows detection of potentially unwanted programs (*executable files that can run as spyware or adware*) and these can then be blocked, or removed;

- ***Scan for Tracking Cookies*** - this parameter of the Anti-Spyware component defines that cookies should be detected; (*HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts*)

- ***Scan inside archives*** - this parameters defines that scanning should check all files even those stored inside archives, e.g. ZIP, RAR, ...

- ***Use Heuristics*** - heuristic analysis (*dynamic emulation of the scanned object's instructions in a virtual computer environment*) will be one of the methods used for virus detection during scanning;

- ***Scan system environment*** - scanning will also check the system areas of your computer.

Further you should decide whether you want to have scanned

- ***All file types*** with the possibility of defining exceptions from scanning by providing a list of comma separated file extensions that should not be scanned; or

- ***Selected file types*** - you can specify that you want to scan only files that are possibly infectable (*files that cannot get infected will not be scanned, for instance some plain text files, or some other non-executable files*), including media files (*video, audio files - if you leave this box unchecked, it will reduce the scanning time even more, because these files are often quite large and are not too likely to be infected by a virus*). Again, you can specify by extensions which files are those that should always be scanned.

- Optionally, you can decide you want to ***Scan files without extension*** - this option is on by default, and it is recommended that you keep it so unless you

have a real reason to change it. Files with no extension are rather suspicious and should be scanned at all times.

### Scan process priority

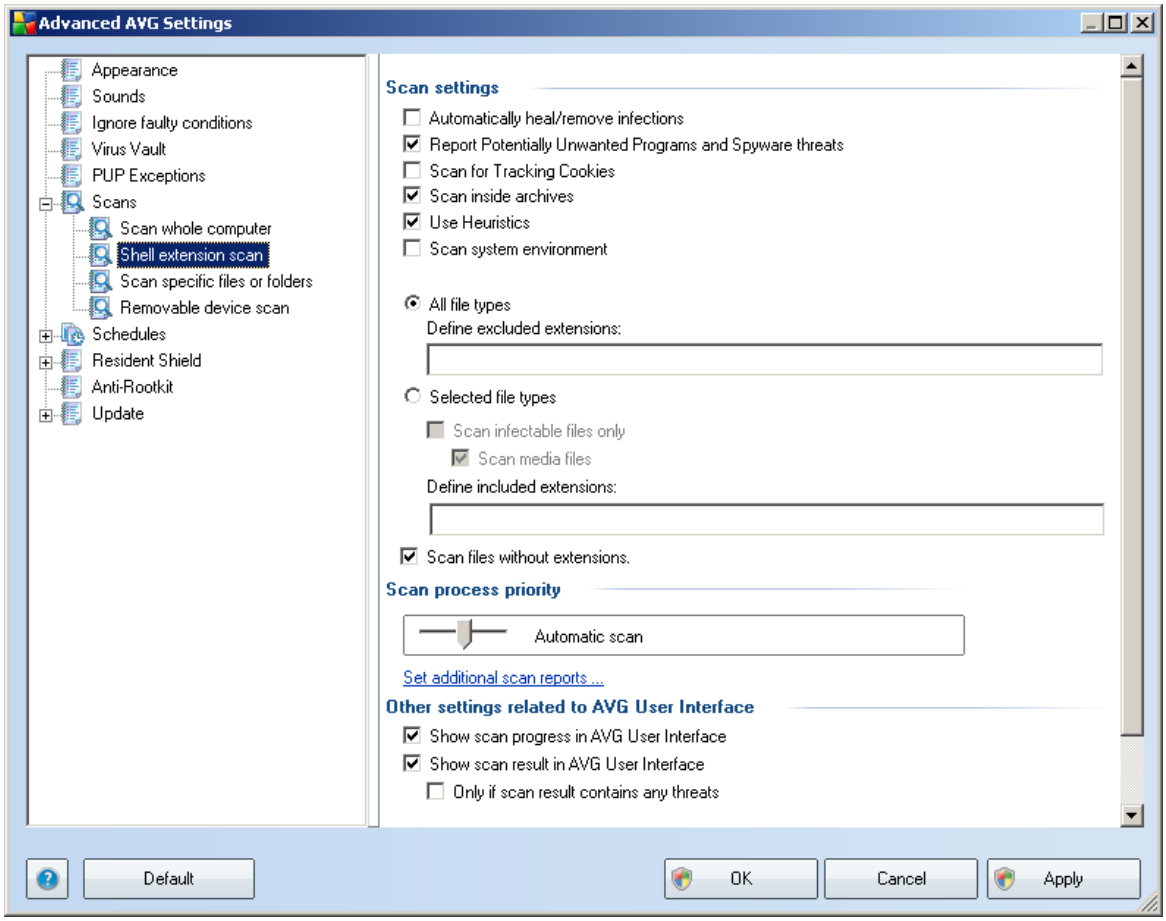
Within the ***Scan process priority*** section you can further specify the desired scanning speed dependent on system resource usage. By default, this option value is set to the medium level of automatic resource usage. If you want the scanning to run faster, it will take less time but system resources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

### Set additional scan reports ...

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

## 10.6.2. Shell Extension Scan

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

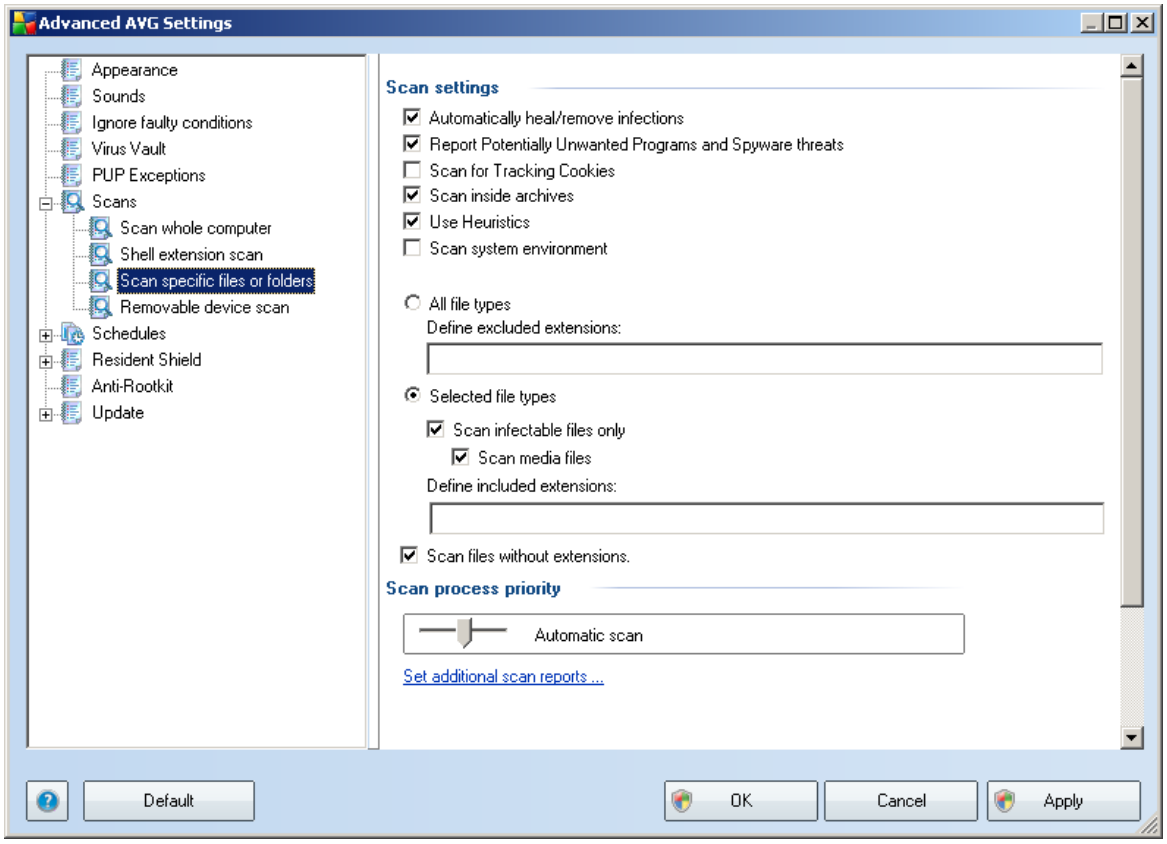



The list of parameters is identical to those available for the ***Scan of the whole computer***. However, the default settings differ: with the ***Scan of the Whole Computer*** most parameters are selected while for the ***Shell extension scan*** ( ***Scanning in Windows Explorer***) only the relevant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

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

### 10.6.3. Scan Specific Files or Folders

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

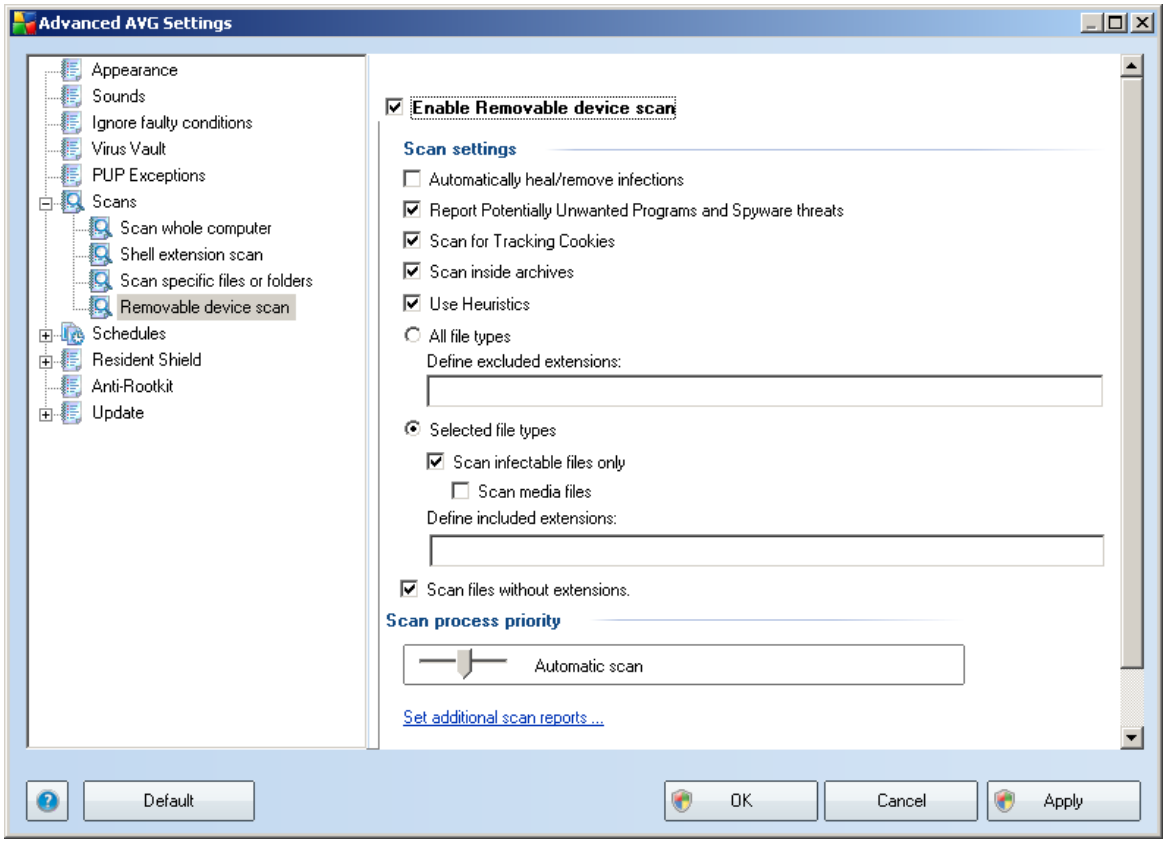



All parameters set up in this configuration dialog apply only to the areas selected for scanning with the ***Scan of specific files or folders***! If you tick the ***Scan for rootkits*** option within this configuration dialog, only a quick rootkit test will be performed, i.e. rootkit scanning of selected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

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

## 10.6.4. Removable Device Scan

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




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

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

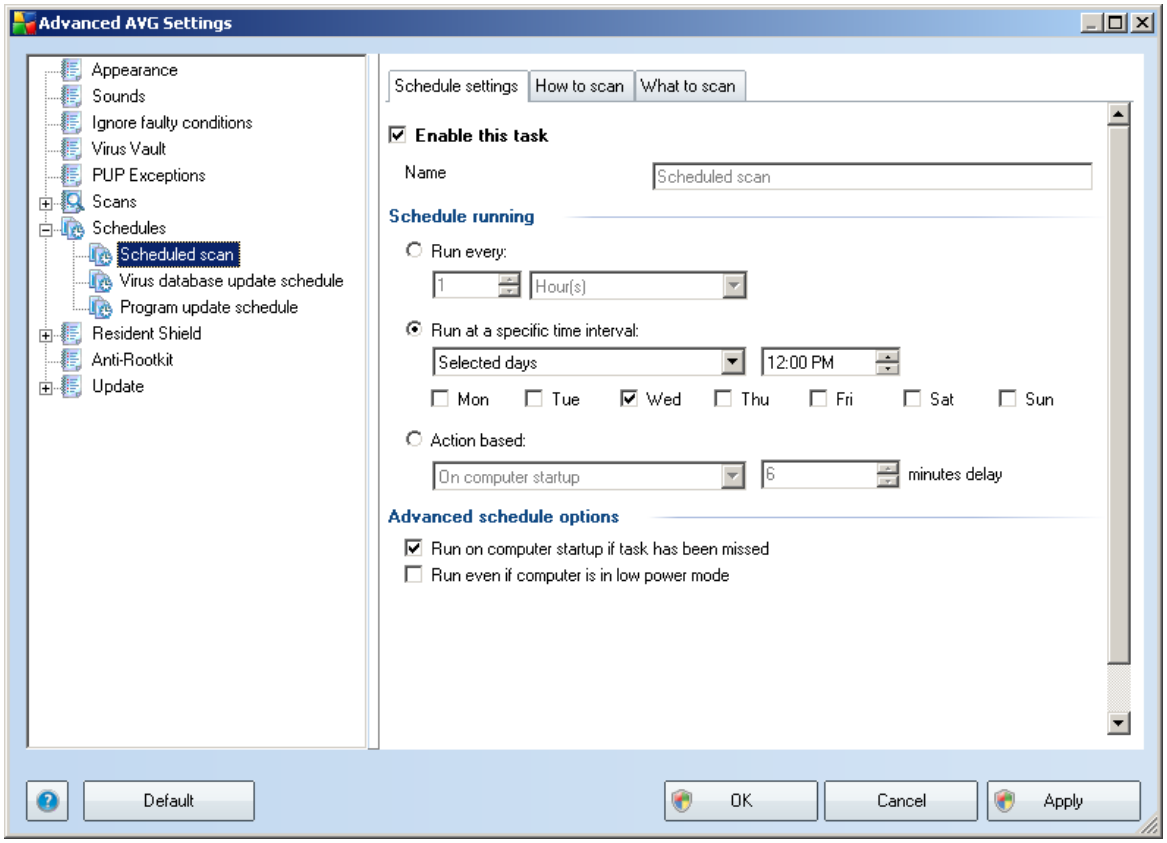
## 10.7. Schedules

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

- Whole computer scan schedule
- Virus database update schedule
- Program update schedule

### 10.7.1. Scheduled Scan

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




On the ***Schedule settings*** tab you can first check/uncheck the ***Enable this task*** item

to simply deactivate the scheduled test temporarily, and switch it on again as the need arises.

Next, in the text field called ***Name*** (*deactivated for all default schedules*) there is the name assigned to this very schedule by the program vendor. For newly added schedules (*you can add a new schedule by mouse right-click over the* ***Scheduled scan*** *item in the left navigation tree*) you can specify your own name, and in that case the text field will be open for editing. Try to always use brief, descriptive and apt names for scans to make it easier to later recognize the scan from others.

