AVG 8.5 File Server Edition

Manual do Usuário

Revisão do documento 85.1 (16.1.2009)

Conteúdo

1. Introdução

Este manual do usuário fornece uma documentação completa para o **AVG 8.5 File Server**.

Parabéns pela aquisição do AVG 8.5 File Server!

AVG 8.5 File Server é um dos vários produtos premiados do AVG criados para fornecer a você paz de espírito e total segurança para o seu computador. Como ocorreu com todos os produtos AVG, o **AVG 8.5 File Server** foi completamente reprojetado para fornecer a proteção e a segurança certificada e renomada do AVG em uma nova forma, mais eficiente e amigável.

O AVG foi projetado e desenvolvido para proteger seu computador e sua atividade de rede. Aproveite a experiência da proteção completa com o AVG.

2. Requisitos de instalação do AVG

2.1. Sistemas operacionais com suporte

AVG 8.5 File Server foi criado para proteger servidores de e-mail em execução nos seguintes sistemas operacionais:

- Windows 2008 x64 Server Edition
- Windows 2003 Server (x86, x64 e Itanium) SP1
- Windows 2000 Server SP4 + Update Rollup 1
- Windows 2000/XP, workstation edition (Kerio MailServer 5.0/6.0)

(e possíveis service packs posteriores para servidores de e-mail específicos)

Nota: AVG 8.5 File Server Edition *deve ser instalado no seu computador para assegurar proteção antivírus e anti-spyware de e-mails por meio do mecanismo de verificação do AVG!*

2.2. Requisitos mínimos de hardware

Estes são os requisitos mínimos de hardware para o**AVG 8.5 File Server**:

- Intel Pentium CPU 300 MHz
- 70 MB de espaço livre em disco rígido (para fins de instalação)
- 64 MB de memória RAM

2.3. Servidores de e-mail suportados

Há diversas instalações do **AVG 8.5 File Server** disponíveis. Cada uma abrange servidores de e-mail específicos, conforme listado a seguir:

- **AVG for MS Exchange 2000/2003 Server** – MS Exchange 2000 Server (com o Service Pack 1 ou superior) e as versões do MS Exchange 2003 Server.

  Nota: para o Exchange 2000 Server - Service Pack 1 (ou posterior) deve ser aplicado antes de você usar o mecanismo do AVG; **AVG for MS**

Exchange 2000/2003 Server utiliza a interface de aplicativo VSAPI 2.0 (ou 2.5 com o Exchange 2003 Server), coberta neste Service Pack.

- **AVG for MS Exchange 2007 Server** – Versão do MS Exchange 2007 Server
- **AVG for Lotus Notes/Domino Server** – Lotus Notes/Domino Server - versão 5.0 e posterior

2.4. Requisitos de hardware recomendados

Os requisitos de hardware recomendados para o **AVG 8.5 File Server**são:

- Intel Pentium CPU 600 MHz
- 70 MB de espaço livre em disco rígido
- 256 MB de memória RAM

2.5. Desinstalar versões anteriores

Se você já tiver uma versão mais antiga do AVG Email Server instalada, deverá desinstalá-la antes de instalar o **AVG 8.5 File Server**. Você deve executar a desinstalação da versão anterior manualmente, utilizando a funcionalidade do Windows.

- No menu inicial ***Iniciar/Configurações/Painel de Controle/Adicionar ou Remover Programas***, selecione o programa correto na lista de softwares instalados. Tome cuidado ao selecionar o programa AVG para desinstalação. Você precisa desinstalar o Email Server Edition antes de desinstalar o AVG File Server Edition.
- Quando tiver desinstalado o Email Server Edition, você poderá prosseguir para desinstalar a versão anterior do AVG File Server Edition. Isso pode ser feito facilmente no menu inicial ***Iniciar/Todos os Programas/AVG/Desinstalar AVG***

Quando o AVG Email Server e o AVG File Server tiverem sido desinstalados com sucesso, prossiga com a instalação do AVG 8.5 File Server Edition mais recente.

2.6. Instalar o AVG File Server

AVG 8.5 File Server Edition é necessário para garantir a proteção anti-vírus e anti-spyware para e-mail utilizando o mecanismo de verificação do AVG! Deve ser instalado ANTES de começar da instalação do **AVG 8.5 File Server**. Para obter detalhes sobre a instalação do **AVG 8.5 File Server Edition**, consulte o documento **AVG 8.5 File Server Edition** Manual do Usuário disponível no site do AVG (www.avg.com), na seção ***Downloads***.

3. Opções de instalação do AVG

O AVG pode ser instalado a partir do arquivo de instalação disponível no CD de instalação ou você pode baixar o arquivo de instalação mais recente nosite do AVG (www.avg.com).

Antes de instalar o AVG, é recomendável que você visite o site da AVG para verificar se há um novo arquivo de instalação. Dessa forma, você poderá garantir a instalação da versão mais recente do AVG 8.5 File Serverdisponível.

Durante o processo de instalação será solicitado o seu número de venda/licença. Certifique-se de tê-lo disponível antes de iniciar a instalação. O número de venda pode ser encontrado na embalagem do CD. Se você adquiriu a sua cópia do AVG on-line, o número da licença foi enviado para você por e-mail.

Para obter mais informações, vá até o capítulo específico, de acordo com o servidor de e-mail instalado.

- AVG para MS Exchange Server Este capítulo abrange o **AVG for MS Exchange 2000/2003 Server** e o **AVG for MS Exchange 2007 Server**. Embora estas edições tenham arquivos de instalação separados, funcionam exatamente da mesma forma (mesmas caixas de diálogo e métodos de configuração).

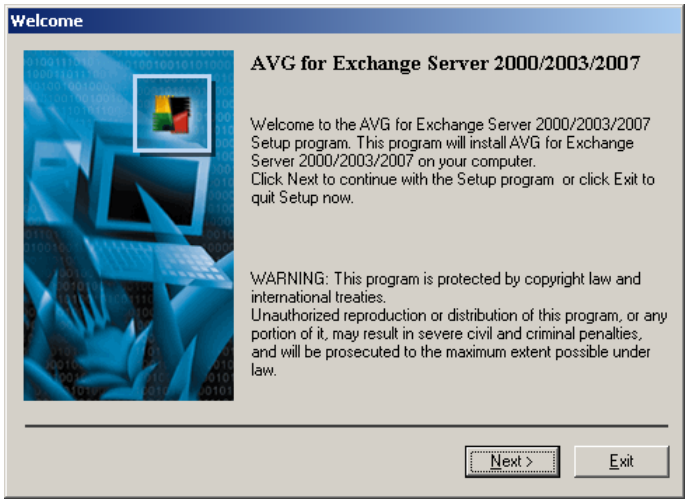
- AVG for Lotus Notes/Domino Server

4. AVG Installation Process

To install AVG on your computer, you need to get the latest installation file. You can use the installation file from the CD that is a part of your box edition but this file might be out-of-date. Therefore we recommended getting the latest installation file online. You can download the file from the AVG website (at www.avg.com) / ***Downloads*** section.

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:

4.1. Início da instalação



O processo de instalação é iniciado com a janela de ***boas-vindas***. Clique no botão ***Avançar*** para seguir para a próxima caixa de diálogo.

4.2. Contrato de licença

Essa caixa de diálogo fornece o contrato de licença completo do AVG. Leia-o cuidadosamente e confirme se leu, compreendeu e aceita o contrato, pressionando o botão ***Aceito***. Se você não concordar com o contrato de licença, pressione o botão ***Não aceito*** e o processo de instalação será encerrado imediatamente.

4.3. Registro

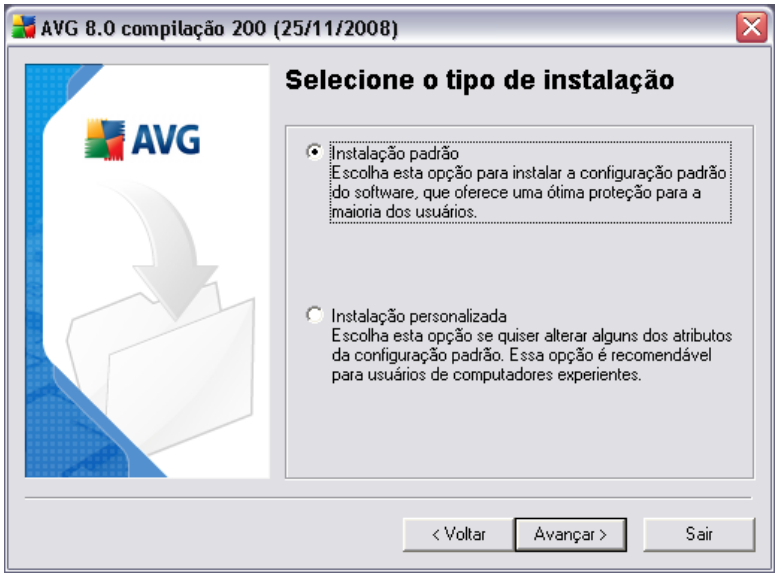
Nesta tela, preencha o seu número de licença do **AVG 8.5 File Server**.

Se você usou um número de licença do **AVG 8.5 File Server** durante a instalação do **AVG 8.5 File Server Edition**, esta tela não será exibida. No entanto, se adquiriu o **AVG 8.5 File Server** e o **AVG 8.5 File Server Edition** separadamente, agora deverá inserir o número de licença do **AVG 8.5 File Server**.

Clique no botão Avançar ***para confirmar as informações fornecidas.***

Depois de confirmar o contrato de licença, você será redirecionado para a caixa de diálogo ***Verificação do Status do Sistema***. Essa caixa de diálogo não requer nenhuma intervenção; o sistema está sendo verificado antes da inicialização da instalação do AVG. Aguarde a conclusão do processo e continue automaticamente para a caixa de diálogo seguinte.

4.4. Select Installation Type



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

For most users, it is highly recommended to keep to the ***standard installation*** that installs AVG in fully automatic mode with settings predefined by the program vendor. This configuration provides maximum security combined with the optimal use of

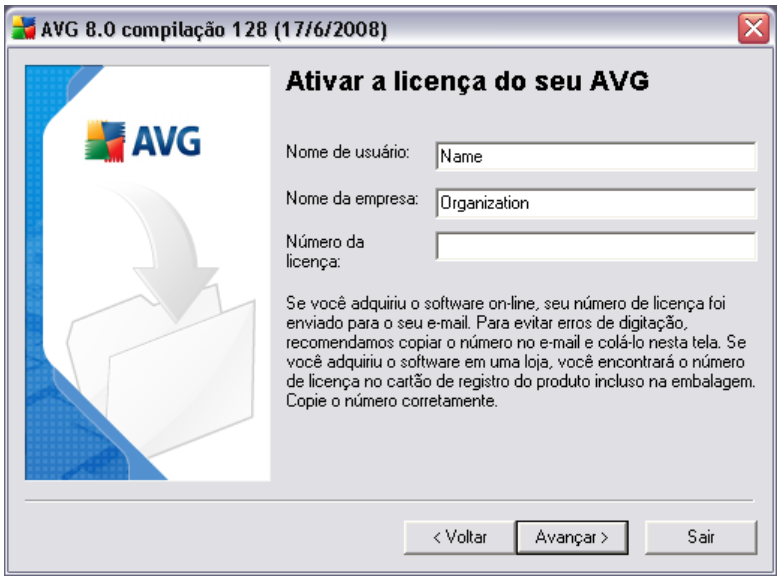
resources. In the future, if the need arises to change the configuration, you will always have the possibility to do so directly in the AVG application.

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

4.5. Activate Your AVG License

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

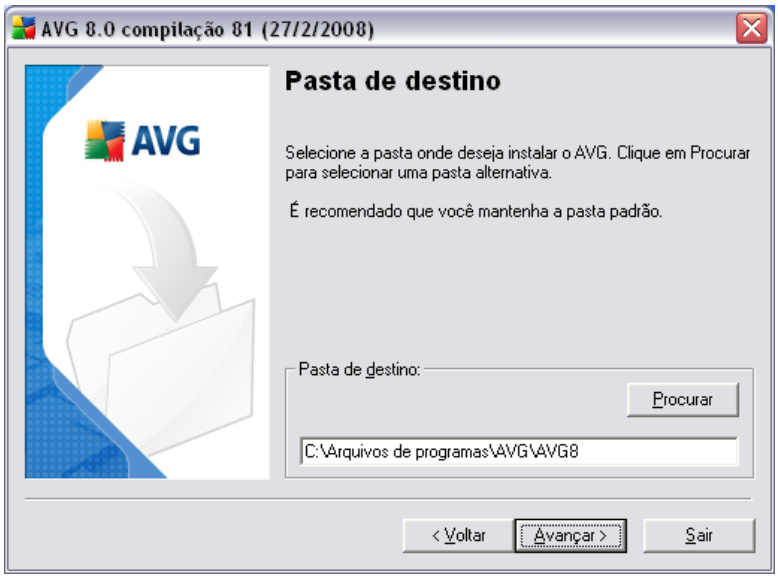
Then enter your license/sales number into the ***License Number*** text field. The license number will be in the confirmation email that you received after purchasing your AVG on-line. You must type in the number exactly as shown. If the digital form of the license number is available (in the email), it is recommended to use the copy and paste method to insert it.



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

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

4.6. 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.

4.7. Custom Installation - Module Selection

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

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

- ***Remote Control Communication Library*** - if you intend to connect AVG to an AVG DataCenter (AVG Network Editions), then you need to select this option.

- ***Additional Installed Languages*** - you can define which language(s) AVG should be installed in. Check the ***Additional installed languages*** item and then select the desired languages from the respective menu.

- ***Email Scanner*** - E-mail scanning provided by AVG 8.5 File Server is only suitable for protecting your e-mail client on the file server itself. By default the ***E-mail Scanner*** is not installed, as it is not normal practice to run an e-mail client on a file server. If you require email scanning for your email server then we recommend purchasing the **AVG 8.0 Email Server Edition**. This edition will provide full protection for your email server application and its file server. You can purchase and download the latest version of **AVG Email Server Edition** from the AVG website (www.avg.com).

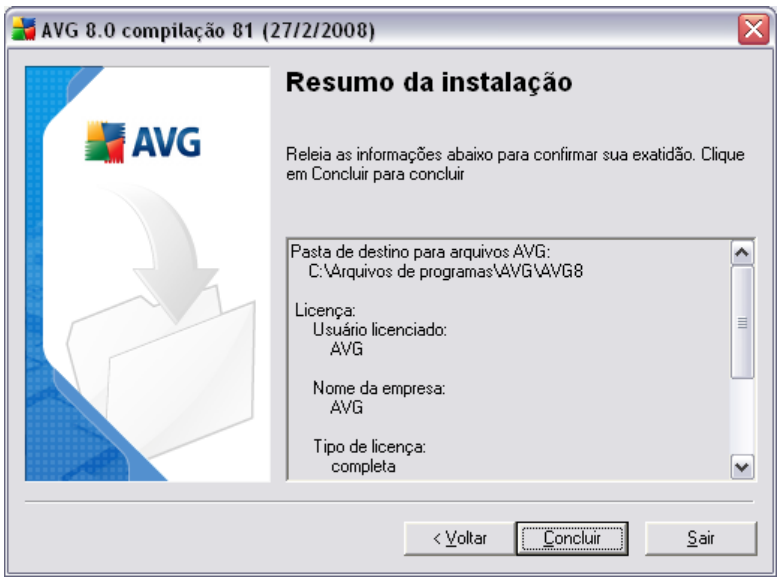
Continue by pressing the ***Next*** button.

4.8. Custom Installation - E-mail Scanning

E-mail scanning provided by **AVG 8.5 File Server** is only suitable for protecting your e-mail client on the file server itself. As it is not normal practice to run an e-mail client on a file server, so by default the ***E-mail Scanner*** is not installed.

Note: If you require email scanning for your email server then we recommend purchasing the **AVG 8.0 Email Server Edition**. This edition will provide full protection for your email server application and it's file server. You can purchase and download the latest version from the AVG website (www.avg.com).

4.9. 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.

4.10.Installing

The ***Installing*** 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.

4.11.Installation Complete

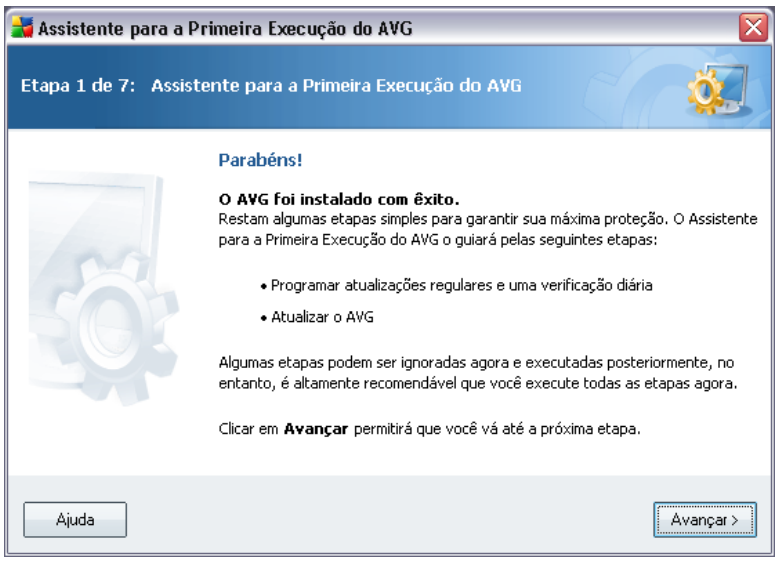
The ***Installation Complete*** dialog is the last step of the AVG installation process. AVG is now installed on your computer and fully functional. The program is running in the background in fully automatic mode.

After the installation, ***AVG Basic Configuration Wizard*** will be launched automatically and in a few steps will lead you through the **AVG 8.5 File Server** elementary configuration. Despite the fact the AVG configuration is accessible any time during AVG run, we deeply recommend to use this option and set up the basic configuration with the wizard's help.

5. AVG Basic Configuration Wizard

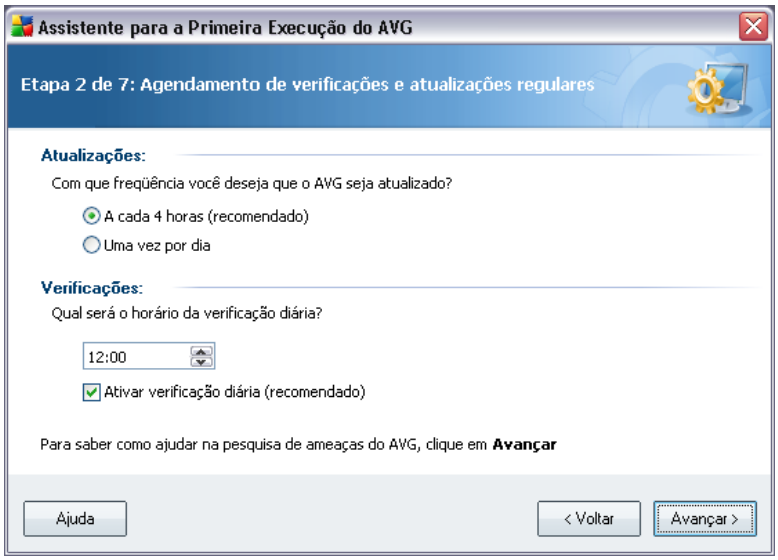
When you first install AVG on your computer, the ***AVG Basic Configuration Wizard*** pops up to help you with initial **AVG 8.5 File Server** settings. Though you can set all of the suggested parameters later on, it is recommended that you take the wizard's tour to secure your computer's protection simply and immediately. Follow the steps described in each of the wizard's windows:

5.1. AVG Essential Configuration



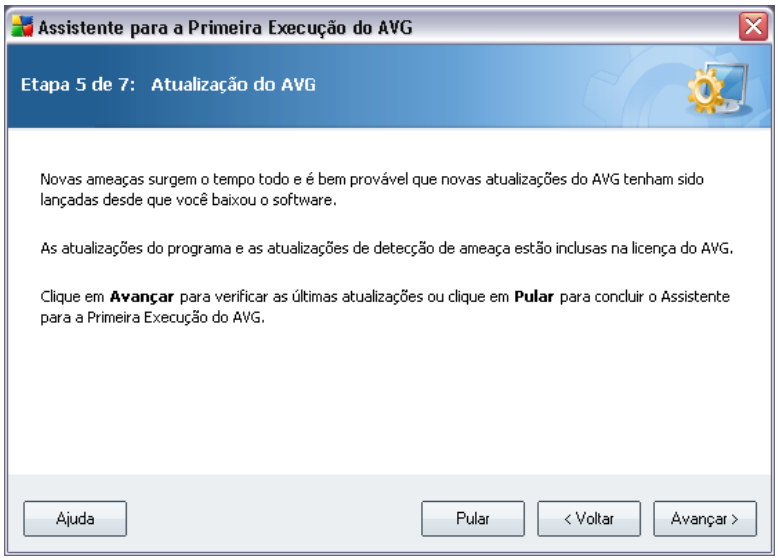
The ***AVG Basic Configuration Wizard*** welcome window briefly summarizes the status of AVG on your computer, and suggests the steps to be taken to complete protection. Click on the ***Next*** button to continue.

5.2. AVG Task Scheduling



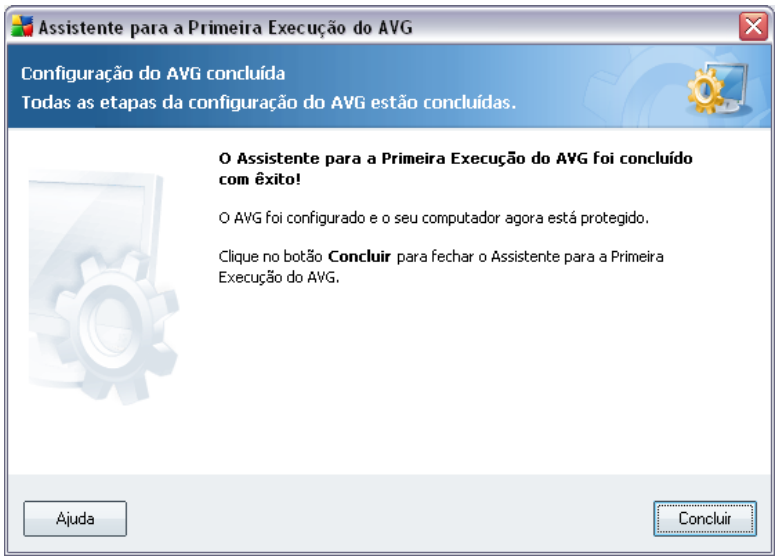
In the ***Schedule regular scans and updates*** dialog set up the interval for new update files accessibility check-up, and define time when the scheduled scan should be launched. It is recommended to keep the default values. Press the ***Next*** button to continue.

