AVG 8.0 Free Edition

User Manual

Contents

1. Introduction

This user manual offers a general overview of the tasks and detection technologies provided by **AVG 8.0 Free**. We will briefly talk about the program installation, initial startup, configuration and use.

AVG 8.0 Free is provided free-of-charge, and its functionality is limited. While using **AVG 8.0 Free** you might discover you would like to have access to further and extended functionality of AVG as provided within the AVG 8.0 products. Then, please visit the AVG website (www.avg.com) for information on AVG 8.0 purchase options.

2. AVG Free Installation Requirements

2.1. Operation Systems Supported

AVG 8.0 Free is intended to protect computers with the following operating systems:

- Windows 2000 Professional SP4 + Update Rollup 1

- Windows XP Home Edition SP2

- Windows XP Professional SP2

- Windows XP Professional x64 Edition SP1

- Windows Vista (x86 and x64, all editions)

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

2.2. Minimum Hardware Requirements

Minimum hardware requirements for **AVG 8.0 Free** are as follows:

- Intel Pentium CPU 1,2 GHz

- 70 MB of free hard drive space (for installation purposes)

- 256 MB of RAM memory

3. AVG Free Installation Process

3.1. AVG Installation Options

To download the installation file of **AVG 8.0 Free** visit the AVG Free website at http://free.avg.com/ and follow the **AVG 8.0 Free** download link.

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

3.2. Installation Launch
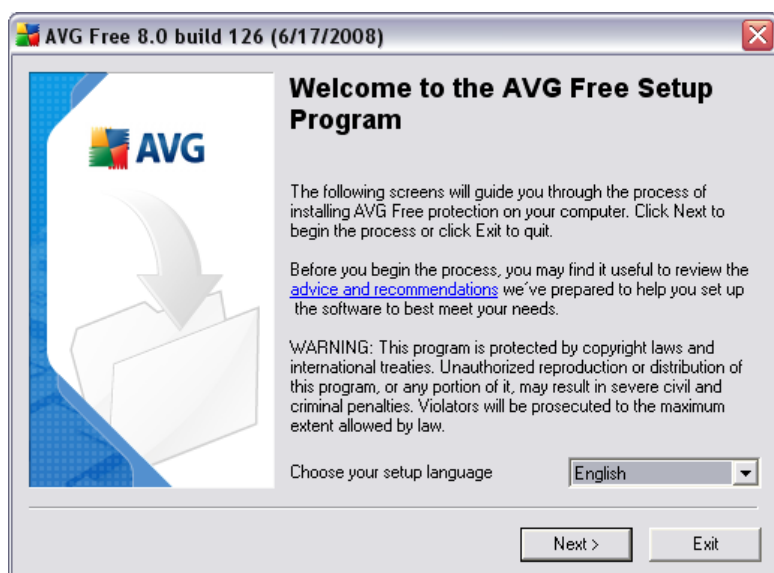
The installation process starts with the ***Welcome to the AVG Setup Program*** window.

3.3. Acceptance Notice

The next dialog provides information on **<%main_product_name_in_text%** terms of use. Please read it carefully and confirm that you have read, understood and accept the agreement by pressing the ***Accept*** button. If you do not agree with the terms of use stated press the ***Don't accept*** button, and the installation process will be

terminated immediately.
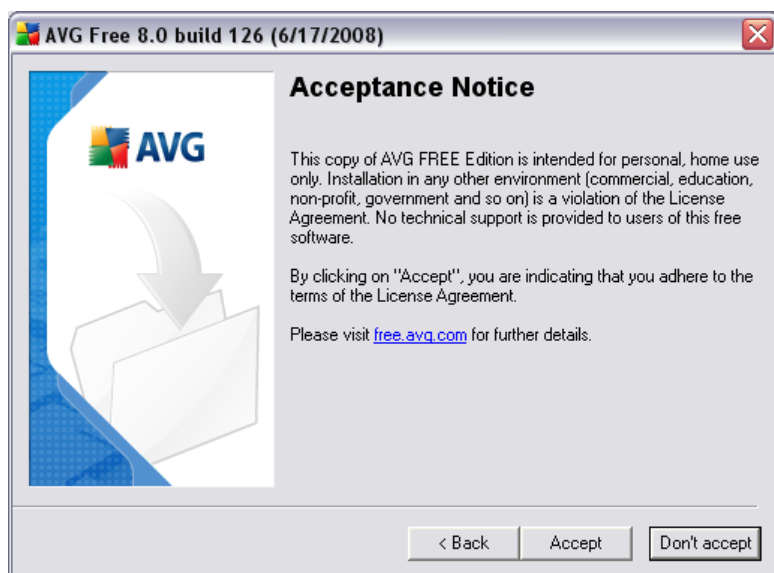
3.4. Checking System Status
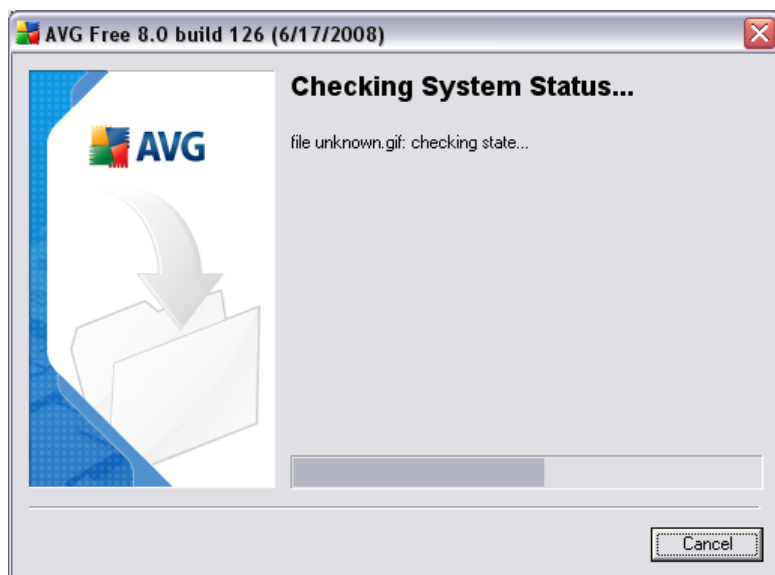
Further you will be redirected to the **Checking System Status** dialog. This dialog does not require any intervention; your system is being checked before the **AVG 8.0 Free** installation can start. Please wait until the process has finished, then continue automatically to the following dialog.

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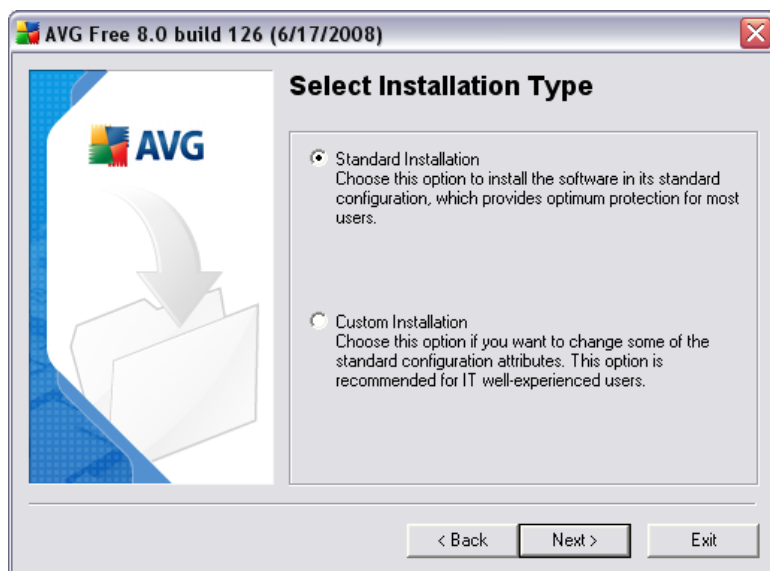
The **Select Installation Type** dialog offers the choice of two installation options: *standard* and *custom* installation.

For most users, it is highly recommended to keep to the **standard installation** that installs **AVG 8.0 Free** in fully automatic mode with settings predefined by the program vendor. This configuration provides maximum security combined with the optimal use of resources. In the future, if the need arises to change the configuration, you will always have the possibility to do so directly in the AVG application.

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

3.6. Activate Your AVG Free License

In the **Activate your AVG Free License** dialog you have to fill in your registration data. Type in your name (**User Name** field). For the **AVG 8.0 Free**, the license number is already provided in the **License number** text field, you do not need to change it.

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

If in the previous step you have selected the standard installation, you will be redirected directly to the **_AVG Security Toolbar_** dialog. If custom installation was selected you will continue with the **_Destination Folder_** dialog.

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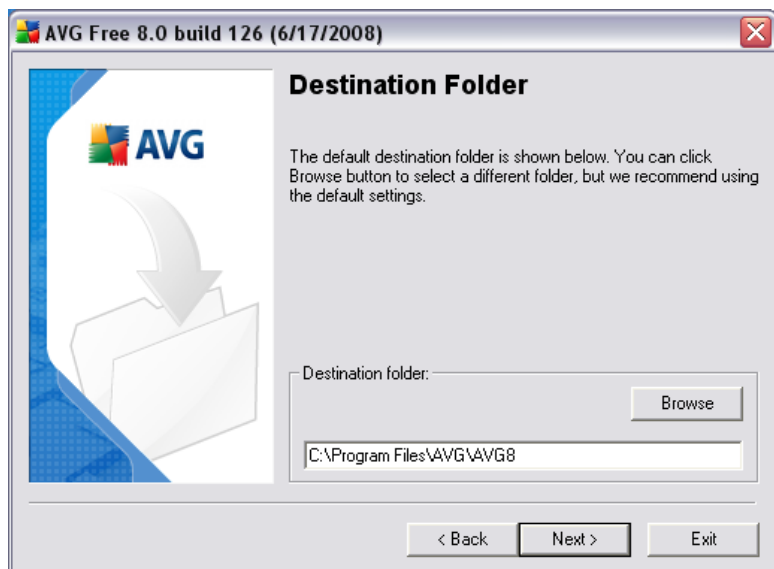
The ***Destination folder*** dialog allows you to specify the location where AVG should be installed. By default, AVG will be installed to the program files folder located on drive C:. If you want to change this location, use the ***Browse*** button to display the drive structure, and select the respective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

3.8. Custom Installation - Component Selection
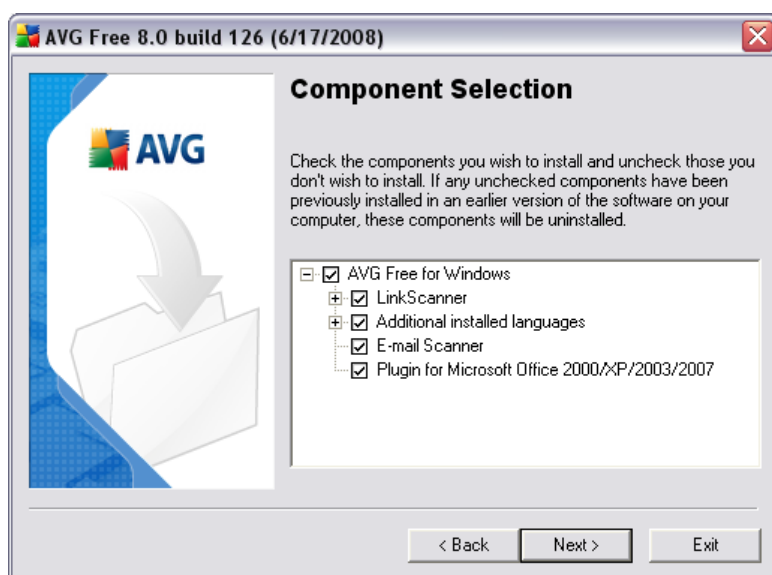
The ***Component Selection*** dialog displays an overview of all **AVG 8.0 Free** components that can be installed. If the default settings do not suit you, you can remove specific components. Should you find out you need some more protection, you might be interested in the full version of AVG - for more information please visit the AVG website (www.avg.com).

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

3.9. Custom Installation - E-mail Scanning

With AVG ***standard installation***, setup will detect your default e-mail client and automatically install the respective e-mail scanning plug-in. Specific plug-ins support the most frequently used e-mail programs: MS Outlook, MS Exchange, The BAT!, Qualcomm Eudora etc.

With AVG ***custom installation***, you can install the ***Personal E-mail Scanner***, a comprehensive tool for e-mail communication scanning that guarantees your emails will be virus-free with any e-mail client you use:
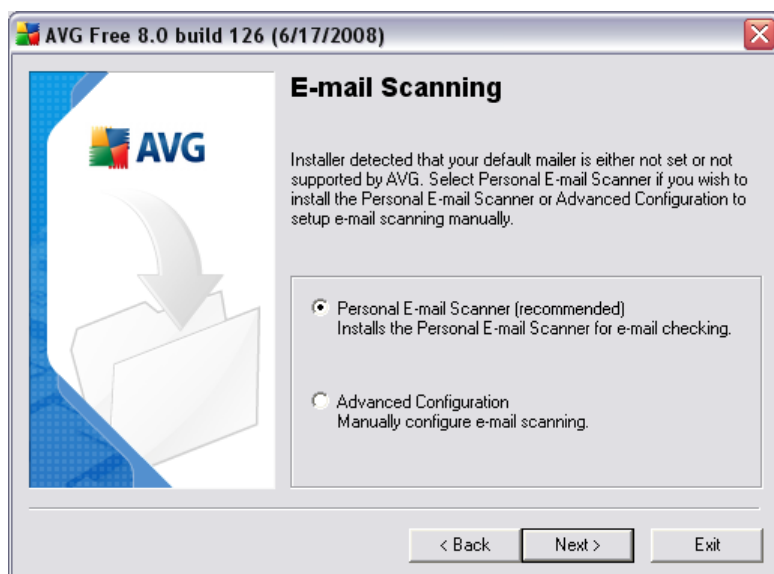
In the **E-mail Scanning** dialog you can choose to install the **Personal E-mail Scanner** to secure your e-mail communication automatically, or you can choose to set up an advanced configuration of e-mail scanning. It is recommended to install the **Personal E-mail Scanner** in fully automatic mode.

However, if you have a valid reason to do so, you can set up the e-mail scanner manually. In the **E-mail Scanning** dialog select the **Advanced Configuration** option and go on to the **E-mail Scanning - Plug-in selection** dialog. In this dialog you can then select the specific plug-ins that are to be installed:
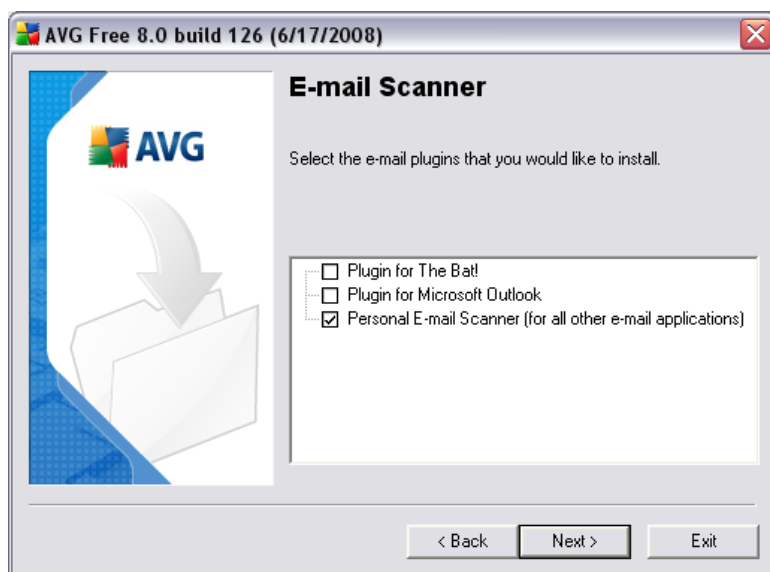
Press the **Next** button to confirm your choice.

3.10.AVG Security Toolbar
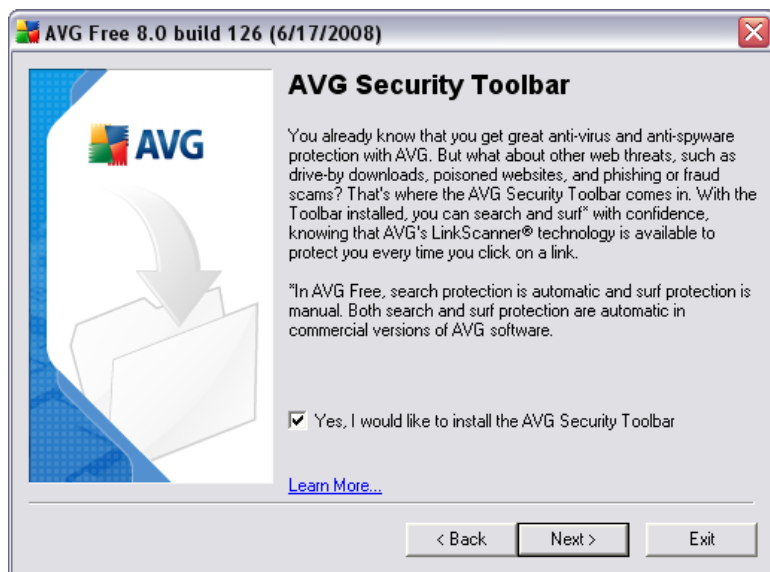
In the **AVG Security Toolbar** dialog decide whether you want to install the **AVG Security Toolbar** feature of your **AVG 8.0 Free**. The **AVG Security Toolbar** works within your Internet browser in conjunction with AVG 8.0 and AVG XPL technologies

to provide you with comprehensive online protection while surfing the Internet.

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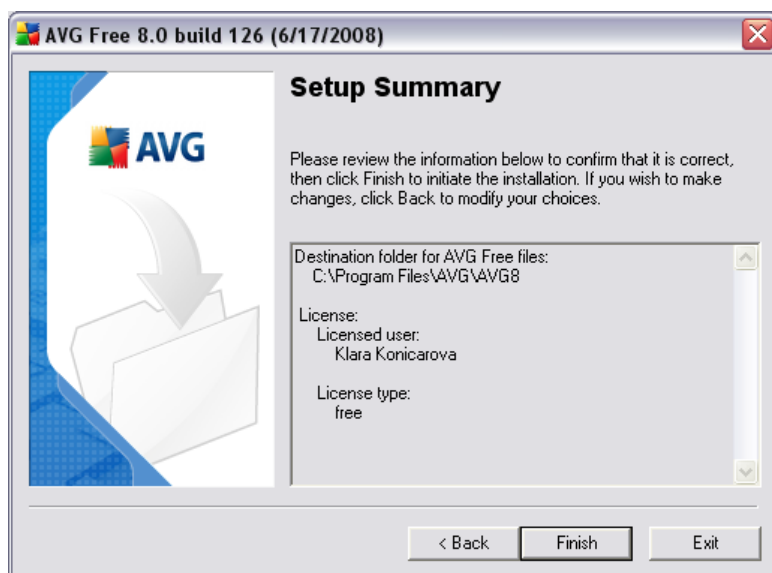
The **Setup Summary** dialog provides an overview of all parameters of the installation process. Please make sure all the information is correct. If so, press the **Finish** button to continue. Otherwise, you can use the **Back** button to return to the respective dialog and correct the information.

3.12.Installing AVG

The **Installing AVG** dialog shows the progress of the installation process, and does not require any intervention. Please wait until the installation is complete, then you will be redirected to the **_Installation Complete_** dialog.

3.13.Installation Complete

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

4. AVG First Run Wizard

After installation, the ***AVG First Run Wizard*** will be launched automatically and in a few steps will lead you through **<main_product_name_in_text%>** elementary configuration. Although AVG configuration is accessible at any time after installation, we recommend that you take this opportunity to set up the basic configuration using the wizard's help.

4.1. Congratulations!

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

4.2. AVG Task Schedule
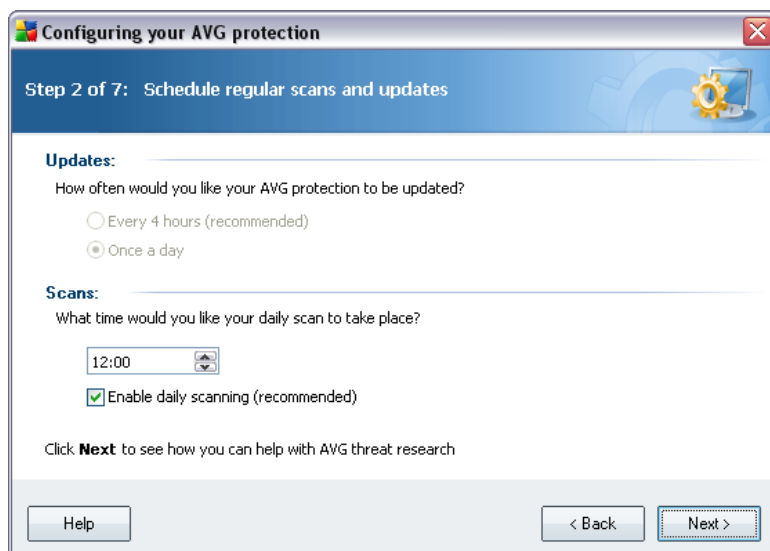
In the **AVG Task Schedule** dialog define time when the scheduled scan should be launched. It is recommended to keep the default values.

As for the updates, with **AVG 8.0 Free** you cannot specify how often you want to check for new updates. **AVG 8.0 Free** updates once a day, by default.

Press the **Next** button to continue.

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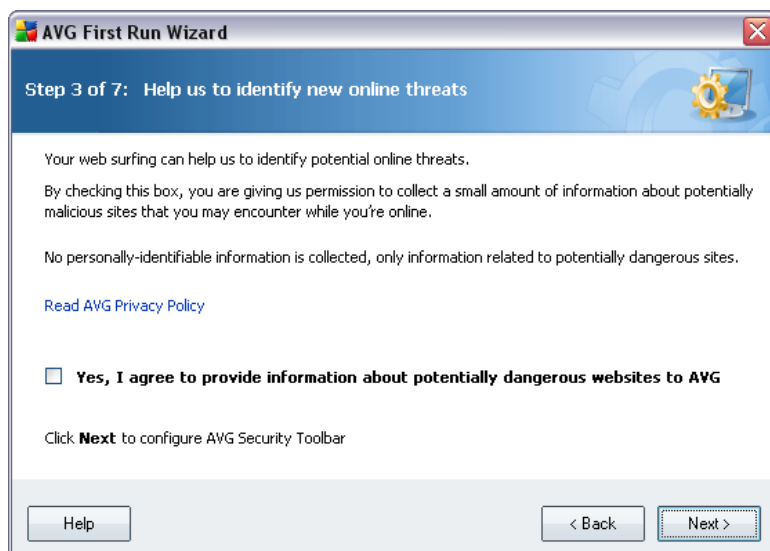
In the *Help us to identify new online threats* dialog decide whether you want to activate the option of reporting of exploits and bad sites found by users either via *AVG Surf-Shield / AVG Search-Shield* features of the **_LinkScanner_** component to feed the database collecting information on malicious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

Press the *Next* button to continue.