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

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

## Schedule running

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

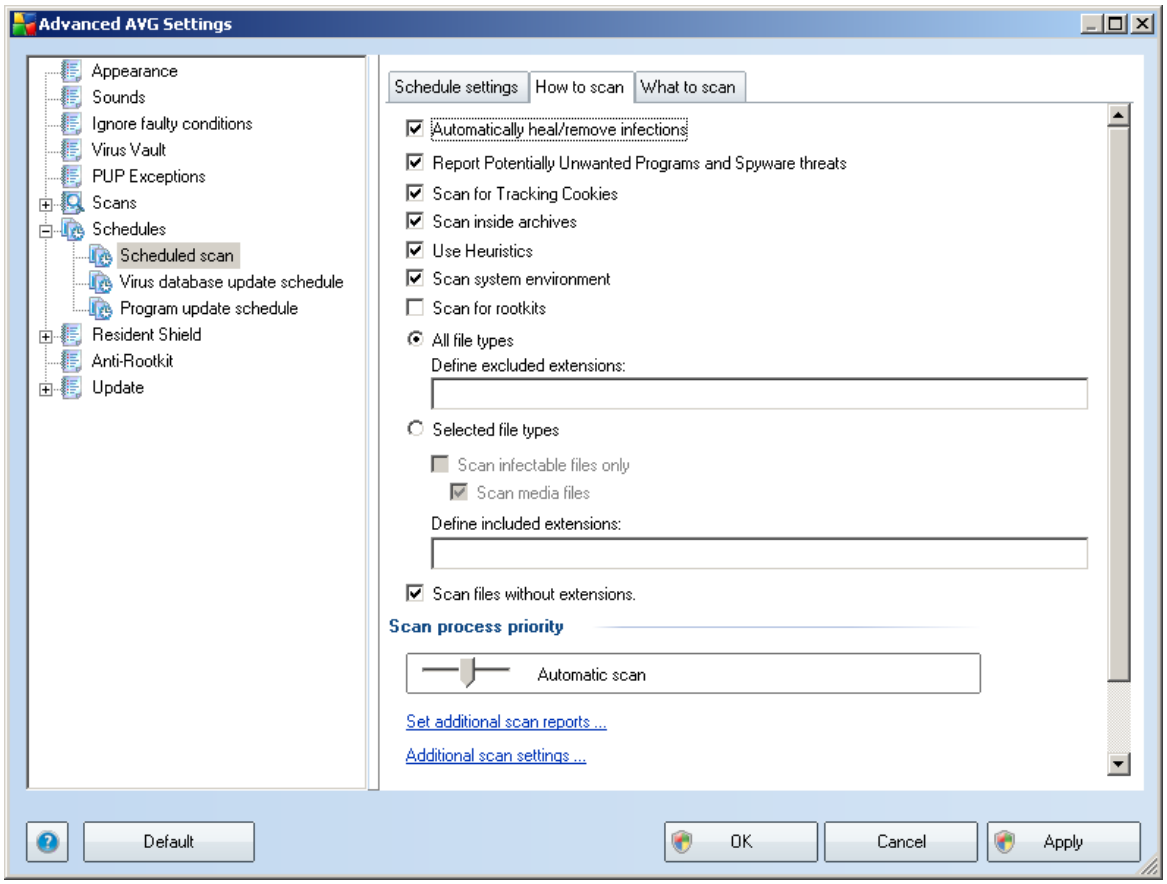
## Advanced schedule options

This section allows you to define under which conditions the scan should/should not be launched if the computer is in low power mode or switched off completely.

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

A new AVG system tray icon then appears (*in full color with a white arrow - see*

*picture above*) informing a scheduled scan is running.




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

- ***Automatically heal/remove infection*** - (*switched on, by default*): if a virus is identified during scanning it can be healed automatically if a cure is available . If the infected file cannot be healed automatically, or if you decide to switch off this option, you will be notified upon virus detection and will have to decide what to do with the detected infection. The recommended action is to remove the infected file to the Virus Vault.

- ***Report Potentially Unwanted Programs and Spyware Threats*** - (*switched*

*on, by default*): this parameter controls the Anti-Virus functionality that allows detection of potentially unwanted programs (*executable files that can run as spyware or adware*) and these can then be blocked, or removed;

- ***Scan for Tracking Cookies*** - (*switched on, by default*): this parameter of the Anti-Spyware component defines that cookies should be detected during scanning; (*HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts*)

- ***Scan inside archives*** - (*switched on, by default*): this parameter defines the scanning should check all files even if they are stored inside an archive, e.g. ZIP, RAR, ...

- ***Use Heuristics*** - (*switched on, by default*): heuristic analysis (*dynamic emulation of the scanned object's instructions in a virtual computer environment*) will be one of the methods used for virus detection during scanning;

- ***Scan system environment*** - (*switched on, by default*): scanning will also check the system areas of your computer;

- ***Scan for rootkits*** - tick this item if you want to include the rootkit detection into scanning of the entire computer. The rootkit detection is also available on its own within the ***Anti-Rootkit*** component;

Further you should decide whether you want to have scanned

- ***All file types*** with the possibility of defining exceptions from scanning by providing a list of comma separated file extensions that should not be scanned; or

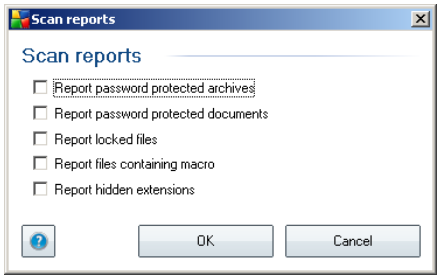
- ***Selected file types*** - you can specify that you want to scan only files that are possibly infectable (*files that cannot get infected will not be scanned, for instance some plain text files, or some other non-executable files*), including media files (*video, audio files - if you leave this box unchecked, it will reduce the scanning time even more, because these files are often quite large and are not too likely to be infected by a virus*). Again, you can specify by extensions which files are those that should always be scanned.

- Optionally, you can decide you want to ***Scan files without extension*** - this option is on by default, and it is recommended that you keep it so unless you have a real reason to change it. Files with no extension are rather suspicious and should be scanned at all times.

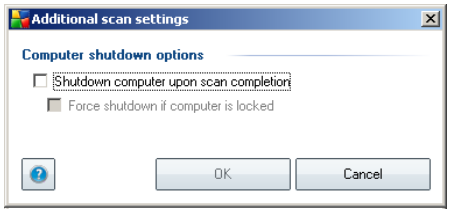
## Scan process priority

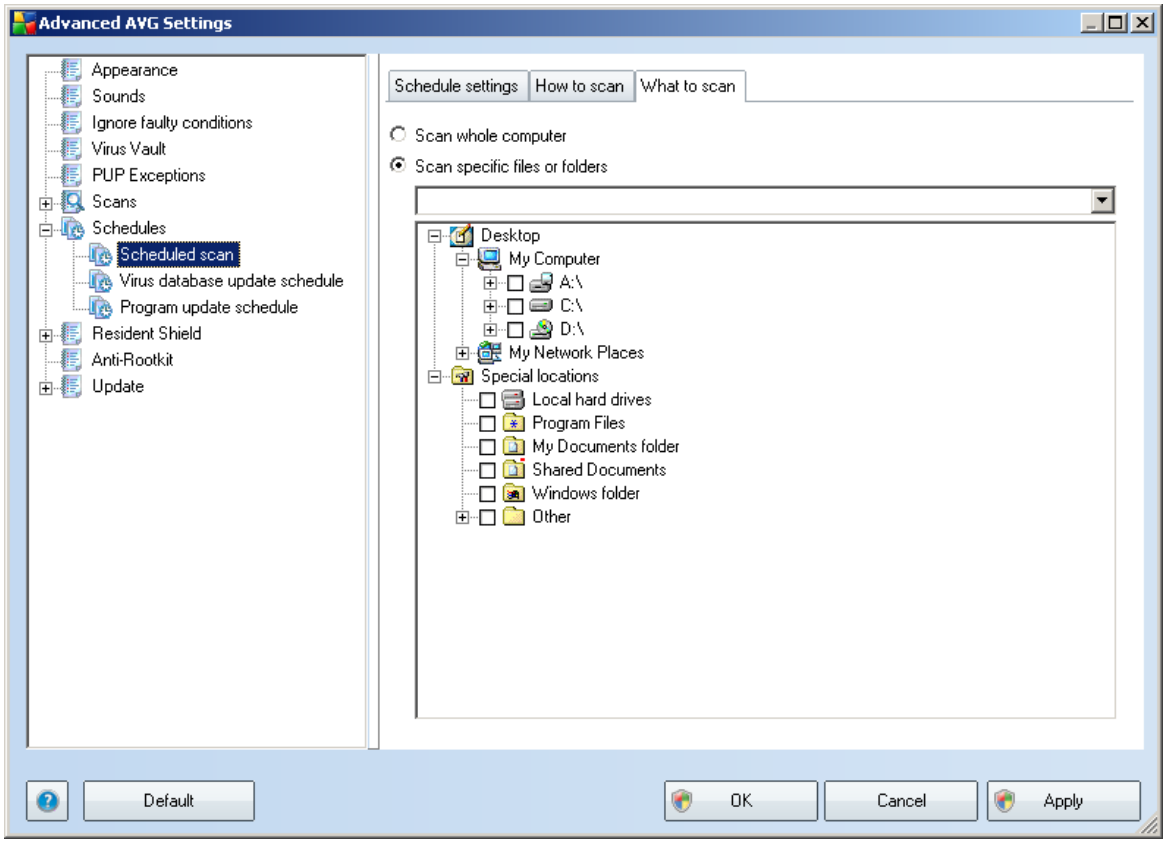
Within the ***Scan process priority*** section you can further specify the desired scanning speed dependent on system resource usage. By default, this option is set to the medium level of automatic resource usage. If you want the scanning to run faster, it will take less time but the system resources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

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



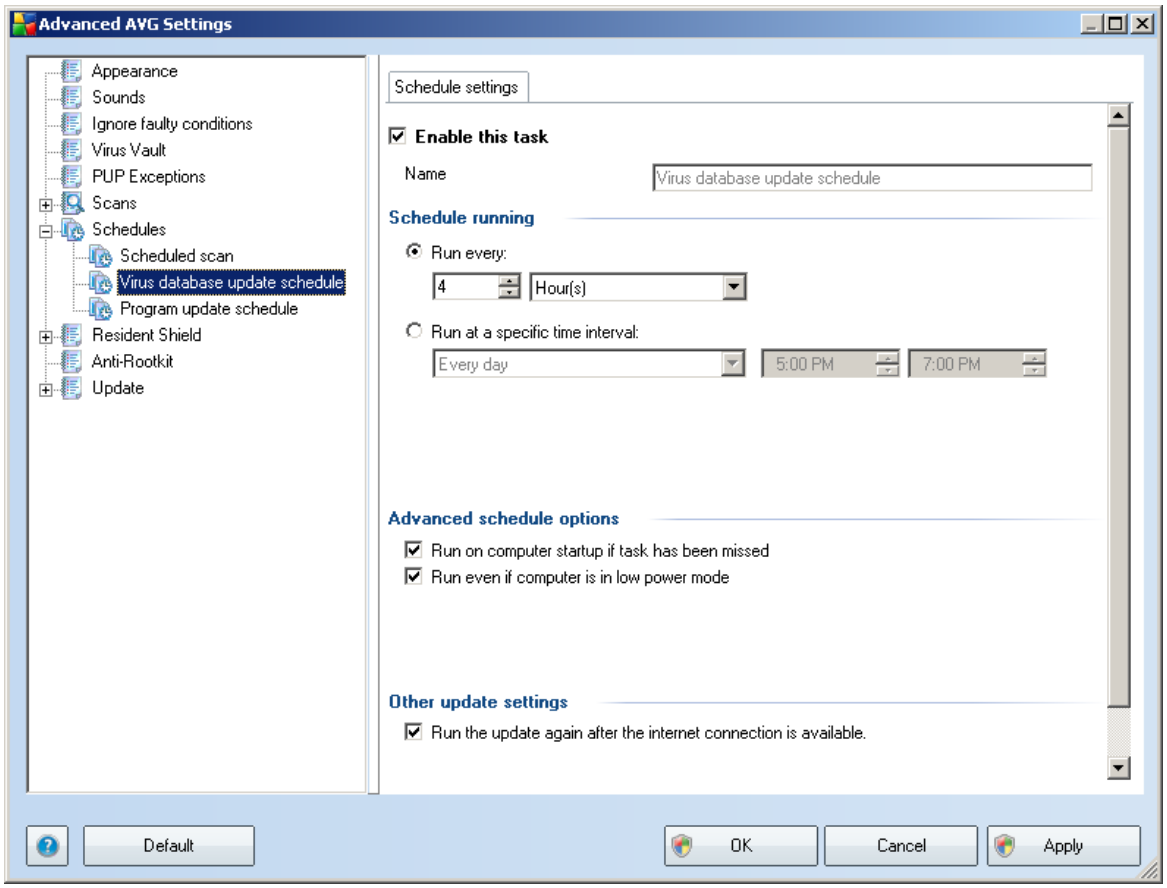

Click the ***Additional scan settings ...*** to open a new ***Computer shutdown options*** dialog where you can decide whether the computer should be shut down automatically once the running scanning process is over. Having confirmed this option (***Shutdown computer upon scan completion***), a new option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






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

## 10.7.2. Virus Database Update Schedule




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

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

In the text field called ***Name*** (*deactivated for all default schedules*) there is the name assigned to this very schedule by the program vendor. For newly added schedules ( *you can add a new schedule by mouse right-click over the* ***Virus database update schedule*** *item in the left navigation tree*) you can specify your own name, and in that case the text field will be open for editing. Try to always use brief, descriptive and apt names for your schedules to make it easier to later recognize them.

## Schedule running

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

## Advanced schedule options

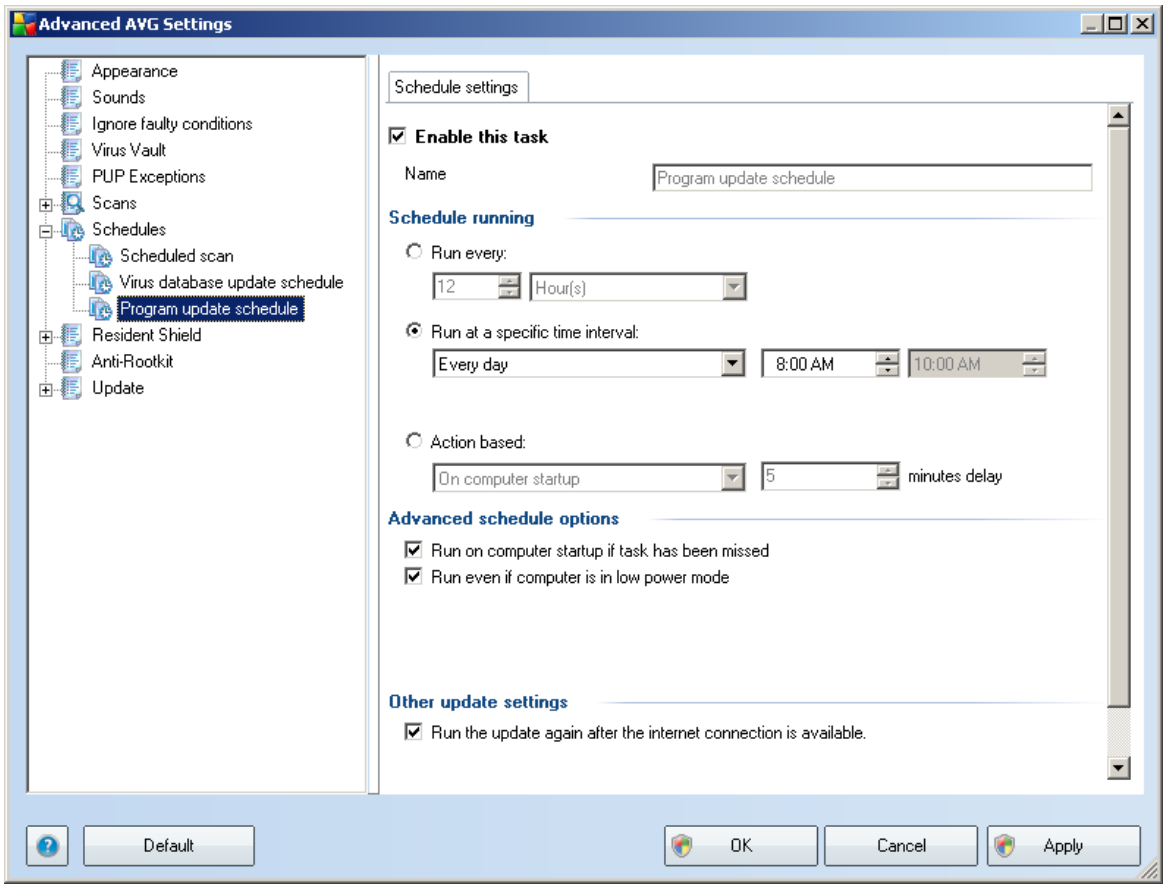
This section allows you to define under which conditions the virus database update should/should not be launched if the computer is in low power mode or switched off completely.

