



# AVG Premium Security 2012

## User Manual

### **Document revision 2012.09 (27.10.2011)**

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 libzip2, Copyright (c) 1996-2002 Julian R. Seward.



## Contents

<b>1. Introduction</b>	<b>7</b>
<b>2. AVG Installation Requirements</b>	<b>8</b>
2.1 Operation Systems Supported	8
2.2 Minimum & Recommended HW Requirements	8
<b>3. AVG Installation Process</b>	<b>9</b>
3.1 Welcome	9
3.2 Activate your license	11
3.3 Select type of installation	12
3.4 Custom options	13
3.5 Install the AVG Security Toolbar	14
3.6 Install progress	15
3.7 Installation was successful	16
<b>4. After Installation</b>	<b>18</b>
4.1 Product registration	18
4.2 Access to user interface	18
4.3 Scanning of the whole computer	18
4.4 Eicar test	18
4.5 AVG default configuration	19
<b>5. AVG User Interface</b>	<b>20</b>
5.1 System Menu	21
5.1.1 File	21
5.1.2 Components	21
5.1.3 History	21
5.1.4 Tools	21
5.1.5 Help	21
5.1.6 Support	21
5.2 Security Status Info	28
5.3 Quick Links	29
5.4 Components Overview	30
5.5 System Tray Icon	31
5.6 AVG gadget	33
<b>6. AVG Components</b>	<b>36</b>



6.1 Anti-Virus .....	36
6.1.1 Scanning Engine .....	36
6.1.2 Resident Protection .....	36
6.1.3 Anti-Spyware Protection .....	36
6.1.4 Anti-Virus Interface .....	36
6.1.5 Resident Shield Detections .....	36
6.2 Link Scanner .....	42
6.2.1 Link Scanner Interface .....	42
6.2.2 Search-Shield detections .....	42
6.2.3 Surf-Shield detections .....	42
6.2.4 Online Shield detections .....	42
6.3 E-mail Protection .....	47
6.3.1 E-mail Scanner .....	47
6.3.2 Anti-Spam .....	47
6.3.3 E-mail Protection Interface .....	47
6.3.4 E-mail Scanner Detections .....	47
6.4 Firewall .....	51
6.4.1 Firewall Principles .....	51
6.4.2 Firewall Profiles .....	51
6.4.3 Firewall Interface .....	51
6.5 Identity Alert .....	55
6.6 Anti-Rootkit .....	55
6.6.1 Anti-Rootkit Interface .....	55
6.7 System Tools .....	57
6.7.1 Processes .....	57
6.7.2 Network Connections .....	57
6.7.3 Autostart .....	57
6.7.4 Browser Extensions .....	57
6.7.5 LSP Viewer .....	57
6.8 Quick Tune .....	63
6.9 Identity Protection .....	64
6.9.1 Identity Protection Interface .....	64
<b>7. My Apps .....</b>	<b>67</b>
7.1 LiveKive .....	67
7.2 Family Safety .....	68
7.3 PC Tuneup .....	68
<b>8. AVG Security Toolbar .....</b>	<b>70</b>



<b>9. AVG Advanced Settings</b>	<b>72</b>
9.1 Appearance	72
9.2 Sounds	75
9.3 Temporarily disable AVG protection	76
9.4 Anti-Virus	77
9.4.1 Resident Shield	77
9.4.2 Cache Server	77
9.5 E-mail protection	83
9.5.1 E-mail Scanner	83
9.5.2 Anti-Spam	83
9.6 Link Scanner	99
9.6.1 Link Scanner settings	99
9.6.2 Online Shield	99
9.7 Scans	103
9.7.1 Whole computer scan	103
9.7.2 Shell extension Scan	103
9.7.3 Specific files or folders scan	103
9.7.4 Removable device scan	103
9.8 Schedules	108
9.8.1 Scheduled Scan	108
9.8.2 Definitions Update Schedule	108
9.8.3 Program Update Schedule	108
9.8.4 Anti-Spam Update Schedule	108
9.9 Update	118
9.9.1 Proxy	118
9.9.2 Dial-up	118
9.9.3 URL	118
9.9.4 Manage	118
9.10 Anti-Rootkit	125
9.10.1 Exceptions	125
9.11 Identity Protection	126
9.11.1 Identity Protection Settings	126
9.11.2 Allowed List	126
9.12 Potentially Unwanted Programs	129
9.13 Virus Vault	132
9.14 Product Improvement Program	132
9.15 Ignore error status	135



<b>10. Firewall Settings</b>	<b>137</b>
10.1 General	137
10.2 Security	138
10.3 Areas and Adapters Profiles	139
10.4 IDS	140
10.5 Logs	142
10.6 Profiles	143
10.6.1 Profile Information	143
10.6.2 Defined Networks	143
10.6.3 Applications	143
10.6.4 System Services	143
<b>11. AVG Scanning</b>	<b>154</b>
11.1 Scanning Interface	154
11.2 Predefined Scans	155
11.2.1 Whole Computer Scan	155
11.2.2 Scan Specific Files or Folders	155
11.2.3 Anti-Rootkit Scan	155
11.3 Scanning in Windows Explorer	165
11.4 Command Line Scanning	165
11.4.1 CMD Scan Parameters	165
11.5 Scan Scheduling	168
11.5.1 Schedule Settings	168
11.5.2 How to Scan	168
11.5.3 What to Scan	168
11.6 Scan Results Overview	178
11.7 Scan Results Details	179
11.7.1 Results Overview Tab	179
11.7.2 Infections Tab	179
11.7.3 Spyware Tab	179
11.7.4 Warnings Tab	179
11.7.5 Rootkits Tab	179
11.7.6 Information Tab	179
11.8 Virus Vault	186
<b>12. AVG Updates</b>	<b>189</b>
12.1 Update launch	189
12.2 Update progress	189



12.3 Update levels .....	190
<b>13. Event History .....</b>	<b>191</b>
<b>14. FAQ and Technical Support .....</b>	<b>193</b>



## 1. Introduction

This user manual provides comprehensive documentation for **AVG Premium Security 2012**.

**AVG Premium Security 2012** provides multiple layers of protection for everything you do online, which means you don't have to worry about identity theft, viruses, or visiting harmful sites. AVG Protective Cloud Technology and AVG Community Protection Network are included, meaning we collect the latest threat information and share it with our community to make sure you receive the best protection:

- Shop and bank online safely with AVG Firewall, Anti-Spam & Identity Protection
- Stay safe on social networks with AVG Social Networking Protection
- Surf and search with confidence with LinkScanner's real-time protection



## 2. AVG Installation Requirements

### 2.1. Operation Systems Supported

**AVG Premium Security 2012** is intended to protect workstations with the following operating systems:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 and x64, all editions)
- Windows 7 (x86 and x64, all editions)

(and possibly higher service packs for specific operating systems)

**Note:** The [ID Protection](#) component is not supported on Windows XP x64. On this operating system you can install AVG Premium Security 2012 but only without the IDP component.

### 2.2. Minimum & Recommended HW Requirements

Minimum hardware requirements for **AVG Premium Security 2012**:

- Intel Pentium CPU 1,5 GHz
- 512 MB of RAM memory
- 1000 MB of free hard drive space (for installation purposes)

Recommended hardware requirements for **AVG Premium Security 2012**:

- Intel Pentium CPU 1,8 GHz
- 512 MB of RAM memory
- 1550 MB of free hard drive space (for installation purposes)



### 3. AVG Installation Process

#### Where do I get the installation file?

To install **AVG Premium Security 2012** on your computer, you need to get the latest installation file. To make sure you are installing the up-to-date version of **AVG Premium Security 2012**, it is recommended to download the installation file from AVG website (<http://www.avg.com/>). The **Support Center / Download** section provides a structured overview of installation files for each AVG edition.

If you are not sure which files you need to download and install, you may want to use the **Select product** service in the bottom of the web page. After you answer three simple questions, this service defines the exact files you need. Press the **Continue** button to get redirected to a complete list of download files customized for your personal needs.

#### What does the installation process look like?

Once you have downloaded and saved the installation file on your hard disk, you can launch the installation process. The installation is a sequence of simple and easy to understand dialogs. Each dialog briefly describes what do at each step of the installation process. Following, we offer a detailed explanation of each dialog window:

#### 3.1. Welcome

The installation process starts with the **Welcome to AVG Installer** dialog:



#### Select the installation language



Here in the dialog you can select the language used for the installation process. In the right hand corner of the dialog click the combo box to roll down the language menu. Select the desired language, and the installation process will proceed further in the language of your choice.

***Attention: At the moment you are only selecting the language of the installation process. The AVG Premium Security 2012 application will be installed in the selected language, and in English that is always installed automatically. However, it is possible to have more languages installed and to work with AVG Premium Security 2012 in any of these. You will be invited to confirm your full selection of alternative languages in one of following setup dialogs named [Custom Options](#).***

### **License Agreement**

Further, the **Welcome to AVG Installer** dialog provides the full wording of the AVG license agreement. Please read it carefully. To confirm that you have read, understood and accept the agreement press the **Accept** button. If you do not agree with the license agreement press the **Decline** button, and the installation process will be terminated immediately.

### **AVG Privacy Policy**

Besides the license agreement, this setup dialog also offers you the option to learn more about AVG privacy policy. In the left-hand bottom corner of the dialog you can see the **AVG Privacy Policy** link. Click it to get redirected to AVG website (<http://www.avg.com/>) where you can find the full extent of AVG Technologies privacy policy principles.

### **Control buttons**

Within the first setup dialog, there are only two control buttons available:

- **Accept** - Click to confirm you have read, understood, and accepted the license agreement. The installation will continue, and you will go on one step further to the following setup dialog.
- **Decline** - Click to refuse the license agreement. The setup process will quit immediately. **AVG Premium Security 2012** will not be installed!



### 3.2. Activate your license

In the **Activate Your License** dialog you are invited to fill in your license number into the provided text field:

AVG Software Installer

AVG

### Activate Your License

License Number:

Example: IQNP6-9BCA8-PUQU2-ASHCK-GP338L-930CB

If you purchased your AVG 2012 software online, your license number will have been sent by email. To avoid typing errors, we recommend copying and pasting the number from the email to this screen.

If you purchased the software in a retail store, you will find the license number on the product registration card included in the package. Please ensure you copy the number correctly.

< Back   Next >   Cancel

#### Where to find the license number

The sales number can be found on the CD packaging in your **AVG Premium Security 2012** box. The license number will be in the confirmation email that you received after purchasing your **AVG Premium Security 2012** 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.

#### How to use the Copy & Paste method

Using the **Copy & Paste** method to enter your **AVG Premium Security 2012** license number into the program ensures that the number is correctly entered. Please follow these steps:

- Open the e-mail containing your license number.
- Click the left mouse button at the beginning of the license number, hold and drag the mouse to the end of the number, and then release the button. The number should now be highlighted.
- Press and hold **Ctrl**, and then press **C**. This copies the number.
- Point and click the position where you would like to paste the copied number.
- Press and hold **Ctrl**, and then press **V**. This pastes the number to the location you selected.



## Control buttons

As within most setup dialogs, there are three control buttons available:

- **Back** - Click to return one step back to the previous setup dialog.
- **Next** - Click to continue the installation and get one step further.
- **Cancel** - Click to exit the setup process immediately; **AVG Premium Security 2012** will not be installed!

## 3.3. Select type of installation



## Types of installation

The **Select type of installation** dialog offers the choice of two installation options: **Quick Install** and **Custom Install**.

For most users, it is highly recommended to keep to the standard quick installation that installs **AVG Premium Security 2012** 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 Premium Security 2012** application. If you have selected the **Quick Install** option, press the **Next** button to proceed to the following [Install the AVG Security Toolbar](#) dialog.

Custom installation should only be used by experienced users who have a valid reason to install **AVG Premium Security 2012** with non-standard settings; e.g. to fit specific system requirements. Having selected this option, press the **Next** button to proceed to the [Custom Options](#) dialog.



### AVG gadget installation

In the right-hand section of the dialog you can find the check box related to [AVG gadget](#) (*supported in Windows Vista/Windows 7*). If you wish to have installed this gadget, mark the respective checkbox. [AVG gadget](#) will then be accessible from the Windows Sidebar providing you an immediate access to the most important features of your **AVG Premium Security 2012**, i.e. [scanning](#) and [updating](#).

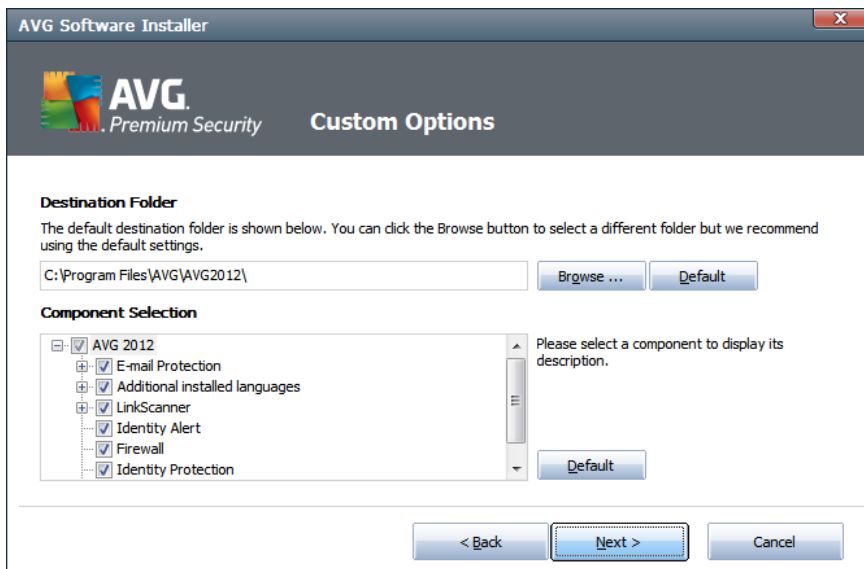
### Control buttons

As within most setup dialogs, there are three control buttons available:

- **Back** - Click to return one step back to the previous setup dialog.
- **Next** - Click to continue the installation and get one step further.
- **Cancel** - Click to exit the setup process immediately; **AVG Premium Security 2012** will not be installed!

## 3.4. Custom options

The **Custom Options** dialog allows you to set up two parameters of the installation:



### Destination Folder

Within the **Destination Folder** section of the dialog you are supposed to specify the location where **AVG Premium Security 2012** should be installed. By default, **AVG Premium Security 2012** will be installed to the program files folder located on drive C:. If you want to change this location, use the **Browse** button to display the drive structure, and select the respective folder.



## Component Selection

The **Component Selection** section provides an overview of all **AVG Premium Security 2012** 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!**

Highlight any item in the **Component Selection** list, and a brief description of the respective component will be displayed on the right side of this section. For detailed information on each component's functionality please consult the [Components Overview](#) chapter of this documentation. To revert to the default configuration pre-set by the software vendor use the **Default** button.

## Control buttons

As within most setup dialogs, there are three control buttons available:

- **Back** - Click to return one step back to the previous setup dialog.
- **Next** - Click to continue the installation and get one step further.
- **Cancel** - Click to exit the setup process immediately; **AVG Premium Security 2012** will not be installed!

## 3.5. Install the AVG Security Toolbar



In the **Install the AVG Security Toolbar** dialog, decide whether you want to install the [AVG Security Toolbar](#). If you do not change the default settings, this component will be installed

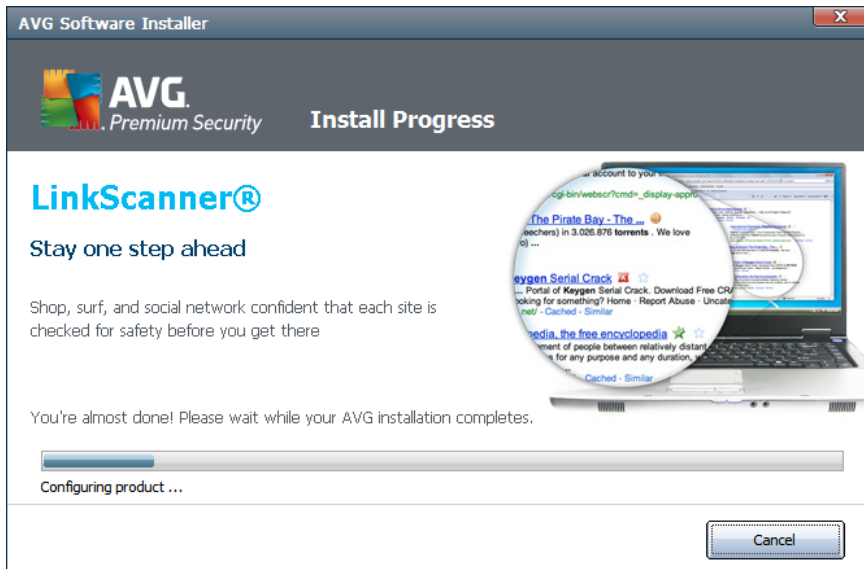


automatically into your Internet browser (*currently supported browsers are Microsoft Internet Explorer v. 6.0 or higher, and Mozilla Firefox v. 3.0 and higher*) and to provide you with comprehensive online protection while surfing the Internet.

Also, you have the option to decide whether you want to choose *AVG Secure Search (powered by Google)* as your default search provider. If so, keep the respective check box marked.

### 3.6. Install progress

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



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

#### Control buttons

In this dialog, there is only one control button available - **Cancel**. This button should only be used if you want to stop the running installation process. Please mind that in such a case your **AVG Premium Security 2012** will not be installed!



### 3.7. Installation was successful

The *Installation was successful* dialog confirms that your **AVG Premium Security 2012** has been fully installed and configured:



#### Product Improvement Program

Here you can decide whether you want to participate in the Product Improvement Program (*for details see chapter [AVG Advanced Settings / Product Improvement Program](#)*) that collects anonymous information on detected threats in order to increase the overall Internet security level. If you agree with this statement, please keep the ***I agree to participate in the AVG 2012 web safety and Product Improvement Program ...*** option checked (*the option is confirmed, by default*).

#### Computer restart

To finalize the installation process you need restart your computer: select whether you want to ***Restart Now***, or you want to postpone this action - ***Restart Later***.

#### Control buttons

In the dialog, the following control buttons are available:

- ***Restart Now (recommended)*** - Restart is required to complete the installation process of **AVG Premium Security 2012**. It is recommended to restart your computer immediately. Only after the restart **AVG Premium Security 2012** is fully installed, and you are safe and protected.
- ***Restart Later*** - If for some reason you cannot restart your computer now, the action can be postponed till later. However, it is recommended to restart immediately. Only after the



restart, **AVG Premium Security 2012** can fully protect your computer!



## 4. After Installation

### 4.1. Product registration

Having finished the **AVG Premium Security 2012** installation, please register your product online on the AVG website (<http://www.avg.com/>). 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.

The easiest way to register is directly from the **AVG Premium Security 2012** user interface. In the main menu please select the [Help/Register now](#) item. You will be redirected to the **Registration** page on the AVG website (<http://www.avg.com/>). Please follow the instructions provided in the page.

### 4.2. Access to user interface

The [AVG main dialog](#) is accessible in several ways:

- double-click the [AVG system tray icon](#)
- double-click the AVG icon on the desktop
- from the menu **Start/Programs/AVG 2012/AVG User Interface**

### 4.3. Scanning of the whole computer

There is a potential risk that a computer virus has been transmitted to your computer prior to **AVG Premium Security 2012** installation. For this reason you should run a [Scan of the whole computer](#) to make sure there are no infections on your PC.

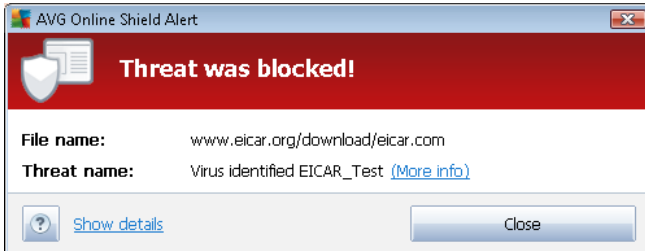
For instructions on running a [Scan of the whole computer](#) consult the chapter [AVG Scanning](#).

### 4.4. Eicar test

To confirm that **AVG Premium Security 2012** 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](http://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 [Online Shield](#) (a part of [LinkScanner](#) component) will react to it with a warning. This notice demonstrates that AVG is correctly installed on your computer.



From the <http://www.eicar.com> website you can also download the compressed version of the EICAR 'virus' (e.g. in the form of *eicar\_com.zip*). [Online Shield](#) allows you to download this file and save it on your local disk but then the [Resident Shield](#) (within [Anti-Virus](#) component) detects the 'virus' as you try to unpack it.

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

#### 4.5. AVG default configuration

The default configuration (*i.e. how the application is set up right after installation*) of **AVG Premium Security 2012** is set up by the software vendor so that all components and functions are tuned up to achieve optimum performance.

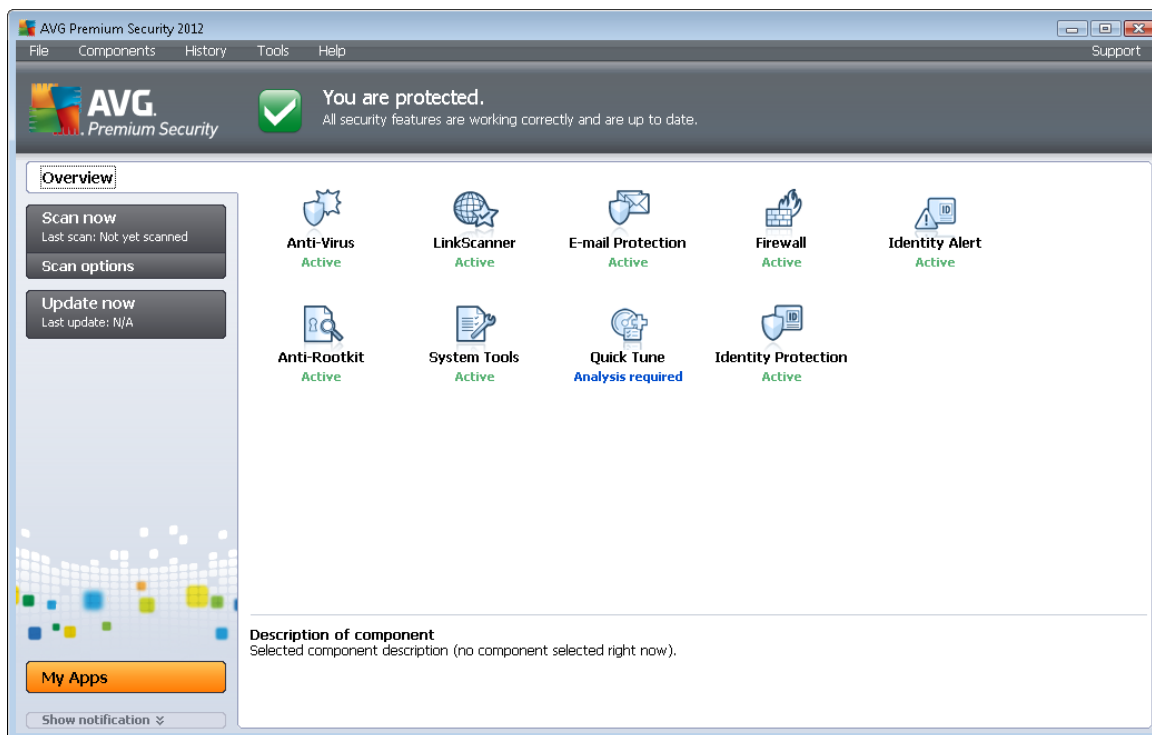
***Unless you have a real reason to do so, do not change the AVG configuration! Changes to settings should only be performed by an experienced user.***

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 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.



## 5. AVG User Interface

AVG Premium Security 2012 opens 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 components, services, and features of **AVG Premium Security 2012** - [details >>](#)
- **Security Status Info** (upper section of the window) provides you with information on the current status of your **AVG Premium Security 2012** - [details >>](#)
- **Quick Links** (left section of the window) allow you to quickly access the most important and most frequently used tasks of **AVG Premium Security 2012** - [details >>](#)
- **My Apps** (left bottom section of the window) open an overview of additional application available for **AVG Premium Security 2012**: [LiveKive](#), [Family Safety](#), and [PC Tuneup](#)
- **Components Overview** (central section of the window) offer an overview of all components installed within **AVG Premium Security 2012** - [details >>](#)
- **System Tray Icon** (bottom right corner of the monitor, on the system tray) indicates the current status of **AVG Premium Security 2012** - [details >>](#)
- **AVG gadget** (Windows sidebar, supported in Windows Vista/7) allows quick access to scanning and update within **AVG Premium Security 2012** - [details >>](#)



## 5.1. 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 Premium Security 2012** main window. Use the system menu to access specific AVG components, feature, and services.

The system menu is divided into five main sections:

### 5.1.1. File

- **Exit** - closes the **AVG Premium Security 2012**'s user interface. However, the AVG application will continue running in the background and your computer will still be protected!

### 5.1.2. 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** detects viruses, spyware, worms, trojans, unwanted executable files or libraries within your system, and protects you from malicious adware - [details >>](#)
- **LinkScanner** protects you from web-based attacks while you search and surf the Internet - [details >>](#)
- **E-mail Protection** checks your incoming e-mail messages for SPAM, and blocks viruses, phishing attacks, or other threats - [details >>](#)
- **Firewall** controls all communication on each network port, protecting you from malicious attacks and blocking all intrusion attempts - [details >>](#)
- **Anti-Rootkit** scans for dangerous rootkits hidden inside applications, drivers, or libraries - [details >>](#)
- **System Tools** offers a detailed summary of the AVG environment and operating system information - [details >>](#)
- **Quick Tune** provides detailed analytical information about your computer status, and offers optimization - [details >>](#)
- **Identity Alert** scours dodgy websites and online networks for potential trade of your identity details - [details >>](#)
- **Identity Protection** is constantly protecting your digital assets against new and unknown threats - [details >>](#)



### 5.1.3. 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](#)
- [E-mail Scanner detection](#) - open a dialog with an overview of mail messages attachments detected as dangerous by the [E-mail Protection](#) component
- [Online Shield findings](#) - open a dialog with an overview of threats detected by [Online Shield](#) service within [LinkScanner](#) component
- [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 Premium Security 2012** actions
- [Firewall log](#) - opens the Firewall settings interface on the [Logs](#) tab with a detailed overview of all Firewall actions

### 5.1.4. Tools

- [Scan computer](#) - 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 specific file. Click this option to open a new window with the tree structure of your disk. Select the desired file, and confirm the scan launch.
- [Update](#) - Automatically launches the update process of **AVG Premium Security 2012**.
- **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 Premium Security 2012 configuration. Generally, it is recommended to keep the default settings of the application as defined by the software vendor.
- [Firewall settings...](#) - Open a standalone dialog for advanced configuration of the [Firewall](#) component.



### 5.1.5. 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 (*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.

**Note:** *If using the trial version of AVG Premium Security 2012, the latter two items appear as **Buy now** and **Activate**, allowing you to buy the full version of the program right away. For AVG Premium Security 2012 installed with a sales number, the items display as **Register** and **Activate**.*

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

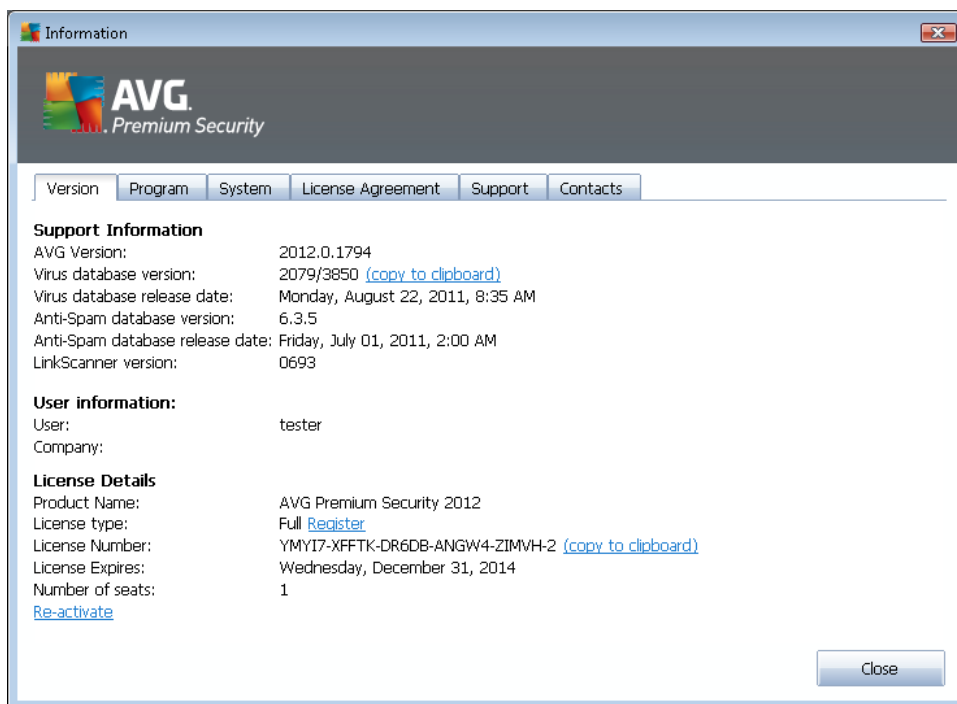
### 5.1.6. Support

The **Support** link opens a new **Information** dialog with all types of information you might need when trying to find help. The dialog includes basic data on your installed AVG program (*program / database version*), license details, and a list of quick support links.

The **Information** dialog is divided into six tabs:



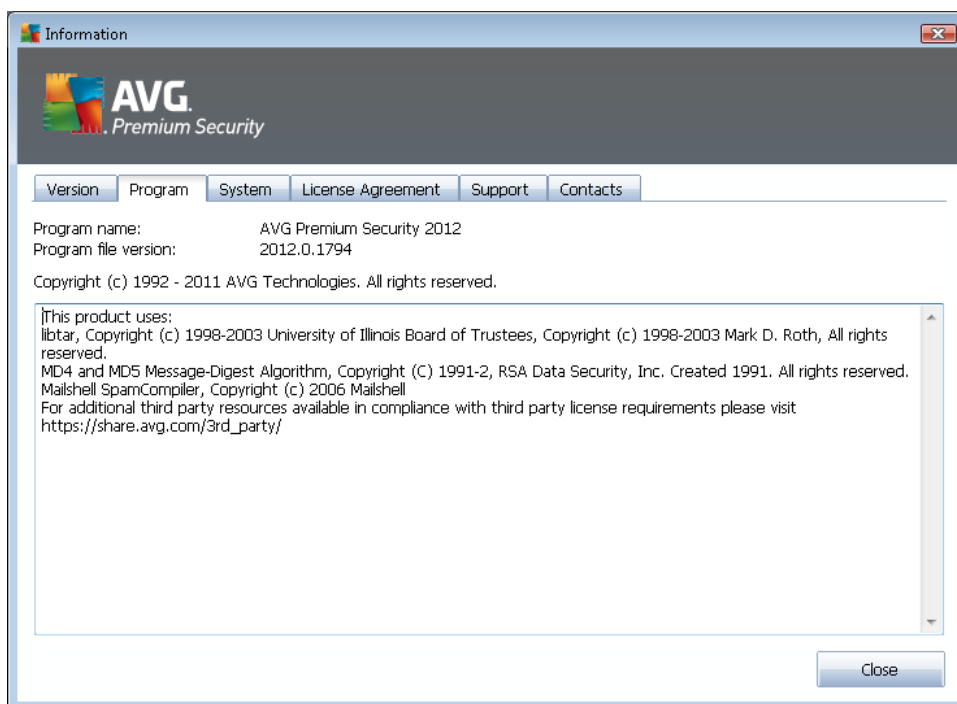
The **Version** tab is divided into three sections:



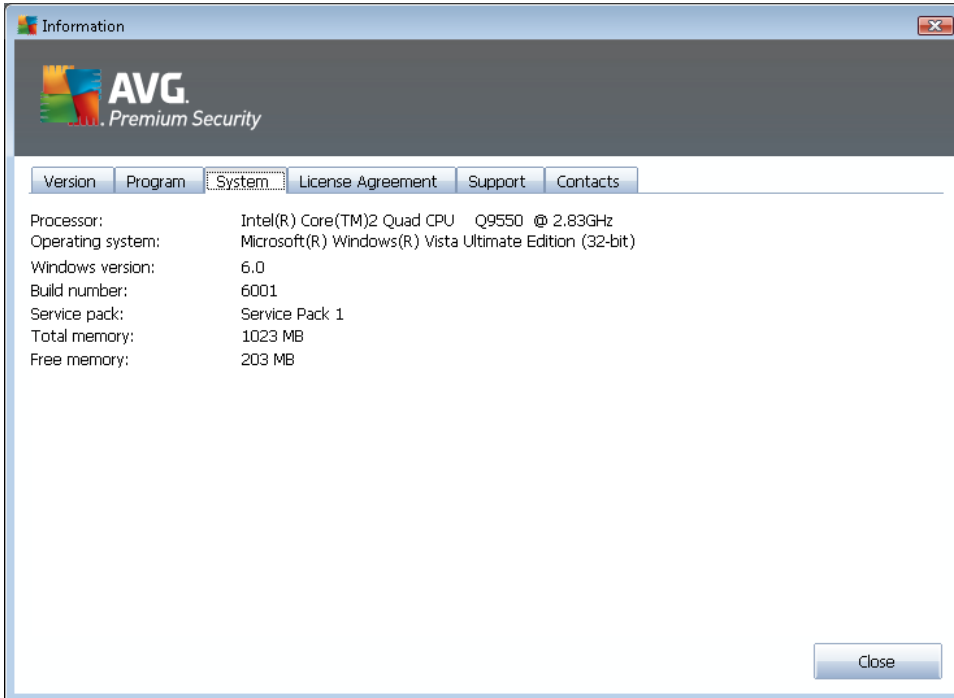
- **Support Information** - Provides information on **AVG Premium Security 2012** version, the virus database version, the [Anti-Spam](#) database version, and [LinkScanner](#) version.
- **User Information** - Provides information on the licensed user and company.
- **License Details** - Provides information on your license (*product name, license type, license number, expiration date, and number of seats*). In this section you can also use the **Register** link to register your **AVG Premium Security 2012** online; this allows you to use the [AVG technical support](#) in its full extent. Also, use the **Re-activate** link to open the **Activate AVG** dialog: fill in your license number into the respective field to either replace your sales number (*that you use during the AVG Premium Security 2012 installation*), or to change your current license number for another (*e.g. when upgrading to a higher AVG product*).



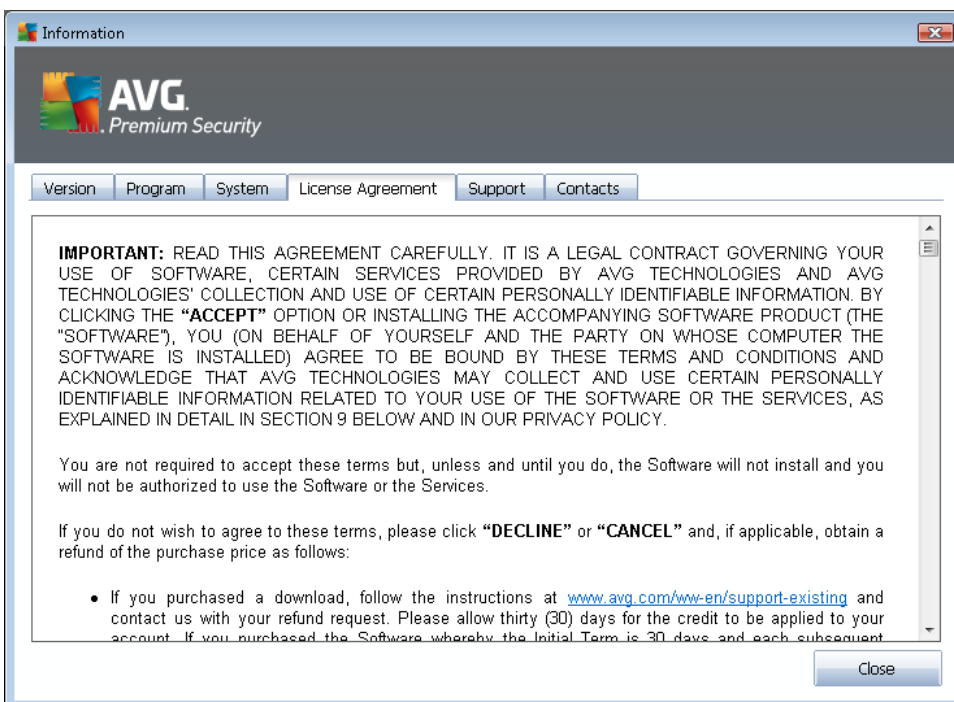
On the **Program** tab you can find information on the **AVG Premium Security 2012** program file version, and on the third parties code used in the product:



The **System** tab offers a list of parameters of your operating system (*processor type, operating system and its version, build number, service packs used, total memory size, and free memory size*):

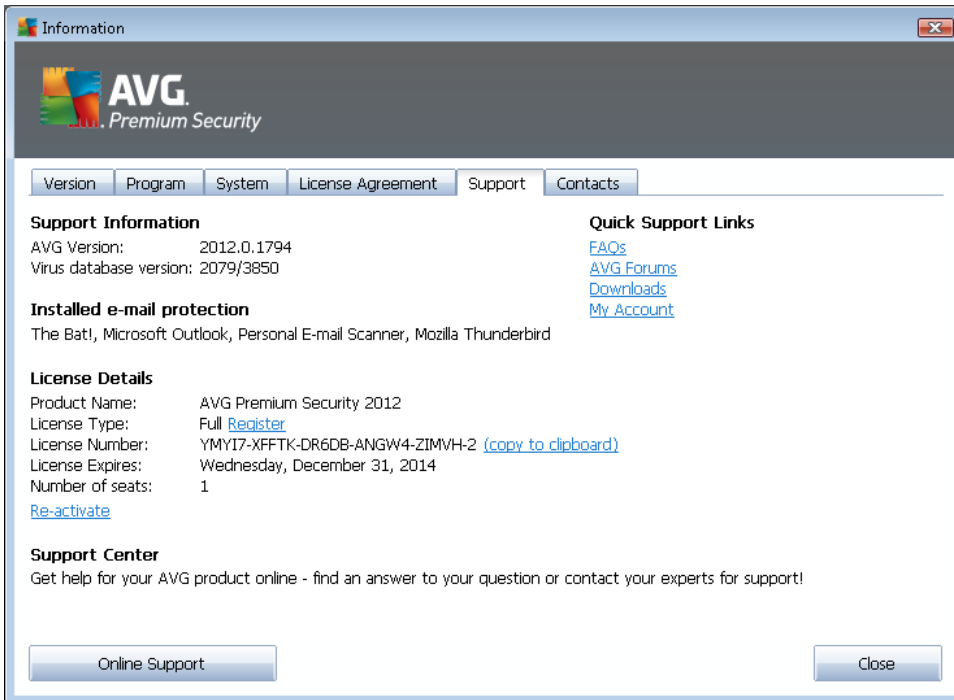


On the **License Agreement** tab you can read the full wording of the license agreement between you and AVG Technologies:



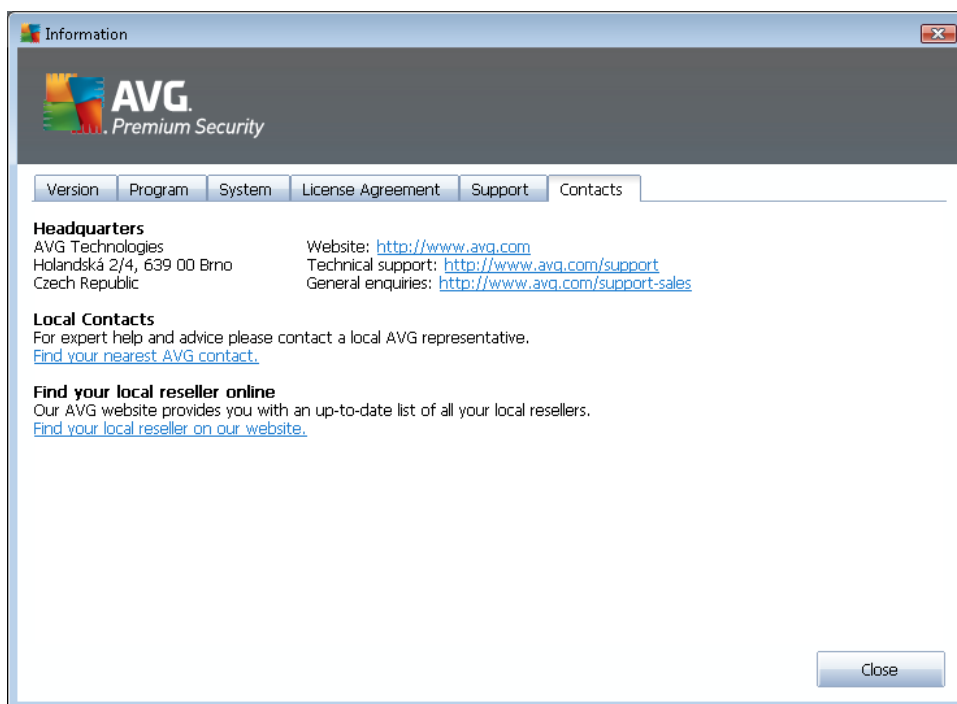


The **Support** tab brings a list of all possibilities of contacting the customer support. Also, it provides links to AVG website (<http://www.avg.com/>), AVG forums, FAQ, ... Further you can find information you might use while contacting the customer support team:





The **Contacts** tab provides a list of all contacts to AVG Technologies, and also contacts to AVG local representatives and resellers:



## 5.2. Security Status Info

The **Security Status Info** section is located in the upper part of the **AVG Premium Security 2012** main window. Within this section you will always find information on the current security status of your **AVG Premium Security 2012**. Please see an overview of icons possibly depicted in this section, and their meaning:



- The green icon indicates that your **AVG Premium Security 2012 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 Premium Security 2012** and you have probably decided to switch some component off for some reason. You are still protected!. However, please pay attention to the problem component's settings! Its name will be provided in the **Security Status Info** section.

The orange 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 your mouse right-click*) over the respective component's icon in the [component overview](#) of



the **AVG Premium Security 2012** main window. Select this option to express you are aware of the component's error state but for some reason you wish to keep your **AVG Premium Security 2012** so and you do not want to be warned by the [system tray icon](#). 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.

Alternatively, the orange icon will also be displayed if your **AVG Premium Security 2012** requires the computer restart (**Restart needed**). Please pay attention to this warning and restart your PC using the **Restart now** button.



- The red icon indicates that **AVG Premium Security 2012 is in critical status!** One or more components does not work properly and **AVG Premium Security 2012** 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.

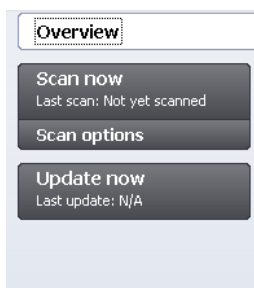
**In case AVG Premium Security 2012 is not set to the optimum performance, a new button named Fix (alternatively Fix all if the problem involves more than one component) appears next to the security status information. Press the button to launch an automatic process of program checkout and configuration. This is an easy way to set AVG Premium Security 2012 to the optimum performance and reach the maximum security level!**

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 Premium Security 2012 status information can also be obtained at any moment from the [system tray icon](#).*

### 5.3. Quick Links

**Quick links** are located on the left side of **AVG Premium Security 2012** [user interface](#). These links allow you to immediately access the most important and most frequently used features of the application, i.e. scanning and update. The quick links are accessible from all dialogs of the user interface:



**Quick links** are graphically divided into three sections:

- **Overview** - Use this link to switch from any currently opened AVG dialog to the default window with an [overview of all installed components](#). (For details see chapter [Components Overview](#))



- **Scan now** - By default, the button provides information of the last scan launched (*i.e. the scan type, and the date of last launch*). Click the **Scan now** command to launch the same scan again. If you want to launch another scan, click the **Scan options** link. This way you open the [AVG scanning interface](#) where you can run scans, schedule scans, or edit their parameters. (*For details see chapter [AVG Scanning](#)*)
- **Update now** - The link provides the date and time of the [update](#) last launch. Press the button to run the update process immediately, and to follow its progress. (*For details see chapter [AVG Updates](#)*)

**Quick links** are accessible from [AVG User Interface](#) at all times. Once you use a quick link to run a specific process, either a scan or an update, the application will switch to a new dialog but the quick links are still available. Moreover, the running process is further graphically depicted in the navigation, so that you have a full control over all launched processes running within **AVG Premium Security 2012** at the moment.

## 5.4. Components Overview

### Components Overview sections

The **Components Overview** section is located in the central part of your **AVG Premium Security 2012** [user interface](#). The section is divided into two parts:

- **Overview of all installed components** consisting of graphic panels for all installed component. Each panel is labeled by the component's icon and providing information on whether the respective component is active or inactive at the moment.
- **Component's description** is located in the bottom part of this dialog. The description briefly explains the component's basic functionality. Also, it provides the information on the current status of the selected component.

### Installed components' list

Within the **AVG Premium Security 2012** the **Components Overview** section contains information on the following components:

- **Anti-Virus** detects viruses, spyware, worms, trojans, unwanted executable files or libraries within your system, and protects you from malicious adware - [details >>](#)
- **LinkScanner** protects you from web-based attacks while you search and surf the Internet - [details >>](#)
- **E-mail Protection** checks your incoming e-mail messages for SPAM, and blocks viruses, phishing attacks, or other threats - [details >>](#)
- **Firewall** controls all communication on each network port, protecting you from malicious attacks and blocking all intrusion attempts - [details >>](#)



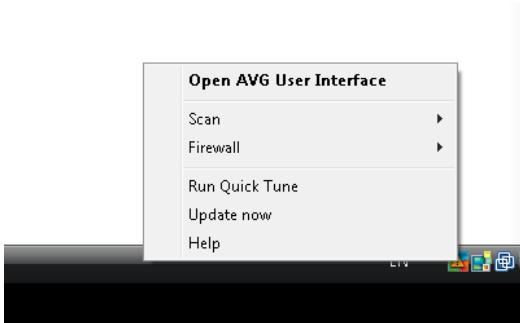
- **Identity Alert** scours dodgy websites and online networks for potential trade of your identity details - [details >>](#)
- **Anti-Rootkit** scans for dangerous rootkits hidden inside applications, drivers, or libraries - [details >>](#)
- **System Tools** offers a detailed summary of the AVG environment and operating system information - [details >>](#)
- **Quick Tune** provides detailed analytical information about your computer status, and offers optimization - [details >>](#)
- **Identity Protection** is constantly protecting your digital assets against new and unknown threats - [details >>](#)

### Actions accessible





- **Move mouse over 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](#).
- **Single-click any component's icon** to open the component's own interface with a list of basic statistical data.
- **Right-click your mouse over a component's icon** to expand a context menu with several options:
  - **Open** - Click this option to open the component's own dialog (*just like with a single-click on the component's icon*).
  - **Ignore the state of this component** - Select this option to express you are aware of the [component's error state](#) but for some reason you wish to keep this status, and you do not want to be warned by the [system tray icon](#).
  - **Open in Advanced settings ...** - This option is only available for some components; i.e. those that provide the possibility of [advanced settings](#).

## 5.5. System Tray Icon

**AVG System Tray Icon** (on your Windows taskbar, right-hand bottom corner of your monitor) indicates the current status of your **AVG Premium Security 2012**. It is visible at all times on your system tray, no matter whether the [user interface](#) of your **AVG Premium Security 2012** is opened or closed:

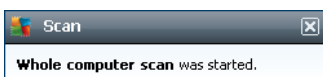


### AVG System Tray Icon display

-  In full color with no added elements the icon indicates that all **AVG Premium Security 2012** components are active and fully functional. However, the icon can also be displayed this way in a situation when one of the components is not fully functional but the user has decided to [ignore the component state](#). (*Having confirmed the ignore the component state option you express you are aware of the [component's error state](#) but for some reason you wish to keep it so, and you do not want to be warned about the situation.*)
-  The icon with an exclamation mark indicates that a component (*or even more components*) are in [error state](#). Always pay attention to such a warning and try to remove the configuration issue of a component that is not set up properly. In order to be able to perform the changes in component's configuration, double click the system tray icon to open the [application user interface](#). For detailed information on which components is in [error state](#) please consult the [security status info](#) section.
-  The system tray icon can further be displayed in full color with a flashing and rotating beam of light. This graphic version signalizes a currently launched update process.
-  The alternative display of a full color icon with an arrow means that one of the **AVG Premium Security 2012** scans is just running.

### AVG System Tray Icon information

**AVG System Tray Icon** further informs on current activities within your **AVG Premium Security 2012**, and on possible status changes in the program (e.g. *automatic launch of a scheduled scan or update, Firewall profile switch, a component's status change, error status occurrence, ...*) via a pop-up window opened from the system tray icon:



### Actions accessible from AVG System Tray Icon

**AVG System Tray Icon** can also be used as a quick link to access the [user interface](#) of **AVG**



**Premium Security 2012**, just double click on the icon. By right-click on the icon you open a brief context menu with the following options:

- **Open AVG User Interface** - Click to open the [user interface](#) of **AVG Premium Security 2012**.
- **Scans** - Click to open the context menu of [predefined scans](#) ([Whole Computer scan](#), [Scan Specific Files or Folders](#), [Anti-Rootkit scan](#)) and select the required scan, it will be launched immediately.
- **Firewall** - Click to open the context menu of [Firewall](#) settings options where you can edit the major parameters: [Firewall status](#) ([Firewall enabled](#)/[Firewall disabled](#)/[Emergency mode](#)), [gaming mode switching](#) and [Firewall profiles](#).
- **Run Quick Tune** - Click to launch the [Quick Tune](#) component.
- **Running scans** - This item is displayed only in case a scan is currently running on your computer. For this scan you can then set its priority, alternatively stop or pause the running scan. Further, the following actions are accessible: [Set priority for all scans](#), [Pause all scans](#) or [Stop all scans](#).
- **Update now** - Launches an immediate [update](#).
- **Help** - Opens the help file on the start page.



## 5.6. AVG gadget

**AVG gadget** displays on the Windows desktop (*Windows Sidebar*). This application is only supported in operating systems Windows Vista and Windows 7. **AVG gadget** offers an immediate access to the most important **AVG Premium Security 2012** functionality, i.e. [scanning](#) and [updating](#):



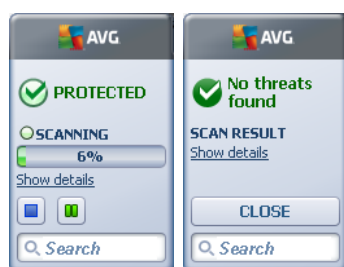
### Quick access to scanning and updating

If needed, **AVG gadget** allows you to launch a scan or an update immediately:

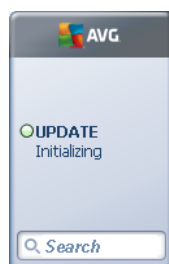
- **Scan now** - Click the **Scan now** link to start the [whole computer scan](#) directly. You can watch the progress of the scanning process in the alternated user interface of the gadget. A brief statistics overview provides information on the number of scanned objects, threats detected, and threats healed. During the scan you can always pause , or stop  the



scanning process. For detailed data related to the scan results please consult the standard [Scan results overview](#) dialog that can be opened directly from the gadget via the **Show details** option (*the respective scan results will be listed under Sidebar gadget scan*).




- **Update now** - Click the **Update now** link to launch the **AVG Premium Security 2012** update directly from within the gadget:




### Social networks access

**AVG gadget** also provides a quick link connecting you to the major social networks. Use the respective button to get connected to AVG communities in Twitter, Facebook, or LinkedIn:


- **Twitter link**  - Opens a new **AVG gadget** interface providing an overview of the latest AVG feeds posted at the Twitter. Follow the **View all the AVG Twitter feeds** link to open your Internet browser in a new window, and you will be redirected directly to the Twitter website, specifically to the page devoted to AVG related news:



- **Facebook link**  - Opens your Internet browser on the Facebook website, specifically on the **AVG community** page.



### Other features accessible via gadget

- **Quick Tune**  - Open the user interface in the [Quick Tune](#) component, and starts the analysis right away.
- **Search box** - Type in a keyword and get the search results immediately in a newly opened window with your default web browser.



## 6. AVG Components

### 6.1. Anti-Virus

The **Anti-Virus** component is a cornerstone of your **AVG Premium Security 2012** and it combines several fundamental features of a security program:

- [Scanning Engine](#)
- [Resident Protection](#)
- [Anti-Spyware Protection](#)

#### 6.1.1. Scanning Engine

The scanning engine that is the base of the **Anti-Virus** component 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 in [Virus Vault](#).