4.4. Yahoo! Search engine
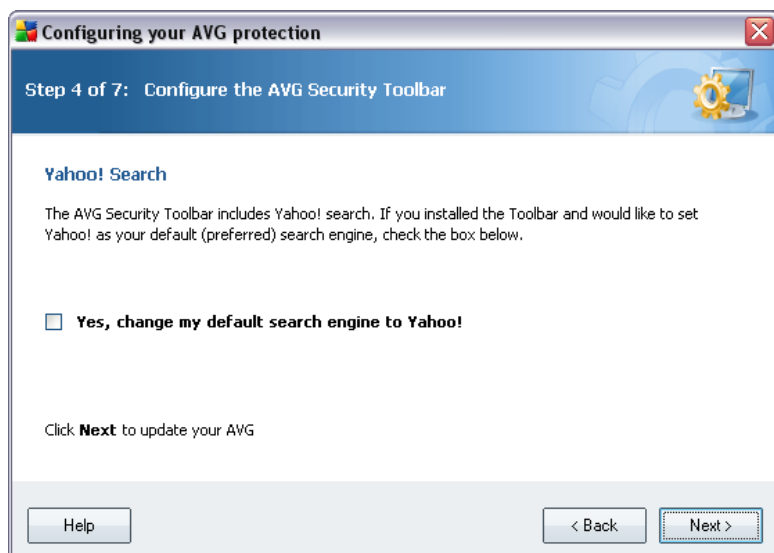
In the **Yahoo! Search** dialog you can tick the check box if you want Yahoo! to become your default search engine.

4.5. Update AVG protection
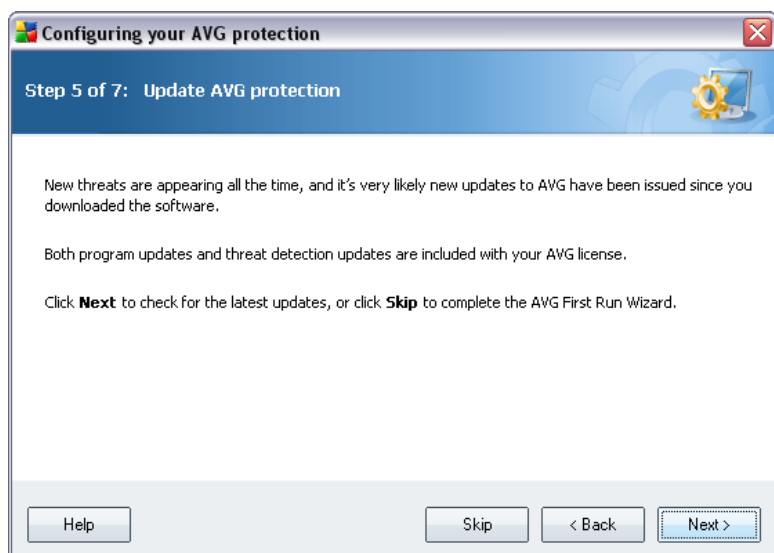
The **Update AVG protection** dialog will automatically check and download the latest

AVG updates. Click on the *Next* button to download the latest update files and perform the update:
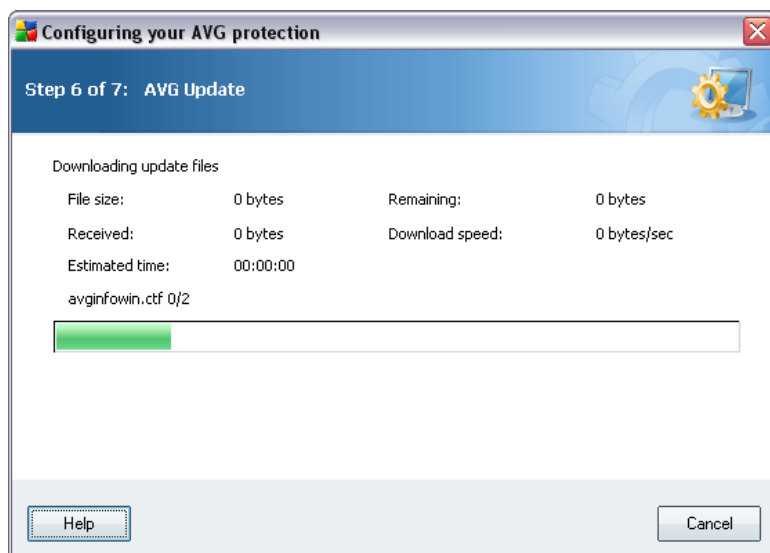
Once the update is finished, continue to the next dialog.

4.6. Register AVG Anti-Virus Free

In the *Register AVG Anti-Virus Free* dialog you are invited to get online to perform your registration in order to be able to get access to all **AVG 8.0 Free** forums and discussions that are the only source of technical support for the free version of AVG.
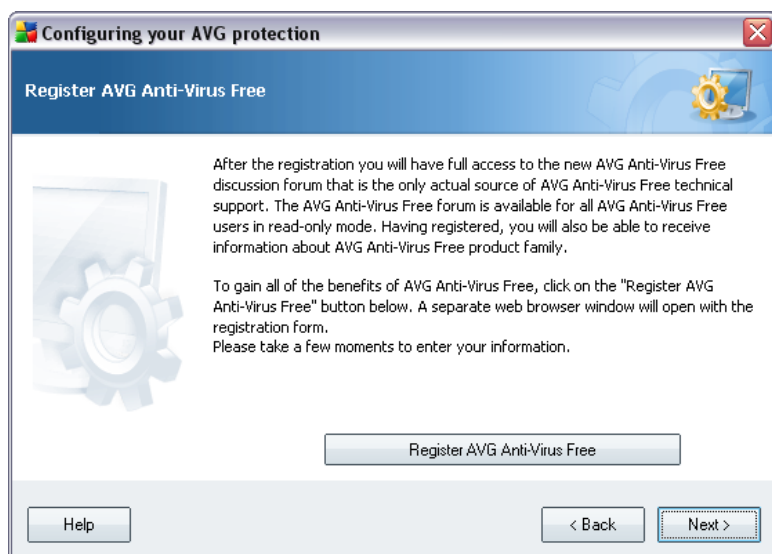
Click the **Register AVG Anti-Virus Free** button to open your web browser and fill in the registration form online. Then continue by pressing the **Next** button.

4.7. AVG Configuration Finished
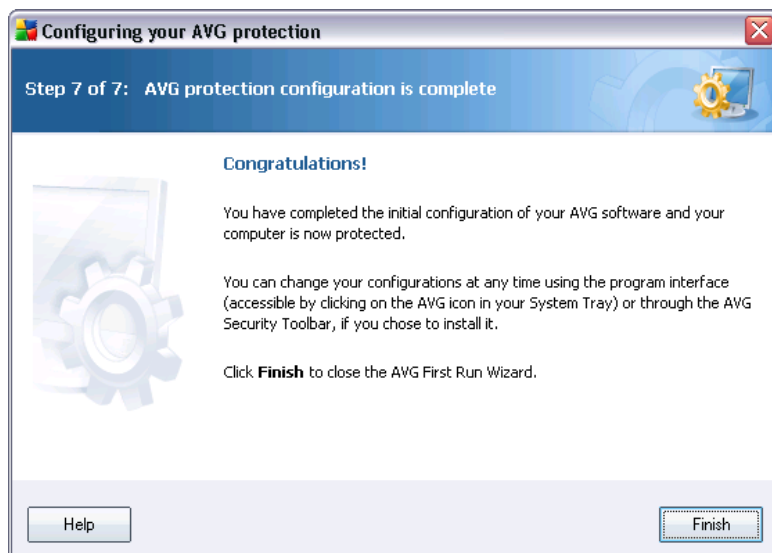
Now your **AVG 8.0 Free** has been configured; press the **Finish** button to start working with AVG.

5. After Installation

5.1. Access to User Interface

The **_AVG Free User Interface_** is accessible in several ways:

- double-click the AVG Free icon on the system tray

- double-click the AVG Free icon on the desktop

- from the menu **_Start/All Programs/AVG Free 8.0/AVG Free User Interface_**

5.2. Scanning of the whole computer

There is a potential risk that a computer virus has been transmitted to your computer prior to **AVG 8.0 Free** installation. For this reason you should run a **_Scan of the whole computer_** to make sure there are no infections on your PC.

For instructions on running a **_Scan of the whole computer_** please consult the chapter **_AVG Scanning_**.

5.3. Eicar Test

To confirm that **AVG 8.0 Free** has been installed correctly you can perform the EICAR test.

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

Try to download the **_eicar.com_** file, and save it on your local disk. Immediately after you confirm downloading of the test file, the **_Resident Shield_** will react to it with a warning. This **_Resident Shield_** notice demonstrates that AVG is correctly installed on your computer.
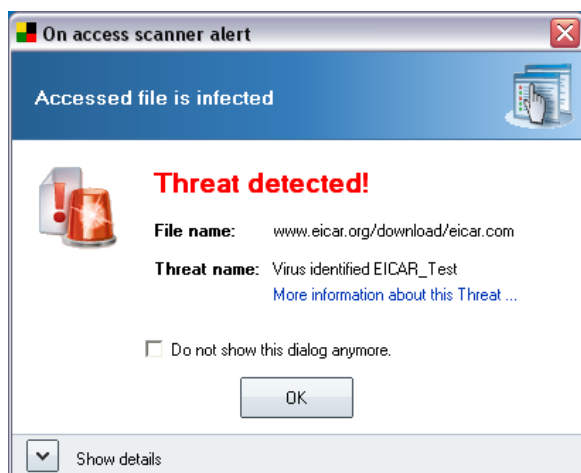
If AVG fails to identify the EICAR test file as a virus, you should check the program configuration again!

5.4. AVG Default Configuration

The default configuration (*i.e. how the application is set up right after installation*) of **AVG 8.0 Free** is set up by the software vendor so that all components and functions are tuned up to achieve optimum performance.

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

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

6. AVG Free User Interface

AVG 8.0 Free open with the main window:

The main window is divided into several sections:

- **System Menu** *(top system line in the window)* is the standard navigation that allows you to access all AVG components, services, and features - [details >>](#)

- **Security Status Info** *(upper section of the window)* provides you with information on the current status of your AVG program - [details >>](#)

- **Quick Links** *(left section of the window)* allow you to quickly access the most important and most frequently used AVG tasks - [details >>](#)

- **Components Overview** *(central section of the window)* offer an overview of all installed AVG components - [details >>](#)

- **Statistics** *(left bottom section of the window)* provide you with all statistical

data regarding the programs operation - <u>details >></u>

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

6.1. System Menu

The **System menu** is the standard navigation used in all Windows applications. It is located horizontally in the very top part of the **AVG 8.0 Free** main window. Use the system menu to access specific AVG components, feature, and services.

The system menu is divided into five main sections:

6.1.1. File

- **Exit** - closes the **AVG 8.0 Free**'s user interface. However, the AVG application will continue running in the background and your computer will still be protected!

6.1.2. 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 <u>overview of all installed components and their status</u>

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

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

- **E-mail Scanner** - opens the default page of the **E-mail Scanner** component

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

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

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

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

6.1.3. 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 Scanner*** 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 8.0 Free** actions.

6.1.4. Tools

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

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

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

- ***Update*** - automatically launches the update process of **AVG 8.0 Free**

- ***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 8.0 Free** configuration. Generally, it is recommended to

keep the default settings of the application as defined by the software vendor.

6.1.5. Help

- **Contents** - opens the AVG help files

- **Get Help Online** - opens the AVG website at the customer support center page

- **Your AVG Web** - opens the AVG homepage (at www.avg.com)

- **About Viruses and Threats** - opens the online **Virus Encyclopedia** where you can look up detailed information on the identified virus

- **Buy now** - opens the AVG website at the online Store where you can purchase a copy of AVG

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

6.2. Security Status Info

The **Security Status Info** section is located in the upper part of the AVG main window. Within this section you will always find information on the current security status of your **AVG 8.0 Free**. Please see an overview of icons possibly depicted in this section, and their meaning:

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

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

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

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

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

6.3. Quick Links

Quick links *(in the left section of the AVG User Interface)* allow you to immediately access the most important and most frequently used AVG features:
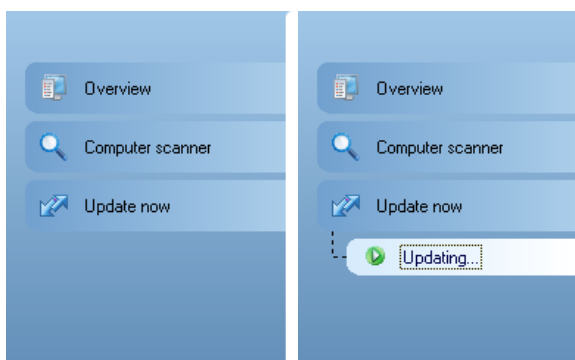
- **Overview** - use this link to switch from any currently opened AVG interface to the default one with an overview of all installed components - see chapter **Components Overview >>**

- **Computer scanner** - use this link to open the AVG scanning interface where you can run tests directly, schedule scans, or edit their parameters - see chapter **AVG Tests >>**

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

These links are accessible from the user interface at all times. Once you use a quick link to run a specific process, the GUI will switch to a new dialog but the quick links

are still available. Moreover, the running process is further graphically depicted - *see picture 2*.

6.4. Components Overview

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

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

- Description of a selected component

Within the **AVG 8.0 Free** the ***Components Overview*** section contains information on the following components:

- ***Anti-Virus*** ensures that your computer is protected from viruses trying to

enter your computer - <u>details >></u>

- ***Anti-Spyware*** scans your applications in the background as you run them - <u>details >></u>

- ***E-mail Scanner*** checks all incoming and outgoing mail for viruses - details >>

- ***License*** provides full wording of the AVG License Agreement - <u>details >></u>

- ***LinkScanner*** checks the search results displayed in your internet browser - <u>details >></u>

- ***Resident Shield*** runs in the background and scans files as they are copied, opened or saved - <u>details >></u>

- ***Update Manager*** controls all AVG updates - <u>details >></u>

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

6.5. Statistics

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

- ***Last scan*** - provides the date when the last scan was performed

- ***Last update*** - provides the date when the last update was launched

- ***Virus DB*** - informs you about the currently installed version of the virus database

- ***AVG version*** - informs you about the AVG version installed *(the number is in the form of 8.0.xx, where 8.0 is the product line version, and xx stands for the number of the build)*

- ***License expires: Free*** - no expiration date is provided within **AVG 8.0 Free**

6.6. System Tray Icon

System Tray Icon (*on your Windows taskbar*) indicates the current status of your **AVG 8.0 Free**. It is visible at all times on your system tray, no matter whether your AVG main window is opened or closed.

If in full color , the **System Tray Icon** indicates that all AVG components are active and fully functional. Also, AVG system tray icon can be displayed in full color if AVG is in error state but you are fully aware of this situation and you have deliberately decided to ***Ignore the component state***. A gray icon coloring with an exclamation mark indicates a problem (inactive component, error status, etc.). Double-click the **System Tray Icon** to open the main window and edit a component.

The system tray icon further informs on current AVG activities and possible status changes in the program (*e.g. automatic launch of a scheduled scan or update, a component's status change, error status occurrence, ...*) via a pop-up window opened from the AVG system tray icon:
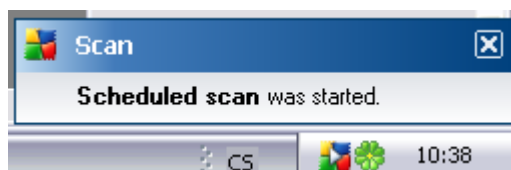
The **System Tray Icon** can also be used as a quick link to access the AVG main window at any time - double click on the icon. By right-click on the **System Tray Icon** you open a brief context menu with the following options:

- **Open AVG User Interface** - click to open the AVG User Interface

- **Update** - launches an immediate update

- **Exit** - click to close AVG *(You only close the user interface, AVG continues to run in the background and your computer is still fully protected!)*

7. AVG Components

7.1. Anti-Virus

7.1.1. Anti-Virus Principles

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

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

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

- Scanning - searching for character strings that are characteristic of a given virus

- Heuristic analysis - dynamic emulation of the scanned object's instructions in a virtual computer environment

- Generic detection - detection of instructions characteristic of the given virus/group of viruses

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

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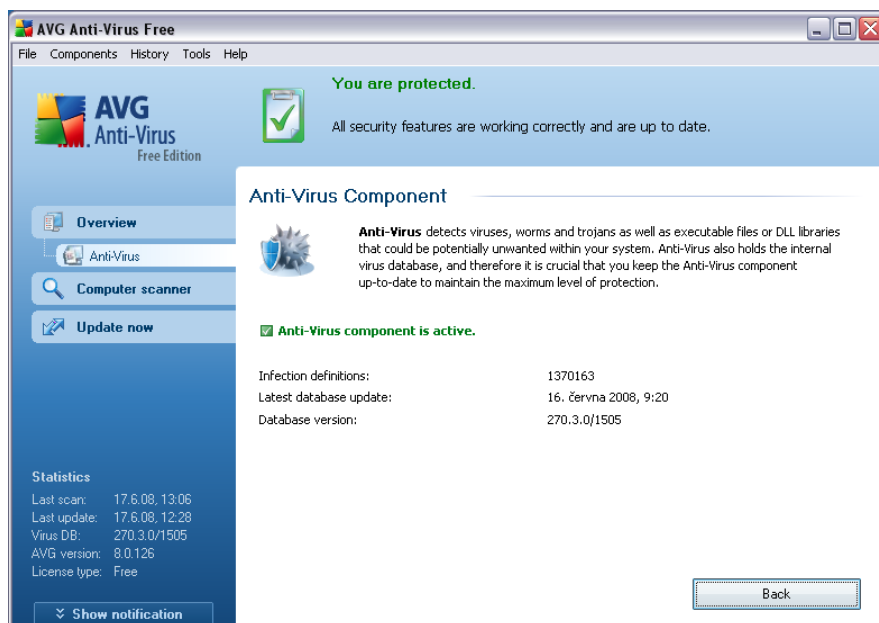
The **Anti-Virus** component's interface provides some basic information on the component's functionality, information on the component's current status (*Anti-Virus component is active.*), and a brief overview of **Anti-Virus** statistics:

- **Infection definitions** - number provides the count of viruses defined in the up-to-date version of the virus database

- **Latest database update** - specifies when and at what time the virus database was last updated

- **Database version** - defines the number of the latest virus database version; and this number increases with every virus base update

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

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

7.2. Anti-Spyware

7.2.1. Anti-Spyware Principles

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

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

There is also the potential risk that malware has been transmitted to your computer prior to AVG installation, or that you have neglected to keep your **AVG 8.0 Free** up-to-date with the latest database and program updates. For this reason, AVG allows you to fully scan your computer for malware/spyware using the scanning feature. It also detects sleeping and non-active malware, i.e. malware that has been downloaded but not yet activated.

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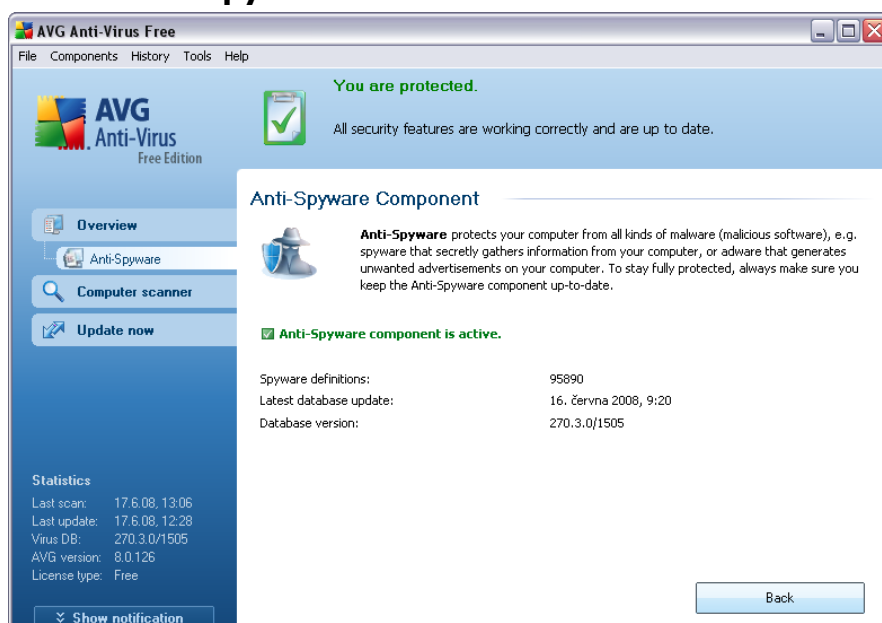
The **Anti-Spyware** component's interface provides a brief overview on the component's functionality, information on the component's current status (*Anti-Spyware component is active.*), and some **Anti-Spyware** statistics:

- **Spyware definitions** - number provides the count of spyware samples defined in the latest spyware database version

- **Latest database update** - specifies when and at what time the spyware database was updated

- **Database version** - defines the number of the latest spyware database version; and this number increases with every virus base update

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

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

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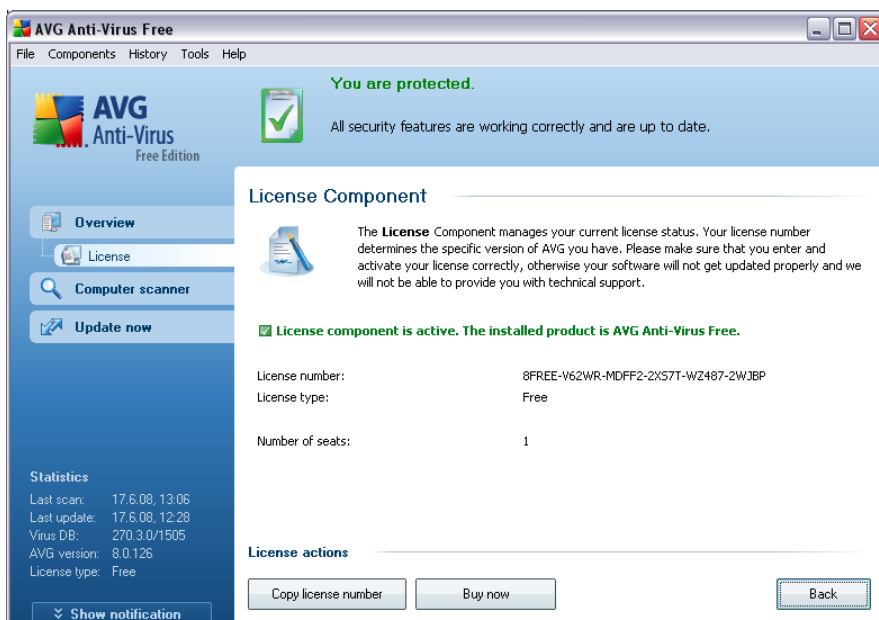
In the *Licence* component interface you will find a brief text describing the component's functionality, information on its current status (*License component is active.*), and the following information:

- **License number** - provides the exact form of your free license number. For **AVG 8.0 Free** the license number is preset automatically and you do not have to enter it.

- **License type** - specifies you are running the free version of AVG.

- **Number of seats** - how many workstations on which you are entitled to install your AVG.

Control buttons

- **Copy license number** - press the button to insert the currently used license number into clipboard (*just like with CTRL+C*), and you can paste it wherever needed

- **Buy now** - opens the AVG website at the online Store where you can purchase the full version of a selected AVG product

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

7.4. Link Scanner

The *LinkScanner* component within **AVG 8.0 Free** consists of two parts that you can switch on/off in the *LinkScanner* component interface:

- **Enable AVG Search-Shield** - (*on by default*): advisory notifying icons on searches performed in Google, Yahoo or MSN having checked ahead the content of sites returned by the search engine. The browsers supported are Internet Explorer and Firefox.

- *Enable AVG Active Surf-Shield - unfortunately, this option is deactivated with* **AVG 8.0 Free***; if you are interested in further and extended functionality within AVG 8.0 full products, please visit the* AVG website (www.avg.com) *for information on AVG 8.0 purchase options.*

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

7.4.1. AVG Search-Shield

When searching Internet with the *AVG Search-Shield* on, all search results returned from the most popular search engines like Yahoo!, Google, MSN, etc. are evaluated for dangerous or suspicious links. By checking these links and marking the bad links, the *AVG Security Toolbar* warns you before you click on dangerous or suspicious links, so you can ensure you only go to safe websites.