## Other update settings

Finally, check the ***Run the update again as soon as the Internet connection is available*** option to make sure than if the internet connection gets corrupted and the update process fails, it will be launched again immediately after the internet connection is restored.

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

## 10.7.3. Program Update Schedule




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

In the text field called ***Name*** (*deactivated for all default schedules*) there is the name assigned to this very schedule by the program vendor. For newly added schedules ( *you can add a new schedule by mouse right-click over the* ***Program update schedule*** *item in the left navigation tree*) you can specify your own name, and in that case the text field will be open for editing. Try to always use brief, descriptive and apt names for your schedules to make it easier to later recognize them.

### Schedule running

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

## Advanced schedule options

This section allows you to define under which conditions the program update should/ should not be launched if the computer is in low power mode or switched off completely.

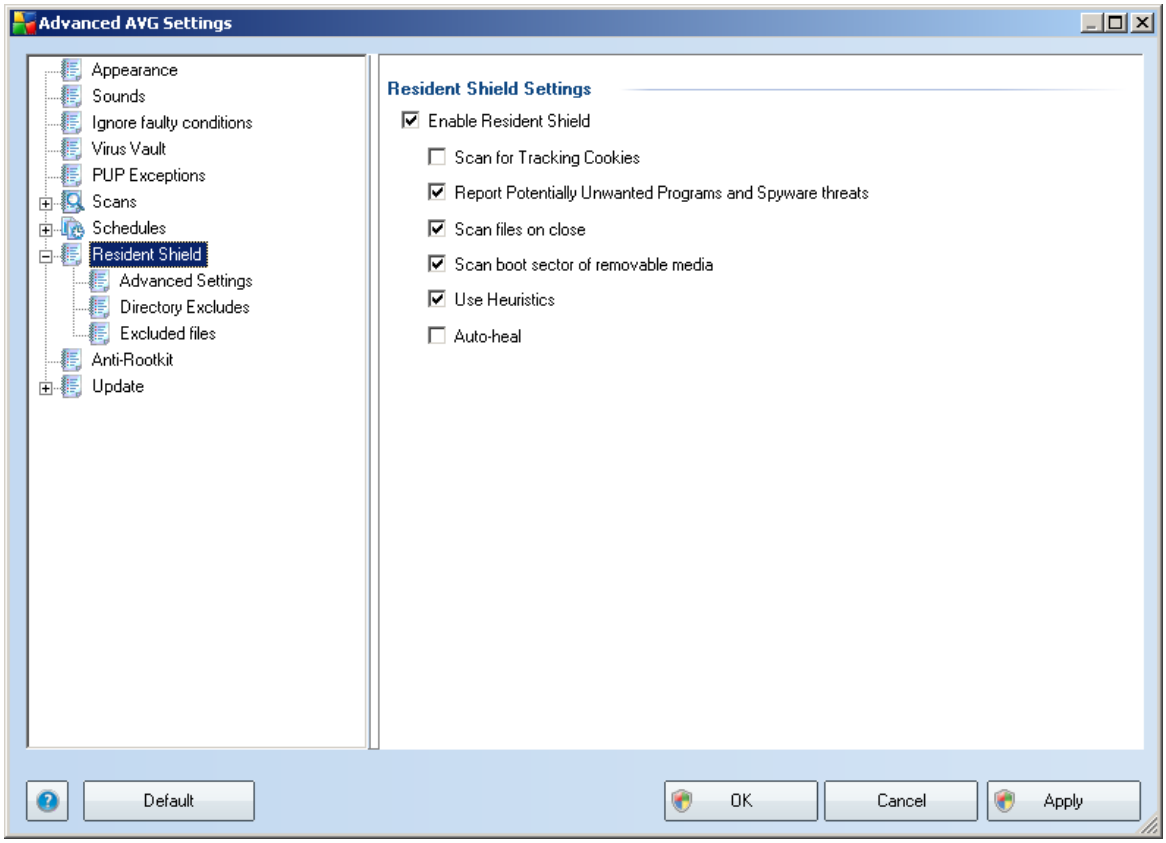
## Other update settings

Check the ***Run the update again as soon as the Internet connection is available*** option to make sure than if the internet connection gets corrupted and the update process fails, it will be launched again immediately after the internet connection is restored.

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

## 10.8. Resident Shield

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




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

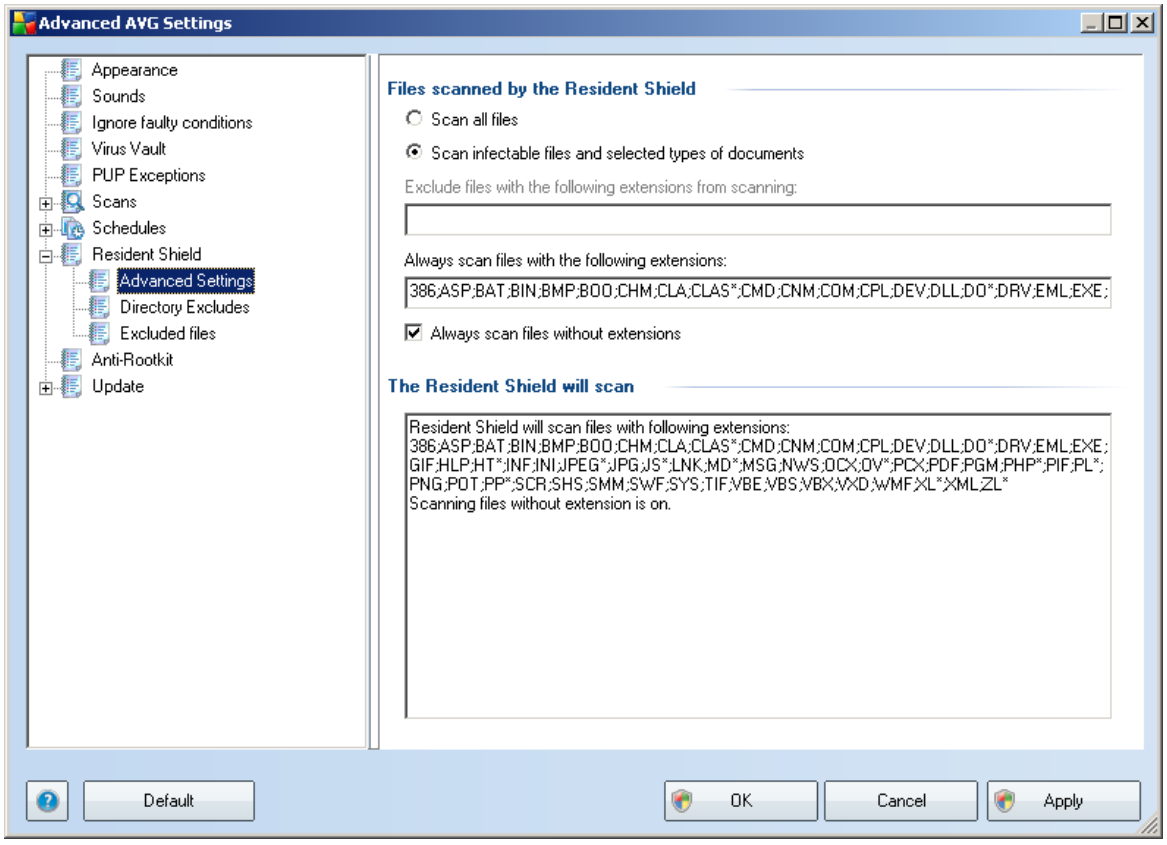
- ***Scan for Tracking cookies*** - this parameter defines that cookies should be detected during scanning. (*HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts*)
- ***Report Potentially Unwanted Programs and Spyware Threats*** - (*switched on by default*) scanning for potentially unwanted programs (*executable*

*applications that can behave as various types of spyware or adware*)

- ***Scan files on close*** - on-close scanning ensures that AVG scans active objects (e.g. applications, documents …) when they are being opened, and also when they are being closed; this feature helps you protect your computer against some types of sophisticated virus
- ***Scan boot sector of removable media*** - (*switched on by default*)
- ***Use Heuristics*** - (*switched on by default*) heuristic analysis will be used for detection (*dynamic emulation of the scanned object's instructions in a virtual computer environment*)
- ***Auto-heal*** - any detected infection will be healed automatically if there is a cure available

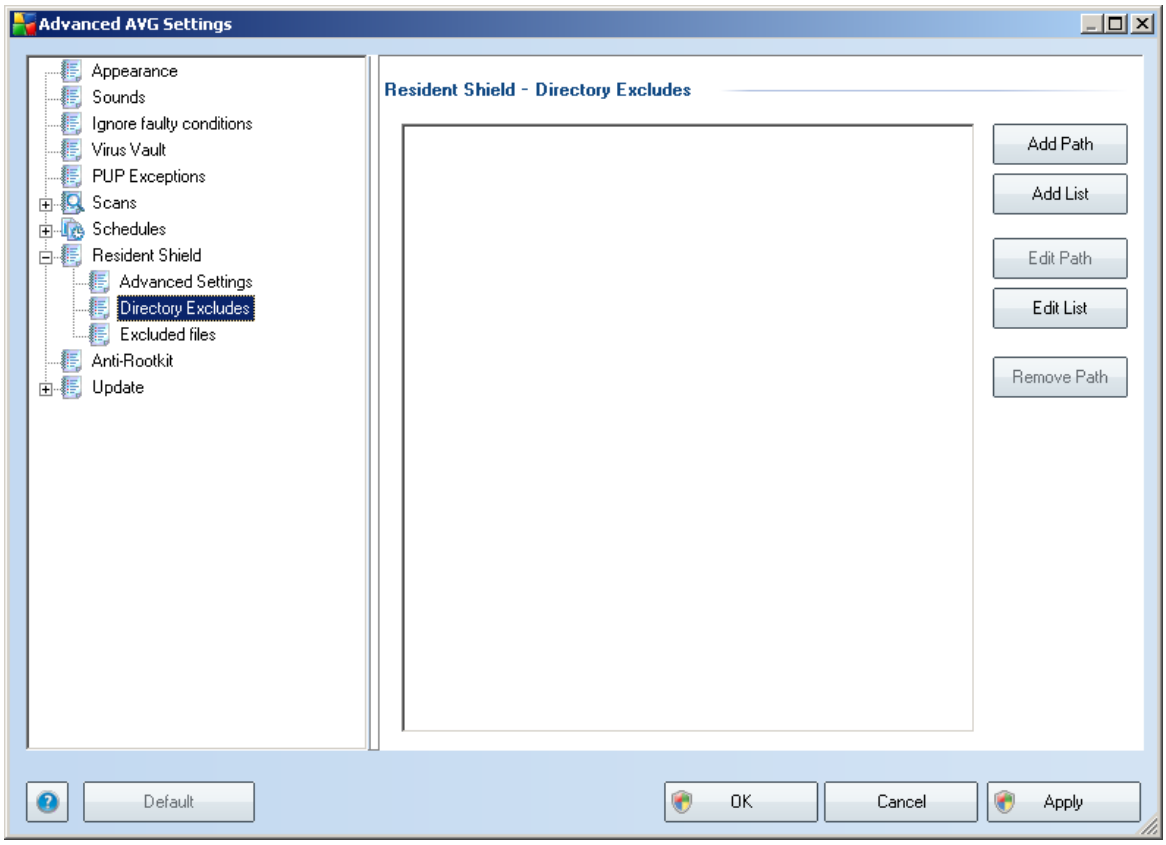
### 10.8.1. Advanced Settings

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




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

## 10.8.2. Directory Exludes




The ***Resident Shield - Directory Excludes*** dialog offers the possibility of defining folders that should be excluded from the ***Resident Shield*** scanning.

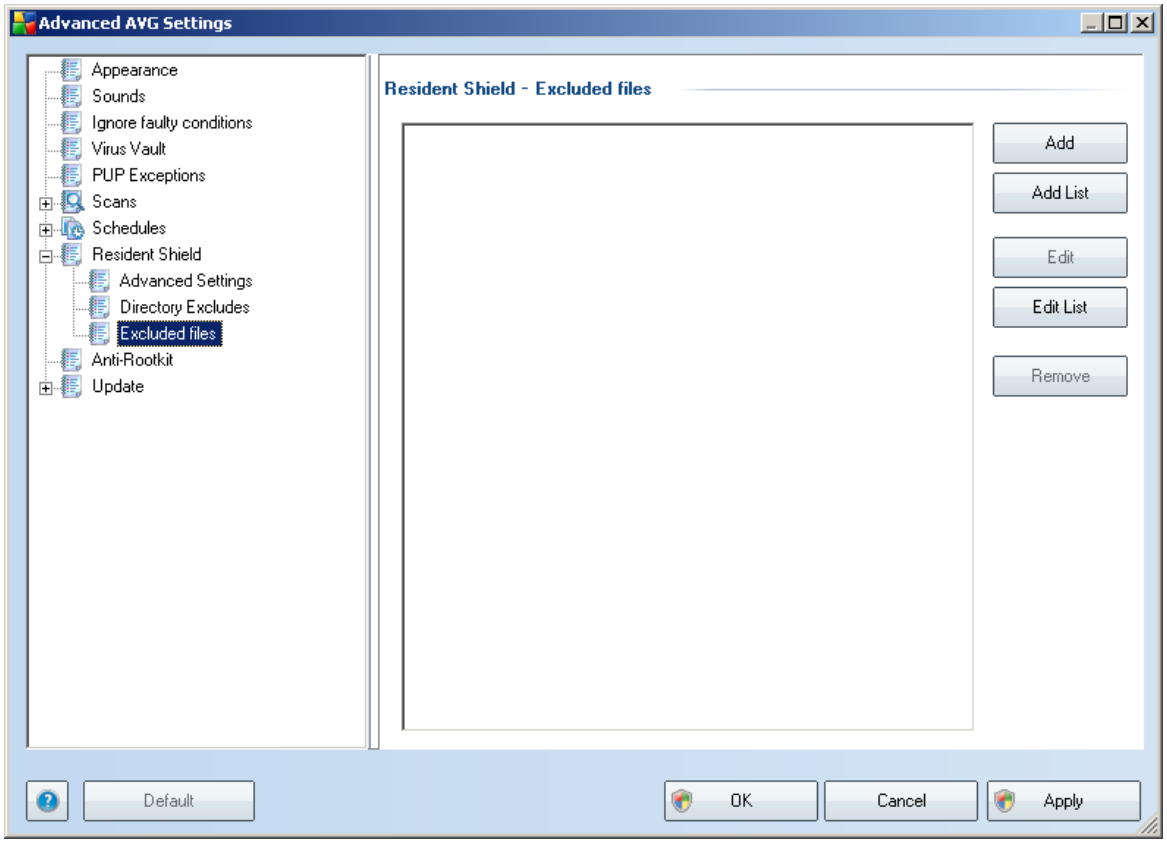
***If this is not essential, we strongly recommend not excluding any directories!***

The dialog provides the following control buttons:

- ***Add path*** – specify directories to be excluded from the scanning by selecting them one by one from the local disk navigation tree
- ***Add list*** – allows you to enter a whole list of directories to be excluded from the ***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

### 10.8.3. Excluded Files




The ***Resident Shield - Excluded files*** dialog behaves just like the previously described ***Resident Shield - Directory Excludes*** but instead of folders you can now define specific files that should be excluded from the ***Resident Shield*** scanning.