5.3. 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.

5.4. AVG Configuration Finished



Now your **AVG 8.5 File Server** has been configured; press the ***Finish*** button to start working with AVG.

6. After Installation

6.1. Product Registration

Having finished the **AVG 8.5 File Server** installation, please register you product online on the AVG website, ***Registration*** page (*follow the instruction provided directly in the page*). After the registration you will be able to gain full access to your AVG User account, the AVG Update newsletter, and other services provided exclusively for registered users.

6.2. Access to User Interface

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

- double-click the AVG icon on the system tray
- double-click the AVG icon on the desktop
- from the menu ***Start/All Programs/AVG 8.0/AVG User Interface***

6.3. Scanning of the whole computer

There is a potential risk that a computer virus has been transmitted to your computer prior to **AVG 8.5 File Server** installation. For this reason you should run a ***Scan of the whole computer*** to make sure there are no infections on your PC.

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

6.4. Eicar Test

To confirm that **AVG 8.5 File Server** has been installed correctly you can perform the EICAR test.

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

Try to download the ***eicar.com*** file, and save it on your local disk. Immediately after you confirm downloading of the test file, the ***Resident Shield*** will react to it with a warning. This ***Resident Shield*** notice demonstrates that AVG is correctly installed on your computer.

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

6.5. AVG Default Configuration

The default configuration (*i.e. how the application is set up right after installation*) of **AVG 8.5 File Server** is set up by the software vendor so that all components and functions are tuned up to achieve optimum performance.

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

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

7. AVG User Interface

AVG 8.5 File Server open with the main window:

The main window is divided into several sections:

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

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

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

7.1. System Menu

The ***System menu*** is the standard navigation used in all Windows applications. It is located horizontally in the very top part of the **AVG 8.5 File Server** main window. Use the system menu to access specific AVG components, feature, and services.

The system menu is divided into five main sections:

7.1.1. File

- ***Exit*** - closes the **AVG 8.5 File Server**'s user interface. However, the AVG application will continue running in the background and your computer will still be protected!

7.1.2. Components

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

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

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

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

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

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

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

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

7.1.3. History

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

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

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

- ***Event History Log*** - opens the history log interface with an overview of all logged **AVG 8.5 File Server** actions.

7.1.4. Tools

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

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

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

- ***Update*** - automatically launches the update process of **AVG 8.5 File Server**

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

- ***Advanced settings*** - opens the ***AVG advanced settings*** dialog where you can edit the **AVG 8.5 File Server** configuration. Generally, it is recommended to keep the default settings of the application as defined by the software vendor.

7.1.5. Help

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

7.2. Security Status Info

The ***Security Status Info*** section is located in the upper part of the AVG main window. Within this section you will always find information on the current security status of your **AVG 8.5 File Server**. Please see an overview of icons possibly depicted in this section, and their meaning:

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

 The orange icon warns that one or more components are incorrectly configured and you should pay attention to their properties/settings. There is no critical problem in AVG and you have probably decided to switch some

component off for some reason. You are still protected by AVG. However, please pay attention to the problem component's settings! Its name will be provided in the ***Security Status Info*** section.

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

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

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

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

7.3. Quick Links

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

- ***Overview*** - use this link to switch from any currently opened AVG interface to the default one with an overview of all installed components - see chapter ***Components Overview >>***

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

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

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

7.4. Components Overview

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

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

- Description of a selected component

Within the **AVG 8.5 File Server** the ***Components Overview*** section contains information on the following components:

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

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

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

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

- ***Update Manager*** controls all AVG updates - details >>

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

7.5. Statistics

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

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

7.6. System Tray Icon

System Tray Icon (*on your Windows taskbar*) indicates the current status of your **AVG 8.5 File Server**. It is visible at all times on your system tray, no matter whether your AVG main window is opened or closed.

If in full color  , the ***System Tray Icon*** indicates that all AVG components are active and fully functional. 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*** 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 two 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!)*

8. AVG Components

8.1. Anti-Virus

8.1.1. Anti-Virus Principles

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

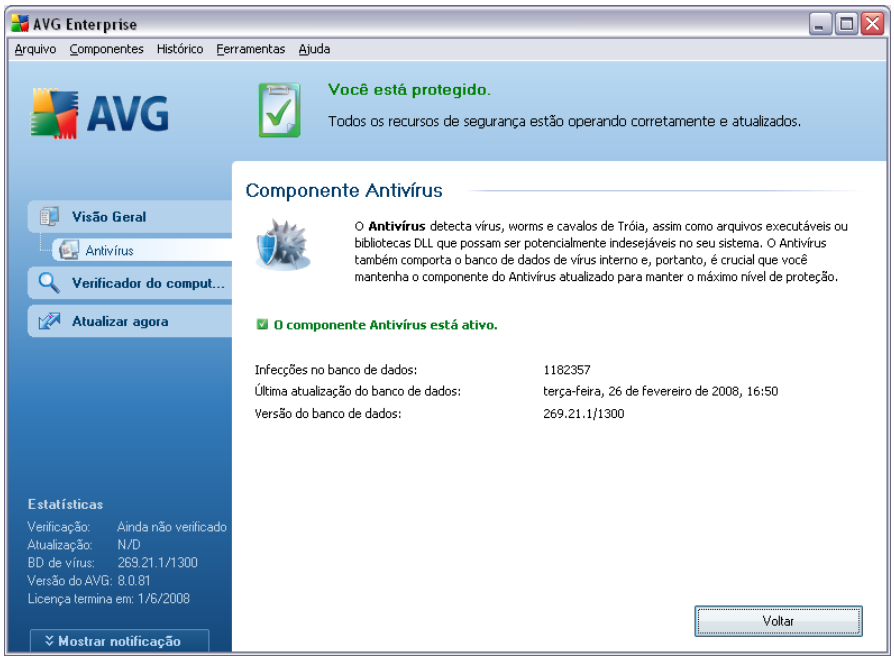
The important feature of antivirus protection is that no known virus can run on the computer!

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

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

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

8.1.2. Anti-Virus Interface



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

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

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

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

8.2. Anti-Spyware

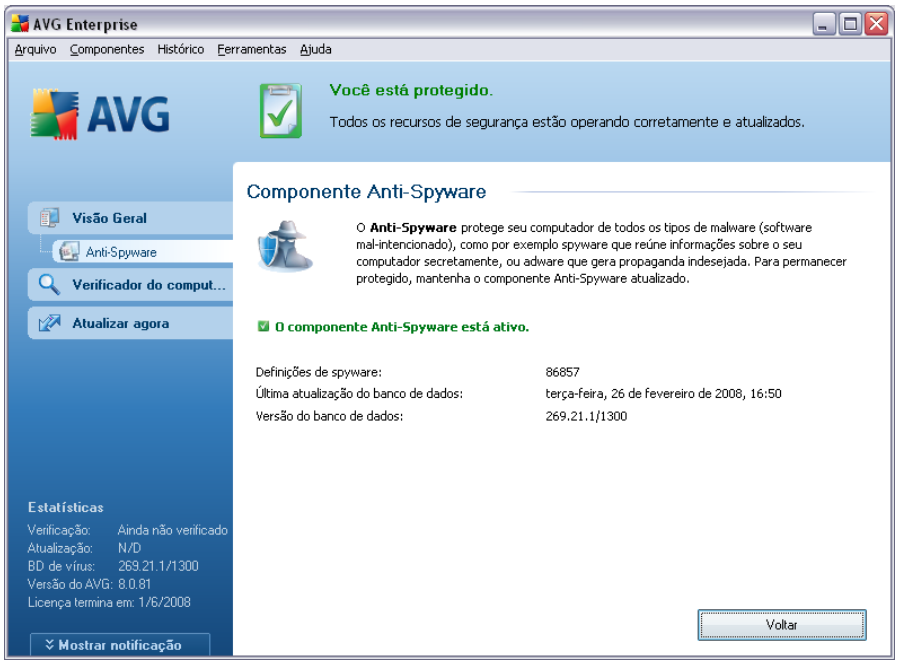
8.2.1. Anti-Spyware Principles

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

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

There is also the potential risk that malware has been transmitted to your computer prior to AVG installation, or that you have neglected to keep your **AVG 8.5 File Server** up-to-date with the latest database and program updates. For this reason, AVG allows you to fully scan your computer for malware/spyware using the scanning feature. It also detects sleeping and non-active malware, i.e. malware that has been downloaded but not yet activated.

8.2.2. Anti-Spyware Interface



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

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

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

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

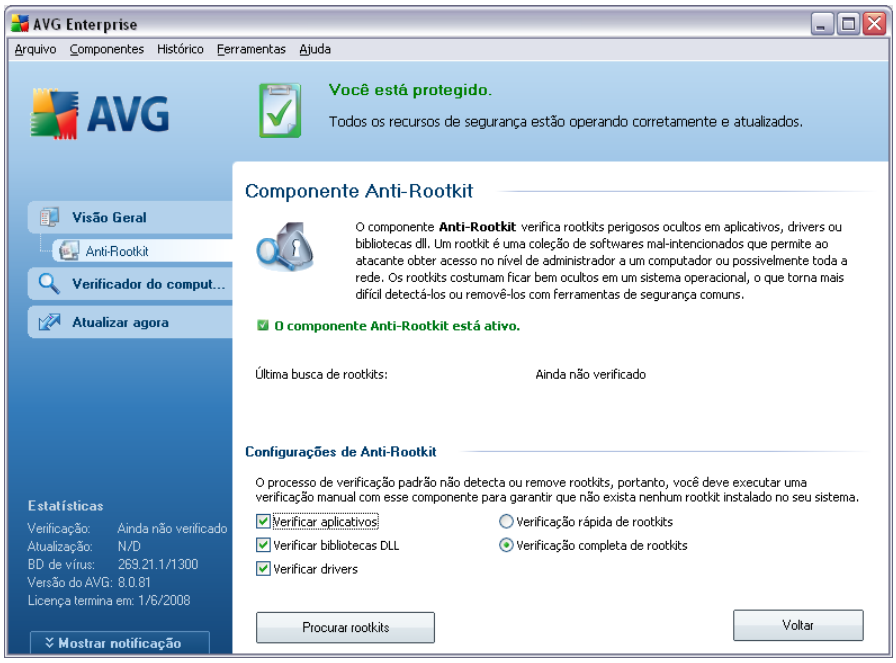
8.3. Anti-Rootkit

8.3.1. Anti-Rootkit Principles

Anti-Rootkit is a specialized tool detecting and effectively removing dangerous rootkits, i.e. programs and technologies that can camouflage the presence of malicious software on your computer.

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

8.3.2. Anti-Rootkit Interface



The ***Anti-Rootkit*** user interface provides a brief description of the component's functionality, informs on the component's current status (*Anti-Rootkit component is active.*) and also brings information on the last time the ***Anti-Rootkit*** test was launched.

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

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

Further you can pick the rootkit scanning mode:

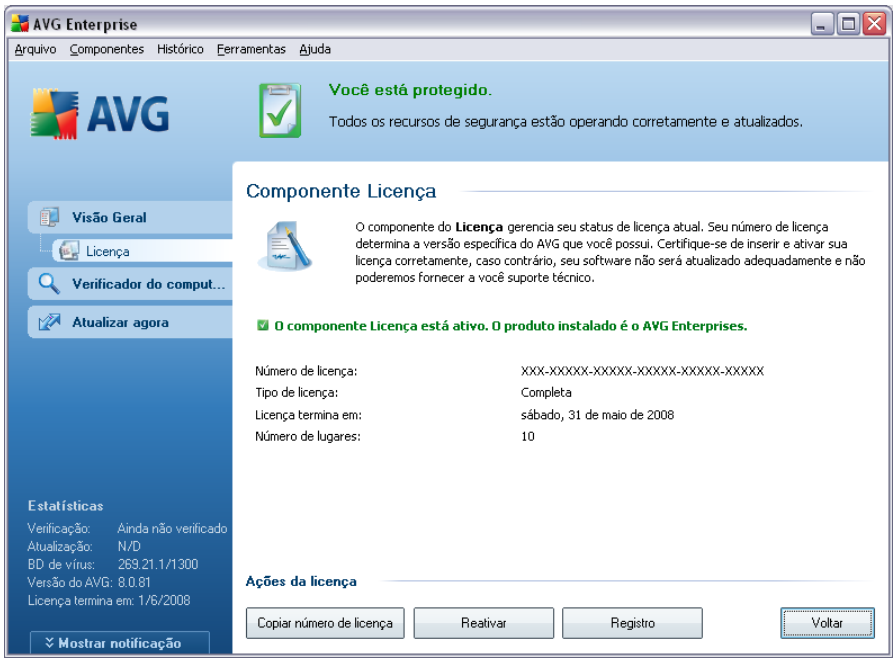
- ***Quick rootkit scan*** - scans only the system folder (*typically c:\Windows*)
- ***Full rootkit scan*** - scans all accessible disks except for A: and B:

Control buttons available:

- ***Search for rootkits*** - since the rootkit scan is not an implicit part of the ***Scan of the whole computer***, you can run the rootkit scan directly from the ***Anti-Rootkit*** interface using this button

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

8.4. License



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

- ***License number*** - provides the exact form of your license number. When entering your license number, you have to be absolutely precise and type it exactly as shown. For your comfort, the ***License*** dialog offers the ***Copy license number*** button: press the button to copy the license number into the clipboard, and then you can simply paste it anywhere you like (***CTRL+V***).

- ***License type*** - specifies the product edition defined by your license number.

- ***License expires*** - this date determines the period of validity of your license. If you want to go on using AVG after this date you have to renew your license.

The license renewal can be performed online on the AVG website.

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

Control buttons

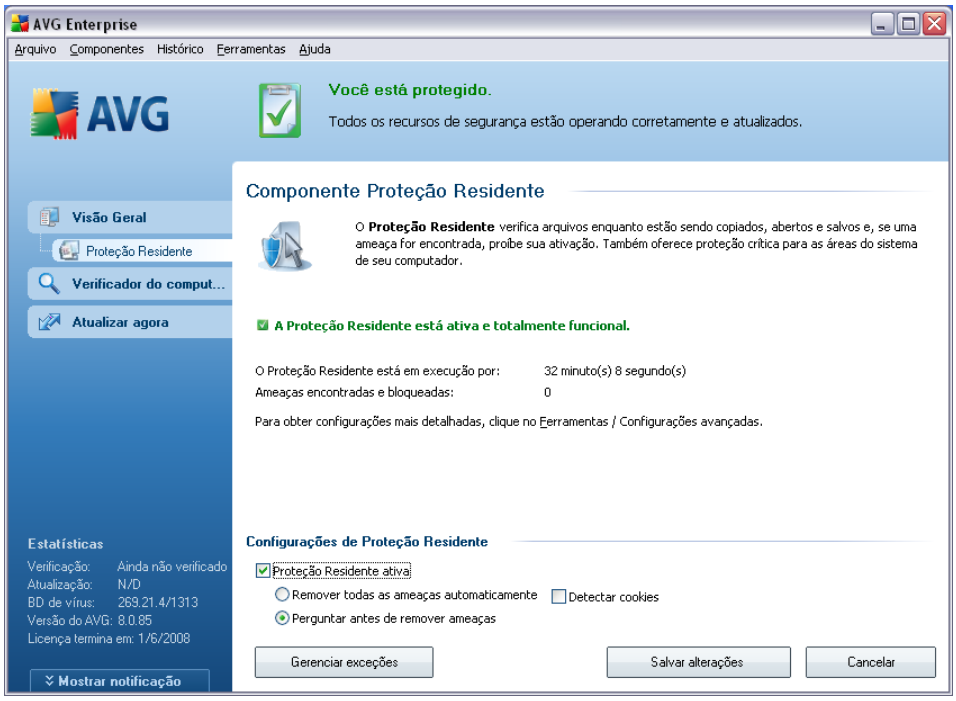
- ***Copy license number*** - press the button to insert the currently used license number into clipboard (*just like with CTRL+C*), and you can paste it wherever needed
- ***Re-activate*** - opens the ***Activate AVG*** dialog with the data you have entered in the ***Personalize AVG*** dialog of the installation process. Within this dialog you can enter your license number to either replace the sales number (*the number you have installed AVG with*), or to replace the old license number (*e. g. when upgrading to a new AVG product*).
- ***Register*** - connects to the registration website at www.avg.com. Please fill in your registration data; only customers who register their AVG product can receive free technical support.
- ***Back*** - press this button to return to the default AVG user interface (components overview)

8.5. Resident Shield

8.5.1. 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.

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

Basic component configuration

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

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

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

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

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

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

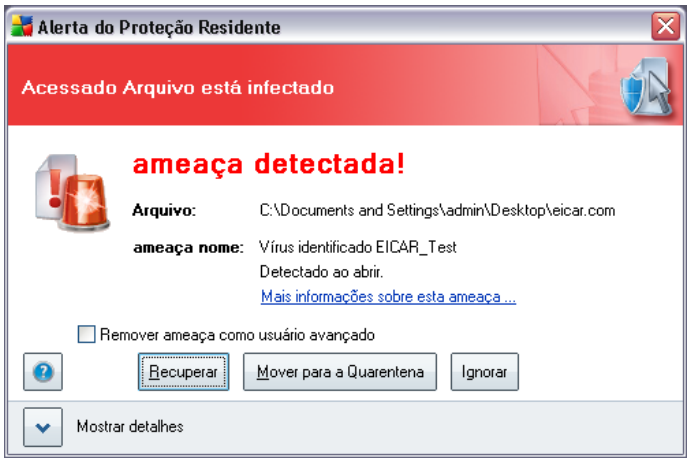
Control buttons

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

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

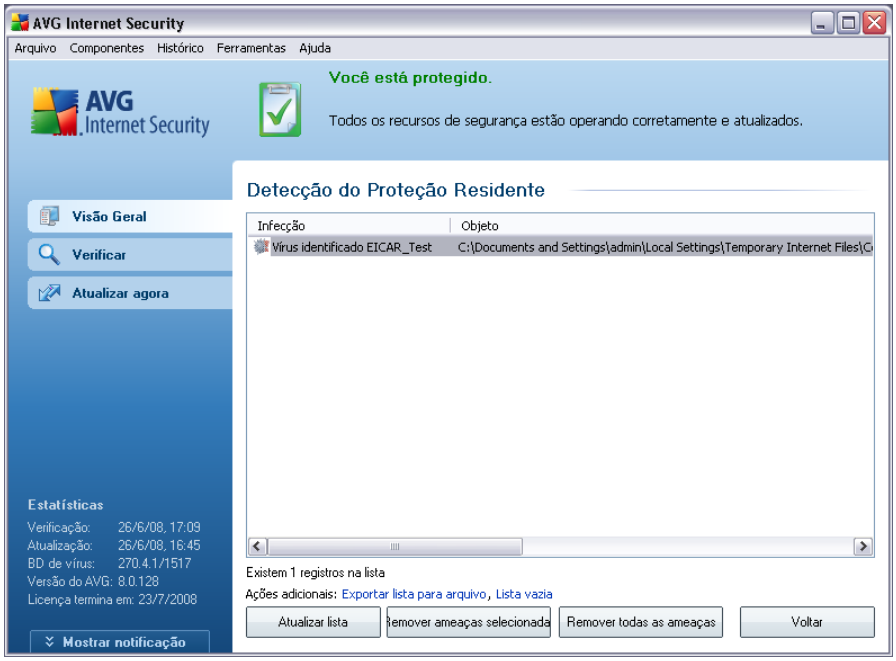
8.5.3. Resident Shield Detection

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



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

- ***Heal*** - if a cure is available, AVG will heal the infected file automatically; this option is the recommended action to be taken
- ***Move to Vault*** - the virus will be moved to AVG ***Virus Vault***
- ***Ignore*** - we strictly recommend NOT TO use this option unless you have a very good reason to do so!