***The important feature of AVG Premium Security 2012 protection is that no known virus can run on the computer!***

#### Detection methods

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. **Anti-Virus** uses the following detection methods:

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

Where just a single technology might fall short of detecting or identifying a virus, **Anti-Virus** combines several technologies to ensure that your computer is protected from viruses. **AVG Premium Security 2012** 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 Premium Security 2012** 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.

***AVG Premium Security 2012 provides non-stop protection to your computer!***



### 6.1.2. Resident Protection

**AVG Premium Security 2012** gives you continuous protection in form of so called resident protection. The **Anti-Virus** component scans every single file (*with specific extensions or without extensions at all*) that is being opened, saved, or copied. It guards the system areas of the computer, and removable media (*flash disk etc.*). In case a virus is discovered 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 the resident protection runs "in the background". You only get notified when threats are found; at the same time, **Anti-Virus** blocks activation of the threat and removes it.

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

### 6.1.3. Anti-Spyware Protection

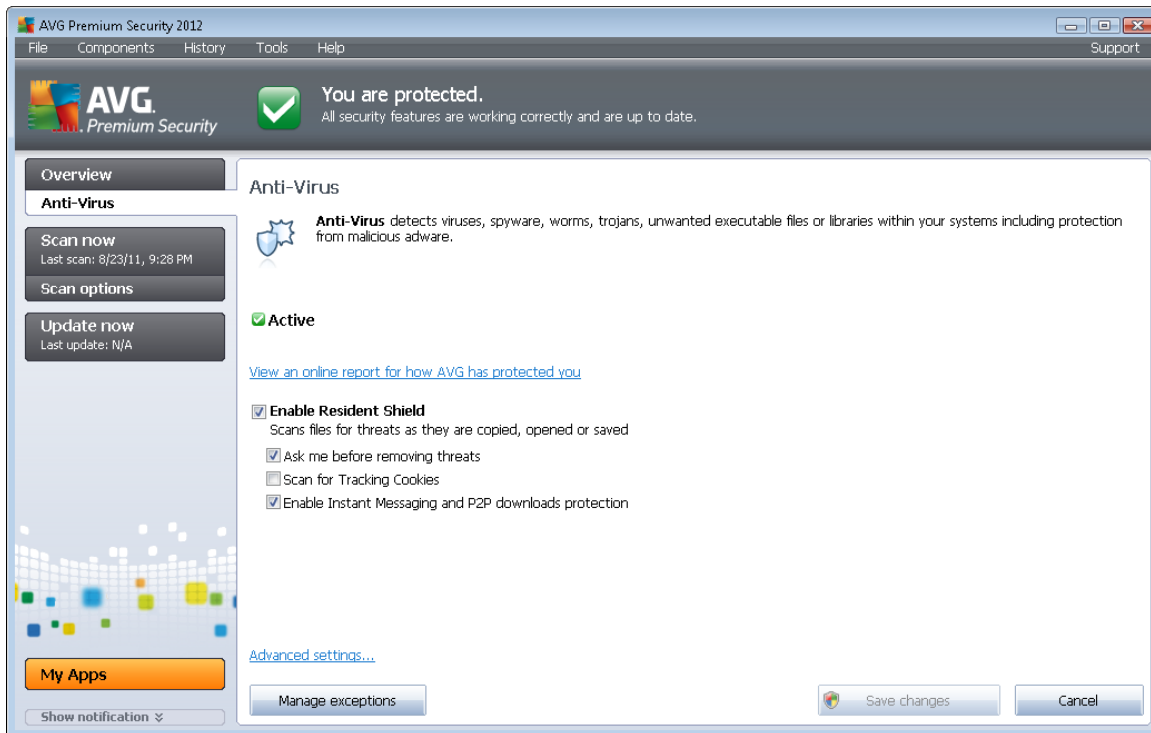
**Anti-Spyware** consists of a spyware database used for identifying known types of spyware definitions. AVG spyware experts work hard to identify and describe the latest spyware patterns as soon as they emerge, and then add the definitions to the database. Via the update process, these new definitions are downloaded to your computer so that you are always reliably protected even against the latest spyware types. **Anti-Spyware** allows you to fully scan your computer for malware/spyware. It also detects sleeping and non-active malware, i.e. malware that has been downloaded but not yet activated.

#### What is a spyware?

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.

### 6.1.4. Anti-Virus Interface

The **Anti-Virus** component's interface provides brief information on the component's functionality, information on the component's current status (*Active*), and basic configuration options of the component:



## Configuration options

The dialog provides some elementary configuration options of features available within the **Anti-Virus** component. Following you can find a brief description of these:

- **View an online report for how AVG has protected you** - The link redirects you to a specific page on AVG website (<http://www.avg.com/>). In the page you can find a detailed statistical overview of all **AVG Premium Security 2012** activities performed on your computer within a specified period of time, and in a total.
- **Enable Resident Shield** - This option allows you to easily switch on/off resident protection. 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. By default, the function is on, and it is recommended to keep it so! With resident protection on you can further decide how the possibly detected infections should be treated:
  - **Ask me before removing threats** - Keep the option checked to confirm you want to be asked any time a threat is detected before it is removed to [Virus Vault](#). This choice has no impact on the security level, and it only reflects your preferences.
  - **Scan for Tracking Cookies** - Independently on previous options, you can decide whether you want to scan for tracking cookies. (*Cookies are 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.*) In specific cases you can switch this



option on to achieve maximum security levels, however it is switched off by default.

- **Enable Instant Messaging and P2P downloads protection** - Check this item if you wish to verify that the instant messaging communication (e.g. ICQ, MSN Messenger, ...) is virus free.
- **Advanced settings...** - Click the link to get redirected to the respective dialog within the [Advanced settings](#) of **AVG Premium Security 2012**. There you can edit the component's configuration in detail. However, please note that the default configuration of all components is set up so that **AVG Premium Security 2012** provides optimum performance, and maximum security. Unless you have a real reason to do so, it is recommended to keep the default configuration!

### Control buttons

Within the dialog you may use the following control buttons:

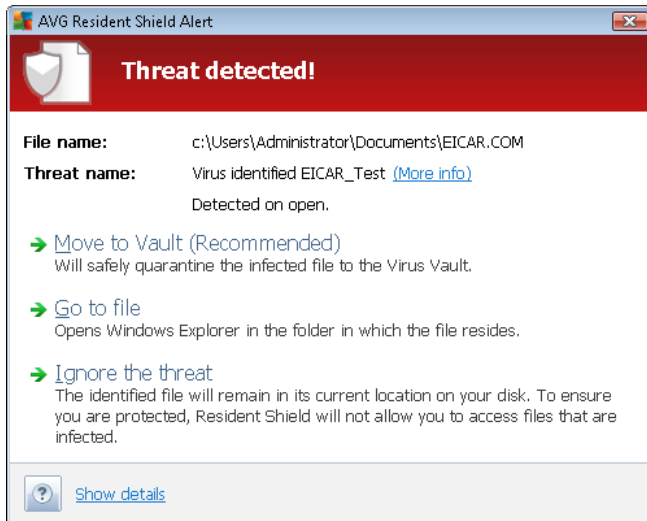
- **Manage exceptions** - Open a new dialog named **Resident Shield - Exceptions**. The configuration of exceptions from Resident Shield scanning is also accessible from the main menu, following the sequence of [Advanced settings / Anti-Virus / Resident Shield / Exceptions](#) (please see the respective chapter for detailed description). Within the dialog you may specify files and folders that should be excluded from the Resident Shield scanning. If this is not essential, we strongly recommend not excluding any items! The dialog provides the following control buttons:
  - **Add Path** – Specify a directory (or directories) to be excluded from the scanning by selecting them one by one from the local disk navigation tree.
  - **Add File** – Specify files to be excluded from the scanning by selecting them one by one from the local disk navigation tree.
  - **Edit Item** – Allows you to edit the specified path to a selected file or folder.
  - **Remove Item** – Allows you to delete the path to a selected item from the list.
  - **Edit List** - Allows you to edit the entire list of defined exceptions in a new dialog that behaves like a standard text editor.
- **Apply** - Save all changes to the component's settings performed in this dialog, and return to the main [user interface](#) of **AVG Premium Security 2012** (components overview).
- **Cancel** - Call off all changes to the component's settings performed in this dialog. No changes will be saved. You will return to the main [user interface](#) of **AVG Premium Security 2012** (components overview).

## 6.1.5. Resident Shield Detections

### Threat detected!



**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:



Within this warning dialog you will find data on the file that was detected and assigned as infected (*File name*), the name of the recognized infection (*Threat name*), and a link to the [Virus encyclopedia](#) where you can find detailed information on the detected infection, if known (*More info*).

Further, you have to decide what action should be taken now. Several alternative options are available. **Please note that, upon specific conditions (what kind of file is infected, and where it is located), not all of the options are always available!**

- **Heal** - this button only appears if the detected infection can be healed. Then, it removes it from the file, and restores the file to the original state. If the file itself is a virus, use this function to delete it (*i.e. removed to the [Virus Vault](#)*)
- **Move to Vault (Recommended)** - the virus will be moved to [Virus Vault](#)
- **Go to file** - this option redirects you to the exact location of the suspicious object (*opens new Windows Explorer window*)
- **Ignore the threat** - we strictly recommend NOT TO use this option unless you have a very good reason to do so!

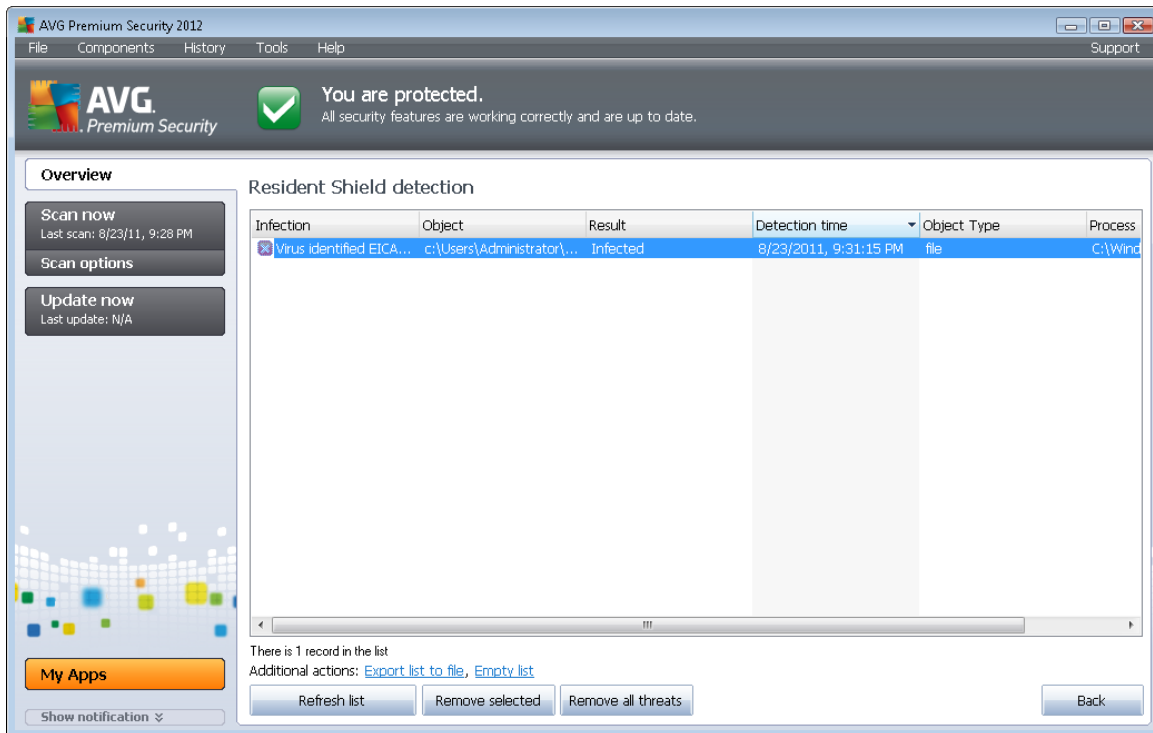
**Note:** It may happen that the size of the detected object exceeds the free space limit in Virus Vault. If so, a warning message pops up informing you about the issue as you try to move the infected object to Virus Vault. However, the Virus Vault size can be edited. It is defined as an adjustable percentage of the real size of your hard disk. To increase the size of your Virus Vault, go to the [Virus Vault](#) dialog within the [AVG Advanced Settings](#), via the 'Limit Virus Vault size' option.

In the bottom section of the dialog you can find the link **Show details** - click it to open a pop-up window with detailed information on the process running while the infection was detected, and the process' identification.



## Resident Shield detections overview

The entire overview of all threats detected by [Resident Shield](#) can be found in the **Resident Shield detection** dialog accessible from system menu option [History / Resident Shield detection](#):



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](#)



[main dialog](#) (components overview).

## 6.2. Link Scanner

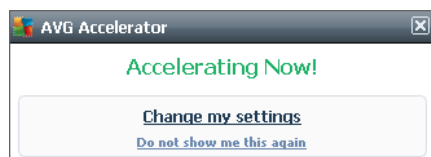
**LinkScanner** protects you from the increasing number of 'here today, gone tomorrow' threats on the web. These threats can be hidden on any type of website, from governments to big, well-known brands to small businesses, and they rarely stick around on those sites for more than 24 hours.

**LinkScanner** protects you by analyzing the web pages behind all the links on any web page you're viewing and making sure they're safe at the only time that matters – when you're about to click that link.

***LinkScanner is not intended for server platforms protection!***

The **LinkScanner** technology consists of the following main features:

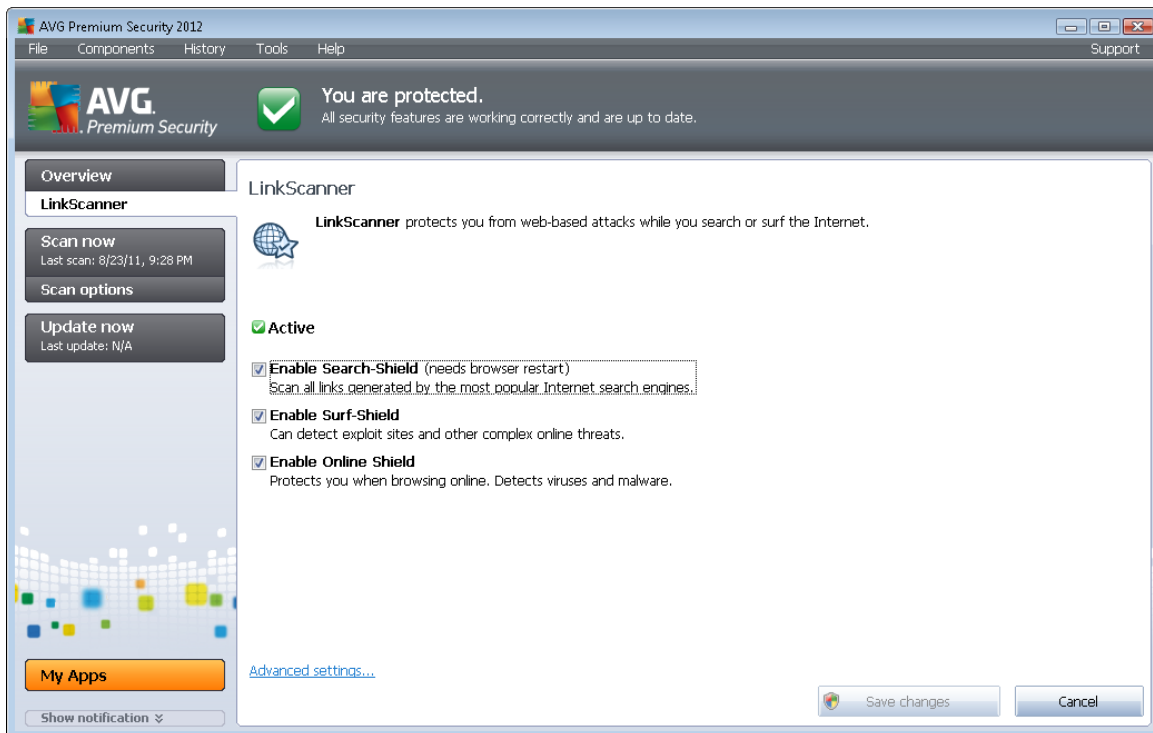
- **Search-Shield** contains list of websites (*URL addresses*) which are known to be dangerous. When searching with Google, Yahoo! JP, eBay, Twitter, Digg, SlashDot, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, and Seznam, all results of the search are checked according to this list and a verdict icon is shown (*for Yahoo! search results only "exploited website" verdict icons are shown*).
- **Surf-Shield** scans the contents of the websites you are visiting, regardless of the websites address. Even if some website is not detected by **Search-Shield** (*e.g. when a new malicious website is created, or when a previously clean website now contains some malware*), it will be detected and blocked by **Surf-Shield** once you try to visit it.
- **Online Shield** works as a real-time protection when surfing the Internet. It scans the contents of visited web pages, and possible files included in them, even before these are displayed in your web browser or downloaded to your computer. **Online Shield** detects viruses and spyware contained in the page you are about to visit and stops the download instantly so that no threats ever get to your computer.
- **AVG Accelerator** allows smoother online video playback and makes additional downloads easier. When the video-acceleration process is in progress, you will be notified via the system tray pop-up window.





### 6.2.1. Link Scanner Interface

The [LinkScanner](#) component main dialog provides a brief description of the component's functionality and information on its current status (*Active*):



In the bottom part of the dialog some basic configuration of the component is available:

- **Enable [Search-Shield](#)** - (on by default): Uncheck the box only if you have a good reason to switch off the Search Shield functionality.
- **Enable [Surf-Shield](#)** - (on by default): Active (*real-time*) protection against exploitive sites as they are accessed. Known malicious site connections and their exploitive content is blocked as they are accessed by the user via a web browser (*or any other application that uses HTTP*).
- **Enable [Online Shield](#)** - (on by default): Real-time scanning of the web pages you are about to visit for possible viruses or spyware. If these are detected, the download stops immediately so that no threats ever get to your computer.






### 6.2.2. Search-Shield detections

When searching Internet with the **Search-Shield** on, all search results returned from the most popular search engines (*Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, and SlashDot*) are evaluated for dangerous or suspicious links. By checking these links and marking the bad links, the [LinkScanner](#) warns you before you click on dangerous or suspicious links, so you can ensure you only go to safe websites.

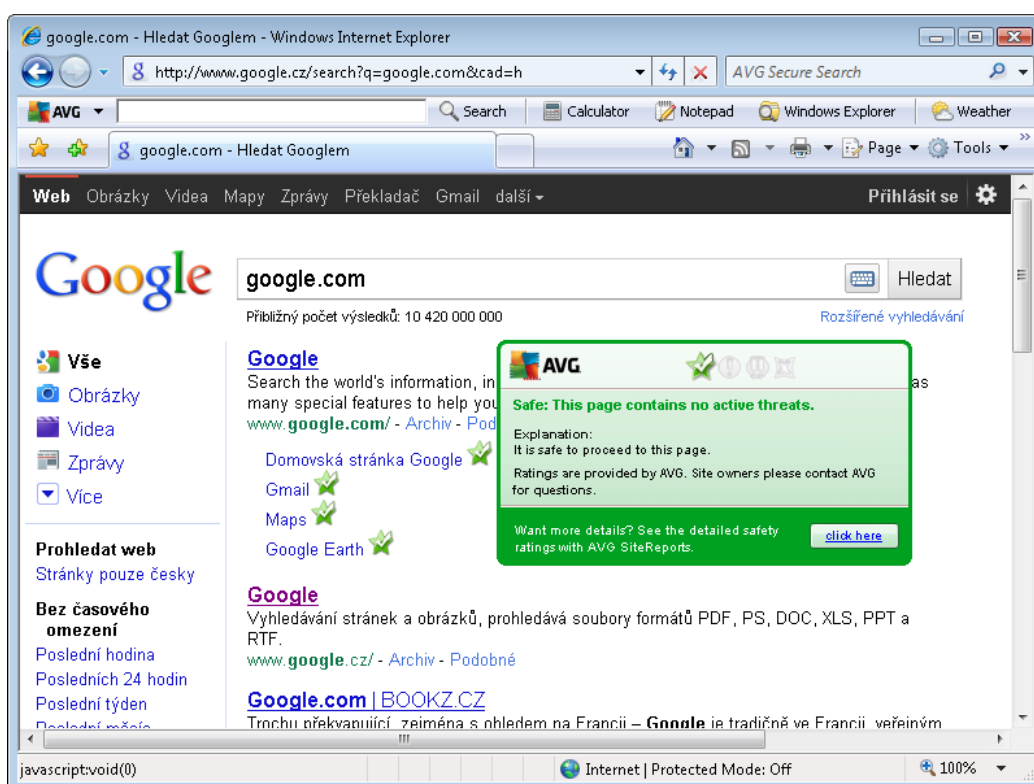
While a link is being evaluated on the search results page, you will see a graphic sign next to the



link informing that the link verification is in progress. When the evaluation is complete, the respective informative icon will be displayed:

-  The linked page is safe.
-  The linked page does not contain threats but is somewhat suspicious (*questionable in origin or motive, therefore not recommended for e-shopping etc.*).
-  The linked page can be either safe itself, but containing further links to positively dangerous pages; or suspicious in code, though not directly employing any threats at the moment.
-  The linked page contains active threats! For your own safety, you will not be allowed to visit this page.
-  The linked page is not accessible, and so could not be scanned.

Hovering over an individual rating icon will display details about the particular link in question. Information include additional details of the threat (*if any*):

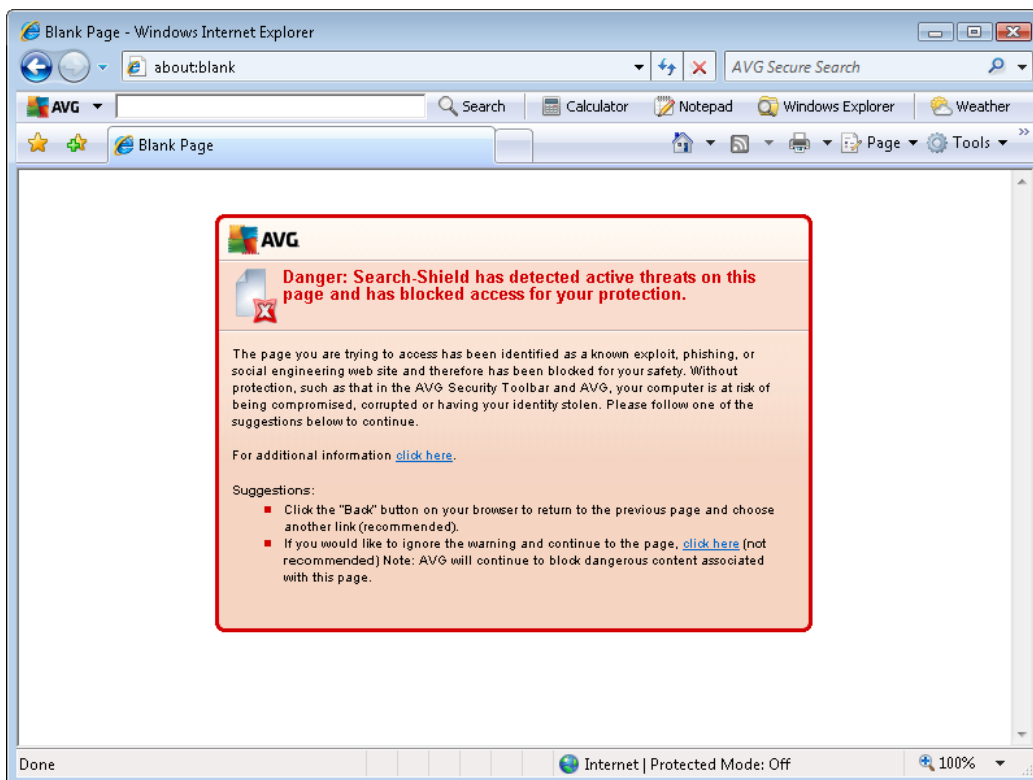




### 6.2.3. Surf-Shield detections

This powerful protection will block malicious content of any webpage you try to open, and prevent it from being downloaded to your computer. With this feature enabled, clicking a link or typing in a URL to a dangerous site will automatically block you from opening the web page thus protecting you from inadvertently being infected. It is important to remember that exploited web pages can infect your computer simply by visiting the affected site, for this reason when you request a dangerous webpage containing exploits or other serious threats, the [LinkScanner](#) will not allow your browser to display it.

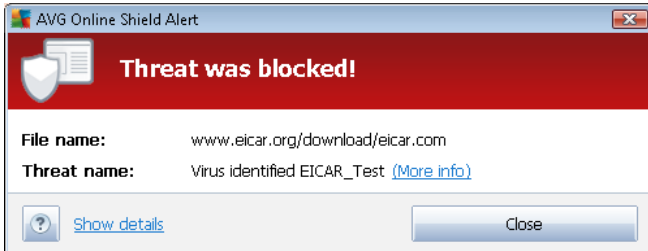
If you do encounter a malicious web site, within your web browser the [LinkScanner](#) will warn you with a screen similar to:



***Entering such web site is highly risky and it cannot be recommended!***

### 6.2.4. Online Shield detections

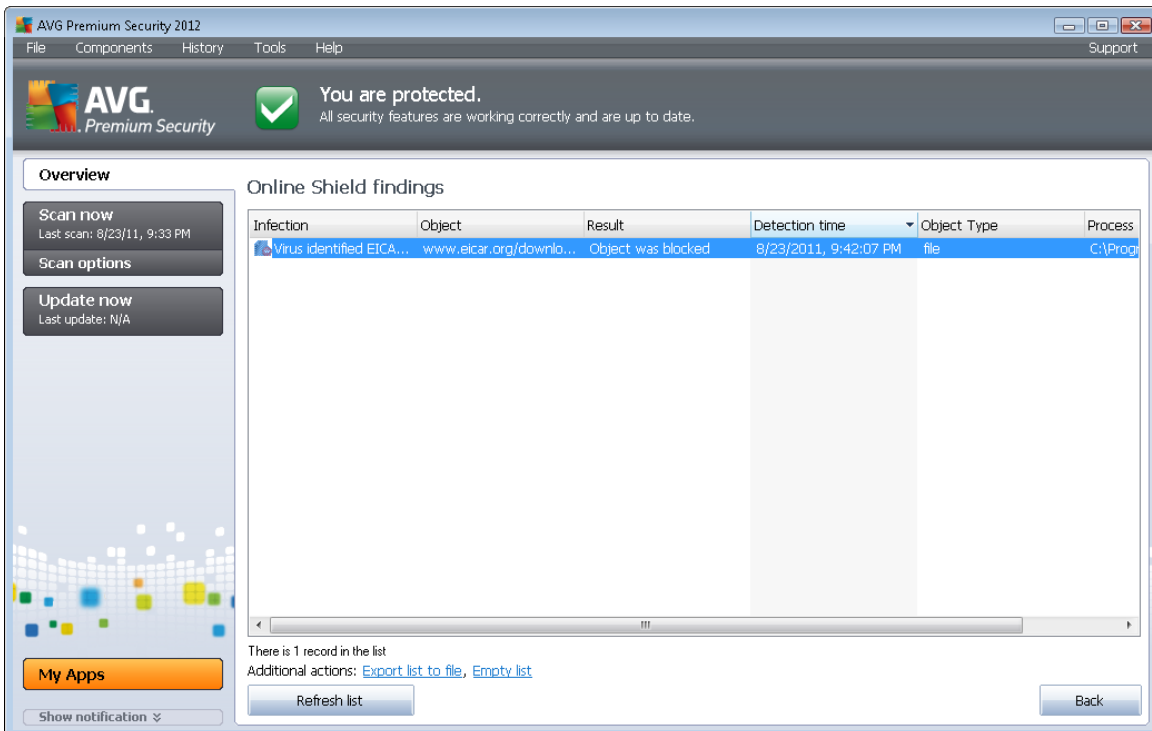
**Online Shield** scans the content of visited web pages and possible files included in them even before these are displayed in your web browser or downloaded to your computer. If a threat is detected, you will be warned immediately with the following dialog:



Within this warning dialog you will find data on the file that was detected and assigned as infected (*File name*), the name of the recognized infection (*Threat name*), and a link to the [Virus encyclopedia](#) where you can find detailed information on the detected infection (*if known*). The dialog provides the following buttons:

- **Show details** - click the **Show details** button to open a new pop-up window where you can find information on the process running while the infection was detected, and the process' identification.
- **Close** - click the button to close the warning dialog.

The suspect web page will not be opened, and the threat detection will be logged in the list of **Online Shield findings** - this overview of detected threats is accessible via system menu [History / Online Shield findings](#).



For each detected object the following information is provided:

- **Infection**- description (*possibly even name*) of the detected object



- **Object** - object source (*web page*)
- **Result** - action performed with the detected object
- **Detection time** - date and time the threat was detected and blocked
- **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**).

### Control buttons

- **Refresh list** - update the list of finding detected by **Online Shield**
- **Back** - switch back to the default [AVG main dialog](#) (*components overview*)

## 6.3. E-mail Protection

One of the most common sources of viruses and trojans is via e-mail. Phishing and spam make e-mail an even greater source of risks. Free e-mail accounts are more likely to receive such malicious e-mails (*as they rarely employ anti-spam technology*), and home users rely quite heavily on such e-mail. Also home users, surfing unknown sites and filling in online forms with personal data (*such as their e-mail address*) increase exposure to attacks via e-mail. Companies usually use corporate e-mail accounts and employ anti-spam filters etc, to reduce the risk.

The **E-mail Protection** component is responsible for scanning every e-mail message, sent or received; whenever a virus is detected in an e-mail, it is removed to the [Virus Vault](#) immediately. The component can also filter out certain types of e-mail attachments, and add a certification text to infection-free messages. **E-mail Protection** consists of two main functions:

- [E-mail Scanner](#)
- [Anti-Spam](#)

### 6.3.1. E-mail Scanner

**Personal E-mail Scanner** scans incoming/outgoing e-mails automatically. You can use it with e-mail clients that do not have their own plug-in in AVG (*but can be also used to scan e-mail messages for e-mail clients that AVG supports with a specific plug-in, i.e. Microsoft Outlook, The Bat, and Mozilla Thunderbird*). Primarily, it is to be used with e-mail applications like Outlook Express, Incredimail, etc.

During AVG [installation](#) there are automatic servers created for e-mail control: one for checking incoming e-mails and the second one for checking outgoing e-mails. Using these two servers e-mails are automatically checked on ports 110 and 25 (*standard ports for sending/receiving e-mails*).



**E-mail Scanner** works as an interface between e-mail client and e-mail servers on the Internet.

- **Incoming mail:** While receiving a message from the server, the **E-mail Scanner** component tests it for viruses, removes infected attachments, and adds certification. When detected, viruses are quarantined in [Virus Vault](#) immediately. Then the message is passed to the e-mail client.
- **Outgoing mail:** Message is sent from e-mail client to E-mail Scanner; it tests the message and its attachments for viruses and then sends the message to the SMTP server (*scanning of outgoing e-mails is disabled by default, and can be set up manually*).

**E-mail Scanner is not intended for server platforms!**

### 6.3.2. Anti-Spam

#### How does Anti-Spam work?

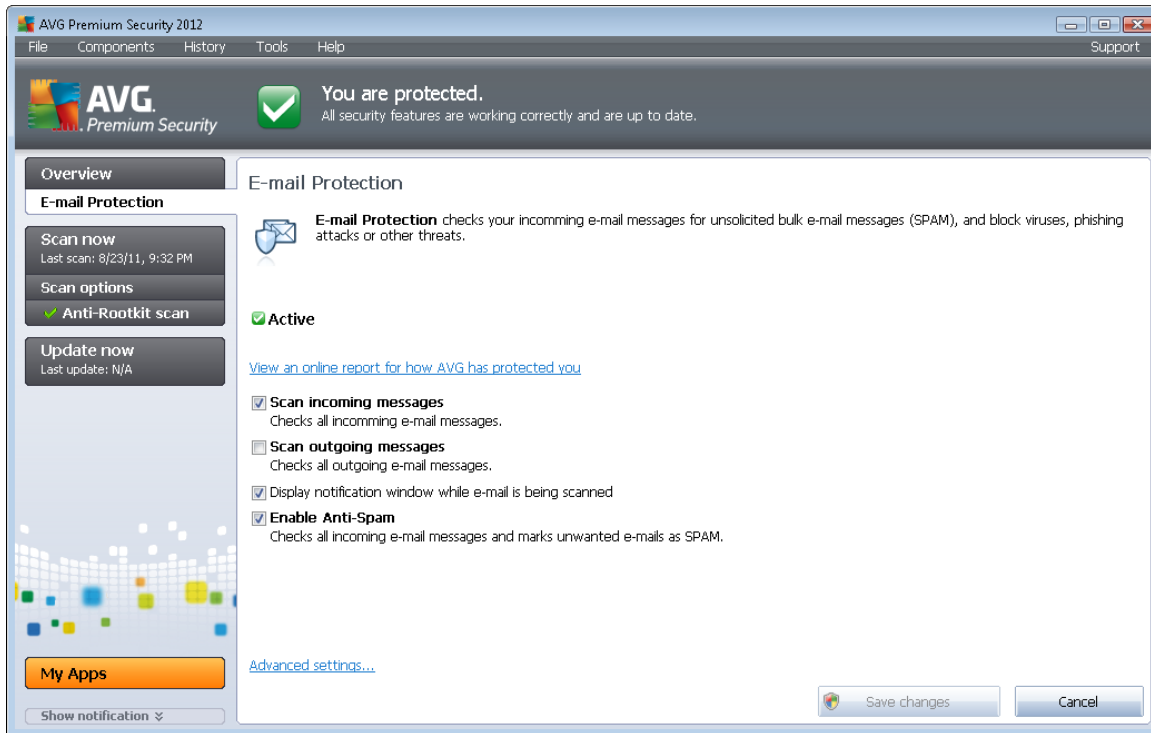
**Anti-Spam** checks all incoming e-mail messages and marks unwanted e-mails as spam. **Anti-Spam** can modify the subject of the email (*that has been identified as spam*) by adding a special text string. You can then easily filter your emails in your email client. **Anti-Spam** component uses several analyzing methods to process each e-mail message, offering maximum possible protection against unwanted e-mail messages. **Anti-Spam** uses a regularly updated database for the detection of spam. It is also possible to use [RBL servers](#) (*public databases of "known spammer" email addresses*) and to manually add email addresses to your [Whitelist](#) (*never mark as spam*) and [Blacklist](#) (*always mark as spam*).

#### What is a spam?

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



### 6.3.3. E-mail Protection Interface



In the **E-mail Protection** dialog you can find a brief text describing the component's functionality, and information on its current status (*Active*). Use the **View an online report for how AVG has protected you** link to review detailed statistics of **AVG Premium Security 2012** activities and detections on a dedicated page of AVG website (<http://www.avg.com/>).

#### Basic E-mail Protection settings

In the **E-mail Protection** dialog you can further edit some elementary features of the component's functionality:

- **Scan incoming messages** (*on by default*) - Tick the box to specify that all e-mails delivered to your account should be scanned for viruses.
- **Scan outgoing messages** (*off by default*) - Tick the box to confirm all e-mail sent from your account should be scanned for viruses.
- **Display notification window while e-mail is being scanned** (*on by default*) - Mark the item to confirm you want to be informed via notification dialog displayed over the [AVG icon on the system tray](#) during the scanning of your e-mail.
- **Enable [Anti-Spam](#)** (*on by default*) - Mark the item to specify whether you want to have your incoming mail filtered for unsolicited e-mail.

**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 **E-mail Protection** dialog are as follows:

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

### 6.3.4. E-mail Scanner Detections

Infection	Object	Result	Detection time	Object Type
Virus identified EICA...	eicar_com.zip	Moved to Virus Vault	8/23/2011, 9:28:36 PM	file

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

- **Infection**- description (possibly even name) of the detected object
- **Object** - object location
- **Result** - action performed with the detected object
- **Detection time** - date and time the suspicious object was detected



- **Object Type** - type of the detected object

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

### Control buttons

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

- **Refresh list** - Updates the list of detected threats.
- **Back** - Switches you back to the previously displayed dialog.

## 6.4. Firewall

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

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

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

**Computers that are not protected by Firewall become an easy target to computer hackers and data thefts.**

**Recommendation:** *Generally it is not recommended to use more than one firewall on an individual computer. The security of the computer is not enhanced if you install more firewalls. It is more probable that some conflicts between these two applications will occur. Therefore we recommend that you use only one firewall on your computer and deactivate all others, thus eliminating the risk of possible conflict and any problems related to this.*

### 6.4.1. Firewall Principles

In **AVG Premium Security 2012**, **Firewall** controls all traffic on every network port of your computer. Based on the defined rules, **Firewall** evaluates applications that are either running on your computer (*and want to connect to the Internet/local network*), or applications that approach your computer from outside trying to connect to your PC. For each of these applications **Firewall** then either allows or forbids the communication on the network ports. By default, if the application is unknown (*i.e. has no defined Firewall rules*), **Firewall** will ask you if you wish to allow or block the



communication attempt.

**AVG Firewall is not intended for server platforms!**

#### What AVG Firewall can do:

- Allow or block communication attempts of known [applications](#) automatically, or ask you for confirmation
- Use complete [profiles](#) with predefined rules, according to your needs
- [Switch profiles](#) automatically when connecting to various networks, or using various network adapters

#### 6.4.2. Firewall Profiles

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

#### Available profiles

- **Allow all** - a [Firewall](#) system profile that has been pre-set by the manufacturer and is always present. When this profile is activated, all network communication is allowed and no safety policy rules are applied, as if the [Firewall](#) protection was switched off (i.e. all applications are allowed but packets are still being checked - to completely disable any filtering you need to disable Firewall). This system profile cannot be duplicated, deleted, and its settings cannot be modified.
- **Block all** - a [Firewall](#) system profile that has been pre-set by the manufacturer and is always present. When this profile is activated, all network communication is blocked, and the computer is neither accessible from outer networks, nor can communicate outside. This system profile cannot be duplicated, deleted, and its settings cannot be modified.
- **Custom profiles** - the custom profiles enable you to take advantage of automatic profile switching which can be especially useful if you connect to various networks frequently (e.g. with a notebook). Custom profiles are generated automatically after **AVG Premium Security 2012** installation, and covering any individual needs for [Firewall](#) policy rules. The following custom profiles are available:
  - **Directly connected to the Internet** – suitable for common desktop home computers or notebooks connected directly to the Internet, without any extra protection. This option is also recommended when you connect your notebook to various unknown and probably unsecured networks (e.g. in the Internet cafe, hotel room, etc.). The strictest [Firewall](#) policy rules of this profile ensure that such computer is adequately protected.



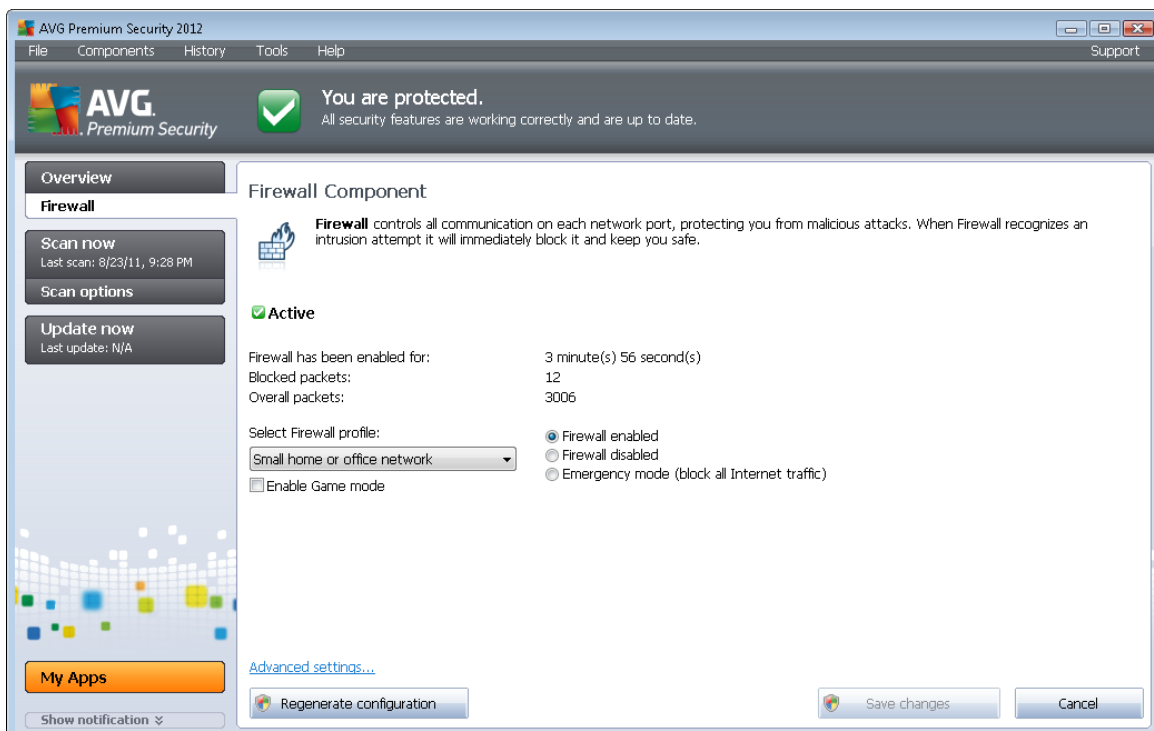
- **Computer within domain** – suitable for computers in a local network, typically at school or work. It is assumed that the network is professionally administered and protected by some additional measures, so the security level can be lower than in the above mentioned cases, allowing access to shared folders, disk units etc.
- **Small home or office network** – suitable for computers in a small network, typically at home or in a small business. Usually, this kind of network has no "central" administrator, and only consists of several computers connected together, often sharing a printer, scanner or similar device, which the [Firewall](#) rules must reflect.

### Profile switching

The profile switching feature allows the [Firewall](#) to switch automatically to the defined profile when using a certain network adapter, or when connected to a certain type of network. If no profile has been assigned to a network area yet, then upon next connection to that area, the [Firewall](#) will display a dialog asking you to assign a profile. You can assign profiles to all local network interfaces or areas and specify further settings in the [Areas and Adapters Profiles](#) dialog, where you can also disable the feature if you do not wish to use it (*then, for any kind of connection, the default profile will be used*).

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

### 6.4.3. Firewall Interface





The main dialog named **Firewall Component** provides some basic information on the component's functionality, its status (*Active*), and a brief overview of component's statistics:

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

### Basic Firewall settings

- **Select Firewall profile** - from the roll-down menu select one of the defined profiles (*for a detailed description of each profile and its recommended use please consult chapter [Firewall Profiles](#)*)
- **Enable Game mode** - Check this option to ensure that when running full-screen applications (*games, presentations, movies, etc.*), the [Firewall](#) will not display dialogs asking you whether you want to allow or block communication for unknown applications. In case an unknown application tries to communicate over the network at that time, the [Firewall](#) will allow or block the attempt automatically according to settings in the current profile. **Note:** With the gaming mode on, all scheduled tasks (scans, updates) are postponed till the application is closed.
- Further, in this basic settings section you can select from three alternative options defining the current status of the [Firewall](#) component:
  - **Firewall enabled (by default)** - select this option to allow communication to those applications that are assigned as 'allowed' in the set of rules defined within selected [Firewall](#) profile.
  - **Firewall disabled** - this option switches [Firewall](#) off completely, all network traffic is allowed but not checked!
  - **Emergency mode (block all Internet traffic)** - select this option to block all traffic on every single network port; [Firewall](#) is still running but all network traffic is stopped.

**Please note:** The software vendor has set up all AVG Premium Security 2012 components to give optimum performance. Unless you have a real reason to do so, do not change the AVG configuration. Any changes to settings should only be performed by an experienced user. If you need to change Firewall configuration, select the system menu item **Tools/Firewall settings** and edit the Firewall configuration in the newly opened [Firewall Settings](#) dialog.

### Control buttons

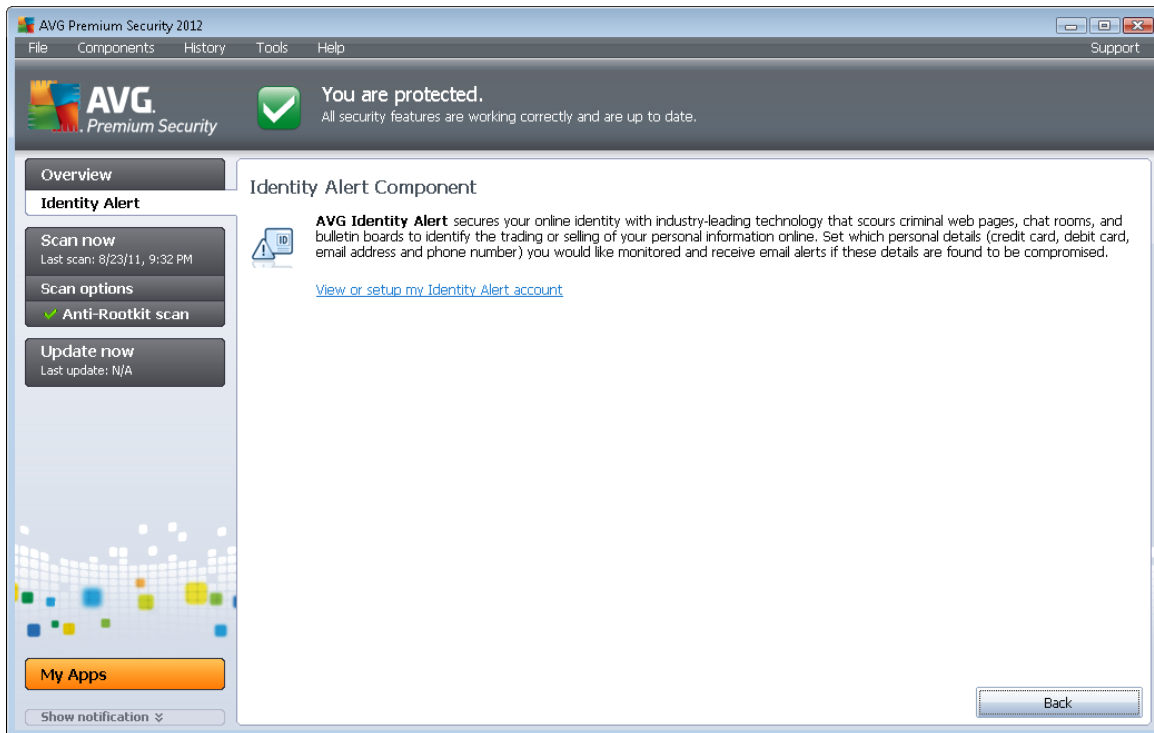
- **Regenerate configuration** - press this button to overwrite the current [Firewall](#) configuration, and to revert to the default configuration based on automatic detection.



- **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 main dialog](#) (*components overview*).

## 6.5. Identity Alert

The **Identity Alert** component provides access to a web-based service designed to discreetly monitor your personal details online. The details can include the following: credit card number, e-mail address, telephone (cell phone) number, etc. The monitoring is done on regular basis by verifying that these details have not been subject to potential misuse. Whenever the service detects anything suspicious, you will get notified via e-mail.



The **Identity Alert** dialog offers the only control element, and this is the **View or setup my Identity Alert account** link. Click the link to get online, and directly on the dedicated page on AVG website (<http://www.avg.com/>) you can register and set up all necessary details (*registration is required for you to be able to use this service*).

**Please note that since the service is web-based, and only runs online, you will need to be connected to the Internet in order to access the Identity Alert component.**

## 6.6. Anti-Rootkit

**Anti-Rootkit** is a specialized tool detecting and effectively removing dangerous rootkits, i.e. programs and technologies that can camouflage the presence of malicious software on your computer. **Anti-Rootkit** is able to detect rootkits based on a predefined set of rules. Please note, that all rootkits are detected (*not just the infected*). In case **Anti-Rootkit** finds a rootkit, it does not necessarily mean the rootkit is infected. Sometimes, rootkits are used as drivers or they are a part

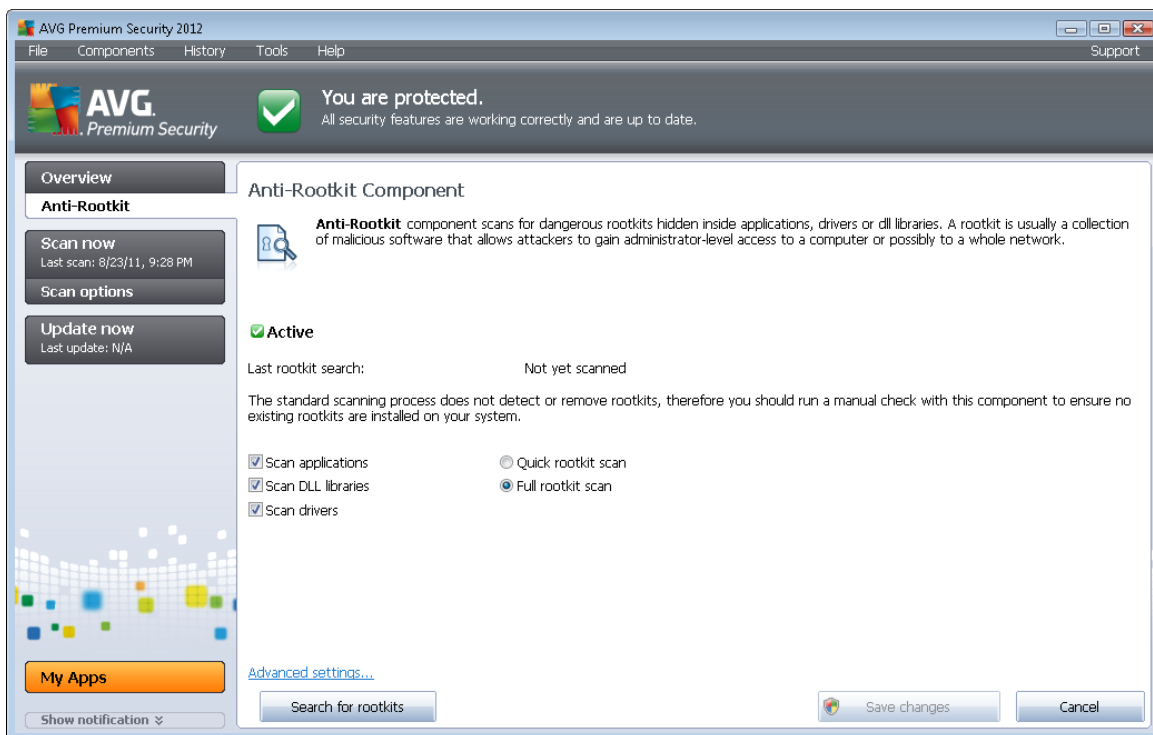


of correct applications.

### What is a rootkit?

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

### 6.6.1. Anti-Rootkit Interface



The **Anti-Rootkit** dialog provides a brief description of the component's functionality, informs on the component's current status (*Active*), and also brings information on the last time the **Anti-Rootkit** test was launched (**Last rootkit search**). The **Anti-Rootkit** dialog further provides the [Tools/Advanced Settings](#) link. Use the link to get redirected to the environment for advanced configuration of **Anti-Rootkit** component.

***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.***



### Basic Anti-Rootkit settings

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

- **Scan applications**
- **Scan DLL libraries**
- **Scan drivers**

Further you can pick the rootkit scanning mode:

- **Quick rootkit scan** - Scans all running processes, loaded drivers and the system folder (typically *c:\Windows*).
- **Full rootkit scan** - Scans all running processes, loaded drivers, the system folder (typically *c:\Windows*), plus all local disks (including the flash disk, but excluding floppy disk/CD drives).

### Control buttons

- **Search for rootkits** - Since the rootkit scan is not an implicit part of the [Scan of the whole computer](#), you can run the rootkit scan directly from the **Anti-Rootkit** interface using this button.
- **Save changes** - Press this button to save all changes made in this interface and to return to the default [AVG main dialog](#) (components overview).
- **Cancel** - Press this button to return to the default [AVG main dialog](#) (components overview) without having saved any changes you made.