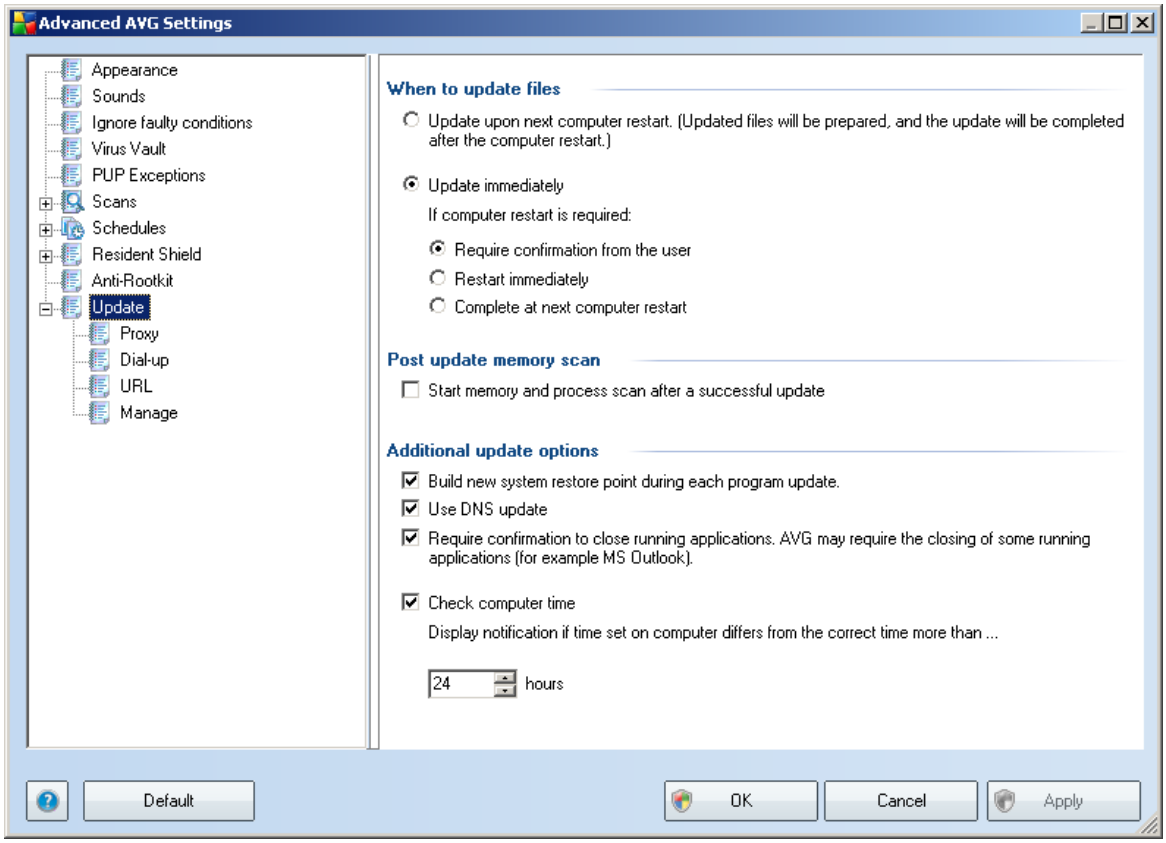
***If this is not essential, we strongly recommend not excluding any files!***

The dialog provides the following control buttons:

- ***Add*** – specify directories to be excluded from the scanning by selecting them one by one from the local disk navigation tree
- ***Add list*** – allows you to enter a whole list of directories to be excluded from the ***Resident Shield*** scanning

- ***Edit*** – allows you to edit the specified path to a selected folder
- ***Edit list*** – allows you to edit the list of folders
- ***Remove*** – allows you to delete the path to a selected folder from the list

## 10.9. Update




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

### When to update files

In this section you can select between two alternative options: update can be scheduled for the next PC restart or you can launch the update immediately. By default, the immediate update option is selected since this way AVG can secure the

maximum safety level. Scheduling an update for the next PC restart can only be recommended if you are sure the computer gets restarted regularly, at least daily.

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

- ***Require confirmation from the user*** - you will be asked to approve a PC restart needed to finalize the update process
- ***Restart immediately*** - the computer will be restarted automatically immediately after the update process has finished, and your approval will not be required
- ***Complete at next computer restart*** - the update process finalization will be postponed until the next computer restart - again, please keep in mind that this option is only recommended if you can be sure the computer gets restarted regularly, at least daily

## Post update memory scan

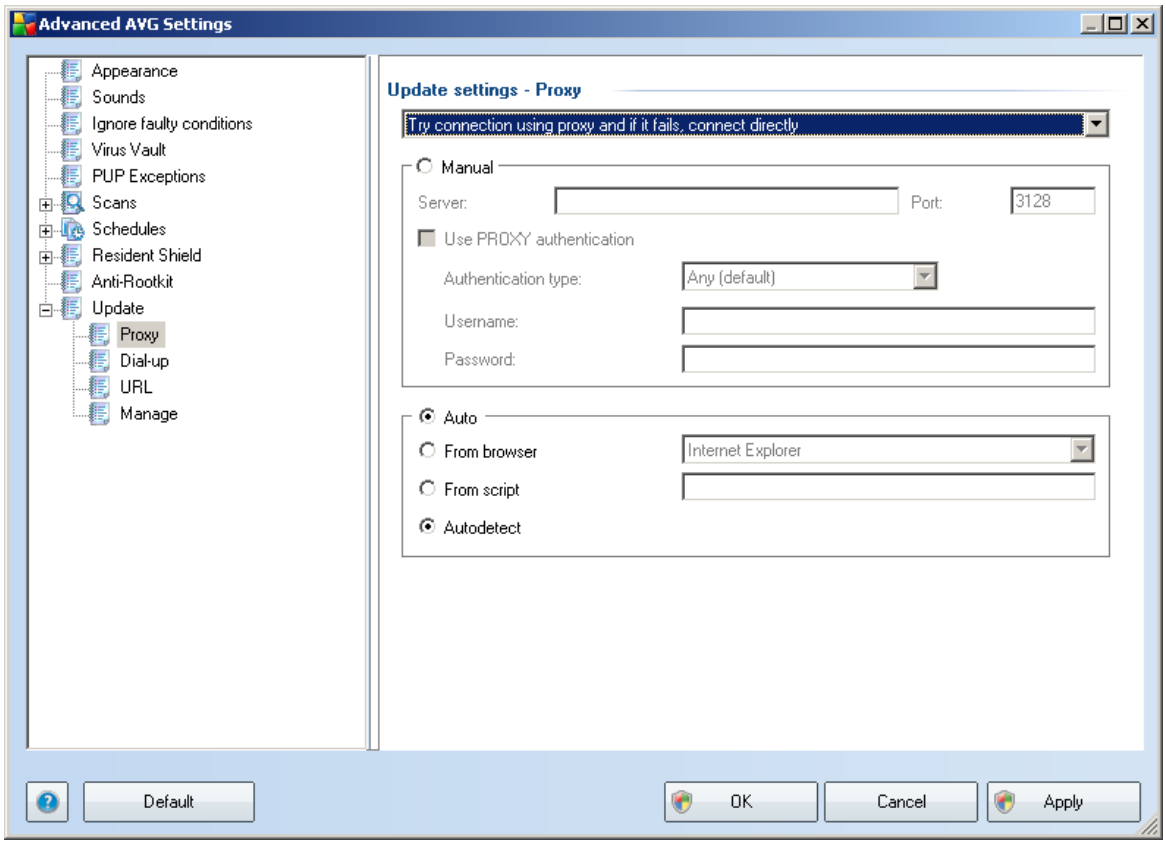
Mark this check box to define you want to launch a new memory scan after each successfully completed update. The latest downloaded update might have contained new virus definitions, and these could be applied in the scanning immediately.

## Additional update options

- ***Build new system restore point after each program update*** - before each AVG program update launch, a system restore point is created. In case the update process fails and your operating system crashes you can always restore your OS in its original configuration from this point. This option is accessible via Start / All Programs / Accessories / System tools / System Restore, but any changes can be recommended to experienced users only! Keep this check-box ticked if you want to make use of this functionality.
- ***Use DNS update*** - mark this check box to confirm you want to use the update files detection method that eliminates data amount transferred between the update server and AVG client;
- ***Require confirmation to close running applications*** (*switched on by default*) will help you make sure no currently running applications will be closed without your permission - if required for the update process to be finalized;

- ***Check computer time*** - mark this option to declare you wish to have notification displayed in case the computer time differs from the correct time more than specified number of hours.

### 10.9.1. 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. Then, in the first item of the ***Update settings - Proxy*** dialog you have to select from the combo box menu whether you want to:

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

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

## Manual configuration

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

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

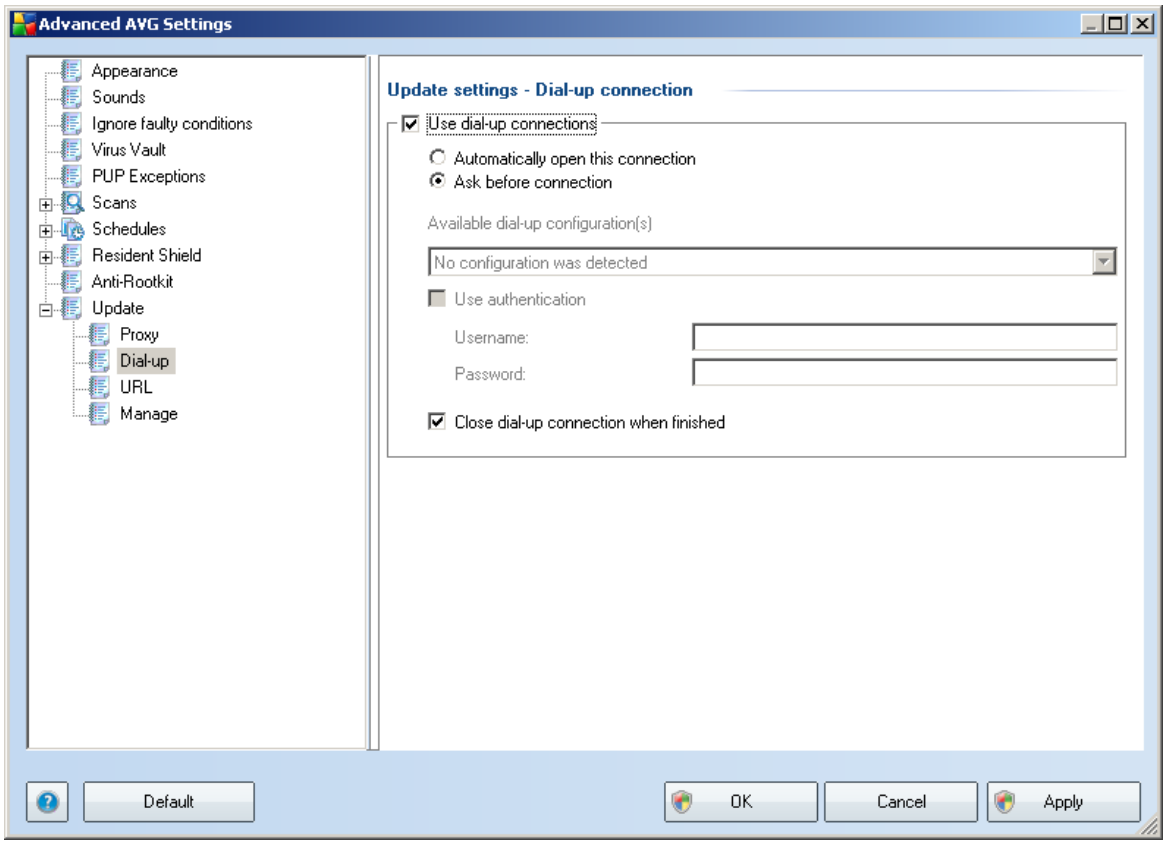
The proxy server can also have configured specific rules for each user. If your proxy server is set up this way, check the ***Use PROXY authentication*** option to verify that your user name and password are valid for connecting to the Internet via the proxy server.