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
- ***Object Type*** - type of the detected object
- ***Process*** - what action was performed to call out the potentially dangerous object so that it could be detected

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

8.6. Update Manager

8.6.1. 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!*

8.6.2. 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

Basic component configuration

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

Further you can define when the update should be launched:

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

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

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

Control buttons

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

- ***Update now*** - launches an immediate update on demand
- ***Save changes*** - press this button to save and apply any changes made in this dialog

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

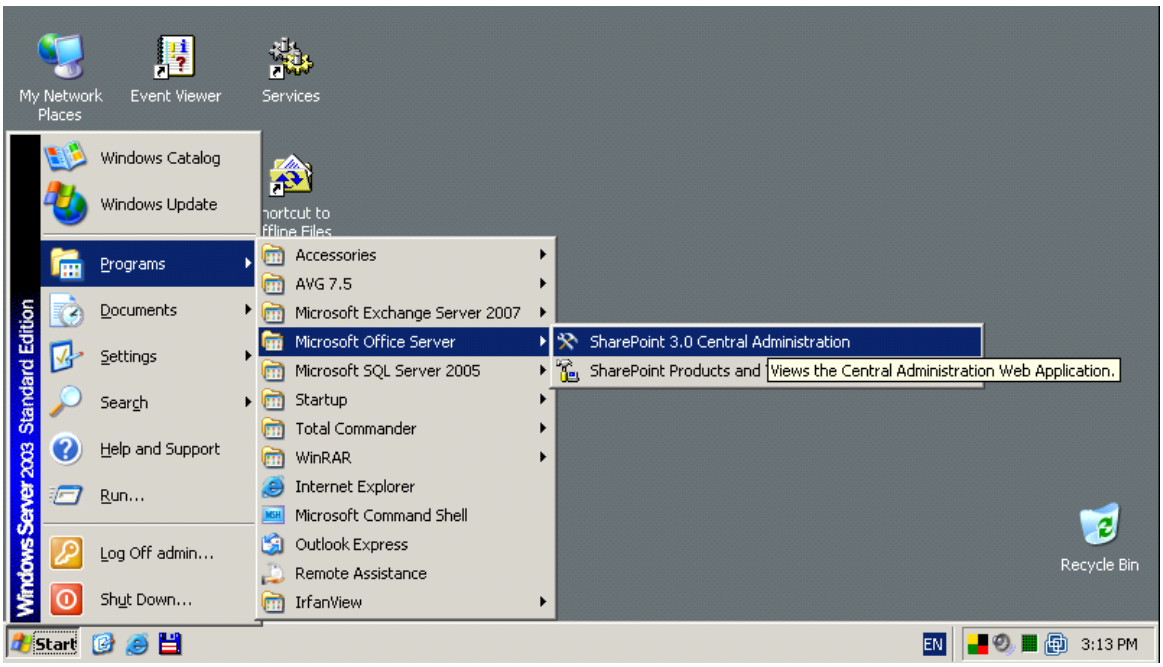
9. AVG for SharePoint Portal Server

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

9.1. Program Maintenance

AVG 8.5 for SharePoint Portal Server uses the Microsoft SP VSAPI 1.4 virus-scanning interface for the protection of your server against possible virus infection. The objects on the server are tested for the presence of malware when they are downloaded and/or uploaded from or on the server by your users. The configuration of the anti-virus protection can be set up using the ***Central Administration*** interface of your SharePoint Portal Server. Within the ***Central Administration*** you can also view and manage the **AVG 8.5 for SharePoint Portal Server** log file.

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

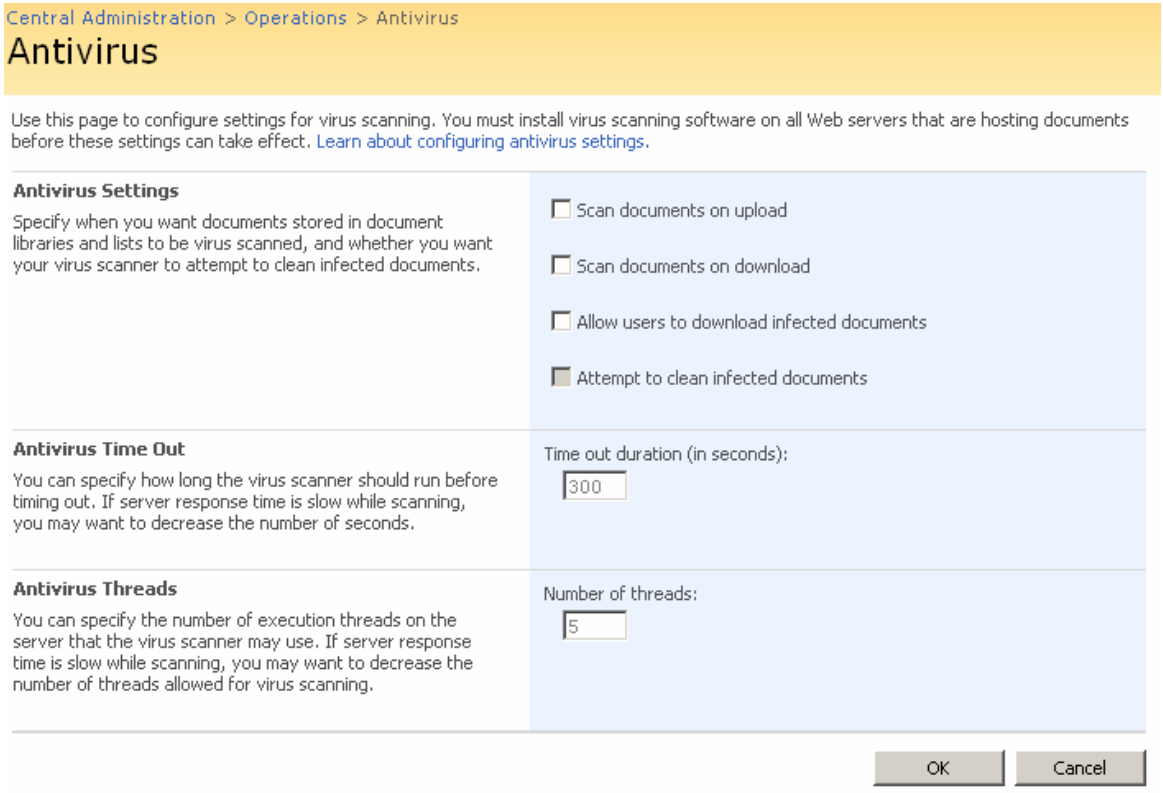


You can also enter the ***SharePoint Portal Server Central Administration*** web page remotely using the proper access rights and URL.

9.2. AVG for SPPS Configuration - SharePoint 2007

In the ***SharePoint 3.0 Central Administration*** interface you can easily configure the performance parameters and actions of the **AVG 8.5 for SharePoint Portal Server** scanner. Choose the ***Operations*** option in the ***Central Administration*** section. A new dialog will appear. Select ***Antivirus*** item in the ***Security Configuration*** part.

The following window will then be displayed:



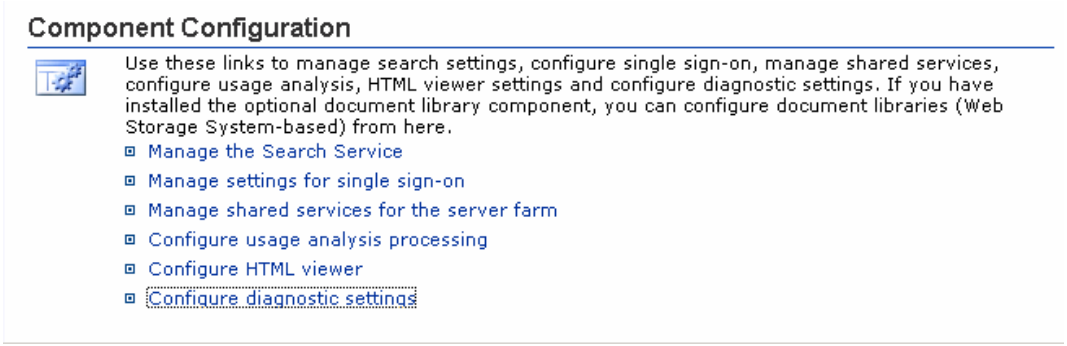
You can configure various **AVG 8.5 for SharePoint Portal Server** anti-virus scanning actions and performance features here:

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

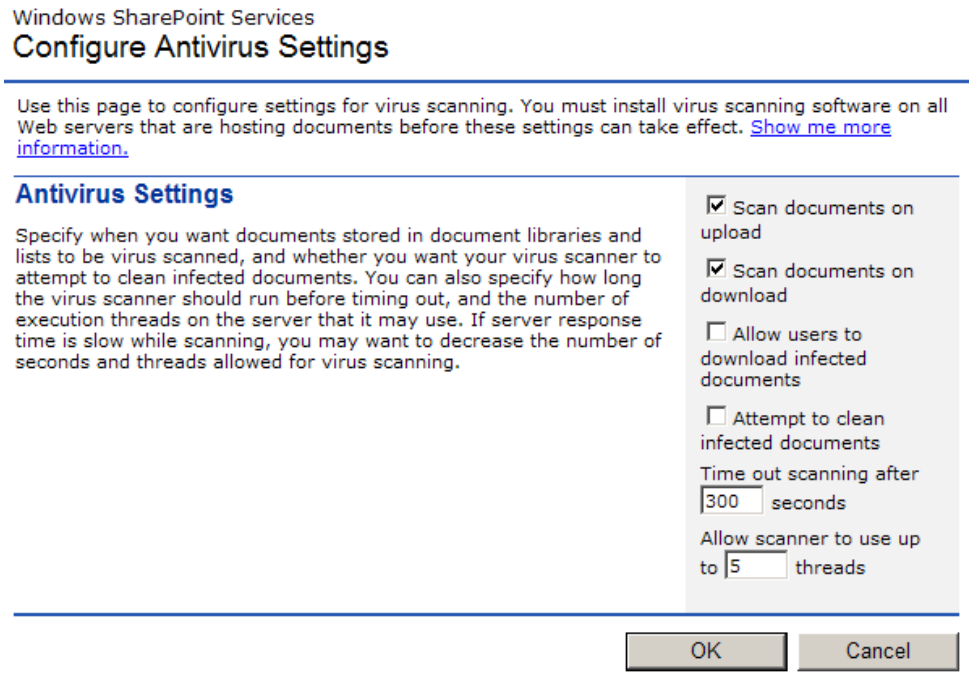
- ***Number of threads*** – you can specify the number of virus scanning threads that can run simultaneously; increasing the number may speed up the scanning due to the higher level of parallelism, but it can increase the server's response time on the other hand

9.3. AVG for SPPS Configuration - SharePoint 2003

In the ***SharePoint Portal Server Central Administration*** interface you can easily configure the performance parameters and actions of the **AVG 8.5 for SharePoint Portal Server** scanner. Choose the ***Antivirus Actions Configuration*** option in the ***Security Configuration*** section:



The following window will then be displayed:



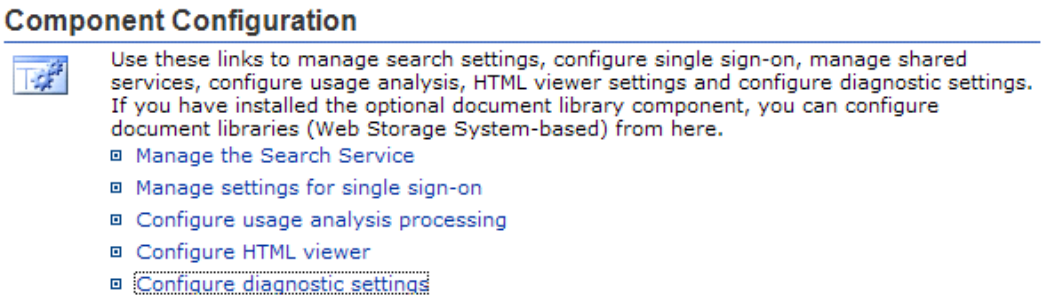
You can configure various **AVG 8.5 for SharePoint Portal Server** anti-virus scanning actions and performance features here:

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

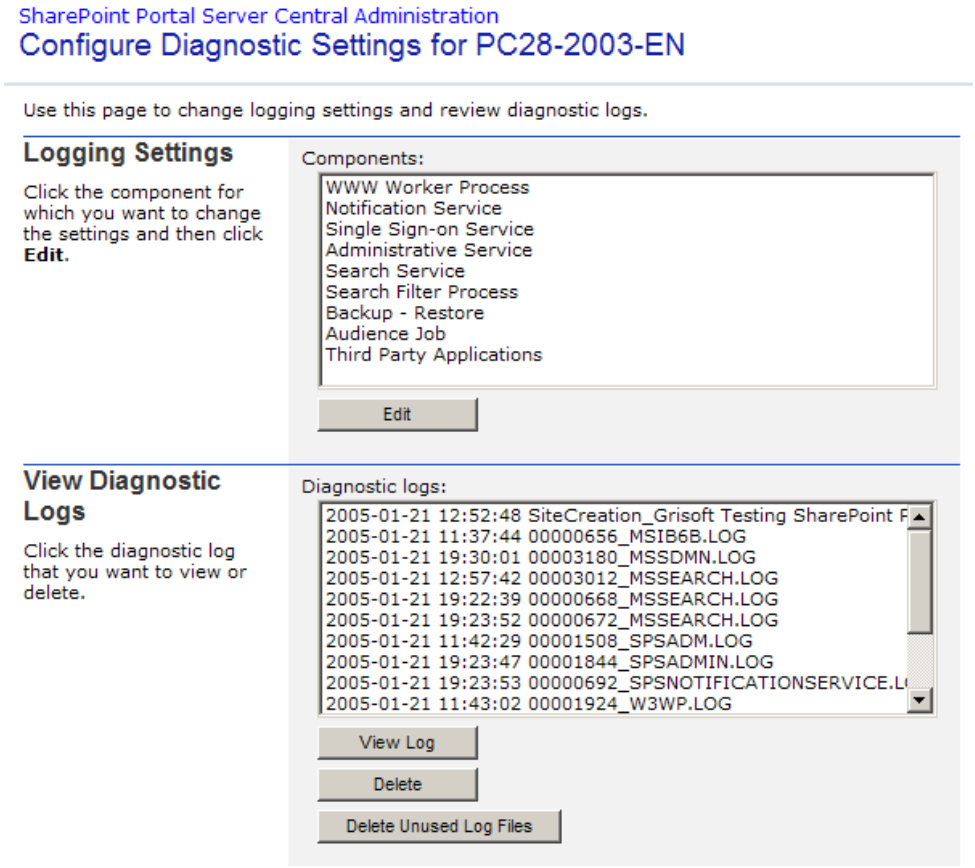
but it can increase the server's response time on the other hand

9.4. AVG for SPPS Edition Diagnostics

The diagnostics messages of **AVG 8.5 for SharePoint Portal Server** can be viewed after choosing the ***Diagnostics Settings Configuration*** in the ***SharePoint Central Administration's Component Configuration*** section:



All diagnostics information related to **AVG 8.5 for SharePoint Portal Server** performance are stored in the *_AVG4SPS.LOG file. The contents of this file can be viewed after choosing it in the ***Display diagnostics protocols*** section of the ***Diagnostics Settings Configuration*** window:



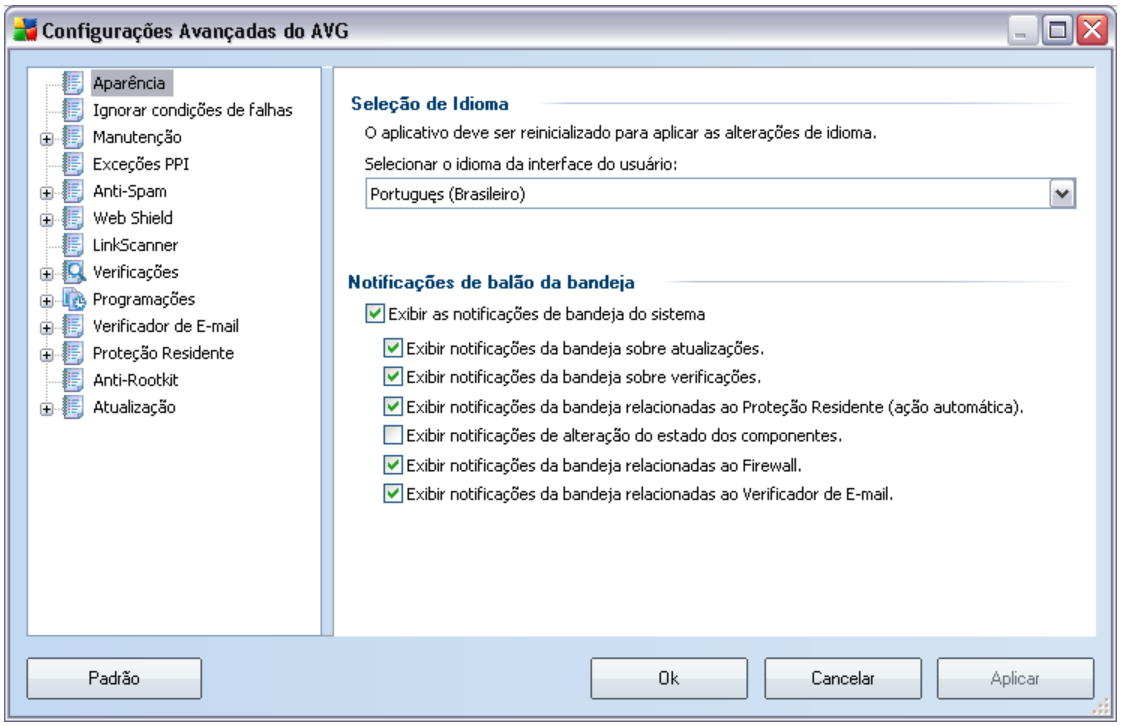
Press the ***View log*** button to view the log file of **AVG 8.5 for SharePoint Portal Server**.

10. AVG Advanced Settings

The advanced configuration dialog of **AVG 8.5 File Server** opens in a new window named ***Advanced AVG Settings***. The window is divided into two sections: the left part offers a tree-arranged navigation to the program configuration options. Select the component you want to change the configuration of (*or its specific part*) to open the editing dialog in the right-hand section of the window.

10.1.Appearance

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



Language selection

In the ***Language selection*** section you can chose your desired language from the drop-down menu; the language will then be used for the entire AVG user interface. The drop-down menu only offers those languages you have previously selected to be installed during the installation process (see chapter Custom Installation - Component Selection). However, to finish switching the application to another language you have

to restart the user interface; follow these steps:

- Select the desired language of the application and confirm your selection by pressing the ***Apply*** button (right-hand bottom corner)
- Press the ***OK*** button to close the ***Advanced AVG Settings*** editing dialog
- Close the AVG user interface via the system menu item option ***File/Exit***
- Re-open the AVG user interface by one of these options: double-click the AVG system tray icon, double-click the AVG icon on your desktop, or via the menu ***Start/All Programs/AVG 8.0/AVG User Interface*** (see chapter ***Access to User Interface***). The user interface will then be displayed in the newly selected language.

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!

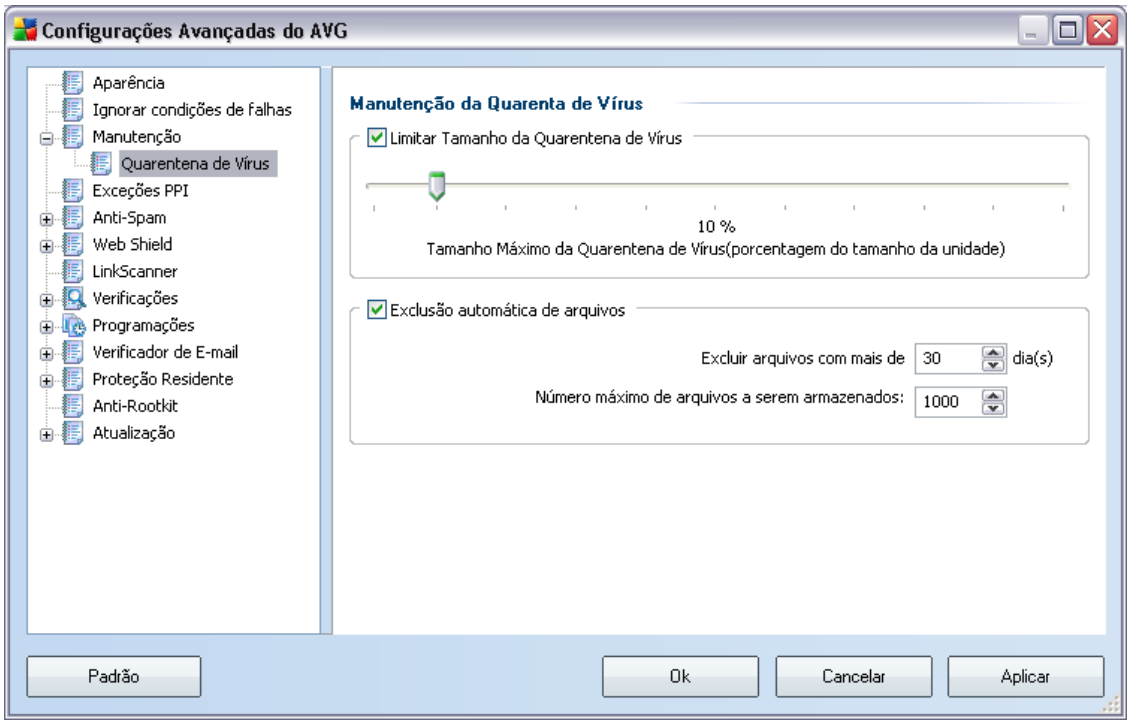
However, if for some reason you decide you do not wish these notifications to be displayed, or you would like only certain notifications (related to a specific AVG component) to be displayed, you can define and specify your preferences by checking/unchecking the following options:

- ***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.

10.2.Virus Vault



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

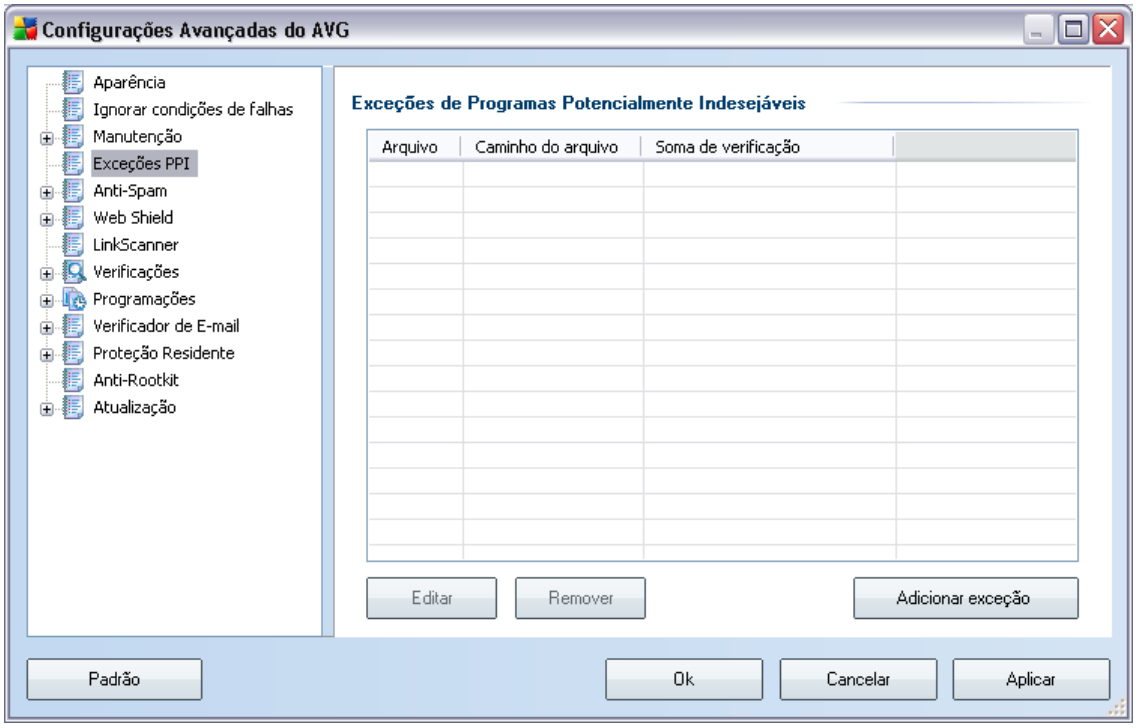
- ***Limit Virus vault size*** - use the slider to set up the maximum size of the ***Virus Vault***. The size is specified proportionally compared to the size of your

local disk.