## 6.7. System Tools

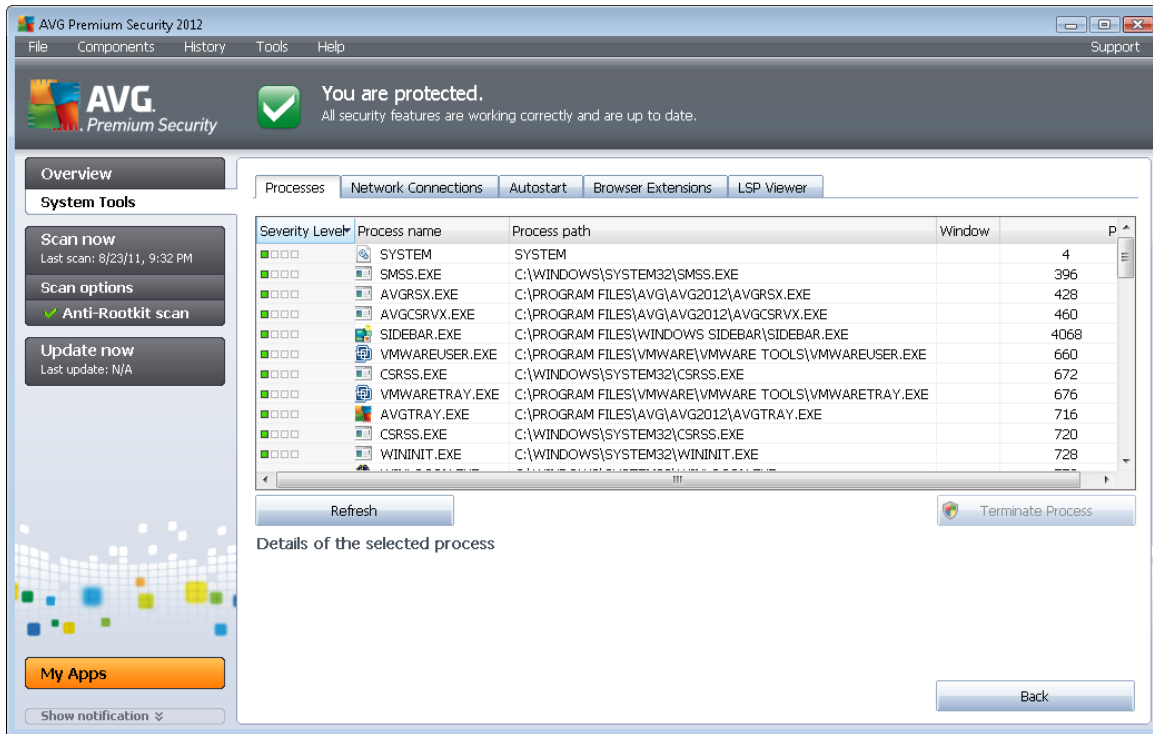
**System Tools** refer to tools offering a detailed summary of the **AVG Premium Security 2012** environment and the operating system. The component displays an overview of:

- [Processes](#) - list of processes (*i.e. running applications*) that are currently active on your computer
- [Network connections](#) - list of currently active connections
- [Autostart](#) - list of all applications that are executed during Windows system start-up
- [Browser Extensions](#) - list of plug-ins (*i.e. applications*) that are installed inside your Internet browser
- [LSP Viewer](#) - list of Layered Service Providers (*LSP*)



**Specific overviews can also be edited but this is only recommended for highly experienced users!**

### 6.7.1. Processes



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

- **Severity Level** – graphical identification of the respective process severity on a four-levels scale from less important (■□□□) up to critical (■□□■)
- **Process name** - name of the running process
- **Process path** - physical path to the running process
- **Window** - if applicable, indicates application Window name
- **PID** - process identification number is a unique Windows internal process identifier

#### Control buttons

The control buttons available within the **Processes** tab are as follows:

- **Refresh** - updates the list of processes according to the current status
- **Terminate Process** - you can select one or more applications and then terminate them by



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

- **Back** - switches you back to the default [AVG main dialog](#) (components overview)

## 6.7.2. Network Connections

Application	Protocol	Local Address	Remote Address	State
[System Process]	UDP	AutoTest-VST32:137		
[System Process]	TCP	AutoTest-VST32:139	AutoTest-VST32:0	Listening
[System Process]	TCP	AutoTest-VST32:49182	192.168.183.1:445	Connected
[System Process]	TCP	AutoTest-VST32:445	AutoTest-VST32:0	Listening
[System Process]	TCP6	[0:0:0:0:0:0:0:0]:445	[0:0:0:0:0:0:0:0]:0	Unknown
[System Process]	UDP	AutoTest-VST32:138		
[System Process]	TCP6	[0:0:0:0:0:0:0:0]:5357	[0:0:0:0:0:0:0:0]:0	Unknown
[System Process]	TCP	AutoTest-VST32:5357	AutoTest-VST32:0	Listening
wininit.exe	TCP	AutoTest-VST32:49152	AutoTest-VST32:0	Listening
wininit.exe	TCP6	[0:0:0:0:0:0:0:0]:49152	[0:0:0:0:0:0:0:0]:0	Unknown
svchost.exe	UDP6	[0:0:0:0:0:0:0:0]:5355		
svchost.exe	UDP6	[0:0:0:0:0:0:0:0]:62323		
svchost.exe	UDP	AutoTest-VST32:500		
svchost.exe	UDP	AutoTest-VST32:5355		
svchost.exe	UDP	AutoTest-VST32:1900		
svchost.exe	TCP6	[0:0:0:0:0:0:0:0]:49156	[0:0:0:0:0:0:0:0]:0	Unknown
svchost.exe	UDP6	[0:0:0:0:0:0:0:0]:1900		
svchost.exe	TCP	AutoTest-VST32:49156	AutoTest-VST32:0	Listening
svchost.exe	UDP6	[0:0:0:0:0:0:0:0]:500		

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

- **Application** - name of the application related to the connection (*with the exception of Windows 2000 where the information is not available*)
- **Protocol** - transmission protocol type used for the connection:
  - TCP - protocol used in conjunction with Internet Protocol (IP) to transmit information over the Internet
  - UDP - alternative to TCP protocol
- **Local address** - IP address of the local computer and the port number used
- **Remote address** - IP address of the remote computer and the port number connected to. If possible, it will also look up the host name of the remote computer.
- **State** - indicates the most probable current state (*Connected, Server should close, Listen, Active close finished, Passive close, Active close*)



To list only external connections, tick the **Hide local connections** checkbox in the bottom section of the dialog under the list.

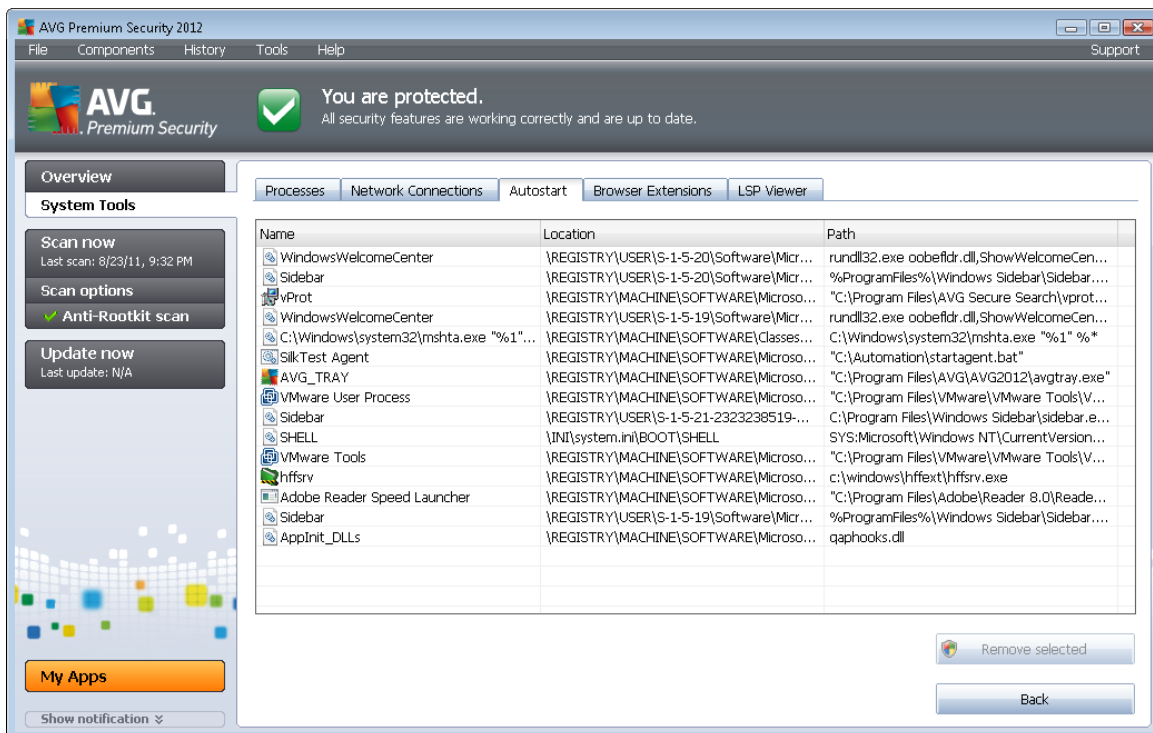
### Control buttons

The control buttons available within the **Network Connections** tab are as follows:

- **Terminate Connection** - closes one or more connections selected in the list
- **Terminate Process** - closes one or more applications related to connections selected in the list
- **Back** - switch back to the default [AVG main dialog](#) (components overview).

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

### 6.7.3. Autostart



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

### Control buttons

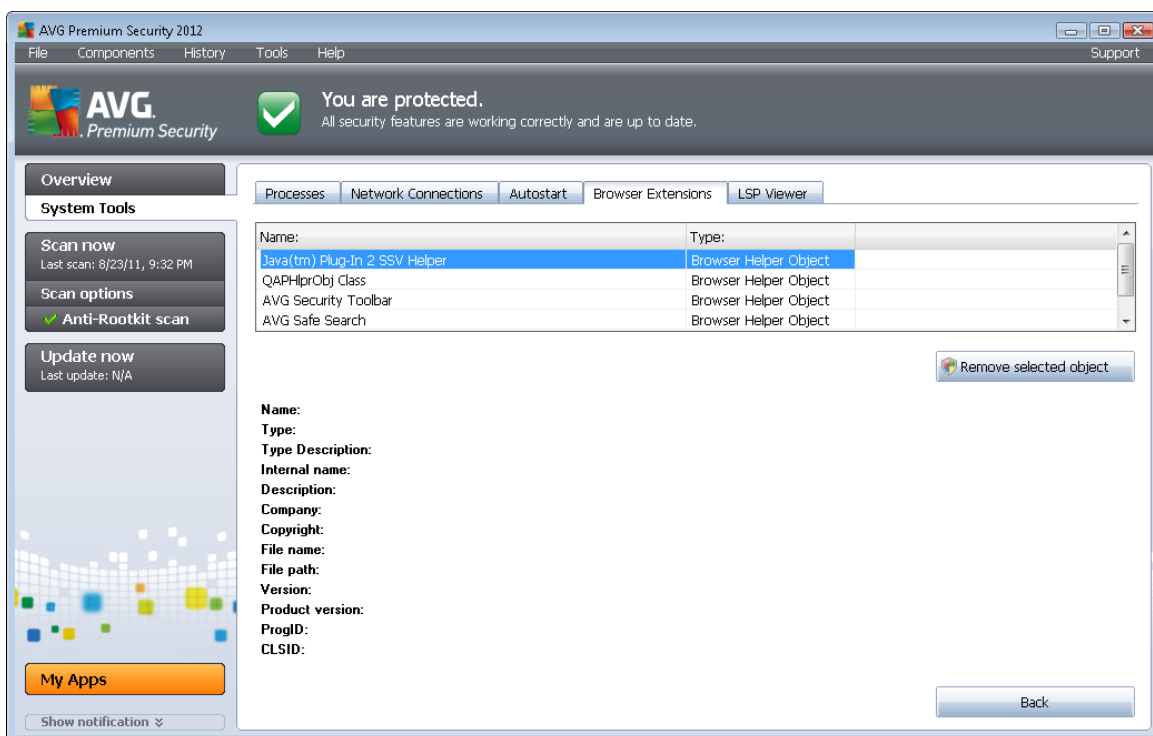


The control buttons available within the **Autostart** tab are as follows:

- **Remove selected** - press the button to delete one or more selected entries.
- **Back** - switches you back to the default [AVG main dialog](#) (*components overview*).

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

#### 6.7.4. Browser Extensions



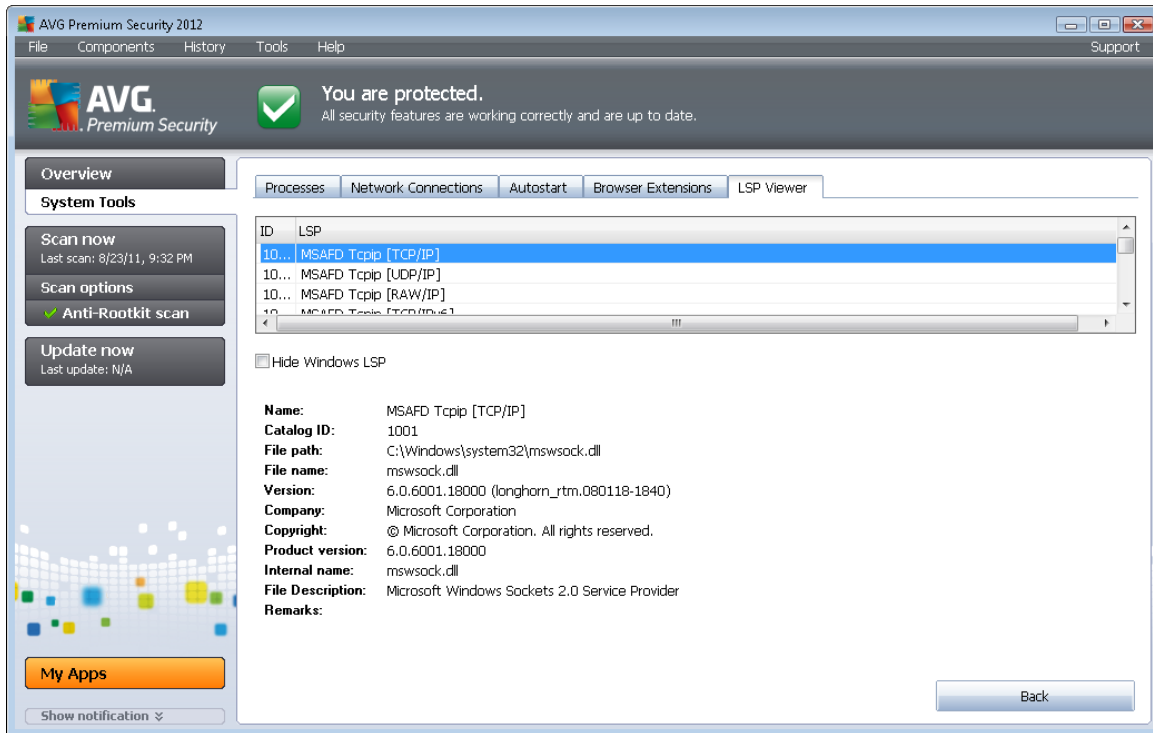
The **Browser Extensions** dialog contains a list of plug-ins (*i.e. applications*) that are installed inside your Internet browser. This list may contain regular application plug-ins as well as potential malware programs. Click on an object in the list to obtain detailed information on the selected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

#### Control buttons

The control buttons available within the **Browser Extensions** tab are as follows:

- **Remove selected object** - removes the plug-in that is currently highlighted in the list. **We strongly suggest not to delete any plug-ins from the list, unless you are absolutely sure that they represent a real threat!**
- **Back** - switches you back to the default [AVG main dialog](#) (*components overview*).

## 6.7.5. LSP Viewer



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

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

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

### Control buttons

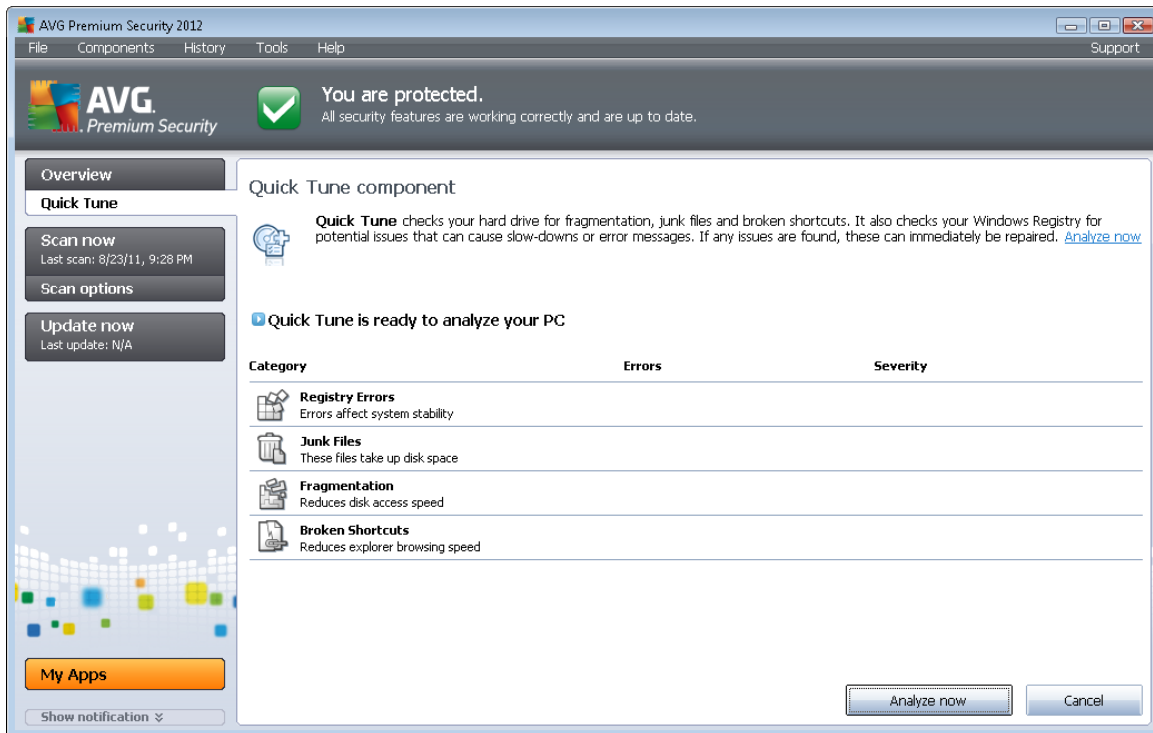
The control buttons available within the **LSP Viewer** tab are as follows:

- **Hide Windows LSP** - to include Windows LSP in the list, uncheck this item.
- **Back** - switches you back to the default [AVG main dialog](#) (*components overview*).



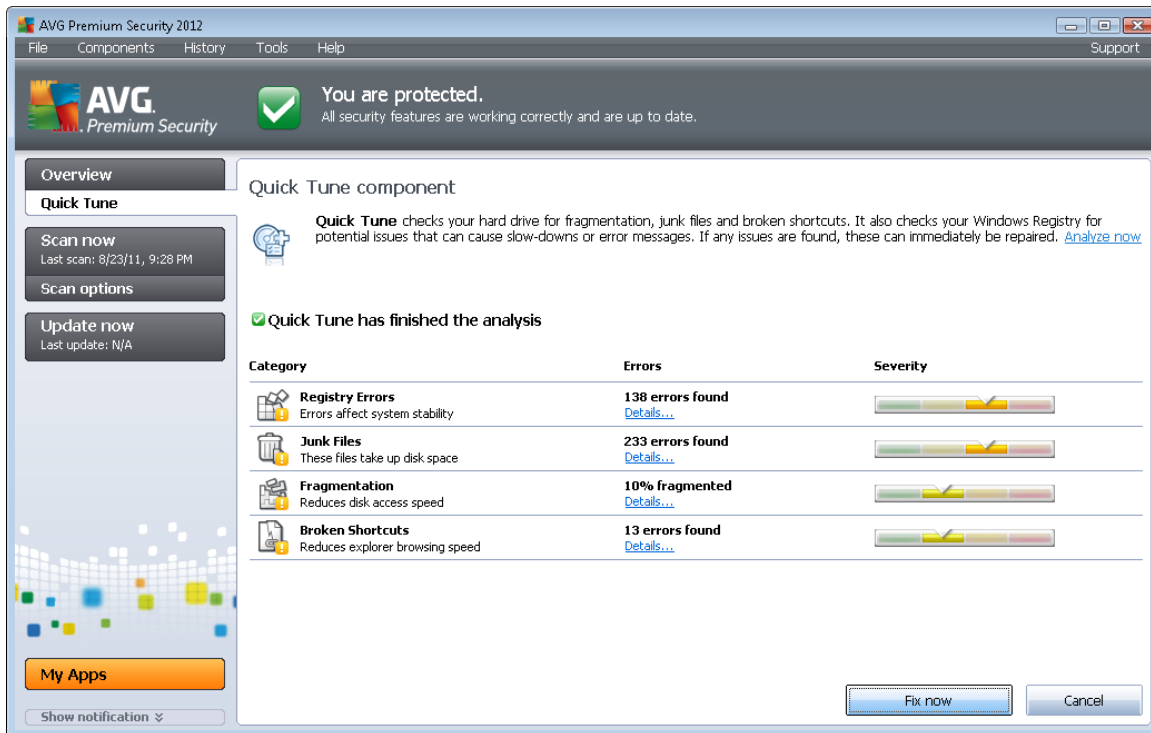
## 6.8. Quick Tune

The **Quick Tune** component is an advanced tool for detailed system analysis and correction, as to how the speed and overall performance of your computer might be improved. The following categories can be analysed and fixed: registry errors, junk files, fragmentation, and broken shortcuts.



- **Registry Errors** will give you the number of errors in Windows Registry that might be slowing your computer down, or causing error messages to appear.
- **Junk Files** will give you the number of files that use up your disk space, and can be most likely done without. Typically, these will be many kinds of temporary files, and files in the Recycle Bin.
- **Fragmentation** will calculate the percentage of your harddisk that is fragmented, i.e. used for a long time so that most files are now scattered on different parts of the physical disk.
- **Broken Shortcuts** will find shortcuts that no longer work, lead to non-existing locations etc.

To start the analysis of your system, press the **Analyze now** button. You will then be able to watch the analysis progress and its results directly in the chart:



The results overview provides the number of detected system problems (**Errors**) divided according to the respective categories tested. The analysis results will also be displayed graphically on an axis in the **Severity** column.

### Control buttons

- **Analyze now** (displayed before the analysis starts) - press this button to launch the immediate analysis of your computer
- **Fix now** (displayed once the analysis is finished) - press the button to fixing all found errors. You will get an overview of the result as soon as the correction process is finished.
- **Cancel** - press this button to stop the running analysis, or to return to the default [AVG main dialog](#) (components overview) once the analysis is completed

## 6.9. Identity Protection

**Identity Protection** is an anti-malware component that protects you from all kinds of malware (spyware, bots, identity theft, ...) using behavioral technologies and provide zero day protection for new viruses. **Identity Protection** is focused on preventing identity thieves from stealing your passwords, bank account details, credit card numbers and other personal digital valuables from all kinds of malicious software (malware) that target your PC. It makes sure that all programs running on your PC are operating correctly. **Identity Protection** spots and blocks suspicious behavior on a continuous basis and protects your computer from all new malware.

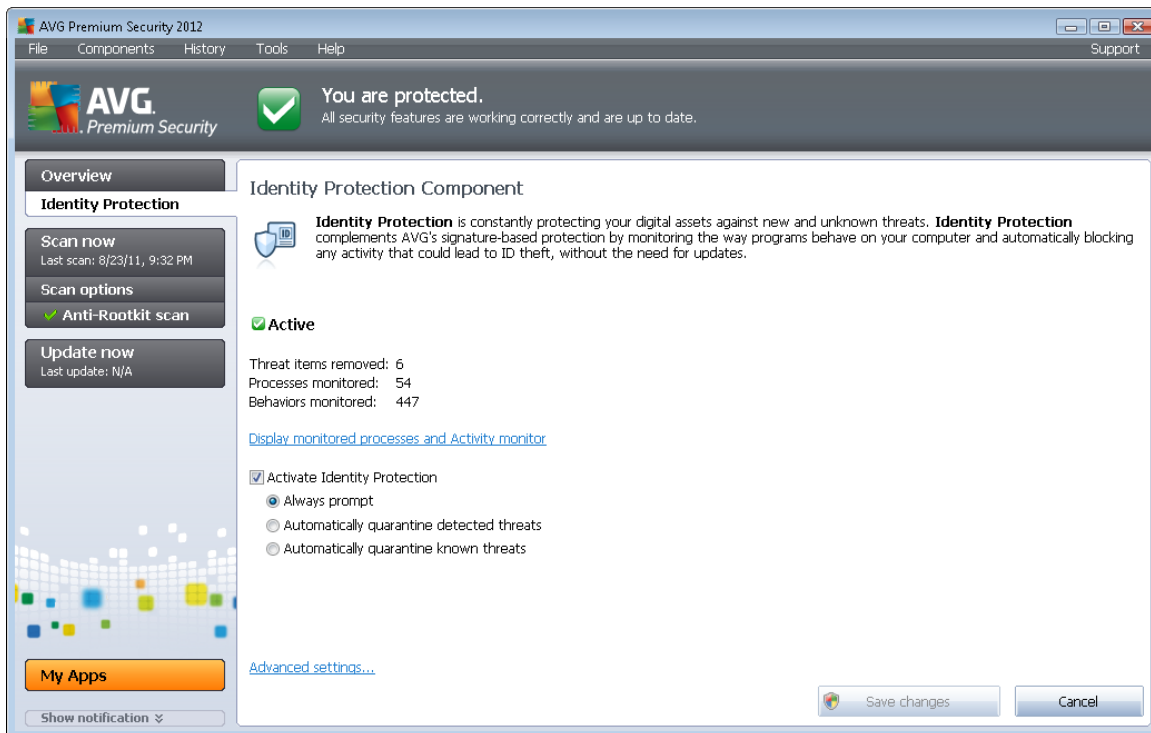
**Identity Protection** gives your computer a realtime protection against new and even unknown



threats. It monitors all (*including hidden*) processes and over 285 different behaviour patterns, and can determine if something malicious is happening within your system. For this reason, it can reveal threats not even yet described in the virus database. Whenever an unknown piece of code comes onto your computer, it is immediately watched for malicious behaviour, and tracked. If the file is found to be malicious, **Identity Protection** will remove the code into the [Virus Vault](#) and undo any changes that have been made to the system (*code injections, registry changes, ports opening etc*). You do not need to initiate a scan to be protected. The technology is very proactive, rarely needs updating, and is always on guard.

**Identity Protection is a complimentary protection to [Anti-Virus](#). We strongly recommend you have the both components installed, in order to have complete protection for your PC!**

### 6.9.1. Identity Protection Interface



**Identity Protection** dialog provides a brief description of the component's basic functionality, its status (*Active*), and some statistical data:

- **Threat items removed** - gives the number of applications detected as malware, and removed
- **Processes monitored** - number of currently running applications that are being monitored by IDP
- **Behaviors monitored** - number of specific actions running within the monitored applications

Below you can find the [Display monitored processes and Activity monitor](#) link that will take you to the user interface of the [System tools](#) component where you can find a detailed overview of all



monitored processes.

### Basic Identity Protection settings

In the bottom part of the dialog you can edit some elementary features of the component's functionality:

- **Activate Identity Protection** - (*on by default*): check to activate the IDP component, and to open further editing options.

In some cases, **Identity Protection** may report that some legitimate file is suspicious or dangerous. Since **Identity Protection** detects threats based on their behavior, this usually occurs when some program tries to monitor key presses, install other programs or a new driver is installed on the computer. Therefore please select one of the following options specifying **Identity Protection** component's behavior in case of a suspicious activity detection:

- **Always prompt** - if an application is detected as malware, you will be asked whether it should be blocked (*this option is on by default and it is recommended not to change it unless you have a real reason to do so*)
- **Automatically quarantine detected threats** - all applications detected as malware will be blocked automatically
- **Automatically quarantine known threats** - only those applications that are with absolute certainty detected as malware will be blocked
- **Advanced settings...** - Click the link to get redirected to the respective dialog within the [Advanced settings](#) of **AVG Premium Security 2012**. There you can edit the component's configuration in detail. However, please note that the default configuration of all components is set up so that **AVG Premium Security 2012** provides optimum performance, and maximum security. Unless you have a real reason to do so, it is recommended to keep the default configuration!

### Control buttons

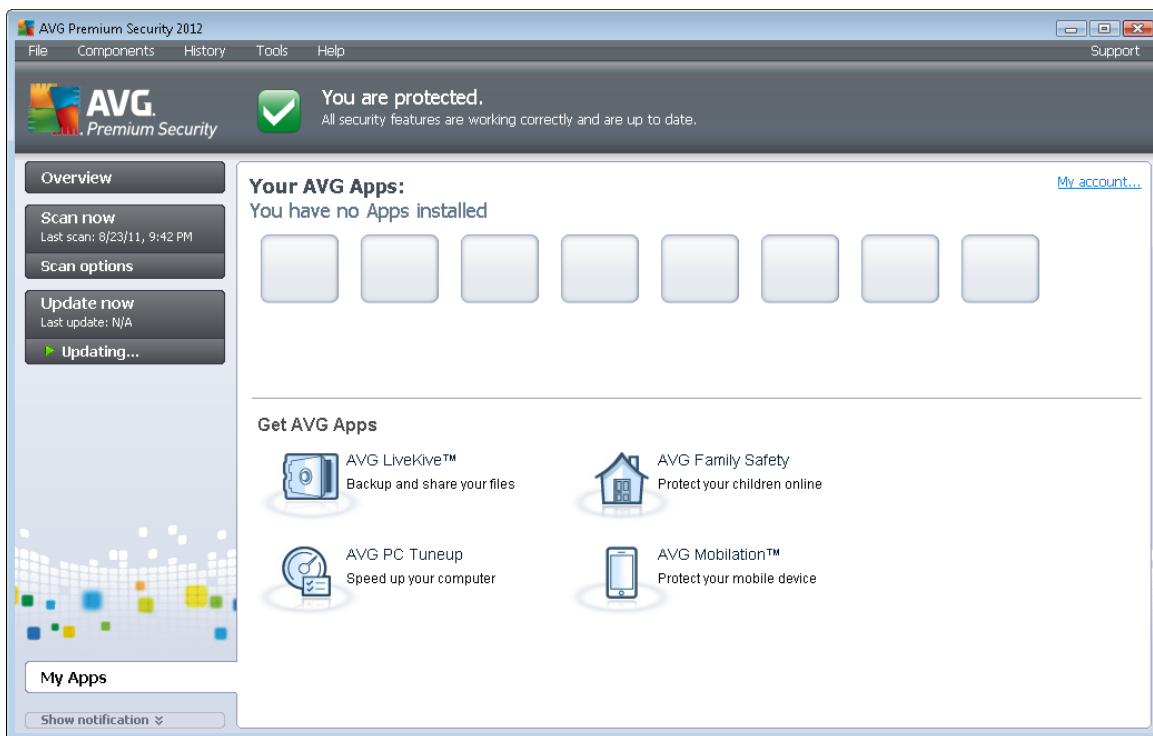
The control buttons available within the **Identity Protection** interface are as follows:

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



## 7. My Apps

Each of the following applications of [LiveKive](#), [Family Safety](#), and [PC Tuneup](#) is available as a standalone AVG product, and an optional part of your **AVG Premium Security 2012** installation. Within the **Your AVG Apps** dialog (accessible via the **My Apps** button directly from the AVG main dialog) you can see an overview of applications already installed, and ready to be installed optionally:



### 7.1. LiveKive

**LiveKive** is dedicated to online data backup on secured servers. **LiveKive** automatically backs up all your files, photos and music to one safe place, allowing you to share them with family and friends and access them from any web-enabled device, including iPhones and Android devices. **LiveKive** features include:

- Safety measure in case your computer and/or harddisk gets corrupted
- Access to your data from any device connected to the Internet
- Easy organizing
- Sharing with anyone you authorize

**For detailed information please visit the dedicated AVG webpage, where you can also download the component immediately. To do so, you may use the LiveKive link within the [My Apps](#) dialog.**



## 7.2. Family Safety

**Family Safety** helps you protect your children from inappropriate websites, media content and online searches, and provides you with reports regarding their online activity. You can set the appropriate level of protection for each of your children and monitor them separately via unique logins.

*For detailed information please visit the dedicated AVG webpage, where you can also download the component immediately. To do so, you may use the Family Safety link within the [My Apps](#) dialog.*

## 7.3. PC Tuneup

**PC Tuneup** application is an advanced tool for detailed system analysis and correction, as to how the speed and overall performance of your computer might be improved. **PC Tuneup** features include:

- Disk Cleaner - Removes junk files that slow down a computer.
- Disk Defrag - Defragments disk drives and optimizes system files placement.
- Registry Cleaner - Repairs registry errors to increase PC stability.
- Registry Defrag - Compacts the registry eliminating memory-consuming gaps.
- Disk Doctor - Finds bad sectors, lost clusters and directory errors and fixes them.
- Internet Optimizer - Tailors the one-size-fits-all settings to a specific Internet connection.
- Track Eraser - Removes the history of computer and Internet usage.
- Disk Wiper - Wipes free space on disks to prevent the recovery of sensitive data.
- File Shredder - Erases selected files beyond recovery on a disk or USB stick.
- File Recovery - Recovers accidentally deleted files from disks, USB sticks or cameras.
- Duplicate File Finder - Helps to find and remove duplicate files that waste disk space.
- Services Manager - Disables unnecessary services slowing down a computer.
- Startup Manager - Allows a user to manage programs that start automatically on Windows boot.
- Uninstall Manager - Completely uninstalls the software programs that you no longer need.
- Tweak Manager - Allows a user to tune hundreds of hidden Windows settings.
- Task Manager - Lists all running processes, services and locked files.
- Disk Explorer - Shows which files take up the most space on a computer.



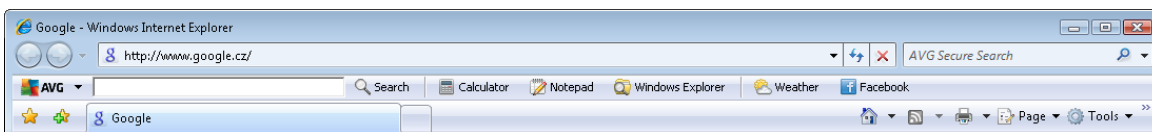
- System Information - Provides detailed information about installed hardware and software.

*For detailed information please visit the dedicated AVG webpage, where you can also download the component immediately. To do so, you may use the PC Tuneup link within the [My Apps](#) dialog.*



## 8. AVG Security Toolbar

**AVG Security Toolbar** is a tool that closely cooperates with the [LinkScanner](#) component, and guards your maximum security while browsing the Internet. Within **AVG Premium Security 2012**, the installation of **AVG Security Toolbar** is optional; during the [installation process](#) you were invited to decide whether the component should be installed. **AVG Security Toolbar** is available directly in your Internet browser. At the moment, the supported Internet browsers are Internet Explorer (*version 6.0 and higher*), and/or Mozilla Firefox (*version 3.0 and higher*). No other browsers are supported (*in case you are using some alternative Internet browser, e.g Avant Browser, you can meet unexpected behavior*).



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

- **AVG logo** with the drop-down menu:
  - **Use AVG Secure Search** - Allows you to search directly from the **AVG Security Toolbar** using the **AVG Secure Search** engine. All search results are continuously checked by the [Search-Shield](#) service, and you can feel absolutely safe online.
  - **Current Threat Level** - Opens the virus lab web page with a graphical display of the current threat level on the web.
  - **AVG Threat Labs** - Opens the specific **AVG Threat Lab** website (at <http://www.avgthreatlabs.com>) where you can find information on various websites security and current threat level online.
  - **Toolbar Help** - Opens the online help covering all **AVG Security Toolbar** functionality.
  - **Submit Product feedback** - Opens a web page with a form that you can fill in and tell us how you feel about **AVG Security Toolbar**.
  - **About...** - Opens a new window with the information on currently installed **AVG Security Toolbar** version.
- **Search field** - Search the Internet using the **AVG Security Toolbar** to be absolutely secure and comfortable since all displayed search results are hundred percent safe. Fill in the keyword or a phrase into the search field, and press the **Search** button (*or Enter*). All search results are continuously checked by the [Search-Shield](#) service (*within the [LinkScanner](#) component*).
- Shortcut buttons for quick access to these applications: **Calculator**, **Notepad**, **Windows Explorer**
- **Weather** - The button opens a new dialog providing information on the current weather in your location, and the weather forecast for the upcoming two days. This information is being



updated regularly, every 3-6 hours. In the dialog, you can change the desired location manually, and to decide whether you want to see the temperature info in Celsius or Fahrenheit.



- **Facebook** - This buttons allows you connect to the [Facebook](#) social network directly from within the **AVG Security Toolbar**.

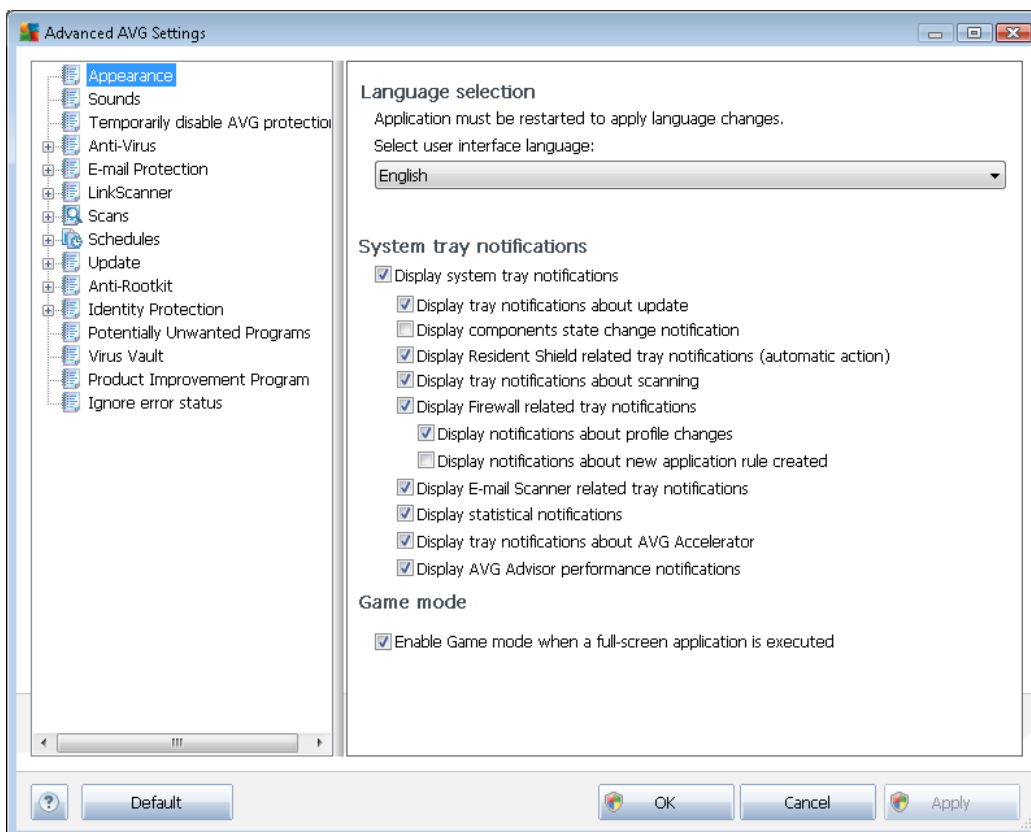


## 9. AVG Advanced Settings

The advanced configuration dialog of **AVG Premium Security 2012** 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.

### 9.1. Appearance

The first item of the navigation tree, **Appearance**, refers to the general settings of the **AVG Premium Security 2012** [user interface](#), and provides a few elementary options of the application's behavior:

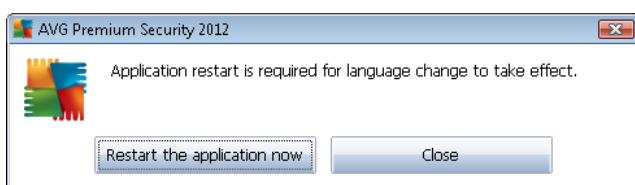


#### Language selection

In the **Language selection** section you can choose your desired language from the drop-down menu. The selected language will then be used for the entire **AVG Premium Security 2012** [user interface](#). The drop-down menu only offers those languages you have previously selected to be installed during the [installation process](#) (see [chapter Custom options](#)) plus English (*English is always installed automatically, by default*). To finish switching your **AVG Premium Security 2012** to another language you have to restart the application. Please follow these steps:



- In the drop-down menu, select the desired language of the application
- Confirm your selection by pressing the **Apply** button (*right-hand bottom corner of the dialog*)
- Press the **OK** button confirm
- A new dialog pops-up informing you that in order to change the language of the application, you need to restart your **AVG Premium Security 2012**
- Press the **Restart the application now** button to agree with the program restart, and wait a second for the language change to take effect:



### System tray notifications

Within this section you can suppress display of system tray notifications on the status of the **AVG Premium Security 2012** application. By default, the system notifications are allowed to be displayed. It is highly recommended to keep this configuration! System notifications inform for example on scanning or updating process launch, or on status change of a **AVG Premium Security 2012** component. You should certainly pay attention to these announcement!

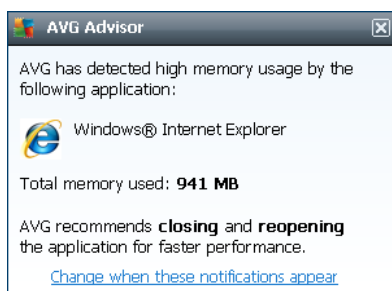
However, if for some reason you decide that you do not wish to be informed this way, or that you would like to see only certain notifications (*related to a specific AVG Premium Security 2012 component*) to be displayed, you can define and specify your preferences by checking/unchecking the following options:

- **Display system tray notifications** (*on, by default*) - By default, all notifications are displayed. Uncheck this item to completely turn off the display of all system notifications. When turned on, you can further select what specific notifications should be displayed:
  - **Display tray notifications about update** (*on, by default*) - Decide whether information regarding **AVG Premium Security 2012** update process launch, progress, and finalization should be displayed.
  - **Display components state change notifications** (*off, by default*) - 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](#) reporting a problem in any **AVG Premium Security 2012** component.
  - **Display Resident Shield related tray notifications (automatic action)** (*on, by default*) - Decide whether information regarding file saving, copying, and opening processes should be displayed or suppressed (*this configuration only demonstrates*



if the Resident Shield [Auto-heal](#) option is on).

- **Display tray notifications about scanning** (on, by default) - Decide whether information upon automatic launch of the scheduled scan, its progress and results should be displayed.
- **Display [Firewall](#) related tray notifications** (on, by default) - Decide whether information concerning [Firewall](#) status and processes, e.g. component's activation/deactivation warnings, possible traffic blocking etc. should be displayed. This item provides two more specific selection options (for detailed explanation of each of them please consult the [Firewall](#) chapter of this document):
  - **Display notifications about profile changes** (on, by default) - Notifies you about automatic changes of [Firewall](#) profiles.
  - **Display notifications about new application rule created** (off, by default) - Notifies you about automatic creation of [Firewall](#) rules for new applications based on a safe list.
- **Display [E-mail Scanner](#) related tray notifications** (on, by default) - Decide whether information upon scanning of all incoming and outgoing e-mail messages should be displayed.
- **Display statistical notifications** (on, by default) - Keep the option checked to allow regular statistical review notification to be displayed in the system tray.
- **Display tray notification about AVG Accelerator** (on, by default) - Decide whether information upon **AVG Accelerator** activities should be displayed. **AVG Accelerator** service that allows smoother online video playback and makes additional downloads easier.
- **Display AVG Advice performance notifications** (on, by default) - **AVG Advice** watches the supported Internet browsers (*Internet Explorer, Chrome, Firefox, Opera, and Safari*) performance, and will inform you in case your browser overuses the recommended amount of memory. In such a situation your computer performance may be slowed down significantly, and it is advised to restart your Internet browser to speed the processes up. Leave the **Display AVG Advice performance notifications** item on to be informed.



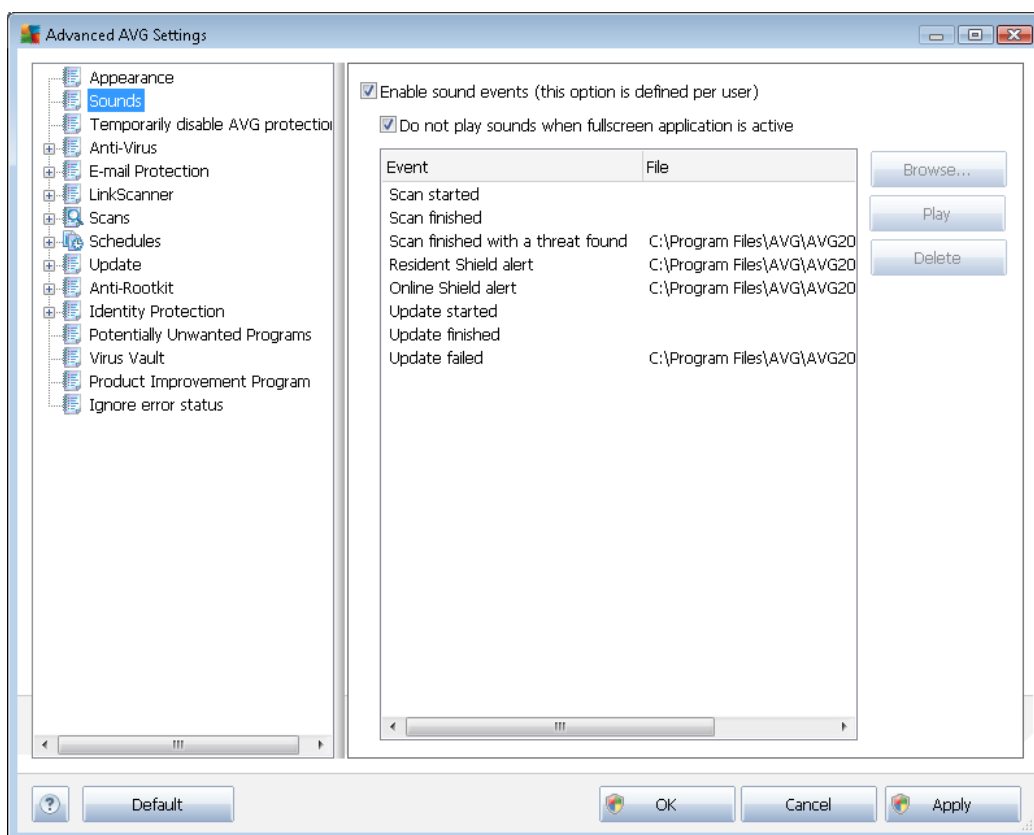
## Gaming mode



This AVG function is designed for full-screen applications where possible AVG information balloons ( displayed e.g. when a scheduled scan is started) would be disturbing (they could minimize the application 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).

## 9.2. Sounds

Within the **Sounds** dialog you can specify whether you want to be informed about specific **AVG Premium Security 2012** actions by a sound notification:



The settings are only valid for the current user account. That means, each user on the computer can have their own sound settings. If you want to allow the sound notification, keep the **Enable sound events** option checked (the option is on, by default) to activate the list of all relevant actions. Further, you may want to check the **Do not play sounds when fullscreen application is active** option to suppress the sound notification in situations when it might be disturbing (see also the [Gaming mode section of the Advanced settings/Appearance chapter in this document](#)).

### Control buttons

- **Browse** - Having selected the respective event from the list, use the **Browse** button to search your disk for the desired sound file you want to assign to it. (Please note that only \*.wav sounds are supported at the moment!)

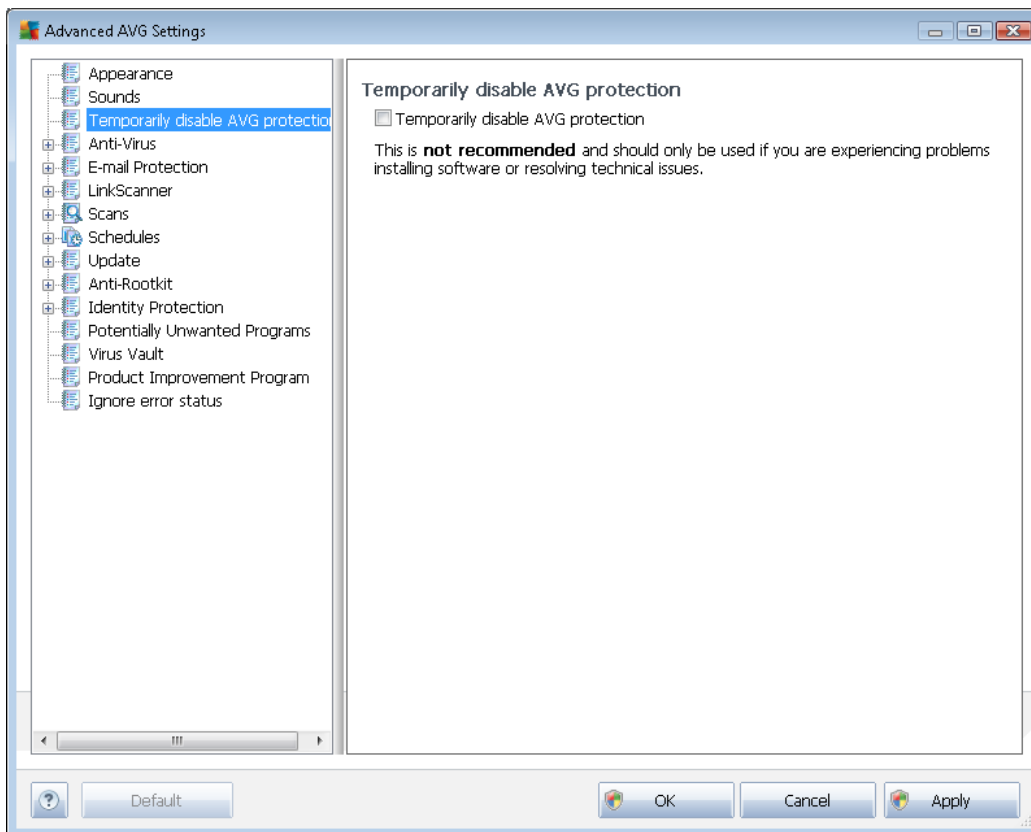


- **Play** - To listen to the selected sound, highlight the event in the list and push the **Play** button.
- **Delete** - Use the **Delete** button to remove the sound assigned to a specific event.

### 9.3. Temporarily disable AVG protection

In the **Temporarily disable AVG protection** dialog you have the option of switching off the entire protection secured by your **AVG Premium Security 2012** at once.

**Please remember that you should not use this option unless it is absolutely necessary!**



In most cases, it is **not necessary** to disable **AVG Premium Security 2012** before installing new software or drivers, not even if the installer or software wizard suggests that running programs and applications be shut down first to make sure there are no unwanted interruptions during the installation process. Should you really experience problem during installation, try to [deactivate the resident protection \(Enable Resident Shield\)](#) first. If you do have to temporarily disable **AVG Premium Security 2012**, you should re-enable it as soon as you're done. If you are connected to the Internet or a network during the time your antivirus software is disabled, your computer is vulnerable to attacks.

#### How to disable AVG protection



- Mark the **Temporarily disable AVG protection** check box, and confirm your choice by pressing the **Apply** button
- In the newly open **Temporarily disable AVG protection** dialog specify for how long you wish to disable your **AVG Premium Security 2012**. By default, the protection will be turned off for 10 minutes which should be sufficient for any common task such as installing new software etc. Note that the initial time limit that can possibly be set is 15 minutes, and cannot be overridden by your own value for security reasons. After the time period specified, all deactivated components will be automatically activated again.