## Automatic configuration

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

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

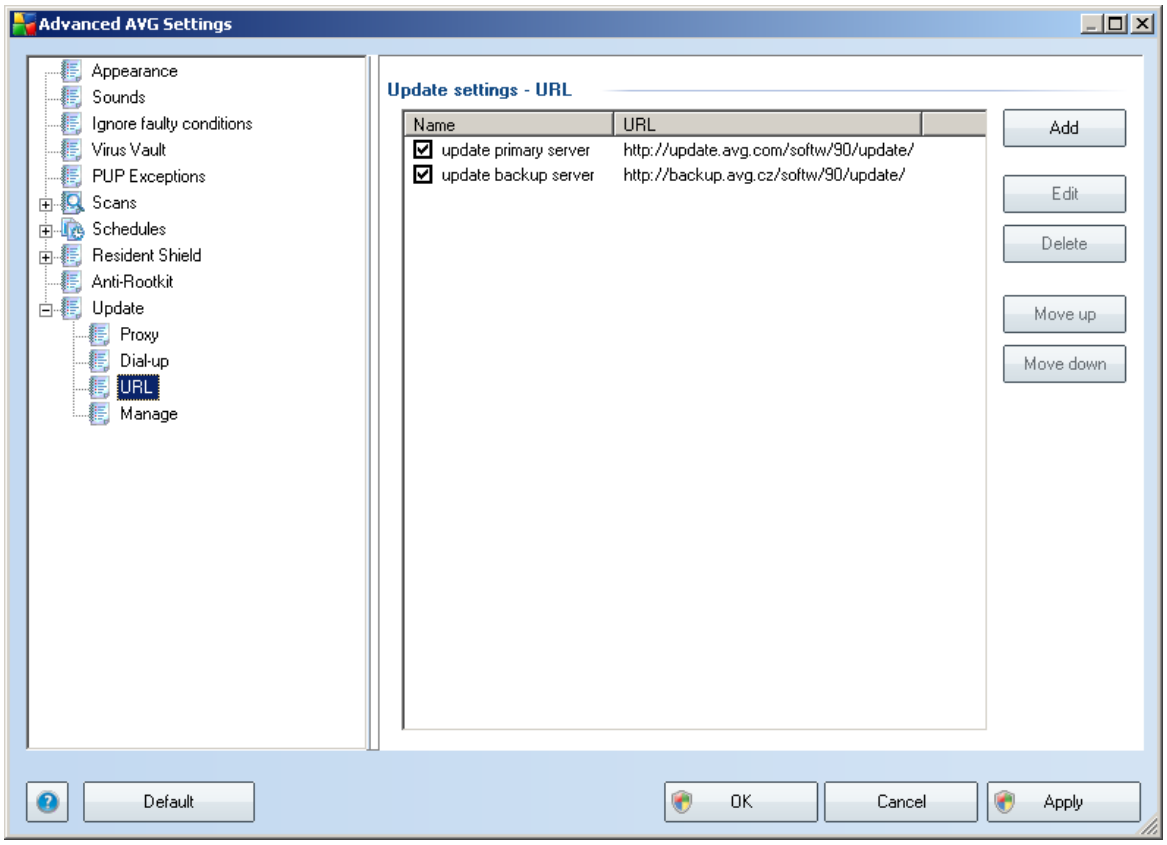
### 10.9.2. Dial-up




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

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

### 10.9.3. URL

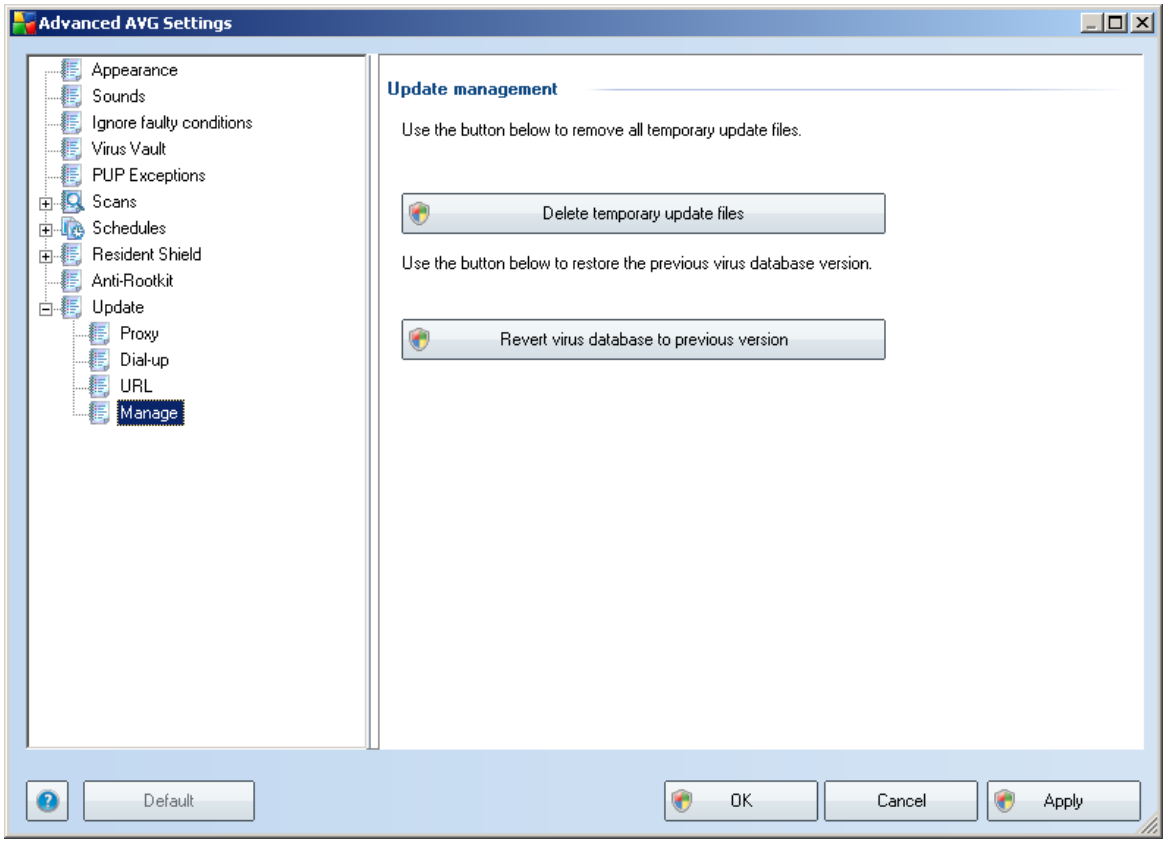



The ***URL*** dialog offers a list of Internet addresses from which the update files can be downloaded. The list and its items can be modified using the following control buttons:

- ***Add*** – opens a dialog where you can specify a new URL to be added to the list
- ***Edit*** - opens a dialog where you can edit the selected URL parameters
- ***Delete*** – deletes the selected URL from the list
- ***Move Up*** – moves the selected URL one position up in the list
- ***Move Down*** - moves the selected URL one position down in the list

### 10.9.4. Manage

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

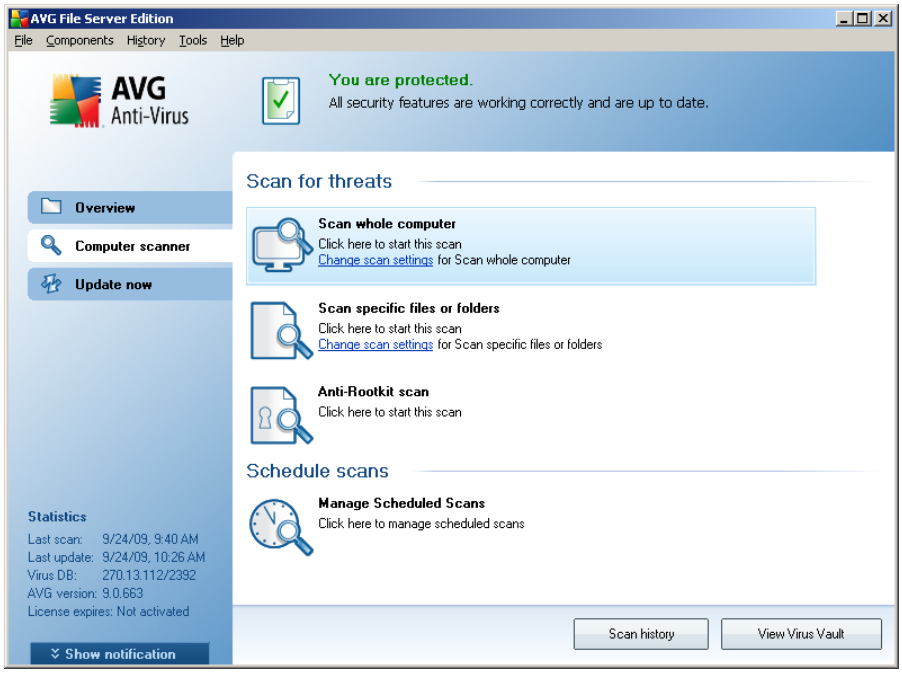



- ***Delete temporary update files*** - press this button to delete all redundant update files from your hard disk (*by default, these files are being saved for 30 days*)
- ***Revert virus database to previous version*** – press this button to delete the latest virus base version from your hard disk,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

# 11. AVG Scanning

Scanning is a crucial part of **AVG 9.0 File Server** functionality. You can run on-demand tests or schedule them to run periodically at convenient times.

## 11.1. Scanning Interface




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

- overview of predefined scans - three types of scans defined by the software vendor are ready to be used immediately on demand or scheduled:
  - ***Scan whole computer***
  - ***Scan specific files or folders***
  - ***Anti-Rootkit scan***
- scan scheduling section - where you can define new tests and create new schedules as needed.

### Control buttons

Control buttons available within the testing interface are the following:

- ***Scan history*** - displays the Scan results overview dialog with the entire history of scanning
- ***View Virus Vault*** - opens a new window with the Virus Vault - a space where detected infections are quarantined

## 11.2. Predefined Scans

One of the main features of **AVG 9.0 File Server** is on-demand scanning. On-demand tests are designed to scan various parts of your computer whenever suspicion of possible virus infection arises. Anyway, it is strongly recommended to carry out such tests regularly even if you think that no virus can be found on your computer.

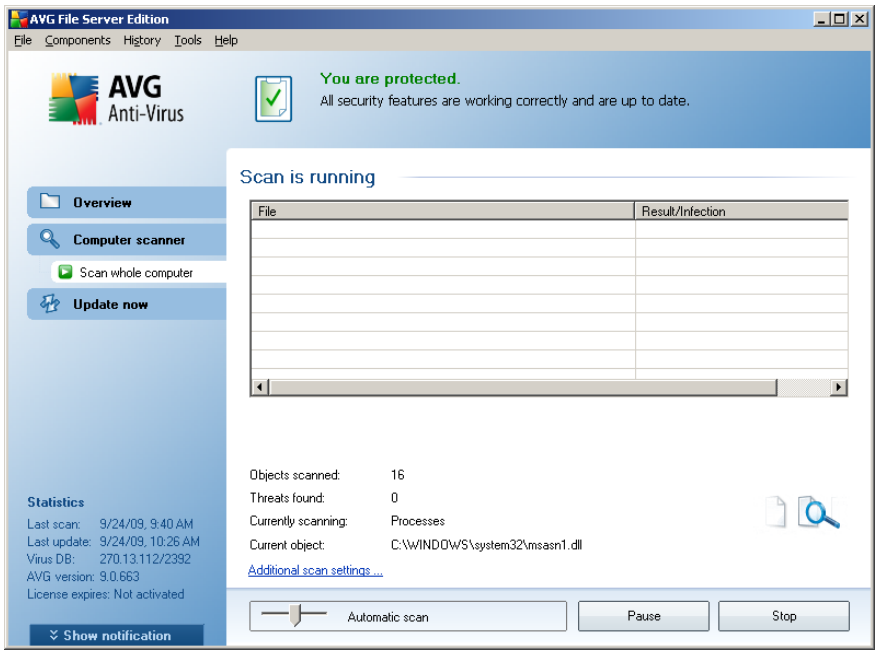
In the **AVG 9.0 File Server** you will find the following types of scanning predefined by the software vendor:

### 11.2.1. Scan Whole Computer

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

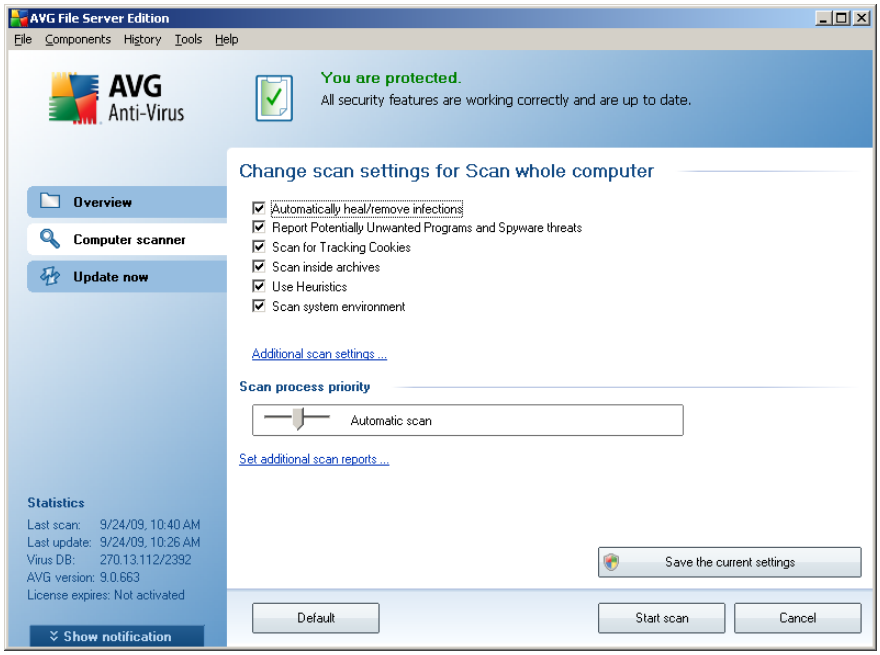
### Scan launch

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



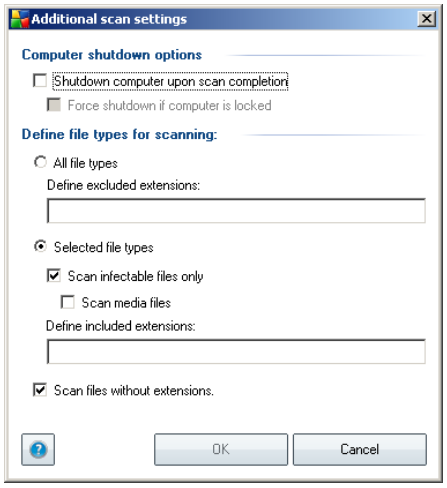

## Scan configuration editing

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




- ***Scanning parameters*** - in the list of scanning parameters you can switch on/ off specific parameters as needed. By default, most of the parameters are switched on and these will be used automatically during scanning.

- ***Additional scan settings*** - the link opens a new ***Additional scan settings*** dialog where you can specify the following parameters:



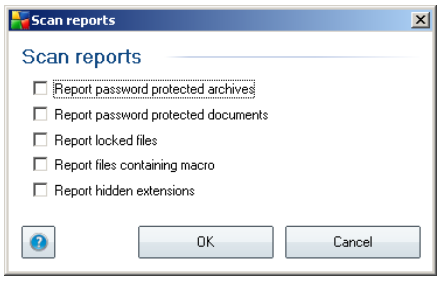

  - ***Computer shutdown options*** - decide whether the computer should be

shut down automatically once the running scanning process is over. Having confirmed this option (***Shutdown computer upon scan completion***), a new option activates that allows the computer to shut down even if it is currently locked (***Force shutdown is computer is locked***).

- ***Define file types for scanning*** - further you should decide whether you want to have scanned:
  - ***All file types*** with the possibility of defining exceptions from scanning by providing a list of comma separated file extensions that should not be scanned; or
  - ***Selected file types*** - you can specify that you want to scan only files that are possibly infectable (*files that cannot get infected will not be scanned, for instance some plain text files, or some other non-executable files*), including media files (*video, audio files - if you leave this box unchecked, it will reduce the scanning time even more, because these files are often quite large and are not too likely to be infected by a virus*). Again, you can specify by extensions which files are those that should always be scanned.
  - Optionally, you can decide you want to ***Scan files without extension*** - this option is on by default, and it is recommended that you keep it so unless you have a real reason to change it. Files with no extension are rather suspicious and should be scanned at all times.

- ***Scan process priority*** - you can use the slider to change the scanning process priority. By default, the priority is set to medium level (*Automatic scan* ) that optimizes the scanning process speed and the use of system resources. Alternatively, you can run the scanning process slower which means the system resources load will be minimized (*useful when you need to work on the computer but you do not care so much how long the scanning takes*), or faster with increased system resources requirements (*e.g. when the computer is temporarily unattended*).