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

10.3.PUP Exceptions

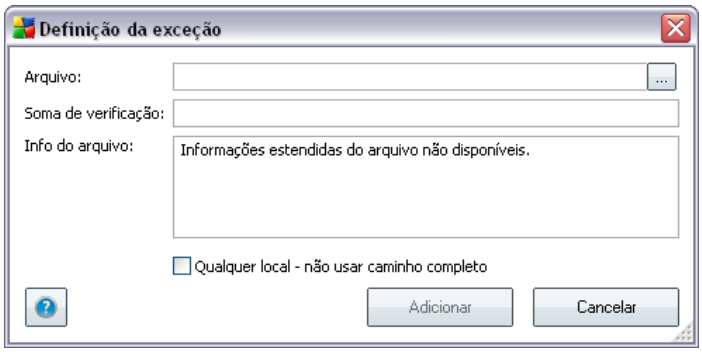
AVG is able to analyze and detect executable applications or DLL libraries that could be potentially unwanted within the system. In some cases the user may wish to keep certain unwanted programs on the computer, (programs that were installed on purpose). Some programs, especially free ones, include adware.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

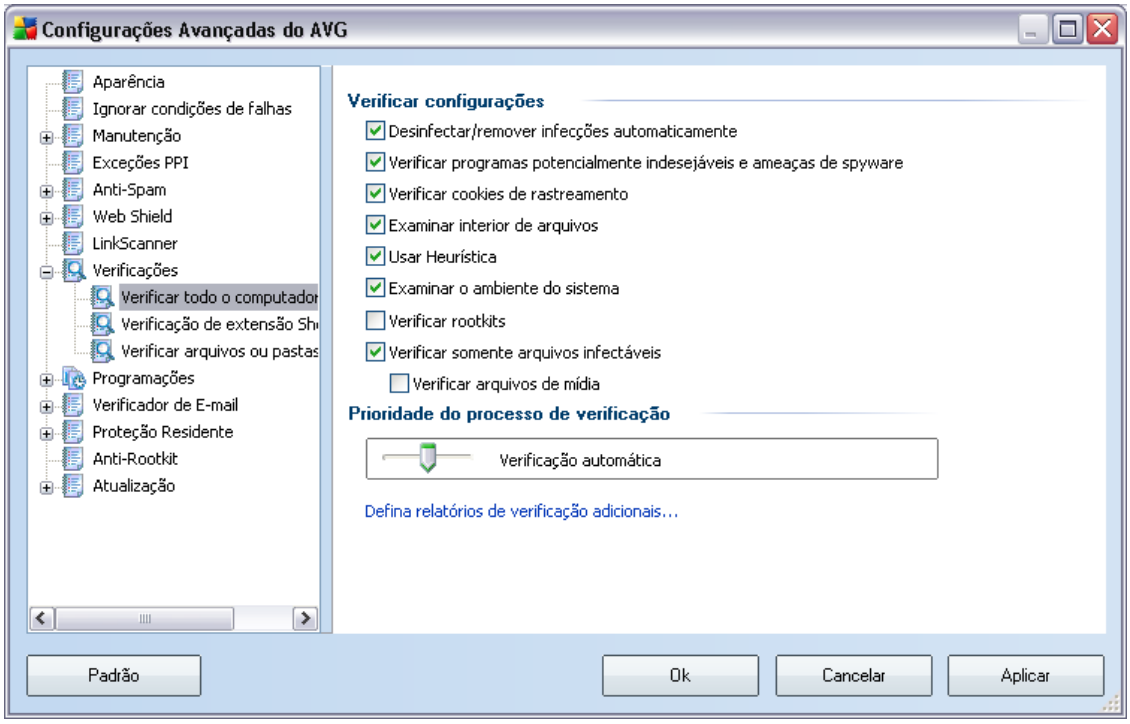
10.4.Scans

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

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

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

- ***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 media files*** – check to scan media files (Video, Audio etc.). If you leave this box unchecked, it will reduce the scanning time even more, because these files are often quite large and are not too likely to be

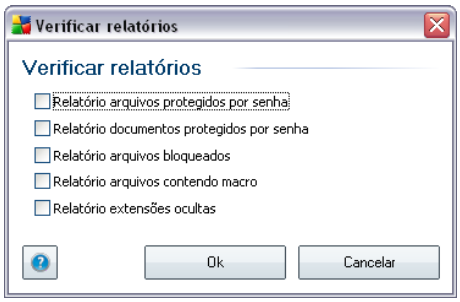
infected by a virus.

Scan process priority

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

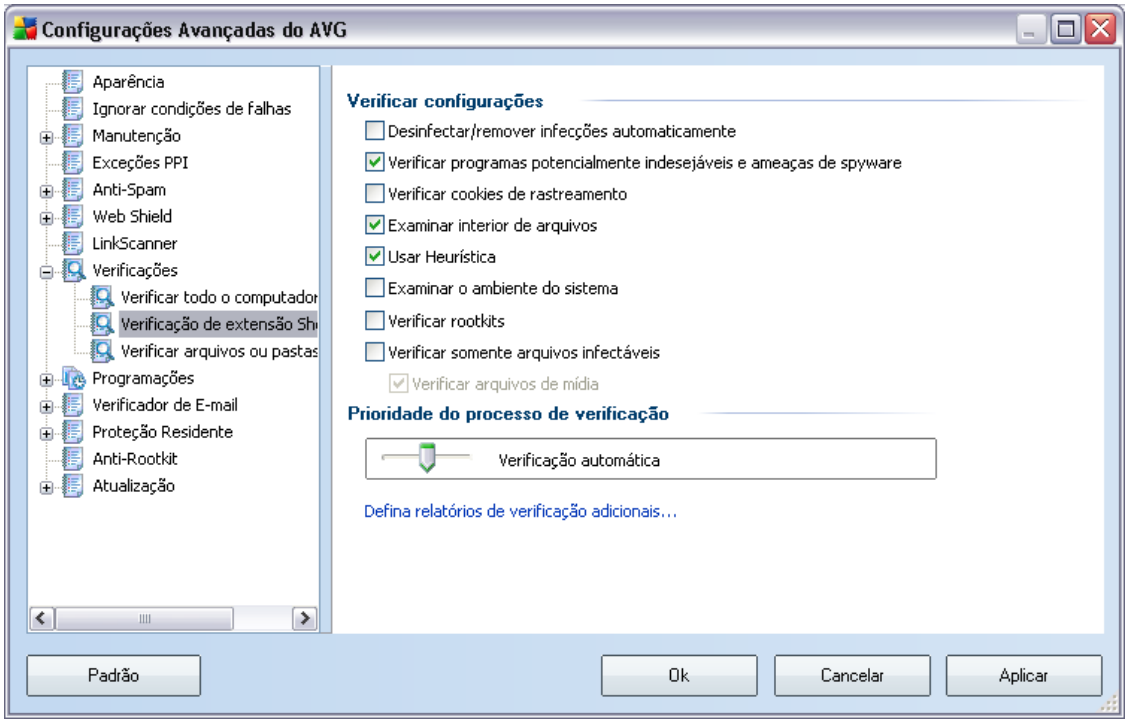
Set additional scan reports ...

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



10.4.2.Shell Extension Scan

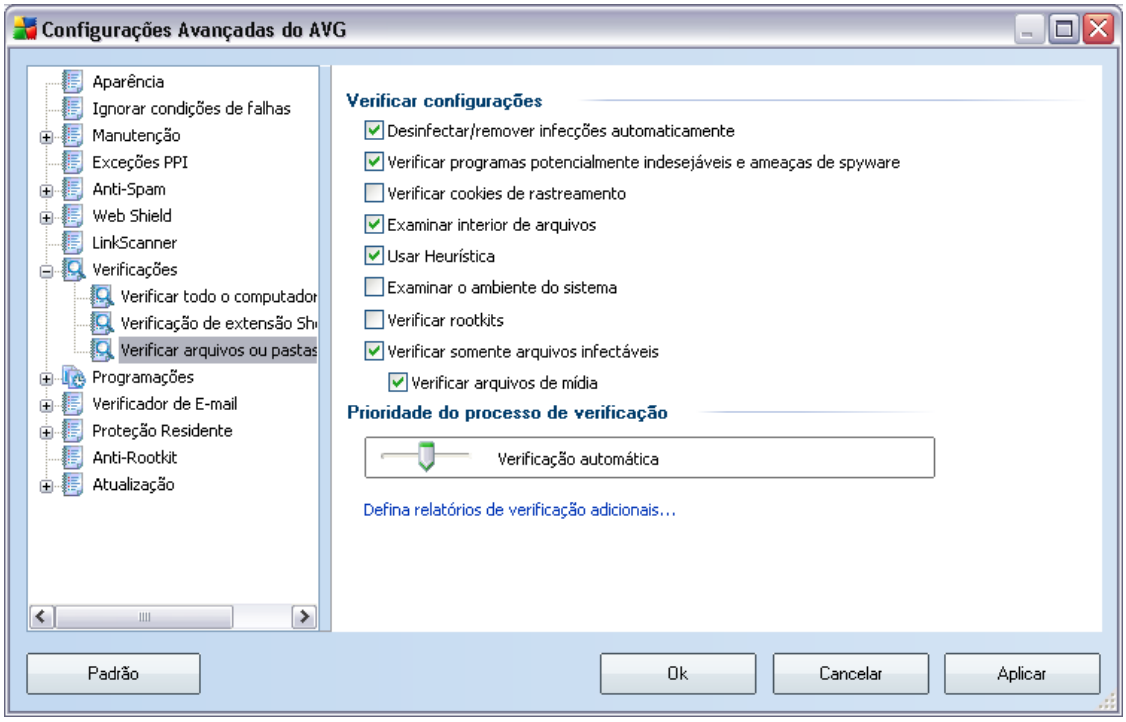
Similar to the previous ***Scan whole computer*** item, this item named ***Shell extension scan*** also offers several options for editing the scan predefined by the software vendor. This time the configuration is related to scanning of specific objects launched directly from the Windows Explorer environment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

10.4.3.Scan Specific Files or Folders

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

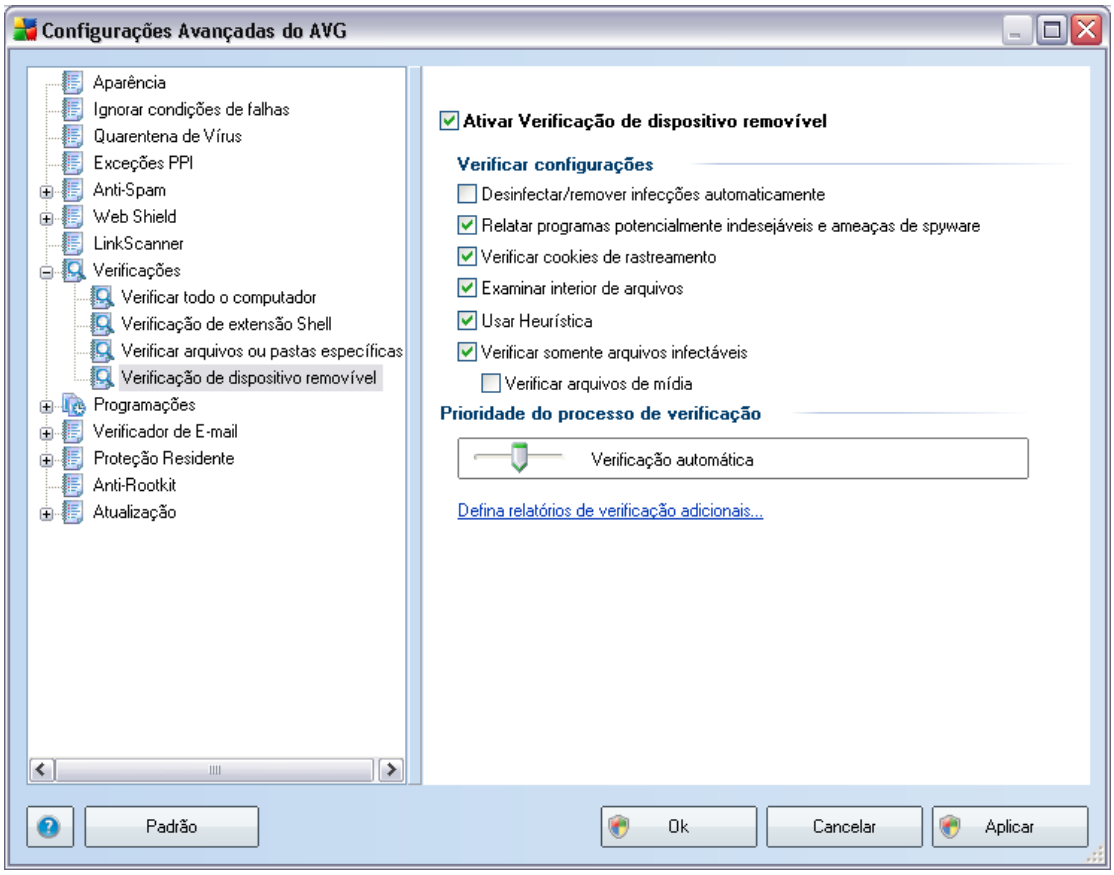


All parameters set up in this configuration dialog apply only to the areas selected for scanning with the ***Scan of specific files or folders***! If you tick the ***Scan for rootkits*** option within this configuration dialog, only a quick rootkit test will be performed, i.e. rootkit scanning of selected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

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

10.4.4.Removable Device Scan

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



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

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

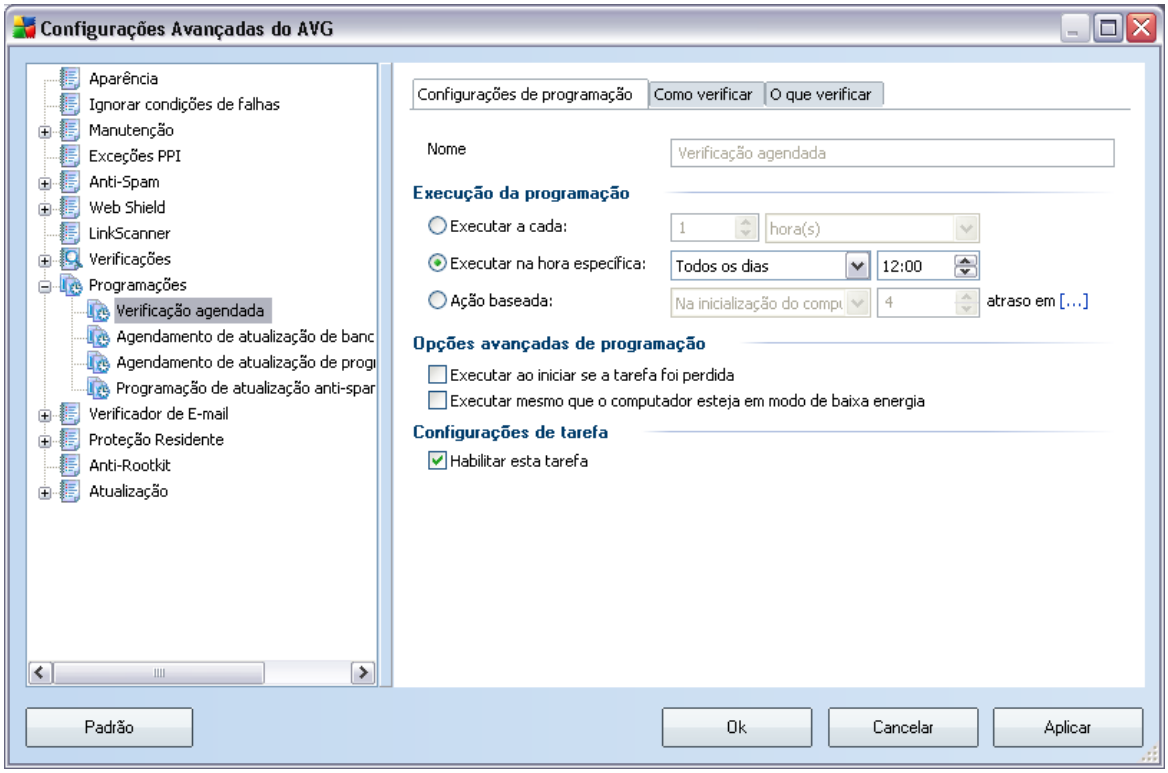
10.5.Schedules

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

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

10.5.1.Scheduled Scan

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



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

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

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

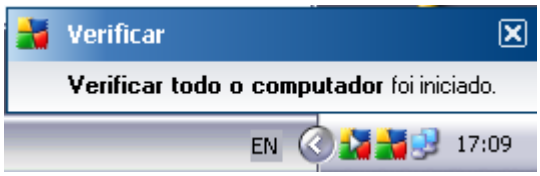
Example: *It is not appropriate to call the scan by the name of "New scan" or "My scan" since these names do not refer to what the scan actually checks. On the other hand, an example of a good descriptive name would be "System areas scan" etc. Also it is not necessary to specify in the scan's name whether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

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

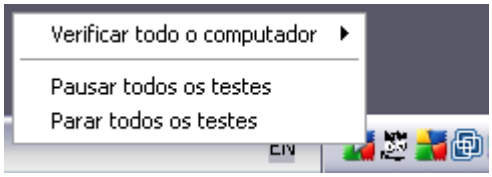
- ***Schedule running*** - specify time intervals for the newly scheduled scan launch. The timing can either be defined by the repeated scan launch after a certain period of time (***Run every ...***) or by defining an exact date and time (***Run at specific time ...***), or possibly by defining an event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

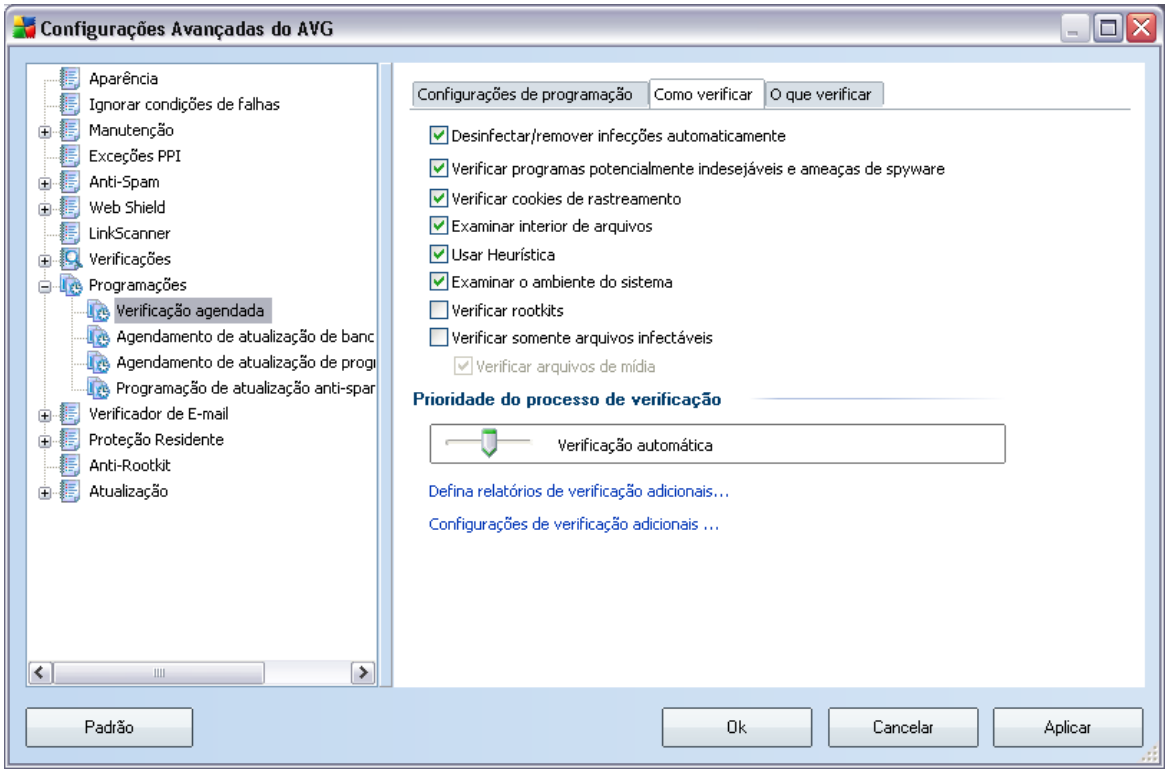
- ***Advanced schedule options*** - this section allows you to define under which conditions the scan should/should not be launched if the computer is in low power mode or switched off completely.

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



A new AVG system tray icon then appears (*in full color with a white arrow - see picture above*) informing a scheduled scan is running. Right-click on the running scan AVG icon to open a context menu where you can decide to pause or even stop the running scan:





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*** - (*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 parameter defines the scanning should check all files even if they are stored inside an archive, e.g. ZIP, RAR, ...