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

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

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

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

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

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

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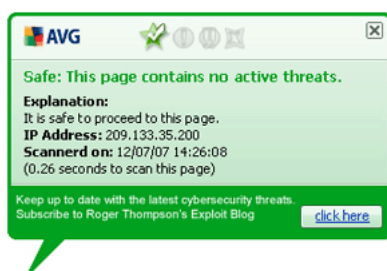
7.5. Resident Shield

7.5.1. Resident Shield Principles

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

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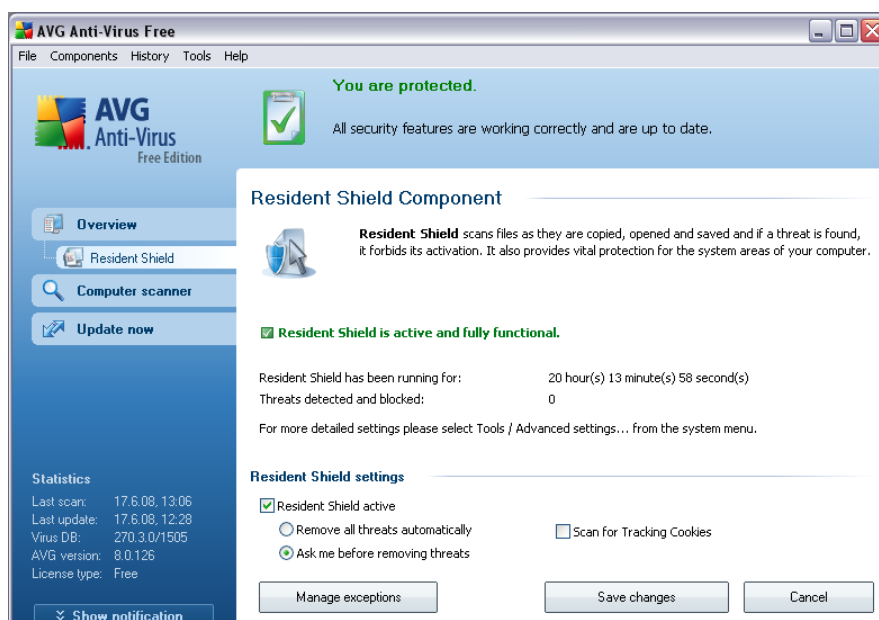
Besides an overview of the most important statistical data and the information on the component's current status (*Resident Shield is active and fully functional*), the **Resident Shield** interface offers some elementary component settings options, too. The statistics is as follows:

- **Resident Shield has been running for** - provides the time since the latest component's launch

- **Threats detected and blocked** - number of detected infections that were prevented from being run/opened

Basic component configuration

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

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

     o either automatically (**Remove all threats automatically**)

     o or only after the user's approval (**Ask me before removing threats**)

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

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

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

Control buttons

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

- **Manage exceptions** - opens the **Resident Shield - Directory Excludes** dialog where you can define folders that should be left out from the **Resident Shield** scanning

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

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

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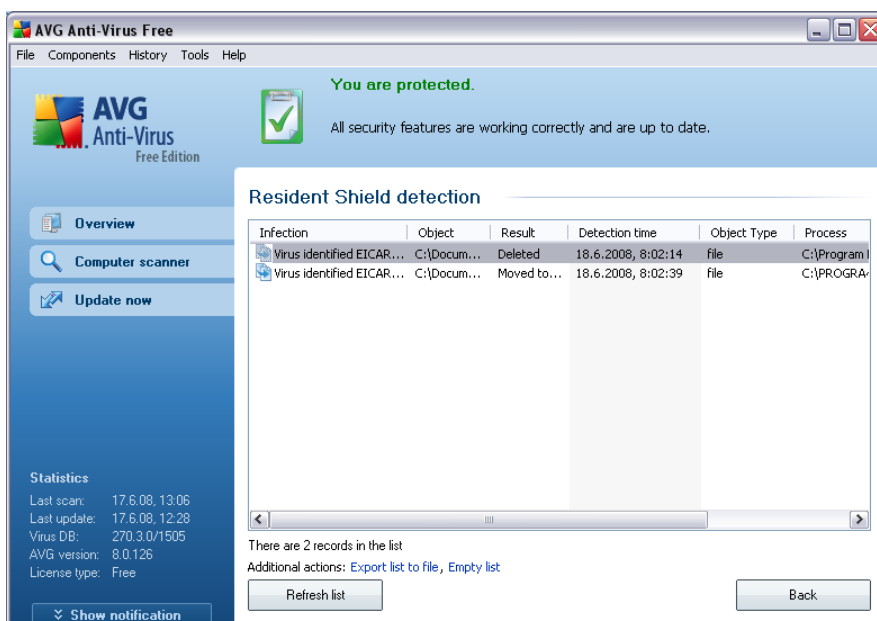
The **Resident Shield detection** offers an overview of objects that were detected by the **Resident Shield**, evaluated as dangerous and either cured or moved to the **Virus Vault**. For each detected object the following information is provided:

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

- **Object** - object location

- **Result** - action performed with the detected object

- **Detection Time** - exact time when the threat 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

7.6. Update Manager

7.6.1. Update Manager Principles

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

It is crucial to update your AVG regularly!

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

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

7.6.2. Update Manager Interface
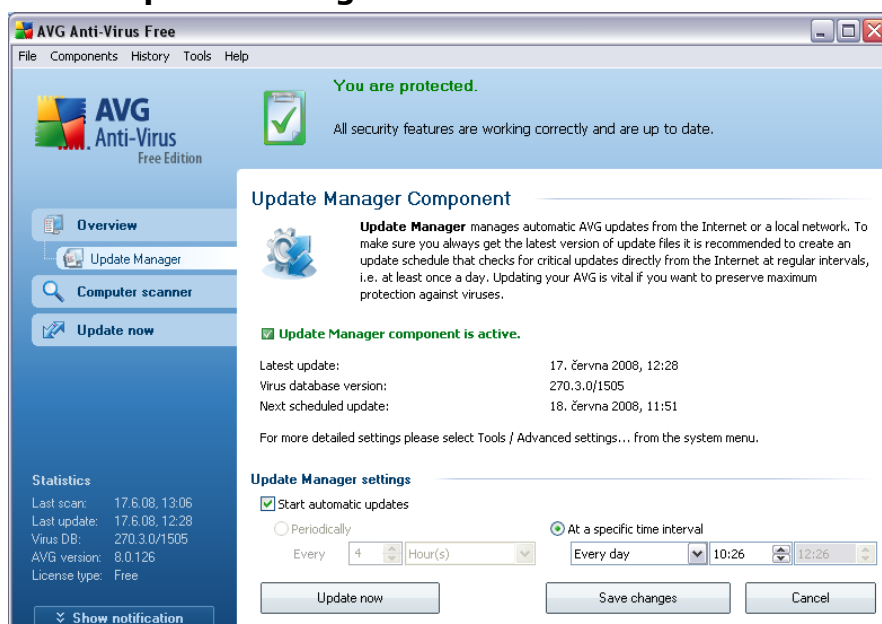
The **Update Manager**'s interface displays information about the component's

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

- **Latest update** - specifies when and at what time the database was updated

- **Virus database version** - defines the number of the latest virus database version; and this number increases with every virus base update

- **Next scheduled update** - specifies when and at what time the next update is scheduled to

Basic component configuration

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

Further you can define when the update should be launched:

- o **Periodically** - with **AVG 8.0 Free** you are limited to one update per day so this option is disabled! If you feel you would like to have access to to further and extended functionality within AVG 8.0 full products, please visit the [AVG website](#) ([www.avg.com](#)) for information on AVG 8.0 purchase options.

- o **At a specific time** - define the exact day and time

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

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

Control buttons

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

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

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

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

7.7. AVG Security Toolbar

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

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

The *AVG Security Toolbar* consists of the following:

- *AVG logo button* - provides access to general toolbar items. Click the logo button to get redirected to the AVG website (www.avg.com). Clicking the pointer next to the AVG icon will open the following:

  - o *Toolbar Info* - link to the *AVG Security Toolbar* home page with detailed information on the toolbar's protection

  - o *Launch AVG 8.0* - opens the AVG 8 user interface

  - o *Options* - opens a configuration dialog where you can adjust your *AVG Security Toolbar* settings to suit your needs; the dialog is divided into two tabs:

    - ➢ *General* - on this tab you can find two sections named *Buttons* and *Ratings*.

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

      The *Ratings* section allows you to determine what type of ratings do you want to be displayed for your search results. By default all ratings are visible but you may hide some of them (*when searching from the Yahoo! search box, only safe results are displayed*).
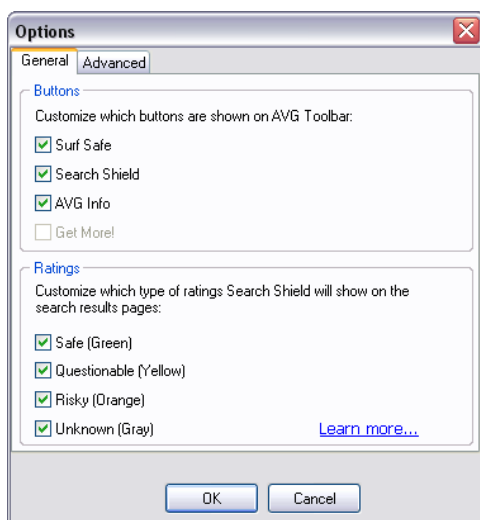
> ➢ **Advanced** - on this tab you can edit the **AVG Security Toolbar** protection features. By default, both the **AVG Search-Shield** and **AVG Active Surf-Shield** features are enabled.
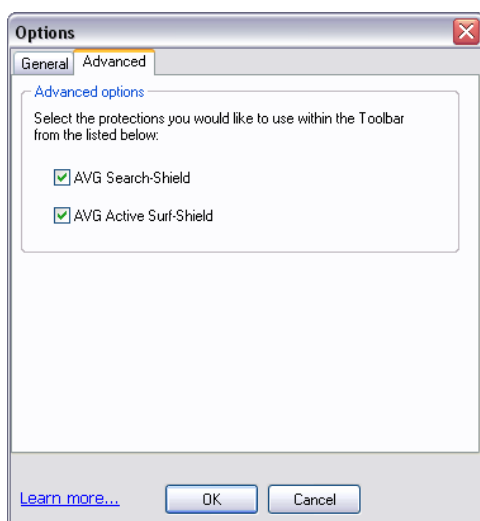
    o **Update** - checks for new updates for your **AVG Security Toolbar**

    o **Help** - provides options to open the help file, contact **AVG technical support**, or view the details of the current version of the toolbar

• **Yahoo! powered search box** - easy and safe way to search the web using

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

- *AVG Active Surf-Shield button - unfortunately, this option is deactivated with **AVG 8.0 Free**; if you are interested in further and extended functionality within AVG 8.0 full products, please visit the* AVG website *(*www.avg.com*) for information on AVG 8.0 purchase options.*

- ***AVG Search-Shield button*** - on/off button controls the status of the ***AVG Search-Shield*** protection

- ***AVG Info button*** - provides links to important security information located on the AVG website (www.avg.com)

8. AVG Advanced Settings

The advanced configuration dialog of **AVG 8.0 Free** 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.

8.1. Appearance

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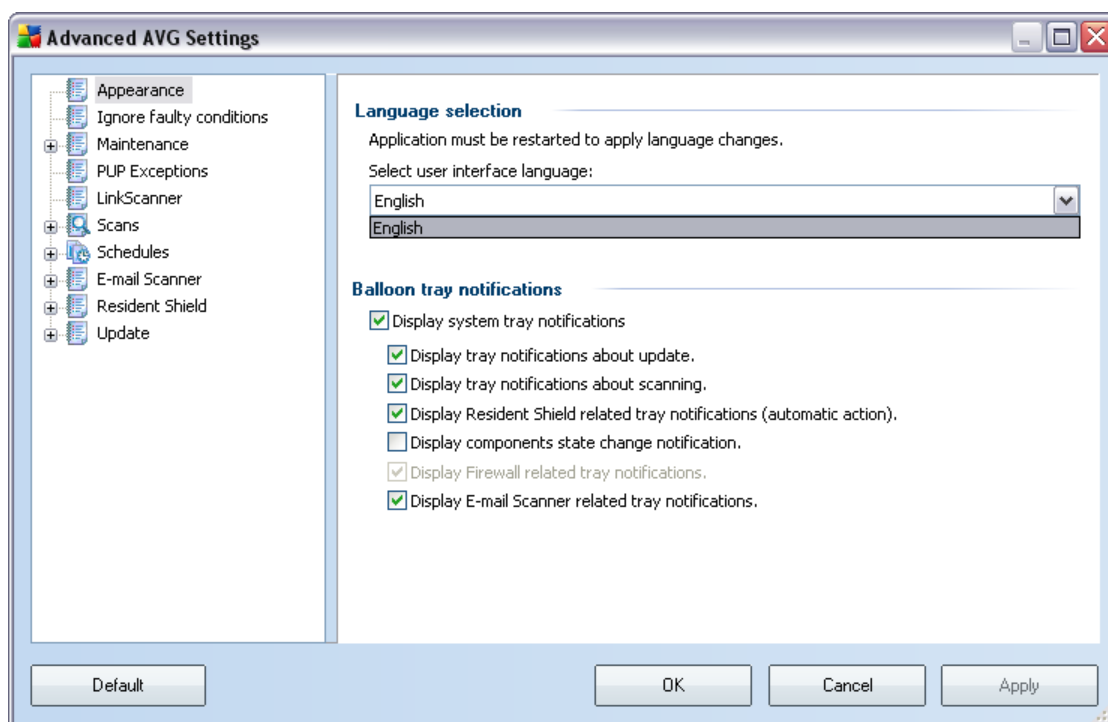
Language selection

AVG 8.0 Free is available in English only. If you feel you would like to have AVG localized to your mother language, please visit the AVG website (www.avg.com) for information on AVG 8.0 purchase options.

Balloon tray notifications

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

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

- ***Display system tray notifications*** - by default, this item is checked (*switched on*), and notifications are displayed. Uncheck this item to completely turn off the display of all balloon notifications. When turned on, you can further select what specific notifications should be displayed:

    - ○ ***Display tray notifications about [update](#)*** - decide whether information regarding AVG update process launch, progress, and finalization should be displayed;

    - ○ ***Display tray notifications about [scanning](#)*** - decide whether information upon automatic launch of the scheduled scan, its progress and results should be displayed;

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

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

    - ○ ***Display E-mail Scanner related tray notifications*** - decide whether information upon scanning of all incoming and outgoing e-mail messages should be displayed.

8.2. Ignore Faulty Conditions

In the *Ignore faulty components conditions* dialog you can tick those components that you do not want to get informed about:
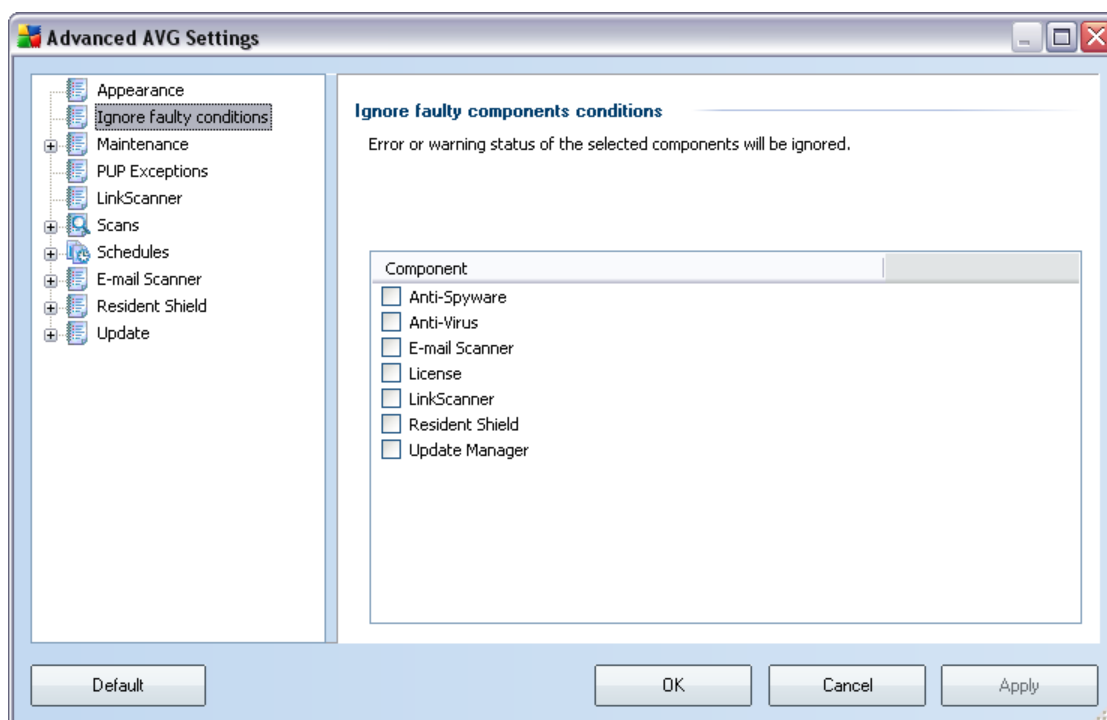
By default, no component is selected in this list. It means that if any component get to an error status, you will be informed about it immediately via:

- **system tray icon** - while all parts of AVG are working properly, the icon is displayed in four colors; however, if an error occurs, the icons switches to grey color with a red exclamation mark,

- text description of the existing problem in the **Security Status Info** section of the AVG main window

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

displayed in grey color, the icon cannot actually report any possible further error that might appear.

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

8.3. Maintenance

The **Maintenance** item opens the editing interface where you can set up ***Virus Vault*** maintenance parameters:

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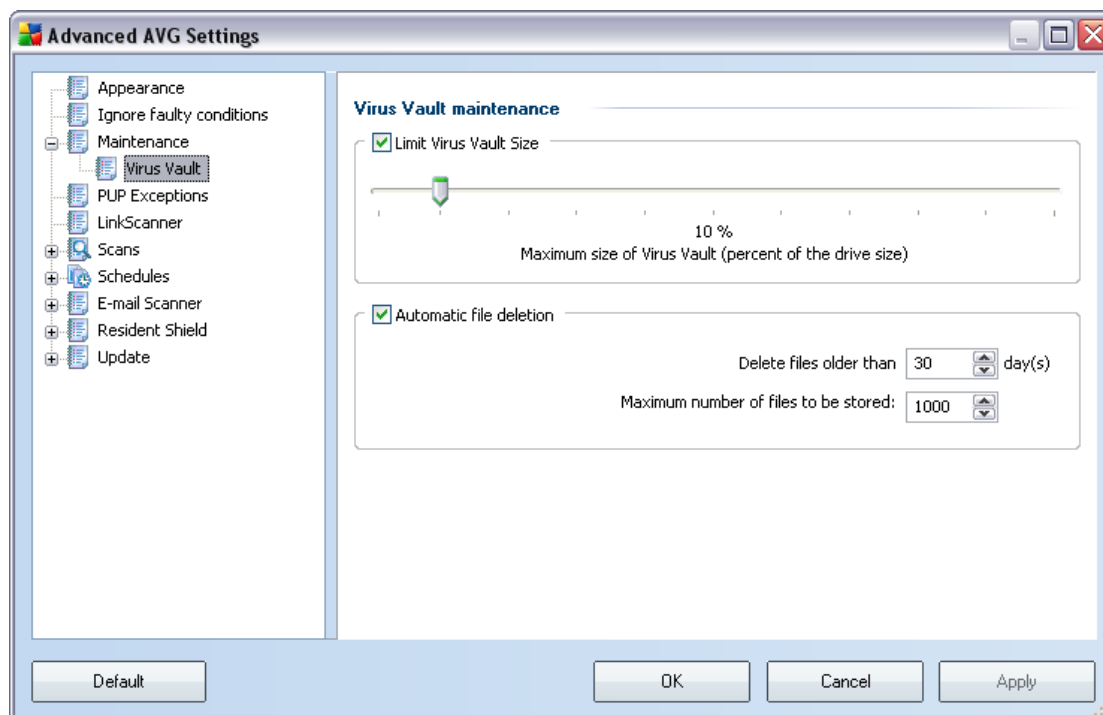
The **Virus Vault maintenance** dialog allows you to define several parameters regarding the administration of objects stored in the ***Virus Vault***:

- **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**)

8.4. PUP Exceptions

AVG is able to analyze and detect executable applications or DLL libraries that could be potentially unwanted within the system. In some cases the user may wish to keep certain unwanted programs on the computer, (programs that were installed on purpose). Some programs, especially free ones, include adware. Such adware might be detected and reported by AVG as a **potentially unwanted program**. If you wish to keep such a program on your computer, you can define it as a potentially unwanted program exception:
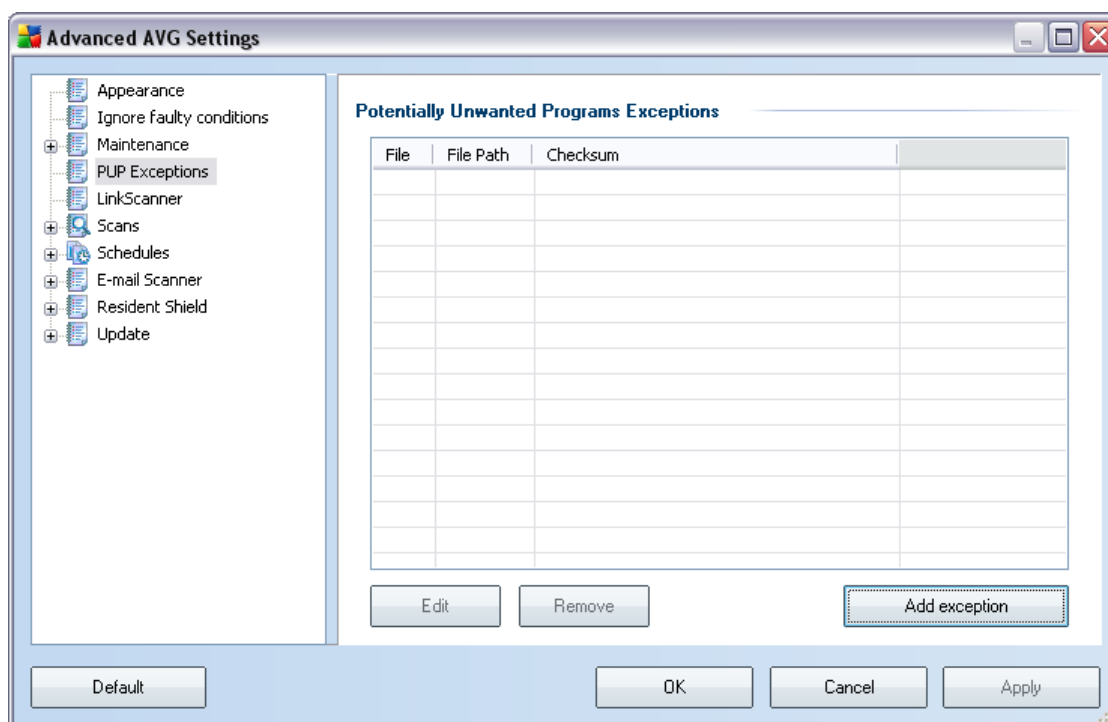
The **Potentially Unwanted Programs Exceptions** dialog displays a list of already defined and currently valid exceptions from potentially unwanted programs. You edit, delete, or add new exception.