- ***Set additional scan reports*** - the link opens a new ***Scan reports*** dialog where you can select what types of possible findings should be reported:




***Warning:*** *These scan settings are identical to the parameters of a newly defined scan - as described in the chapter* ***AVG Scanning / Scan scheduling/ How to Scan****. Should you decide to change the default configuration of the* ***Scan the whole computer*** *you can then save your new setting as the default configuration to be used for all further scans of the whole computer.*

## 11.2.2. Scan Specific Files or Folders

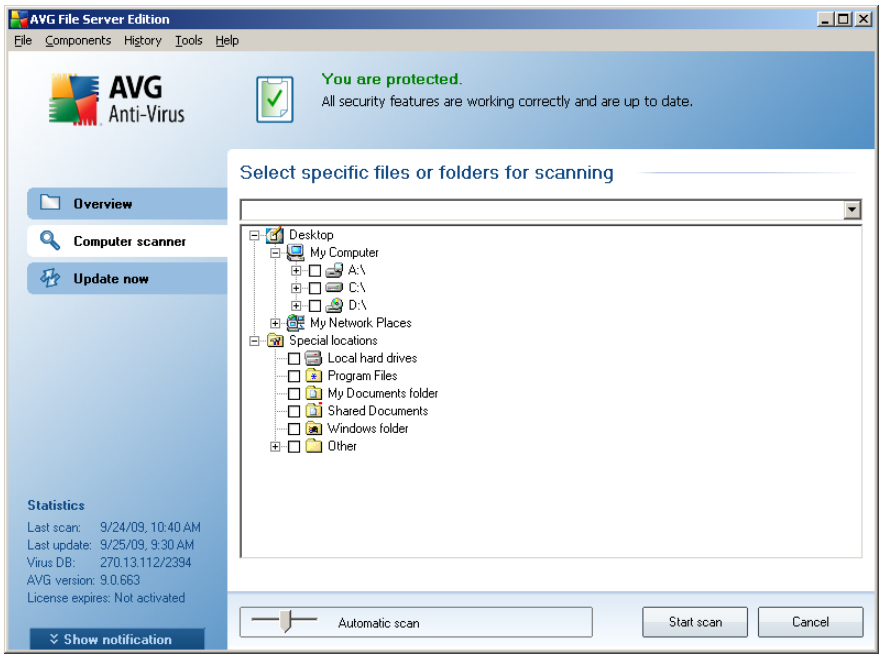
***Scan specific files or folders*** - scans only those areas of your computer that you have selected to be scanned (*selected folders, hard disks, floppy discs, CDs, etc.*). The scanning progress in case of virus detection and its treatment is the same as with the scan of the whole computer: any virus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

### Scan launch

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

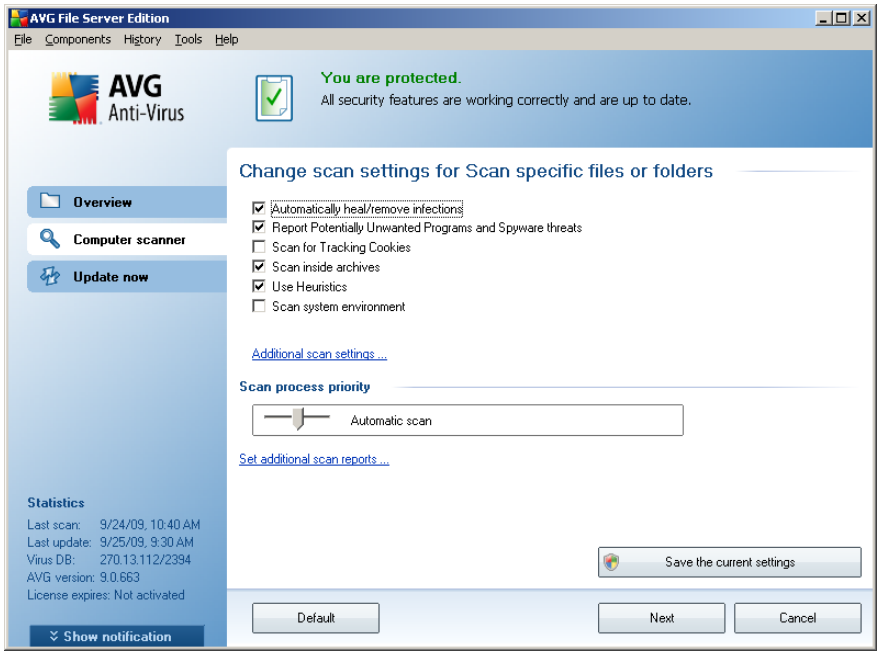
There is also a possibility of having a specific folder scanned while all its subfolders are excluded from this scanning; to do that write a minus sign "**-**" in front of the automatically generated path (*see screenshot*). To exclude the entire folder from scanning use the "!" parameter.

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



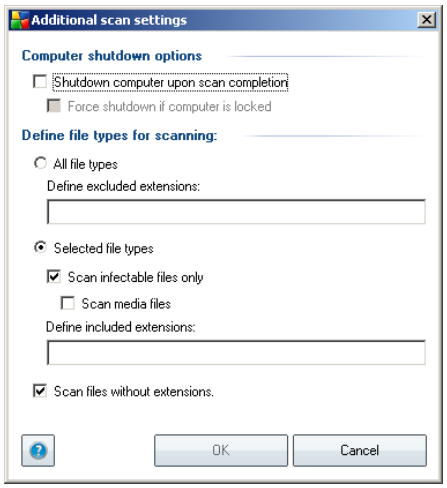

## Scan configuration editing

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




- ***Scanning parameters*** - in the list of scanning parameters you can switch on/off specific parameters as needed (*for detailed description of this settings please consult chapter AVG Advanced Settings / Scans / Scan Specific Files or Folders*).

- ***Additional scan settings*** - the link opens a new Additional scan settings dialog where you can specify the following parameters:



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

- ***Define file types for scanning*** - further you should decide whether you want to have scanned:

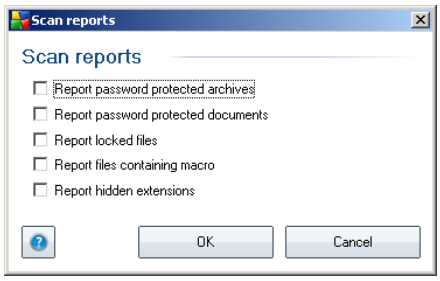
  - ***All file types*** with the possibility of defining exceptions from scanning by providing a list of comma separated file extensions that should not be scanned; or

  - ***Selected file types*** - you can specify that you want to scan only files that are possibly infectable (*files that cannot get infected will not be scanned, for instance some plain text files, or some other non-executable files*), including media files (*video, audio files - if you leave this box unchecked, it will reduce the scanning time even more, because these files are often quite large and are not too likely to be infected by a virus*). Again, you can specify by extensions which files are those that should always be scanned.

  - Optionally, you can decide you want to ***Scan files without extension*** - this option is on by default, and it is recommended that you keep it so unless you have a real reason to change it. Files with no extension are rather suspicious and should be scanned at all times.

- ***Scan process priority*** - you can use the slider to change the scanning process priority. By default, the priority is set to medium level (*Automatic scan* ) that optimizes the scanning process speed and the use of system resources. Alternatively, you can run the scanning process slower which means the system resources load will be minimized (*useful when you need to work on the computer but you do not care so much how long the scanning takes*), or faster with increased system resources requirements (*e.g. when the computer is temporarily unattended*).

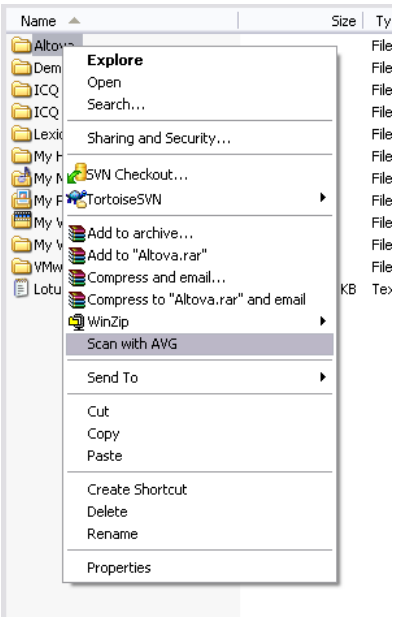
- ***Set additional scan reports*** - the link opens a new ***Scan Reports*** dialog where you can select what types of possible findings should be reported:




***Warning:*** *These scan settings are identical to the parameters of a newly defined scan - as described in the chapter* ***AVG Scanning / Scan scheduling/ How to Scan****. Should you decide to change the default configuration of the* ***Scan specific files or folders*** *you can then save your new setting as the default configuration to be used for all further scans of specific files or folders. Also, this configuration will be used as a template for all of your newly scheduled scans (all customized scans are based on the current configuration of the Scan of selected files or folders).*

## 11.3. Scanning in Windows Explorer

Besides the pre-defined scans launched for the entire computer or its selected areas, **AVG 9.0 File Server** also offers the option of quick scanning of a specific object directly in the Windows Explorer environment. If you want to open an unknown file and you cannot be sure of its content, you may want to have it checked on demand. Follow these steps:



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

## 11.4. Command Line Scanning

Within **AVG 9.0 File Server** there is the option of running the scan from the command line. You can use this option for instance on servers, or when creating a batch script to be launched automatically after the computer boot. From the command line, you can launch the scanning with most parameters as offered in AVG graphical user interface.

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

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

### Syntax of the command

The syntax of the command follows:

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

### Scanning parameters

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

more detailed explanation of the options, see the command line parameters overview.

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

### CMD scanning launched from graphic interface

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

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

## 11.4.1. CMD Scan Parameters

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

- ***/SCAN*** Scan specific files or folders /SCAN=path;path (e.g. /SCAN=C:\;D:\)
- ***/COMP*** Scan whole computer
- ***/HEUR*** Use heuristic analyse
- ***/EXCLUDE*** Exclude path or files from scan
- ***/@*** Command file /file name/
- ***/EXT*** Scan these extensions /for example EXT=EXE,DLL/
- ***/NOEXT*** Do not scan these extensions /for example NOEXT=JPG/
- ***/ARC*** Scan archives
- ***/CLEAN*** Clean automatically
- ***/TRASH*** Move infected files to the Virus Vault
- ***/QT*** Quick test
- ***/MACROW*** Report macros

- ***/PWDW*** Report password-protected files
- ***/IGNLOCKED*** Ignore locked files
- ***/REPORT*** Report to file /file name/
- ***/REPAPPEND*** Append to the report file
- ***/REPOK*** Report uninfected files as OK
- ***/NOBREAK*** Do not allow CTRL-BREAK to abort
- ***/BOOT*** Enable MBR/BOOT check
- ***/PROC*** Scan active processes
- ***/PUP*** Report "Potentially unwanted programs"
- ***/REG*** Scan registry
- ***/COO*** Scan cookies
- ***/?*** Display help on this topic
- ***/HELP*** Display help on this topic
- ***/PRIORITY*** Set scan priority /Low, Auto, High/ (see Advanced settings / Scans)
- ***/SHUTDOWN*** Shutdown computer upon scan completion
- ***/FORCESHUTDOWN*** Force computer shutdown upon scan completion
- ***/ADS*** Scan Alternate Data Streams (NTFS only)

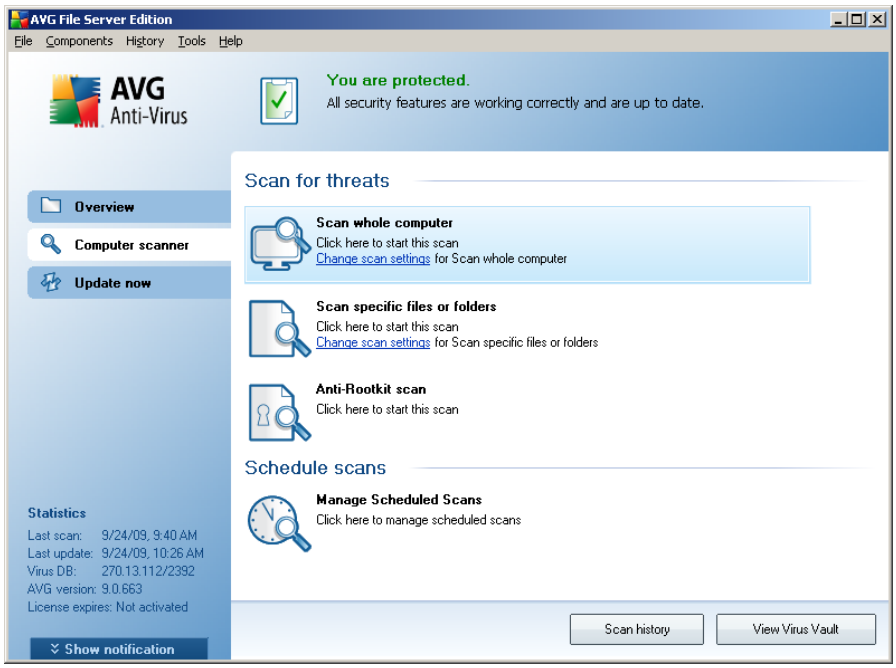
## 11.5. Scan Scheduling

With **AVG 9.0 File Server** you can run scanning on demand (for instance when you suspect an infection has been dragged to your computer) or based on a scheduled plan. It is highly recommended to run the scans based on a schedule: this way you can make sure your computer is protected from any possibility of getting infected, and you will not have to worry about if and when to launch the scan.

You should launch the ***Scan whole computer*** regularly, at least once a week.

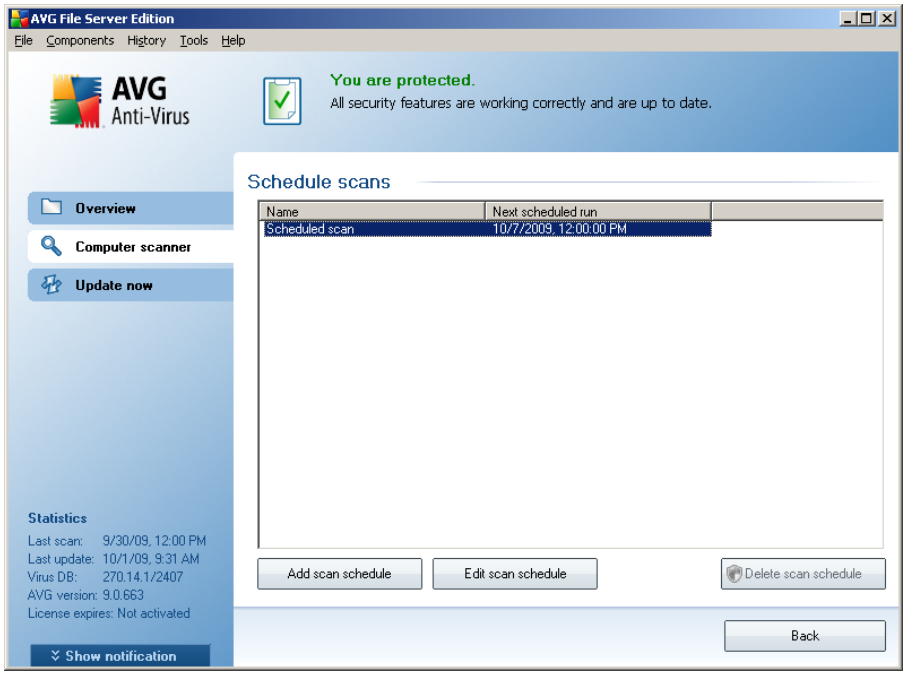
However, if possible, launch the scan of your entire computer daily - as set up in the scan schedule default configuration. If the computer is "always on" then you can schedule scans out of working hours. If the computer is sometimes switched off, then schedule scans to occur on a computer start-up when the task has been missed.

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




## Schedule scans

Click the graphical icon within the ***Schedule scans*** section to open a new ***Schedule scans*** dialog where you find a list of all currently scheduled scans:




You can edit / add scans using the following control buttons:

- ***Add scan schedule*** - the button opens the ***Settings for scheduled scan*** dialog, ***Schedule settings*** tab. In this dialog you can specify the parameters of the newly defined test.

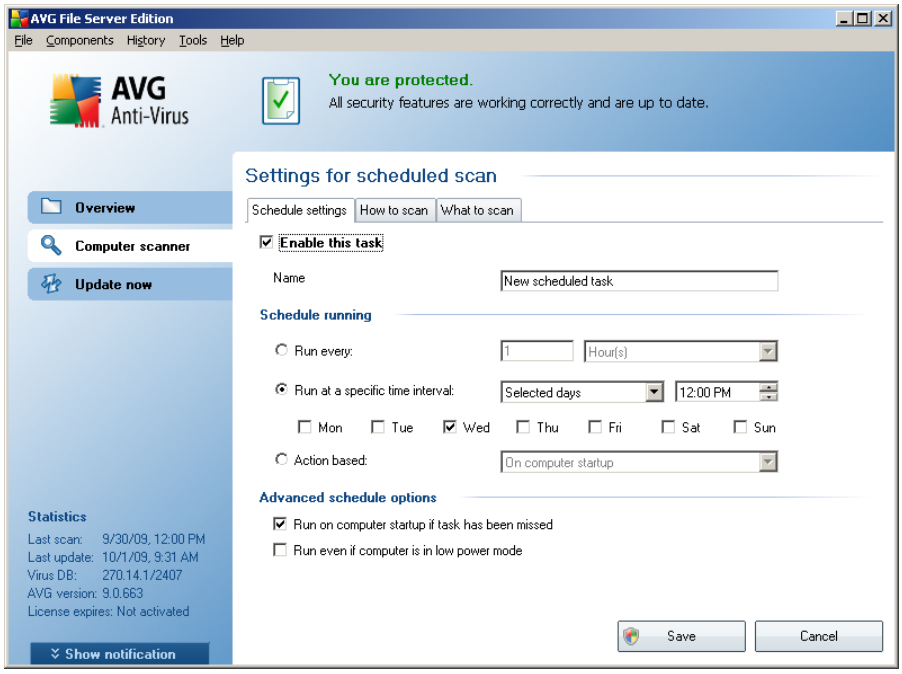
- ***Edit scan schedule*** - this button can only be used if you have already previously selected an existing test from the list of scheduled tests. In that case the button appears as active and you can click it to switch to the ***Settings for scheduled scan*** dialog, ***Schedule settings*** tab. Parameters of the selected test are already specified in here and can be edited.