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

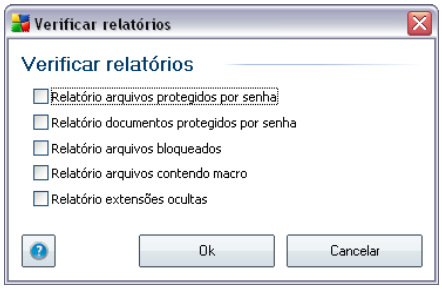
- ***Scan system environment*** - (*switched on, by default*): scanning will also check the system areas of your computer;

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

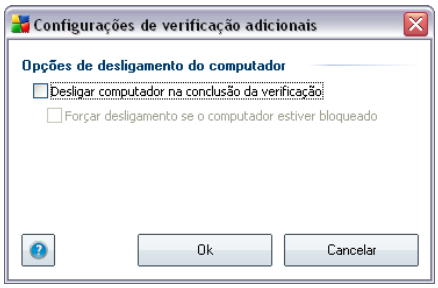
- ***Scan infectable files only*** - (*switched off, by default*): with this option switched on, scanning will not be applied to files that cannot get infected. These can be for instance some plain text files, or some other non-executable files.

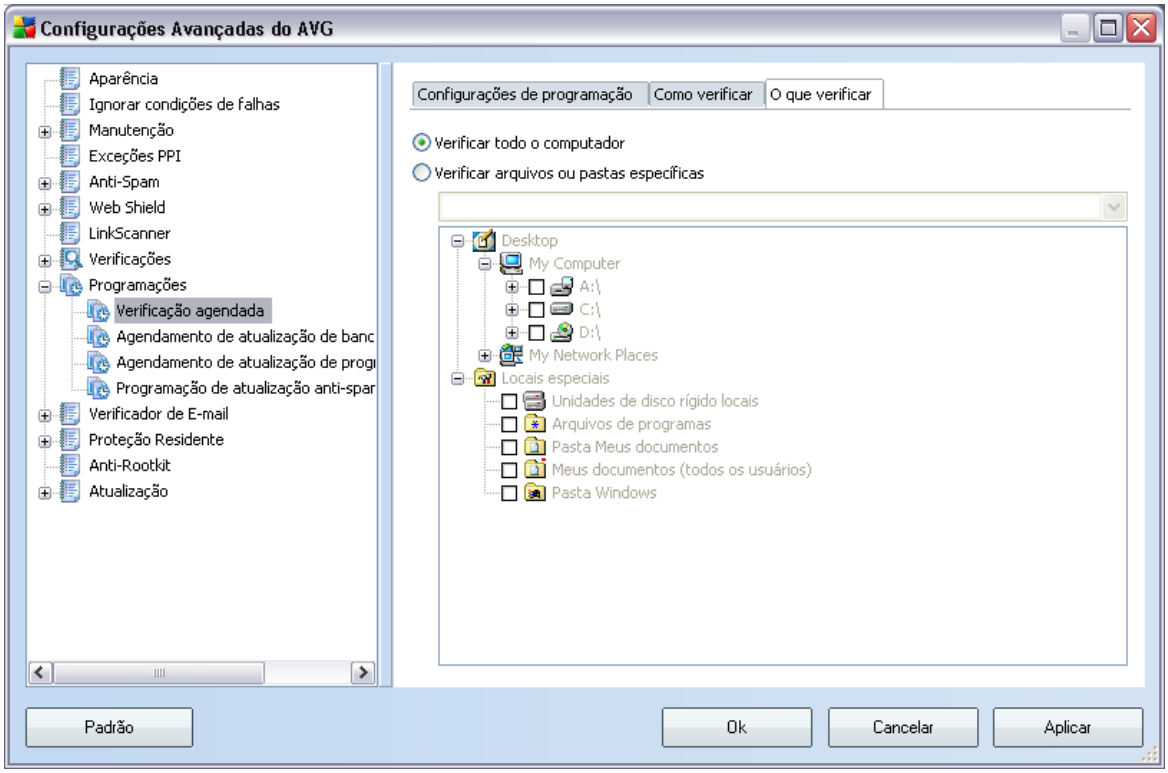
Within the ***Scan process priority*** section you can further specify the desired scanning speed dependent on system resource usage. By default, this option is set to the medium level of automatic resource usage. If you want the scanning to run faster, it will take less time but the system resources 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:



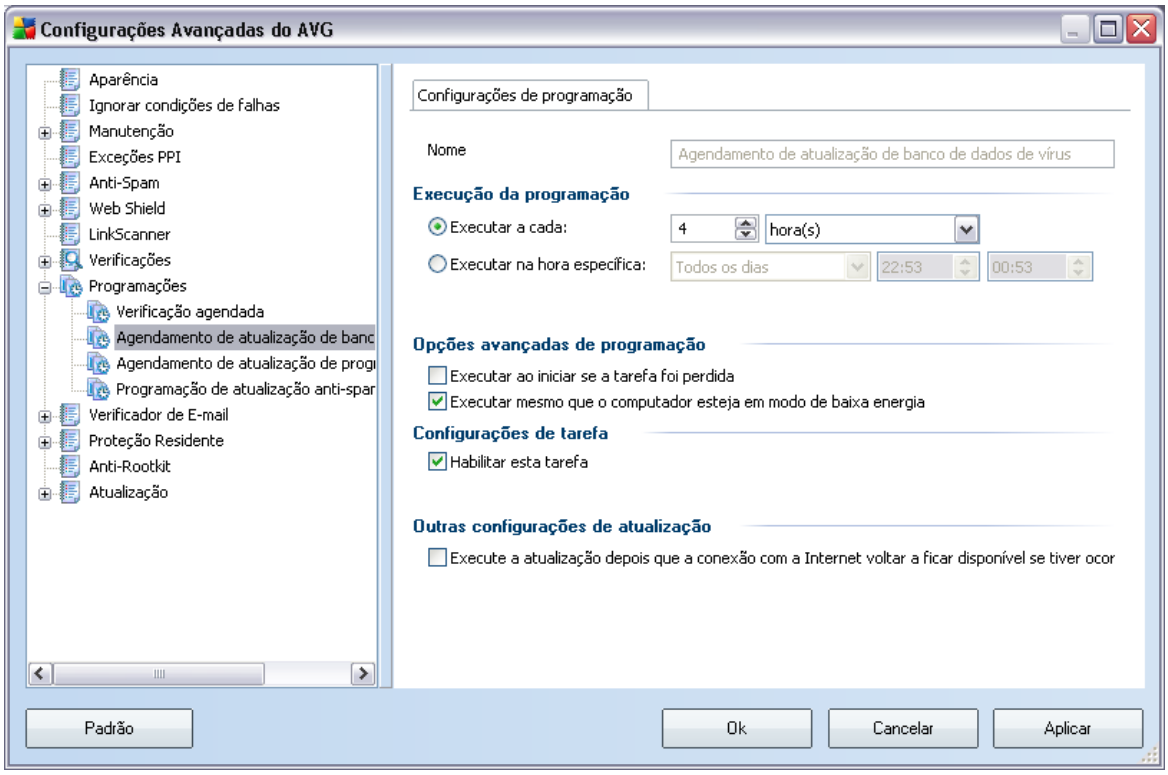
Click the ***Additional scan settings ...*** to open a new ***Computer shutdown options*** dialog where you can decide whether the computer should be shut down automatically once the running scanning process is over. Having confirmed this option (***Shutdown computer upon scan completion***), a new option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

10.5.2.Virus Database Update Schedule



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

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

Give a name to the virus database update schedule you are about to create. Type the name into the text field by the ***Name*** item. Try to use brief, descriptive and appropriate names of update schedules to make it easier to recognize the schedule among others later.

- ***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***

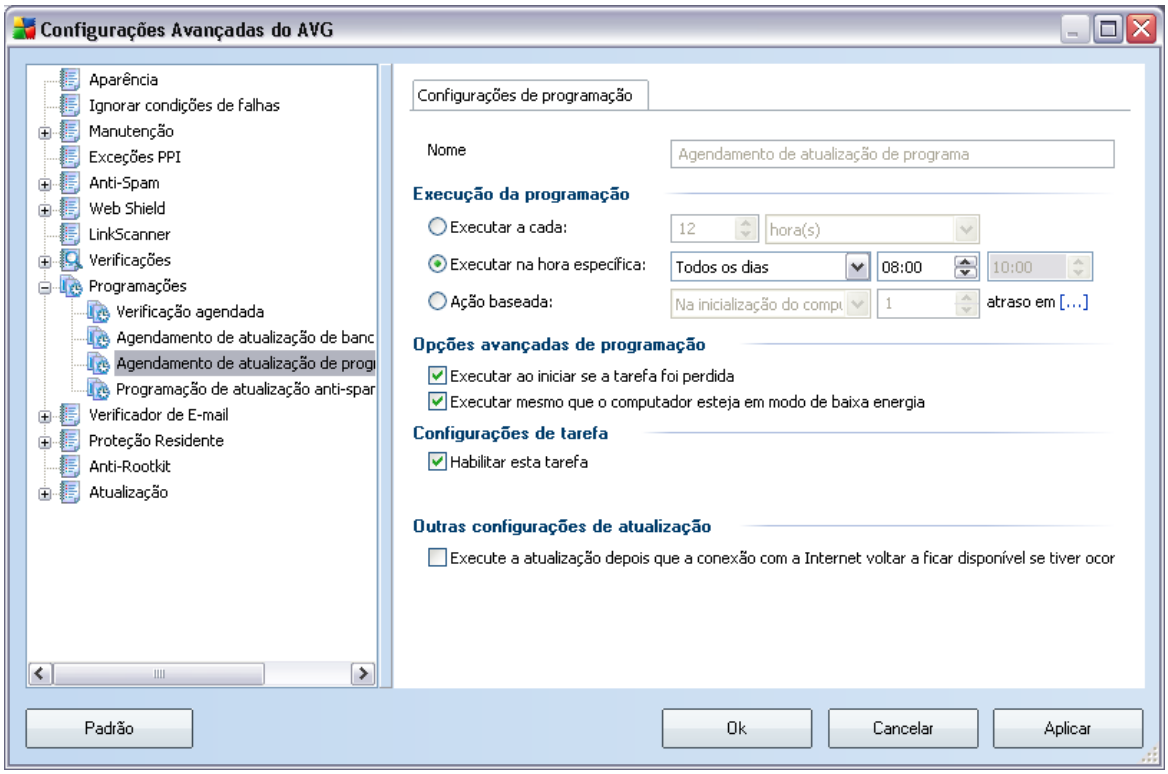
computer startup).

- ***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.

- ***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.

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

10.5.3.Program Update Schedule



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

Next, give a name to the program update schedule you are about to create. Type the name into the text field by the ***Name*** item. Try to use brief, descriptive and appropriate names of update schedules to make it easier to recognize the schedule among others later.

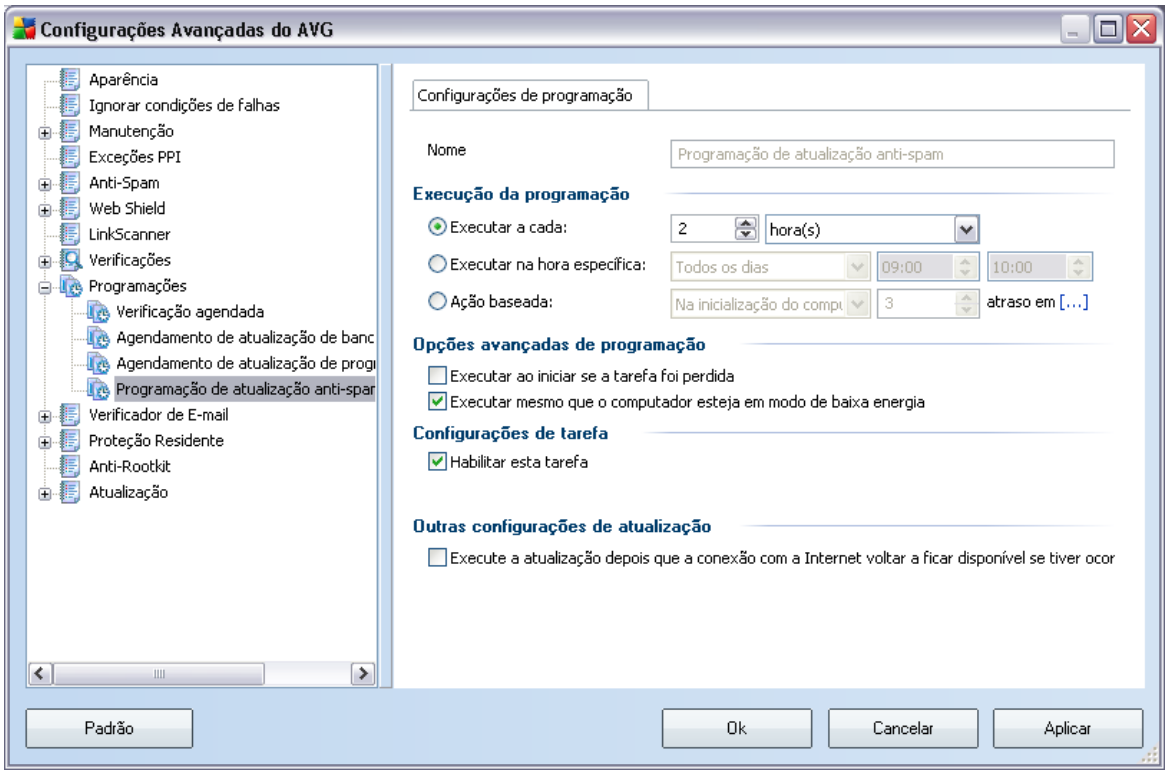
- ***Schedule running*** - specify the time intervals for the newly scheduled program update launch. The timing can either be defined by the repeated update launch after a certain period of time (***Run every ...***) or by defining an exact date and time (***Run at specific time ...***), or possibly 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.

- ***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.

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

10.5.4.Anti-Spam Update Schedule



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

Basic ***Anti-Spam*** update scheduling is covered within the ***Update Manager*** component. Within this dialog you can set up some detailed parameters of the update schedule:

Next, give a name to the ***Anti-Spam*** update schedule you are about to create. Type the name into the text field by the ***Name*** item. Try to use brief, descriptive and appropriate names of update schedules to make it easier to recognize the schedule among others later.

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

based on computer startup).

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

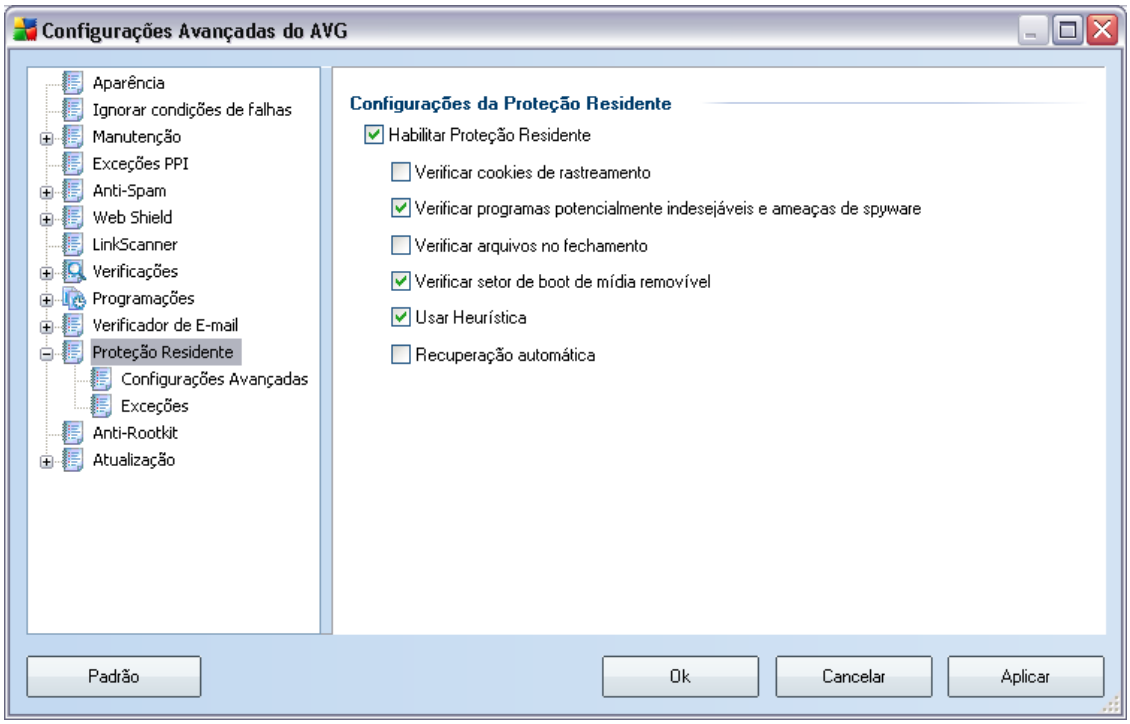
- ***Task settings*** - in this section you can uncheck the ***Enable this task*** item to simply deactivate the scheduled ***Anti-Spam*** update temporarily, and switch it on again as the need arises.

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

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

10.6.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:

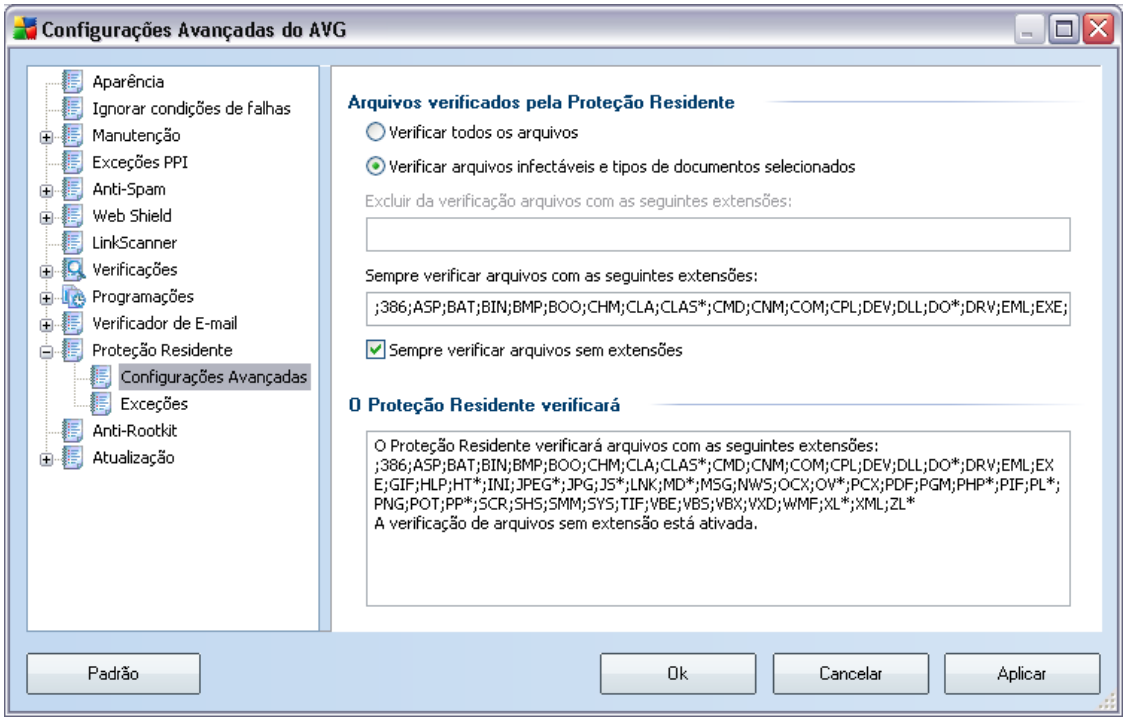
- ***Scan cookies*** - this parameter defines that cookies should be detected during scanning. (*HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts*)
- ***Scan Potentially Unwanted Programs*** - (*switched on by default*) scanning for potentially unwanted programs (*executable applications that can behave as various types of spyware or adware*)
- ***Scan on process closing*** - on-close scanning ensures that AVG scans active objects (e.g. applications, documents …) when they are being opened, and

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

- ***Scan boot sector of removable media*** - (*switched on by default*)
- ***Use Heuristics*** - (*switched on by default*) heuristic analysis will be used for detection (*dynamic emulation of the scanned object's instructions in a virtual computer environment*)
- ***Auto-heal*** - any detected infection will be healed automatically if there is a cure available

10.6.1.Advanced Settings

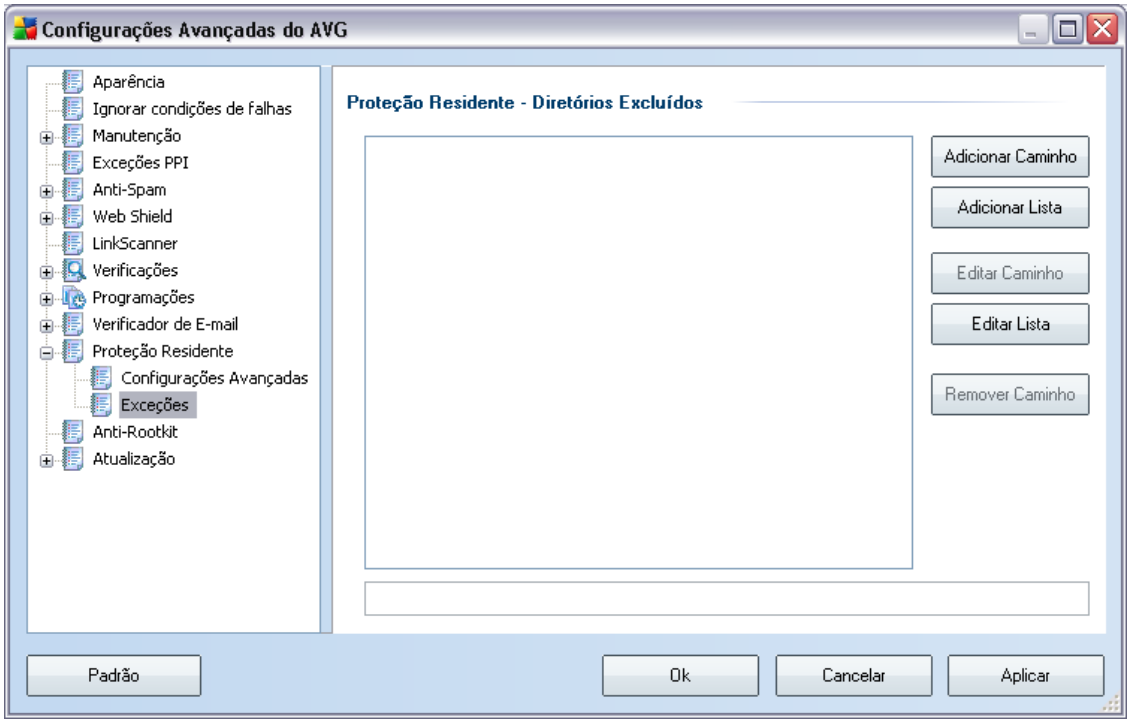
In the ***Files scanned by the Resident Shield*** dialog it is possible to configure which files will be scanned (*by specific extensions*):



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

all circumstances.