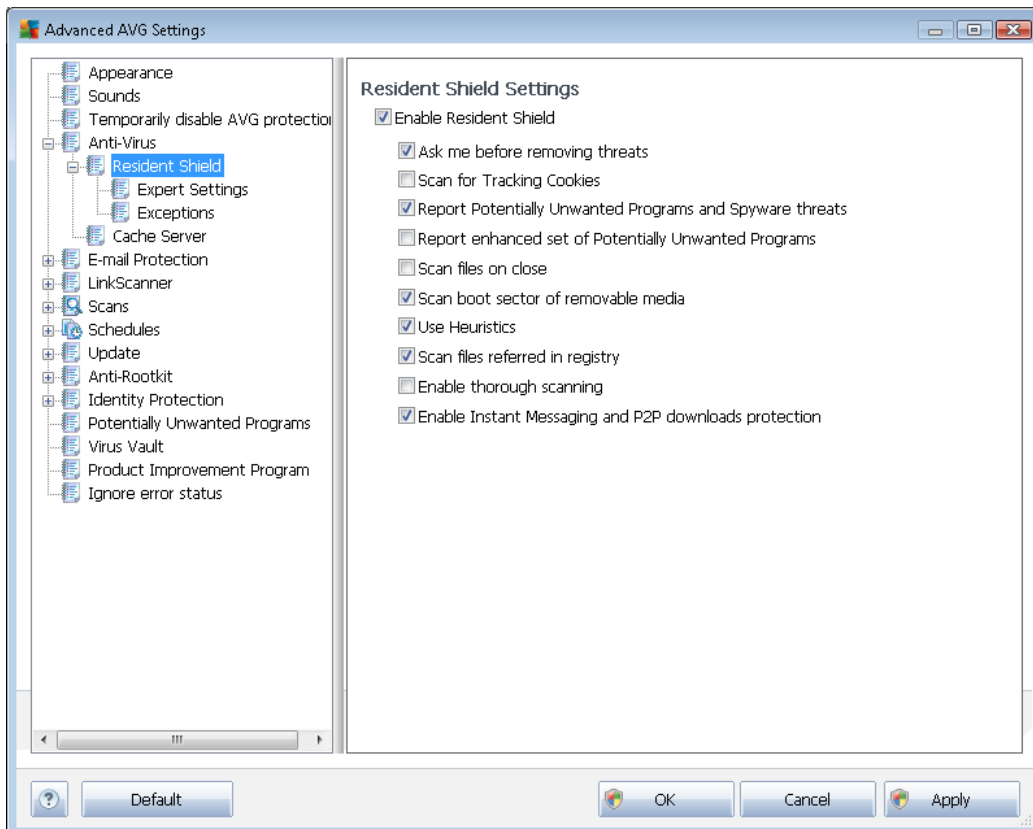
## 9.4. Anti-Virus

The **Anti-Virus** component protects your computer continuously from all known types of viruses and spyware (including so-called *sleeping and non-active malware, i.e. malware that has been downloaded but not yet activated*).



### 9.4.1. Resident Shield

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

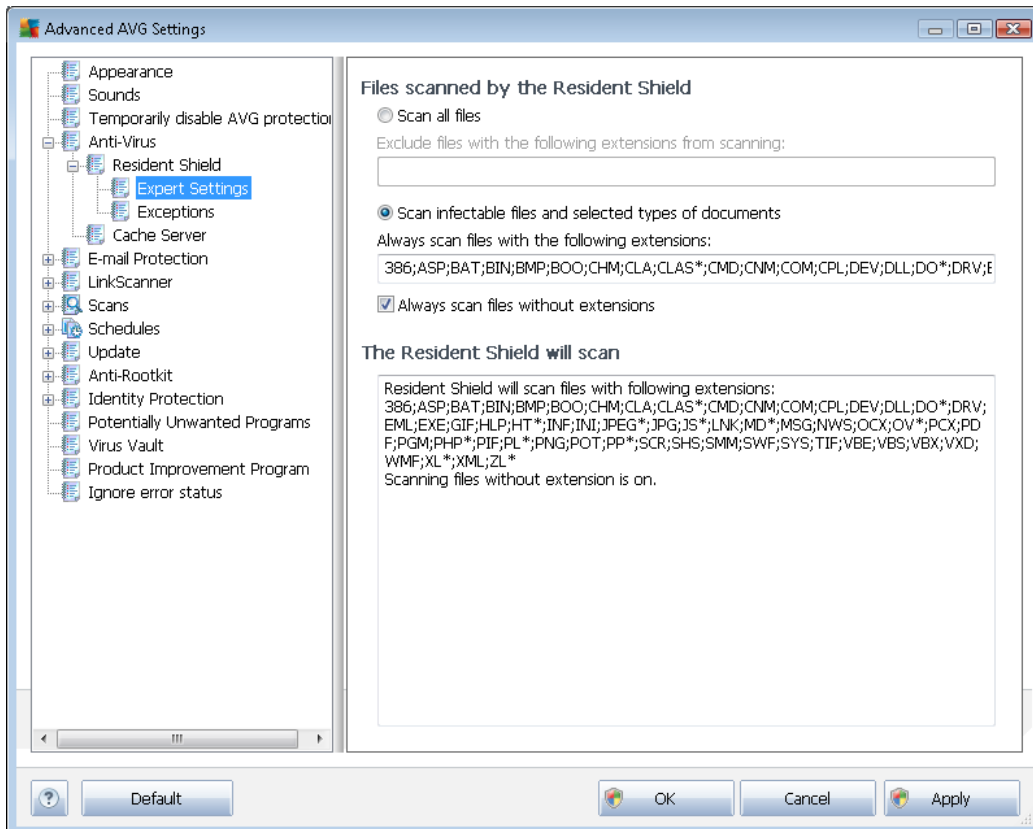
- **Ask me before removing threats** (*on by default*) - Check to ensure that the Resident Shield will not perform any action automatically; instead it will display a dialog describing the detected threat, allowing you to decide what should be done. If you leave the box unchecked, **AVG Premium Security 2012** will automatically heal the infection, and if not possible, the object will be moved into the [Virus Vault](#).
- **Scan for Tracking cookies** (*off by default*) - 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** (*on by default*) - Check to activate the [Anti-Spyware](#) engine, and scan for spyware as well as for viruses. [Spyware](#) represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend to keep this feature activated as it increases your computer security.



- **Report enhanced set of Potentially Unwanted Programs** (*off by default*) - Mark to detect extended package of [spyware](#): programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it can possibly block legal programs, and is therefore switched off by default.
- **Scan files on close** (*off by default*) - 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** (*on by default*)
- **Use Heuristics** (*on by default*) - [Heuristic analysis](#) will be used for detection (*dynamic emulation of the scanned object's instructions in a virtual computer environment*).
- **Scan files referred in registry** (*on by default*) - This parameter defines that AVG will scan all executable files added to startup registry to avoid a known infection being executed upon next computer startup.
- **Enable thorough scanning** (*off by default*) - In specific situations (*in a state of extreme emergency*) you may check this option to activate the most thorough algorithms that will check all possibly threatening objects into the deep. Remember though that this method is rather time consuming.
- **Enable Instant Messaging protection and P2P download protection** (*on by default*) - Check this item if you wish to verify that the instant messaging communication (e.g. *ICQ, MSN Messenger, ...*) and P2P downloads are virus free.



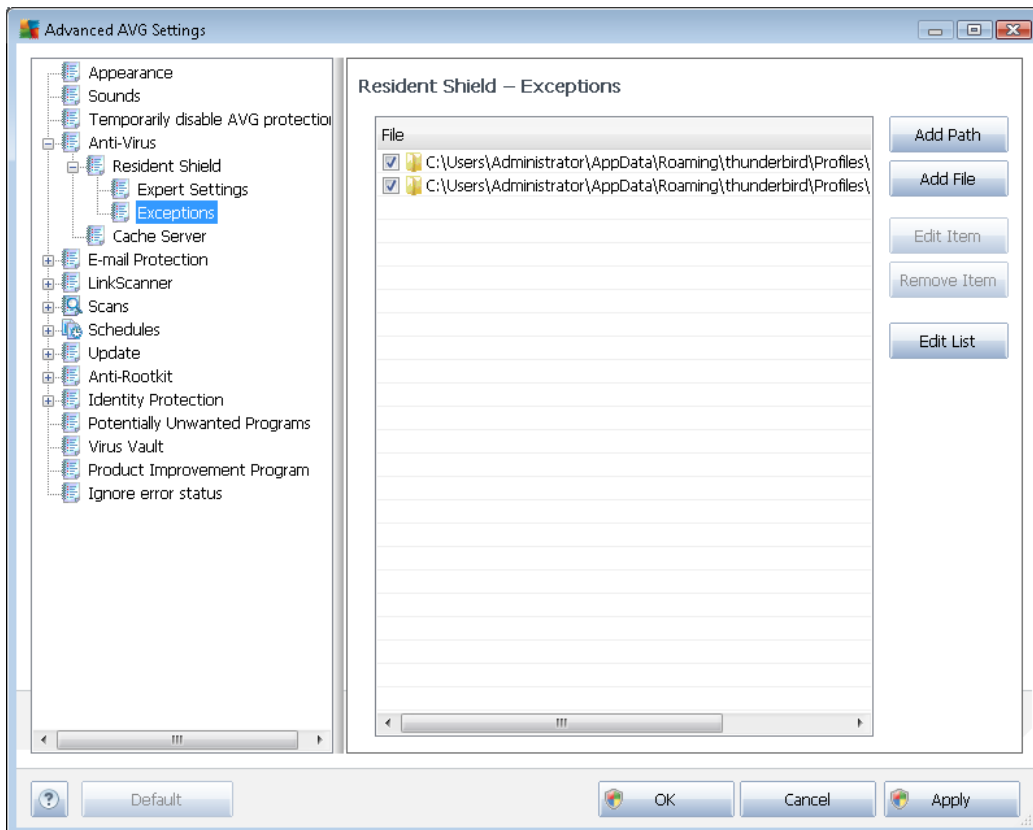
In the **Files scanned by the Resident Shield** dialog it is possible to configure which files will be scanned (*by specific extensions*):



Mark the respective check box to decide whether you want to **Scan all files** or **Scan infectable files and selected types of documents** only. If you have decided for the latter option, 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.

Check the **Always scan files without extensions** (*on by default*) to ensure that even files with no extension and unknown format should be scanned by the Resident Shield. We recommend to keep this feature switched on, as files without extensions are suspicious.

The below section called **The Resident Shield will scan** further summarizes the current settings, displaying a detailed overview of what the **Resident Shield** will actually scan.



The **Resident Shield - Exceptions** dialog offers the possibility of defining files and/or folders that should be excluded from the **Resident Shield** scanning.

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

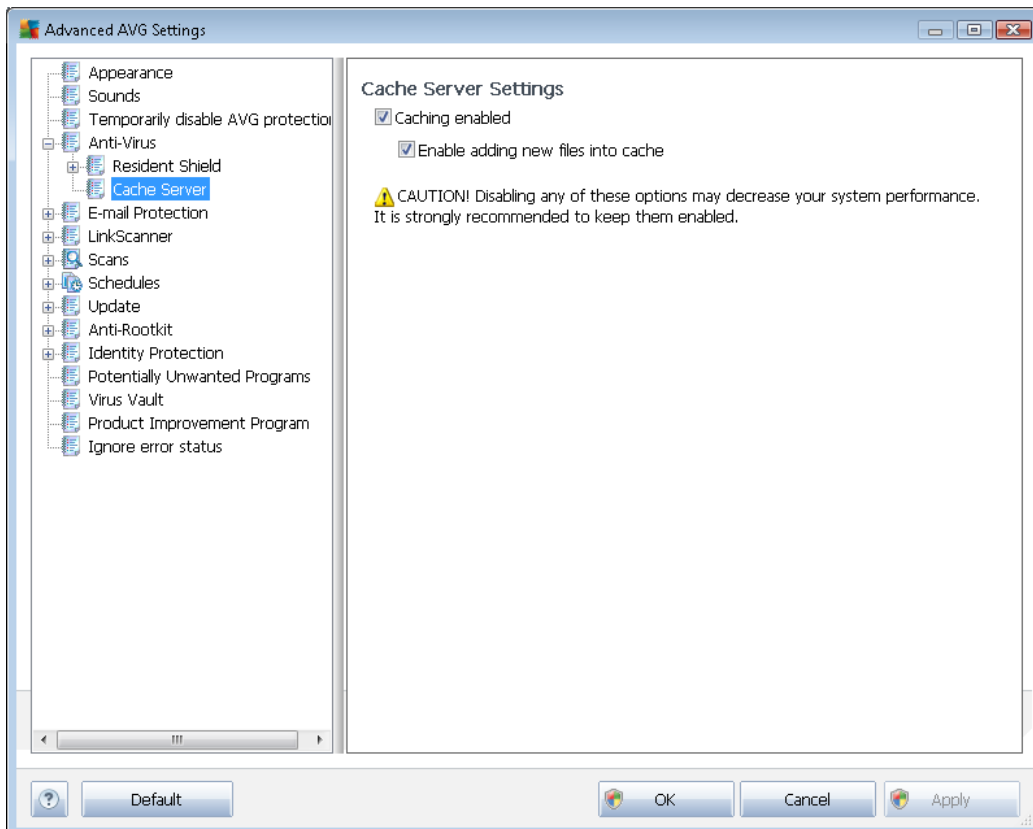
### Control buttons

The dialog provides the following control buttons:

- **Add Path** – specify a directory (directories) to be excluded from the scanning by selecting them one by one from the local disk navigation tree
- **Add File** – specify files to be excluded from the scanning by selecting them one by one from the local disk navigation tree
- **Edit Item** – allows you to edit the specified path to a selected file or folder
- **Remove Item** – allows you to delete the path to a selected item from the list
- **Edit List** - allows you to edit the entire list of defined exceptions in a new dialog that behaves like a standard text editor

### 9.4.2. Cache Server

The **Cache Server Settings** dialog refers to the cache server process designed to speed up all types of **AVG Premium Security 2012** scans:



It cache server gathers and keeps information of trustworthy files (*a files is considered trustworthy if signed with digital signature of a trustworthy source*). These files are then automatically taken for safe, and do not need to be re-scanned; therefore these files are skipped during scanning.

The **Cache Server Settings** dialog offers the following options of configuration:

- **Caching enabled** (*on by default*) - uncheck the box to switch off the **Cache Server**, and empty the cache memory. Please note that scanning might slow down, and overall performance of your computer decrease, as every single file in use will be scanned for viruses and spyware first.
- **Enable adding new files into cache** (*on by default*) - uncheck the box to stop adding more files into the cache memory. Any already cached files will be kept and used until caching is turned off completely, or until the next update of the virus database.

***Unless you have a good reason to switch the cache server off, we strongly recommend that you keep the default settings and let both the option on! Otherwise you may experience a significant decrease of your system speed and performance.***

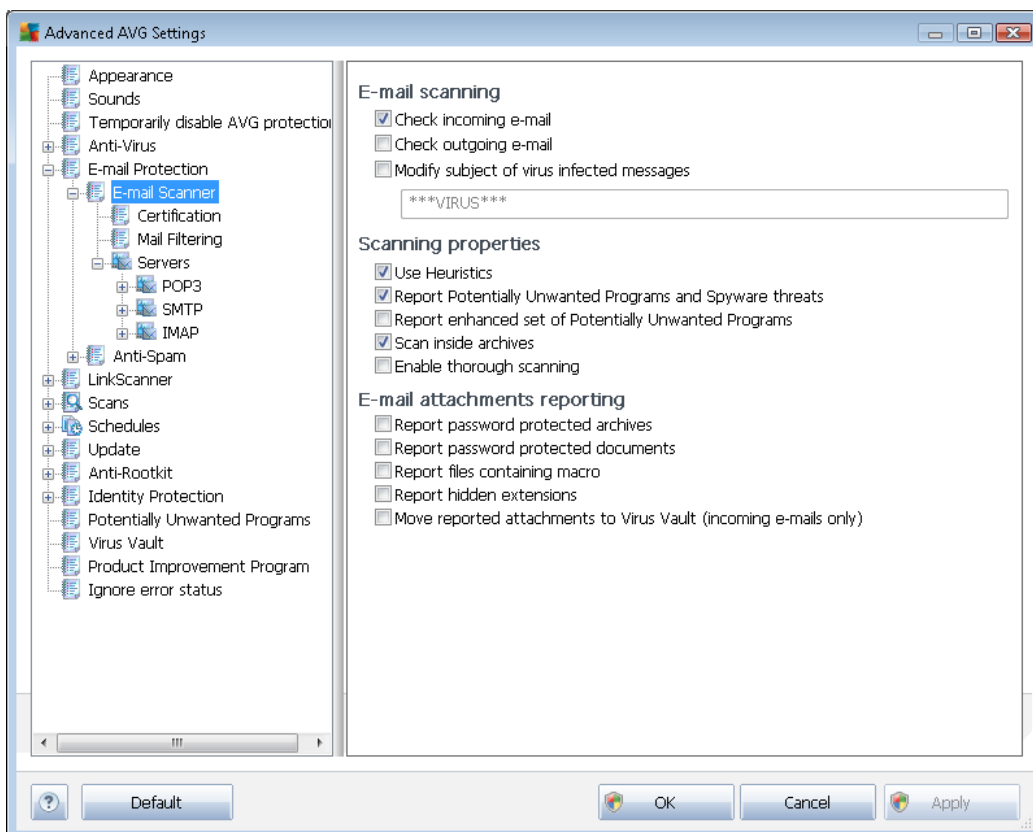


## 9.5. E-mail protection

In the **E-mail protection** section you can edit detailed configuration of [E-mail Scanner](#) and [Anti-Spam](#):

### 9.5.1. E-mail Scanner

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



### E-mail scanning

In this section, you can set these basics for incoming and/or outgoing e-mail messages:

- **Check incoming e-mail** (*on by default*) - mark to switch on/off the option of scanning of all e-mail messages delivered to your e-mail client
- **Check outgoing e-mail** (*off by default*) - mark to switch on/off the option of scanning of all e-mails sent from your account
- **Modify subject of virus infected messages** (*off by default*) - if you want to be warned the scanned e-mail message was detected as infectious, mark this item and fill in the desired text into the text field. This text will then be added to the "Subject" field for each detected e-mail message for easier identification and filtering. The default value is **\*\*\*VIRUS\*\*\*** which we recommend to keep.



## Scanning properties

In this section, you can specify how the e-mail messages will be scanned:

- **Use Heuristics** (*on by default*) - check to use heuristics detection method when scanning e-mail messages. When this option is on, you can filter e-mail attachments not only by extension but also the actual contents of the attachment will be considered. The filtering can be set in the [Mail Filtering](#) dialog.
- **Report Potentially Unwanted Programs and Spyware threats** (*on by default*) - check to activate the [Anti-Spyware](#) engine, and scan for spyware as well as for viruses. [Spyware](#) represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend to keep this feature activated as it increases your computer security.
- **Report enhanced set of Potentially Unwanted Programs** (*off by default*) - mark to detect extended package of [spyware](#): programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it can possibly block legal programs, and is therefore switched off by default.
- **Scan inside archives** (*on by default*) - check to scan contents of archives attached to e-mail messages.
- **Enable thorough scanning** (*off by default*) - in specific situations (*e.g. suspicious of your computer being infected by an virus or exploit*) you may check this option to activate the most thorough scanning algorithms that will scan even those areas of your computer that can hardly get infected, just to be absolutely sure. Remember though that this method is rather time consuming.

## E-mail attachments reporting

In this section, you can set additional reports about potentially dangerous or suspicious files. Please note that no warning dialog will be displayed, only a certification text will be added to the end of the e-mail message, and all such reports will be listed in the [E-mail Scanner detection](#) dialog:

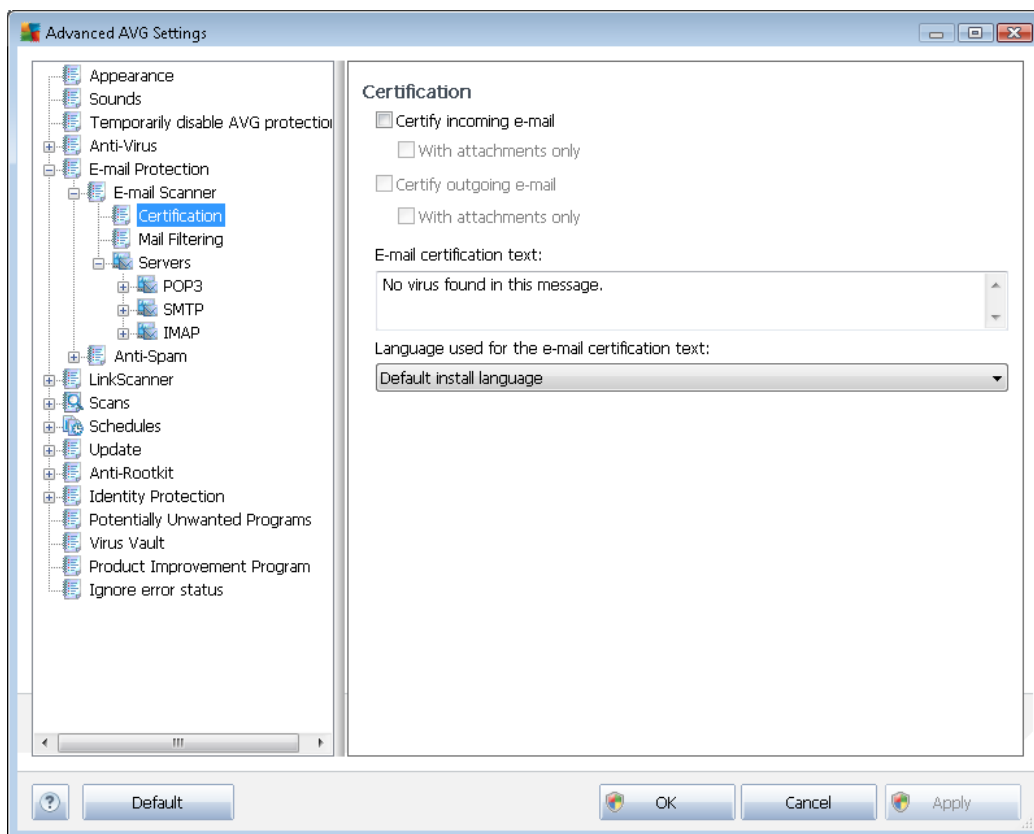
- **Report password protected archives** – archives (*ZIP, RAR etc.*) that are protected by password are not possible to scan for viruses; check the box to report these as potentially dangerous.
- **Report password protected documents** – documents protected by password are not possible to scan for viruses; check the box to report these as potentially dangerous.
- **Report files containing macro** – a macro is a predefined sequence of steps aimed to make certain tasks easier for a user (*MS Word macros are widely known*). As such, a macro can contain potentially dangerous instructions, and you might like to check the box to ensure that files with macros will be reported as suspicious.
- **Report hidden extensions** – hidden extension can make e.g. a suspicious executable file



"something.txt.exe" appear as harmless plain text file "something.txt"; check the box to report these as potentially dangerous.

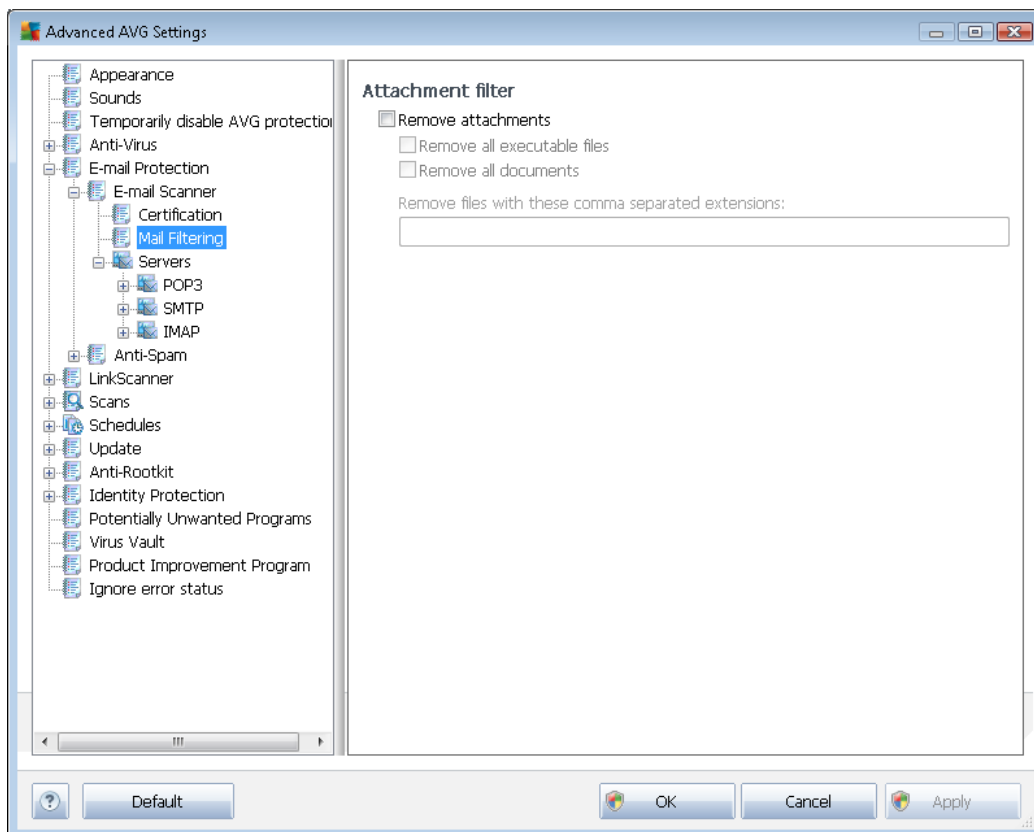
- **Move reported attachments to Virus Vault** - specify whether you wish to be notified via e-mail about password protected archives, password protected documents, macro containing files and/or files with hidden extension detected as an attachment of the scanned e-mail message. If such a message is identified during scanning, define whether the detected infectious object should be moved to the [Virus Vault](#).

In the **Certification** dialog you can mark the specific check boxes to decide whether you want to certify your incoming mail (**Certify incoming e-mail**) and/or outgoing mail (**Certify outgoing e-mail**). For each of these options you can further specify the **With attachments only** parameter so that the certification is only added to a-mail messages with attachments:



By default, the certification text consists of just a basic information that states *No virus found in this message*. However, this information can be extended or changed according to your needs: write the desired text of certification into the **E-mail certification text** field. In the **Language used for the e-mail certification text** section you can further define in which language the automatically generated part of certification (*No virus found in this message*) should be displayed.

**Note:** Please mind that only the default text will be displayed in the requested language, and your customized text will not be translated automatically!



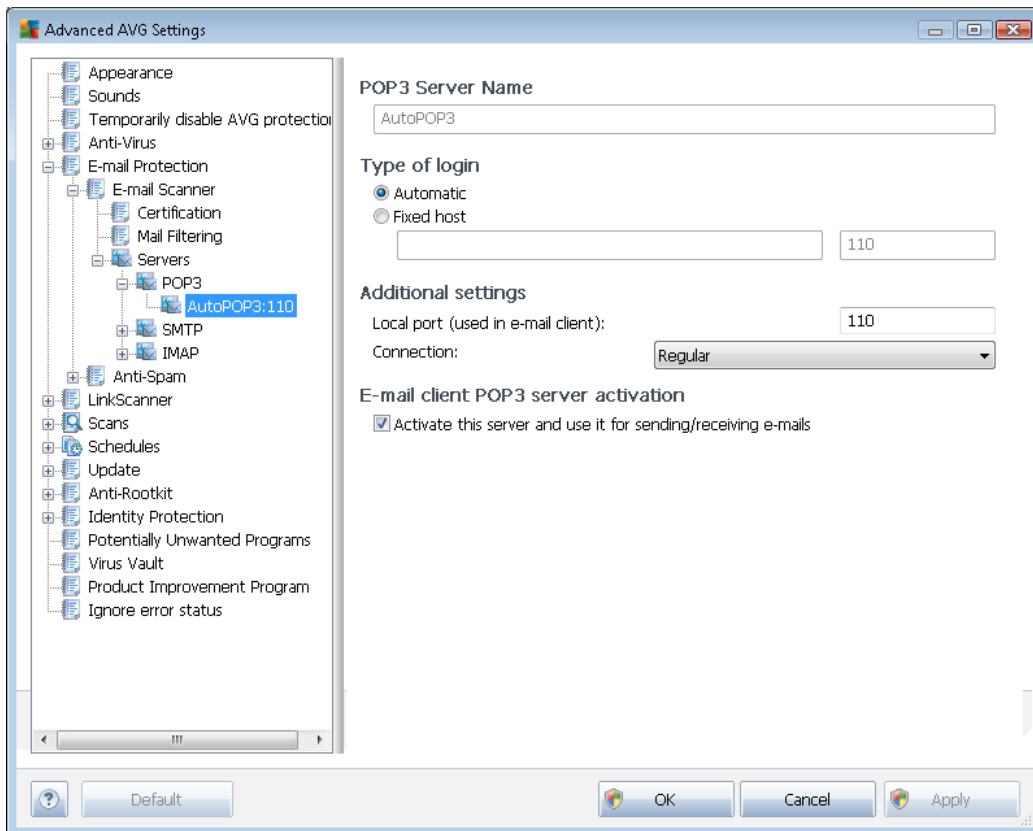
The **Attachment filter** dialog allows you to set up parameters for e-mail messages attachment scanning. By default, the **Remove attachments** option is switched off. If you decide to activate it, all e-mail message attachments detected as infectious or potentially dangerous will be removed automatically.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

- **Remove all executable files** - all \*.exe files will be deleted
- **Remove all documents** - all \*.doc, \*.docx, \*.xls, \*.xlsx files will be deleted
- **Remove files with these comma separated extensions** - will remove all files with the defined extensions

In the **Servers** section you can edit parameters of the [E-mail Scanner](#) servers:

- [POP3 server](#)
- [SMTP server](#)
- [IMAP server](#)

Also, you can define new server for incoming or outgoing mail, using the **Add new server** button.

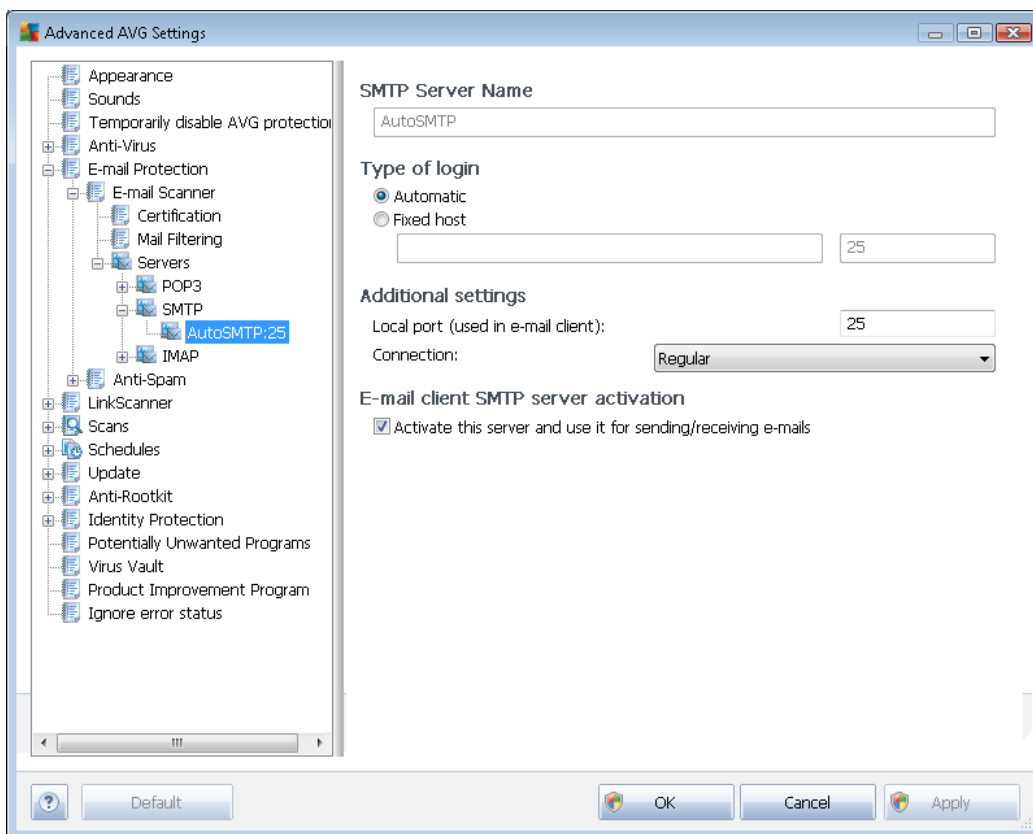


In this dialog (opened via **Servers / POP3**) you can set up a new [E-mail Scanner](#) server using the POP3 protocol for incoming mail:

- **POP3 Server Name** - in this field you can specify the name of newly added servers (to add a POP3 server, click the right mouse button over the POP3 item of the left navigation menu). For automatically created "AutoPOP3" server this field is deactivated.
- **Type of login** - defines the method for determining the mail server used for incoming mail:
  - **Automatic** - Login will be carried out automatically, according to your e-mail client settings.
  - **Fixed host** - In this case, the program will always use the server specified here. Please specify the address or name of your mail server. The login name remains unchanged. For a name, you may use a domain name (for example, *pop.acme.com*) as well as an IP address (for example, *123.45.67.89*). If the mail server uses a non-standard port, you can specify this port after the server name by using a colon as the delimiter (for example, *pop.acme.com:8200*). The standard port for POP3 communication is 110.
- **Additional settings** - specifies more detailed parameters:



- **Local port** - specifies the port on which the communication from your mail application should be expected. You must then specify in your mail application this port as the port for POP3 communication.
- **Connection** - in the drop-down menu, you can specify which kind of connection to use (*regular/SSL/SSL default*). If you choose SSL connection, the data sent is encrypted without the risk of being traced or monitored by a third party. This feature is also only available when the destination mail server supports it.
- **E-mail client POP3 server activation** - check/uncheck this item to activate or deactivate the specified POP3 server

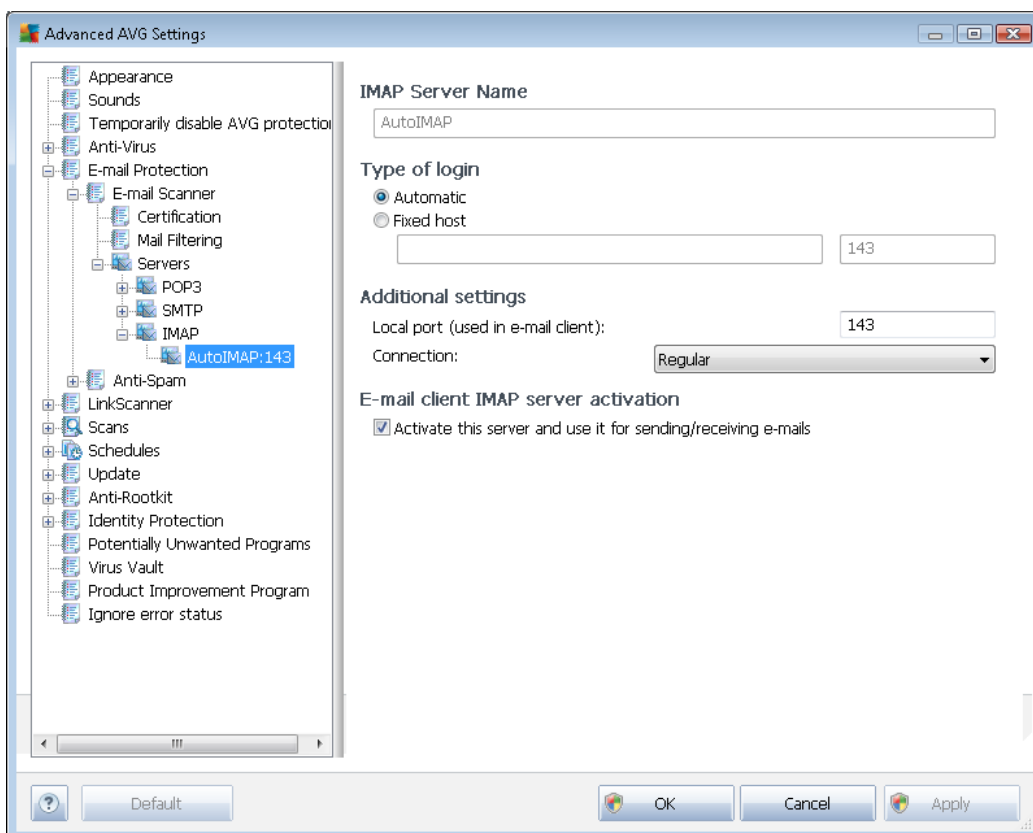


In this dialog (*opened via **Servers / SMTP***) you can set up a new [E-mail Scanner](#) server using the SMTP protocol for outgoing mail:

- **SMTP Server Name** - in this field you can specify the name of newly added servers (*to add a SMTP server, click the right mouse button over the SMTP item of the left navigation menu*). For automatically created "AutoSMTP" server this field is deactivated.
- **Type of login** - defines the method for determining the mail server used for outgoing mail:
  - **Automatic** - login will be carried out automatically, according to your e-mail client settings



- **Fixed host** - in this case, the program will always use the server specified here. Please specify the address or name of your mail server. You may use a domain name (for example, *smtp.acme.com*) as well as an IP address (for example, *123.45.67.89*) for a name. If the mail server uses a non-standard port, you can type this port behind the server name using a colon as the delimiter (for example, *smtp.acme.com:8200*). The standard port for SMTP communication is 25.
- **Additional settings** - specifies more detailed parameters:
  - **Local port** - specifies the port on which the communication from your mail application should be expected. You must then specify in your mail application this port as the port for SMTP communication.
  - **Connection** - in this drop-down menu, you can specify which kind of connection to use (*regular/SSL/SSL default*). If you choose SSL connection, the data sent is encrypted without the risk of being traced or monitored by a third party. This feature is available only when the destination mail server supports it.
- **E-mail client SMTP server activation** - check/uncheck this box to activate/deactivate the above specified SMTP server

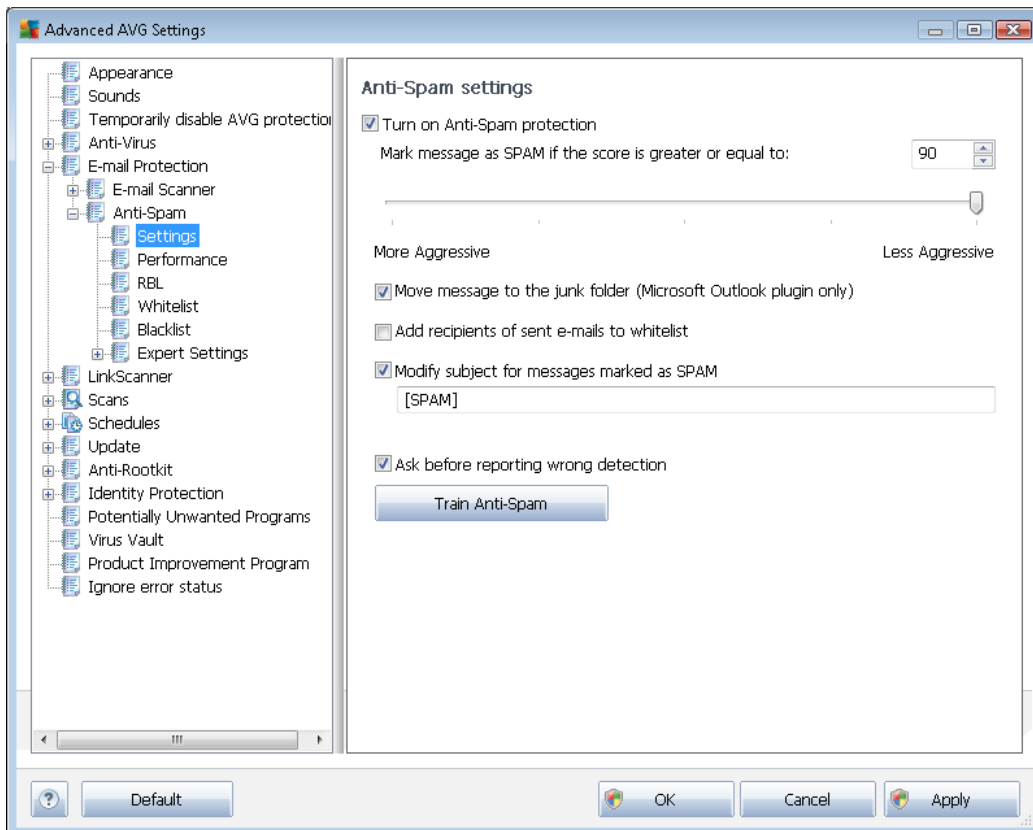


In this dialog (opened via **Servers / IMAP**) you can set up a new [E-mail Scanner](#) server using the IMAP protocol for outgoing mail:



- **IMAP Server Name** - in this field you can specify the name of newly added servers (*to add a IMAP server, click the right mouse button over the IMAP item of the left navigation menu* ). For automatically created "AutoIMAP" server this field is deactivated.
- **Type of login** - defines the method for determining the mail server used for outgoing mail:
  - **Automatic** - login will be carried out automatically, according to your e-mail client settings
  - **Fixed host** - in this case, the program will always use the server specified here. Please specify the address or name of your mail server. You may use a domain name (*for example, smtp.acme.com*) as well as an IP address (*for example, 123.45.67.89*) for a name. If the mail server uses a non-standard port, you can type this port behind the server name using a colon as the delimiter (*for example, imap.acme.com:8200*). The standard port for IMAP communication is 143.
- **Additional settings** - specifies more detailed parameters:
  - **Local port** - specifies the port on which the communication from your mail application should be expected. You must then specify in your mail application this port as the port for IMAP communication.
  - **Connection** - in this drop-down menu, you can specify which kind of connection to use (*regular/SSL/SSL default*). If you choose SSL connection, the data sent is encrypted without the risk of being traced or monitored by a third party. This feature is available only when the destination mail server supports it.
- **E-mail client IMAP server activation** - check/uncheck this box to activate/deactivate the above specified IMAP server

### 9.5.2. Anti-Spam



In the **Anti-Spam settings** dialog you can check/uncheck the **Turn on Anti-Spam protection** checkbox to allow/forbid the anti-spam scanning of e-mail communication. This option is on by default, and as always, it is recommended to keep this configuration unless you have a real reason to change it.

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

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

- **Value 80-90** - E-mail messages likely to be spam will be filtered out. Some non-spam messages may be incorrectly filtered as well.
- **Value 60-79** - Considered as a quite aggressive configuration. E-mail messages that are possibly spam will be filtered out. Non-spam messages are likely to be caught as well.
- **Value 50-59** - Very aggressive configuration. Non-spam e-mail messages are as likely to be caught as real spam messages. This threshold range is not recommended for normal use.

In the **Anti-Spam settings** dialog you can further define how the detected spam e-mail messages



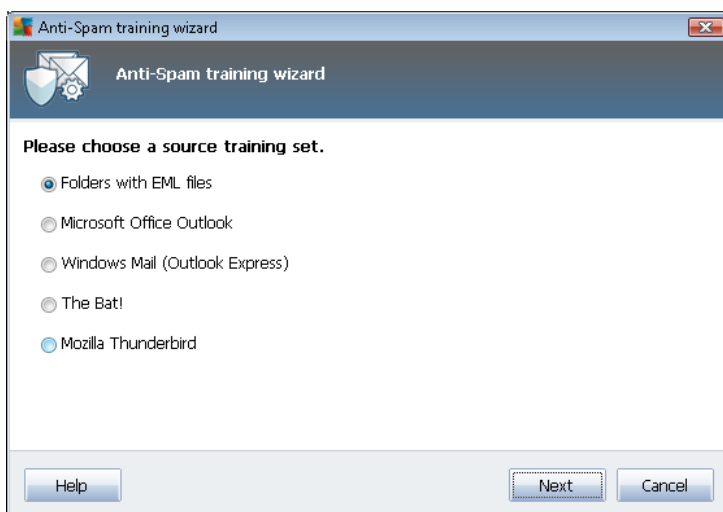
should be treated:

- **Move message to the junk folder** (*Microsoft Outlook plugin only*) - Mark this check box to specify that each detected spam message should be automatically moved to the specific junk folder within your MS Outlook.e-mail client. At the moment, the feature is not supported in other mail clients.
- **Add recipients of sent e-mails to [whitelist](#)** - Tick this check box to confirm that all recipients of sent e-mails can be trusted, and all e-mail messages coming from their e-mail accounts can be delivered.
- **Modify subject for messages marked as SPAM** - Tick this check box if you would like all messages detected as spam to be marked with a specific word or character in the e-mail subject field; the desired text can be typed in the activated text field.
- **Ask before reporting wrong detection** - Provided that during the [installation process](#) you agreed to participate in the [Product Improvement Program](#). If so, you allowed reporting of detected threats to AVG. The reporting is taken care of automatically. However, you may mark this check box to confirm you want to be asked before any detected spam gets reported to AVG to make sure the message should really be classified as spam.

## Control buttons

**Train Anti-Spam** button open the [Anti-Spam training wizard](#) described in details in the [next chapter](#).

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



There are the following options to choose from:

- **A specific e-mail client** - if you use one of the listed e-mail clients (*MS Outlook, Outlook*



*Express, The Bat!*), simply select the respective option

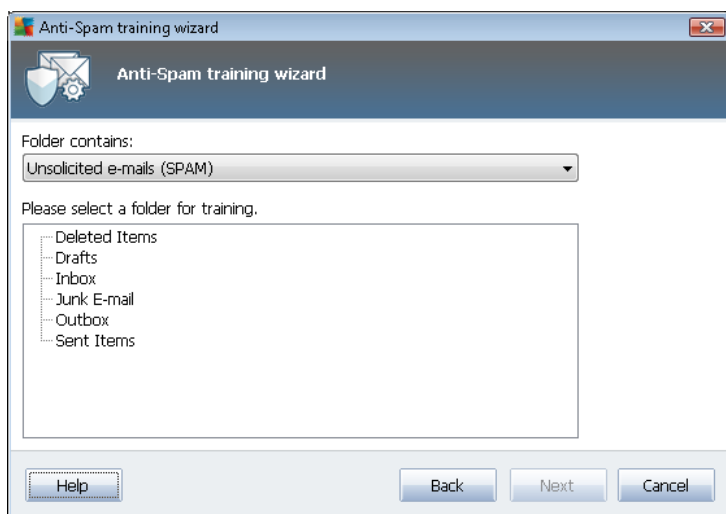
- **Folder with EML files** - if you use any other e-mail program, you should first save the messages to a specific folder (*in .eml format*), or make sure that you know the location of your e-mail client message folders. Then select **Folder with EML files**, which will enable you to locate the desired folder in the next step

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

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

Dialog displayed in this step depends on your previous selection.

### Folders with EML files



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

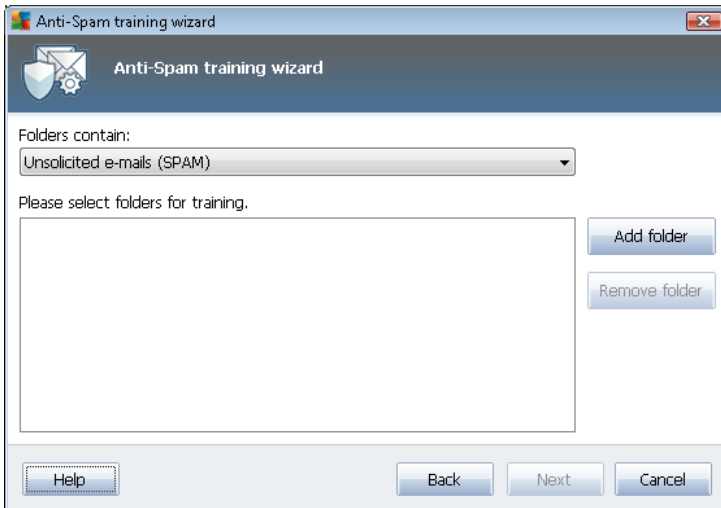
In the **Folders contain** drop-down menu, set one of the two options - whether the selected folder contains wanted (*HAM*), or unsolicited (*SPAM*) messages. Please note that you will be able to filter the messages in the next step, so the folder does not have to contain only training e-mails. You can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

When done, click **Next** and proceed to [Message filtering options](#).

### Specific e-mail client



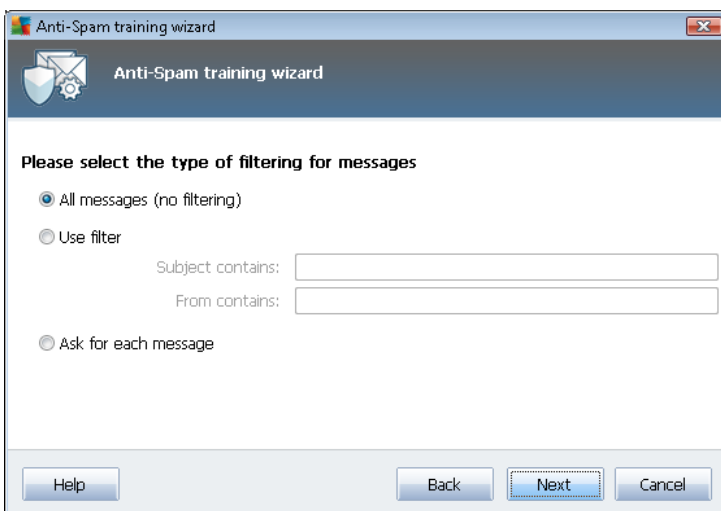
Once you confirm one of the options, new dialog will appear.



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

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

When done, click **Next** and proceed to [Message filtering options](#).



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

- **All messages (no filtering)** - If you are sure that the selected folder contains only

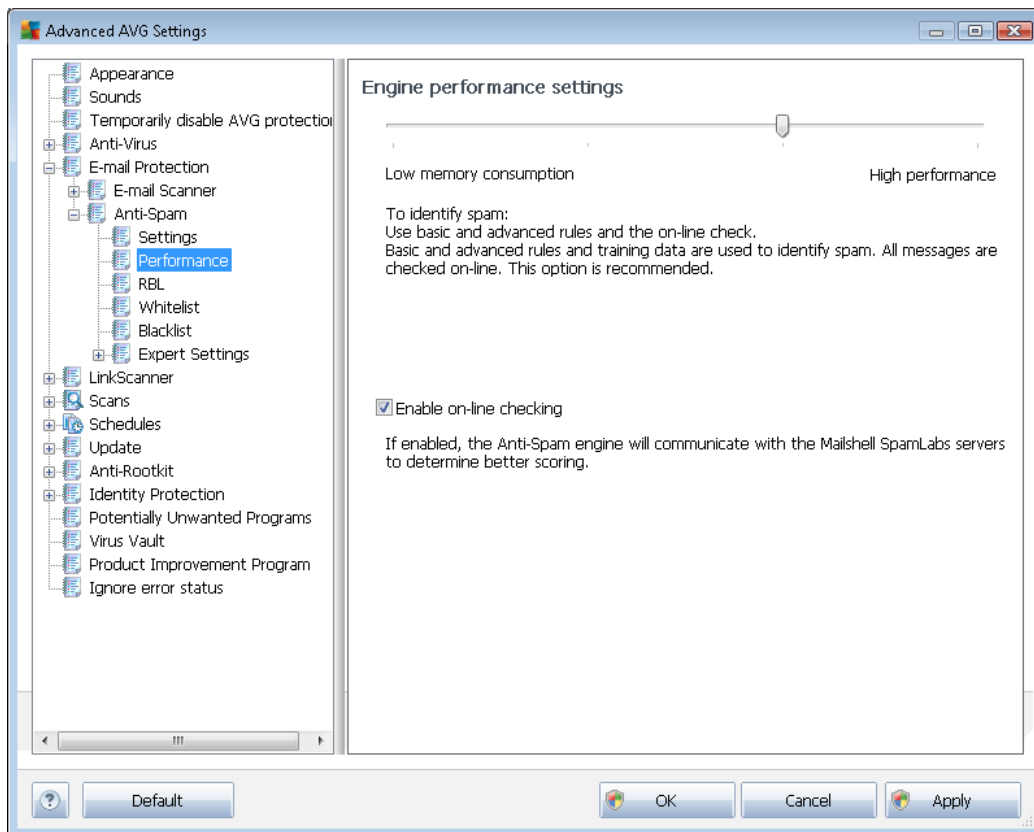


messages you want to use for training, select the **All messages (no filtering)** option.

- **Use filter** - For more advanced filtering, select the **Use filter** option. You can fill in a word ( *name*), part of a word, or phrase to be searched for in the e-mail subject and/or the sender's field. All messages matching exactly the entered criteria will be used for the training, without further prompting. When you fill in both text fields, addresses that match just one of the two conditions will be used, too!
- **Ask for each message** - If you are unsure about the messages contained in the folder, and you want the wizard to ask you about every single message (*so that you can determine whether to use it for training or not*), select the **Ask for each message** option.

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

The **Engine performance settings** dialog (*linked to via the Performance item of the left navigation*) offers the **Anti-Spam** component performance settings:



Move the slider left or right to change the level of scanning performance ranging between **Low memory / High performance** modes.