Control buttons

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

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

- ***Add exception*** - open an editing dialog where you can define parameters of the new exception to be created:
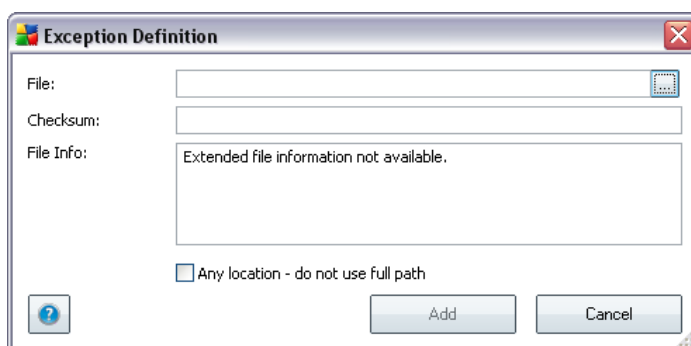
- o ***File*** - type the full path to the file that you want to mark as an exception

- o ***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.

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

- o ***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

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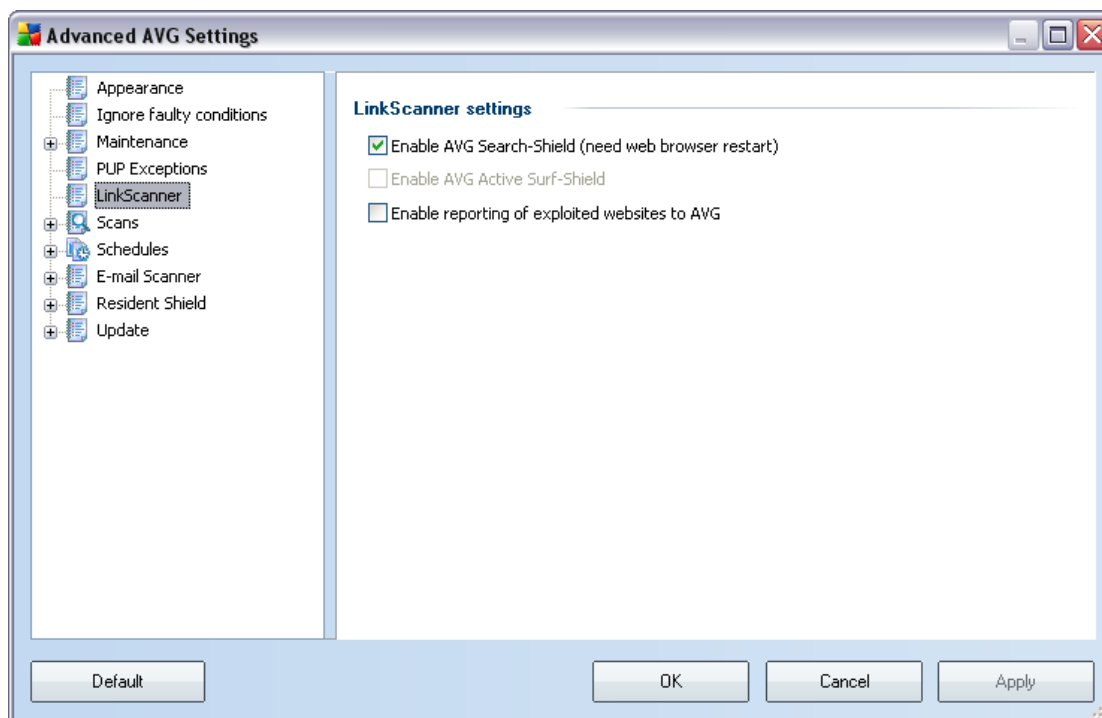
The **LinkScanner settings** dialog allows you to switch on/off the two elementary features of the **LinkScanner**:

- **Enable AVG Search Shield** - (*on by default*): advisory notifying icons on searches performed in Google, Yahoo or MSN having checked ahead the content of sites returned by the search engine. The browsers supported are Internet Explorer and Firefox.

- *Enable AVG Active Surf-Shield - unfortunately, this option is deactivated with* ***AVG 8.0 Free****; if you are interested in further and extended functionality within AVG 8.0 full products, please visit the* AVG website (www.avg.com) *for information on AVG 8.0 purchase options.*

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

8.6. Scans

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

- **_Scan Whole Computer_** - standard predefined scan of the entire computer

- **_Scan Specific Files or Folders_** - standard predefined scan of selected areas of your computer

- **_Scanning in Windows Explorer_** - specific scanning of a selected object directly from the Windows Explorer environment

8.6.1. Scan Whole Computer

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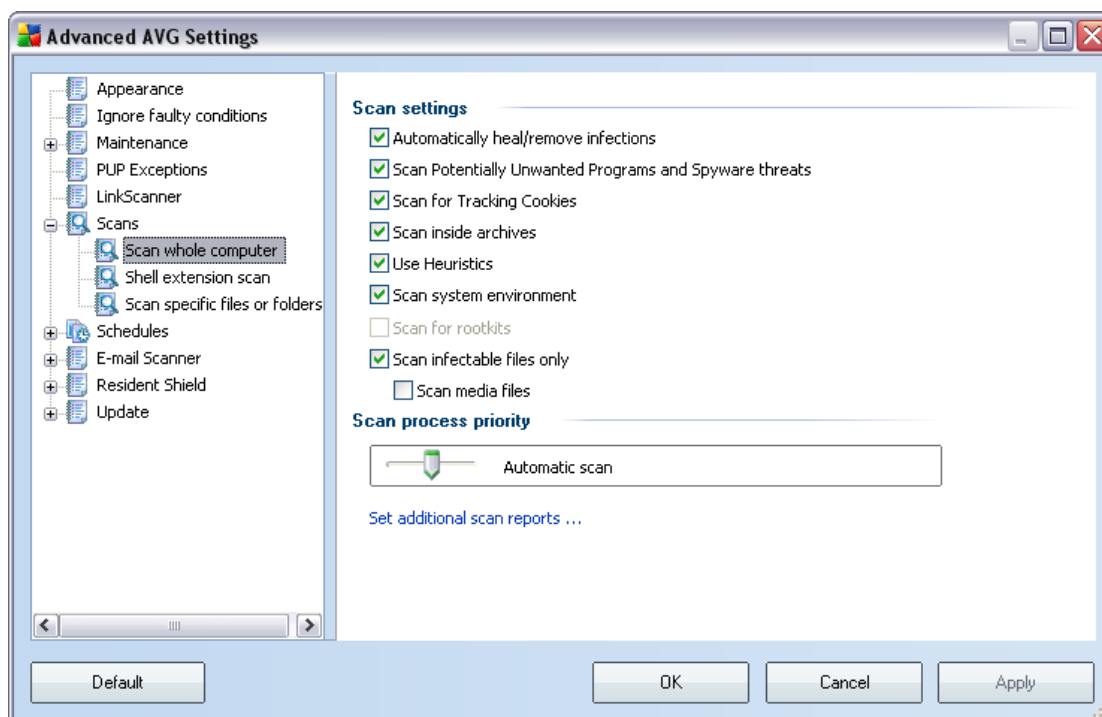
Scan settings

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

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

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

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

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

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

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

- *Scan for rootkits - - unfortunately, this option is deactivated with* **AVG 8.0 Free***; if you are interested in further and extended functionality within AVG 8.0 full products, please visit the* AVG website (www.avg.com) *for information on AVG 8.0 purchase options*;

- **Scan infectable files only** - with this option switched on, files that cannot get infected will not be scanned. These can be for instance some plain text files, or some other non-executable files.

Scan process priority

Within the **Scan process priority** section you can further specify the desired scanning speed dependent on system resource usage. By default, this option value is

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

Set additional scan reports ...

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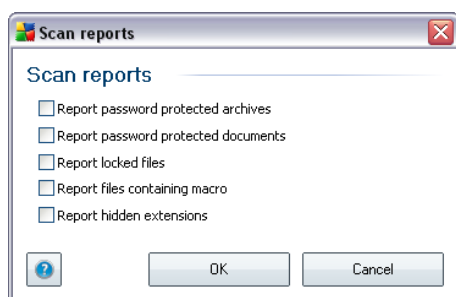
8.6.2. Shell Extension Scan

Similar to the previous ***Scan whole computer*** item, this item named ***Shell extension scan*** also offers several options for editing the scan predefined by the software vendor. This time the configuration is related to scanning of specific objects launched directly from the Windows Explorer environment (*shell extension*), see chapter ***Scanning in Windows Explorer***:
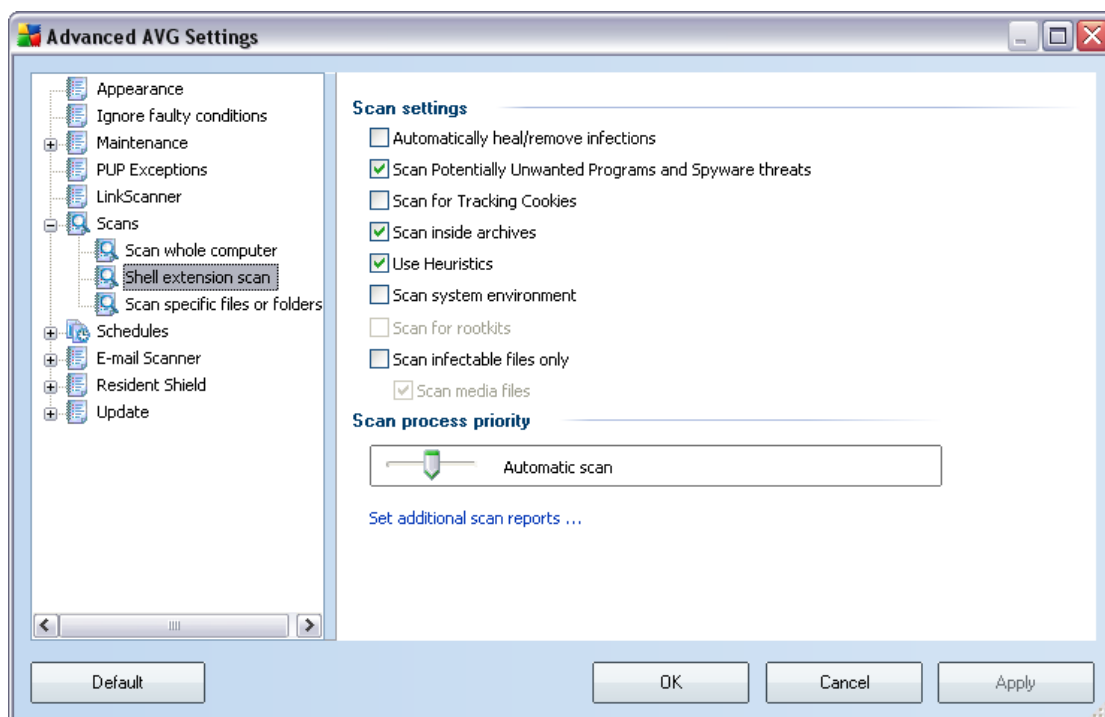
The list of parameters is identical to those available for the ***Scan of the whole computer*** . However, the default settings differ: with the **Scan of the Whole Computer** most parameters are selected while for the **Shell extension scan** (***Scanning in Windows Explorer***) only the relevant parameters are switched on.

8.6.3. Scan Specific Files or Folders

The editing interface for **Scan specific files or folders** is identical to the ***Scan Whole Computer*** editing dialog. All configuration options are the same; however, the default settings are more strict for the ***Scan of the whole computer***:
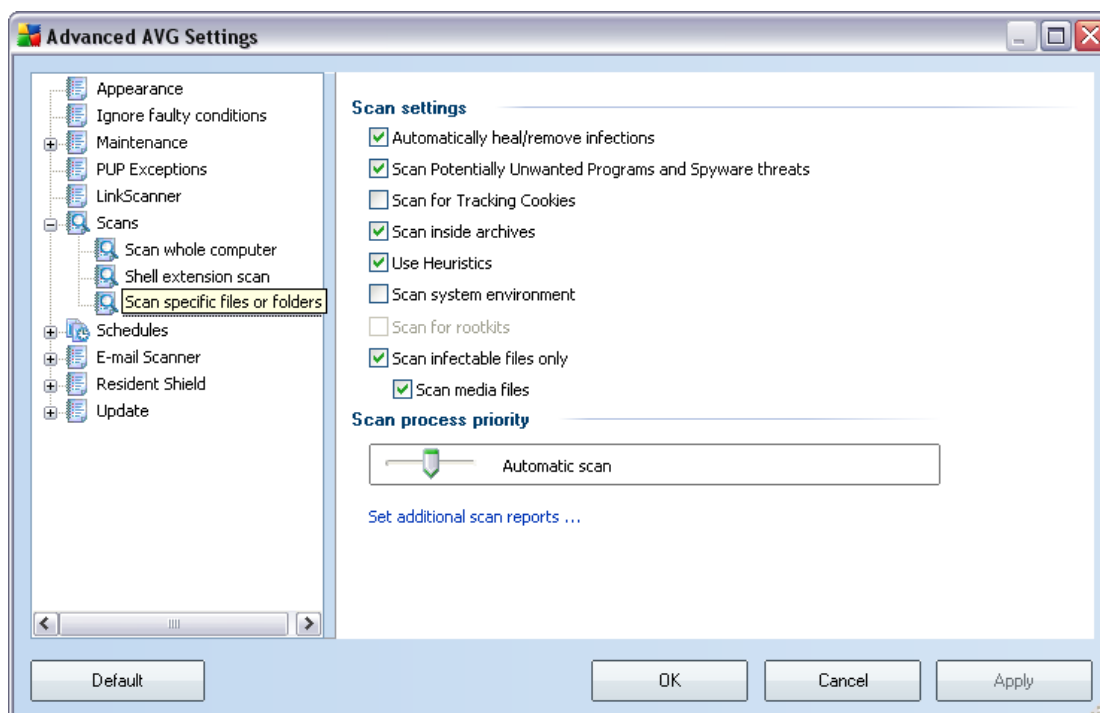
All parameters set up in this configuration dialog apply only to the areas selected for scanning with the ***Scan of specific files or folders***!

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

8.7. Schedules

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

- Whole computer scan schedule

- Virus database update schedule

- Program update schedule

8.7.1. Scheduled Scan

Parameters of the scheduled (default) scan can be edited on the three following tabs. Note that with **AVG 8.0 Free** no additional schedules can be created. Therefore if you are interested in further and extended functionality within AVG 8.0 full products,

please visit the AVG website (www.avg.com) for information on AVG 8.0 purchase options.
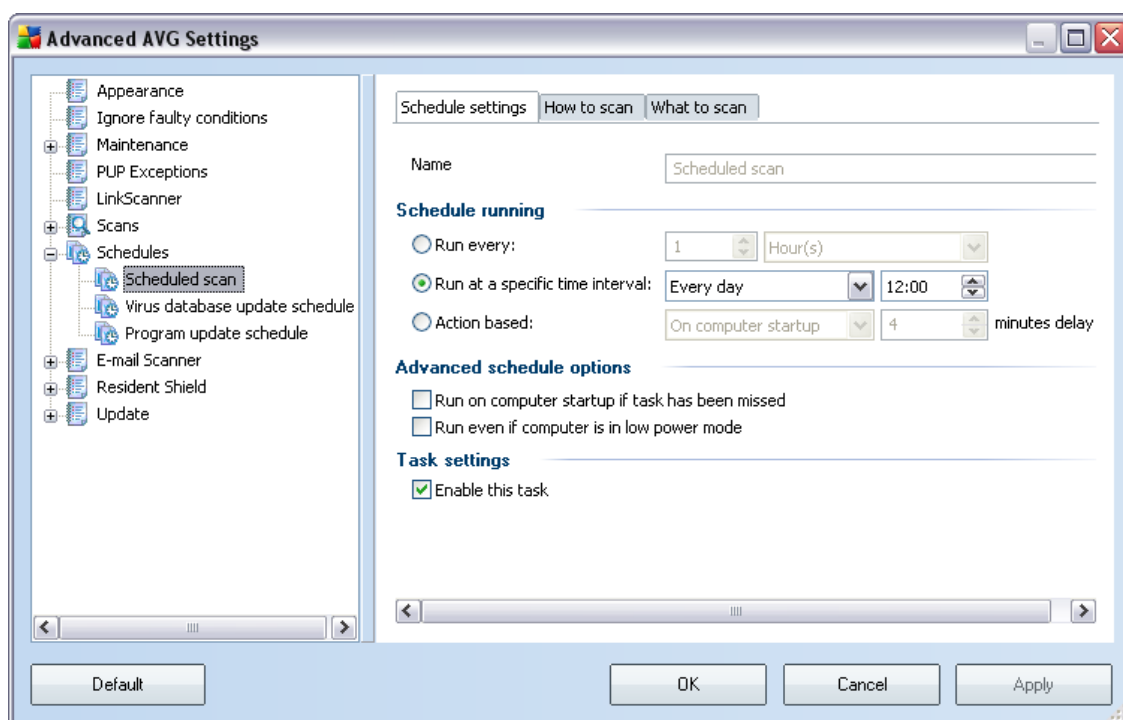
In this dialog you can define the following parameters of the scan:

- *Name - unfortunately, this option is deactivated with **AVG 8.0 Free***; *the Scan of a whole computer is the only scanning you can schedule. If you are interested in further and extended functionality within AVG 8.0 full products, please visit the* AVG website (www.avg.com) *for information on AVG 8.0 purchase options.*

- **Schedule running** - specify the intervals for the scheduled scan launch.

  - ➢ **Run every** - run the scan every 'n' number of hours. E.g. every 4 hours.

  - ➢ **Run at specific time interval** - select **Every day**, or select a specific day of the week (*however, it is recommended to run the scan daily!*), and specify what time of day the scan should start.

  - ➢ **Action based** - run the scan on computer startup.

Note: More comprehensive options are available in full versions of AVG.

- ***Advanced schedule options***

  - ➢ ***Run on computer startup if task has been missed*** - if the scan cannot run at the scheduled time/interval, then it will run the next time the computer restarts.

  - ➢ ***Run even if computer is in low power mode*** - this option applies to battery powered computers such as notebooks. The default action is for AVG to postpone scanning when the computer's power resources are low.

- ***Task settings*** - in the section you can uncheck the ***Enable this task*** item to simply deactivate the scheduled test. ***Not recommended***.

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

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

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

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

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

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

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

- *Scan for rootkits - - unfortunately, this option is deactivated with* **AVG 8.0 Free**; *if you are interested in further and extended functionality within AVG 8.0 full products, please visit the* AVG website (www.avg.com) *for information on AVG 8.0 purchase options*;

  - **Scan infectable files only** - (*switched off, by default*): with this option switched on, scanning will not be applied to files that cannot get infected. These can be for instance some plain text files, or some other non-executable files.

Within the **Scan process priority** section you can further specify the desired scanning speed dependent on system resource usage. By default, this option is set to the medium level of automatic resource usage. If you want the scanning to run faster, it will take less time but the system resources usage will increase significantly during the scan, and will slow down your other activities on the PC (*this option can be used*

when your computer is switched on but nobody is currently working on it). On the other hand, you can decrease the system resources usage by extending the scanning duration.

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

Click the **Additional scan settings ...** to open a new **Computer shutdown options** dialog where you can decide whether the computer should be shut down automatically once the running scanning process is over. Having confirmed this option (**Shutdown computer upon scan completion**), a new option activates that allows the computer to shut down even if it is currently locked (**Force shutdown is computer is locked**).
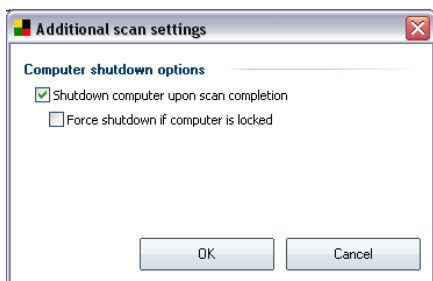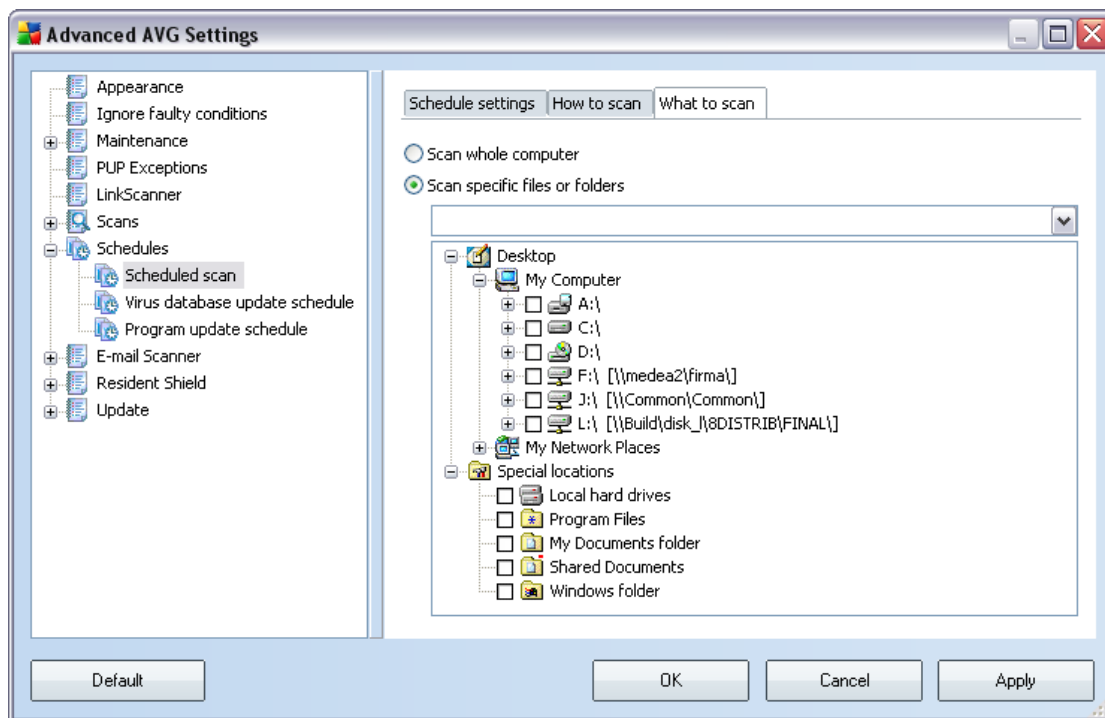
On the **What to scan** tab you can define whether you want to schedule scanning of the whole computer or scanning of specific files or folders. If you select scanning of specific files or folders, in the bottom part of this dialog the displayed tree structure activates and you can specify the folders to be scanned.