10.6.2.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, the new settings will only take effect after the computer is restarted!

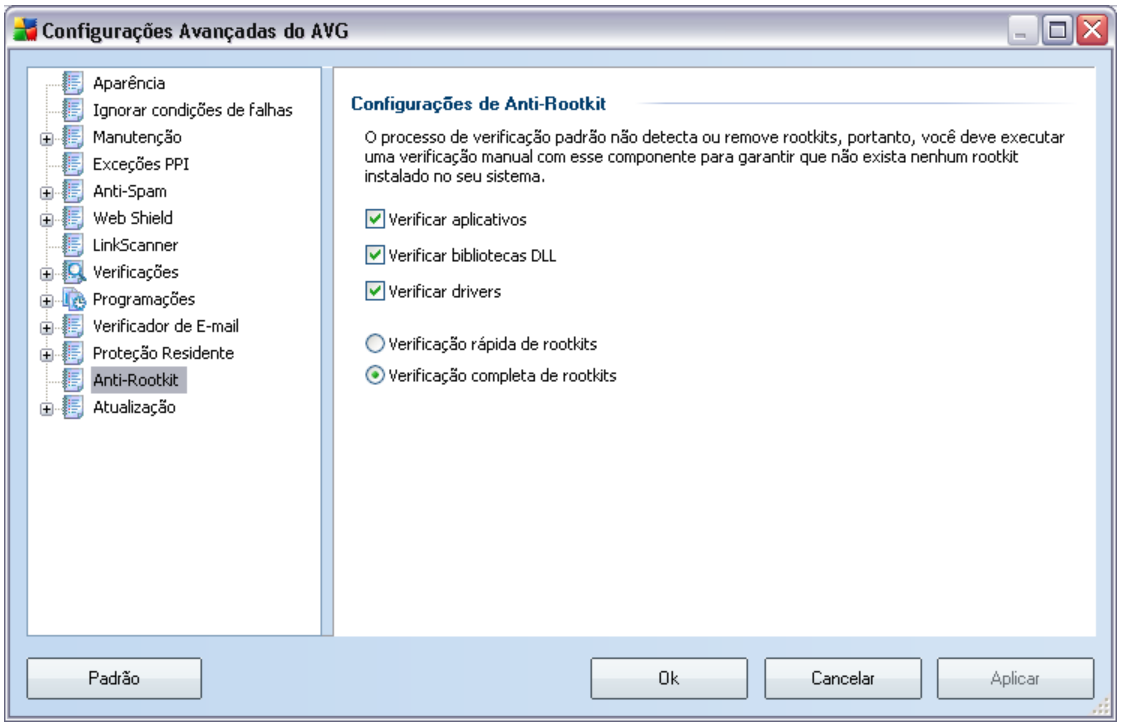
The dialog provides the following control buttons:

- ***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

10.7.Anti-Rootkit

In this dialog you can edit the ***Anti-Rootkit*** component's configuration:



Editing of all functions of the ***Anti-Rootkit*** component as provided within this dialog is also accessible directly from the ***Anti-Rootkit component's interface***.

Mark up the respective check-boxes to specify objects that should be scanned:

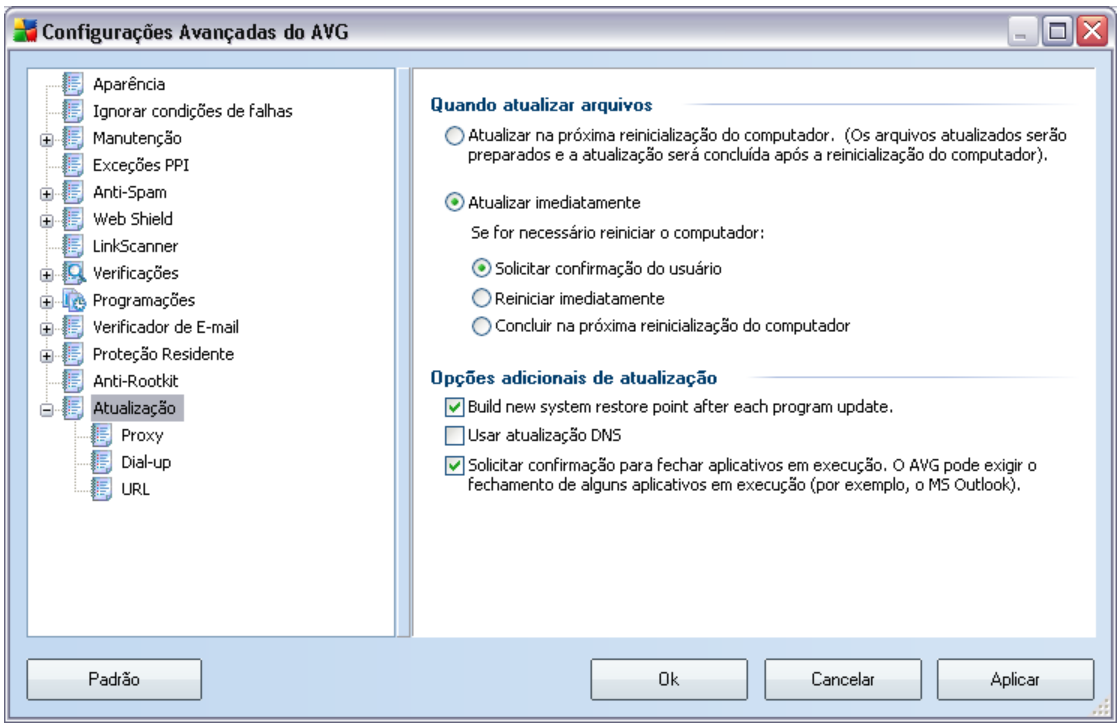
- ***Scan applications***
- ***Scan DLL libraries***
- ***Scan drivers***

Further you can pick the rootkit scanning mode:

- ***Quick rootkit scan*** - scans only the system folder (*typically c:\Windows*)

- ***Full rootkit scan*** - scans all accessible disks except for A: and B:

10.8.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

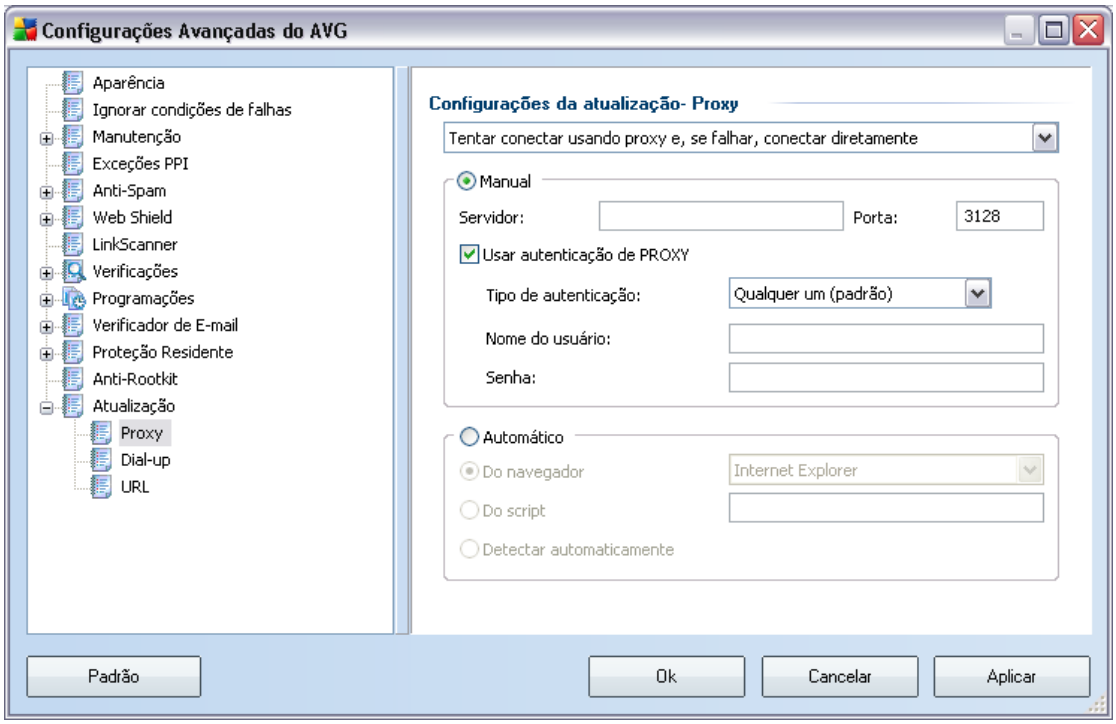
- ***Build new system restore point after each program update*** - before each AVG program update launch, a system restore point is created. In case the update process fails and your operating system crashes you can always restore your OS in its original configuration from this point. This option is 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;

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

10.8.1.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*)

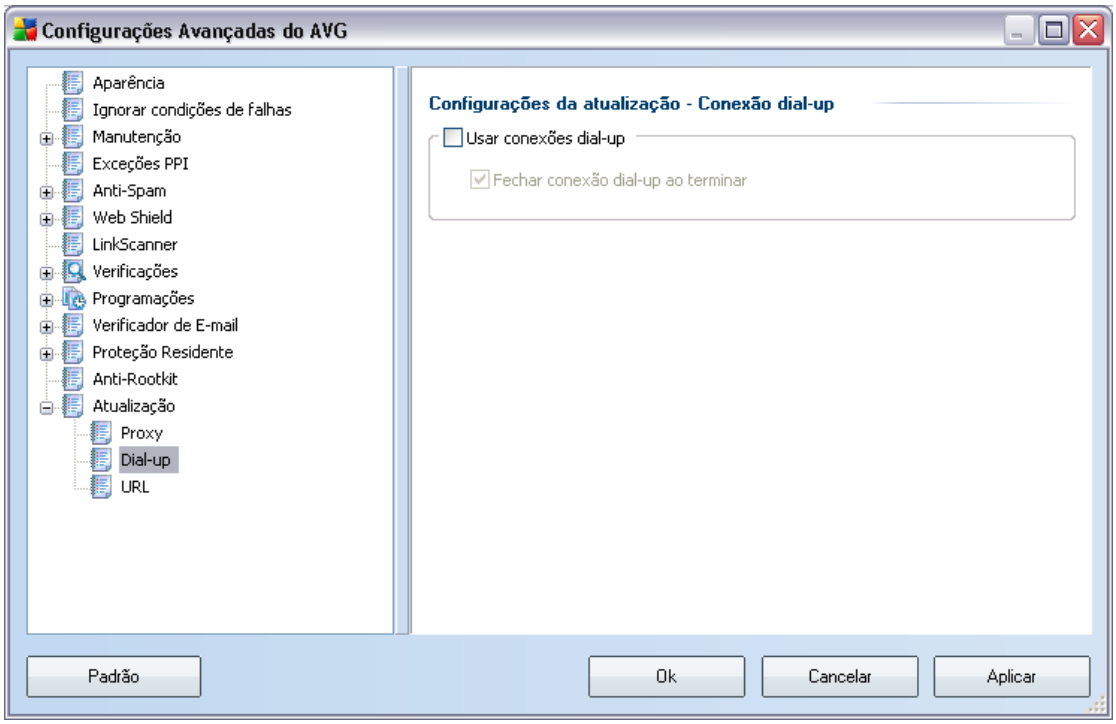
The proxy server can also have configured specific rules for each user. If your proxy server is set up this way, check the ***Use PROXY authentication*** option to verify that your user name and password are valid for connecting to the Internet via the proxy server.

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

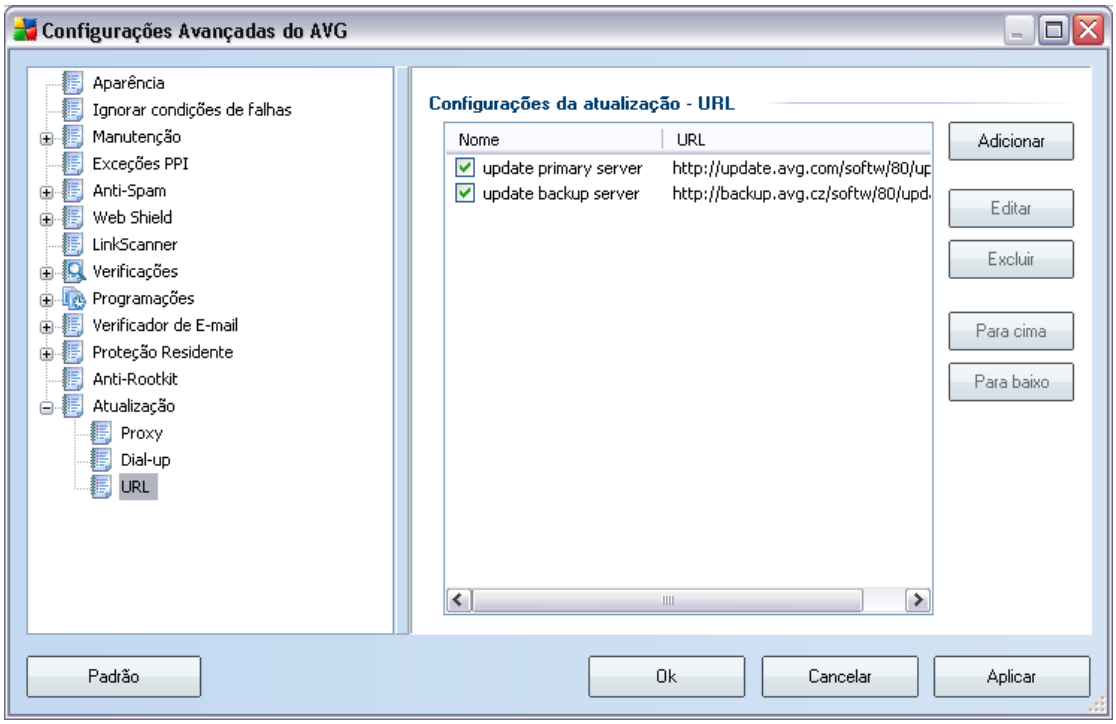
10.8.2.Dial-up



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

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

10.8.3.URL



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

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

10.8.4.Manage

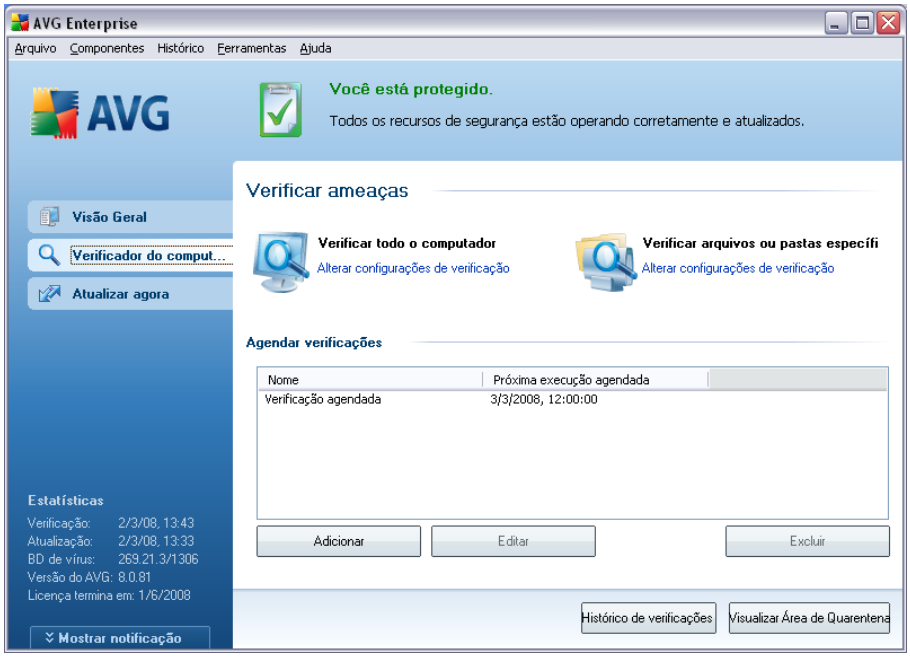
The ***Manage*** dialog offers two options accessible via two buttons:

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

11. AVG Scanning

Scanning is a crucial part of **AVG 8.5 File Server** functionality. You can run on-demand tests or schedule them to run periodically at convenient times.

11.1.Scanning Interface



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

- overview of predefined scans - 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 Virus Vault - a space where detected infections are quarantined

11.2.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.

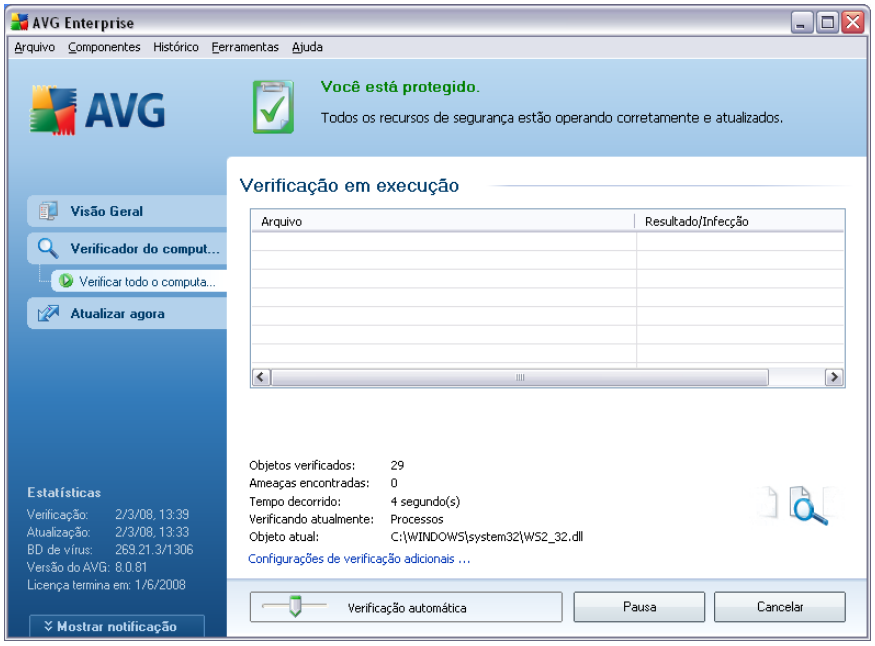
In the **AVG 8.5 File Server** you will find two types of scanning predefined by the software vendor:

11.2.1.Scan Whole Computer

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

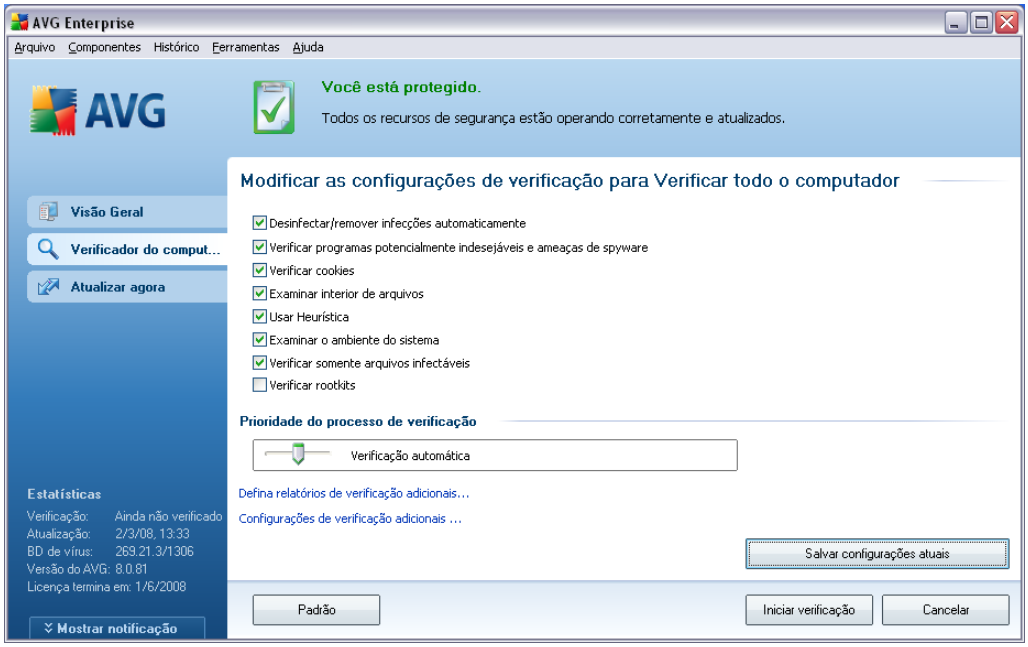
Scan launch

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



Scan configuration editing

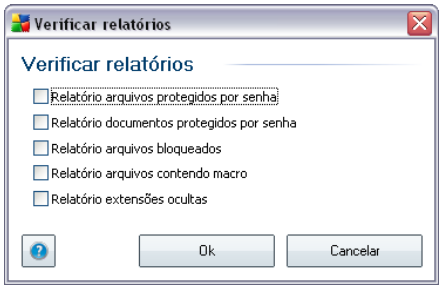
You have the option of editing the predefined default settings of the ***Scan of the whole computer***. Press the ***Change scan settings*** link to get to the ***Change scan settings for Scan whole computer*** dialog. ***It is recommended to keep to the default settings unless you have a valid reason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



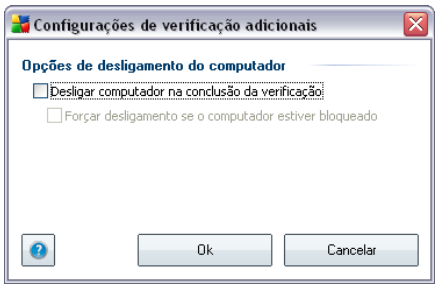
- ***Scanning parameters*** - in the list of scanning parameters you can switch on/off specific parameters as needed. By default, most of the parameters are switched on and these will be used automatically during scanning.