- **Low memory** - during the scanning process to identify spam, no rules will be used. Only



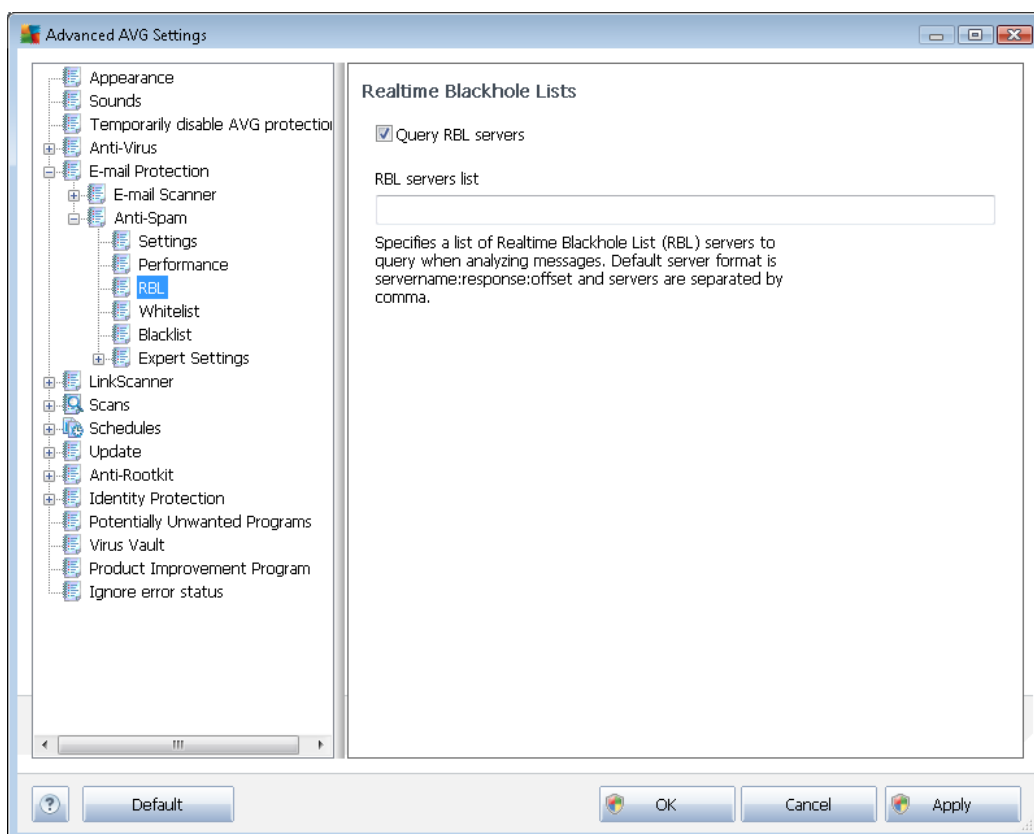
training data will be used for identification. This mode is not recommended for common use, unless the computer hardware is really poor.

- **High performance** - this mode will consume large amount of memory. During the scanning process to identify spam, the following features will be used: rules and spam database cache, basic and advanced rules, spammer IP addresses and spammer databases.

The **Enable on-line checking** item is on by default. It results in more precise spam detection via communication with the [Mailshell](#) servers, i.e. the scanned data will be compared with [Mailshell](#) databases online.

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

The **RBL** item open an editing dialog called **Realtime Blackhole Lists** when you can switch on/off the **Query RBL servers** function:



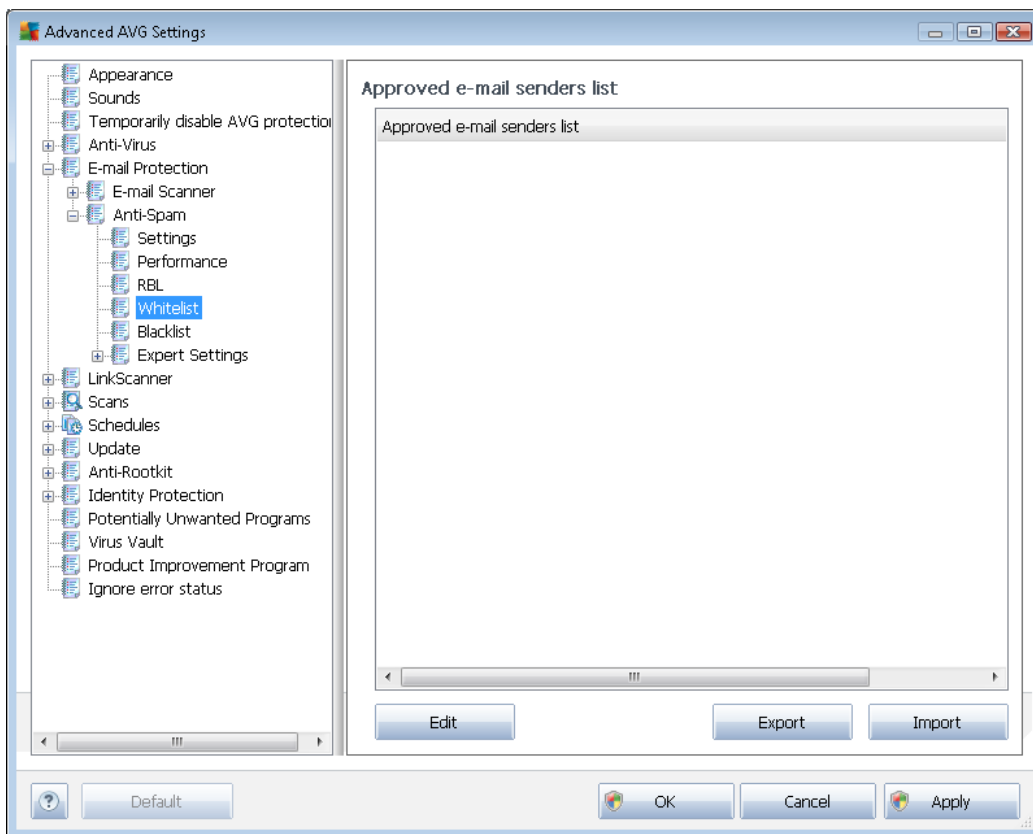
The RBL (*Realtime Blackhole List*) server is a DNS server with an extensive database of known spam senders. When this feature is switched on, all e-mail messages will be verified against the RBL server database and marked as spam if identical to any of the database entries. The RBL servers databases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



The **RBL servers list** allows you to define specific RBL server locations (*please note, that enabling this feature may, on some systems and configurations, slow down the e-mail receiving process, as every single message must be verified against the RBL server database*).

**No personal data is sent to the server!**

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



In the editing interface you can compile a list of senders that you are sure will never send you unwanted messages (spam). You can also compile a list of full domain names (e.g. *avg.com*), that you know do not generate spam messages. Once you have such a list of senders and/or domain names prepared, you can enter them by either of the following methods: by direct entry of each e-mail address or by importing the whole list of addresses at once.

### Control buttons

The following control buttons are available:

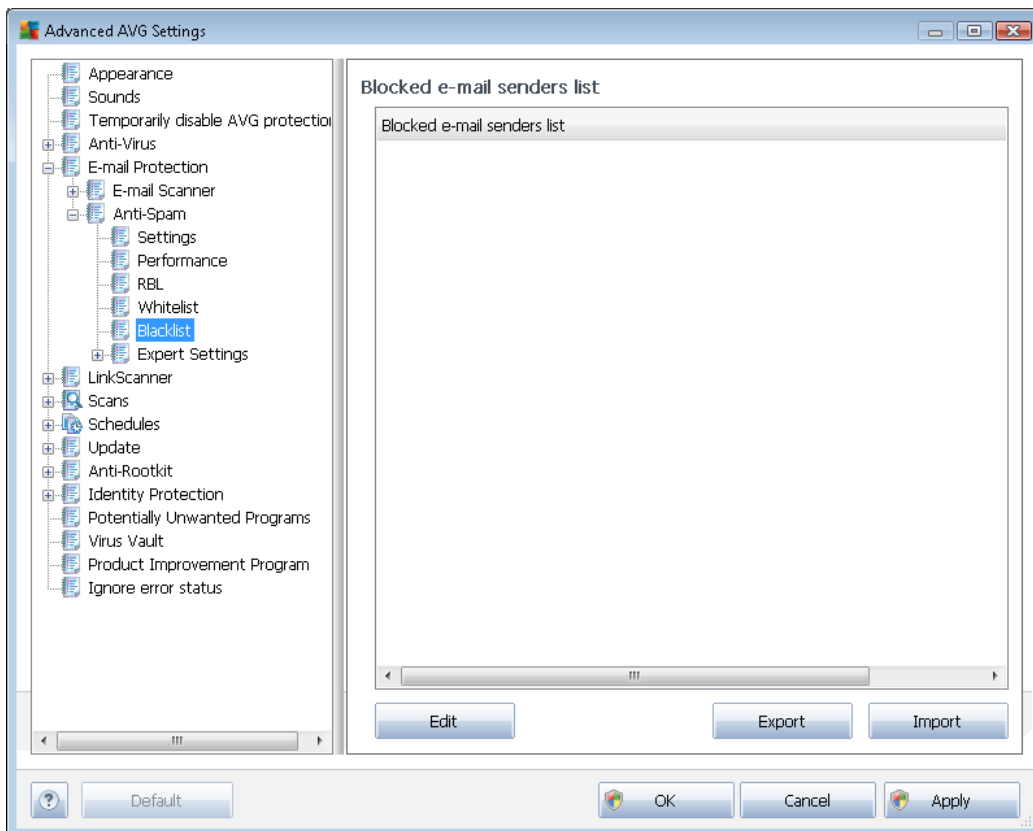
- **Edit** - press this button to open a dialog, where you can manually enter a list of addresses (



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

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

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



In the editing interface you can compile a list of senders that you expect to send you unwanted messages (*spam*). You can also compile a list of full domain names (e.g. *spammingcompany.com*), that you expect or receive spam messages from. All e-mail from the listed addresses/domains will be identified as spam. Once you have such a list of senders and/or domain names prepared, you can enter them by either of the following methods: by direct entry of each e-mail address or by importing the whole list of addresses at once.

### Control buttons



The following control buttons are available:

- **Edit** - press this button to open a dialog, where you can manually enter a list of addresses (you can also use copy and paste). Insert one item (sender, domain name) per line.
- **Export** - if you decide to export the records for some purpose, you can do so by pressing this button. All records will be saved to a plain text file.
- **Import** - if you already have a text file of email addresses/domain names prepared, you can simply import it by selecting this button.

***The Advanced Settings branch contains extensive setting options for the Anti-Spam component. These settings are intended exclusively for experienced users, typically network administrators who need to configure the antispam protection in full detail for the best protection of e-mail servers. For this reason, there is no extra help available for the individual dialogs; however, there is a brief description of each respective option directly in the user interface.***

***We strongly recommend not changing any settings unless you are fully familiar with advanced settings of Spamcatcher (MailShell Inc.). Any inappropriate changes may result in bad performance or incorrect component functionality.***

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

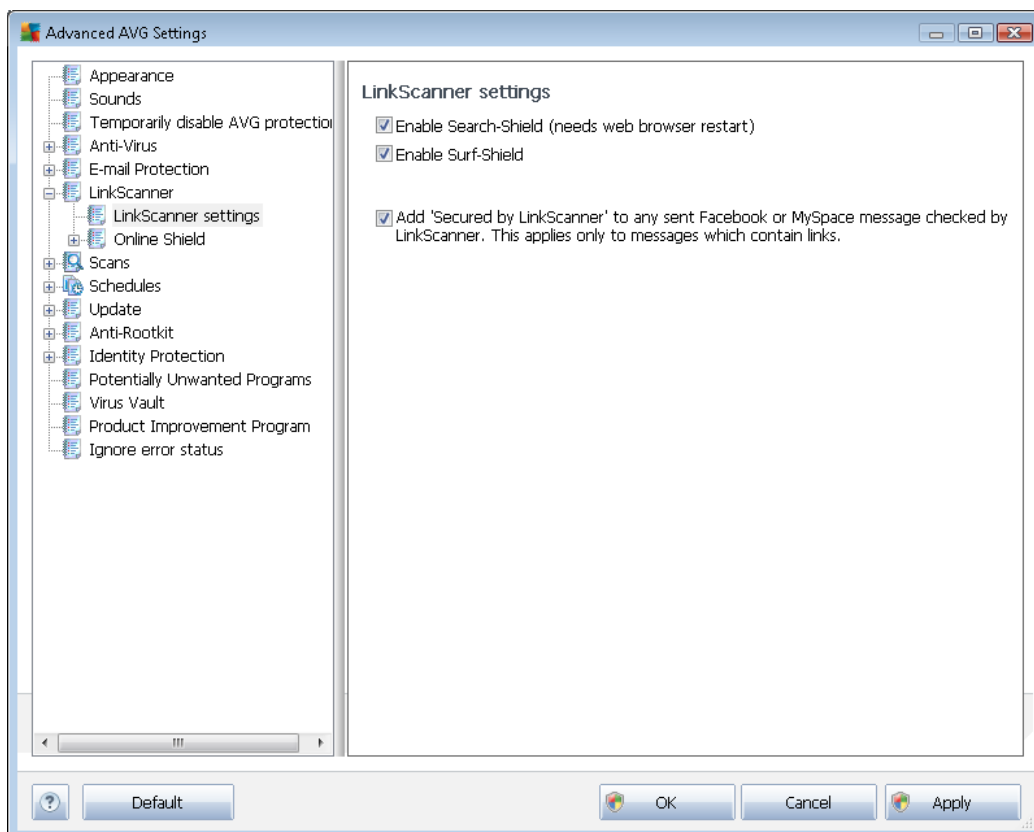
- **Cache** - fingerprint, domain reputation, LegitRepute
- **Training** - maximum word entries, auto training threshold, weight
- **Filtering** - language list, country list, approved IPs, blocked IPs, blocked countries, blocked charsets, spoofed senders
- **RBL** - RBL servers, multihit, threshold, timeout, maximum IPs
- **Internet connection** - timeout, proxy server, proxy authentication

## 9.6. Link Scanner



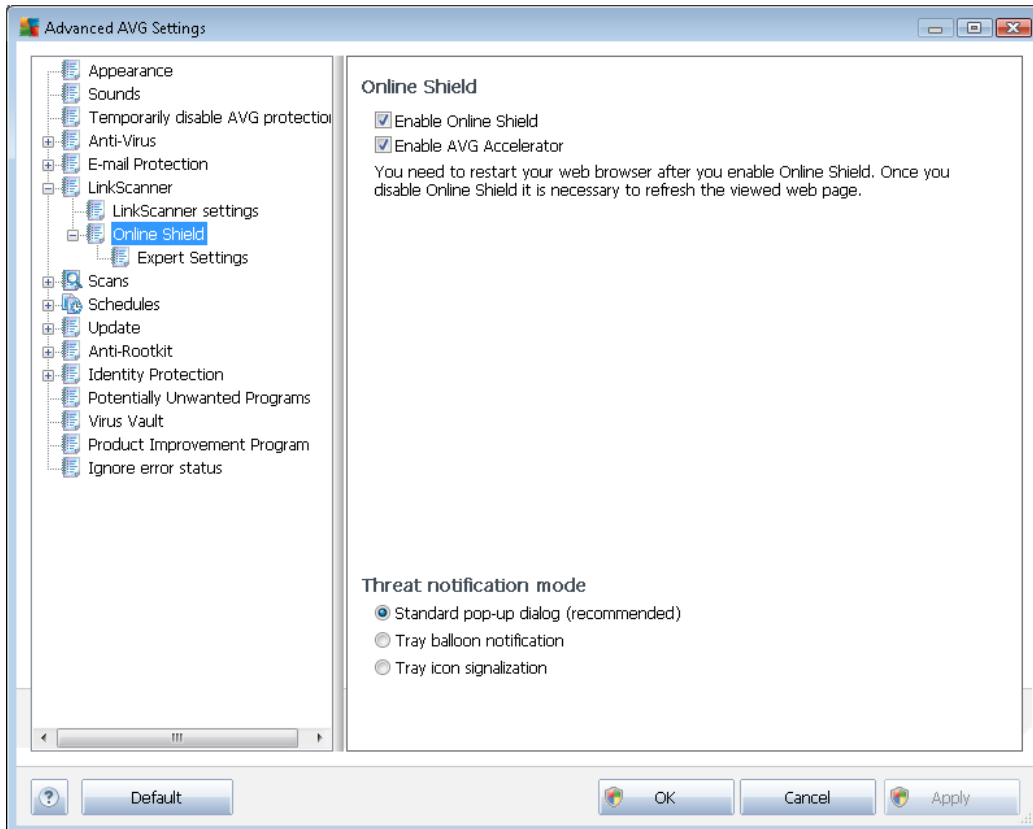
### 9.6.1. Link Scanner settings

The [LinkScanner settings](#) dialog allows you to switch on/off the elementary features of the [LinkScanner](#):



- **Enable Search-Shield** - (on by default): advisory notifying icons on searches performed with Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, or SlashDot having checked ahead the content of sites returned by the search engine.
- **Enable Surf-Shield** - (on by default): active (*real-time*) protection against exploitive sites as they are accessed. Known malicious site connections and their exploitive content is blocked as they are accessed by the user via a web browser (*or any other application that uses HTTP*).
- **Add 'Secured by LinkScanner' ...** - (off by default): mark this item to confirm you wish to enter the certification notice on [LinkScanner](#) check into all messages containing active hyperlinks, that were sent from Facebook and MySpace social networks.

## 9.6.2. Online Shield

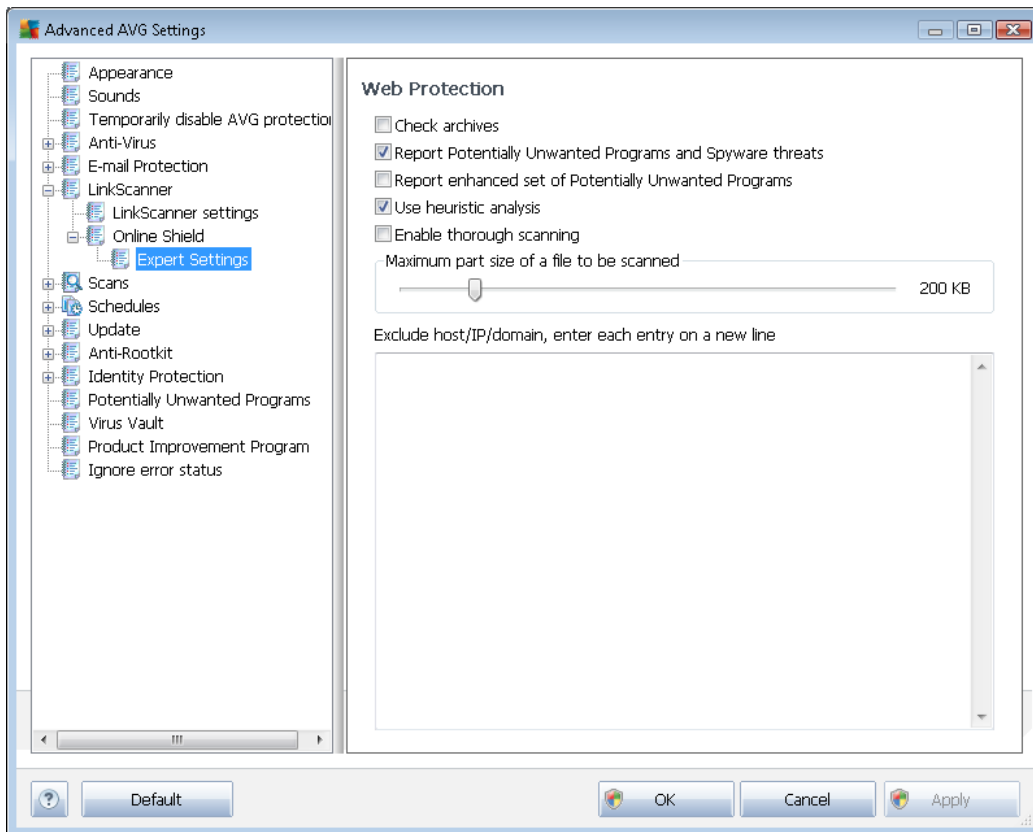


The **Online Shield** dialog offers the following options:

- **Enable Online Shield** (*on, by default*) - Activate/deactivate the entire **Online Shield** service. For further advanced settings of **Online Shield** please continue to the subsequent dialog called [Web Protection](#).
- **Enable AVG Accelerator** (*on, by default*) - Activate/deactivate the **AVG Accelerator** service that allows smoother online video playback and makes additional downloads easier.

### Threat notification mode

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



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

- **Enable Web protection** - this option confirms that the **Online Shield** should perform scanning of the www pages content. Provided this option is on (*by default*), you can further switch on/off these items:
  - **Check archives** - (*off by default*): scan the content of archives possibly included in the www page to be displayed.
  - **Report Potentially Unwanted Programs and Spyware threats** - (*on by default*): check to activate the [Anti-Spyware](#) engine, and scan for spyware as well as for viruses. [Spyware](#) represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend to keep this feature activated as it increases your computer security.
  - **Report enhanced set of Potentially Unwanted Programs** - (*off by default*): mark to detect extended package of [spyware](#): programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it can possibly block legal programs, and is therefore switched off by default.



- **Use heuristic analysis** - (on by default): scan the content of the page to be displayed using the [heuristic analysis](#) method (*dynamic emulation of the scanned object's instructions in a virtual computer environment*).
- **Enable thorough scanning** (off by default) - in specific situations (*suspicious of your computer being infected*) you may check this option to activate the most thorough scanning algorithms that will scan even those areas of your computer that can hardly get infected, just to be absolutely sure. Remember though that this method is rather time consuming.
- **Maximum part size of a file to be scanned** - if included files are present in the displayed page you can also scan their content even before these are downloaded to your computer. However, scanning of large files takes quite some time and the web page download might be slowed significantly. You can use the slide bar to specify the maximum size of a file that is still to be scanned with **Online Shield**. Even if the downloaded file is bigger than specified, and therefore will not be scanned with Online Shield, you are still protected: in case the file is infected, the **Resident Shield** will detect it immediately.
- **Exclude host/IP/domain** - into the text field you can type the exact name of a server (*host, IP address, IP address with mask, or URL*) or a domain that should not be scanned by **Online Shield**. Therefore exclude only host that you can be absolutely sure would never provide dangerous website content.

## 9.7. Scans

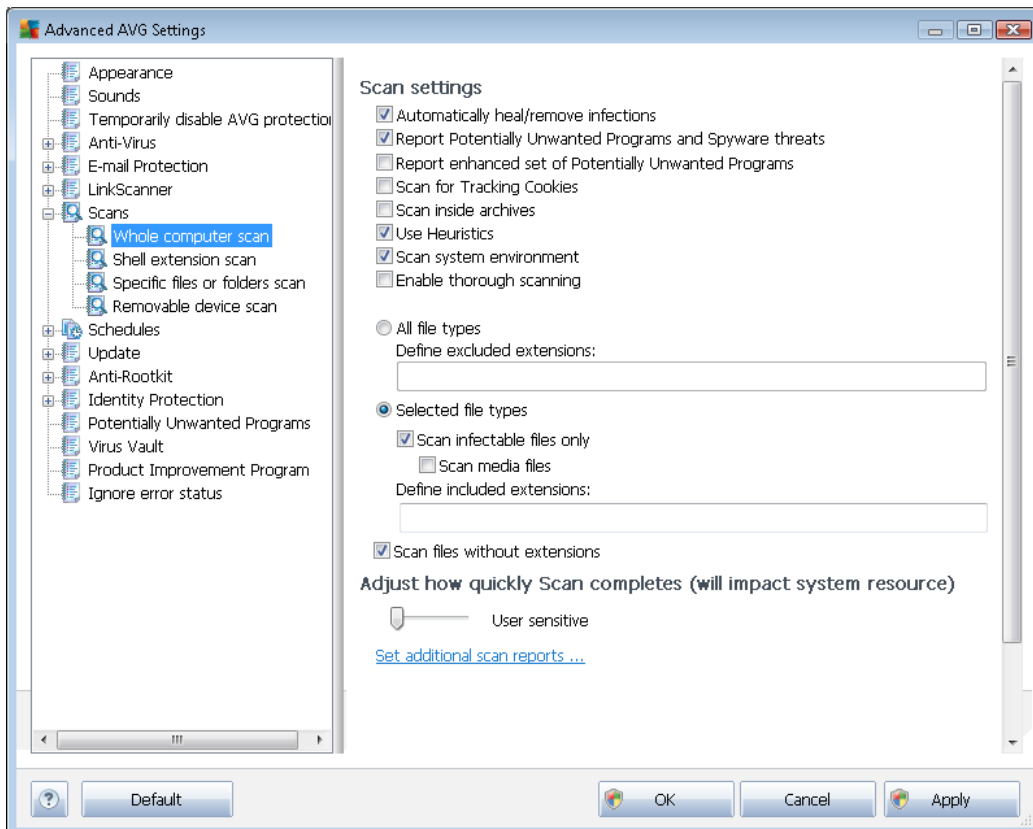
The advanced scan settings is divided into four categories referring to specific scan types as defined by the software vendor:

- [Whole Computer scan](#) - standard predefined scan of the entire computer
- [Shell Extension Scan](#) - specific scanning of a selected object directly from the Windows Explorer environment
- [Specific Files or Folders Scan](#) - standard predefined scan of selected areas of your computer
- [Removable Device Scan](#) - specific scanning of removable devices attached to your computer



### 9.7.1. Whole computer scan

The **Whole Computer scan** option allows you to edit parameters of one of the scans predefined by the software vendor, [Whole computer scan](#):



#### Scan settings

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

- **Automatically heal/remove infection** (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, the infected object will be moved to the [Virus Vault](#).
- **Report Potentially Unwanted Programs and Spyware threats** (on by default) - check to activate the [Anti-Spyware](#) engine, and scan for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend to keep this feature activated as it increases your computer security.
- **Report enhanced set of Potentially Unwanted Programs** (off by default) - mark to detect extended package of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an



additional measure that increases your computer security even more, however it can possibly block legal programs, and is therefore switched off by default.

- **Scan for Tracking Cookies** (off by default) - 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** (off by default) - this parameters defines that scanning should check all files stored inside archives, e.g. ZIP, RAR, ...
- **Use Heuristics** (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** (on by default) - scanning will also check the system areas of your computer.
- **Enable thorough scanning** (off by default) - in specific situations (*suspicious of your computer being infected*) you may check this option to activate the most thorough scanning algorithms that will scan even those areas of your computer that can hardly get infected, just to be absolutely sure. Remember though that this method is rather time consuming.

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 (*having been saved, the commas change into semicolons*) file extensions that should not be scanned;
- **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.

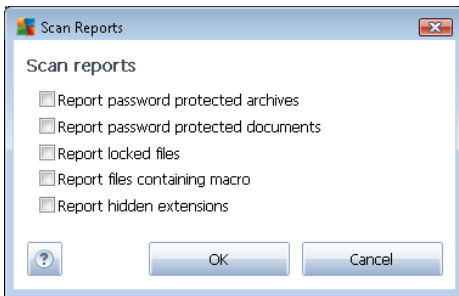
### Adjust how quickly Scan completes

Within the **Adjust how quickly scan completes** section you can further specify the desired scanning speed dependent on system resource usage. By default, this option value is set to *user sensitive* 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.



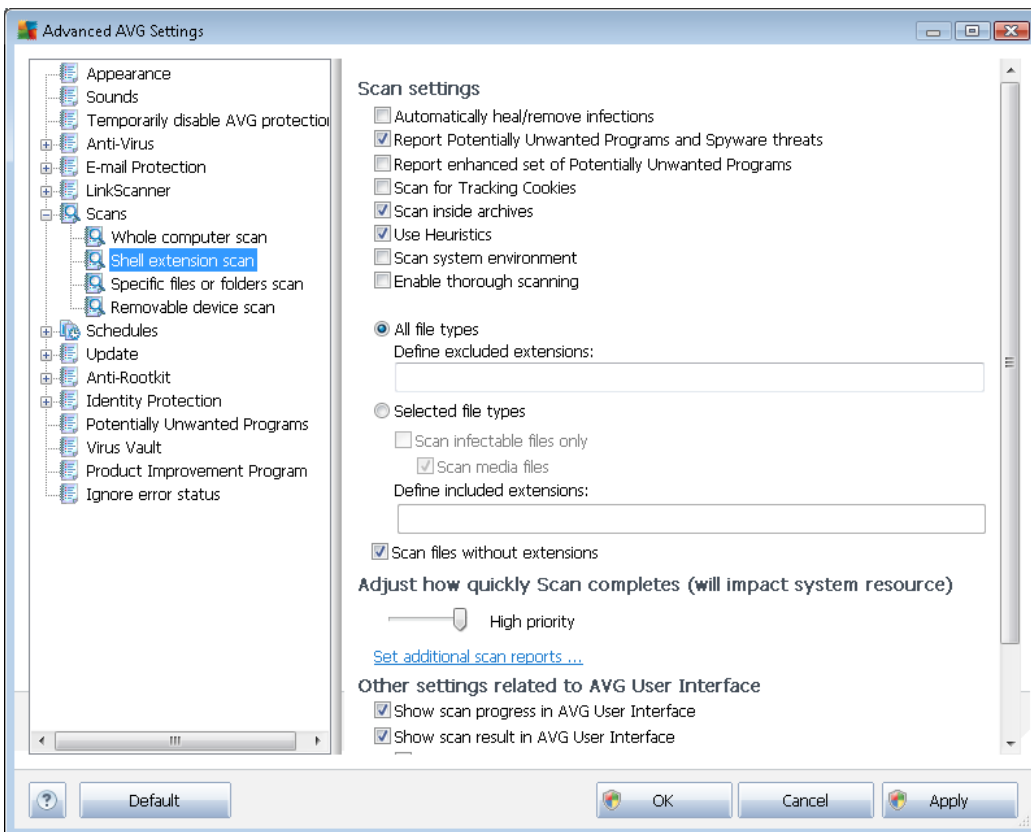
### Set additional scan reports ...

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:



### 9.7.2. Shell extension Scan

Similar to the previous [Whole Computer scan](#) 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,



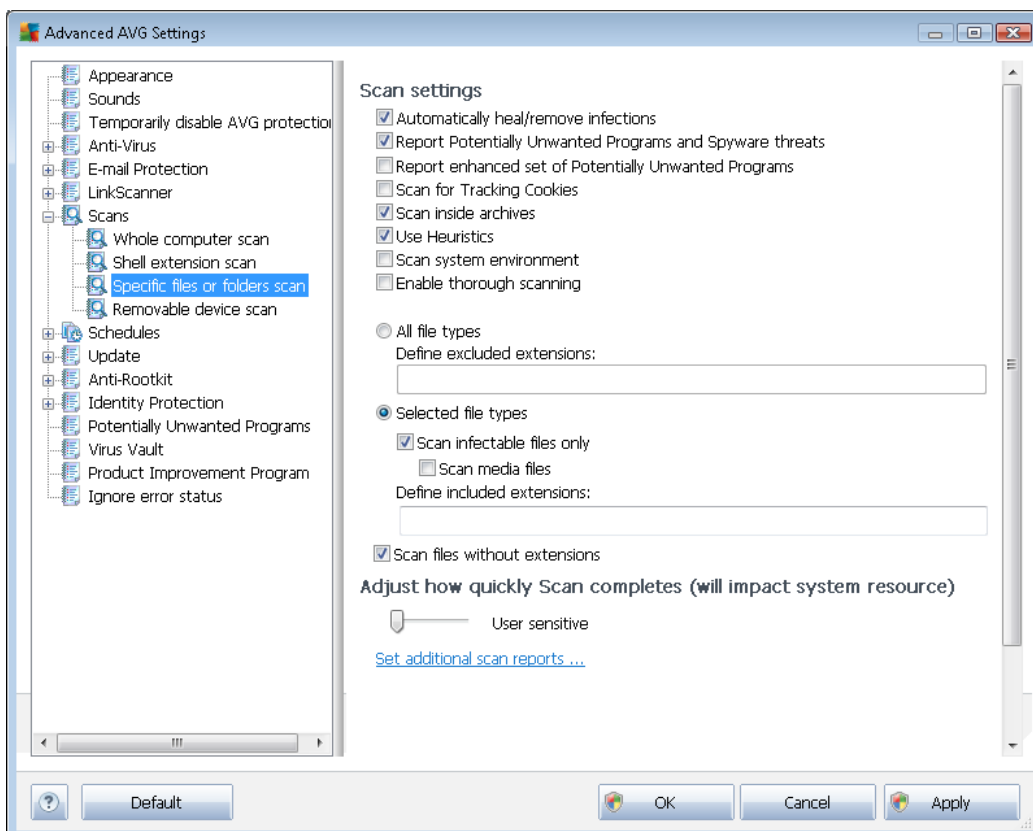
the default settings differ (for instance, Whole Computer scan by default does not check the archives but it does scan the system environment, while with the Shell Extension Scan it is the other way).

**Note:** For a description of specific parameters please consult the chapter [AVG Advanced Settings / Scans / Whole Computer scan](#).

Compared to [Whole Computer scan](#) dialog, the **Shell extension scan** dialog also includes the section named **Other settings related to AVG User Interface**, where you can specify whether you want the scan progress and scan results to be accessible from the AVG user interface. Also, you can define that the scan result should only be displayed in case an infection is detected during scanning.

### 9.7.3. Specific files or folders scan

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

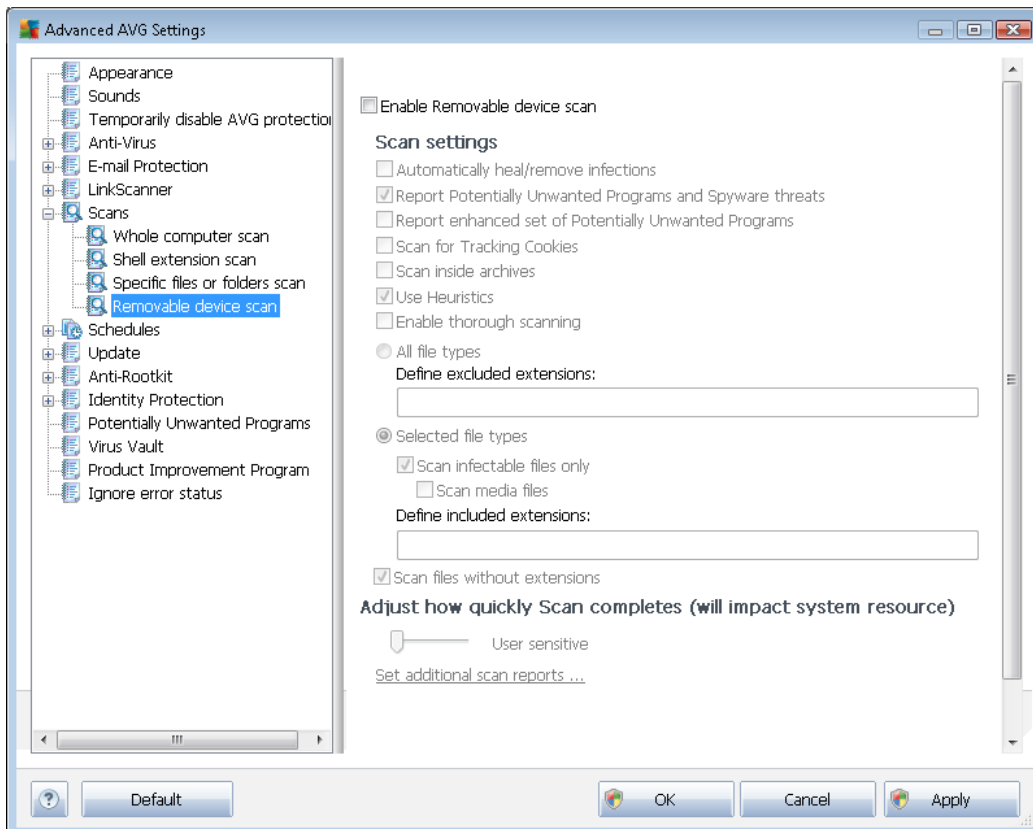


All parameters set up in this configuration dialog apply only to the areas selected for scanning with the [Scan of specific files or folders](#)!

**Note:** For a description of specific parameters please consult the chapter [AVG Advanced Settings / Scans / Whole Computer scan](#).

#### 9.7.4. Removable device scan

The editing interface for *Removable device scan* is also very similar to the [Whole Computer scan](#) 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 / Whole Computer scan](#).

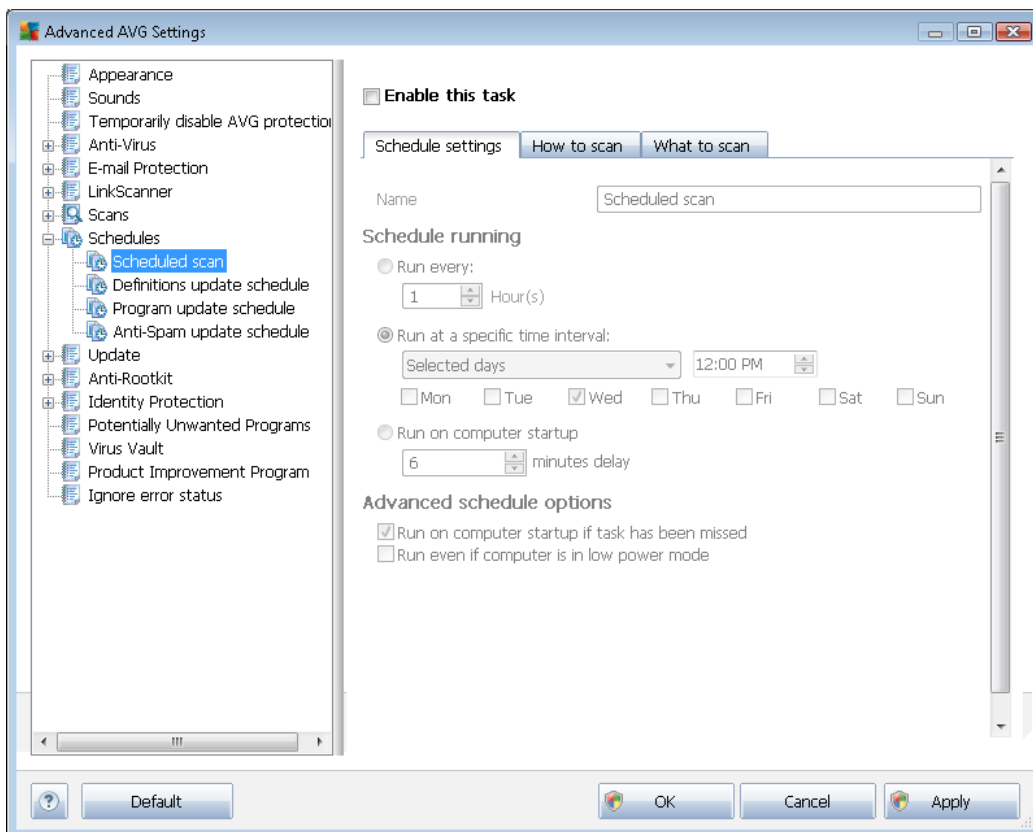
#### 9.8. Schedules

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

- [Scheduled scan](#)
- [Definitions update schedule](#)
- [Program update schedule](#)
- [Anti-Spam update schedule](#)

### 9.8.1. Scheduled Scan

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

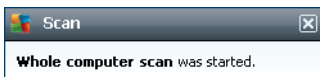
#### Schedule running



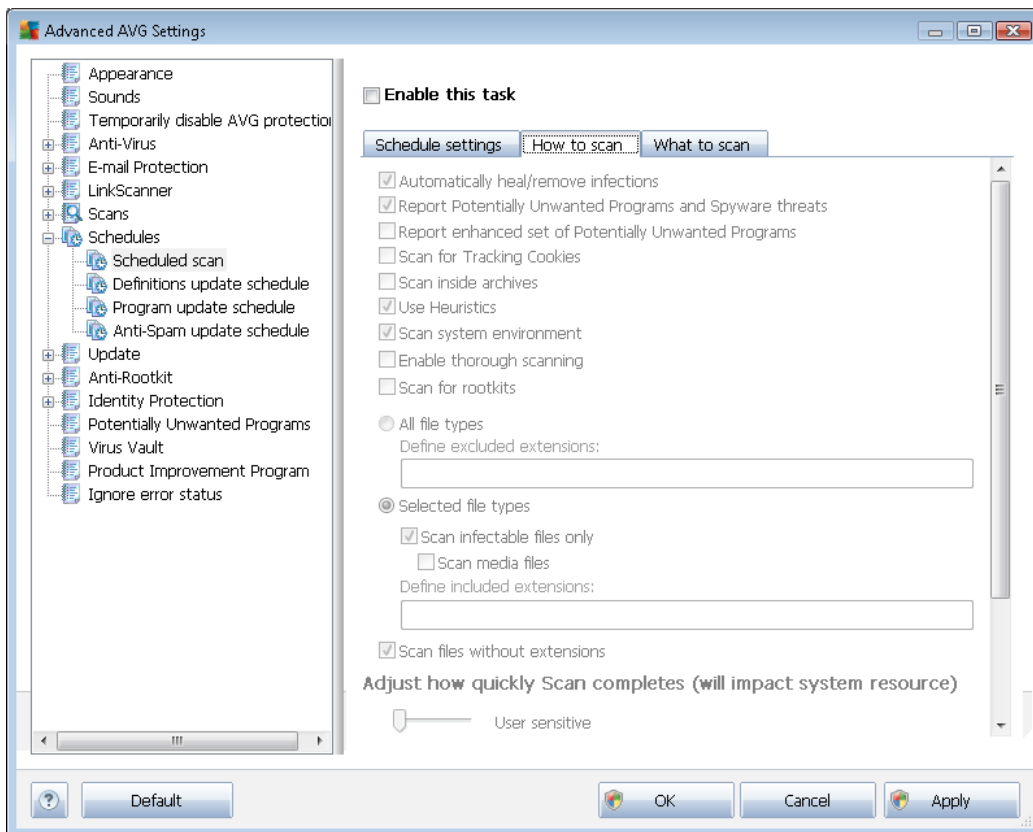
Here, you can specify time intervals for the newly scheduled scan launch. The timing can either be defined by the repeated scan launch after a certain period of time (**Run every ...**) or by defining an exact date and time (**Run at specific time interval ...**), or possibly by defining an event that the scan launch should be associated with (**Run 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 flash light*) informing a scheduled scan is running. Right-click on the running scan AVG icon to open a context menu where you can decide to pause or even stop the running scan, and also change the priority of the currently running 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 the predefined configuration:**

- **Automatically heal/remove infection** (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, the infected object will be moved to the [Virus Vault](#).
- **Report Potentially Unwanted Programs and Spyware threats** (on by default): check to activate the [Anti-Spyware](#) engine, and scan for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend to keep this feature activated as it increases your computer security.
- **Report enhanced set of Potentially Unwanted Programs** (off by default): mark to detect extended package of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it can possibly block legal programs, and is therefore switched off by default.
- **Scan for Tracking Cookies** (off 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** (off 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** (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** (on by default): scanning will also check the system areas of your computer;
- **Enable thorough scanning** (off by default) - in specific situations (*suspicious of your computer being infected*) you may check this option to activate the most thorough scanning algorithms that will scan even those areas of your computer that can hardly get infected, just to be absolutely sure. Remember though that this method is rather time consuming.
- **Scan for rootkits** (off by default): 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 (*having been saved, the commas change into semicolons*) file extensions that should not be scanned;
- **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.

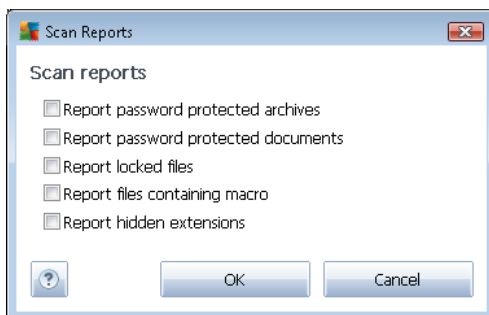
- Optionally, you can decide you want to **Scan files without extension** - this option is on by default, and it is recommended that you keep it so unless you have a real reason to change it. Files with no extension are rather suspicious and should be scanned at all times.

### Adjust how quickly Scan completes

Within the **Adjust how quickly Scan completes** section you can further specify the desired scanning speed dependent on system resource usage. By default, this option value is set to *user sensitive* 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.

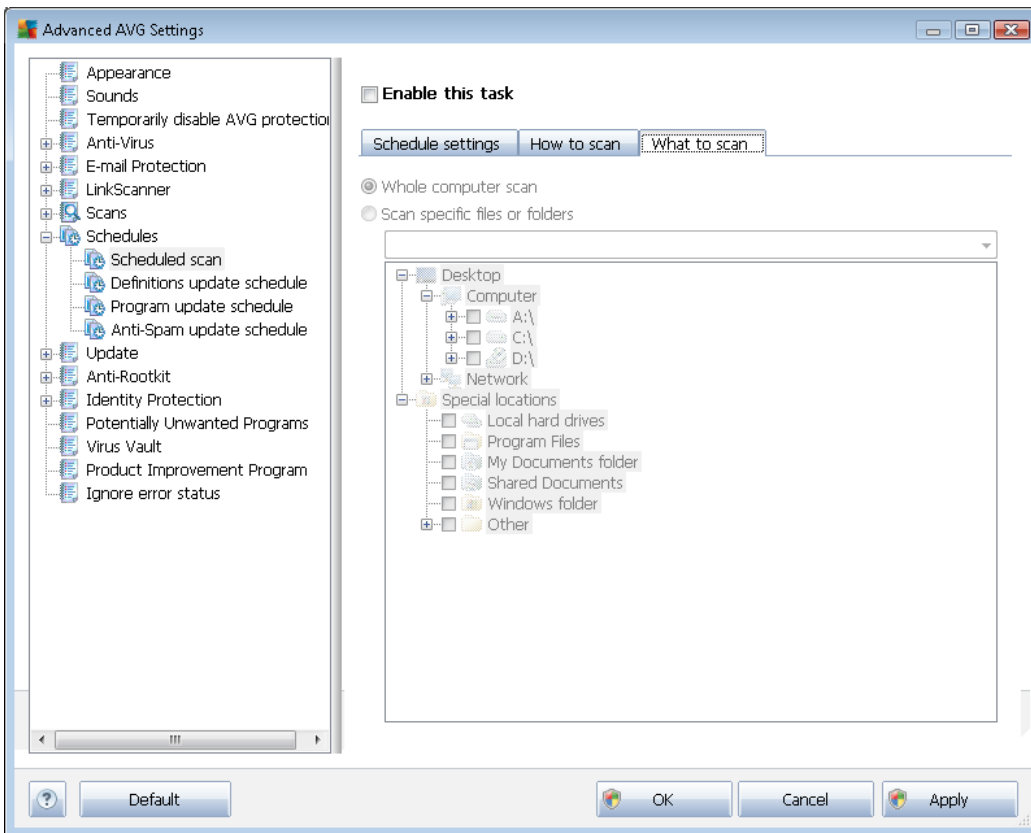
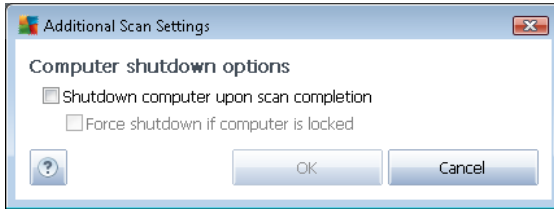
### Set additional scan reports

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:



### Additional scan settings

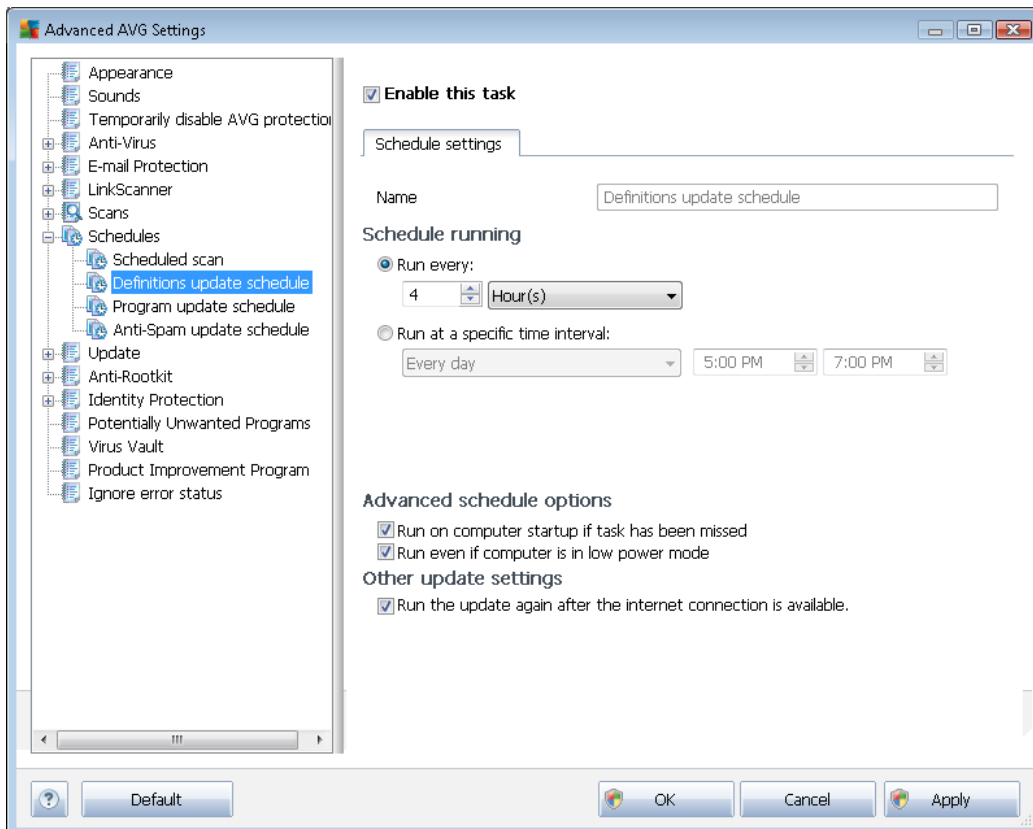
Click the **Additional scan settings ...** to open a new **Computer shutdown options** dialog where you can decide whether the computer should be shut down automatically once the running scanning process is over. Having confirmed this option (**Shutdown computer upon scan completion**), a new option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

## 9.8.2. Definitions Update Schedule

If *really necessary*, you can uncheck the **Enable this task** item to simply deactivate the scheduled definitions update temporarily, and switch it on again later:



Within this dialog you can set up some detailed parameters of the definitions 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.

### Schedule running

In this section, specify the time intervals for the newly scheduled definitions 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 ...**).

### Advanced schedule options

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

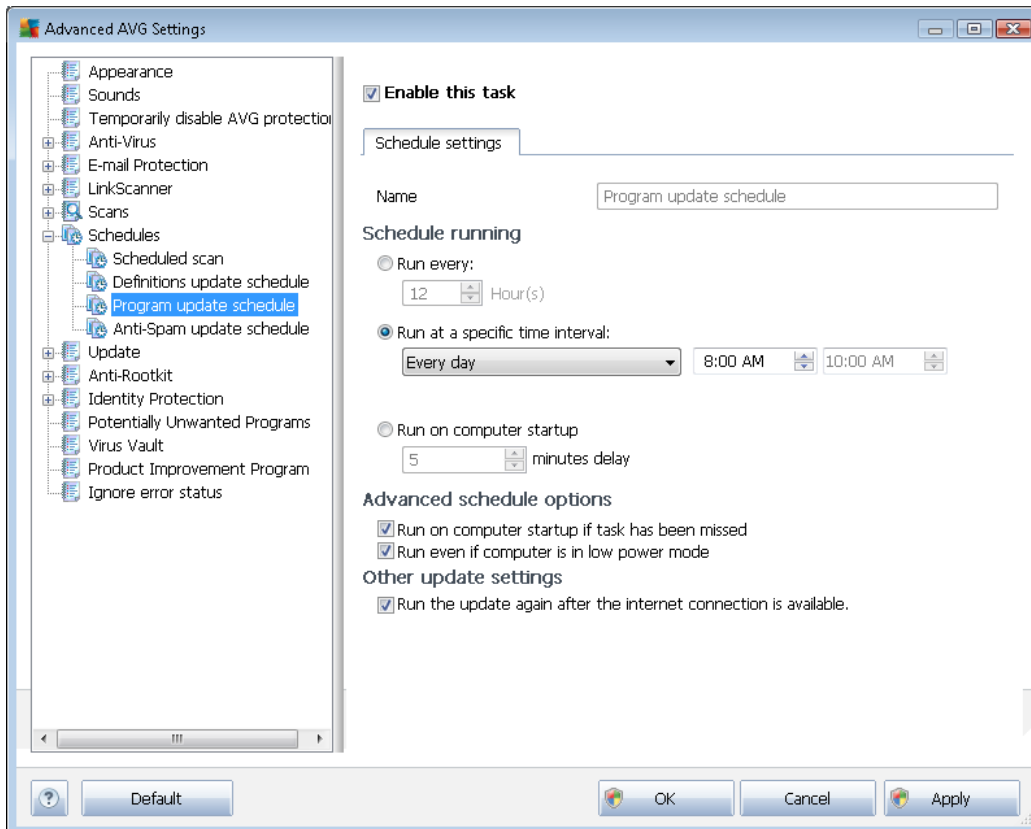


## Other update settings

Finally, check the **Run the update again as soon as the Internet connection is available** option to make sure that 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 [Advanced Settings/Appearance](#) dialog).