- ***Delete scan schedule*** - this button is also active if you have already previously selected an existing test from the list of scheduled tests. This test can then be deleted from the list by pressing the control button. However, you can only remove your own tests; the ***Whole computer scan schedule*** pre-defined within the default settings can never be deleted.

- ***Back*** - return to AVG scanning interface

### 11.5.1. Schedule Settings

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




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

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

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

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

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

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

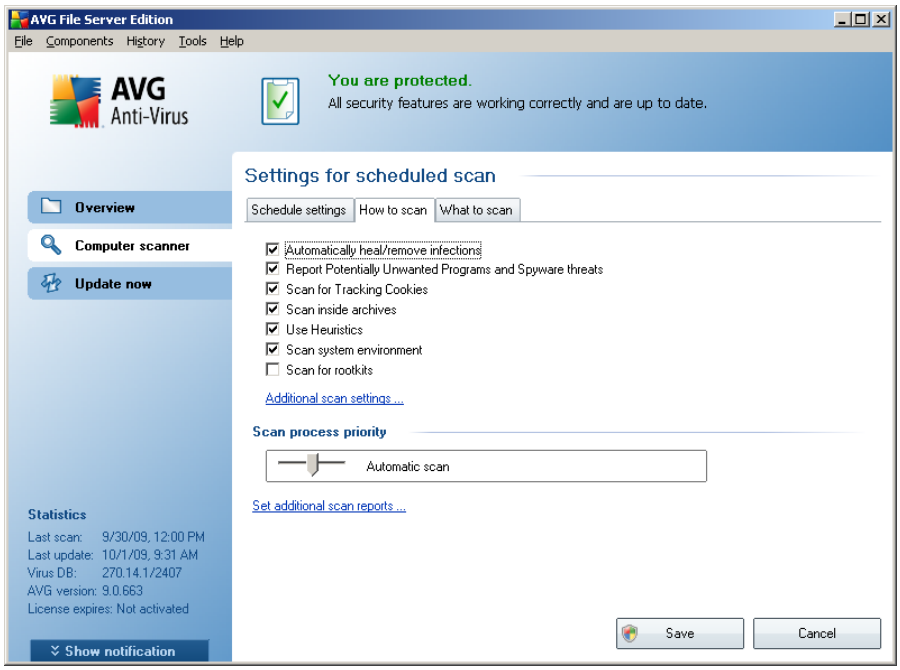
## Control buttons of the Settings for scheduled scan dialog

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

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

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

## 11.5.2. How to Scan




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

- ***Automatically heal/remove infection*** - (*switched on, by default*): if a virus is identified during scanning it can be healed automatically if a cure is available . In case the infected file cannot be healed automatically, or if you decide to switch off this option, you will be notified upon a virus detection and will have to decide what to do with the detected infection. The recommended action is to remove the infected file to the ***Virus Vault***.

- ***Report Potentially Unwanted Programs and Spyware threats*** - (*switched on, by default*): this parameter controls the ***Anti-Virus*** functionality that allows detection of potentially unwanted programs (*executable files that can run as spyware or adware*) and these can then be blocked, or removed;

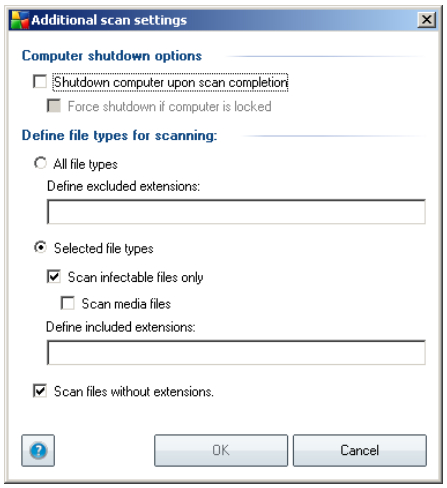
- ***Scan for Tracking Cookies*** - (*switched on, by default*): this parameter of the ***Anti-Spyware*** component defines that cookies should be detected during scanning (*HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of*

*their electronic shopping carts*);

- ***Scan inside archives*** - (*switched on, by default*): this parameters defines that the scanning should check all files even if these are packed inside some type of archive, e.g. ZIP, RAR, ...
- ***Use Heuristics*** - (*switched on, by default*): heuristic analysis (*dynamic emulation of the scanned object's instructions in a virtual computer environment*) will be one of the methods used for virus detection during scanning;
- ***Scan system environment*** - (*switched on, by default*): scanning will also check the system areas of your computer;
- ***Scan for rootkits*** - tick this item if you want to include the rootkit detection into scanning of the entire computer. The rootkit detection is also available on its own within the ***Anti-Rootkit*** component;

Then, you can change the scan configuration as follows:

- ***Additional scan settings*** - the link opens a new ***Additional scan settings*** dialog where you can specify the following parameters:




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

- o ***Define file types for scanning*** - further you should decide whether you want to have scanned:
  - ➢ ***All file types*** with the possibility of defining exceptions from scanning by providing a list of comma separated file extensions that should not be scanned; or
  - ➢ ***Selected file types*** - you can specify that you want to scan only files that are possibly infectable (*files that cannot get infected will not be scanned, for instance some plain text files, or some other non-executable files*), including media files (*video, audio files - if you leave this box unchecked, it will reduce the scanning time even more, because these files are often quite large and are not too likely to be infected by a virus*). Again, you can specify by extensions which files are those that should always be scanned.
  - ➢ Optionally, you can decide you want to ***Scan files without extension*** - this option is on by default, and it is recommended that you keep it so unless you have a real reason to change it. Files with no extension are rather suspicious and should be scanned at all times.

- ***Scan process priority*** - you can use the slider to change the scanning process priority. By default, the priority is set to medium level (*Automatic scan* ) that optimizes the scanning process speed and the use of system resources. Alternatively, you can run the scanning process slower which means the system resources load will be minimized (*useful when you need to work on the computer but you do not care so much how long the scanning takes*), or faster with increased system resources requirements (*e.g. when the computer is temporarily unattended*).

- ***Set additional scan reports*** - the link opens a new ***Scan reports*** dialog where you can select what types of possible findings should be reported:

***Note:*** *By default, the scanning configuration is set up for optimum performance. Unless you have a valid reason to change the scanning settings it is highly*

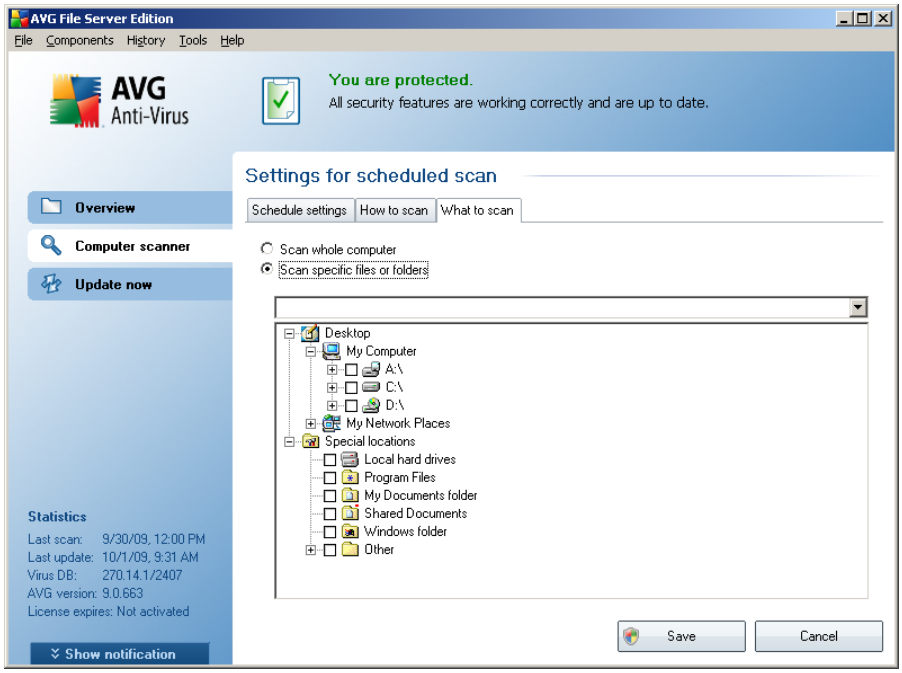
*recommended to stick to the predefined configuration. Any configuration changes should be performed by experienced users only. For further scanning configuration options see the **Advanced settings** dialog accessible via the **File / Advanced setting** system menu item.*

### Control buttons

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

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

## 11.5.3. What to Scan



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

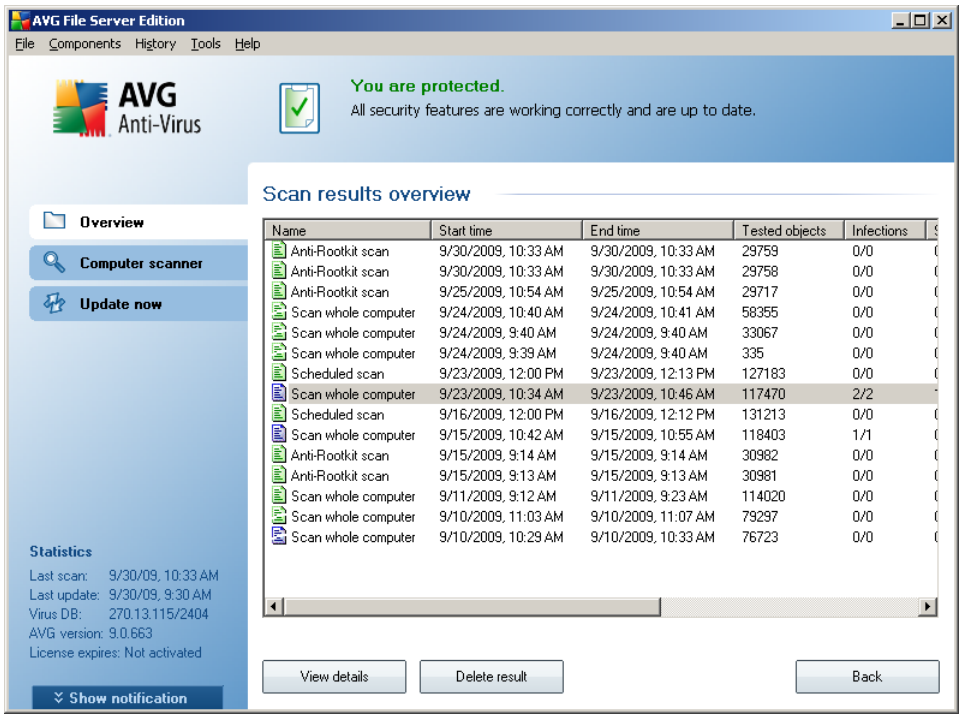
## Control buttons of the Settings for scheduled scan dialog

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

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

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

## 11.6. Scan Results Overview




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

- ***Name*** - scan designation; it can either be the name of one of the predefined scans, or a name you have given to your own scheduled scan. Every name includes an icon indicating the scan result:

  - green icon informs there was no infection detected during the scan

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

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

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

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

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

**Control buttons**

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

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

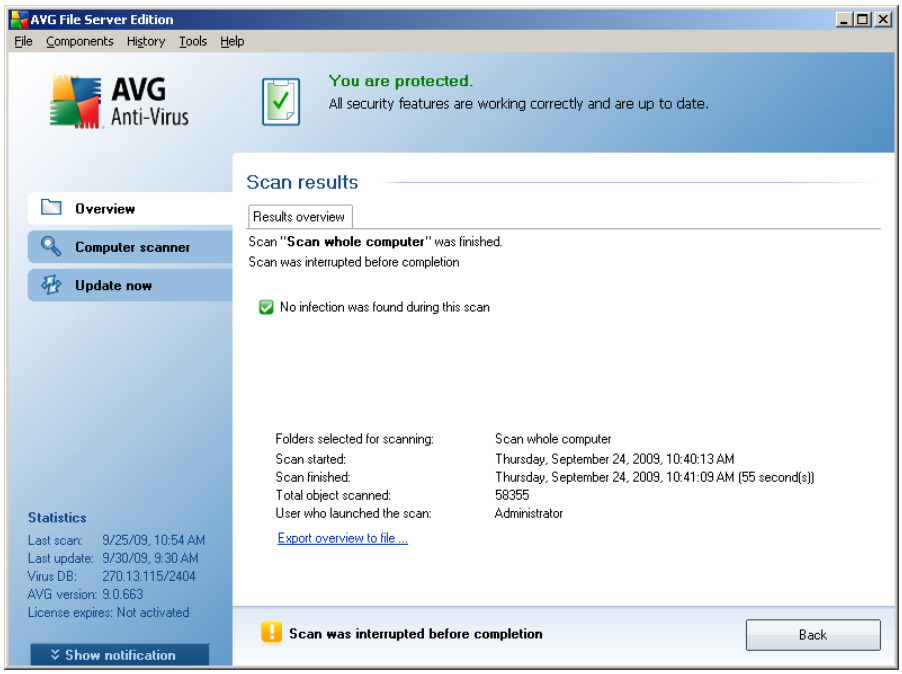
## 11.7. Scan Results Details

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

The dialog is further divided into several tabs:

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

### 11.7.1. Results Overview Tab




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

- detected virus infections / spyware

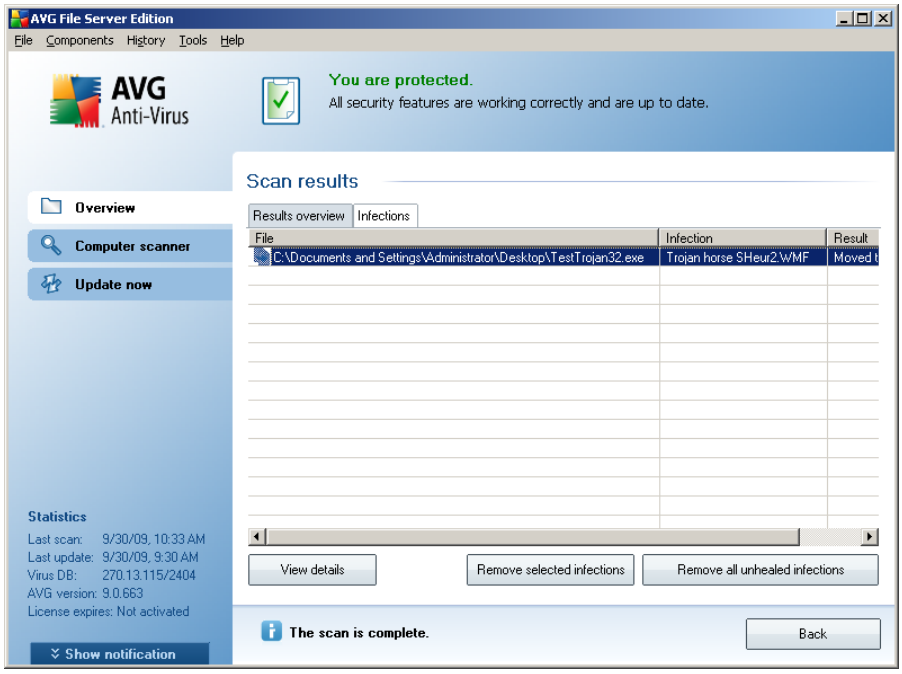
- removed virus infections / spyware
- the number of virus infections / spyware that cannot be removed or healed