8.7.2. Virus Database Update Schedule
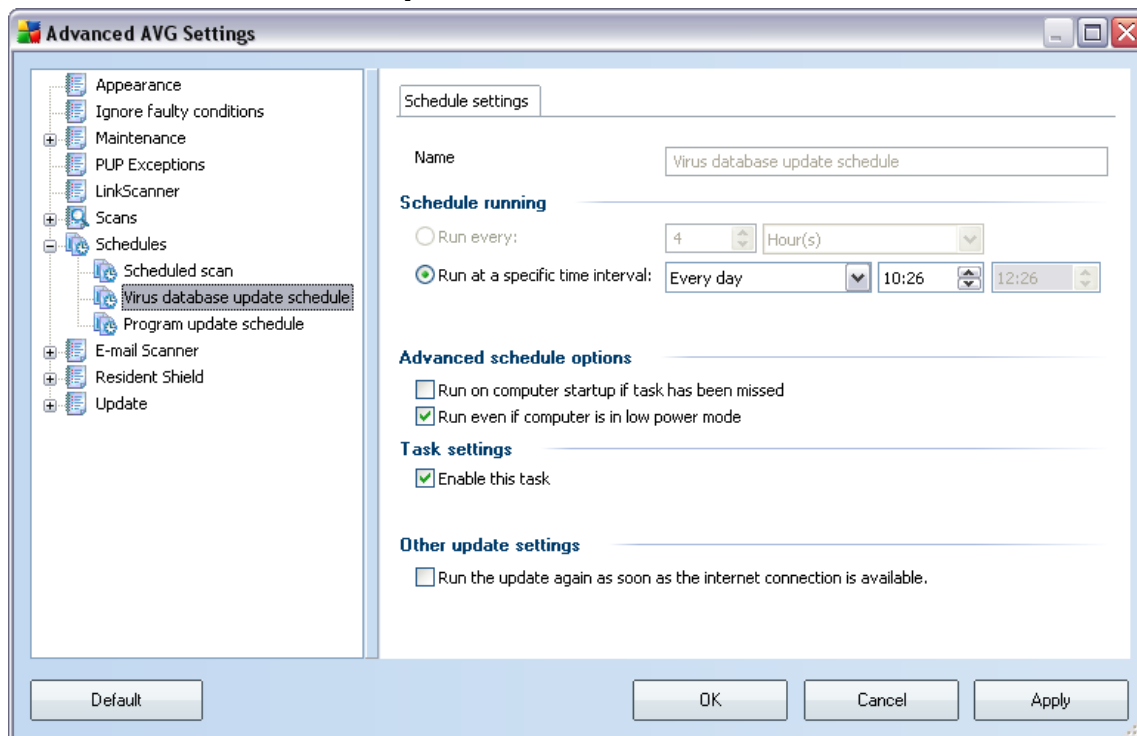
The basic virus database update scheduling is covered within the **_Update Manager_** component. Within this dialog you can set up some detailed parameters of the virus database update schedule:

- **_Schedule running_** - specify the time intervals for the newly scheduled virus database update launch. The timing can either be defined by the repeated update launch after a certain period of time (**_Run every ..._**) or by defining an exact date and time (**_Run at specific time ..._**), or possibly by defining an event that the update launch should be associated with (**_Action based on computer startup_**).

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

- **_Task settings_** - in this section you can uncheck the **_Enable this task_** item to simply deactivate the scheduled virus database update temporarily, and switch it on again as the need arises.

- **Other update settings** - check this option to make sure than if the internet connection gets corrupted and the update process fails, it will be launched again immediately after the internet connection is restored.

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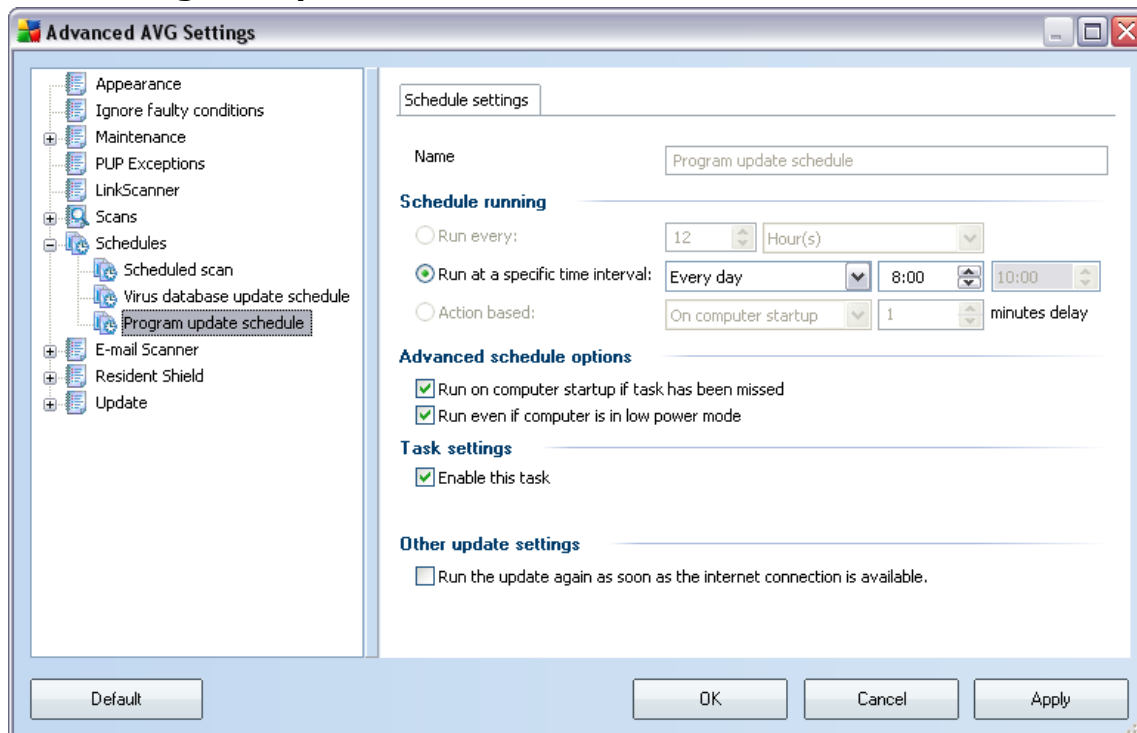
- **Schedule running** - specify the time intervals for the newly scheduled program update launch. The timing can either be defined by the repeated update launch after a certain period of time (**Run every ...**) or by defining an exact date and time (**Run at specific time ...**), or possibly by defining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

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

- **Task settings** - in this section you can uncheck the **Enable this task** item to simply deactivate the scheduled program update temporarily, and switch it on again as the need arises.

- **Other update settings** - check this option to make sure than if the internet connection gets corrupted and the update process fails, it will be launched again immediately after the internet connection is restored.

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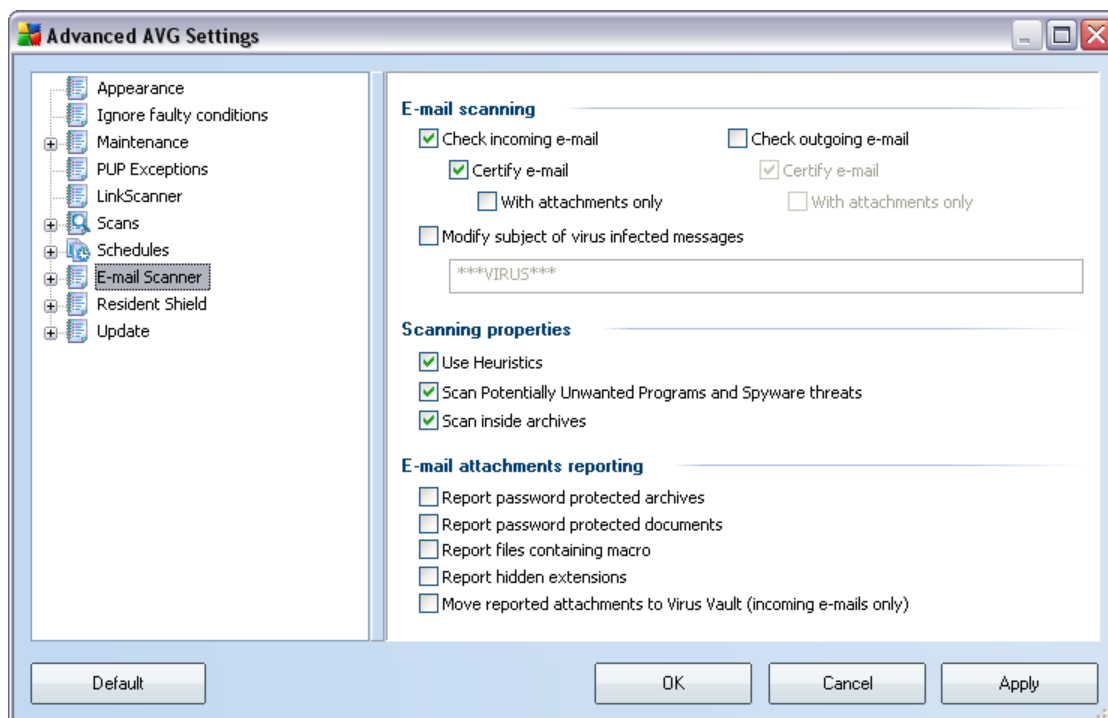
The **E-mail Scanner** dialog is divided into three sections:

- **E-mail scanning** - in this section select whether you want to scan the incoming/outgoing e-mail messages and whether all e-mails should be certified or only e-mails with attachments (e-*mail virus-free certification is not supported in HTML/RTF format*). Additionally you can choose if you want AVG to modify the subject for messages that contain potential viruses. Tick the **Modify subject of virus infected messages** checkbox and change the text respectively (*default value is ***VIRUS****).

- **Scanning properties** - specify whether the <u>heuristic analysis</u> method should be used during scanning (**Use heuristic**), whether you want to check for the presence of <u>potentially unwanted programs</u> (**Scan Potentially Unwanted Programs**), and whether archives should be scanned too (**Scan inside archives**).

- **E-mail attachments reporting** - specify whether you wish to be notified via e-mail about password protected archives, password protected documents, macro containing files and/or files with hidden extension detected as an attachment of the scanned e-mail message. If such a message is identified during scanning, define whether the detected infectious object should be moved to the **_Virus Vault_**.

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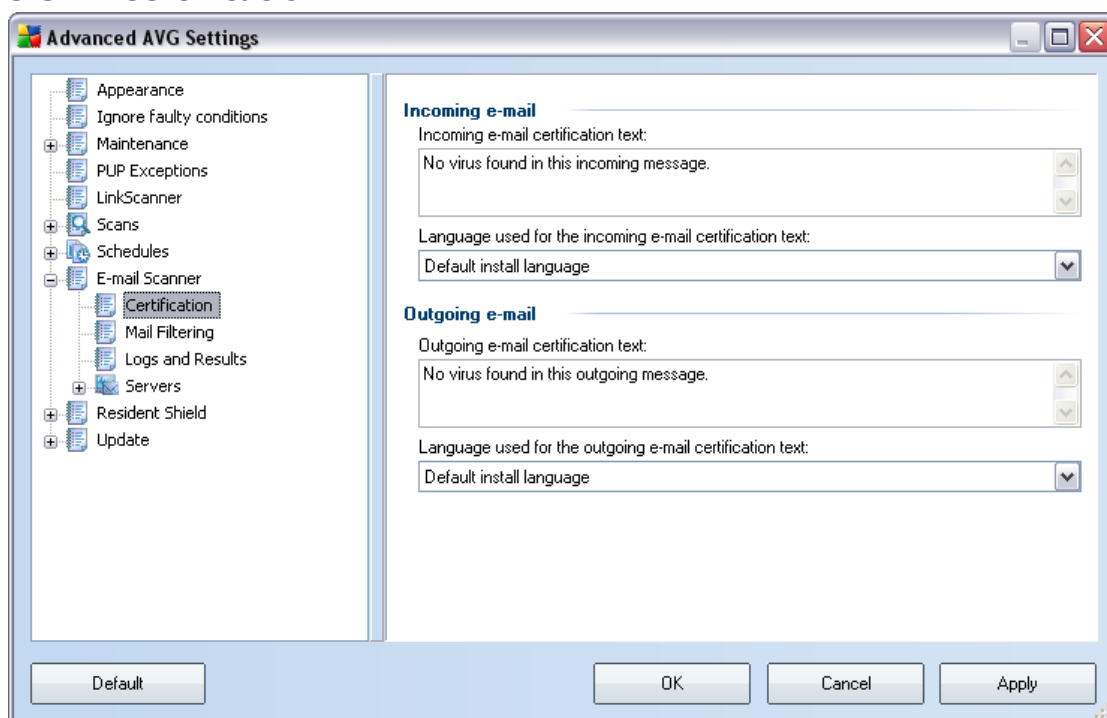
In the **Certification** dialog you can specify exactly what text the certification note should contain, and in what language. This should be specified separately for **Incoming mail** and **Outgoing mail**.

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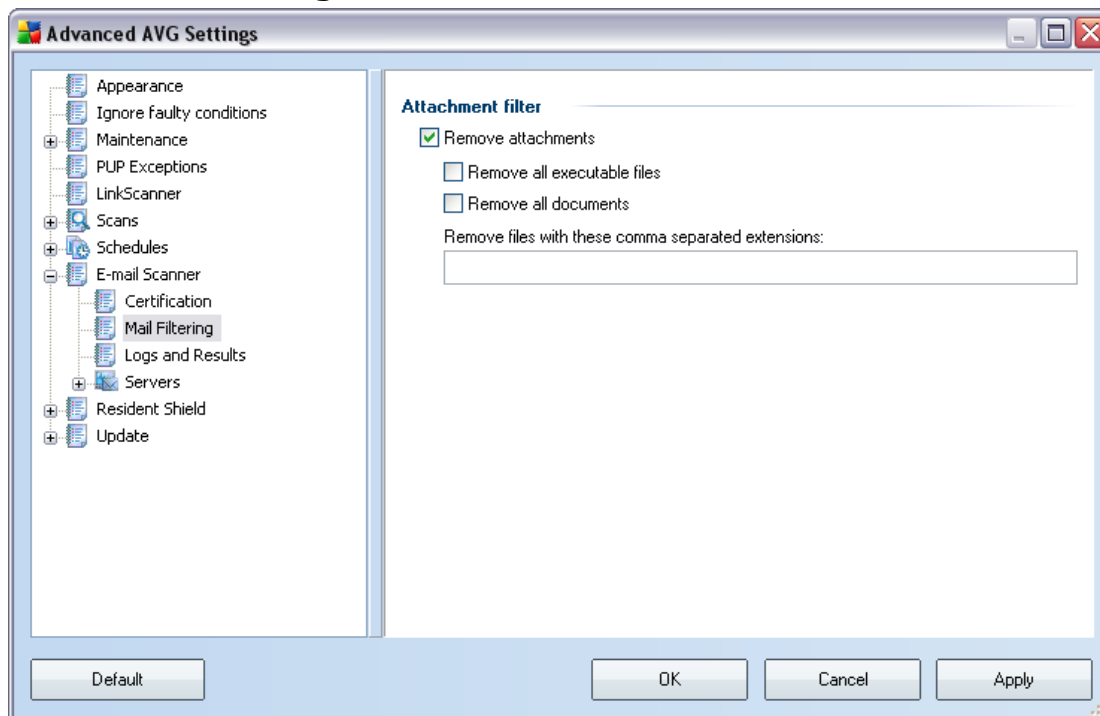
The **Attachment filter** dialog allows you to set up parameters for e-mail messages attachment scanning. By default, the **Remove attachments** option is switched off. If you decide to activate it, all e-mail message attachments detected as infectious or potentially dangerous will be removed automatically.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

- **Remove all executable files** - all *.exe files will be deleted

- **Remove all documents** - all *.doc files will be deleted

- **Remove files with these extensions** - will remove all files with the defined extensions

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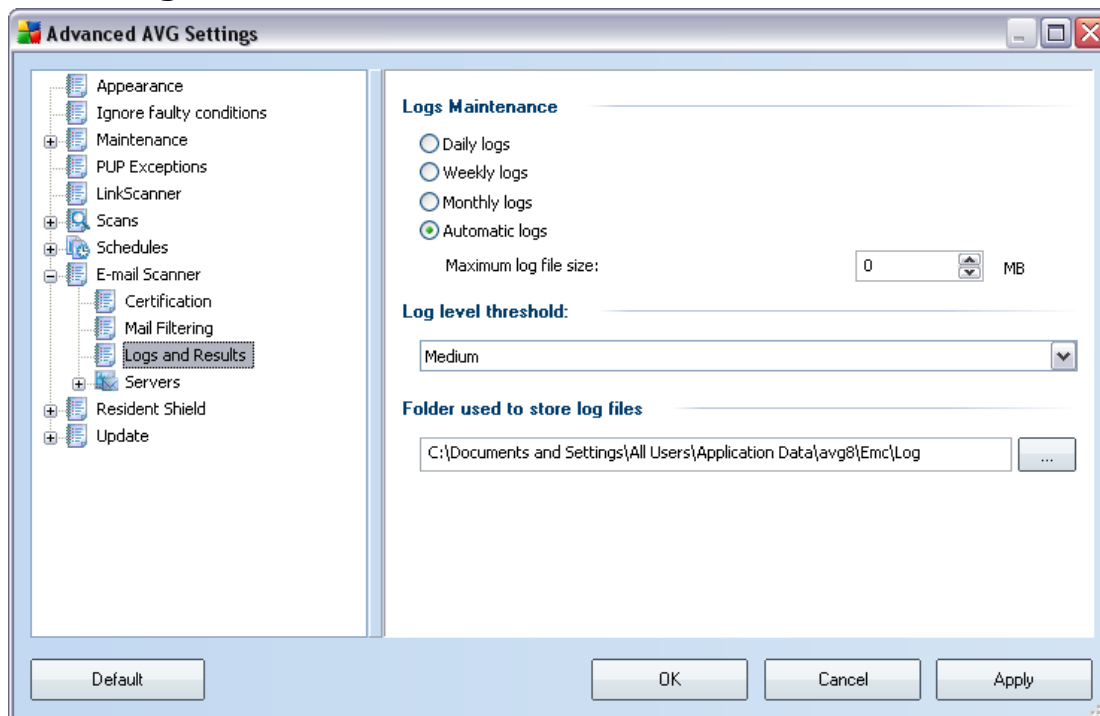
The dialog opened via the **Logs and Results** navigation item allows you to specify parameters for e-mail scanning results maintenance. The dialog is divided into several sections:

- **Logs Maintenance** - define whether you want to log e-mail scanning information daily, weekly, monthly, ... ; and also specify the maximum size of the log file (*in MB*)

- **Log level threshold** - the medium level is set up by default - you can select a lower level (*logging elementary connection information*) or higher level (*logging of all traffic*)

- **Folder used to store log files** - define where the log file should be located

8.8.4. Servers

In the **Servers** section you can edit parameters of the **E-mail Scanner** component servers, or set up a new server for incoming or outgoing email.
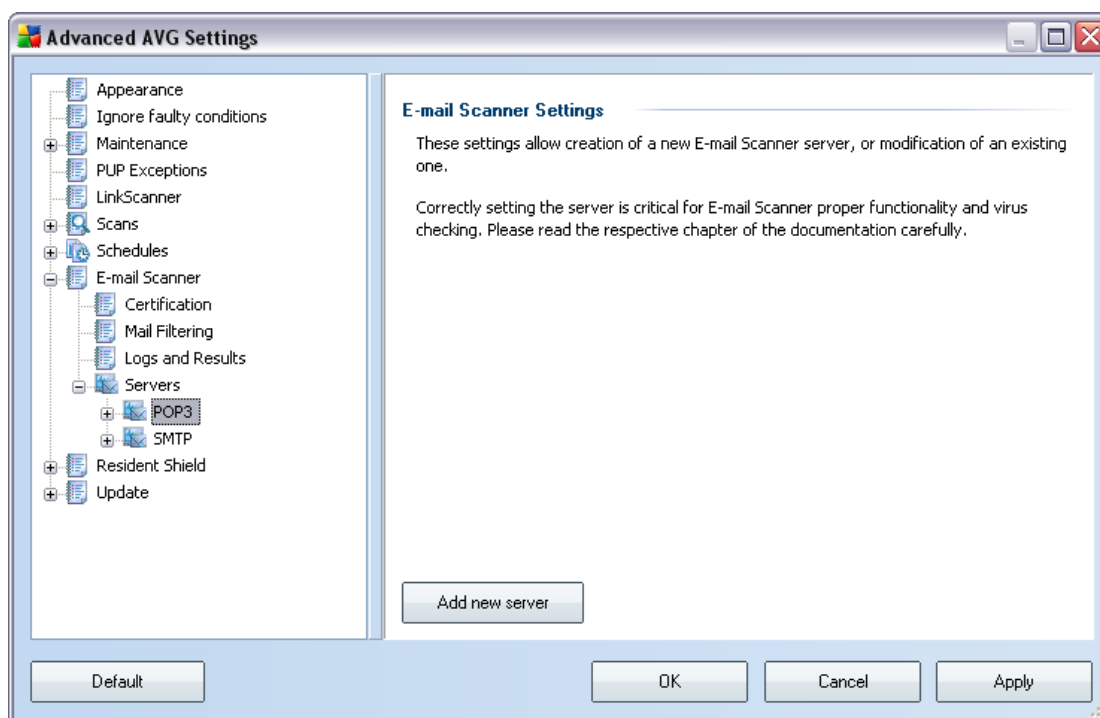
To add a new server, use the **Add new server** button in the left hand bottom corner of this dialog. Alternatively you can just right click your mouse over the POP3 (*incoming mail*) or SMTP item (*outgoing mail*) to open the context menu and select **New server**, and define its name and type in the newly opened dialog window:
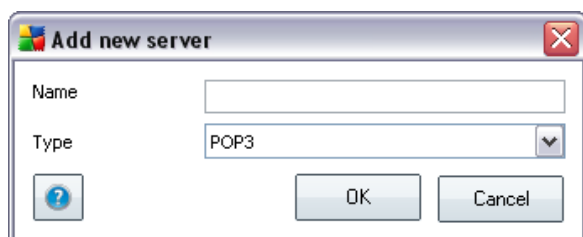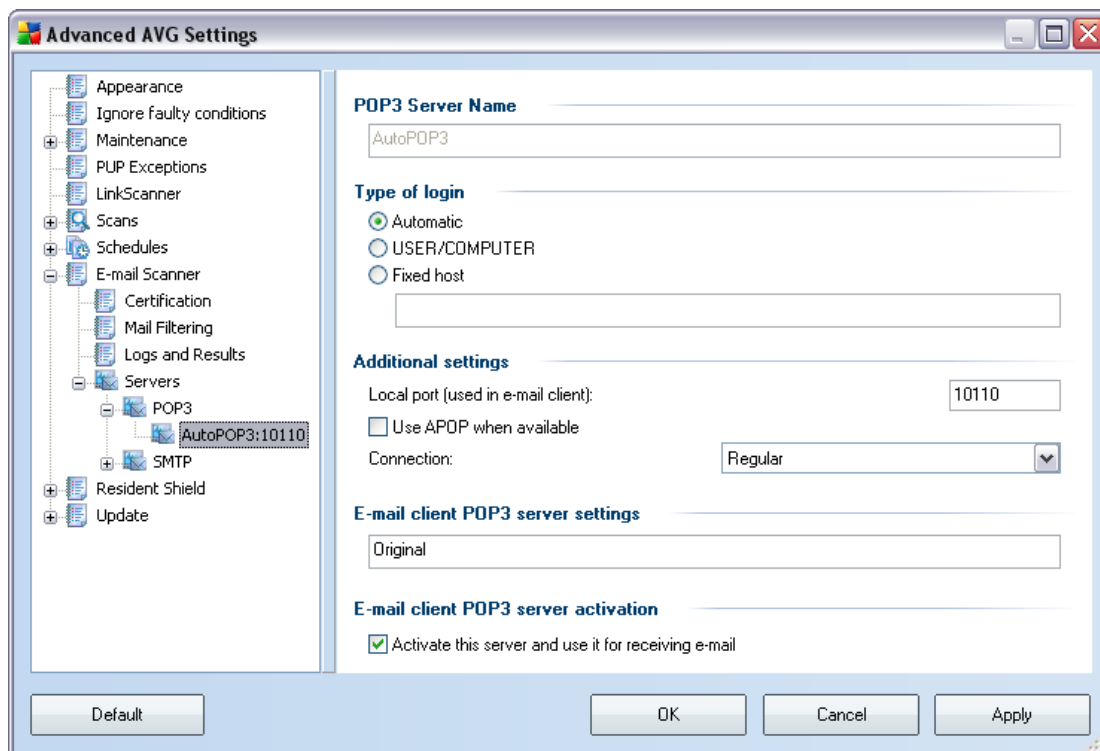
In this dialog (opened via **Servers / POP3**) you can set up a new **E-mail Scanner** server using the POP3 protocol for incoming mail:

- *POP3 Server Name - unfortunately, this option is deactivated with **AVG 8.0 Free***; *if you are interested in further and extended functionality within AVG 8.0 full products, please visit the* AVG website (www.avg.com) *for information on AVG 8.0 purchase options.*

- **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;

  - **USER/COMPUTER** - the simplest and the most frequently used method for determining the destination mail server is the proxy method. To use this method, specify the name or address (or also the port) as part of the login user name for the given mail server, separating them with the / character. For example, for the account user1 on the server

pop.acme.com and the port 8200 you would use
user1/pop.acme.com:8200 for the login name;

o **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:

o **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;

o **Use APOP when available** - this option provides more secure mail
server login. This makes sure that the **E-mail Scanner** uses an
alternative method of forwarding the user account password for login,
sending the password to the server not in an open, but in an encrypted
format using a variable chain received from the server. Naturally, this
feature is available only when the destination mail server supports it;

o **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.

o **E-mail client POP3 server settings** - provides brief information on the
configuration settings required to correctly configure your e-mail client
(so that the **E-mail Scanner** will check all incoming mail). This is a
summary based on the corresponding parameters specified in this dialog
and other related dialogs.

o **E-mail client POP3 server activation** (*switched on, by default*) - if
needed, allows you to temporarily switch off the server with the above
specified settings.