### 9.8.3. Program Update Schedule

If **really necessary**, you can uncheck the **Enable this task** item to simply deactivate the scheduled program update temporarily, and switch it on again later:



In the text field called **Name** (deactivated for all default schedules) there is the name assigned to this very schedule by the program vendor.

## 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.

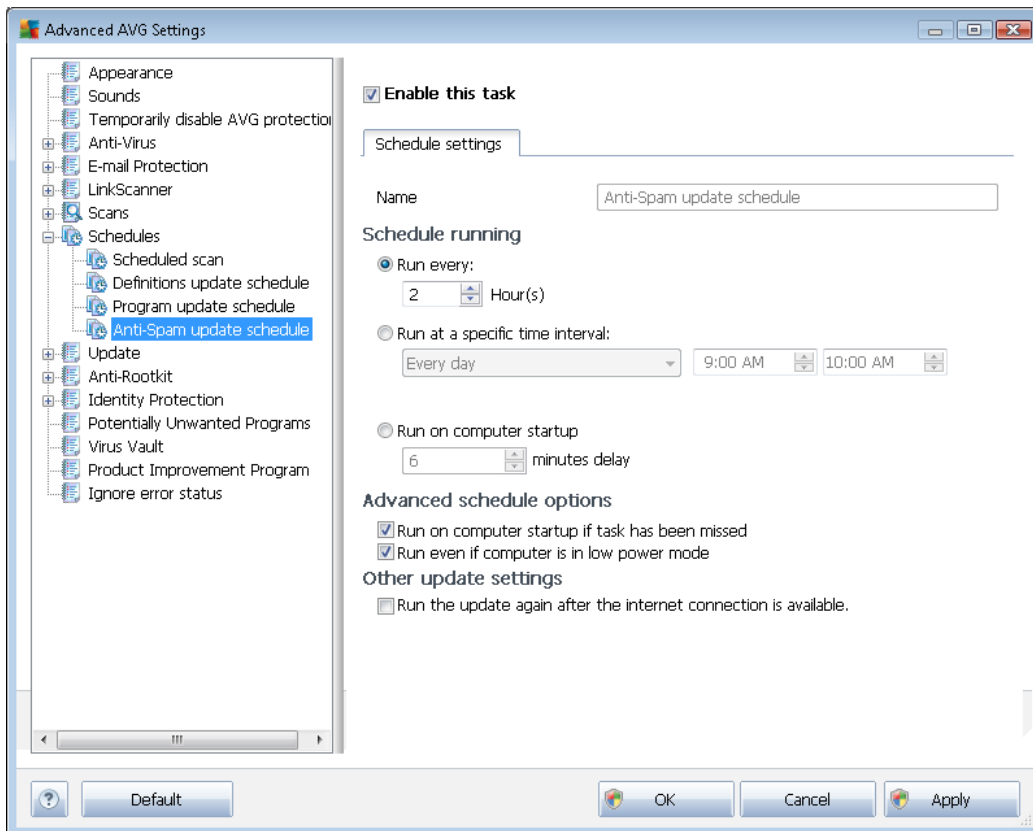
### **Other update settings**

Check the ***Run the update again as soon as the Internet connection is available*** option to make sure that 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 [Advanced Settings/Appearance](#) dialog).

**Note:** *If a time coincidence of a scheduled program update and scheduled scan occurs, the update process is of higher priority and the scan will get interrupted.*

### 9.8.4. Anti-Spam Update Schedule

If really necessary, you can uncheck the **Enable this task** item to simply deactivate the scheduled [Anti-Spam](#) update temporarily, and switch it on again later:



Within this dialog you can set up some detailed parameters of the 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.

#### Schedule running

Here, specify the time intervals for the newly scheduled [Anti-Spam](#) update launch. The timing can either be defined by the repeated [Anti-Spam](#) update 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 update launch should be associated with (**Action based on computer startup**).

#### Advanced schedule options

This section allows you to define under which conditions the [Anti-Spam](#) update should/should not be launched if the computer is in low power mode or switched off completely.



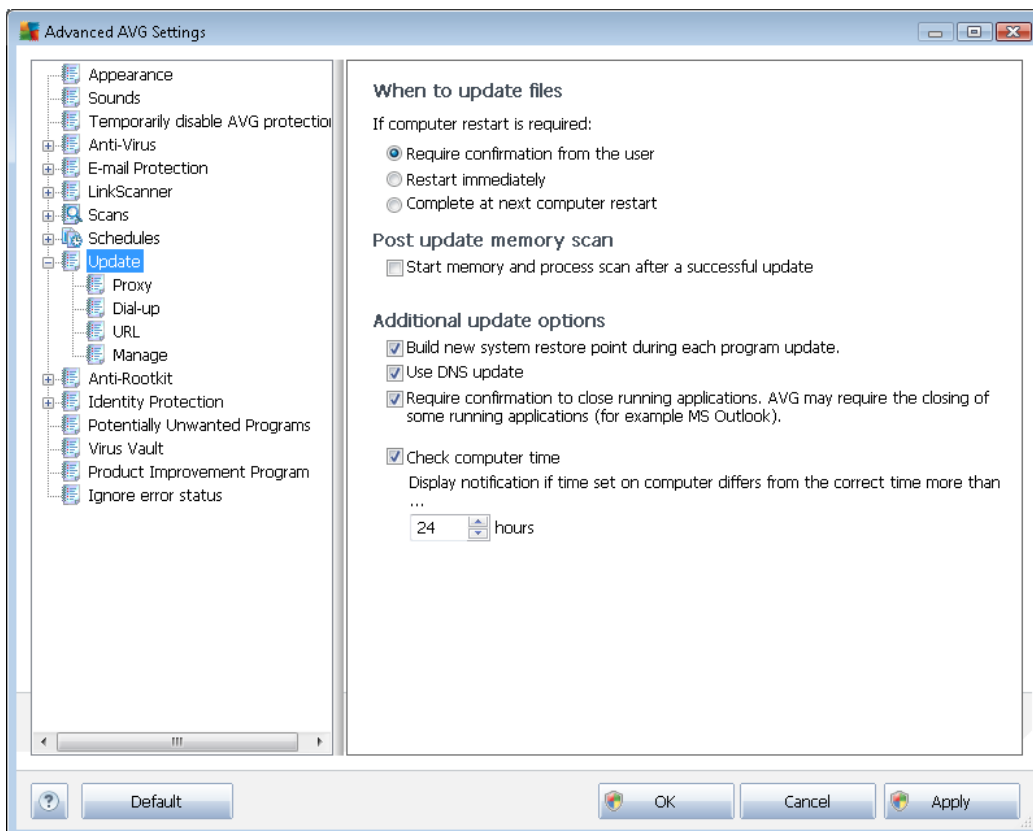
## Other update settings

Check the **Run the update again as soon as the Internet connection is available** option to make sure that if the internet connection gets corrupted and the [Anti-Spam](#) update process fails, it will be launched again immediately after the internet connection is restored.

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

## 9.9. 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 among three alternative options to be used in case the update process requires your PC restart. The update finalization can be scheduled for the next PC restart, or you can launch the restart immediately:



- **Require confirmation from the user (by default)** - 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. Please keep in mind that this option is only recommended if you are sure the computer gets restarted regularly, at least once a day!

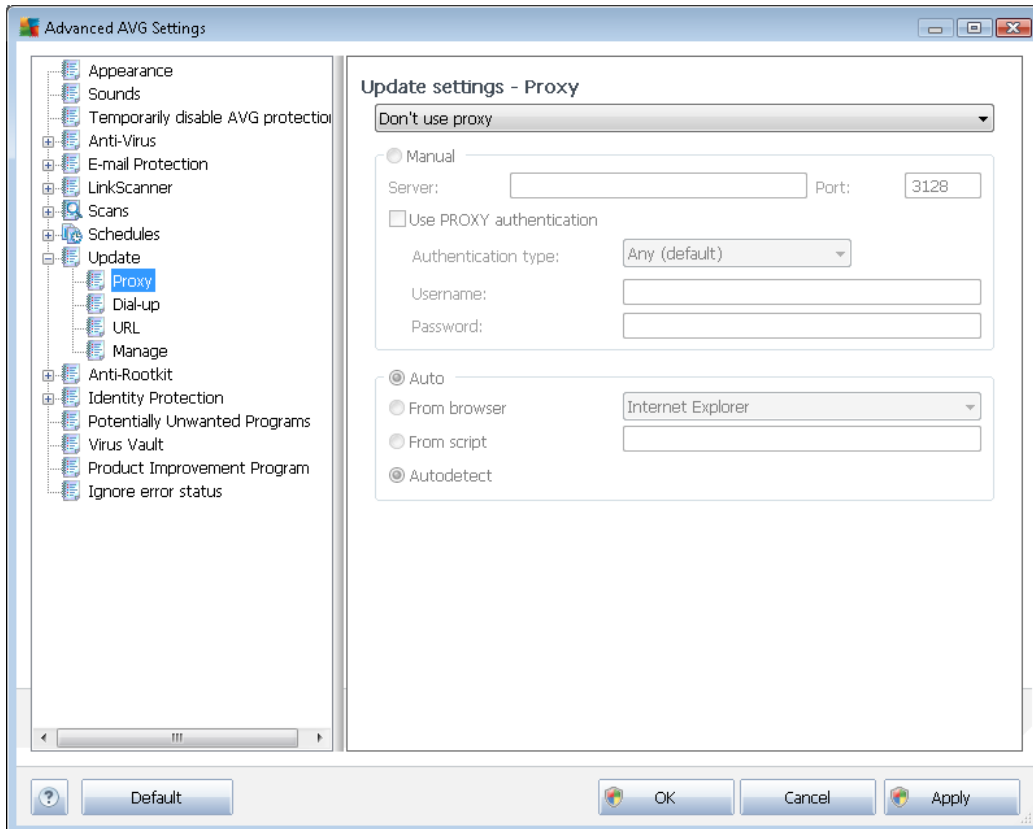
### Post update memory scan

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 during 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 (on by default)** - with this item marked, once the update is launched, your **AVG Premium Security 2012** looks up the information about the latest virus database version and the latest program version on the DNS server. Then only the smallest indispensably required update files are downloaded, and applied. This way the total amount of data downloaded is minimized, and the update process runs faster.
- **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.

### 9.9.1. 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**
- **Don't use proxy** - default settings
- **Try connection using proxy and if it fails, connect directly**

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.

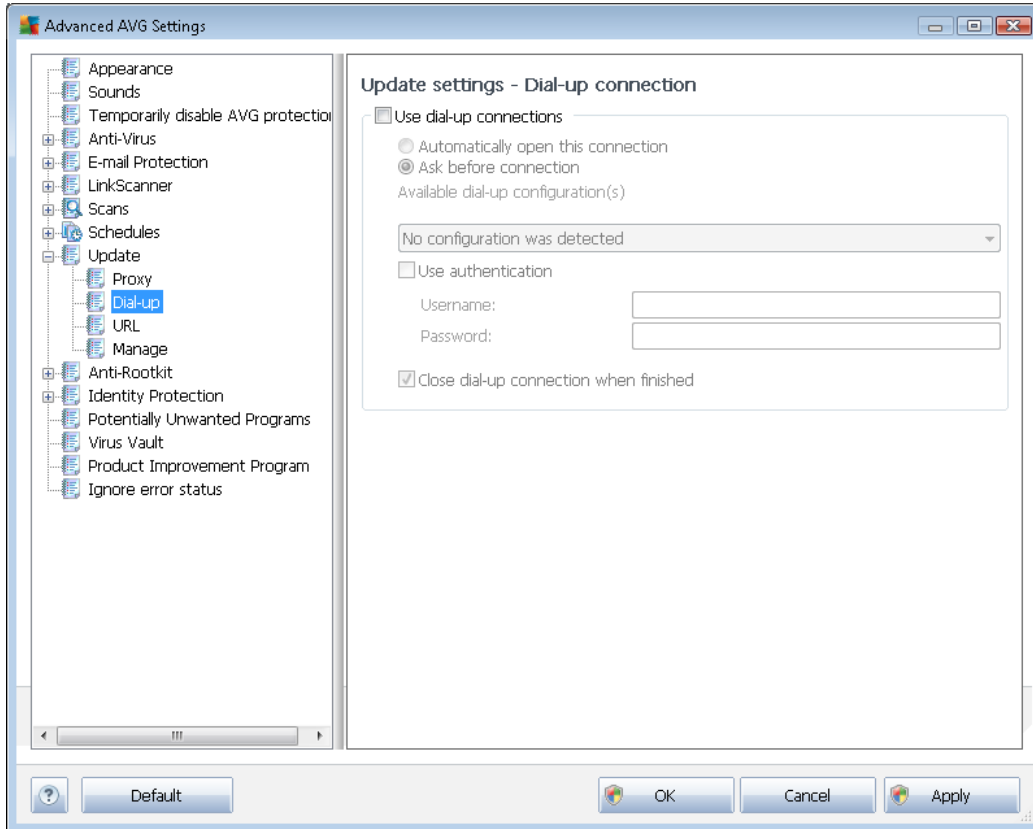
### **Automatic configuration**

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

### **9.9.2. Dial-up**

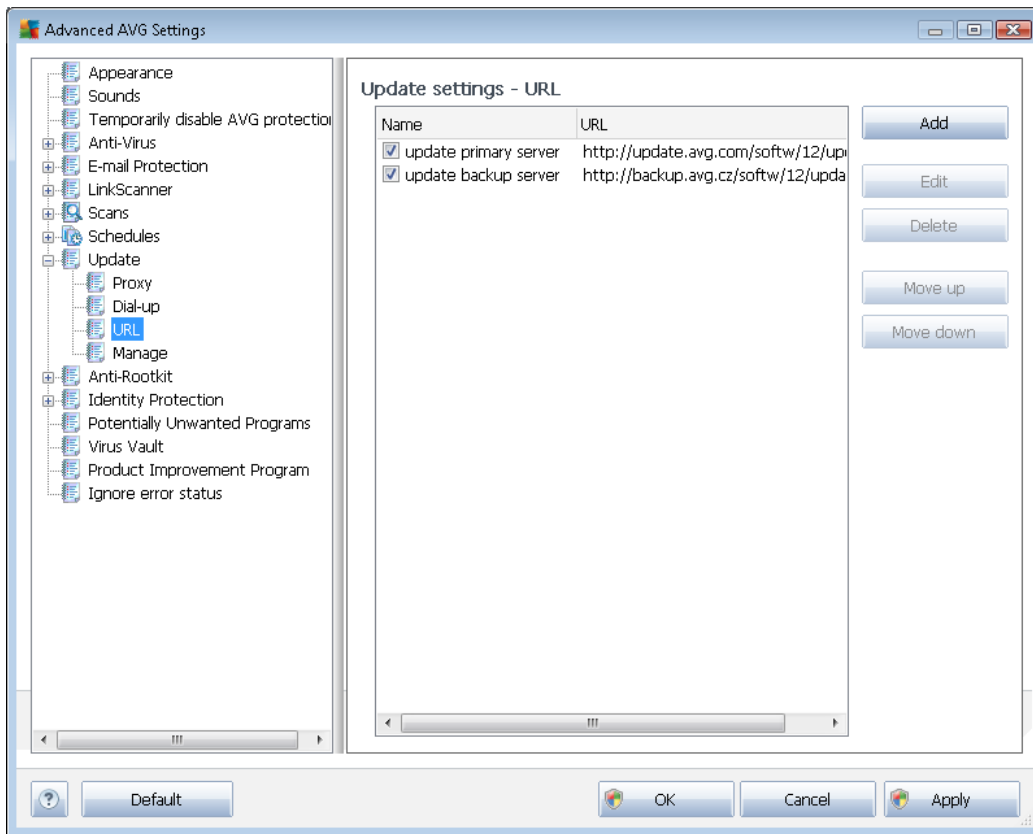
All parameters optionally defined in the **Update settings - Dial-Up connection** dialog refer to the dial-up connection to the Internet. The dialog's fields are inactive until you check the **Use dial-up connections** option that activates the fields:



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***).

### 9.9.3. URL

The **URL** dialog offers a list of Internet addresses from which the update files can be downloaded:



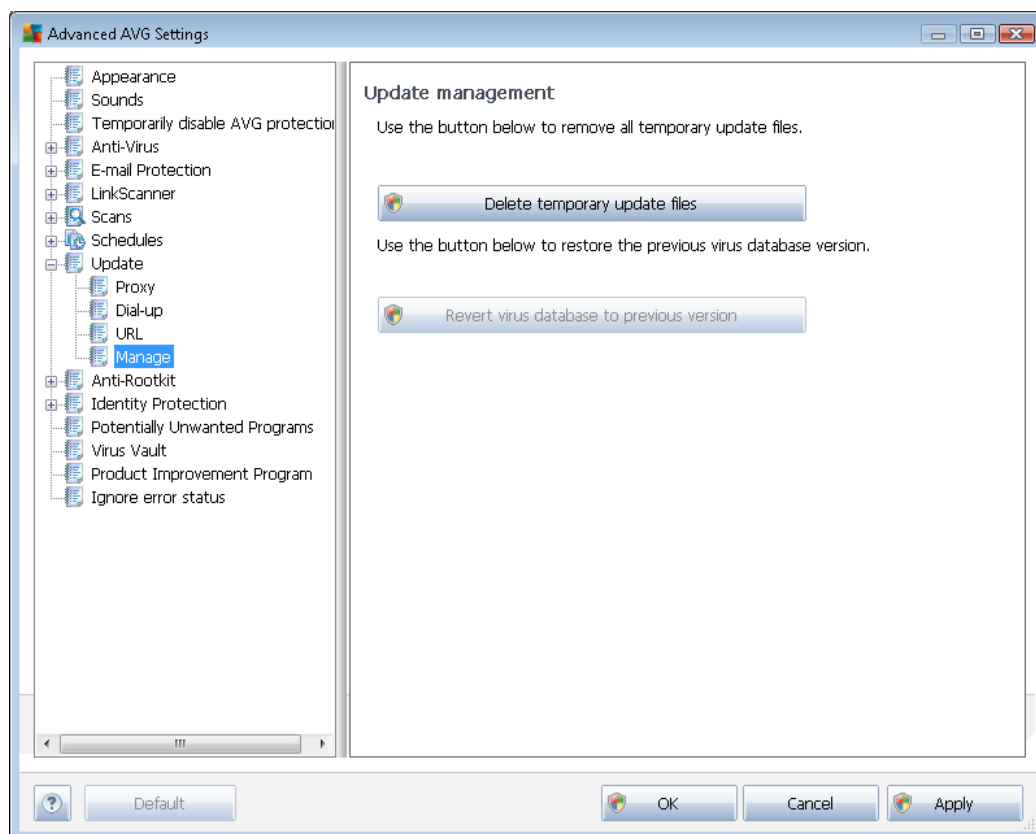
#### Control buttons

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

### 9.9.4. Manage

The **Update management** dialog offers two options accessible via two buttons:

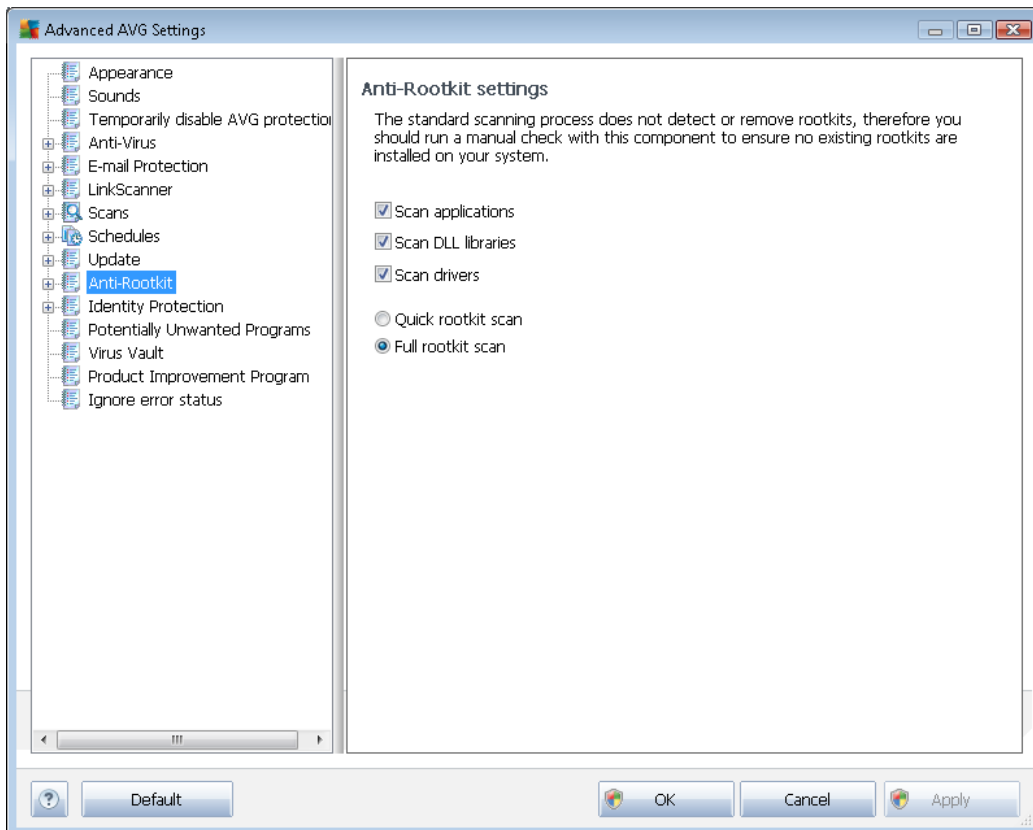


- **Delete temporary update files** - press this button to delete all redundant update files from your hard disk (*by default, these files are being saved for 30 days*)
- **Revert virus database to previous version** – press this button to delete the latest virus base version from your hard disk, and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



## 9.10. Anti-Rootkit

In the **Anti-Rootkit settings** dialog you can edit the [Anti-Rootkit](#) component's configuration:



Editing of all functions of the [Anti-Rootkit](#) component as provided within this dialog is also accessible directly from the [Anti-Rootkit component's interface](#).

**Scan applications**, **Scan DLL libraries** (*dynamic libraries*), and **Scan drivers** enable you to specify in detail what should be included in the Anti-Rootkit scan. These settings are intended for advanced users; we recommend to keep all options switched on.

Further you can pick the rootkit scanning mode:

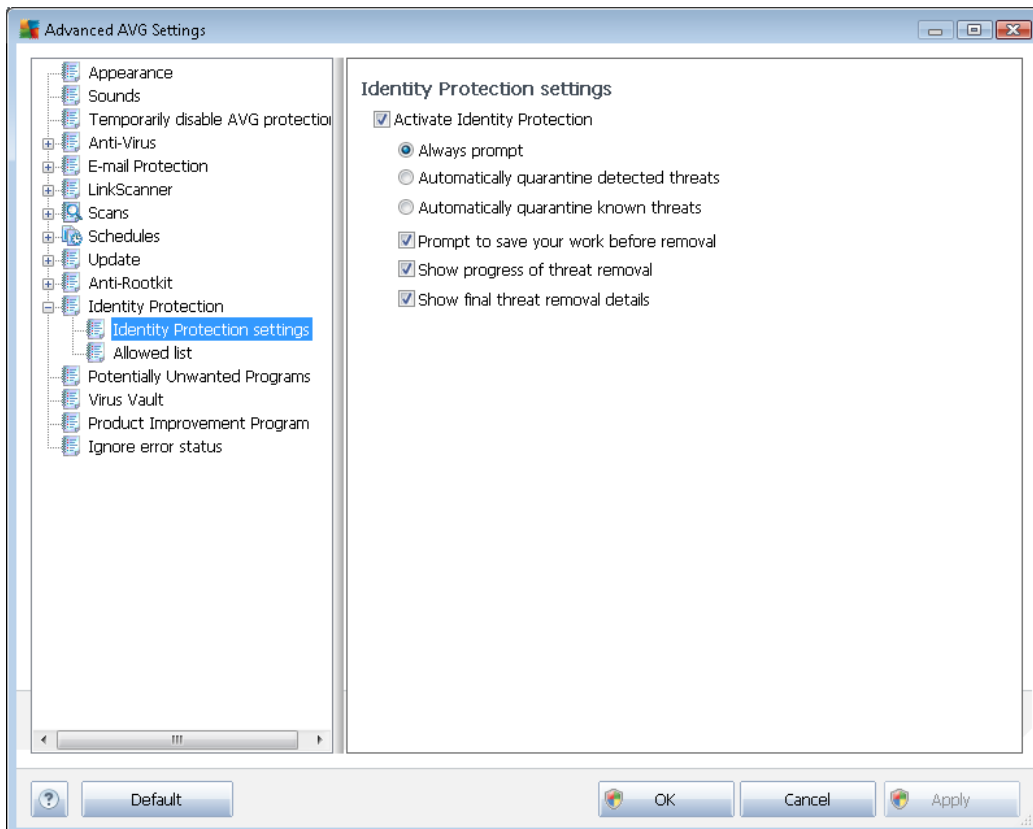
- **Quick rootkit scan** - scans all running processes, loaded drivers and the system folder (typically *c:\Windows*)
- **Full rootkit scan** - scans all running processes, loaded drivers, the system folder (typically *c:\Windows*), plus all local disks (*including the flash disk, but excluding floppy disk/CD drives*)





### 9.11.1. Identity Protection Settings

The **Identity Protection settings** dialog allows you to switch on/off the elementary features of the [Identity Protection](#) component:



**Activate Identity Protection** (on by default) – uncheck to turn off the [Identity Protection](#) component.

**We strongly recommend not to do this unless you have to!**

When the [Identity Protection](#) is activated, you can specify what to do when a threat is detected:

- **Always prompt** (on by default) - when a threat is detected, you will be asked whether it should be moved to quarantine to make sure no applications you want to run are removed.
- **Automatically quarantine detected threats** - mark this check box to define you want have all possibly detected threats moved to the safe space of [Virus Vault](#) immediately. Keeping the default settings, when a threat is detected, you will be asked whether it should be moved to quarantine to make sure no applications you want to run are removed.
- **Automatically quarantine known threats** - keep this item marked if you wish all applications detected as possible malware to be automatically and immediately moved to [Virus Vault](#).

Further you can assign specific items to optionally activate more [Identity Protection](#) functionality:





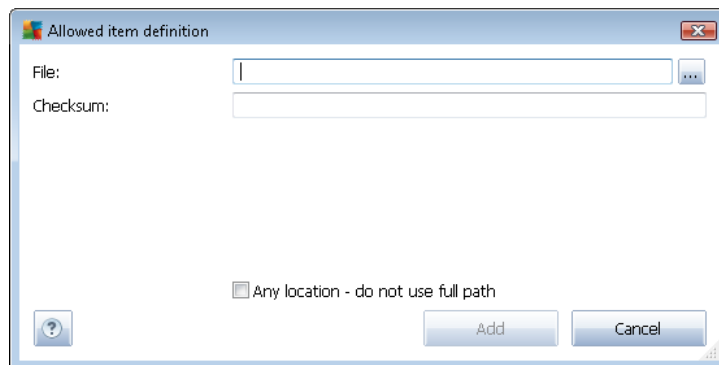
less important (■□□□) up to critical (■□□■)

- **Process path** - path to the application's (*process*) executable file location
- **Date allowed** - date when you manually assigned the application as safe

### Control buttons

The control buttons available within the **Identity Protection Allowed list** dialog are as follows:

- **Add** - press this button to add a new application to the allowed list. The following dialog pops-up:

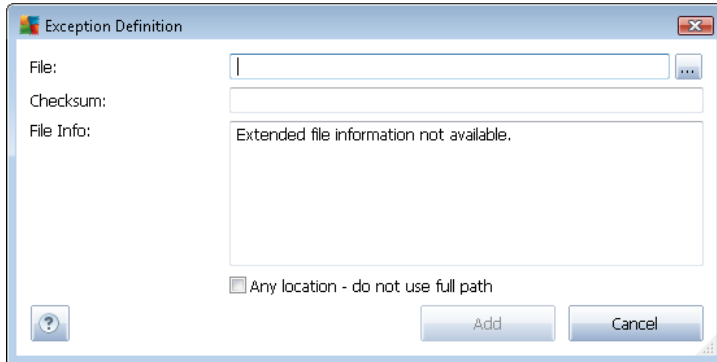


- **File** - type the full path to the file (*application*) that you want to mark as an exception
- **Checksum** - displays the unique 'signature' of the chosen file. This checksum is an automatically generated string of characters, which allows AVG to unequivocally distinguish the chosen file from other files. The checksum is generated and displayed after successful addition of the file.
- **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
- **Remove** - press to remove the selected application from the list
- **Remove all** - press to remove all listed applications

## 9.12. Potentially Unwanted Programs

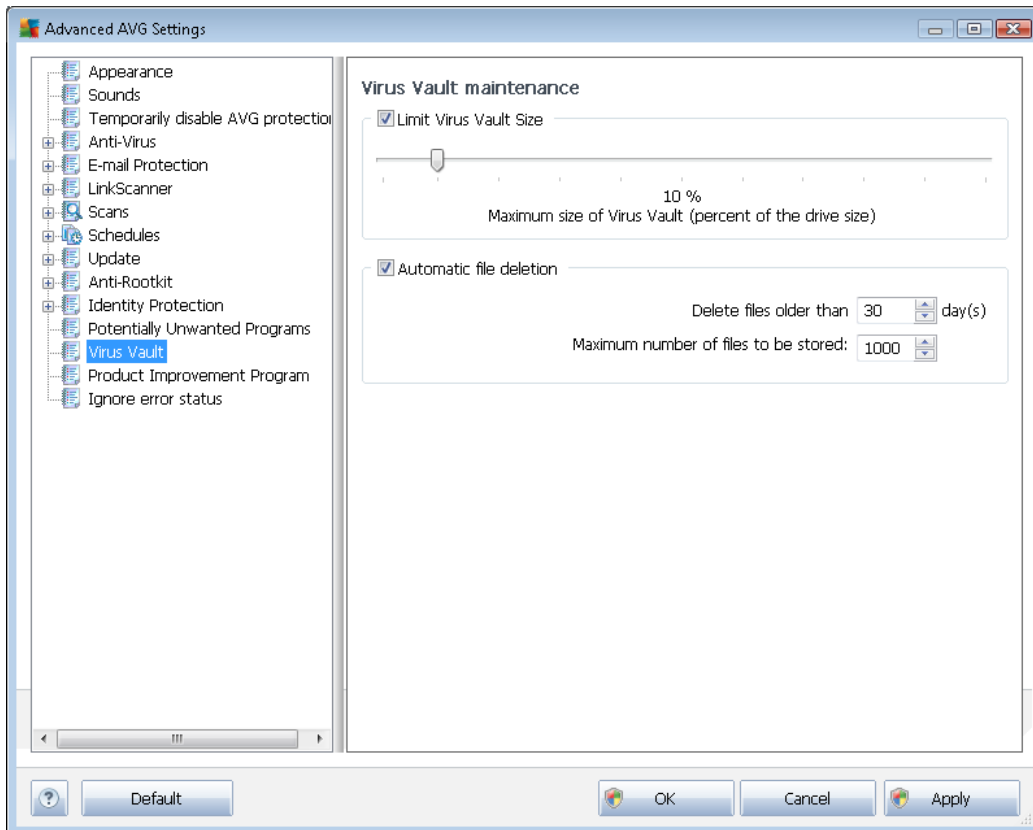
**AVG Premium Security 2012** is able to analyze and detect executable applications or DLL libraries that could be potentially unwanted within the system. In some cases the user may wish to keep certain unwanted programs on the computer (programs that were installed on purpose). Some programs, especially free ones, include adware. Such adware might be detected and reported by **AVG Premium Security 2012** 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:





- **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. If the checkbox is marked, the specified file is defined as an exception no matter where it is located (*however, you have to fill in the full path to the specific file anyway; the file will then be used as a unique example for the possibility that two files of the same name appear in your system*).

### 9.13. Virus Vault



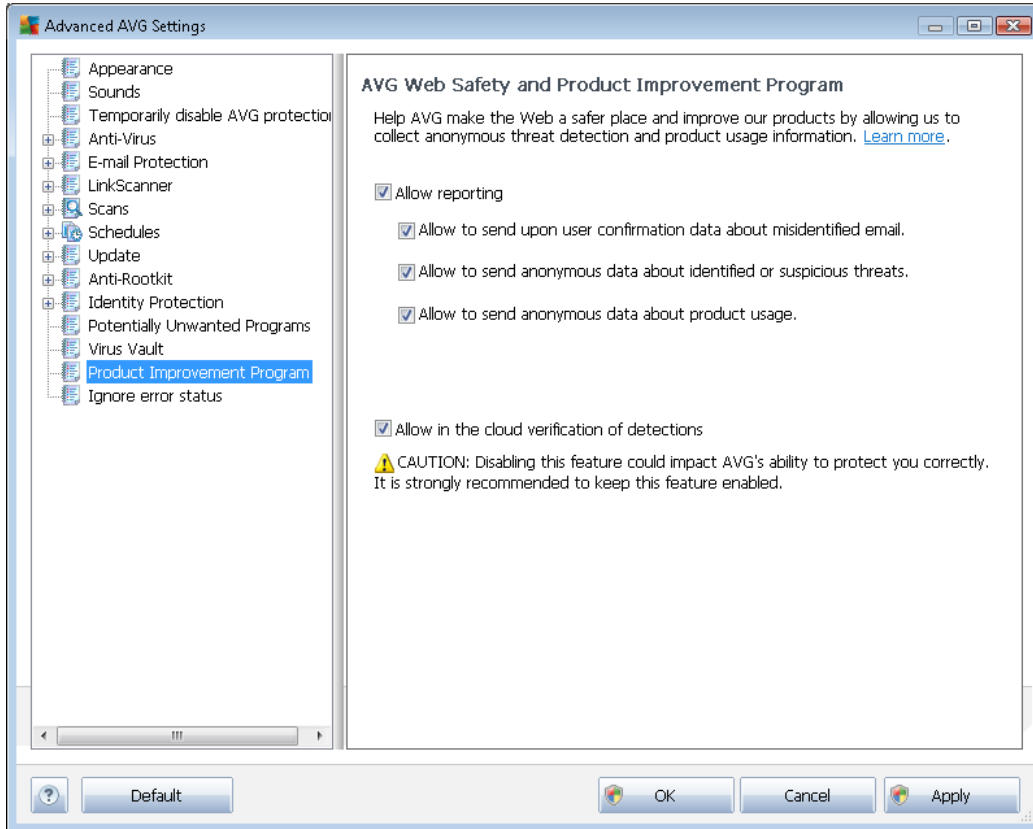
The **Virus Vault maintenance** dialog allows you to define several parameters regarding the administration of objects stored in the [Virus Vault](#):

- **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**).

### 9.14. Product Improvement Program

The **AVG Web Safety and Product Improvement Program** dialog invites you to participate in AVG product improvement, and to help us increase the overall Internet security level. Keep the **Allow reporting** option marked to enable reporting of detected threats to AVG laboratories. This helps us to collect up-to-date information on the latest threats from all participants worldwide, and in return we can improve protection for everyone.

**The reporting is taken care of automatically, therefore does not cause you any inconvenience. No personal data is included in the reports.** Reporting of detected threats is optional, however, we do ask you to keep this option switched on. It helps us improve protection for both you and other AVG users.



Within the dialog, the following setting options are available:

- **Allow reporting** (on by default) - If you want to help us further improve **AVG Premium Security 2012**, keep the checkbox marked. This will enable reporting all encountered threats to AVG, so we will be able to collect up-to-date information on malware from all participants worldwide, and in return improve protection for everyone. The reporting is taken care of automatically, therefore does not cause you any inconvenience, and no personal data is included in the reports.
  - **Allow to send upon user confirmation data about misidentified e-mail** (on by default) – send information about e-mail messages incorrectly identified as spam, or about spam messages that were not detected by the [Anti-Spam](#) component. When sending this kind of information, you will be asked for confirmation.
  - **Allow to send anonymous data about identified or suspicious threats** (on by default) – send information about any suspicious or positively dangerous code or behaviour pattern (can be a virus, spyware, or malicious webpage you are trying to access) detected on your computer.
  - **Allow to send anonymous data about product usage** (on by default) – send basic statistics about the application usage, such as number of detections, scans launched, successful or unsuccessful updates etc.
- **Allow in the cloud verification of detections** (on by default) – detected threats will be



checked if really infected, to sort out false positives.

### Most common threats

Nowadays, there are far more threats out there than plain viruses. Authors of malicious codes and dangerous websites are very innovative, and new kinds of threats emerge quite often, the vast majority of which are on the Internet. Here are some of the most common:

- **Virus** is a malicious code that copies and spreads itself, often unnoticed until the damage is done. Some viruses are a serious threat, deleting or deliberately changing files on their way, while some viruses can do something seemingly harmless, like playing a piece of music. However, all viruses are dangerous due to the basic ability of multiplying – even a simple virus can take up all the computer memory in an instant, and cause a breakdown.
- **Worm** is a subcategory of virus which, unlike a normal virus, does not need a "carrier" object to attach to; it sends itself to other computers self-contained, usually via e-mail, and as a result often overloads e-mail servers and network systems.
- **Spyware** is usually defined as a malware category (*malware = any malicious software, including viruses*) encompassing programs – typically Trojan horses – aimed at stealing personal information, passwords, credit card numbers, or infiltrating a computer and allowing the attacker to control it remotely; of course, all without the computer owner's knowledge or consent.
- **Potentially unwanted programs** are a type of spyware that can be may but not necessarily have to be dangerous to your computer. A specific example of a PUP is adware, software designed to distribute advertisements, usually by displaying ad pop-ups; annoying, but not really harmful.
- **Tracking cookies** can also be considered a kind of spyware, as these small files, stored in the web browser and sent automatically to the "parent" website when you visit it again, can contain data such as your browsing history and other similar information.
- **Exploit** is a malicious code that takes advantage of a flaw or vulnerability in an operating system, Internet browser, or other essential program.
- **Phishing** is an attempt to acquire sensitive personal data by shamming a trustworthy and well-known organization. Usually, the potential victims are contacted by a bulk e-mail asking them to e.g. update their bank account details. In order to do that, they are invited to follow the link provided which then leads to a fake website of the bank.
- **Hoax** is a bulk e-mail containing dangerous, alarming or just bothering and useless information. Many of the above threats use hoax e-mail messages to spread.
- **Malicious websites** are ones that deliberately install malicious software on your computer, and hacked sites do just the same, only these are legitimate websites that have been compromised into infecting visitors.

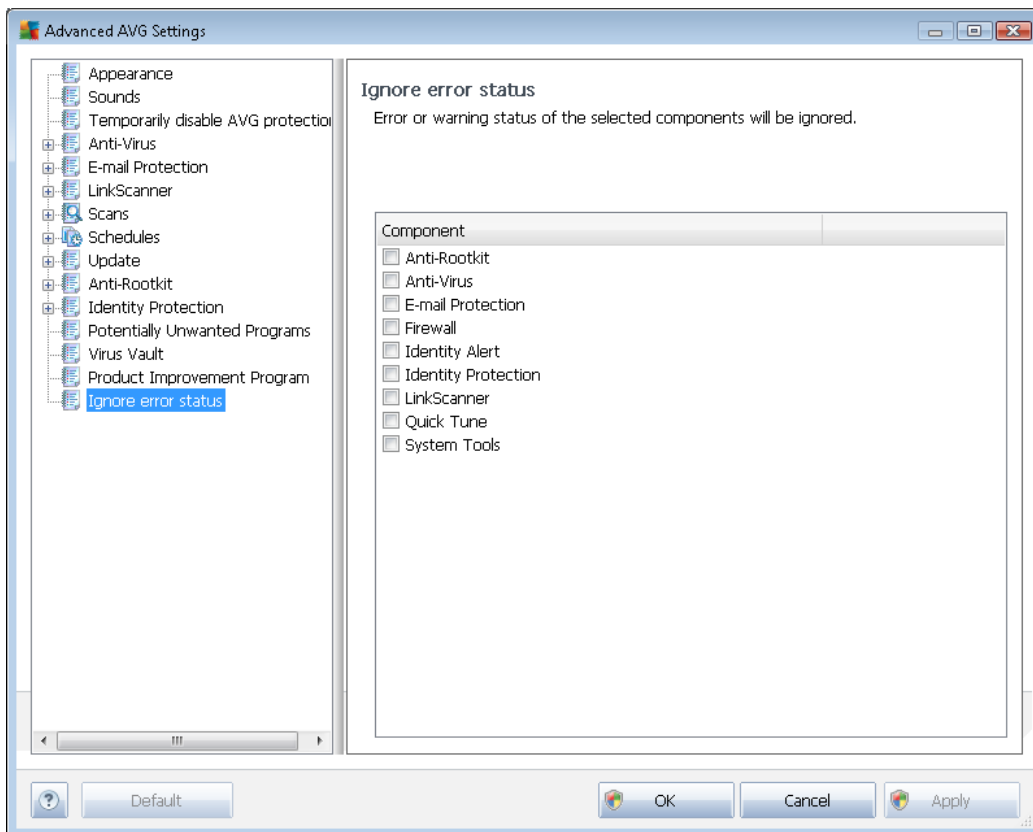
**To protect you from all of these different kinds of threats, AVG Premium Security 2012 includes specialized components. For brief description of these please consult the**



[Components Overview](#) chapter.

## 9.15. Ignore error status

In the **Ignore error status** 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 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 (*Ignore component state*) is also available for specific components directly from the [components overview in the AVG main window](#).



## 10. Firewall Settings

The [Firewall](#) configuration opens in a new window where in several dialogs can set up very advanced parameters of the component.

**However, the software vendor has set up all AVG Premium Security 2012 components to give optimum performance. Unless you have a real reason to do so, do not change the default configuration. Any changes to settings should only be performed by an experienced user only!**

### 10.1. General

The **General information** dialog is divided into two sections:



#### Firewall status

In the **Firewall status** section you can switch the [Firewall](#) status as the need arises:

- **Firewall enabled** - select this option to allow communication to those applications that are assigned as 'allowed' in the set of rules defined within selected [Firewall profile](#).
- **Firewall disabled** - this option switches [Firewall](#) off completely, all network traffic is allowed but not checked!
- **Emergency mode (block all Internet traffic)** - select this option to block all traffic on every single network port; [Firewall](#) is still running but all network traffic is stopped.



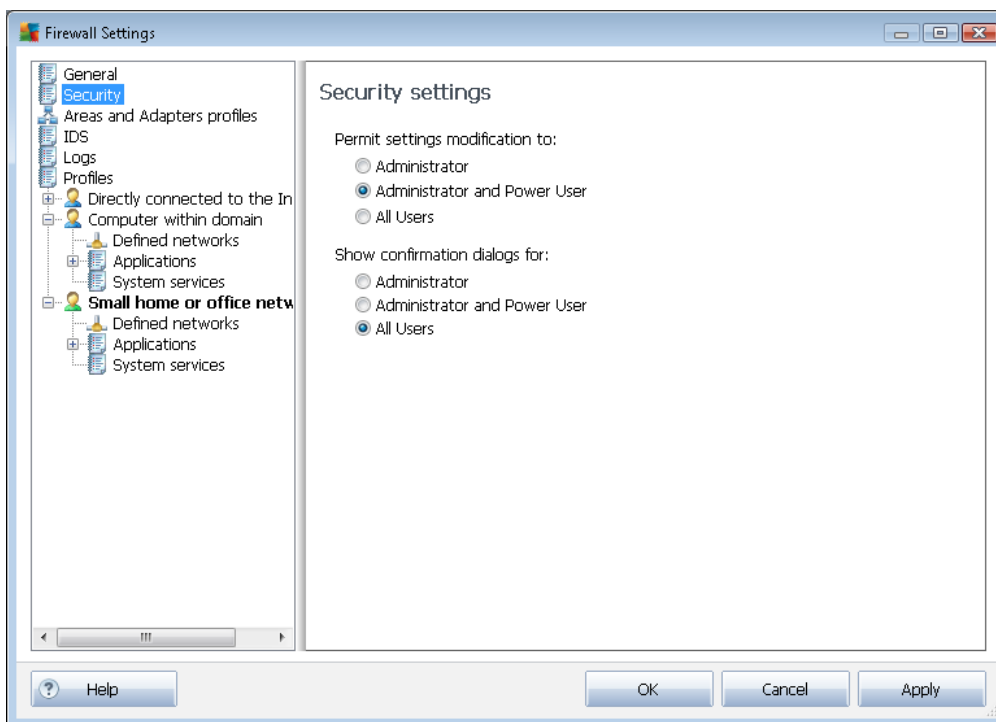
- **Enable all traffic to VPN (on by default)** - if you use a VPN (Virtual Private Network) connection, e.g. to connect to your office from home, we recommend to check the box. **AVG Firewall** will automatically search through your network adapters, find those used for VPN connection, and allow all applications to connect to the target network (*only applies to applications with no specific Firewall rule assigned*). On a standard system with common network adapters, this simple step should save you from having to set up a detailed rule for each application that you need to use over VPN.

**Note:** To enable VPN connection at all, it is necessary to allow communication to the following system protocols: GRE, ESP, L2TP, PPTP. This can be done in the [System services](#) dialog.

## Settings management

In the **Setting management** section you can **Export** or **Import Firewall** configuration; i.e. export the defined [Firewall](#) rules and settings to the back-up files, or on the other hand to import the entire back up file.

## 10.2. Security



In the **Security settings** dialog you can define general rules of [Firewall](#)'s behavior regardless the selected profile:

- **Permit settings modification to** - specify who is allowed to change the [Firewall](#)'s configuration.



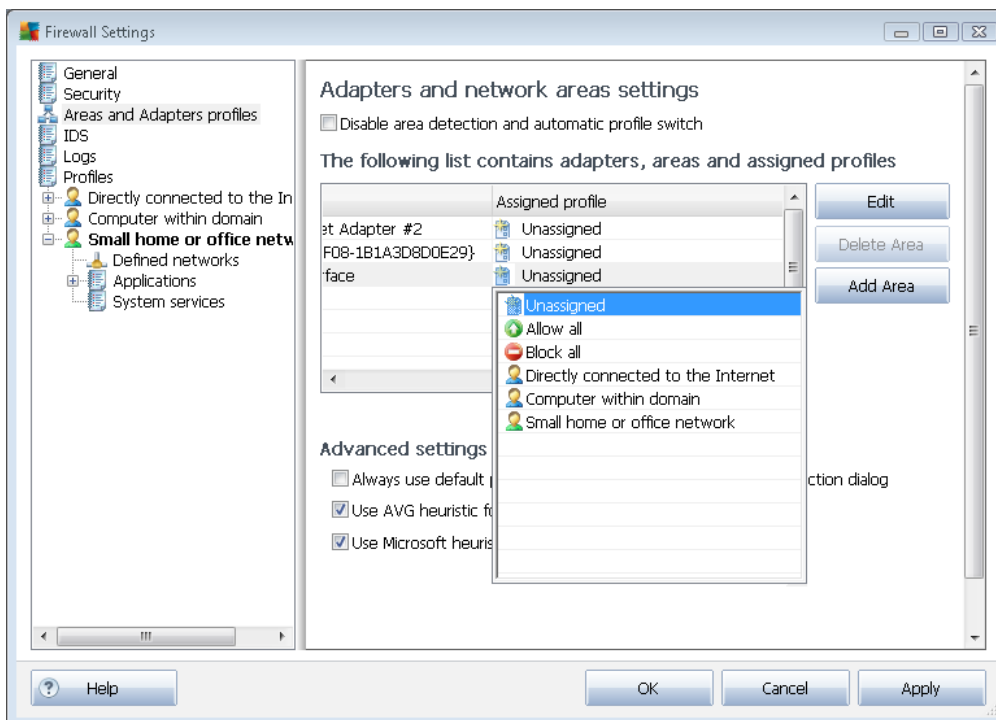
- **Show confirmation dialogs for** - specify to whom the confirmation dialogs (*dialogs asking for decision in situation that is not covered by a defined [Firewall](#) rule*) should be displayed.

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

- **Administrator** – controls the PC completely and has the right of assigning every user into groups with specifically defined authorities.
- **Administrator and Power User** – the administrator can assign any user into a specified group (*Power User*) and define authorities of the group members.
- **All Users** – other users not assigned into any specific group.

### 10.3. Areas and Adapters Profiles

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



- **Disable area detection and automatic profile switch (off by default)** - One of the defined profiles can be assigned to each network interface type, respectively to each area. If you do not wish to define specific profiles, one common profile will be used. However, if you decide to distinguish profiles and assign them to specific adapters and areas, and later on - for some reason - you want to switch this arrangement temporarily, tick the **Disable area detection and automatic profile switch** option.



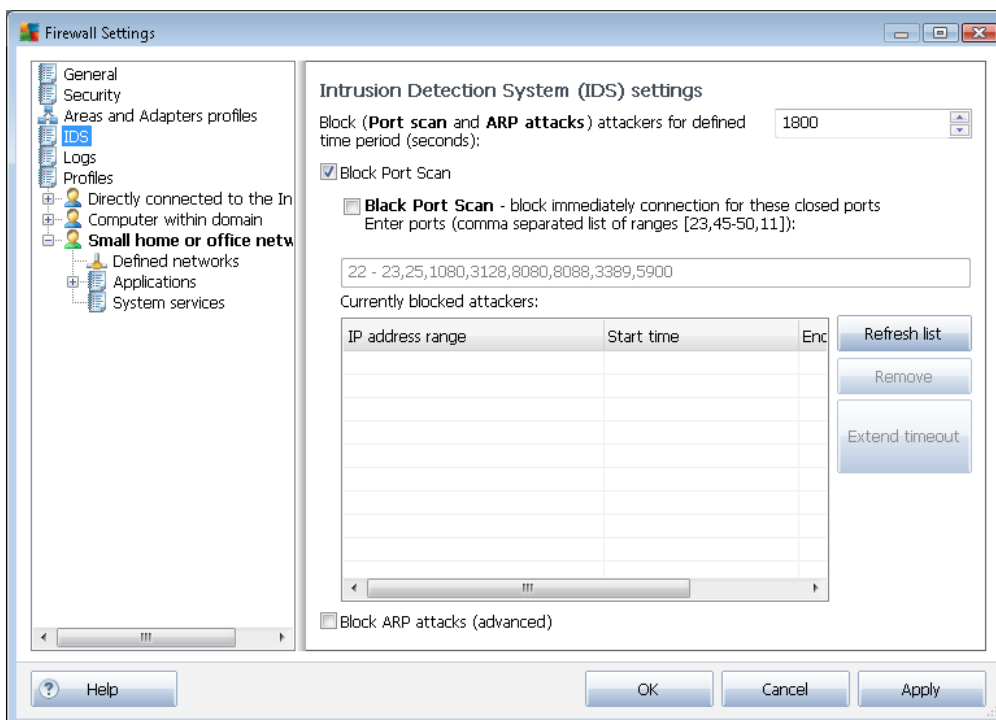
- **List of adapters, areas and assigned profiles** - In this list you can find an overview of detected adapters and areas. To each of them you can assign a specific profile from the menu of defined profiles. To open this menu, left-click the respective item in the list of adapters (*in the Assigned profile column*), and select the profile from the context menu.

## Advanced settings

- **Always use default profile and do not display new network detection dialog** - Whenever your computer connects to a new network, [Firewall](#) will alert you and display a dialog prompting you to select a type of network connection, and assign it a [Firewall profile](#). If you do not want the dialog to be displayed, check this box.
- **Use AVG heuristic for new networks detection** - Enables gathering information about a newly detected network with AVG's own mechanism (*however, this option is only available on VISTA OS, and higher*).
- **Use Microsoft heuristics for new networks detection** - Enables taking information about a newly detected network from the Windows service (*this option is only available on Windows Vista and higher*).