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

### Control buttons

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

## 11.7.2. Infections Tab




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

- ***File*** - full path to the original location of the infected object
- ***Infections*** - name of the detected virus (*for details on specific viruses please*

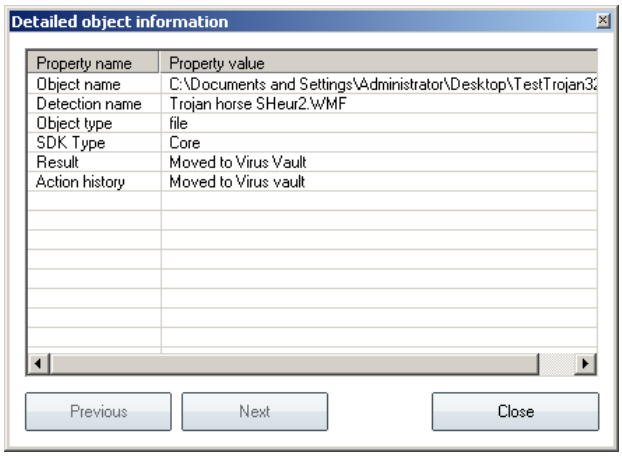
*consult the Virus Encyclopedia online*)

- ***Result*** - defines the current status of the infected object that was detected during scanning:
    - ***Infected*** - the infected object was detected and left in its original location (*for instance if you have switched off the automatic healing option in a specific scan settings*)
    - ***Healed*** - the infected object was healed automatically and left in its original location
    - ***Moved to Virus Vault*** - the infected object was moved to the ***Virus Vault*** quarantine
    - ***Deleted*** - the infected object was deleted
    - ***Added to PUP exceptions*** - the finding was evaluated as an exception and added to the list of PUP exceptions (*configured in the **PUP Exceptions** dialog of the advanced settings*)
    - ***Locked file - not tested*** - the respective object is locked and AVG is therefore unable to scan it
    - ***Potentially dangerous object*** - the object was detected as potentially dangerous but not infected (*it can contain macros, for instance*); the information should be taken as a warning only
    - ***Reboot is required to finish the action*** - the infected object cannot be removed, to remove it completely you have to restart your computer

## Control buttons

There are three control buttons available in this dialog:

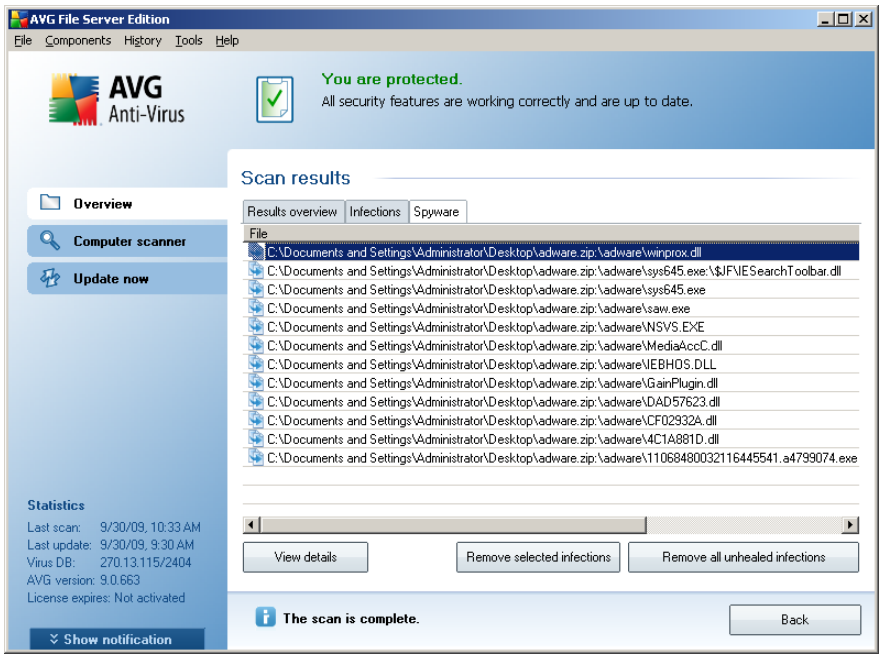
- ***View details*** - the button opens a new dialog window named ***Detailed scan result information***:




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

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

### 11.7.3. Spyware Tab




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

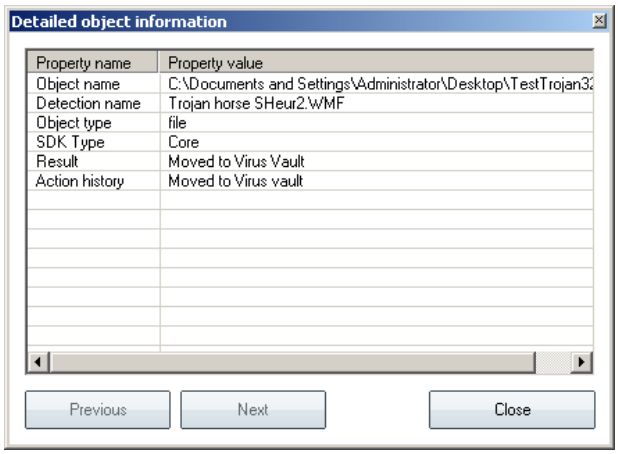
- ***File*** - full path to the original location of the infected object
- ***Infections*** - name of the detected spyware (*for details on specific viruses please consult the* ***Virus Encyclopedia*** *online*)
- ***Result*** - defines the current status of the object that was detected during scanning: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

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

## Control buttons

There are three control buttons available in this dialog:

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




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

- ***Remove selected infections*** - use the button to move the selected finding to the ***Virus Vault***

- ***Remove all unhealed infections*** - this button deletes all findings that cannot be healed or moved to the ***Virus Vault***

- ***Close results*** - terminates the detailed information overview and returns to the ***Scan results overview*** dialog

### 11.7.4. Warnings Tab

The ***Warnings*** tab displays information on "suspected" objects (*typically files*) detected during scanning. When detected by the ***Resident Shield***, these files are blocked from being accessed. Typical examples of this kind of findings are: hidden files, cookies, suspicious registry keys, password protected documents or archives, etc. Such files do not present any direct threat to your computer or security. Information about these files is generally useful in case there is an adware or spyware detected on your computer. If there are only Warnings detected by an AVG test, no action is necessary.

This is a brief description of the most common examples of such objects:

- ***Hidden files*** - The hidden files are by default not visible in Windows, and some viruses or other threats may try to avoid their detection by storing their files with this attribute. If your AVG reports a hidden file which you suspect to be malicious, you can move it to your ***AVG Virus Vault***.

- ***Cookies*** - Cookies are plain-text files which are used by websites to store user-specific information, which is later used for loading custom website layout, pre-filling user name, etc.

- ***Suspicious registry keys*** - Some malware stores its information into Windows registry, to ensure it is loaded on startup or to extend its effect on the operating system.

### 11.7.5. Information Tab

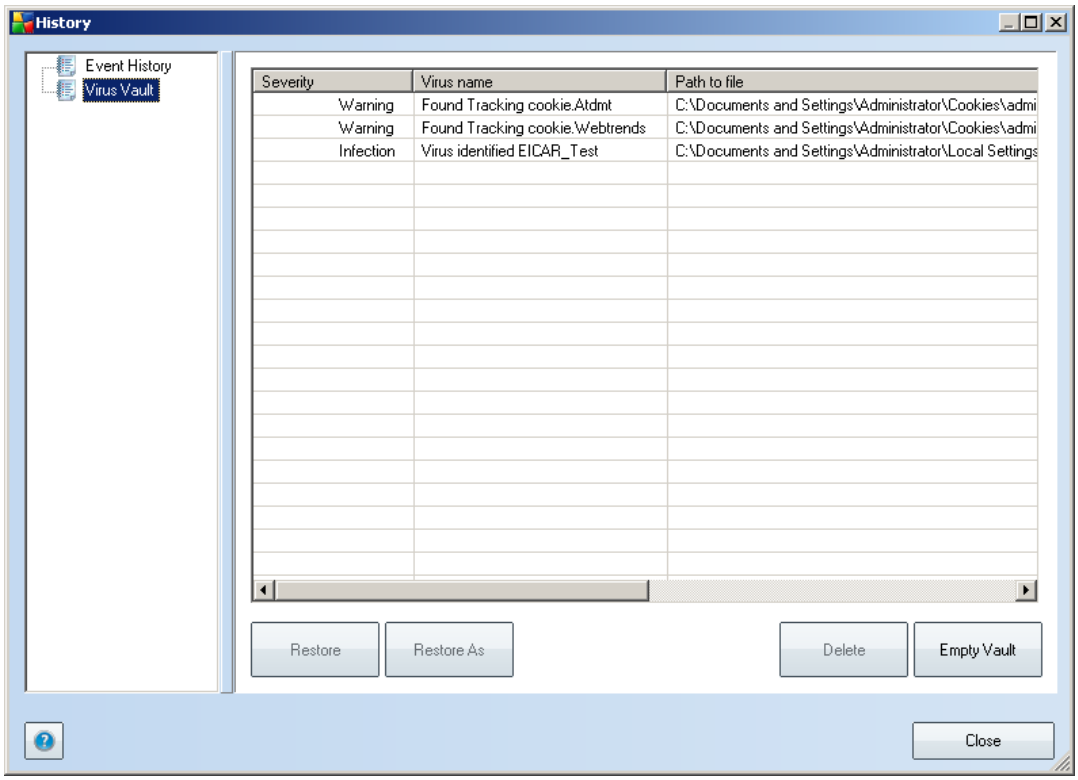
The ***Information*** tab contains data on such "findings" that cannot be categorized as infections, spyware, etc. They can neither be positively labeled as dangerous but they are still worth your attention. AVG scan is able to detect files which may not be infected, but are suspicious. These files are reported either as ***Warning***, or as

***Information***.

The severity ***Information*** can be reported for one of the following reasons:

- ***Run-time packed*** - The file was packed with one of less common run-time packers, which may indicate an attempt to prevent scanning of such file. However, not every report of such file indicates a virus.
- ***Run-time packed recursive*** - Similar to above, however less frequent amongst common software. Such files are suspicious and their removal or submission for analysis should be considered.
- ***Password protected archive or document*** - Password protected files can not be scanned by AVG (*or generally any other anti-malware program*).
- ***Document with macros*** - The reported document contains macros, which may be malicious.
- ***Hidden extension*** - Files with hidden extension may appear to be e.g. pictures, but in fact they are executable files (*e.g. picture.jpg.exe*). The second extension is not visible in Windows by default, and AVG reports such files to prevent their accidental opening.
- ***Improper file path*** - If some important system file is running from other than default path (*e.g. winlogon.exe running from other than Windows folder*), AVG reports this discrepancy. In some cases, viruses use names of standard system processes to make their presence less apparent in the system.
- ***Locked file*** - The reported file is locked, thus cannot be scanned by AVG. This usually means that some file is constantly being used by the system (*e.g. swap file*).

## 11.8. Virus Vault




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

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

- ***Severity*** - provides graphical identification of the respective finding severity on a four-levels scale from unobjectionable (■□□□) up to very dangerous (■■■■ )
- ***Infection type*** - distinguishes finding types based on their infective level (*all listed objects can be positively or potentially infected*)
- ***Virus Name*** - specifies the name of the detected infection according to the

Virus encyclopedia (online)

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

## Control buttons

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

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

# 12. AVG Updates

Keeping your AVG up-to-date is crucial to ensure that all newly discovered viruses will be detected as soon as possible. Since AVG updates are not released according to any fixed schedule but rather in reaction to amount and severity of new threats, it is recommended to check for new updates at least once a day. Checking every 4 hours will guarantee that your AVG Virus base is kept up-to-date also during the day.

## 12.1. Update Levels

AVG offers two update levels to select from:

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

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

## 12.2. Update Types

You can distinguish between two types of update:

- ***On demand update*** is an immediate AVG update that can be performed any time the need arises.
- ***Scheduled update*** - within AVG it is also possible to 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 Process

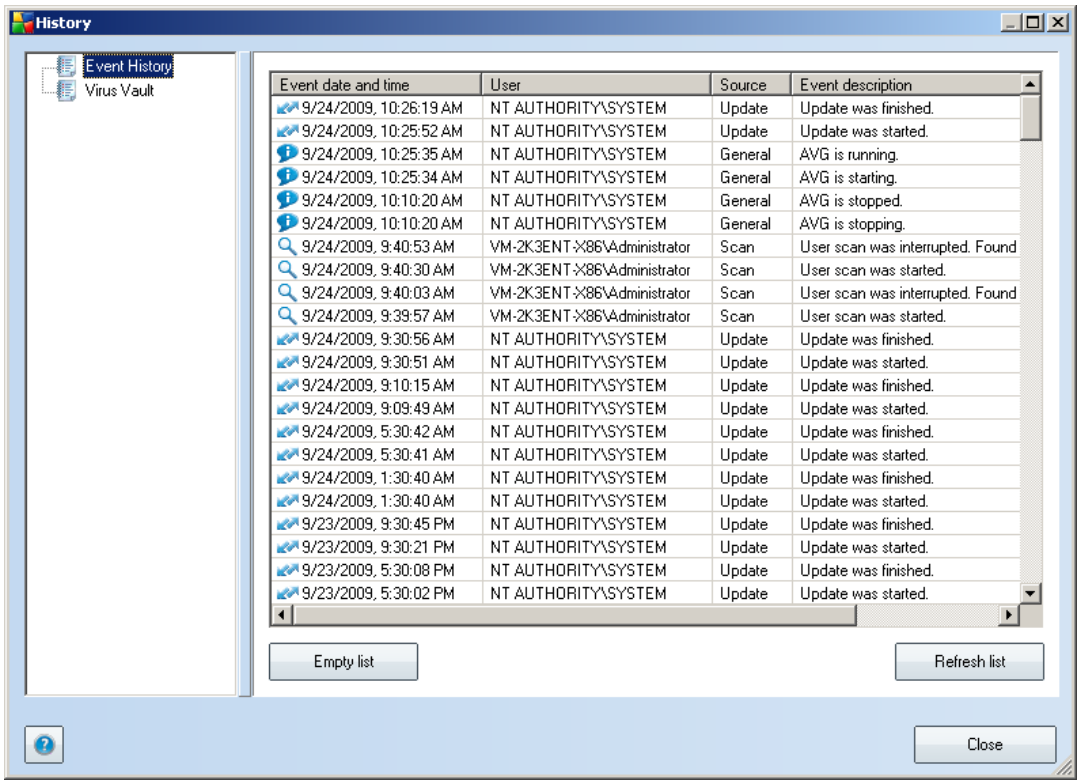
The update process can be launched immediately as the need arises by the ***Update now*** quick link. This link is available at all times from any AVG user interface dialog. However, it is still highly recommended to perform updates regularly as stated in the update schedule editable within the Update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

Once you start the update, AVG will first verify whether there are new update files available. If so, AVG starts their downloading and launches the update process itself. During the update process you will get redirected to the ***Update*** interface where you

can view the process progressing in its graphical representation as well as in an overview of relevant statistic parameters (*update file size, received data, download speed, elapsed time, ...*).

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

# 13. Event History




The ***Event History*** dialog is accessible from the system menu via the ***History/Event History Log*** item. Within this dialog you can find a summary of important events that occurred during **AVG 9.0 File Server** operation. ***Event History*** records the following types of events:

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

## Control buttons

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

# 14. FAQ and Technical Support

Should you have any problems with your AVG, either business or technical, please refer to the ***FAQ*** section of AVG website (http://www.avg.com).

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