In this dialog (opened via **Servers / SMTP**) you can set up a new **E-mail Scanner** server using the SMTP protocol for outgoing mail:
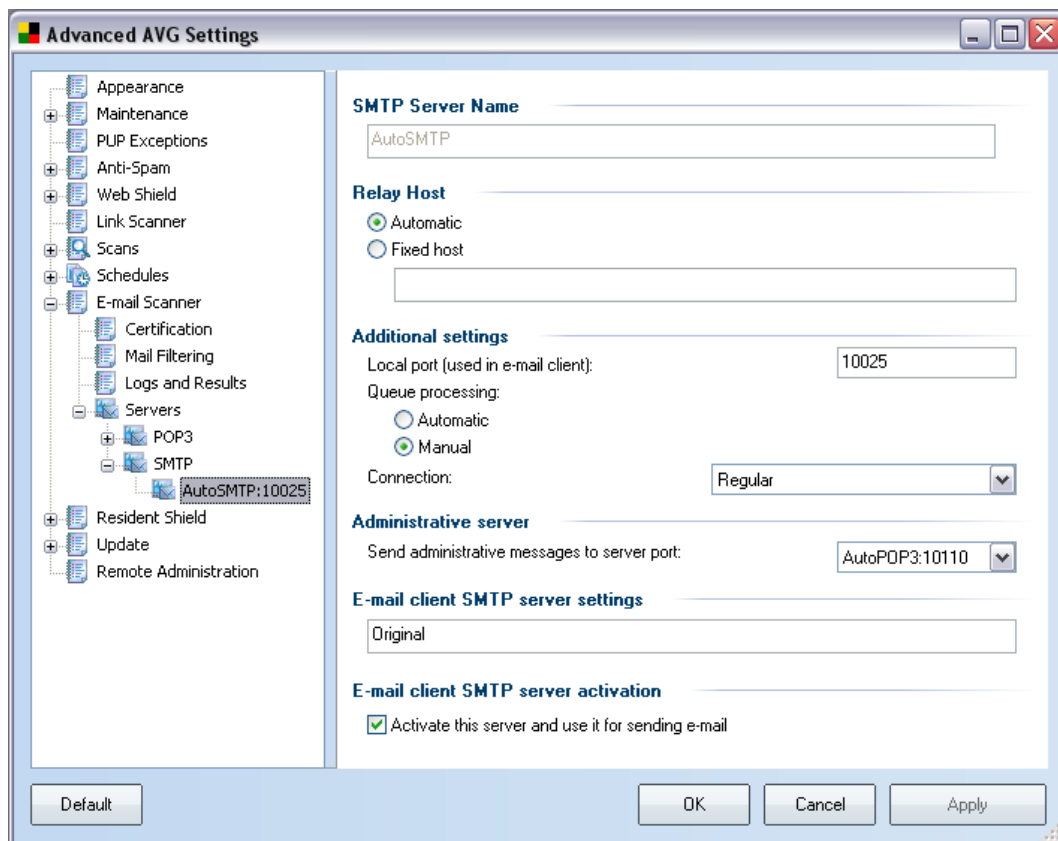
- *SMTP Server Name - unfortunately, this option is deactivated with **AVG 8.0 Free**; if you are interested in further and extended functionality within AVG 8.0 full products, please visit the* AVG website (www.avg.com) *for information on AVG 8.0 purchase options.*

    - **Relay Host** - defines the method for determining the mail server used for outgoing mail:

        - o **Automatic** - login will be carried out automatically, according to your e-mail client settings;

        - o **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:

  o **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;

  o **Queue processing** - determines the behavior of the **E-mail Scanner** when processing the requirements for sending mail messages:

    ➢ Automatic - the outgoing mail is immediately delivered (sent) to the target mail server

    ➢ Manual - the message is inserted into the queue of outgoing messages and sent later

  o **Connection** - in this drop-down menu, you can specify which kind of connection to use (regular/SSL/SSL default). If you choose SSL connection, the data sent is encrypted without the risk of being traced or monitored by a third party. This feature is available only when the destination mail server supports it.

- **Administrative server** - shows the number of the port of the server that will be used for the reverse delivery of administration reports. These messages are generated, for example, when the target mail server rejects the outgoing message or when this mail server is not available.

- **E-mail client SMTP server settings** - provides information on how to configure the client mail application so that outgoing mail messages are checked using the currently modified server for checking the outgoing mail. This is a summary based on the corresponding parameters specified in this dialog and other related dialogs.

- **E-mail client SMTP server activation** (*switched on, by default*) - if needed, allows you to temporarily switch off the server with the above specified settings.

8.9. Resident Shield

The **_Resident Shield_** component performs live protection of files and folders against viruses, spyware and other malware.
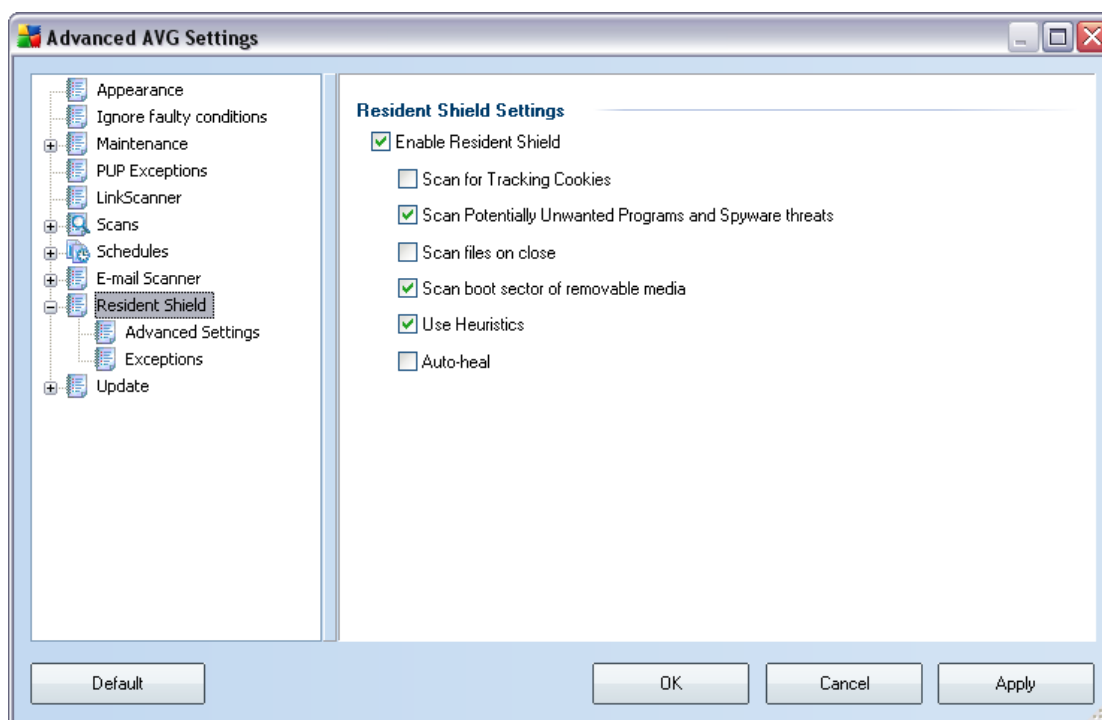
In the **Resident Shield Settings** dialog you can activate or deactivate the **_Resident Shield_** protection completely by checking/unchecking the **Enable Resident Shield** item (*this option is switched on by default*). In addition you can select which **_Resident Shield_** features should be activated:

- **_Scan for Tracking Cookies_** - this parameter defines that cookies should be detected during scanning. (*HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts*)

- **_Scan Potentially Unwanted Programs and Spyware Threats_** - (*switched on by default*) scanning for potentially unwanted programs (*executable applications that can behave as various types of spyware or adware*)

- **_Scan files on close_** - on-close scanning ensures that AVG scans active objects (e.g. applications, documents …) when they are being opened, and

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

- **Scan boot sector of removable media** - (*switched on by default*)

- **Use Heuristics** - (*switched on by default*) [heuristic analysis] will be used for detection (*dynamic emulation of the scanned object's instructions in a virtual computer environment*)

- **Auto-heal** - any detected infection will be healed automatically if there is a cure available

8.9.1. Advanced Settings

In the **Files scanned by the Resident Shield** dialog it is possible to configure which files will be scanned (*by specific extensions*):
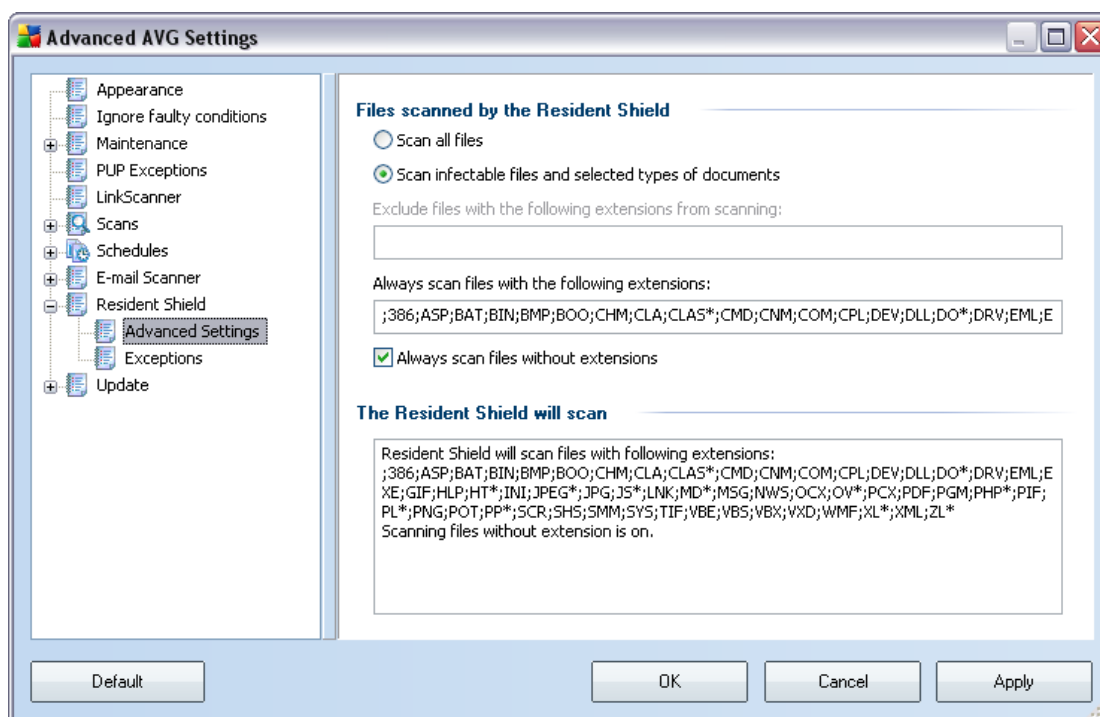
Decide whether you want all files to be scanned or just infectable files - if so, you can further specify a list of extensions defining files that should be excluded from scanning, and also a list of file extensions defining files that must be scanned under all circumstances.

8.9.2. Exceptions
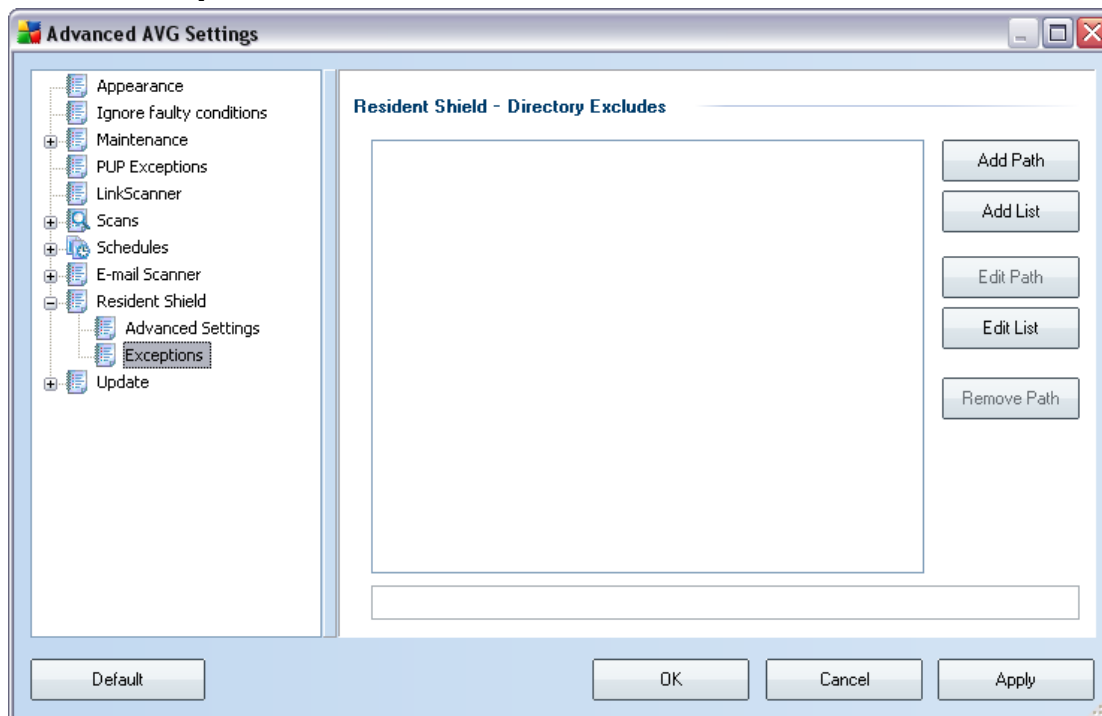
The ***Resident Shield - Directory Excludes*** dialog offers the possibility of defining folders that should be excluded from the **_Resident Shield_** scanning. If this is not essential, we strongly recommend not excluding any directories! If you decide to exclude a folder from **_Resident Shield_** scanning, mark the **Use excludes in Resident Shield** check box. The new settings will only take effect after the computer is restarted!

The dialog provides the following control buttons:

- ***Add path*** – specify directories to be excluded from the scanning by selecting them one by one from the local disk navigation tree

- ***Add list*** – allows you to enter a whole list of directories to be excluded from the **_Resident Shield_** scanning

- ***Edit path*** – allows you to edit the specified path to a selected folder

- ***Edit list*** – allows you to edit the list of folders

- ***Remove path*** – allows you to delete the path to a selected folder from the

list

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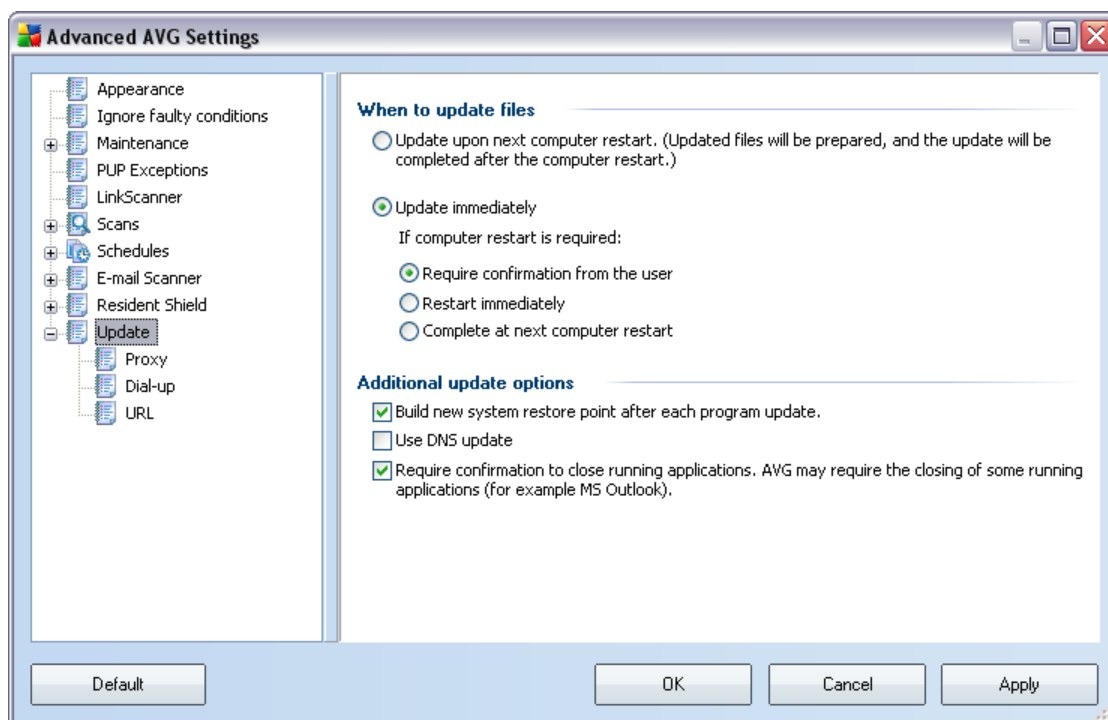
The **Update** navigation item opens a new dialog where you can specify general parameters regarding the AVG update:

When to update files

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

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

- *Require confirmation from the user* - you will be asked to approve a PC

restart needed to finalize the update process

- **Restart immediately** - the computer will be restarted automatically immediately after the update process has finished, and your approval will not be required

- **Complete at next computer restart** - the update process finalization will be postponed until the next computer restart - again, please keep in mind that this option is only recommended if you can be sure the computer gets restarted regularly, at least daily

Additional update options

- **Build new system restore point after each program update** - before each AVG program update launch, a system restore point is created. In case the update process fails and your operating system crashes you can always restore your OS in its original configuration from this point. This option is accessible via **Start / All Programs / Accessories / System tools / System Restore**, but any changes can be recommended to experienced users only! Keep this check-box ticked if you want to make use of this functionality.

- **Use DNS update** - mark this check box to confirm you want to use the update files detection method that eliminates data amount transferred between the update server and AVG client;

- **Require confirmation to close running applications item** (*switched on by default*) will help you make sure no currently running applications will be closed without your permission - if required for the update process to be finalized.

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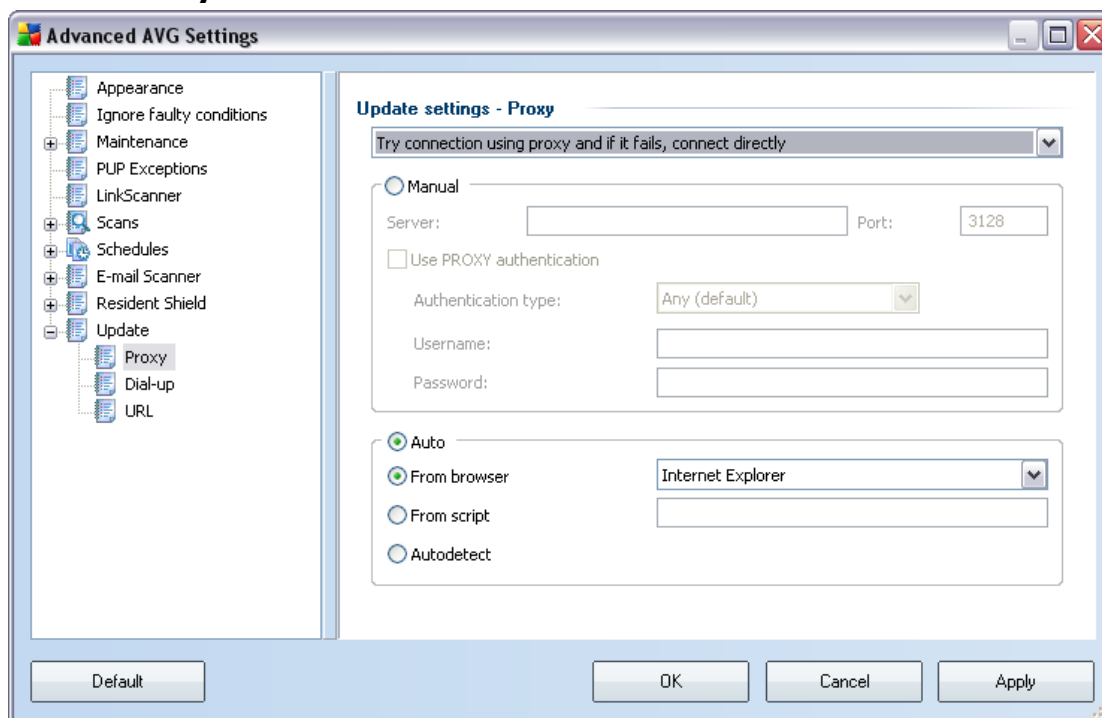
The proxy server is a stand-alone server or a service running on a PC that guarantees safer connection to the Internet. According to the specified network rules you can then access the Internet either directly or via the proxy server; both possibilities can also be allowed at the same time. Then, in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

- **Use proxy**

- **Do not use proxy server**

- **Try connection using proxy and if it fails, connect directly** - default settings

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

Manual configuration

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

- **Server** – specify the server's IP address or the name of the server

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

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

Automatic configuration

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

- **From browser** - the configuration will be read from your default internet browser (*supported browsers being Internet Explorer, Firefox, Mozilla, and Opera*)

- **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

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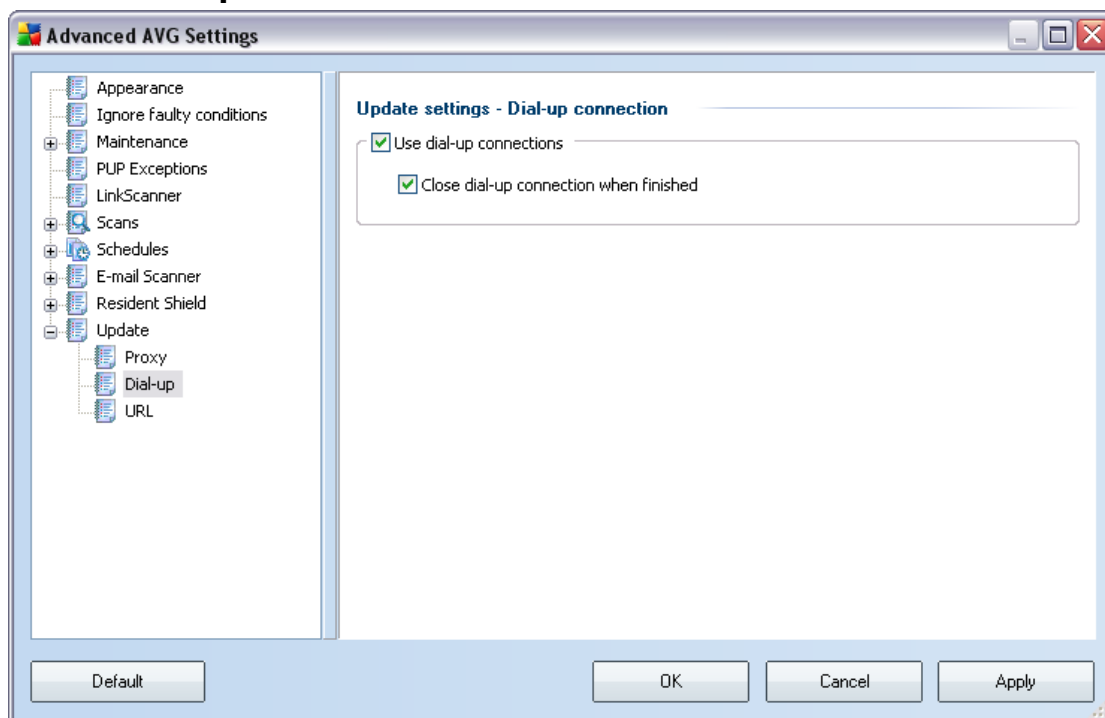
All parameters optionally defined in the *Update settings - Dial-Up connection* dialog refer to the dial-up connection to the Internet. The dialog's fields are inactive until you check the *Use dial-up connections* option that activates the fields.