## 10.4. IDS

The Intrusion Detection System is a special behaviour analysis feature designed to identify and block suspicious communication attempts over specific ports of your computer. You can configure IDS parameters within the **Intrusion Detections System (IDS) settings** dialog:





The **Intrusion Detection System (IDS) settings** dialog offers these configuration options:

- **Block (Port scan and ARP attacks) attackers for defined time period** - Here you can specify for how many seconds should a port be blocked, whenever a suspicious communication attempt is detected on it. By default, the time interval is set to 1800 seconds (*30 minutes*).
- **Block Port Scan (on by default)** – Check the box to block communication attempts over all TCP and UDP ports coming to the computer from outside. For any such connection, five attempts are allowed, and the sixth is blocked. The item is turned on by default, and it is recommended to keep this settings. If you keep the **Block Port Scan** option on, some further detailed configuration is available (*otherwise, the following item will be deactivated*):
  - **Block Port Scan** – Check the box to immediately block any communication attempts over ports specified in the text field below. Individual ports or port ranges should be divided by commas. There is a predefined list of recommended ports should you wish to use this feature.
  - Currently blocked attackers - This section lists any communication attempts that are currently being blocked by the [Firewall](#). Complete history of blocked attempts can be viewed in the [Logs](#) dialog (*tab Port scan logs*).
- **Block ARP attacks (advanced) (off by default)** - Mark this option to activate blocking of special kinds of communication attempts inside a local network detected by **IDS** as potentially dangerous. The time set in **Block attackers for defined time period** applies. We recommend that only advanced users, familiar with the type and risk level of their local network, use this feature.

### Control buttons

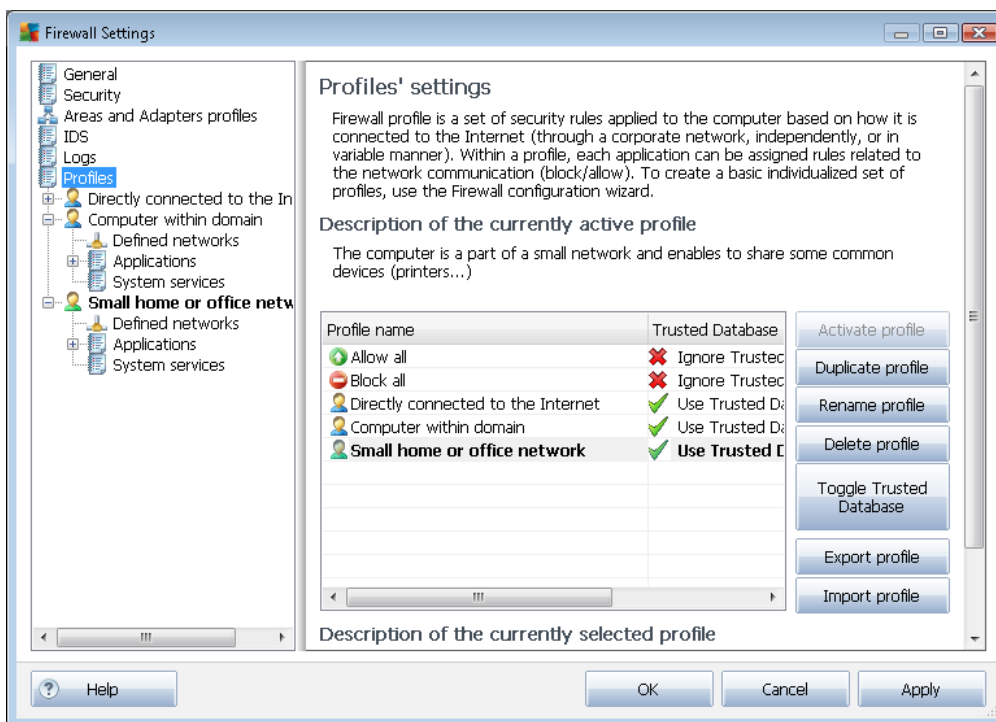
- **Refresh list** - press the button to update the list (*to include any latest blocked attempts*)
- **Remove** - press to cancel a selected blocking
- **Extend timeout** - press to prolong the time period for which a selected attempt is blocked. A new dialog with extended options will appear, allowing you to set specific time and date, or unlimited duration.



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

## 10.6. Profiles

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



System profiles (*Allow all*, *Block all*) cannot be edited. However, all custom [profiles](#) (*Directly connected to the Internet*, *Computer within domain*, *Small home or office network*) can then be edited right in this dialog using the following control buttons:

- **Activate profile** - This button sets the selected profile as active, which means the selected profile configuration will be used by [Firewall](#) to control the network traffic.
- **Duplicate profile** - Creates an identical copy of the selected profile; later you can edit and rename the copy to create a new profile based on the duplicated original one.
- **Rename profile** - Allows you to define a new name for a selected profile.
- **Delete profile** - Deletes the selected profile from the list.
- **Toggle Trusted Database** - For the selected profile you can decide to use the *Trusted Database* information (*Trusted Database is AVG internal database collecting data on trusted and certified applications that can always be allowed to communicate online.*).

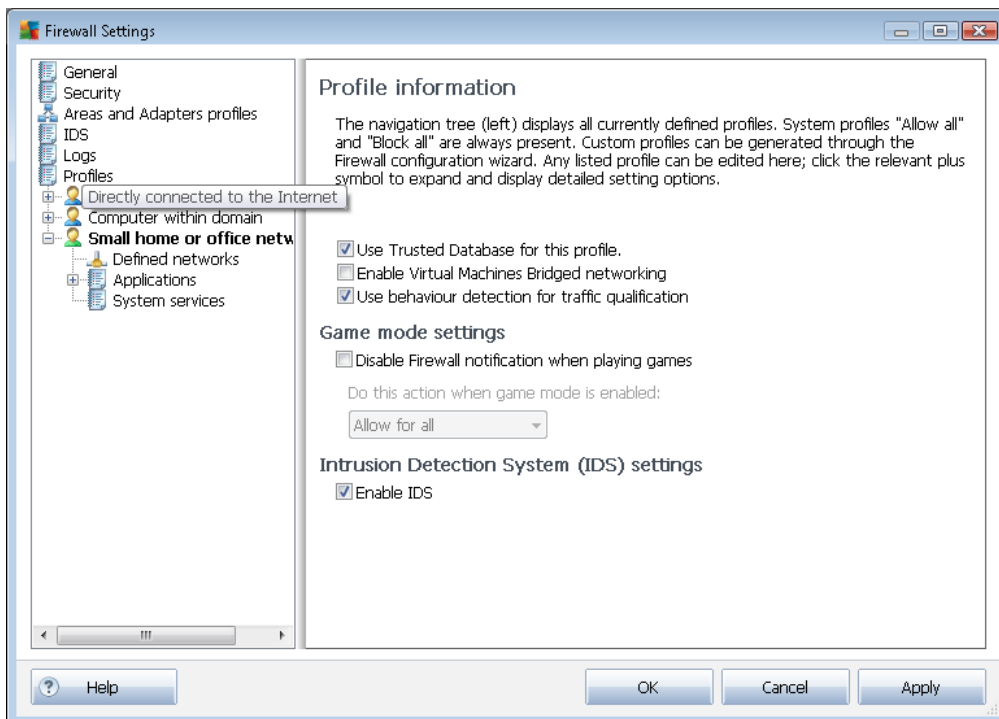


- **Export profile** - Records the selected profile's configuration into a file that will be saved for possible further use.
- **Import profile** - Configures the selected profile's settings based on the data exported from the backup configuration file.

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

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

### 10.6.1. Profile Information



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

- **Use Trusted Database for this profile (on by default)** - Mark the option to activate the *Trusted Database (i.e. AVG internal database collecting information on trusted and certified application communicating online. If there is no rule specified for the respective application yet, it is necessary to find out whether the application can be granted access to the network. AVG searched the Trusted Database first, and if the application is listed, it will be considered safe and will be allowed to communicate over network. Otherwise, you will be invited to decide whether the application should be allowed to communicate over network)* for the respective profile



- **Enable Virtual Machines Bridged networking** (*off by default*) - Tick this item to allow virtual machines in VMware to connect directly to the network.
- **Use behaviour detection for traffic qualification** (*on by default*) - Mark this option to allow [Firewall](#) to use [Identity Protection](#) functionality when evaluating an application - [Identity Protection](#) can tell whether the application shows any suspicious behaviour, or it can be trusted and allowed to communicate online.

### Game mode settings

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

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

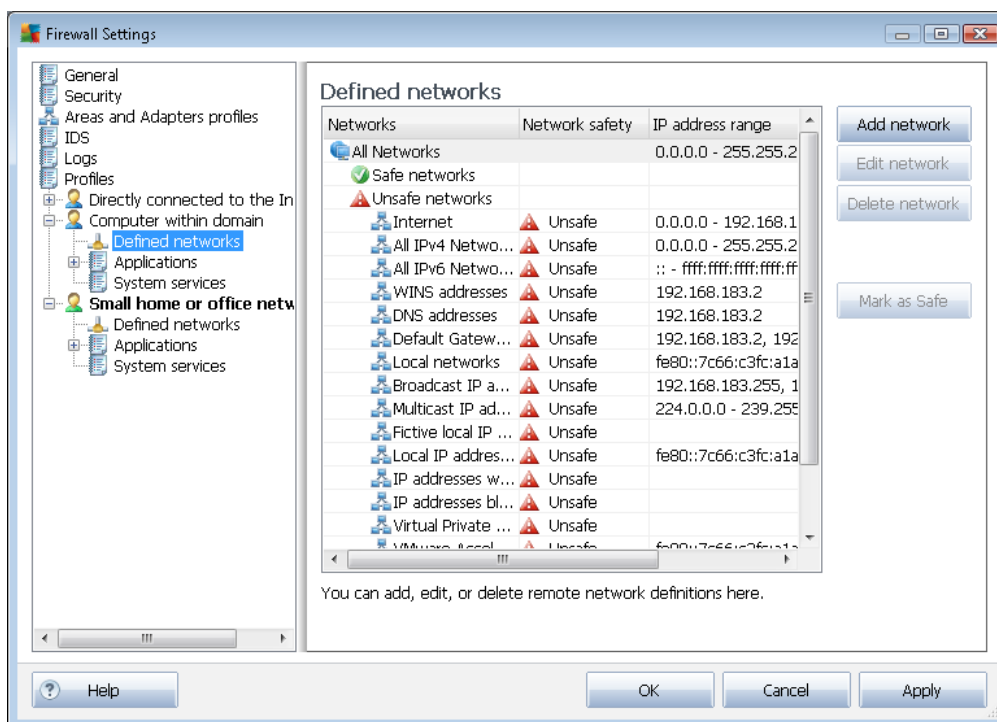
With the gaming mode on, all scheduled tasks (*scans, updates*) are postponed till the application is closed.

### Intrusion Detection System (IDS) settings

Mark the **Enable IDS** check box to activate special behaviour analysis feature designed to identify and block suspicious communication attempts over specific ports of your computer (*for details on this feature settings please consult the [IDS](#) chapter of this documentation*).

## 10.6.2. Defined Networks

The **Defined networks** dialog offers a list of all networks that your computer is connected to.

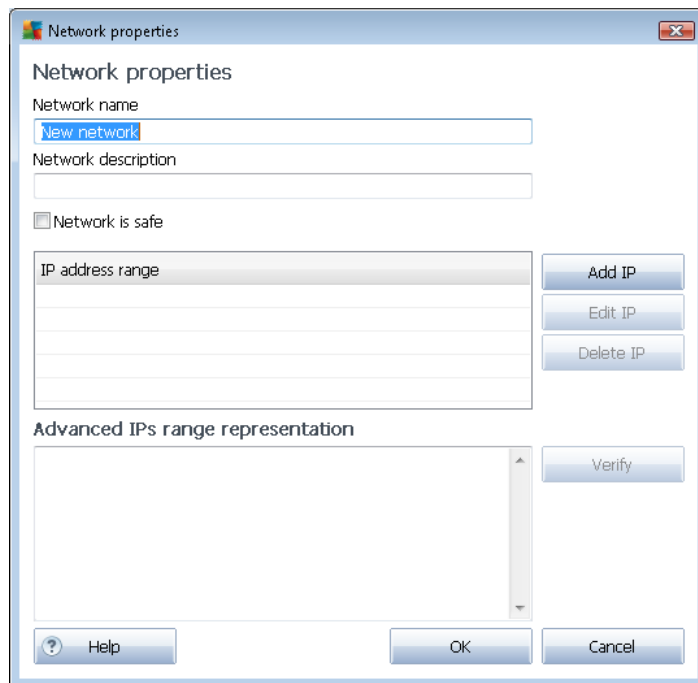


The list provides the following information on every detected network:

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

### Control buttons

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

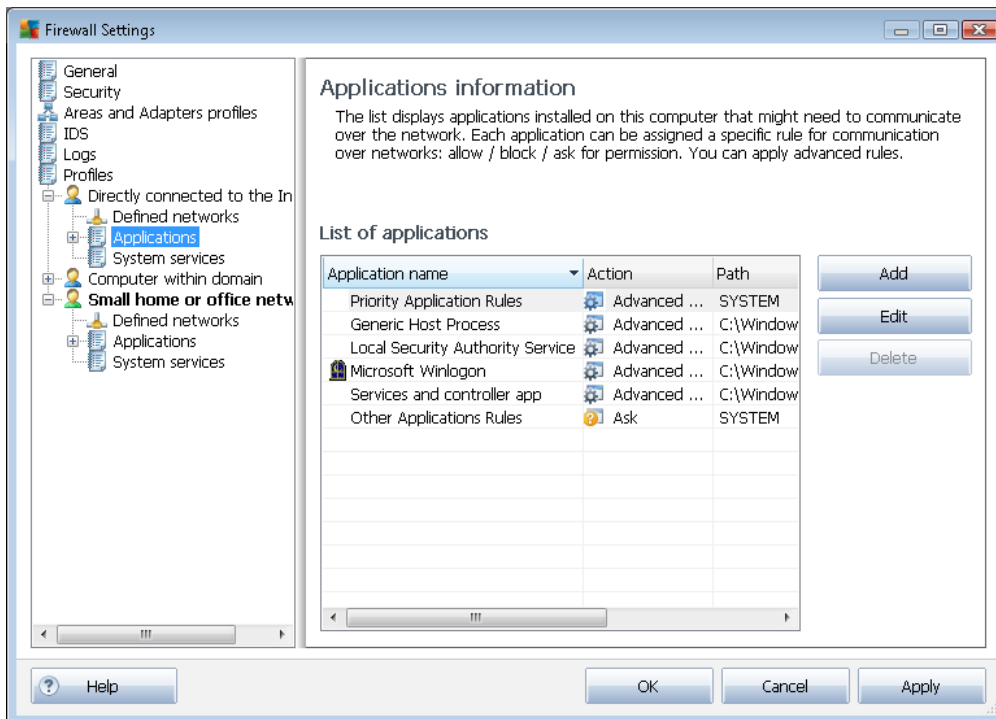


Within this dialog, you can specify the **Network name**, provide the **Network description** and possibly assign the network as safe. The new network can be either defined manually in a standalone dialog opened via the **Add IP** button (alternatively **Edit IP / Delete IP**), within this dialog you can specify the network by providing its IP range or mask. For large number of networks that should be defined as parts of the newly created network you can use the option of **Advance IP range representation**: enter the list of all networks into the respective text field (*any standard format is supported*) and press the **Verify** button to make sure the format can be recognized. Then press **OK** to confirm and save the data.






- **Edit network** - Opens the **Network properties** dialog window (see above) where you can edit parameters of an already defined network (*the dialog is identical with the dialog for adding new network, see the description in the previous paragraph*).
- **Delete network** - Removes the note of a selected network from the list of networks.
- **Mark as safe** - By default, all networks are considered unsafe, and only if you are sure the respective network is safe, you can use this button to assign it so (*and vice versa, once the network is assigned as safe, the button text changes to "Mark as unsafe"*).

### 10.6.3. Applications

The **Applications information** dialog lists all installed applications that might need to communicate over network, and icons for the assigned action:



The applications in the **List of applications** are those detected on your computer (and assigned respective actions). The following action types can be used:

-  - Allow communication for all networks
-  - Allow communication for networks defined as Safe only
-  - Block communication
-  - Display ask dialog (user will be able to decide whether they want to allow or block the communication when the application attempts to communicate over network)
-  - Advanced settings defined

**Please note that only application already installed could be detected, so if you install a new application later, you will have to define Firewall rules for it. By default, when the new application tries to connect over the network for the first time, the Firewall will either create a rule for it automatically according to the Trusted Database, or ask you whether you wish to allow or block the communication. In the latter case, you will be able to save your answer as a permanent rule (which will be then listed in this dialog).**

Of course, you can also define rules for the new application immediately – in this dialog, press **Add** and fill in the application details.



Apart from applications, the list also contains two special items:

- **Priority Application Rules** (*at the top of the list*) are preferential, and are always applied prior to rules of any individual application.
- **Other Applications Rules** (*at the bottom of the list*) are used as a "last instance", when no specific application rules apply, e.g. for an unknown and undefined application. Select action that should be triggered when such application attempts to communicate over network:
  - *Block* – communication will be always blocked.
  - *Allow* – communication will be allowed over any network.
  - *Ask* – you will be invited to decide whether the communication should be allowed, or blocked.

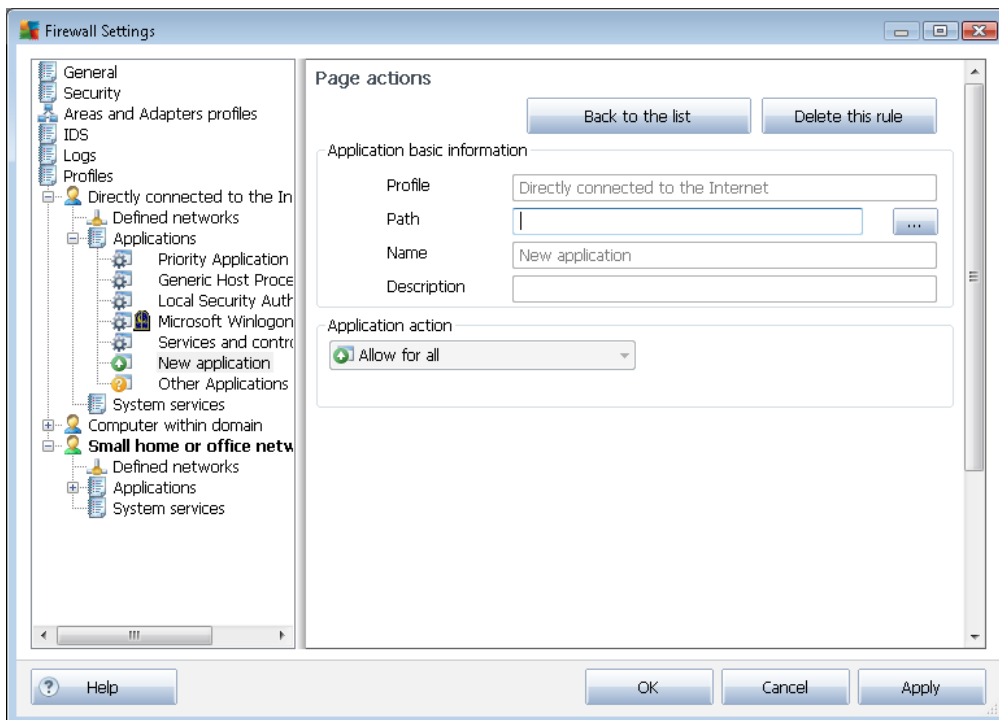
***These items have different setting options from common applications, and are only intended for experienced users. We strongly recommend that you do not modify the settings!***

### **Control buttons**

The list can be edited using the following control buttons:

- **Add** - Opens an empty [Page Actions](#) dialog for defining new application rules.
- **Edit** - Opens the same [Page Actions](#) dialog with data provided for editing of an existing application's rule set.
- **Delete** - Removes the selected application from the list.

In the **Page actions** dialog, you can define settings for the respective application in detail:



### Control buttons

Two control buttons are available at the top of the dialog:

- **Back to the list** - Press the button to display the overview of all defined applications rules.
- **Delete this rule** - Press the button to erase the currently displayed application rule. **Please note that this action cannot be reversed!**

### Application basic information

In this section, fill in the **Name** of the application, and optionally a **Description** (a brief comment for your information). In the **Path** field, enter the full path to the application (the executable file) on the disk; alternatively, you can locate the application in the tree structure conveniently after pressing the "..." button.

### Application action

In the drop-down menu, you can select the [Firewall](#) rule for the application, i.e. what the [Firewall](#) should do when the application tries to communicate over the network:

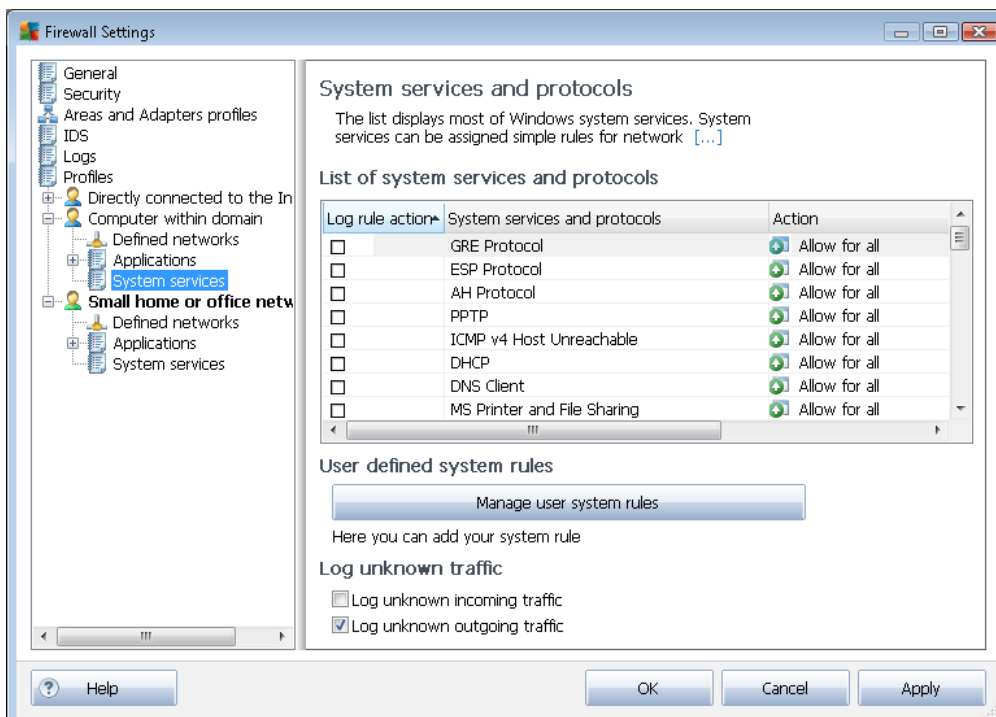


- **Allow for all** - Allows the application to communicate over all defined networks and adapters without limitations.
- **Allow for safe** - Only allows the application to communicate over networks defined as safe (*trustworthy*).
- **Block** - Forbids the communication automatically; the application will not be allowed to connect to any network.
- **Ask** - Displays a dialog enabling you to decide whether you want to allow or block the communication attempt at that moment.
- **Advanced settings** - Displays further extensive and detailed setting options in the bottom part of the dialog in the **Application detail rules** section. The details will be applied according to the list order, so you can **Move up** or **Move down** the rules in the list as required to set their precedence. After clicking a specific rule in the list, the overview of the rule details will be displayed in the bottom part of the dialog. Any blue underlined value can be changed upon clicking in the respective settings dialog. To delete the highlighted rule, simply press **Remove**. To define a new rule, use the **Add** button to open the **Change rule detail** dialog allowing you to specify all necessary details.

#### 10.6.4. System Services

**Any editing within the System services and protocols dialog is intended for EXPERIENCED USERS ONLY!**




The **System services and protocols** dialog lists Windows standard system services and protocols that might need to communicate over the network:





### List of system services and protocols

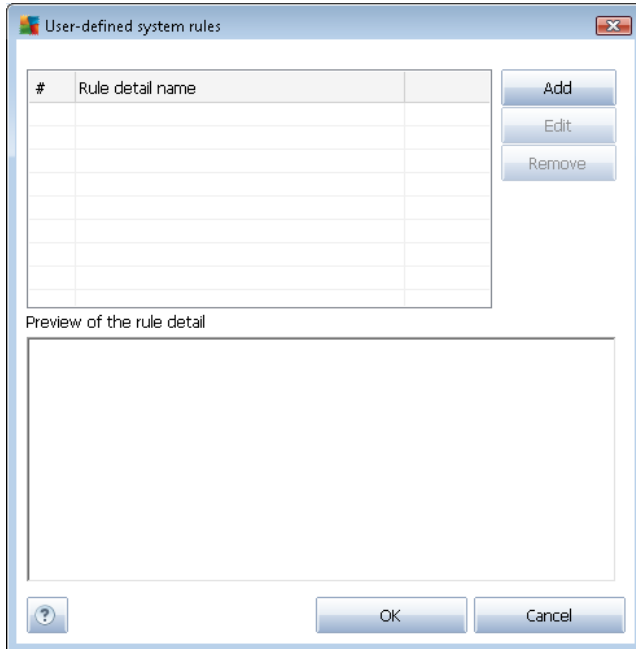
The chart consists of the following columns:

- **Log rule action** - This box enables you to switch on recording each rule application in the [logs](#).
- **System service and protocols** - This column shows a name of the respective system service.
- **Action** - This column displays an icon for the assigned action:
  -  Allow communication for all networks
  -  Allow communication for networks defined as Safe only
  -  Block communication
- **Networks** - This column states on which specific network the system rule applies.

To edit settings of any item in the list (*including the assigned actions*), right-click the item and select **Edit**. **However, editing of system rules should be performed by advanced users only, and it is strongly recommended not to edit system rules!**

### User defined system rules

To open a new dialog for defining your own system service rule (*see picture below*), press the **Manage user system rules** button. The top section of the **User-defined system rules** dialog displays overview of all details of the currently edited system rule, the bottom section then displays the selected detail. User-defined rule details can be edited, added, or deleted by the respective button; manufacturer-defined rule details can only be edited:



***Please mind that detail rule settings are advanced, primarily intended for network administrators who need full control over Firewall configuration. If you are not familiar with types of communication protocols, network port numbers, IP address definitions etc., please do not modify these settings! If you really need to change the configuration, please consult the respective dialog help files for specific details.***

### **Log unknown traffic**

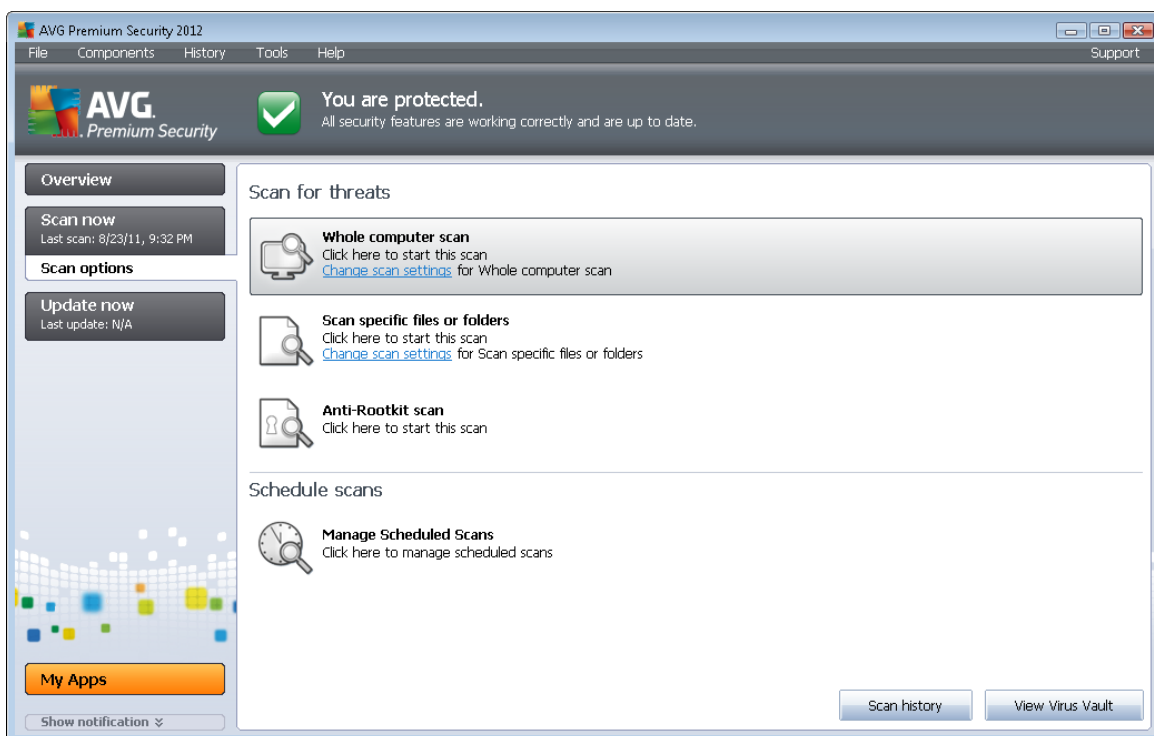
- **Log unknown incoming traffic** (off by default) – Check the box to record in the [Logs](#) every unknown attempt to connect to your computer from outside.
- **Log unknown outgoing traffic** (on by default) – Check the box to record in the [Logs](#) every unknown attempt from your computer to connect to an outside location.



## 11. AVG Scanning

By default, **AVG Premium Security 2012** does not run any scans, as after the initial one, you should be perfectly protected by the resident components of **AVG Premium Security 2012** that are always on guard, and do not let any malicious code get into your computer at all. Of course, you can [schedule a scan](#) to run at regular intervals, or manually launch a scan according to your needs any time.

### 11.1. Scanning Interface



The AVG scanning interface is accessible via the **Scan options** [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:
  - [Whole computer scan](#)
  - [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 Premium Security 2012** 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.

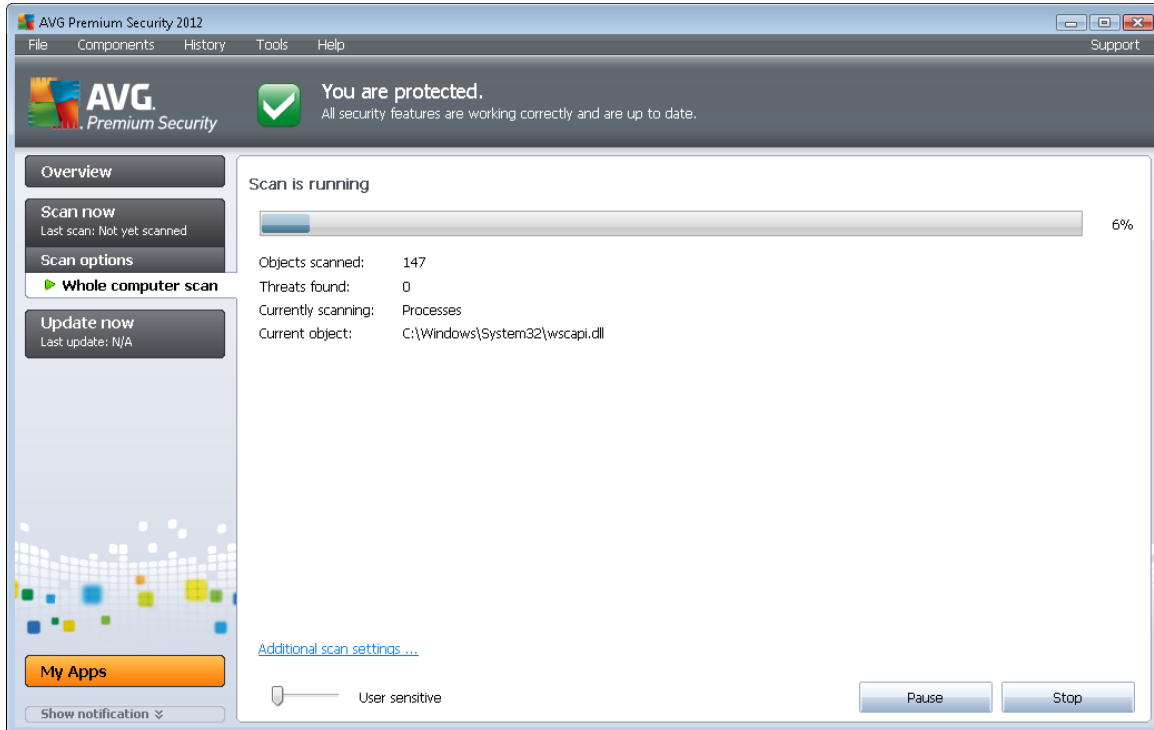
In the **AVG Premium Security 2012** you will find the following types of scanning predefined by the software vendor:

### 11.2.1. Whole Computer Scan

**Whole Computer scan** - 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.

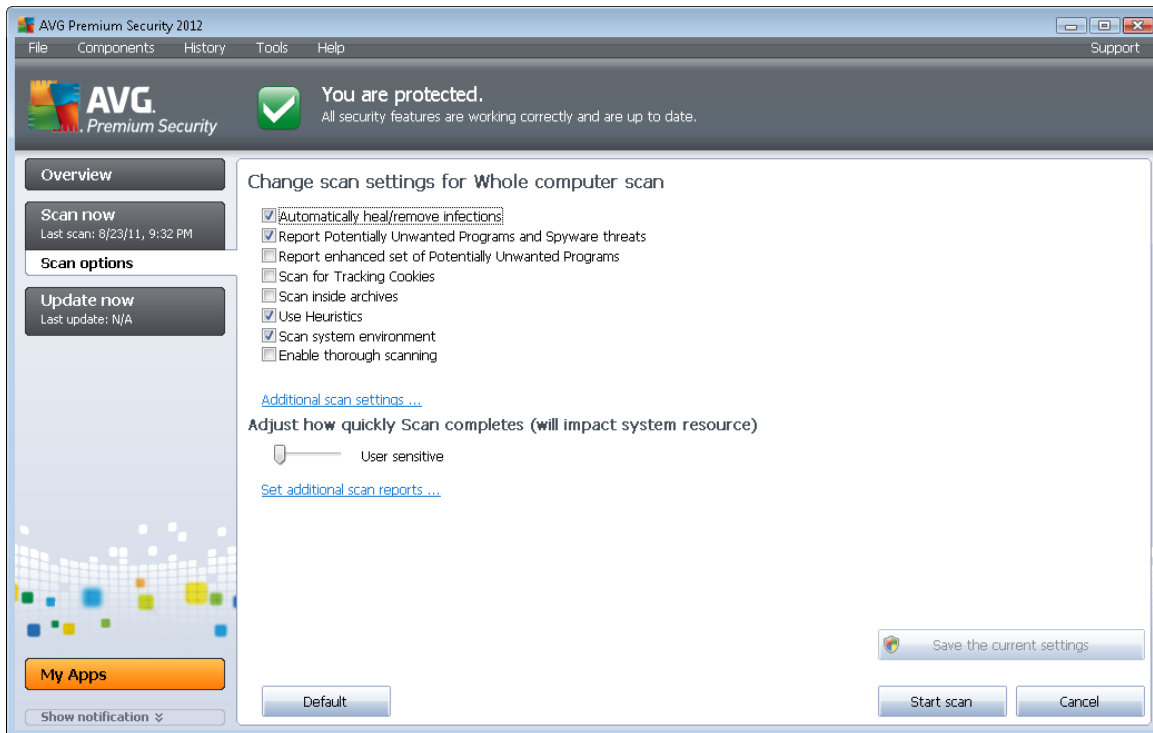
#### Scan launch

The **Whole Computer scan** 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.



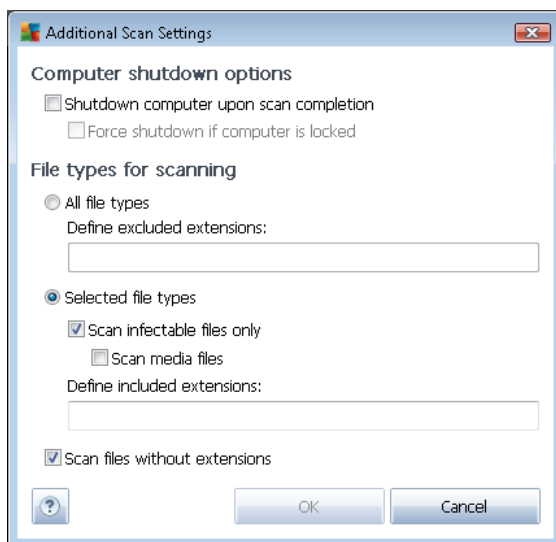
## Scan configuration editing

You have the option of editing the predefined default settings of the **Whole computer scan**. Press the **Change scan settings** link to get to the **Change scan settings for Whole Computer scan** dialog (accessible from the [scanning interface](#) via the Change scan settings link for the [Whole computer scan](#)). **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:
  - **Automatically heal/remove infection** (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, the infected object will be moved to the [Virus Vault](#).
  - **Report Potentially Unwanted Programs and Spyware threats** (on by default) - check to activate the [Anti-Spyware](#) engine, and scan for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend to keep this feature activated as it increases your computer security.
  - **Report enhanced set of Potentially Unwanted Programs** (off by default) - mark to detect extended package of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it can possibly block legal programs, and is therefore switched off by default.
  - **Scan for Tracking Cookies** (off by default) - 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** (off by default) - this parameters defines that scanning should check all files stored inside archives, e.g. ZIP, RAR, ...

- **Use Heuristics** (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** (on by default) - scanning will also check the system areas of your computer.
  - **Enable thorough scanning** (off by default) - in specific situations (*suspicious of your computer being infected*) you may check this option to activate the most thorough scanning algorithms that will scan even those areas of your computer that can hardly get infected, just to be absolutely sure. Remember though that this method is rather time consuming.
- **Additional scan settings** - the link opens a new **Additional scan settings** dialog where you can specify the following parameters:

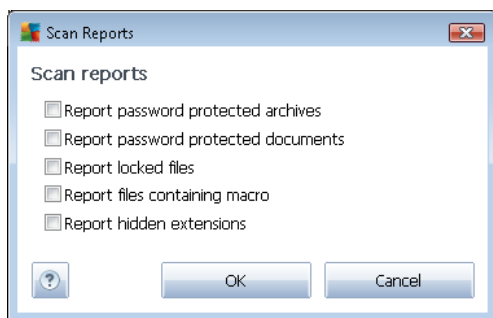


- **Computer shutdown options** - decide whether the computer should be shut down automatically once the running scanning process is over. Having confirmed this option (**Shutdown computer upon scan completion**), a new option activates that allows the computer to shut down even if it is currently locked (**Force shutdown if computer is locked**).
- **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;
  - **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.
- **Adjust how quickly Scan completes** - you can use the slider to change the scanning process priority. By default, this option value is set to *user sensitive* level of automatic resource usage. 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.

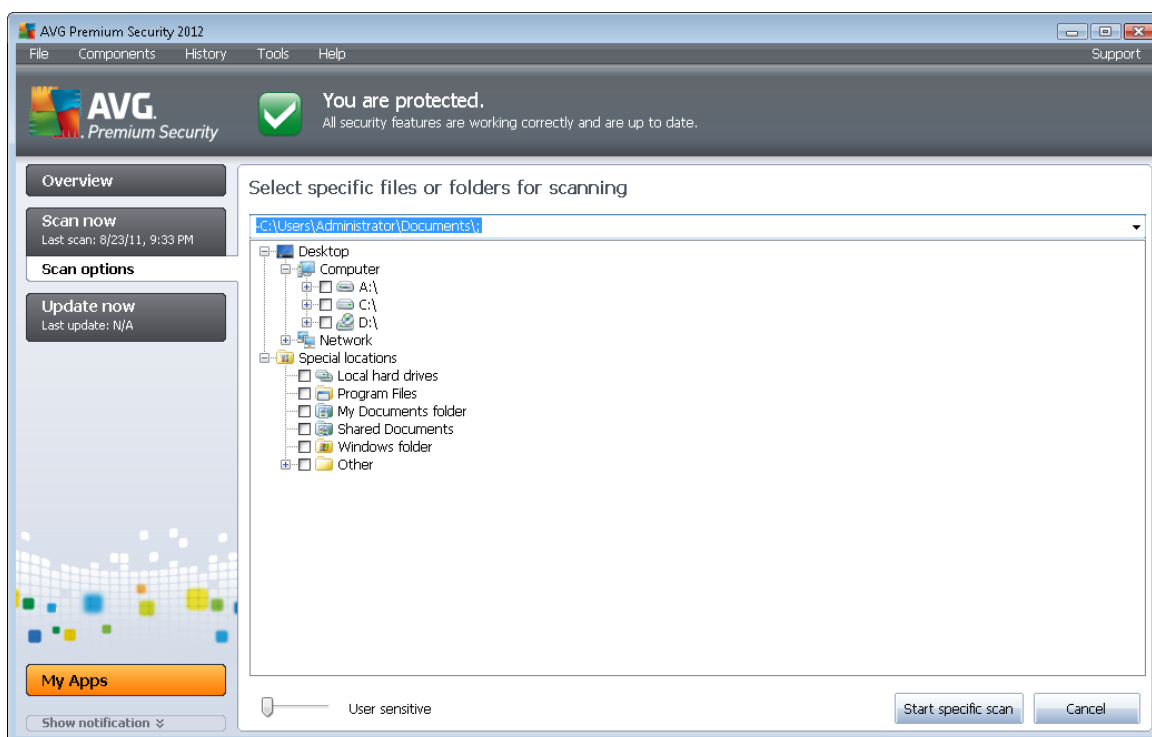
#### Scan launch

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.



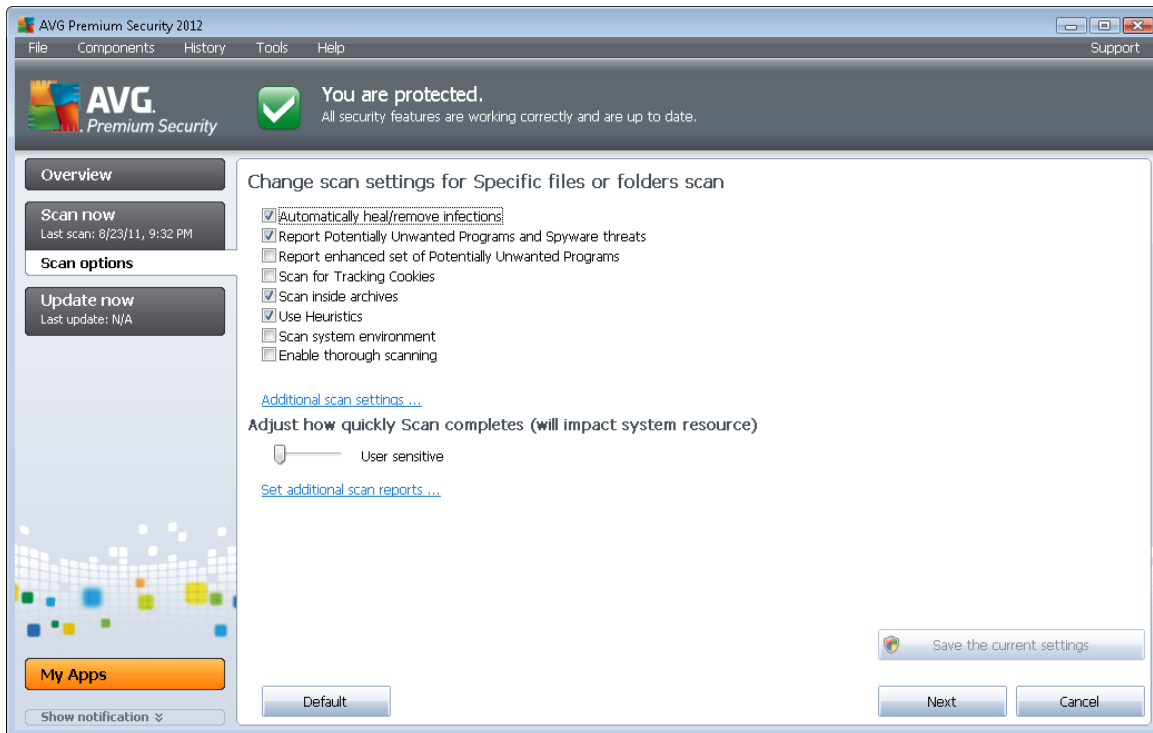
There is also a possibility of having a specific folder scanned while all its subfolders are excluded from this scanning; to do that write a minus sign "-" in front of the automatically generated path (see [screenshot](#)). To exclude the entire folder from scanning use the "!" parameter.

Finally, to launch the scanning, press the **Start scan** button; the scanning process itself is basically identical to the [Whole computer scan](#).



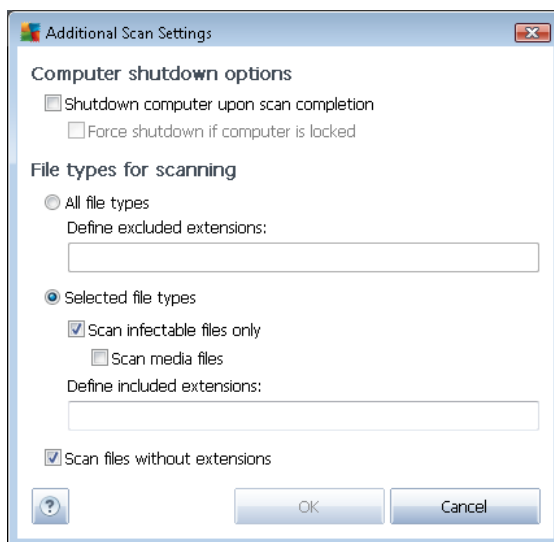
### Scan configuration editing

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:
  - **Automatically heal/remove infection** (*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, the infected object will be moved to the [Virus Vault](#).
  - **Report Potentially Unwanted Programs and Spyware threats** (*on by default*) - check to activate the [Anti-Spyware](#) engine, and scan for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend to keep this feature activated as it increases your computer security.
  - **Report enhanced set of Potentially Unwanted Programs** (*off by default*) - mark to detect extended package of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it can possibly block legal programs, and is therefore switched off by default.
  - **Scan for Tracking Cookies** (*off by default*) - 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** (*on by default*) - this parameters defines that scanning should check all files stored inside archives, e.g. ZIP, RAR, ...

- **Use Heuristics** (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** (off by default) - scanning will also check the system areas of your computer.
  - **Enable thorough scanning** (off by default) - in specific situations (*suspicious of your computer being infected*) you may check this option to activate the most thorough scanning algorithms that will scan even those areas of your computer that can hardly get infected, just to be absolutely sure. Remember though that this method is rather time consuming.
- **Additional scan settings** - the link opens a new **Additional scan settings** dialog where you can specify the following parameters:

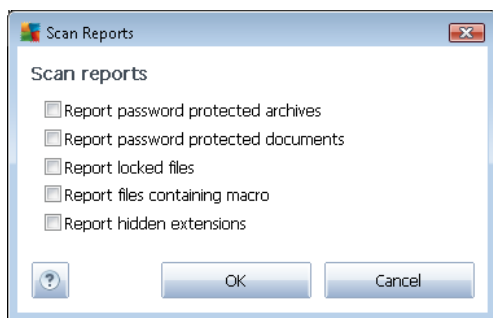


- **Computer shutdown options** - decide whether the computer should be shut down automatically once the running scanning process is over. Having confirmed this option (**Shutdown computer upon scan completion**), a new option activates that allows the computer to shut down even if it is currently locked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



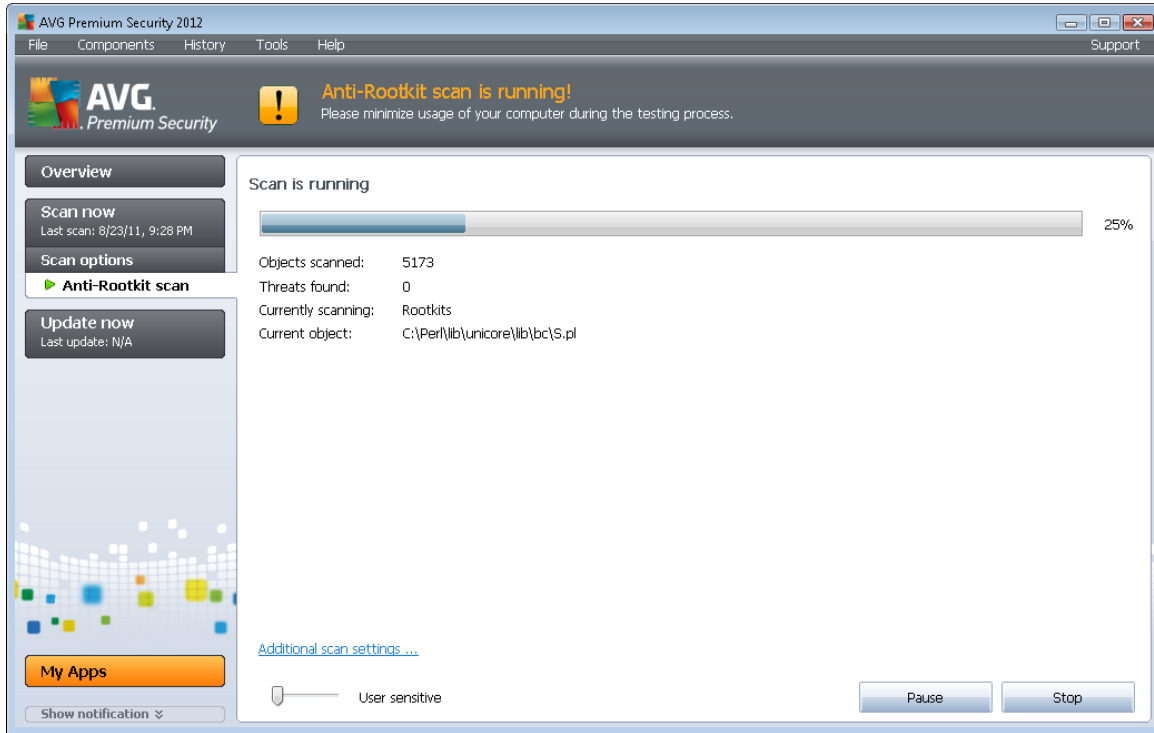
**Warning:** These scan settings are identical to the parameters of a newly defined scan - as described in the chapter [AVG Scanning / Scan scheduling/ How to Scan](#). Should you decide to change the default configuration of the **Scan specific files or folders** you can then save your new setting as 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](#)).

### 11.2.3. Anti-Rootkit Scan

**Anti-Rootkit scan** searches your computer for possible rootkit (*programs and technologies that can cover malware activity in your computer*). If a rootkit is detected, this does not necessarily mean your computer is infected. In some cases, specific drivers or sections of regular applications may be misleadingly detected as rootkits.