8.10.3.URL
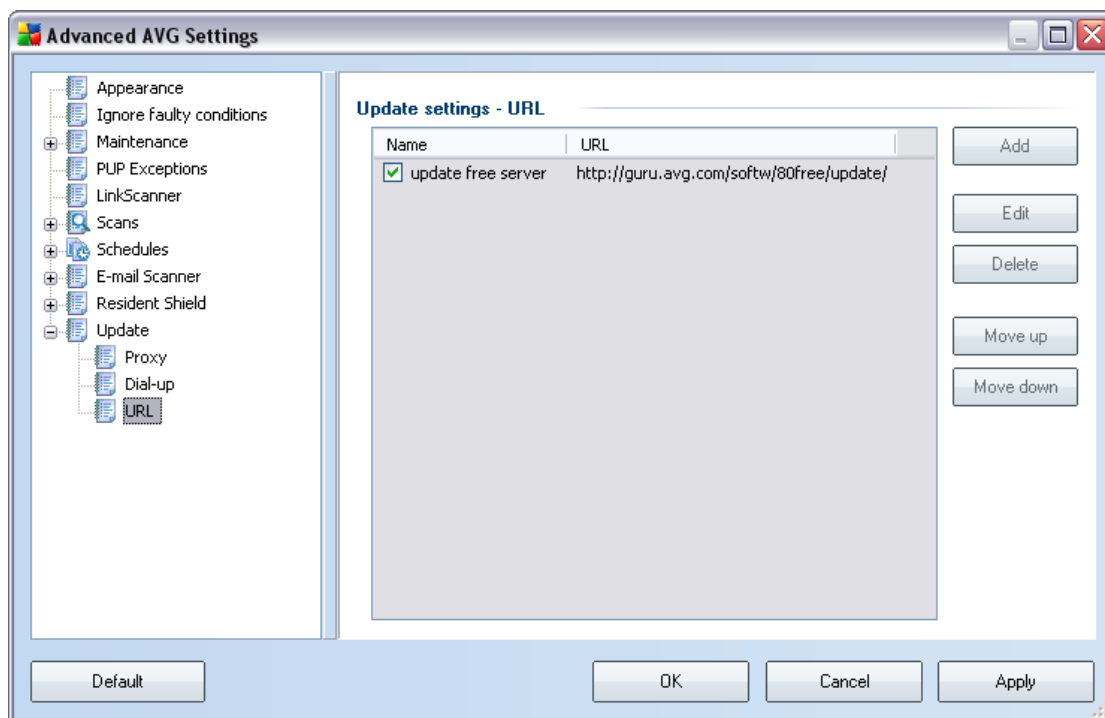
The *URL* dialog offers a list of Internet addresses from which the update files can be downloaded. Unfortunately, this list cannot be modified in **AVG 8.0 Free**; if you are interested in further and extended functionality within AVG 8.0 full products, please visit the AVG website (www.avg.com) for information on AVG 8.0 purchase options.

9. AVG Scanning

Scanning is a crucial part of **AVG 8.0 Free** functionality. You can run on-demand tests or schedule them to run periodically at convenient times.

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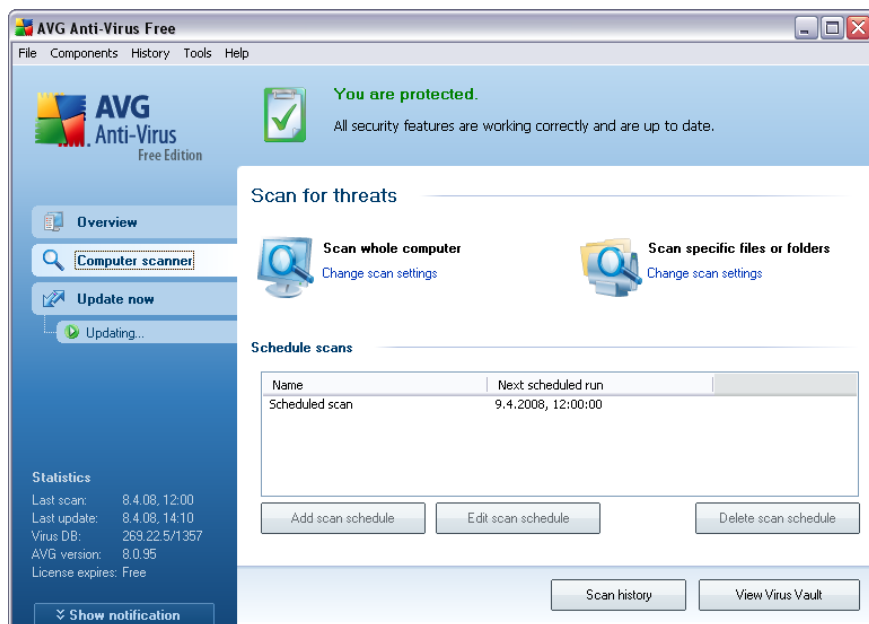
The AVG scanning interface is accessible via the **Computer Scanner** quick link. Click this link to switch to the **Scan for threats** dialog. In this dialog you will find the following:

- overview of predefined scans - two types of test (defined by the software vendor) are ready to be used immediately on demand or scheduled;

- 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 <u>Virus Vault</u> - a space where detected infections are quarantined

9.2. Predefined Scans

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

In the **AVG 8.0 Free** you will find two types of scanning predefined by the software vendor:

9.2.1. Scan Whole Computer

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

Scan launch

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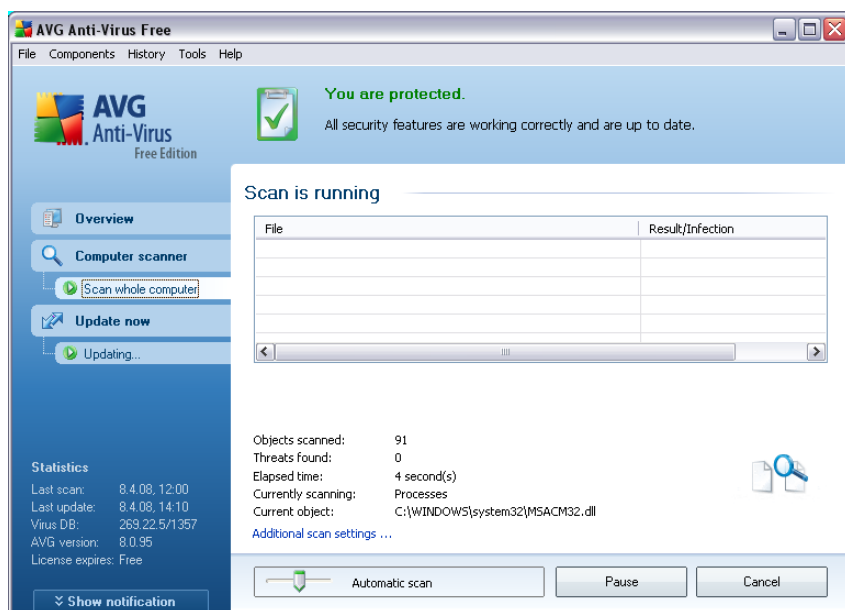
Scan configuration editing

You have the option of editing the predefined default settings of the **Scan of the whole computer**. Press the **Change scan settings** link to get to the **Change scan settings for Scan whole computer** dialog. *It is recommended to keep to the default settings unless you have a valid reason to change them!*
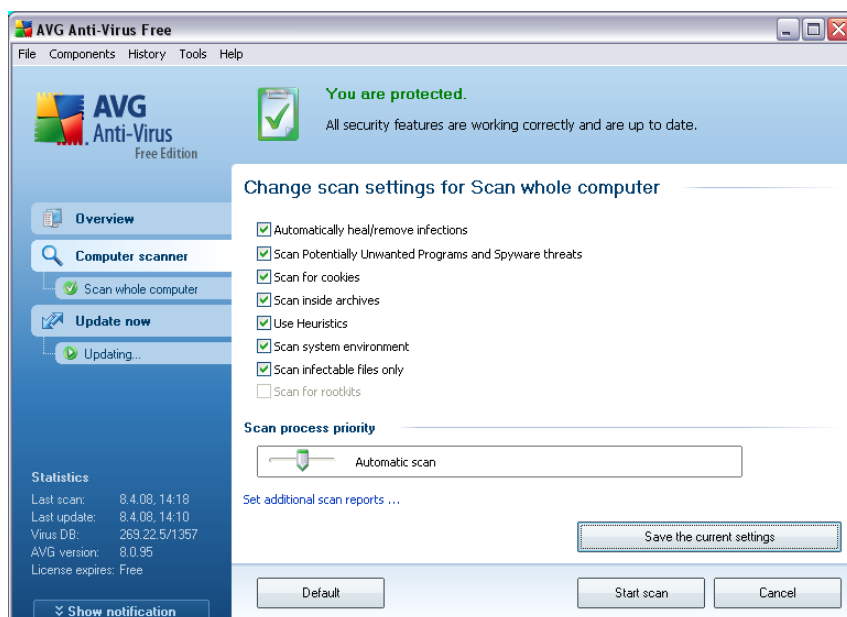
- **Scanning parameters** - in the list of scanning parameters you can switch on/off specific parameters as needed. By default, most of the parameters are switched on and these will be used automatically during scanning.

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

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

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

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.

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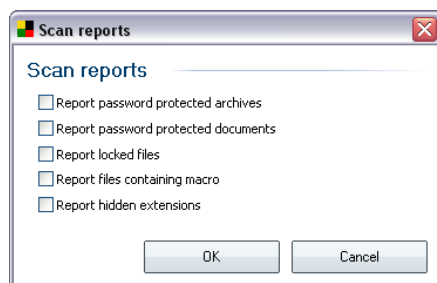
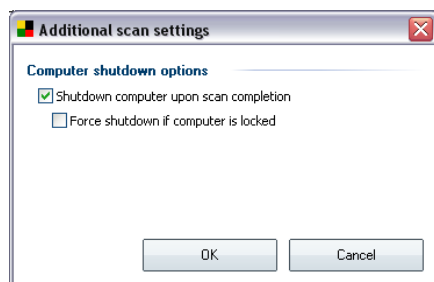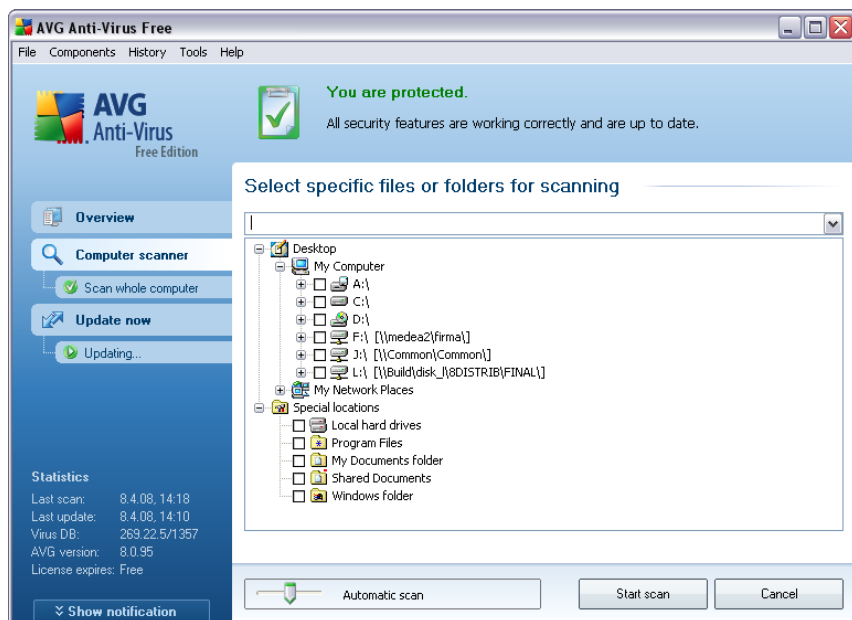[computer](#).

Scan configuration editing

You have the option of editing the predefined default settings of the **Scan of specific files or folders**. Press the **Change scan settings** link to get to the **Change scan settings for Scan of specific files or folders** dialog. **It is recommended to keep to the default settings unless you have a valid reason to change them!**
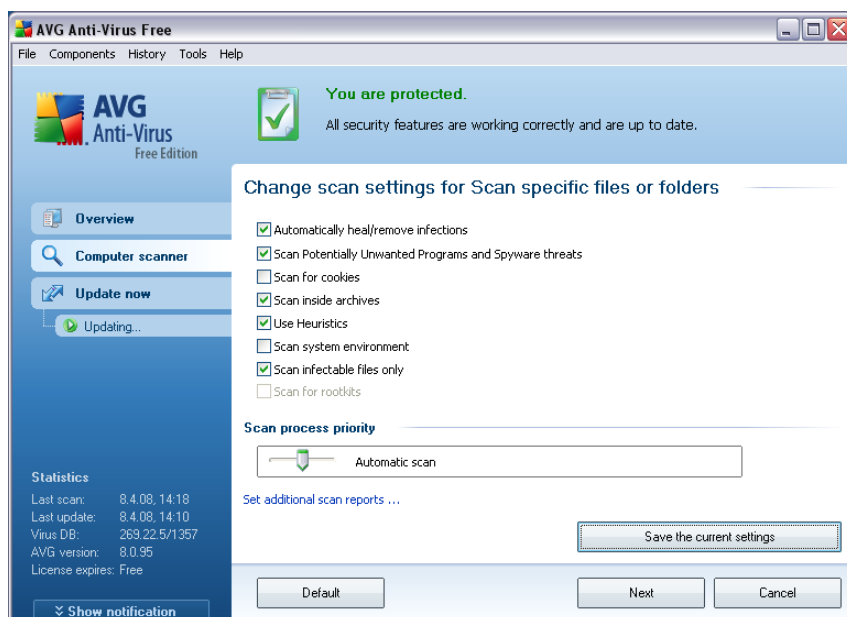
- **Scanning parameters** - in the list of scanning parameters you can switch on/off specific parameters as needed (*for detailed description of this settings please consult chapter AVG Advanced Settings / Scans / Scan Specific Files or Folders*).

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

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

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

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*).

9.3. Scanning in Windows Explorer

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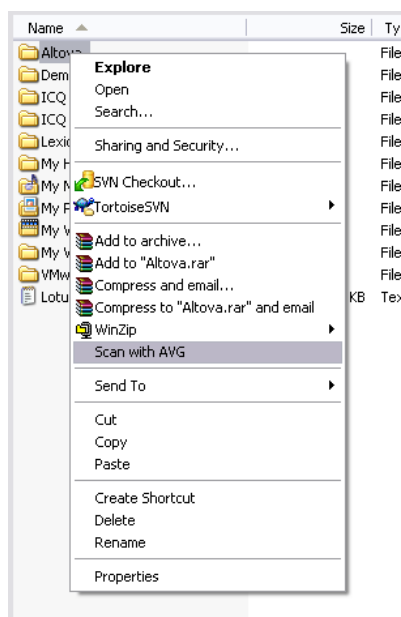
- Within Windows Explorer highlight the file (or folder) you want to check

- Right-click your mouse over the object to open the context menu

- Select the **Scan with AVG** option to have the file scanned with AVG

9.4. Command Line Scanning

Within **AVG 8.0 Free** there is the option of running the scan from the command line. You can use this option for instance on servers, or when creating a batch script to be launched automatically after the computer boot. From the command line, you can launch the scanning with most parameters as offered in AVG graphical user interface.

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

- **avgscanx** for 32 bits OS

- **avgscana** for 64 bits OS

Syntax of the command

The syntax of the command follows:

- ***avgscanx /parameter*** ... e.g. ***avgscanx /comp*** for scanning the whole computer

- ***avgscanx /parameter /parameter*** .. with multiple parameters these should be lined in a row and separated by a space and a slash character

- if a parameters requires specific value to be provided (e.g. the ***/scan*** parameter that requires information on what are the selected areas of your computer that are to be scanned, and you have to provide an exact path to the selected section), the values are divided by commas, for instance: ***avgscanx /scan=C:\,D:***

Scanning parameters

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

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

CMD scanning launched from the graphic interface

When you run your computer in Windows Safe Mode, there is also the 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.

9.4.1. CMD Scan Parameters

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

- ***/SCAN***   Scan specific files or folders /path,path/

- ***/COMP***   Scan whole computer

- ***/HEUR***   Use heuristic analyse

- */EXCLUDE*   Exclude path or files from scan

- */@*   Command file /file name/

- */EXT*   Scan these extensions /for example EXT=EXE,DLL/

- */NOEXT*   Do not scan these extensions /for example NOEXT=JPG/

- */ARC*   Scan archives

- */CLEAN*   Clean automatically

- */TRASH*   Move infected files to the [Virus Vault](#)

- */QT*   Quick test

- */MACROW*   Report macros

- */PWDW*   Report password-protected files

- */IGNLOCKED*   Ignore locked files

- */REPORT*   Report to file /file name/

- */REPAPPEND*   Append to the report file

- */REPOK*   Report uninfected files as OK

- */NOBREAK*   Do not allow CTRL-BREAK to abort

- */BOOT*   Enable MBR/BOOT check

- */PROC*   Scan active processes

- */PUP*   Report "[Potentially unwanted programs](#)"

- */REG*   Scan registry

- */COO*   Scan cookies

- */?*   Display help on this topic

- */HELP*   Display help on this topic

- */PRIORITY*   Set scan priority /Low, Auto, High/ (see [Advanced](#)

settings / Scans)

- **/SHUTDOWN**   Shutdown computer upon scan completion

- **/FORCESHUTDOWN** Force computer shutdown upon scan completion

- **/ADS**   Scan Alternate Data Streams (NTFS only)

9.5. Scan Scheduling

With **AVG 8.0 Free** you can run scanning on demand (for instance when you suspect an infection has been dragged to your computer) or based on a scheduled plan. It is highly recommended to run the scans based on a schedule: this way you can make sure your computer is protected from any possibility of getting infected, and you will not have to worry about if and when to launch the scan.

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

To edit the default schedule, see the AVG scanning interface and find the bottom section called **_Schedule scans_**:
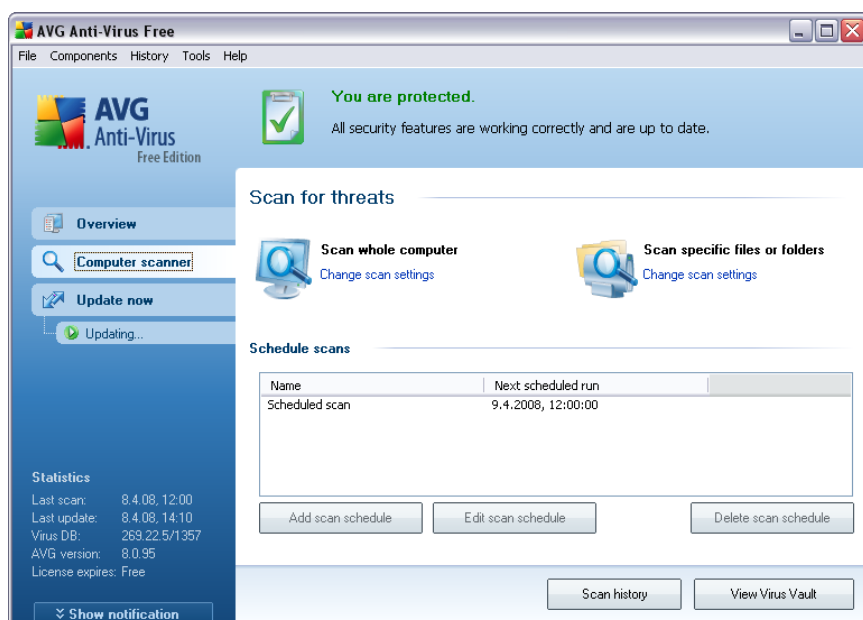
Control buttons for the scan scheduling

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

- *Add scan schedule* - this button is disabled in **AVG 8.0 Free**. If you need to schedule scanning more often and based on your specific needs, please visit the AVG website (www.avg.com) for information on AVG 8.0 purchase options

- *Edit Scan Schedule* - This button is only active when you select a scan from the list of scheduled scans. It will display the *Settings for scheduled scan* dialog, *Schedule settings* tab, where you can edit the selected schedule.

- *Delete scan schedule* - this button is also disabled in **AVG 8.0 Free**.

9.5.1. Schedule Settings

This dialog is divided into three tabs: *Schedule settings* - *see picture below* (the default tab that will be automatically displayed), *How to scan* and *What to scan*.
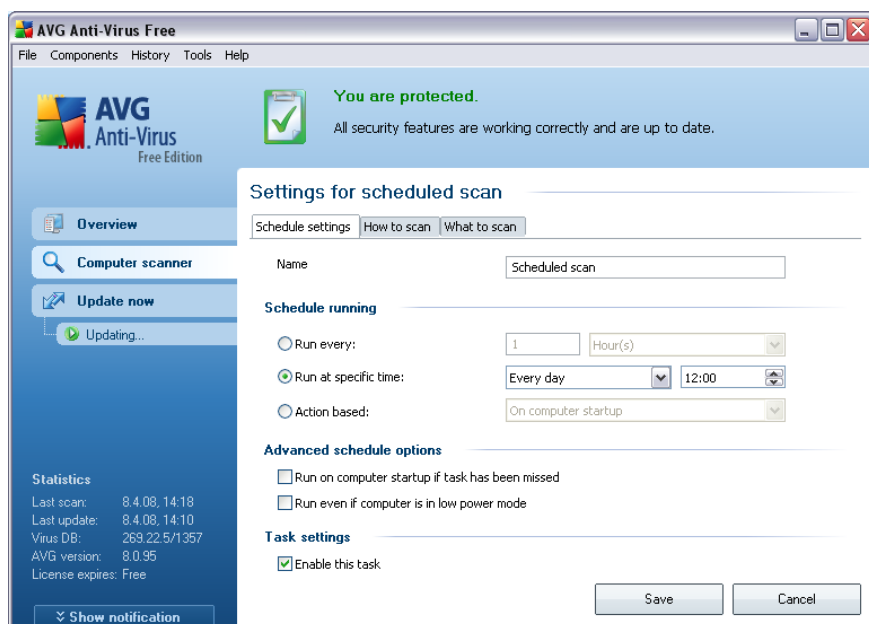
In this dialog you can define the following parameters of the scan:

- *Name* - If you wish, you can rename the default scan.

- **Schedule running** - specify the intervals for the scheduled scan launch.

  - ➢ **Run every** - run the scan every 'n' number of hours. E.g. every 4 hours.

  - ➢ **Run at specific time** - select **Every day**, or select a specific day of the week, and specify what time of day the scan should start.

  - ➢ **Action based** - run the scan on computer startup.

  - **Note**: More comprehensive options are available in full versions of AVG.

- **Advanced schedule options**

  - ➢ **Run on computer startup if task has been missed** - if the scan cannot run at the scheduled time/interval, then it will run the next time the computer restarts.

  - ➢ **Run even if computer is in low power mode** - this option applies to battery powered computers such as notebooks. The default action is for AVG to postpone scanning when the computer's power resources are low.

- **Task settings** - in the section you can uncheck the **Enable this task** item to simply deactivate the scheduled test. **Not recommended**.

Control buttons of the Settings for scheduled scan dialog

- **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]().

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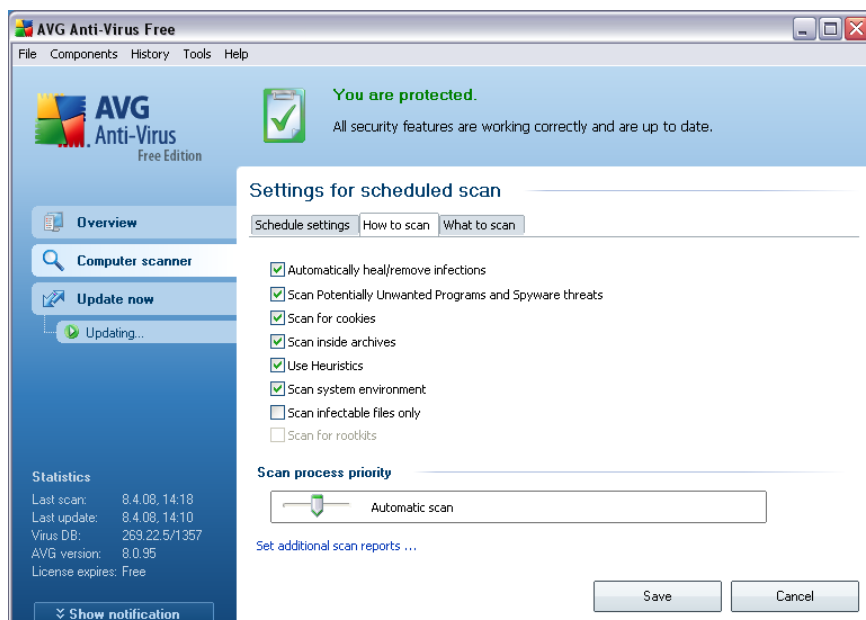
On the **How to scan** tab you will find a list of scanning parameters that can be optionally switched on/off. By default, most parameters are switched on and the functionality will be applied during scanning. Unless you have a valid reason to change these settings we recommend to keep to the pre-defined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

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

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

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

- **Scan inside archives** - (*switched on, by default*): this parameters defines that the scanning should check all files even if these are packed inside some type of archive, e.g. ZIP, RAR, ...

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

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

- **Scan infectable files only** - (*switched off, by default*): if this option is switched on, then scanning will not be applied to files that cannot get infected. These can be for instance some plain text files, or some other non-executable files.

- **Scan for rootkits** - This option is disabled in **AVG 8.0 Free**.

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

Additional scanning options are available via the following hyperlinks:

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

- **Additional scan settings** - the link opens a new **Computer shutdown options** dialog where you can decide whether the computer should be shut

down automatically once the running scanning process is over. Having confirmed this option (**Shutdown computer upon scan completion**), a new option activates that allows the computer to shut down even if it is currently locked (**Force shutdown if computer is locked**).
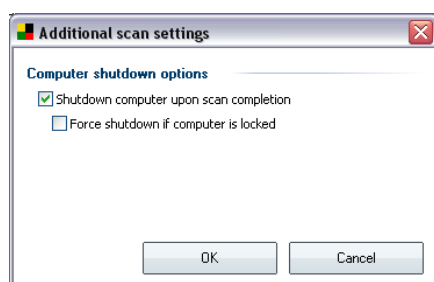
Note: *By default, the scanning configuration is set up for optimum performance. Unless you have a valid reason to change the scanning settings it is highly recommended to stick to the predefined configuration. Any configuration changes should be performed by experienced users only. For further scanning configuration options see the* **Advanced settings** *dialog accessible via the* **File / Advanced setting** *system menu item.*

Control buttons of the Settings for scheduled scan dialog

- **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.

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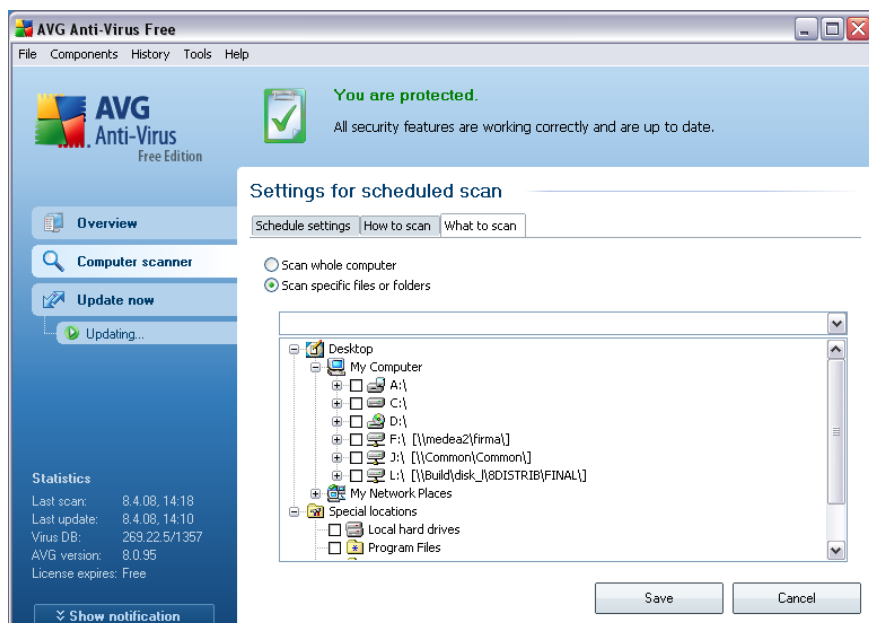
On the **What to scan** tab you can define whether you want to schedule scanning of the whole computer or scanning of specific files or folders. In case you select scanning of specific files or folders, in the bottom part of this dialog the displayed tree structure activates and you can specify which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

Control buttons of the Settings for scheduled scan dialog

- **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.

9.6. Scan Results Overview
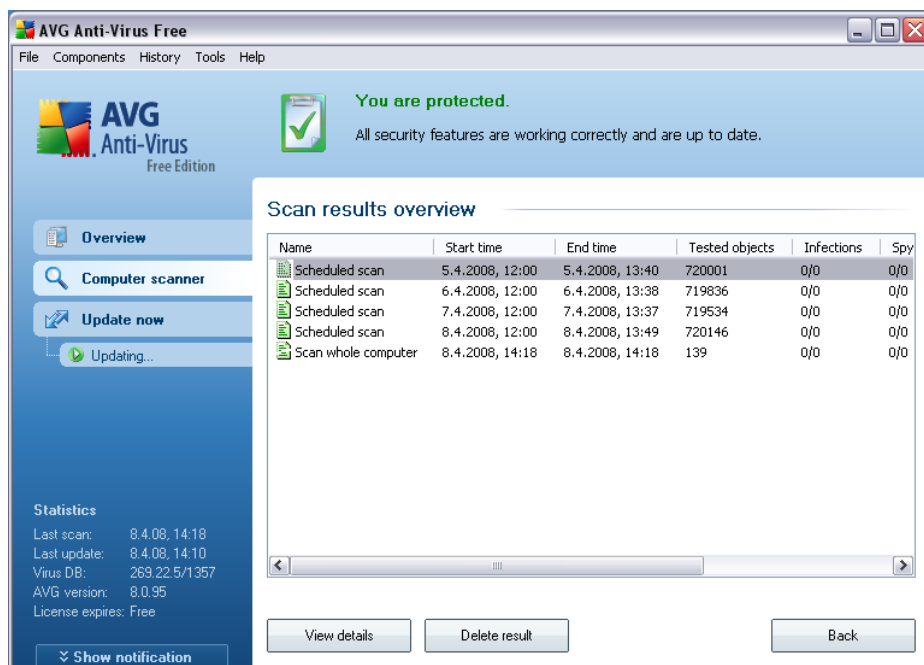

The **Scan results overview** dialog is accessible from the [AVG scanning interface](#) via the **Scan history** button. The dialog provides a list of of all previously launched scans and information of their results:

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

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

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

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

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

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

- **Start time** - date and time when the scan was launched

- **End time** - date and time when the scan ended

- **Tested objects** - number of objects that were checked during scanning

- **Infections** - number of virus infections detected / removed

- **Spyware** - number of spyware detected / removed

- **Scan log information** - information relating to the scanning course and result (typically on its finalization or interruption)

Control buttons

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

- **View details** - this button is only active if a specific scan is selected in the above overview; press it to switch to the **Scan results** dialog to view detailed data on the selected scan

- **Delete result** - this button is only active if a specific scan is selected in the above overview; press it to remove the selected item from the scan results overview

- **Back** - switches back to the default dialog of the AVG scanning interface

9.7. Scan Results Details

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

The dialog is further divided into several tabs:

- **Results Overview** - this tab is displayed at all times and provides statistical data describing the scan progress

- **Infections** - this tab is displayed only if a virus infection was detected during

scanning

- ***Spyware*** - this tab is displayed only if spyware was detected during scanning

- ***Warnings*** - this tab is displayed only if some objects unable to be scanned were detected during scanning

- ***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

9.7.1. Results Overview Tab
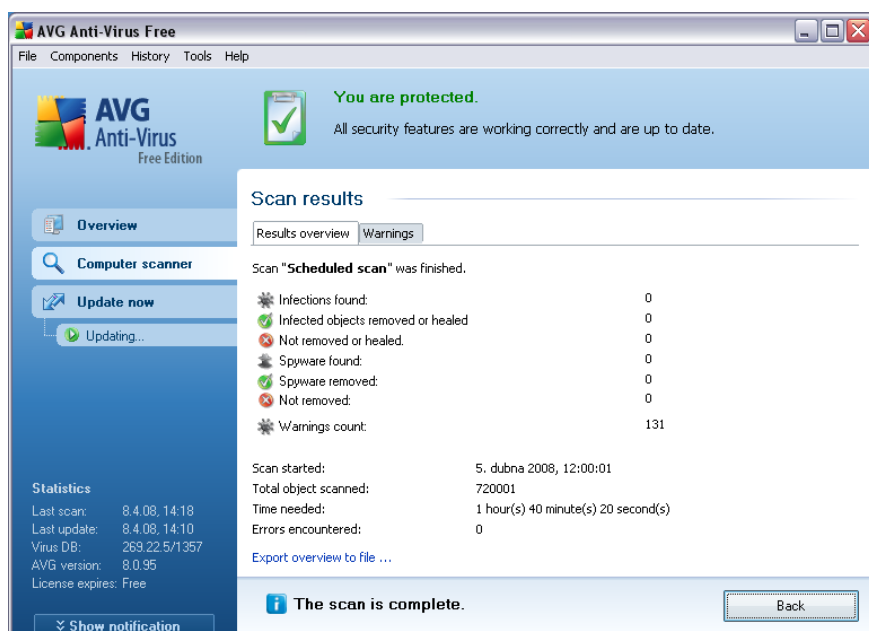
On the **Scan results** tab you can find detailed statistics with information on:

- 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.

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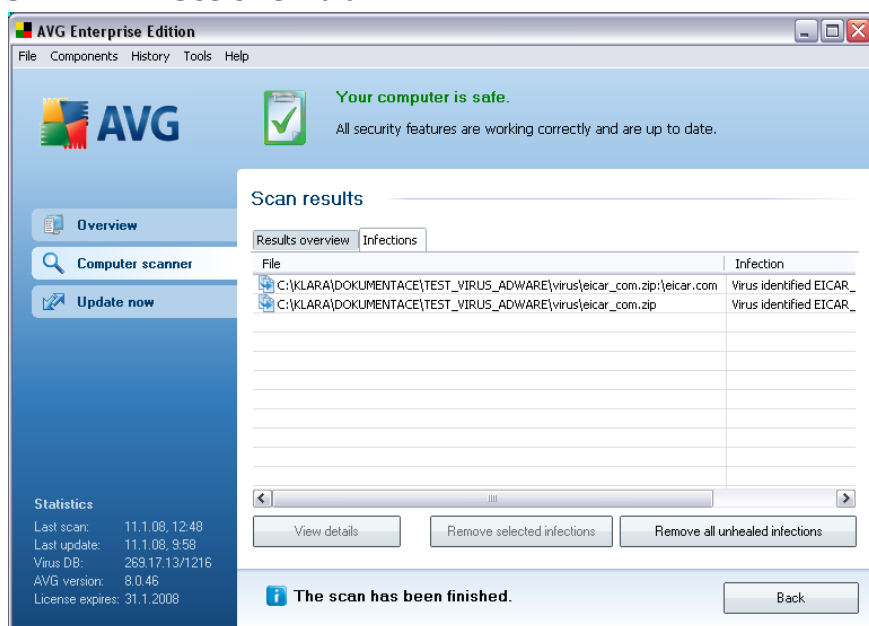
The **Infections** tab is only displayed in the **Scan results** dialog if a virus infection was detected during scanning. The tab is divided into three sections providing the following information:

- **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:

    o **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*)

o **Healed** - the infected object was healed automatically and left in its original location

o **Moved to Virus Vault** - the infected object was moved to the **_Virus Vault_** quarantine

o **Deleted** - the infected object was deleted

o **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*)

o **Locked file - not tested** - the respective object is locked and AVG is therefore unable to scan it

o **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

o **Reboot is required to finish the action** - the infected object cannot be removed, to remove it completely you have to restart your computer

Control buttons

There are three control buttons available in this dialog:

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

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

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

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

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

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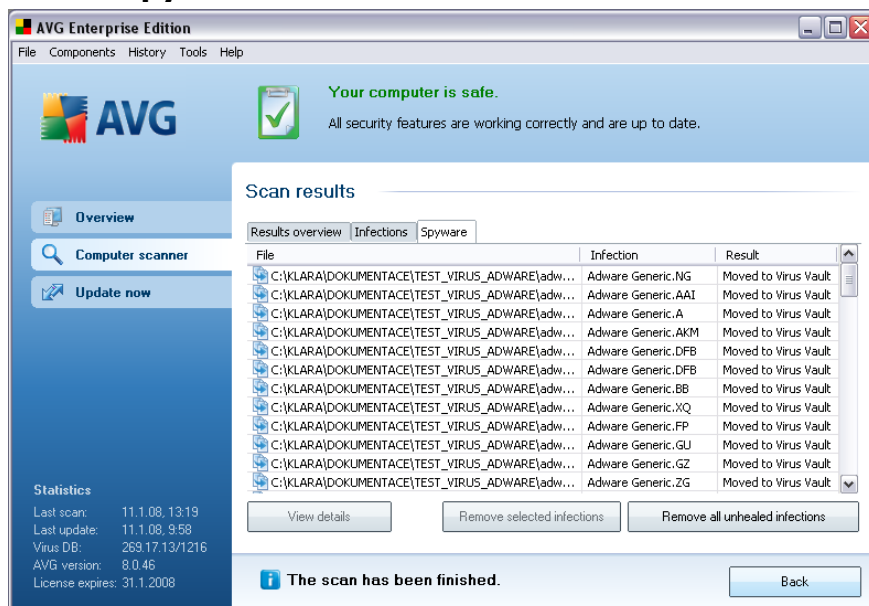
The **Spyware** tab is only displayed in the **Scan results** dialog in if spyware was detected during scanning. The tab is divided into three sections providing the following information:

- **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:

  - o **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)

  - o **Healed** - the infected object was healed automatically and left in its original location

  - o **Moved to Virus Vault** - the infected object was moved to the **Virus Vault** quarantine

  - o **Deleted** - the infected object was deleted

  - o **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*)

  - o **Locked file - not tested** - the respective object is locked and AVG is therefore unable to scan it

  - o **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

  - o **Reboot is required to finish the action** - the infected object cannot be removed, to remove it completely you have to restart your computer

Control buttons

There are three control buttons available in this dialog:

- **View details** - the button opens a new dialog window named **Detailed scan result information**:
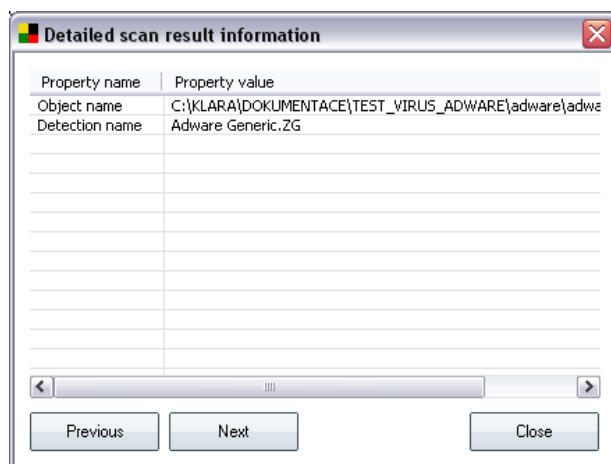
In this dialog you can find information on the location of the detected infectious object (*Property name*). Using the *Previous* / *Next* buttons you can view information on specific findings. Use the *Close* button to leave this dialog.

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

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

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

9.7.4. 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.

9.7.5. Information Tab

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

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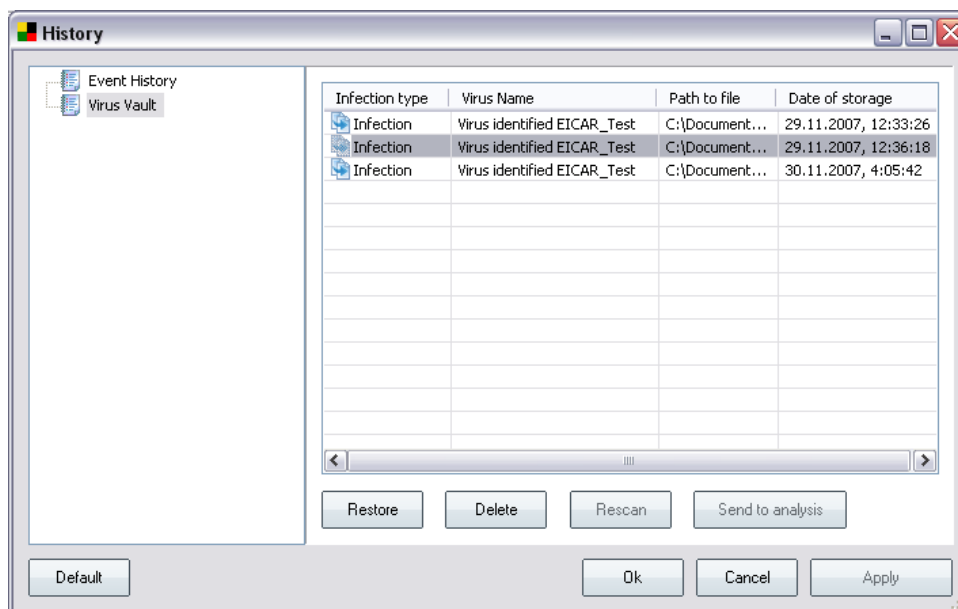
Virus Vault is a safe environment for the management of suspect/infected objects detected during AVG tests. Once an infected object is detected during scanning, and AVG is not able to heal it automatically, you are asked to decide what is to be done with the suspect object. The recommended solution is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

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

- ***Infection type*** - distinguishes finding types based on their infective level (*all listed objects can be positively or potentially infected*)

- ***Virus Name*** - specifies the name of the detected infection according to the Virus encyclopedia (online)

- ***Path to file*** - full path to the original location of the detected infectious file

- ***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

- *Delete* - removes the infected file from the *Virus Vault* completely

- *Rescan* - double-checks the suspected file to make sure it is really infected

- *Send to analysis* - sends the suspected file for deep analysis to the AVG virus labs

10. AVG Updates

10.1. Update Levels

AVG offers two update levels to select from:

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

- **Program update** contains various program changes, fixes and improvements.

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

10.2. Update Types

You can distinguish between two types of update:

- **On demand update** is an immediate AVG update that can be performed any time the need arises.

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

10.3. Update Process

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

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

11. Event History
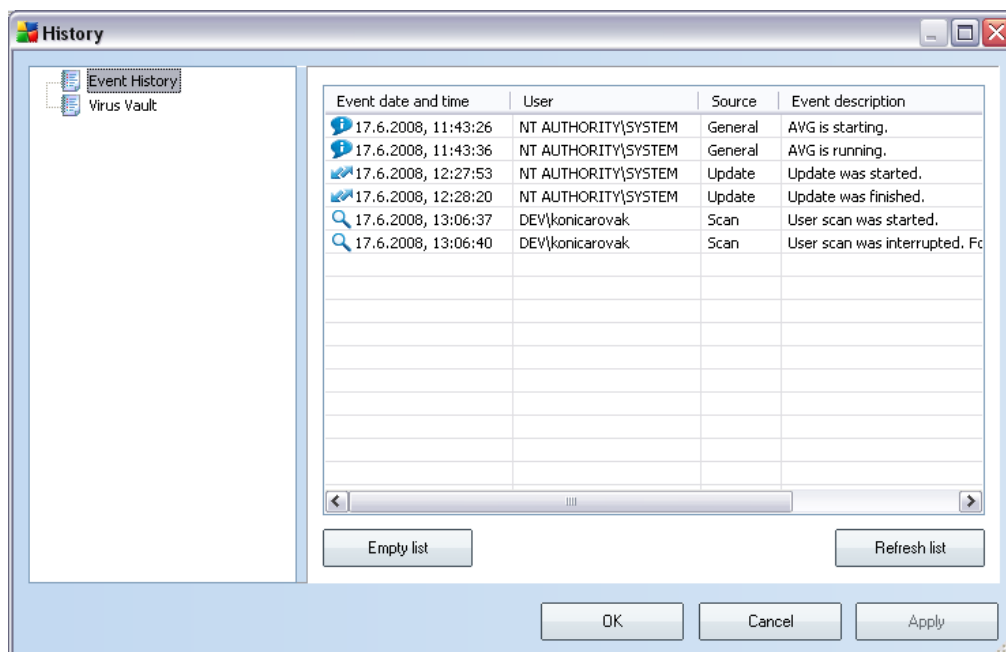
The **Event History** dialog is accessible from the system menu via the **History/Event History Log** item. Within this dialog you can find a summary of important events that occurred during **AVG 8.0 Free** operation. **Event History** records the following types of events:

- Information about updates of the AVG application

- Scanning start, end or stop (including automatically performed tests)

- Events connected with virus detection (by the Resident Shield or scanning) including occurrence location

- Other important events

Control buttons

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

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

12. FAQ and Technical Support

Should you have any problems with your AVG, either business or technical, please refer to the *FAQ* section of the AVG website at www.avg.com. Unfortunately, using **AVG 8.0 Free** you are not entitled to technical support provided to full versions of AVG products. If you have registered your **AVG 8.0 Free**, you can also try to look up some help in AVG forums and discussions. Or, you may want to consider buying the full version of AVG, then please visit the AVG website (www.avg.com) for information on AVG 8.0 purchase options.