#### Scan launch

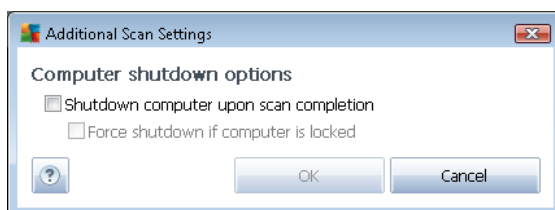
**Anti-Rootkit scan** can be launched directly from the [scanning interface](#) by clicking on the scan's icon. No further specific settings have to be configured for this type of scan, the scanning will start immediately within the **Scan is running** dialog (see *screenshot*). The scanning can be temporarily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



## Scan configuration editing

**Anti-Rootkit scan** is always launched in the default settings, and editing of the scan parameters is only accessible within the [AVG Advanced Settings / Anti-Rootkit](#) dialog. In the scanning interface, the following configuration is available but only while the scan is running:

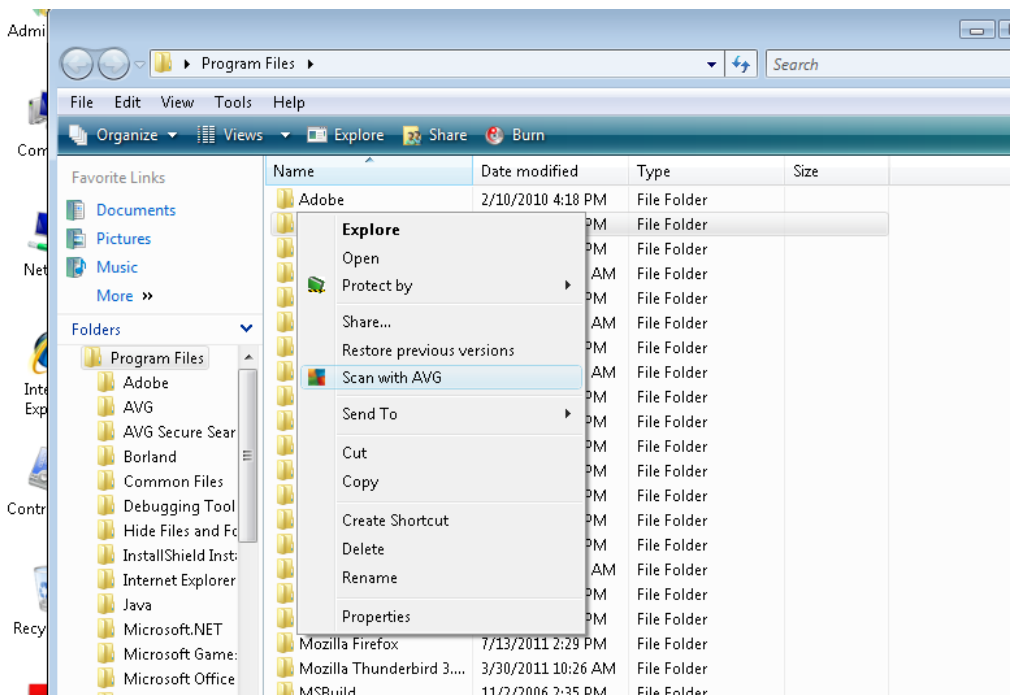
- **Automatic scan** - you can use the slider to change the scanning process priority. By default, this option value is set to *user sensitive* level of automatic resource usage. Alternatively, you can run the scanning process slower which means the system resources load will be minimized (*useful when 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*).
- **Additional scan settings** - this link opens a new **Additional scan settings** dialog where you can define possible computer shutdown conditions related to the **Anti-Rootkit scan** (**Shutdown computer upon scan completion, possibly Force shutdown if computer is locked**):





### 11.3. Scanning in Windows Explorer

Besides the pre-defined scans launched for the entire computer or its selected areas, **AVG Premium Security 2012** 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 Premium Security 2012**

### 11.4. Command Line Scanning

Within **AVG Premium Security 2012** 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 semicolons, 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** [Whole Computer scan](#)
- **/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
- **/LOG** Generate a scan result file
- **/MACROW** Report macros
- **/PWDW** Report password-protected files
- **/ARCBOMBSW** Report archive bombs (*repeatedly compressed archives*)
- **/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](#)
- **/PUPEXT** Report enhanced set of [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



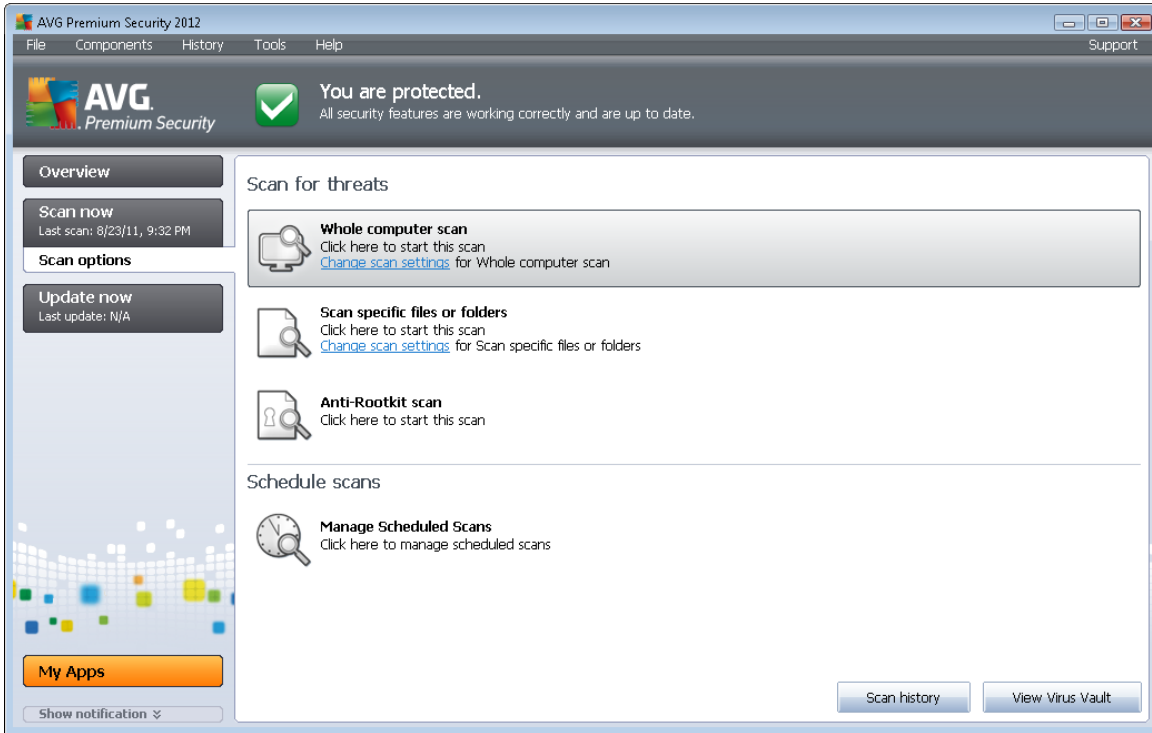
- **/FORCESHUTDOWN** Force computer shutdown upon scan completion
- **/ADS** Scan Alternate Data Streams (*NTFS only*)
- **/HIDDEN** Report files with hidden extension
- **/INFECTABLEONLY** Scan files with infectable extensions only
- **/THOROUGHSCAN** Enable thorough scanning
- **/CLOUDCHECK** Check for false positives
- **/ARCBOMBSW** Report re-compressed archive files

### 11.5. Scan Scheduling

With **AVG Premium Security 2012** 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.

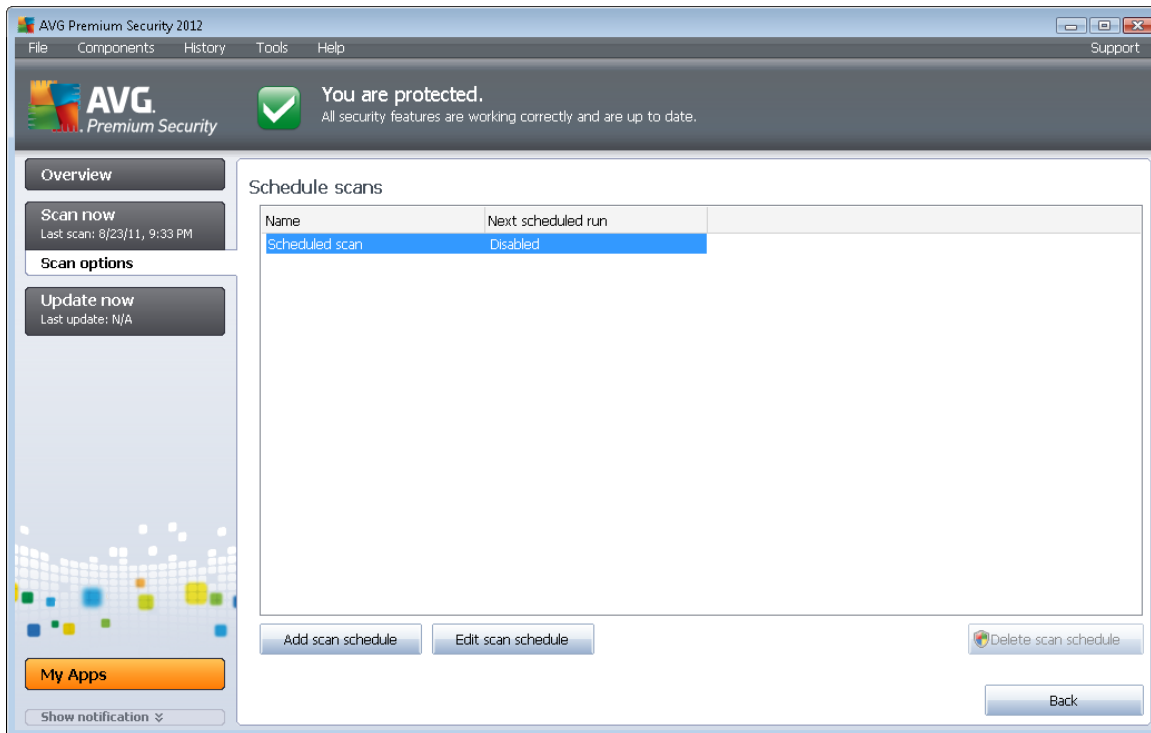
You should launch the [Whole Computer scan](#) regularly, at least once a week. However, if possible, launch the scan of your entire computer daily - as set up in the scan schedule default configuration. If the computer is "always on" then you can schedule scans out of working hours. If the computer 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:

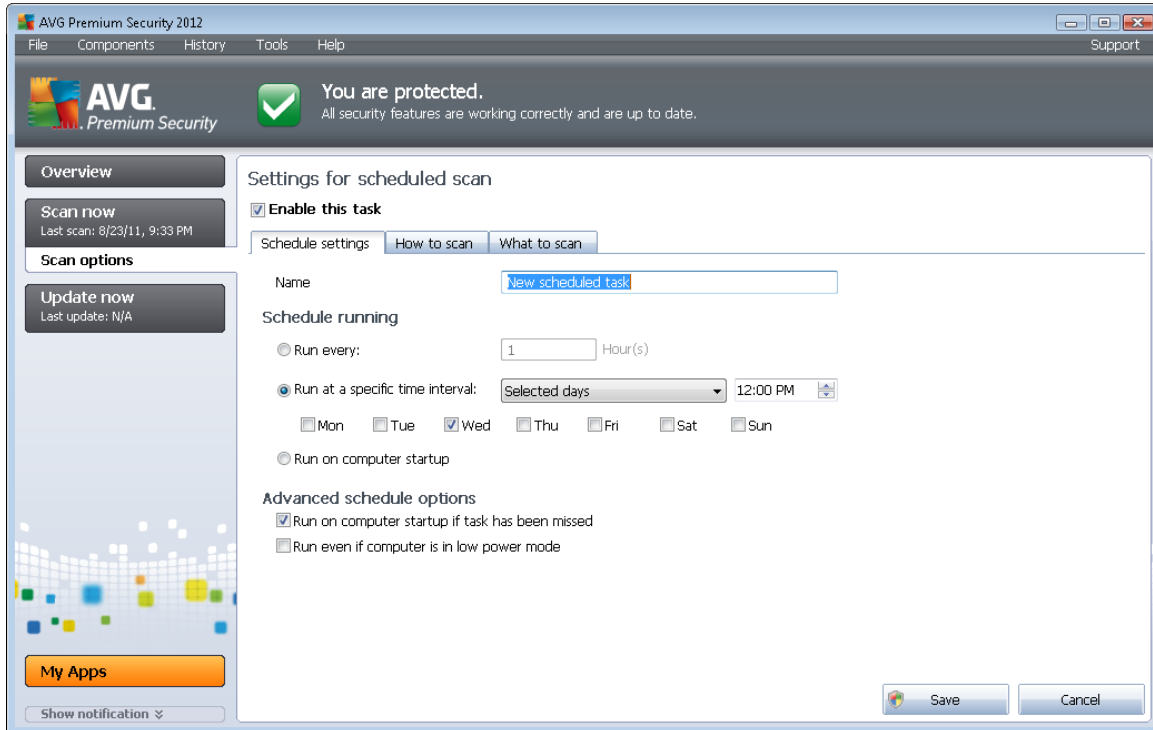


You can edit / add scans using the following control buttons:

- **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.

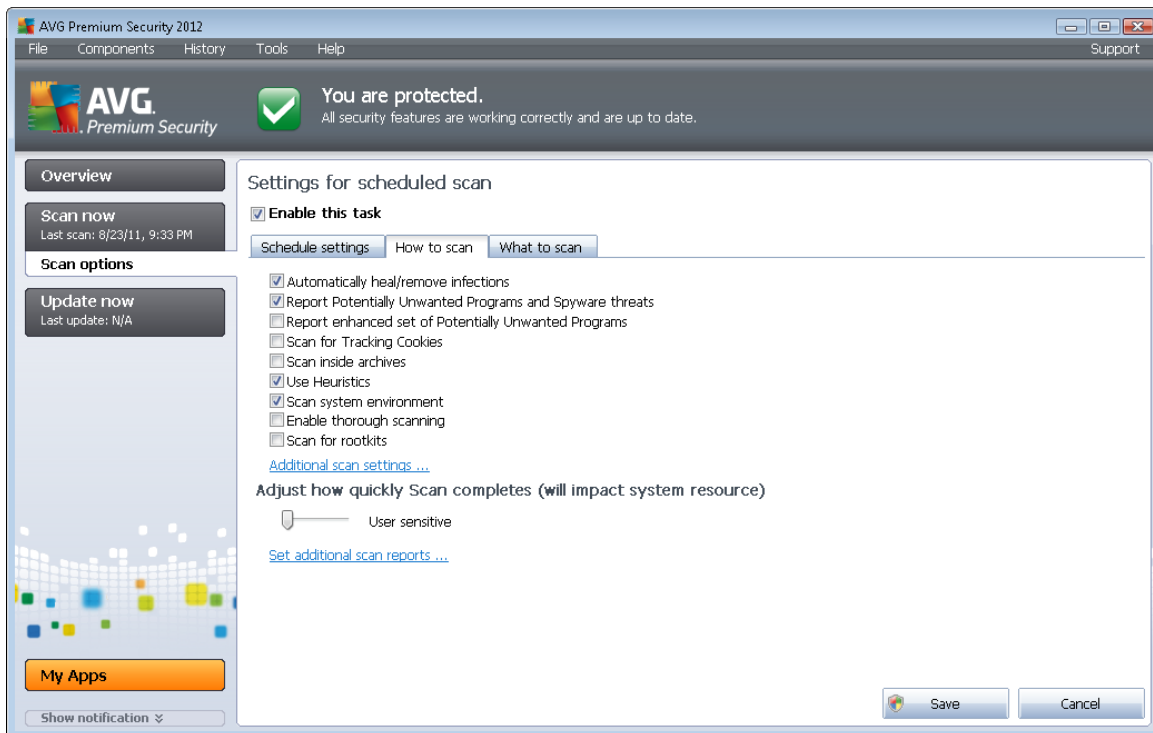
### Control buttons of the Settings for scheduled scan dialog



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 (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 (on by default)**: check to activate the [Anti-Spyware](#) engine, and scan for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security

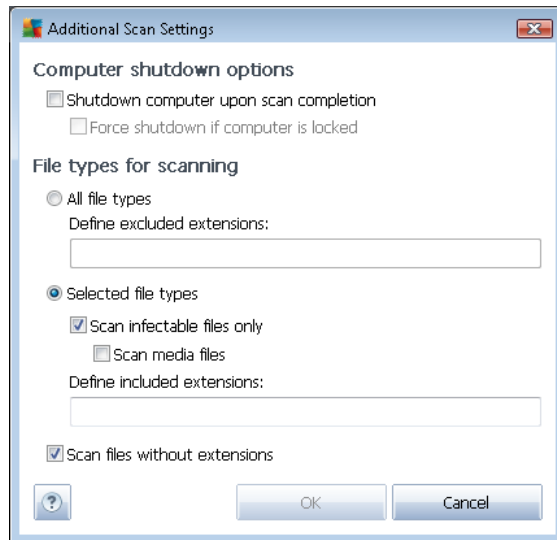


risk, some of these programs can be installed intentionally. We recommend to keep this feature activated as it increases your computer security.

- **Report enhanced set of Potentially Unwanted Programs** (*off by default*): mark to detect extended package of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it can possibly block legal programs, and is therefore switched off by default.
- **Scan for Tracking Cookies** (*off 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** (*off 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** (*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** (*on by default*): scanning will also check the system areas of your computer.
- **Enable thorough scanning** (*off by default*) - in specific situations (*suspicious of your computer being infected*) you may check this option to activate the most thorough scanning algorithms that will scan even those areas of your computer that can hardly get infected, just to be absolutely sure. Remember though that this method is rather time consuming.
- **Scan for rootkits** (*off by default*): 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:

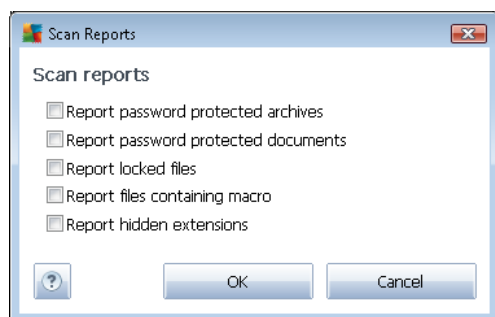
- **Additional scan settings** - the link opens a new **Additional scan settings** dialog where you can specify the following parameters:



- **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 if computer is locked**).
- **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;
  - **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.
- **Adjust how quickly Scan completes** - you can use the slider to change the scanning process priority. By default, this option value is set to *user sensitive* level of automatic resource usage. 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:

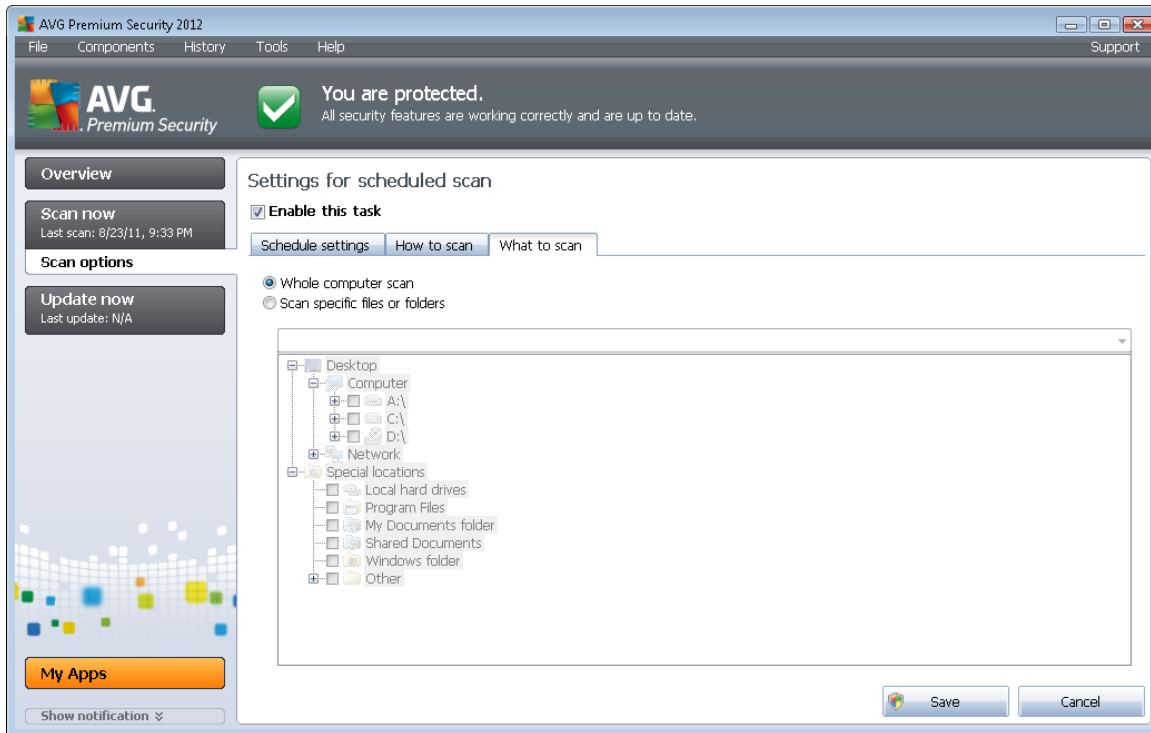


### Control buttons

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 (*expand items by clicking the plus node until you find the folder you wish to scan*). You can select multiple folders by checking the respective boxes. The selected folders will appear in the text field on the top of the dialog, and the drop-down menu will keep your selected scans history for later use. Alternatively, you can enter full path to the desired folder manually (*if you enter multiple paths, it is necessary to separate with semi-colons without extra space*).

Within the tree structure you can also see a branch called **Special locations**. Following find a list of locations that will be scanned once the respective check box is marked:

- **Local hard drives** - all hard drives of your computer
- **Program files**
  - C:\Program Files\
  - in 64-bit version C:\Program Files (x86)
- **My Documents folder**



- for Win XP: C:\Documents and Settings\Default User\My Documents\
- for Windows Vista/7: C:\Users\user\Documents\

- **Shared Documents**

- for Win XP: C:\Documents and Settings\All Users\Documents\
- for Windows Vista/7: C:\Users\Public\Documents\

- **Windows folder** - C:\Windows\

- **Other**

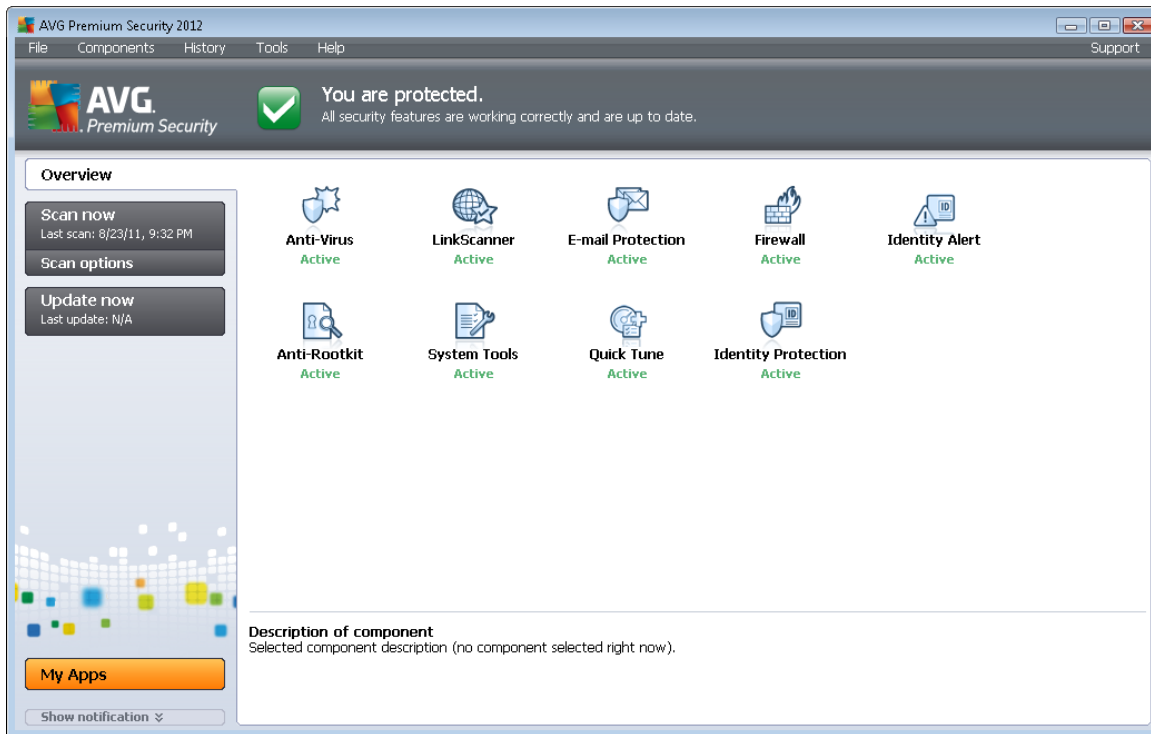
- *System drive* - the hard drive on which the operating system is installed (usually C:)
- *System folder* - C:\Windows\System32\
- *Temporary Files folder* - C:\Documents and Settings\User\Local\ (Windows XP); or C:\Users\user\AppData\Local\Temp\ (Windows Vista/7)
- *Temporary Internet Files* - C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (Windows XP); or C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (Windows Vista/7)

## Control buttons

The same two control buttons are available on all three tabs of the **Settings for scheduled scan** dialog ([Schedule settings](#), [How to scan](#), and [What to scan](#)):


- **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 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
- **Warnings** - number of detected [suspicious objects](#)
- **Rootkits** - number of detected [rootkits](#)
- **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:

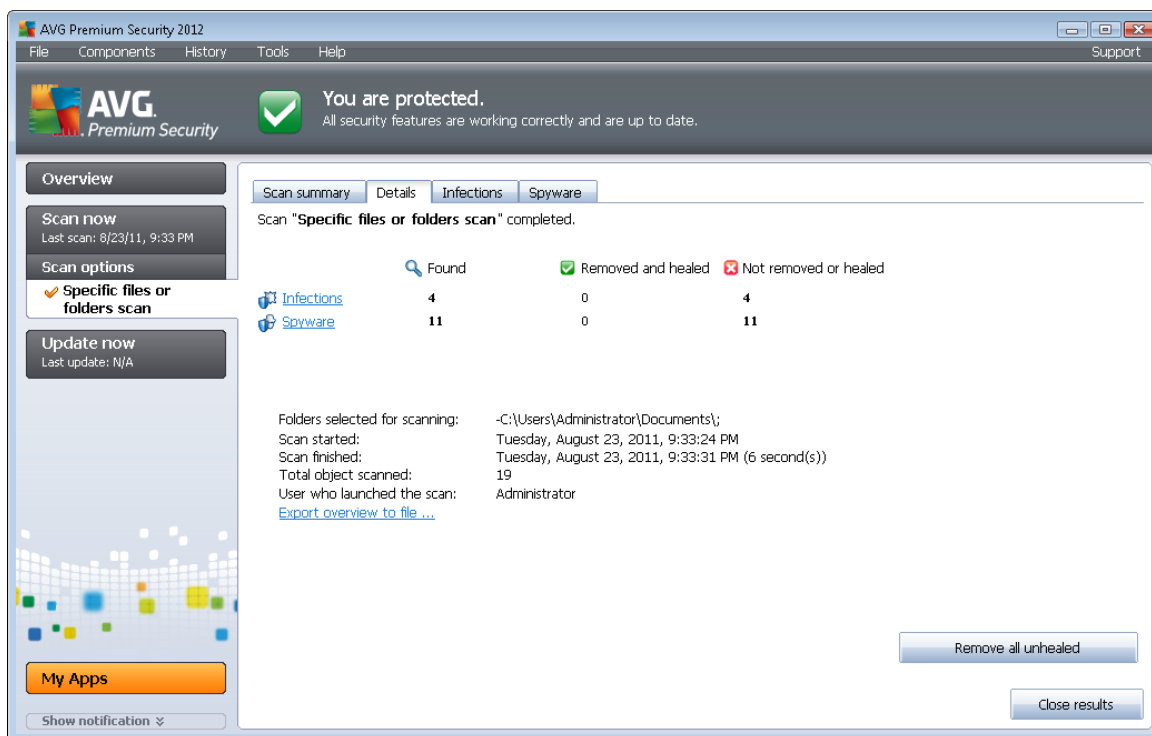
- **View details** - press it to switch to the [Scan results](#) dialog to view detailed data on the selected scan
- **Delete result** - press it to remove the selected item from the scan results overview
- **Back** - switches back to the default dialog of the [AVG scanning interface](#)

## 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 for instance if cookies 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. Also, you will find here information on objects that could not be scanned (e.g. *password protected archives*).

### 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

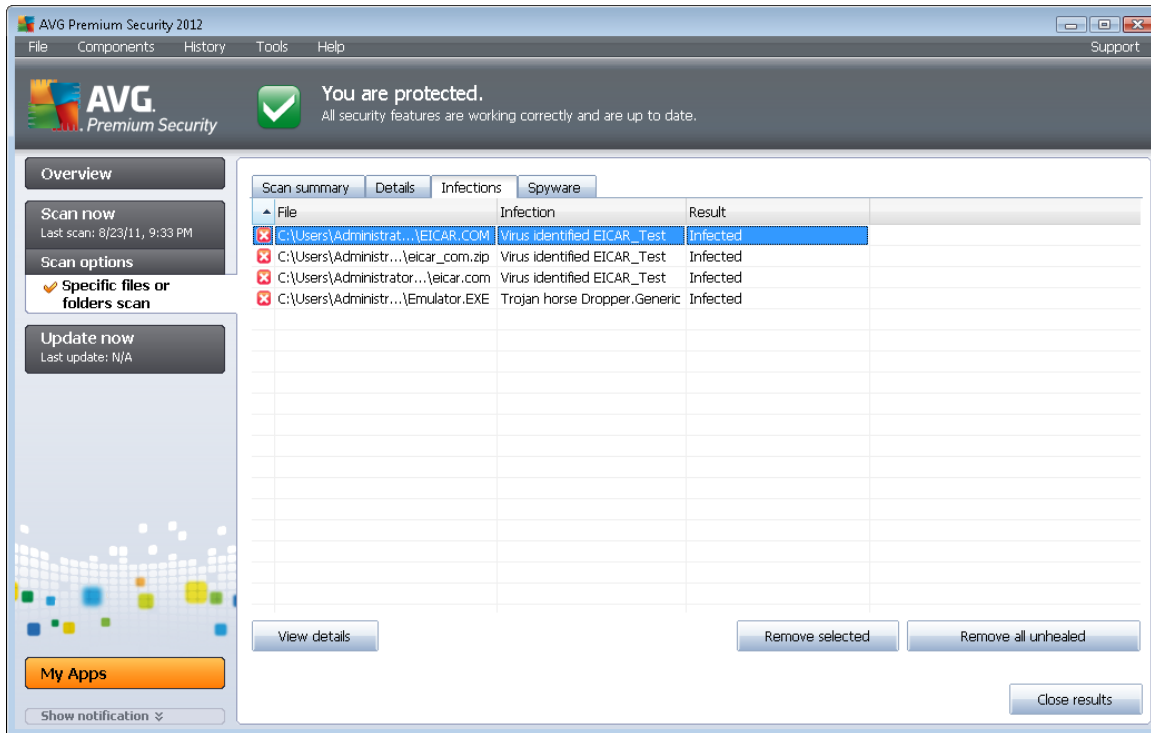
In addition you will find information on the date and exact time of the scan launch, on the total number of scanned objects, on the scanning duration and the number of errors that have occurred during scanning.

#### 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

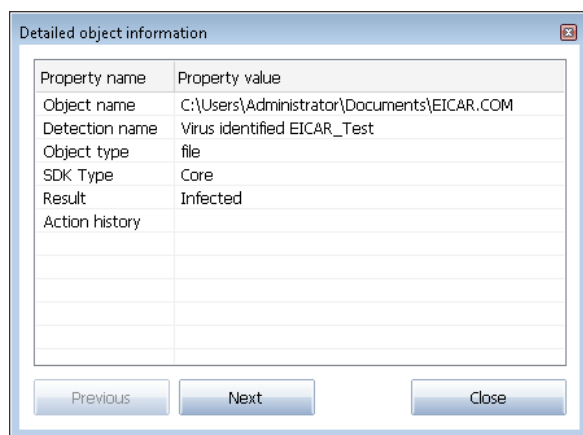
unable to scan it

- **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 object information**:

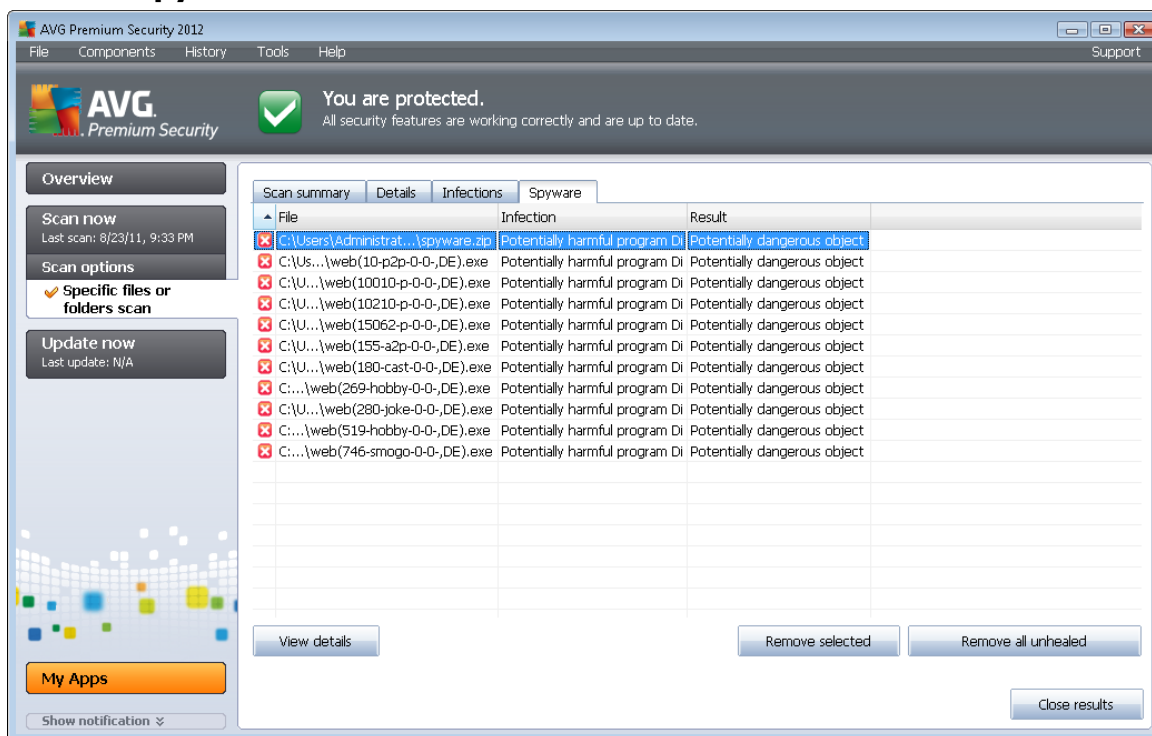


In this dialog you can find detailed information on the detected infectious object (e.g. *infected object name and location, object type, SDK type, detection result and history of actions related to the detected object*). Using the **Previous / Next** buttons you can view information on specific findings. Use the **Close** button to close this dialog.

- **Remove selected** - use the button to move the selected finding to the [Virus Vault](#)
- **Remove all unhealed** - 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

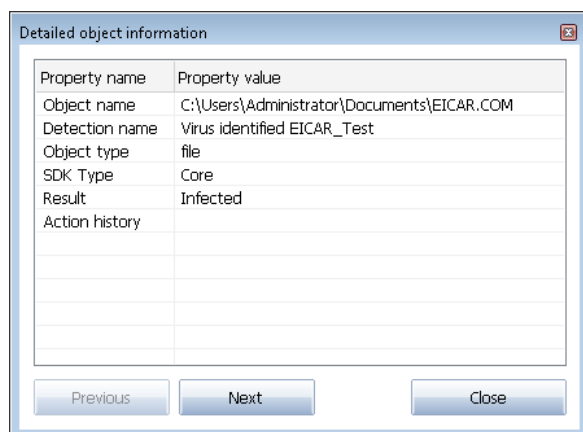
unable to scan it

- **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 object information**:



In this dialog you can find detailed information on the detected infectious object (e.g. *infected object name and location, object type, SDK type, detection result and history of actions related to the detected object*). Using the **Previous / Next** buttons you can view information on specific findings. Use the **Close** button to leave this dialog.

- **Remove selected** - use the button to move the selected finding to the [Virus Vault](#)
- **Remove all unhealed** - 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 in the test results there are only Warnings detected by **AVG**



**Premium Security 2012**, 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 **AVG Premium Security 2012** reports a hidden file which you suspect to be malicious, you can move it to your [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. Rootkits Tab

The **Rootkits** tab displays information on rootkits detected during scanning if you have launched the [Anti-Rootkit scan](#).

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

The structure of this tab is basically the same as the [Infections tab](#) or the [Spyware tab](#).

#### 11.7.6. Information Tab

The **Information** tab contains data on such "findings" that cannot be categorized as infections, spyware, etc. They can neither be positively labeled as dangerous but they are still worth your attention. **AVG Premium Security 2012** scan is able to detect files which may not be infected, but are suspicious. These files are reported either as [Warning](#), or as Information.

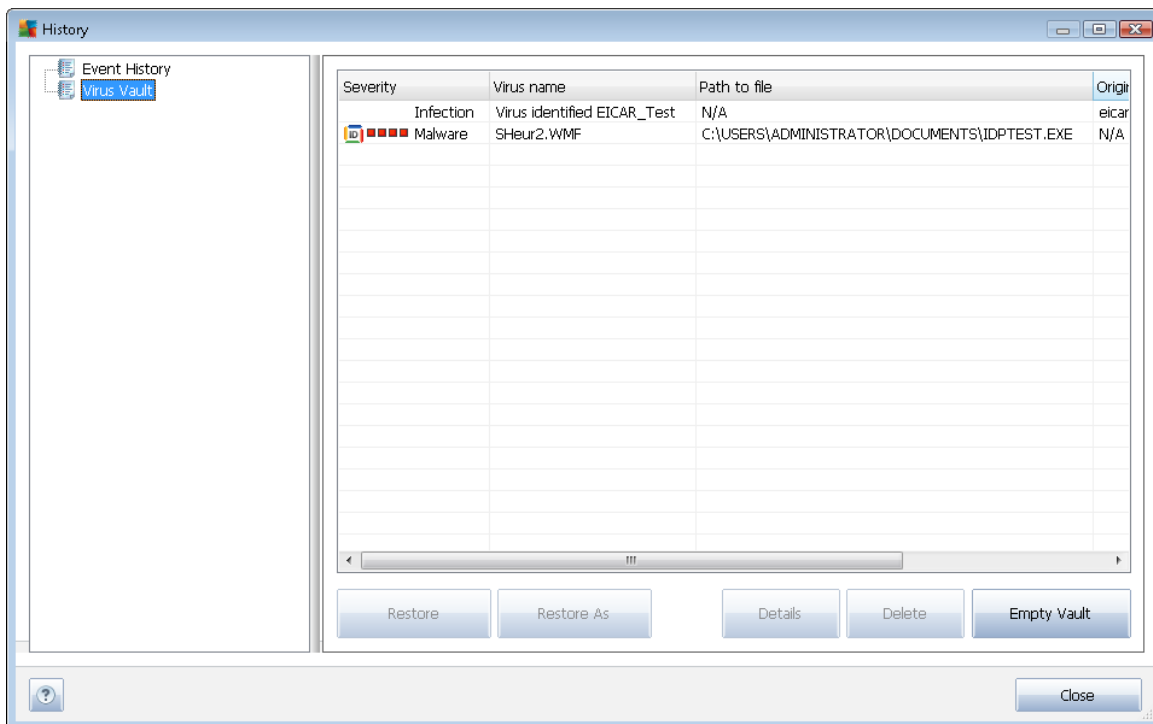
The severity **Information** can be reported for one of the following reasons:

- **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 Premium Security 2012** (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 Premium Security 2012** 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 Premium Security 2012** 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 Premium Security 2012**. 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 main purpose of the **Virus Vault** is to keep any deleted file for a certain period of time, so that you can make sure you do not need the file any more in its original location. Should you find out the file absence causes problems, you can send the file in question to analysis, or restore it to the original location.



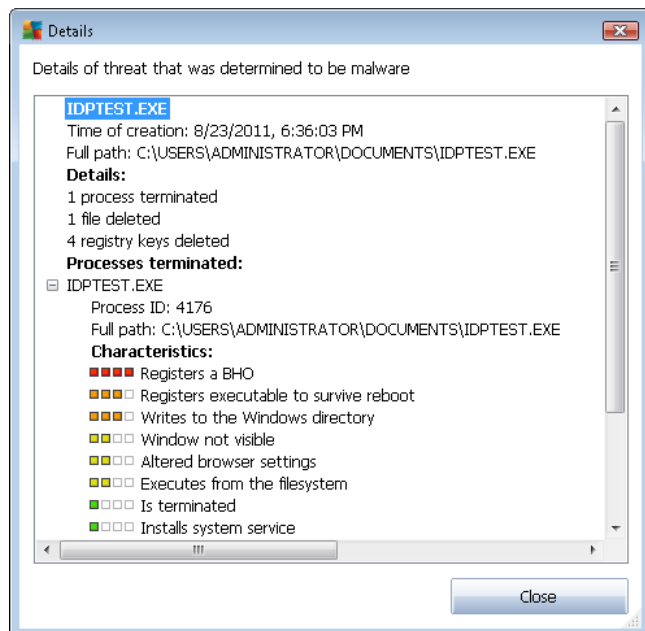
The **Virus vault** interface opens in a separate window and offers an overview of information on quarantined infected objects:

- **Severity** - in case you decided to install the [Identity Protection](#) component within your **AVG Premium Security 2012**, a graphical identification of the respective finding severity on a four-levels scale from unobjectionable (■□□□) up to very dangerous (■□■□) will be provided in this section; and the information on the infection type (*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** - moves the infected file to a selected folder
- **Details** - this button only applies to threats detected by [Identity Protection](#). Upon clicking, it displays synoptic overview of the threat details (*what files/processes have been affected, characteristics of the process etc.*). Please note that for all other items than detected by IDP, this button is greyed out and inactive!



- **Delete** - removes the infected file from the **Virus Vault** completely and irreversibly
- **Empty Vault** - removes all **Virus Vault** content completely. By removing the files from the **Virus Vault**, these files are irreversibly removed from the disk (*not moved to the recycle bin*).



## 12. AVG Updates

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.

Considering all the newly-emerged computer threats, and the speed they spread, it is absolutely crucial to update your **AVG Premium Security 2012** regularly. Best solution is to stick to the program default settings where the automatic update is configured. Please mind that if the virus database of your **AVG Premium Security 2012** is not up-to-date, the program will not be able to detect the latest threats!

***It is crucial to update your AVG regularly! Essential virus definition updates should be daily if possible. Less urgent program updates can be weekly.***

### 12.1. Update launch

To provide maximum security available, **AVG Premium Security 2012** is by default scheduled to look for new updates every four hours. Since AVG updates are not released according to any fixed schedule but rather in reaction to amount and severity of new threats, this check-up is highly important to make sure your AVG virus database is kept up-to-date all the time.

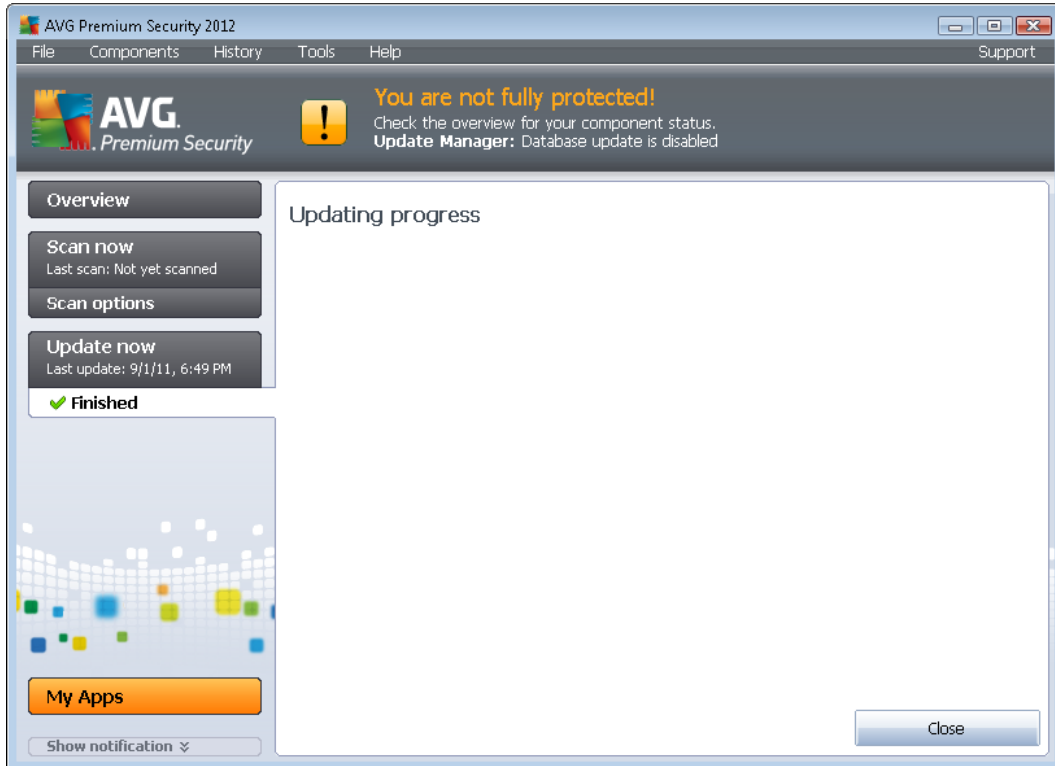
Should you wish to reduce the number of update launches, you can set up your own update launch parameters. However, it is strictly recommended to launch the update at least once a day! The configuration can be edited within the [Advanced settings/Schedules](#) section, specifically in the following dialogs:

- [Definitions update schedule](#)
- [Program update schedule](#)
- [Anti-Spam update schedule](#)

In case you want to check the new update files immediately, use the [Update now](#) quick link in the main user interface. This link is available at all times from any [user interface](#) dialog.

### 12.2. Update progress

Once you start the update, AVG will first verify whether there are new update files available. If so, **AVG Premium Security 2012** 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 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 operating system in its original configuration from this point. This option is accessible via Windows menu: Start / All Programs / Accessories / System tools / System Restore. Recommended to experienced users only!

### 12.3. Update levels

AVG Premium Security 2012 offers two update levels to select from:

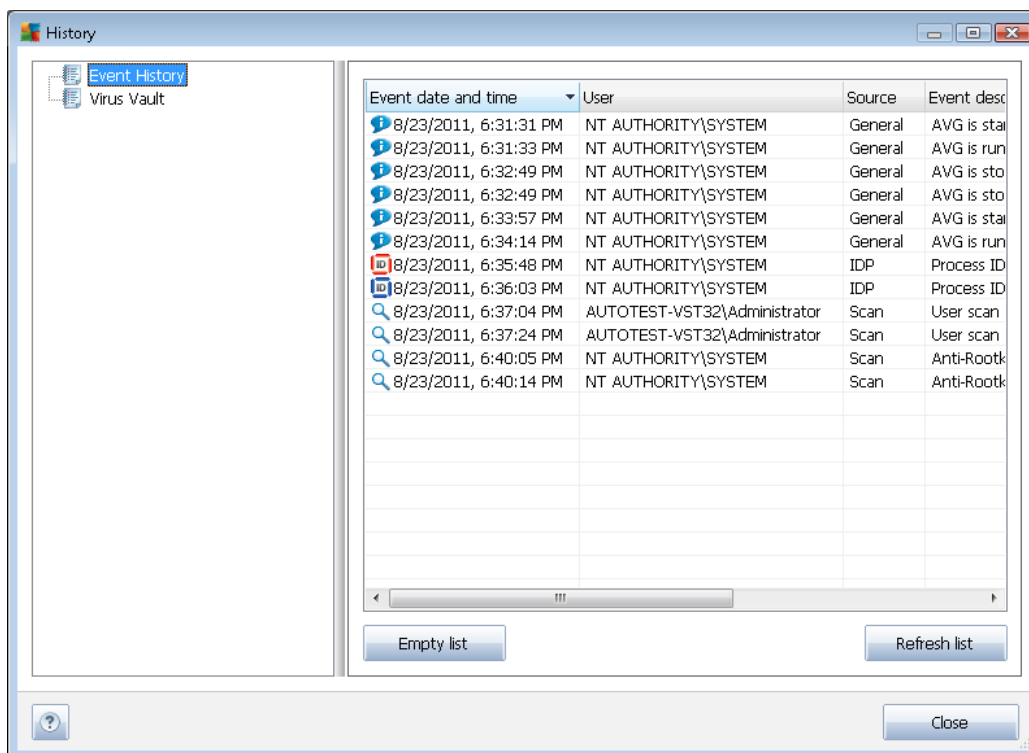
- **Definitions update** contains changes necessary for reliable anti-virus protection. Typically, it does not include any changes to the code and updates only the definition database. This update should be applied as soon as it is available.
- **Program update** contains various program changes, fixes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

When [scheduling an update](#), it is possible to define specific parameters for both update levels:

- [Definitions update schedule](#)
- [Program update schedule](#)

**Note:** If a time coincidence of a scheduled program update and scheduled scan occurs, the update process is of higher priority and the scan will get interrupted.

## 13. Event History



The **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 Premium Security 2012** operation. **History** records the following types of events:

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

For each event, the following information are listed:

- **Event date and time** gives exact date and time the event occurred
- **User** states the name of the user currently logged in at the time of the event occurrence
- **Source** gives the information on a source component or other part of the AVG system that triggered the event
- **Event description** gives brief summary of what actually happened



### Control buttons

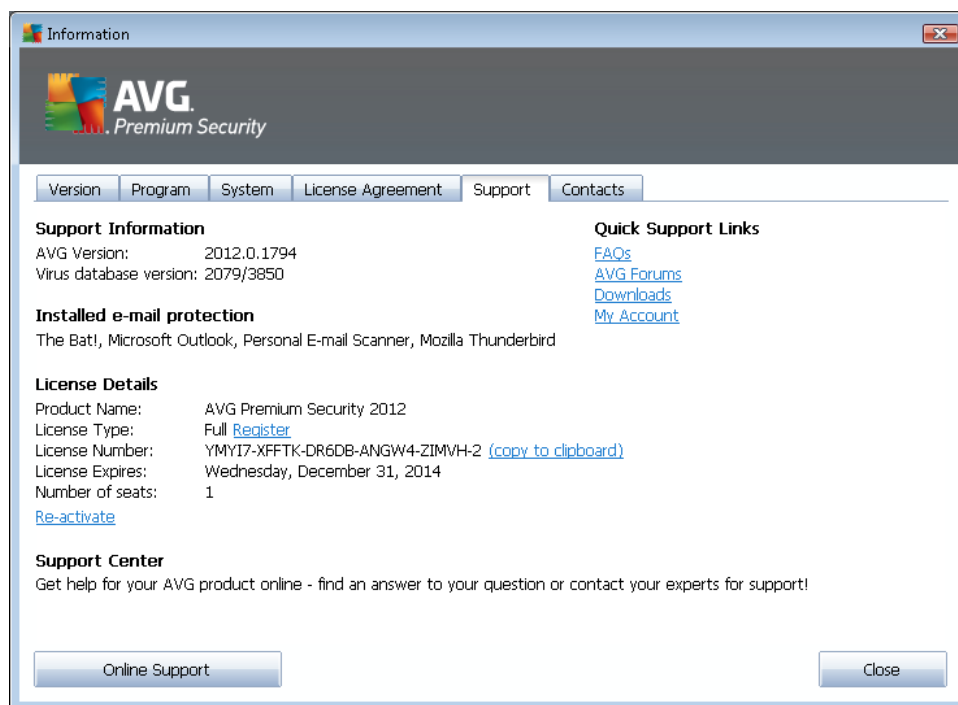
- **Empty list** - press the button to deletes all entries in the list of events
- **Refresh list** - press the button to updates all entries in the list of events



## 14. FAQ and Technical Support

Should you have any sales or technical trouble with your **AVG Premium Security 2012** application, there are several ways to look for help. Please chose from the following options:

- **Get help online:** Right within the AVG application you can reach a dedicated customer support page on AVG website (<http://www.avg.com/>). Select the **Help / Get Help Online** main menu item to get redirected to AVG website with available support avenues. To proceed, please follow the instruction in the web page.
- **Support (main menu link):** The AVG application menu (*on top of the main user interface*) includes the **Support** link that opens a new dialog with all types of information you might need when trying to find help. The dialog includes basic data on your installed AVG program (*program / database version*), license details, and a list of quick support links:



- **Troubleshooting in help file:** A new **Troubleshooting** section is available directly in the help file included in **AVG Premium Security 2012** (*to open the help file, press F1 key in any dialog in the application*). This section provides a list of most frequently occurring situations when a user desires to look up professional help to a technical issue. Please select the situation that best describes your problem, and click it to open detailed instructions leading to the problem solution.
- **AVG website Support Center:** Alternatively, you can look up the solution to your problem on AVG website (<http://www.avg.com/>). In the **Support Center** section you can find a structured overview of thematic groups dealing with both sales and technical issues.
- **Frequently asked questions:** On the AVG website (<http://www.avg.com/>) you can also find a separate and elaborately structured section of frequently asked questions. This section is accessible via **Support Center / FAQ** menu option. Again, all questions are divided in a



well arranged way into sales, technical, and virus categories.

- **About viruses & threats.** A specific chapter of the AVG website (<http://www.avg.com/>) is dedicated to virus issues (*the webpage is accessible from the main menu via the Help / About Viruses and Threats option*). In the menu, select **Support Center / About viruses & threats** to enter a page providing structured overview of information related to online threats. You can also find instructions on removing viruses, spyware, and advice on how to stay protected.
- **Discussion forum:** You can also use the AVG users discussion forum at <http://forums.avg.com>.