- ***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.

11.2.2.Scan Specific Files or Folders

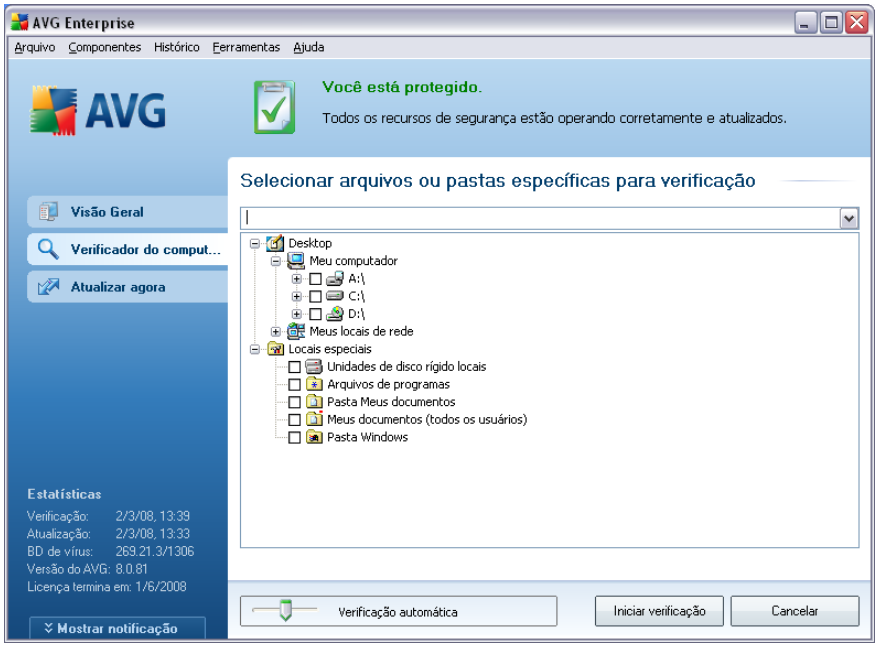
Scan specific files or folders - scans only those areas of your computer that you have selected to be scanned (selected folders, hard disks, floppy discs, CDs, etc.). The scanning progress in case of virus detection and its treatment is the same as with the scan of the whole computer: any virus found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

Scan launch

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

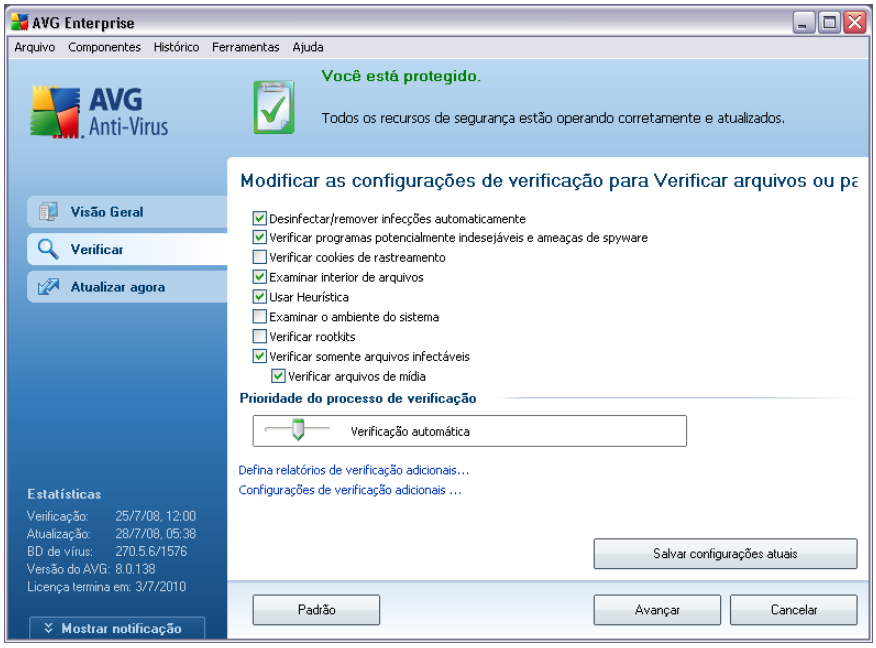
There is also a possibility of having a specific folder scanned while all its subfolders are excluded from this scanning; to do that write a minus sign "**-**" in front of the automatically generated path (*see screenshot*). To exclude the entire folder from scanning use the "!" parameter.

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



Scan configuration editing

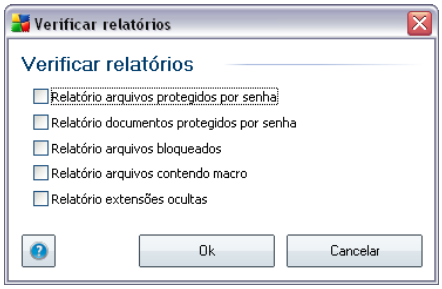
You have the option of editing the predefined default settings of the ***Scan of specific files or folders***. Press the ***Change scan settings*** link to get to the ***Change scan settings for Scan of specific files or folders*** dialog. ***It is recommended to keep to the default settings unless you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



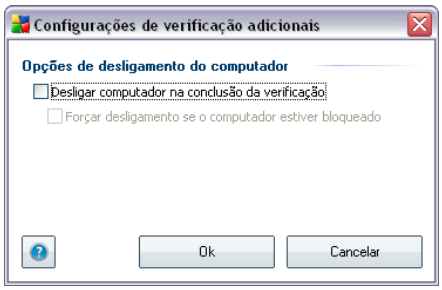
- ***Scanning parameters*** - in the list of scanning parameters you can switch on/off specific parameters as needed (*for detailed description of this settings please consult chapter AVG Advanced Settings / Scans / Scan Specific Files or Folders*).

- ***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***).

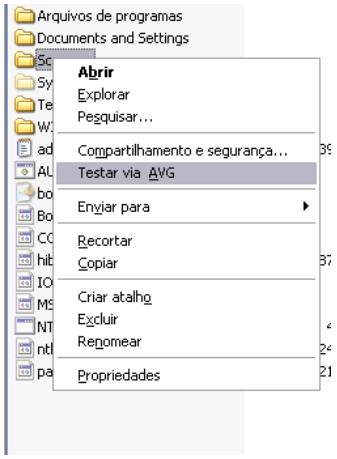


Warning: *These scan settings are identical to the parameters of a newly defined scan - as described in the chapter* ***AVG Scanning / Scan scheduling/ How to Scan****.*

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*).

11.3.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

11.4.Command Line Scanning

Within **AVG 8.5 File Server** there is the option of running the scan from the command line. You can use this option for instance on servers, or when creating a batch script to be launched automatically after the computer boot. From the command line, you can launch the scanning with most parameters as offered in AVG graphical user interface.

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

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

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

- ***/SCAN*** Scan /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/

- ***/SHUTDOWN*** Shutdown computer upon scan completion
- ***/FORCESHUTDOWN*** Force computer shutdown upon scan completion
- ***/ADS*** Scan Alternate Data Streams (NTFS only)

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:***

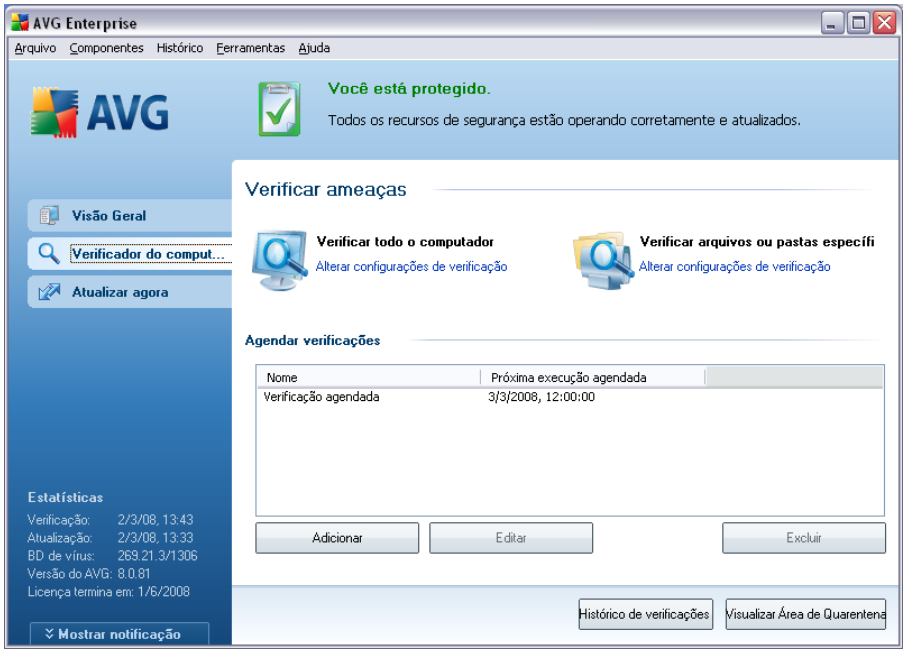
To run the scan press ***Enter***. During scanning you can stop the process by ***Ctrl+C*** or ***Ctrl+Pause***.

11.5.Scan Scheduling

With **AVG 8.5 File Server** you can run scanning on demand (for instance when you suspect an infection has been dragged to your computer) or based on a scheduled plan. It is highly recommended to run the scans based on a schedule: this way you can make sure your computer is protected from any possibility of getting infected, and you will not have to worry about if and when to launch the scan.

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

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



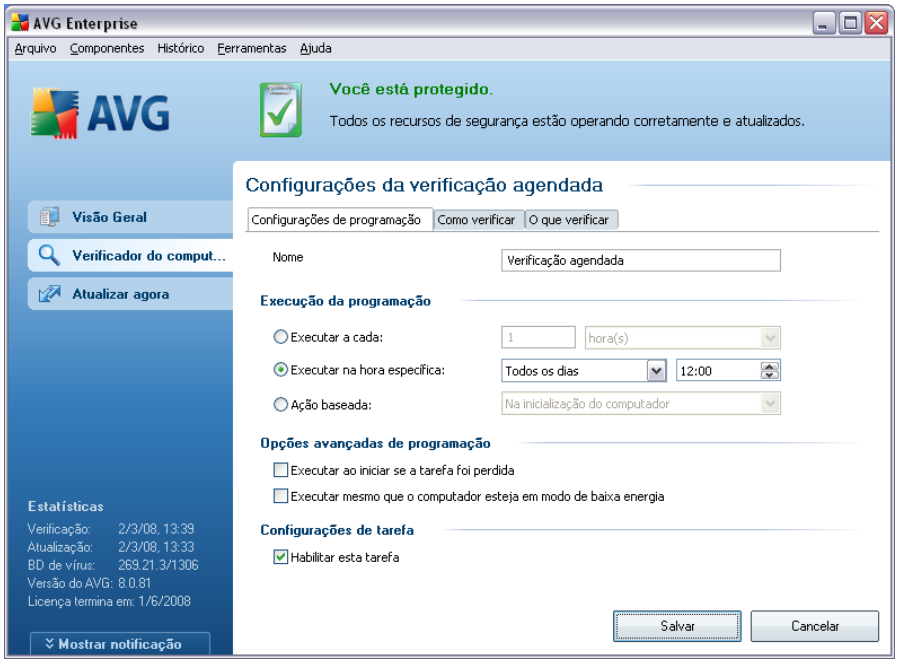
Control buttons for the scan scheduling

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

- ***Add scan schedule*** - the button opens the ***Settings for scheduled scan*** dialog, ***Schedule settings*** tab. In this dialog you can specify the parameters of the newly defined test.
- ***Edit scan schedule*** - this button can only be used if you have already previously selected an existing test from the list of scheduled tests. In that case the button appears as active and you can click it to switch to the ***Settings for scheduled scan*** dialog, ***Schedule settings*** tab. Parameters of the selected test are already specified in here and can be edited.
- ***Delete scan schedule*** - this button is also active if you have already previously selected an existing test from the list of scheduled tests. This test can then be deleted from the list by pressing the control button. However, you can only remove your own tests; the ***Whole computer scan schedule*** pre-defined within the default settings can never be deleted.

11.5.1.Schedule Settings

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



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

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

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

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

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

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

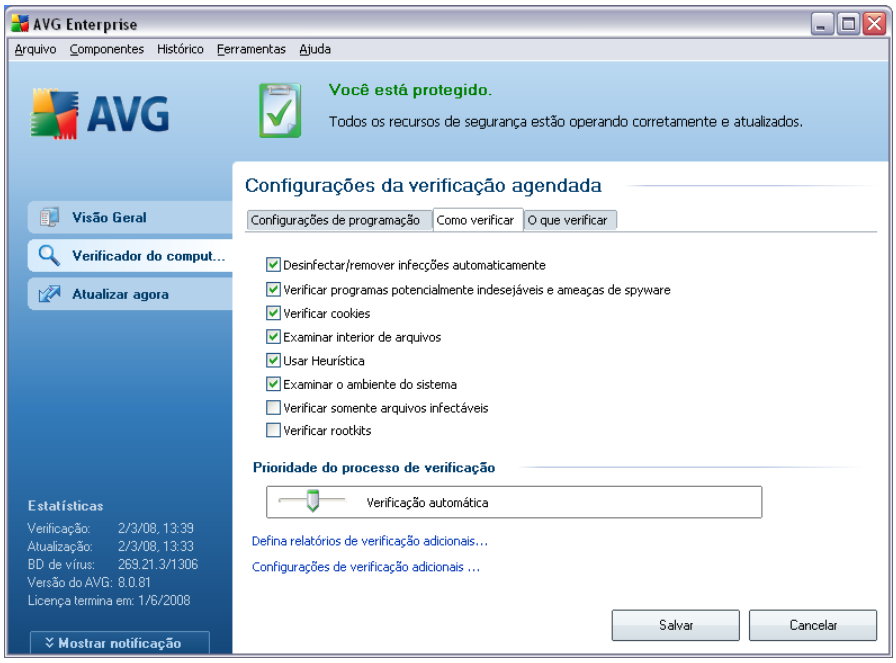
Control buttons of the Settings for scheduled scan dialog

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

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

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

11.5.2.How to Scan



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

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

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

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

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

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

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

    - ***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 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 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.

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.*

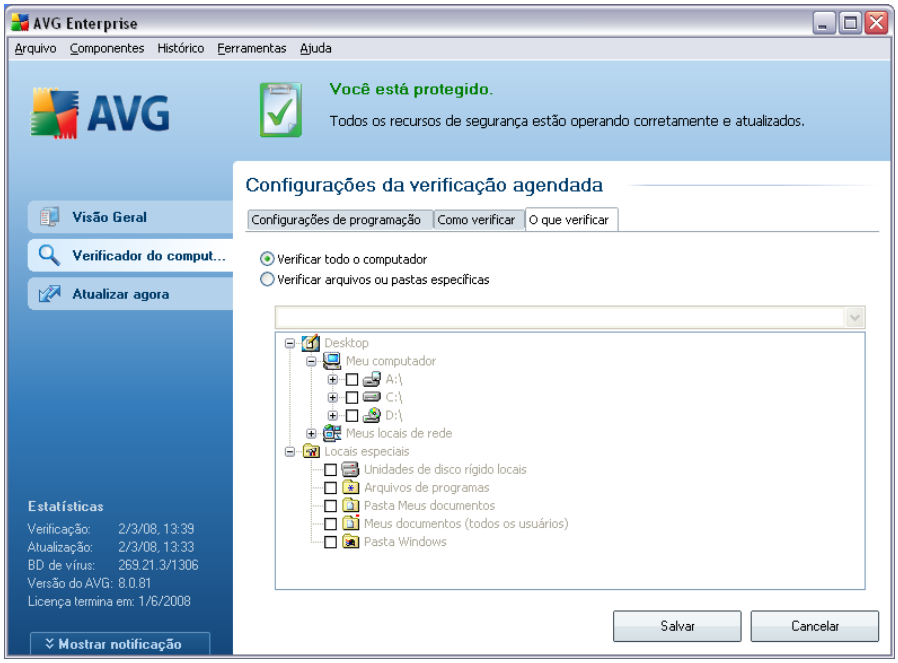
Control buttons of the Settings for scheduled scan dialog

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

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

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

11.5.3.What to Scan



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

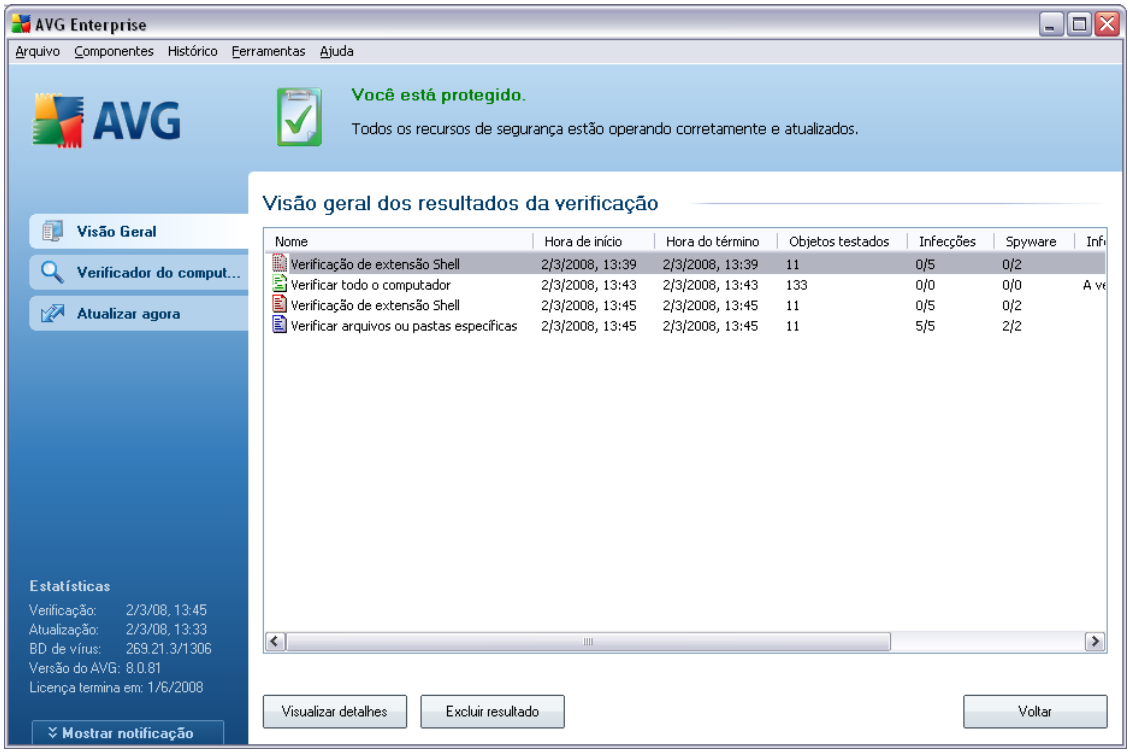
Control buttons of the Settings for scheduled scan dialog

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

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

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

11.6.Scan Results Overview



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

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

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

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

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

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

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

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

Control buttons

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

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

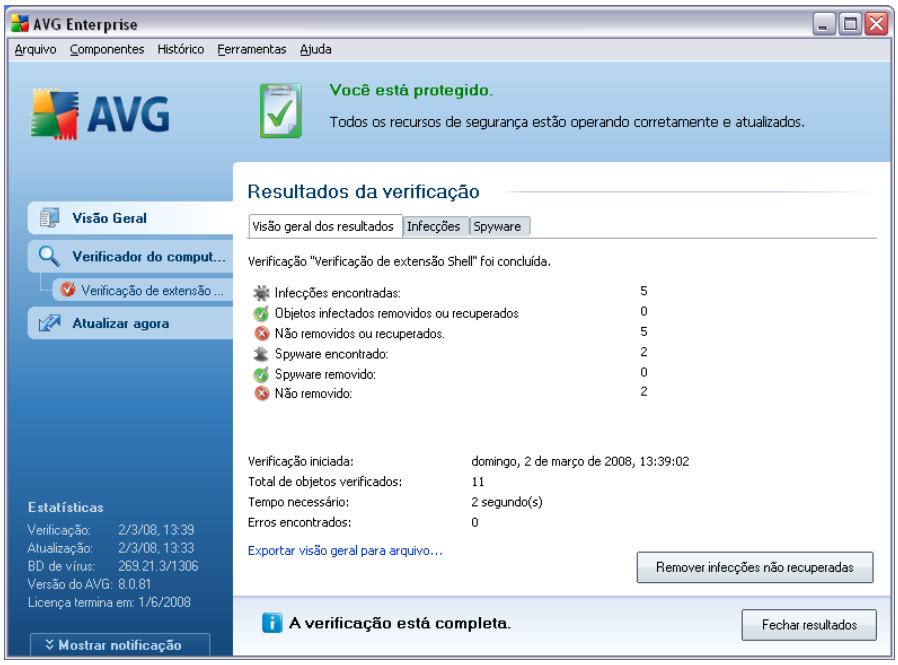
11.7.Scan Results Details

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

The dialog is further divided into several tabs:

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

11.7.1.Results Overview Tab



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

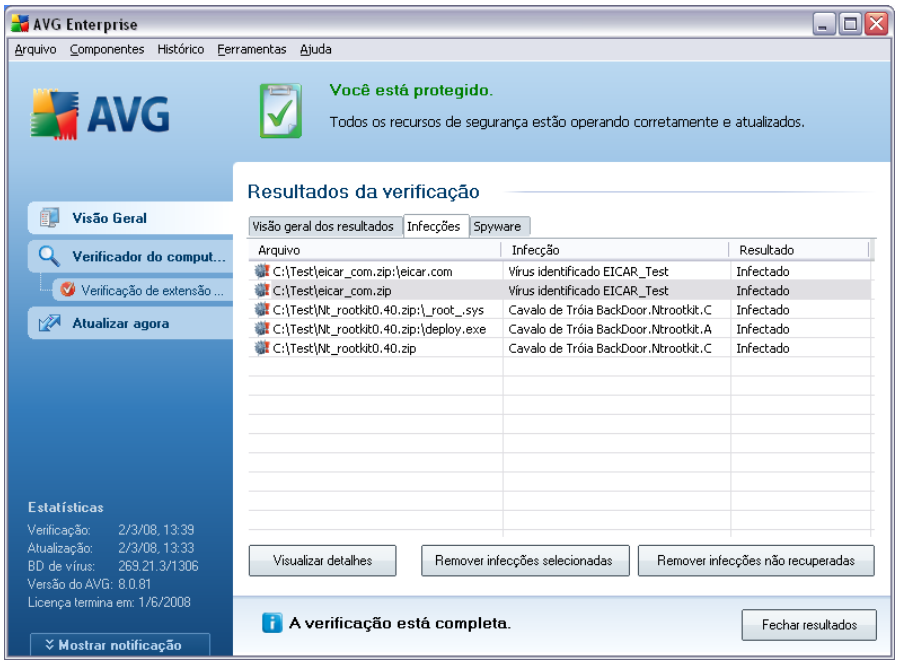
- detected virus infections / spyware
- removed virus infections / spyware
- the number of virus infections / spyware that cannot be removed or healed

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

Control buttons

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

11.7.2.Infections Tab



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

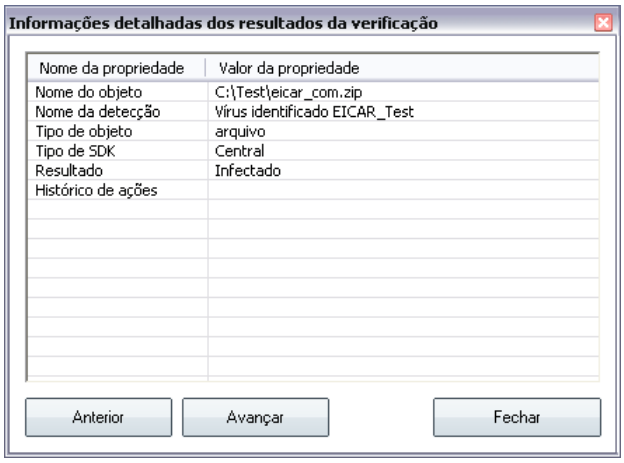
- ***File*** - full path to the original location of the infected object
- ***Infections*** - name of the detected virus (*for details on specific viruses please consult the Virus Encyclopedia online*)
- ***Result*** - defines the current status of the infected object that was detected during scanning: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

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

Control buttons

There are three control buttons available in this dialog:

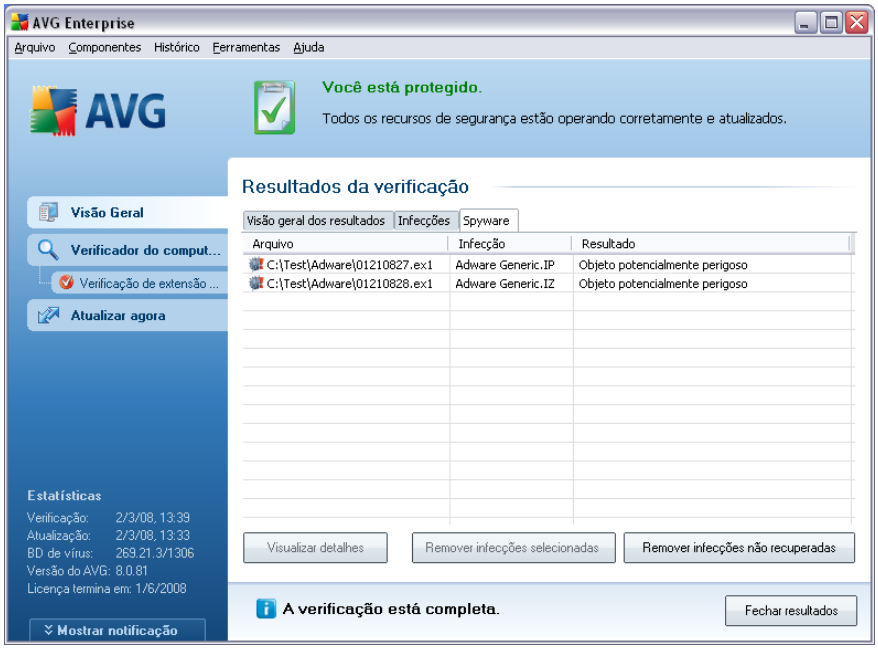
- ***View details*** - the button opens a new dialog window named ***Detailed scan result information***:



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

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

11.7.3.Spyware Tab



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

- ***File*** - full path to the original location of the infected object
- ***Infections*** - name of the detected spyware (*for details on specific viruses please consult the **Virus Encyclopedia** online*)
- ***Result*** - defines the current status of the object that was detected during scanning:
    - ***Infected*** - the infected object was detected and left in its original

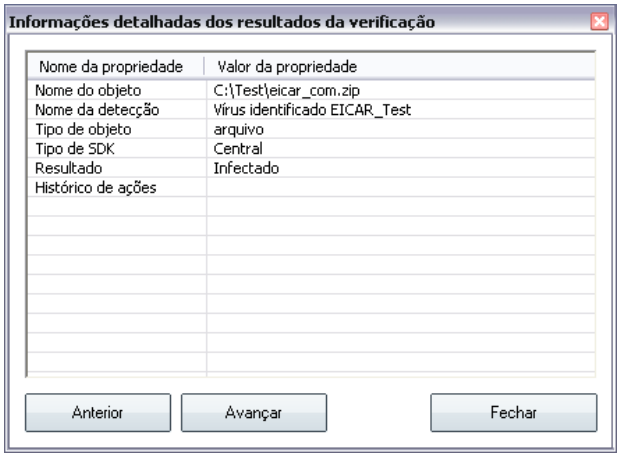
location (for instance if you have switched off the automatic healing option in a specific scan settings)

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

Control buttons

There are three control buttons available in this dialog:

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



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

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

11.7.4.Warnings Tab

The ***Warnings*** tab displays information on "suspected" objects (*typically files*) detected during scanning. When detected by the ***Resident Shield***, these files are blocked from being accessed. Typical examples of this kind of findings are: hidden files, cookies, suspicious registry keys, password protected documents or archives, etc.

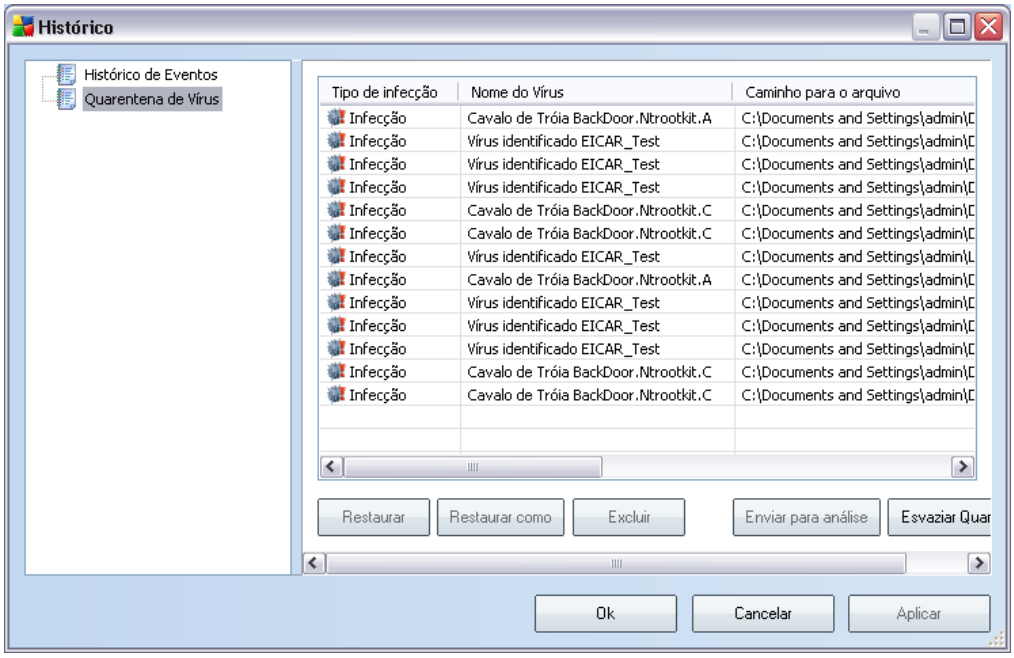
11.7.5.Rootkits Tab

The ***Rootkits*** tab displays information on rootkits detected during scanning. Its structure is basically the same as the ***Infections tab*** or the ***Spyware tab***.

11.7.6.Information Tab

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

11.8.Virus Vault



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

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

- ***Infection type*** - distinguishes finding types based on their infective level (*all listed objects can be positively or potentially infected*)
- ***Virus Name*** - specifies the name of the detected infection according to the Virus encyclopedia (online)

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

Control buttons

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

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

12. AVG Updates

12.1. 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.

12.2. Update Types

You can distinguish between two types of update:

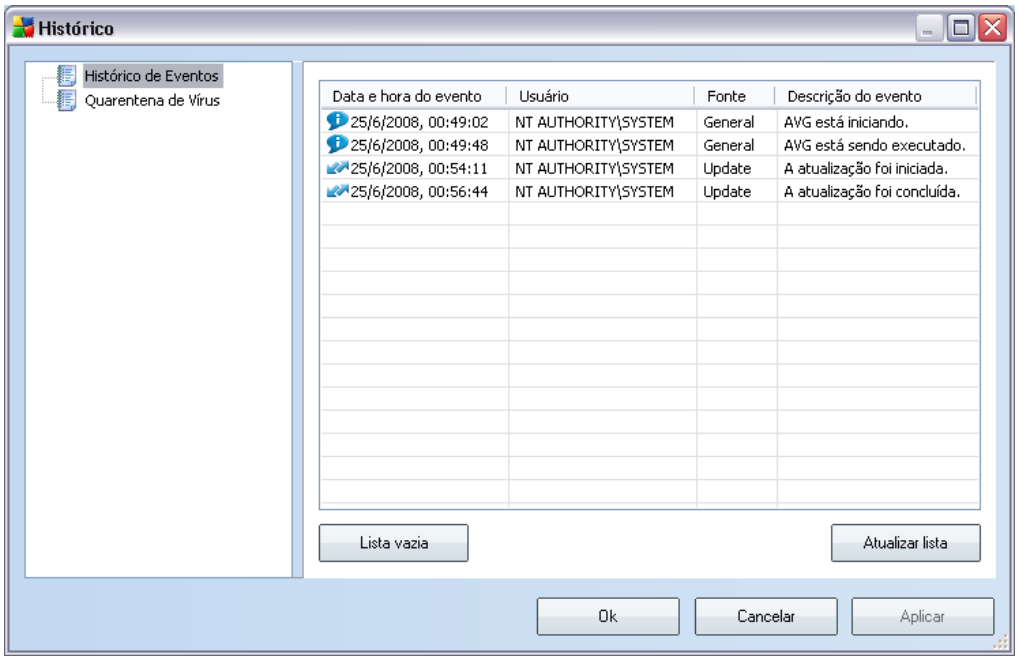
- ***On demand update*** is an immediate AVG update that can be performed any time the need arises.
- ***Scheduled update*** - within AVG it is also possible to pre-set an update plan. The planned update is then performed periodically according to the setup configuration. Whenever new update files are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

12.3. Update Process

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

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

13. Event History



The ***Event History*** dialog is accessible from the system menu via the ***History/Event History Log*** item. Within this dialog you can find a summary of important events that occurred during **AVG 8.5 File Server** operation. ***Event History*** records the following types of events:

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

Control buttons

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

14. Perguntas Freqüentes e Suporte Técnico

Se você tiver algum problema com o seu AVG, seja comercial ou técnico, consulte a seção ***Perguntas Freqüentes*** do site da AVG em www.avg.com.

Caso não consiga obter ajuda dessa forma, contate o departamento de suporte técnico por e-mail. Use o formulário de contato que pode ser acessado do menu do sistema via ***Ajuda/Obter ajuda online***.

15. AVG para MS Exchange Server

Este capítulo abrange o **AVG for MS Exchange 2000/2003 Server** e o **AVG for MS Exchange 2007 Server**. Embora estas edições tenham arquivos de instalação separados, funcionam exatamente da mesma forma (mesmas caixas de diálogo e métodos de configuração).

15.1.Requisitos de instalação específicos

15.1.1.MS Exchange Service Packs

Como o **AVG for MS Exchange 2000/2003 Server** usa a interface de verificação de vírus VSAPI 2.0/2.5, é necessário ter o Service Pack 1 (ou posterior) para o MS Exchange 2000 Server aplicado ao seu sistema. Siga o link abaixo para obter o Service Pack 1 para MS Exchange 2000 Server mais recente:

Service Pack para MS Exchange 2000 Server:

http://www.microsoft.com/technet/prodtechnol/exchange/downloads/2000/sp3/default.mspx

Para o MS Exchange 2003 Server nenhum outro service pack é necessário; no entanto, é recomendável manter o sistema o mais atualizado possível com os últimos service packs e hotfixes, de modo a obter o máximo de segurança disponível.

Service Pack para MS Exchange 2003 Server (opcional):

http://www.microsoft.com/exchange/evaluation/sp2/overview.mspx

No início da instalação, todas as versões de biblioteca do sistema serão examinadas. Se for necessário instalar bibliotecas mais recentes, o instalador renomeará as antigas com uma extensão .delete. Elas serão excluídas após a reinicialização do sistema.

15.2.Instalação

Para instalar o AVG no computador, é necessário obter o arquivo de instalação mais recente. Você pode usar o arquivo de instalação do CD que é parte da edição, mas o arquivo pode estar desatualizado. Dessa forma, é recomendável obter a versão mais recente do arquivo de instalação on-line. Você pode fazer download do arquivo no site da AVG (em www.avg.com) / seção ***Downloads***.

Após fazer download e salvar o arquivo de instalação no disco rígido, você poderá

iniciar o processo de instalação. A instalação é uma seqüência de janelas de caixa de diálogo com uma descrição resumida do que fazer em cada etapa. A seguir, oferecemos uma explicação de cada janela da caixa de diálogo:

15.2.1.Localização

Na janela seguinte, selecione a pasta de instalação de destino. Pressione o botão Procurar para selecionar um local diferente do padrão. Caso você não tenha um motivo real para alterar as configurações padrão, é recomendável manter o local predefinido. Clique no botão Avançar para continuar.

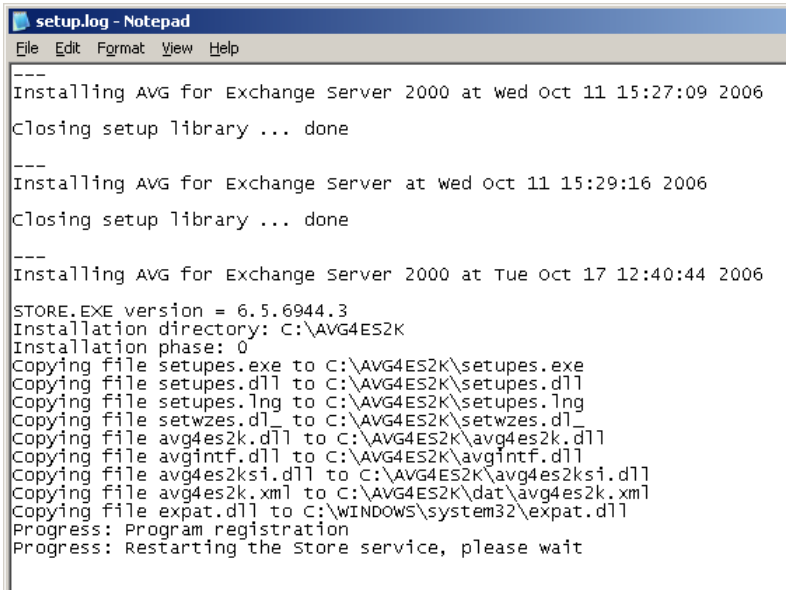
15.2.2.Iniciar a cópia de arquivos

O programa de instalação solicita que você inicie a cópia dos arquivos de instalação antes de concluir o processo. Aceite-o, clicando no botão Avançar.

15.2.3.Instalação Concluída

Quando o assistente de instalação tiver copiado todos os arquivos necessários no disco rígido, a instalação será concluída.

Para visualizar o log de instalação, pressione o botão Log:

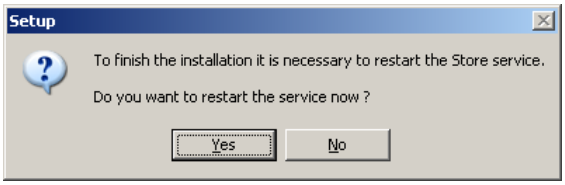


Você também poderá visualizar o log de instalação posteriormente como o arquivo setup.log no seu diretório temporário do sistema.

Pressione o botão ***OK*** na janela ***Instalação Concluída*** para fechar a caixa de diálogo de instalação.

15.2.4.Reinicialização do Serviço de Armazenamento

Durante o processo de instalação ou depois de fechar a caixa de diálogo de configuração, será solicitado reiniciar o serviço de armazenamento do Exchange 2000/2003 Server:



Pressione o botão ***Sim*** para reiniciar o serviço de armazenamento com todos os componentes do **AVG para MS Exchange 2000/2003** incluídos. Em seguida, você poderá começar a usar o produto.

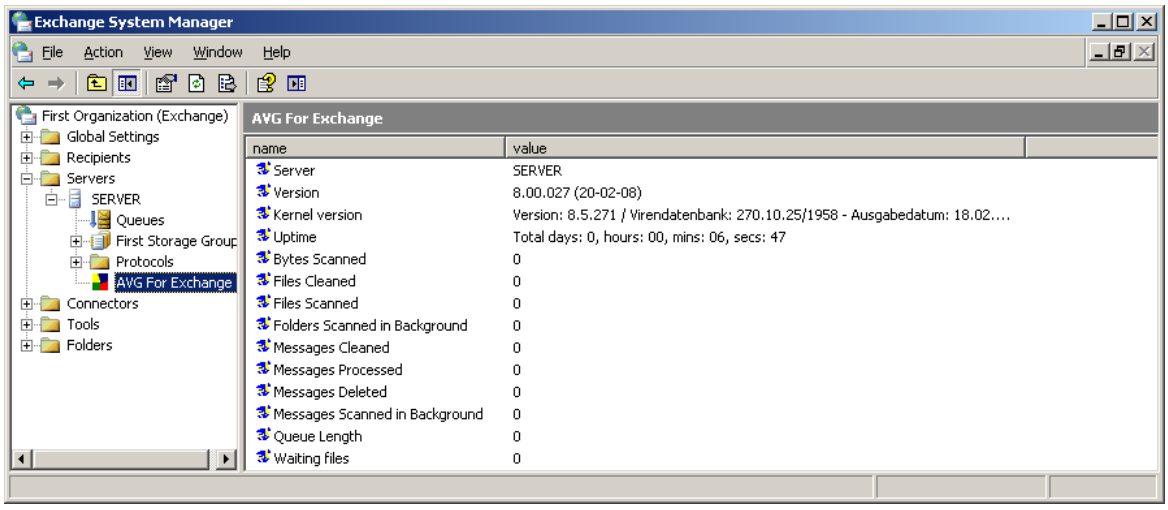
Nota: *reiniciar o serviço tornará o servidor inacessível por algum tempo! Avise os usuários antes de fazer isso, porque todos os que estiverem on-line serão desconectados temporariamente durante a reinicialização.*

15.3.Configuração

Quando o serviço de armazenamento do Exchange for reiniciado após a instalação do 2000/2003 Server**AVG for MS Exchange 2000/2003 Server**, nenhuma outra ação será necessária para iniciá-lo.

15.3.1.Status

Para exibir o status do **AVG**, inicie o aplicativo MS Exchange System Manager. Na ramificação Servidores da árvore de controle *(à esquerda na janela principal)* selecione o servidor específico. Há a ramificação AVG para Exchange na subárvore do servidor . Selecione essa ramificação para abrir a janela de informações mostrando vários dados para visualização.



As informações exibidas na janela incluem nome do servidor, versão do aplicativo, versão do banco de dados, versão do kernel e tempo total de execução do programa desde a última reinicialização. Além disso, itens informando sobre o desempenho antivírus são exibidos aqui *(contadores de monitor de desempenho)*.

O AVG para MS Exchange 2000/2003 Server verifica todas as mensagens no banco de dados de pastas particulares e públicas. Se um vírus for detectado, o AVG para MS Exchange 2000/2003 Server gravará uma mensagem no arquivo de log do AVG e também no Log de eventos.

15.3.2.VSAPI 2.0

API 2.0 (VSAPI 2.0 conforme indicado no MS Exchange 2000 Server) de verificação de vírus não permite a exclusão de arquivos de e-mail infectados. Como não é possível excluir o anexo do e-mail infectado, seu nome de arquivo é alterado: o AVG para Exchange 2000/2003 Server anexa a extensão .virusinfo.txt ao nome do arquivo original. O conteúdo do arquivo é substituído por uma mensagem sobre o vírus conhecido. Se um vírus for encontrado diretamente na mensagem, todo o corpo dessa mensagem será substituído por um aviso informando que um vírus foi encontrado nela.

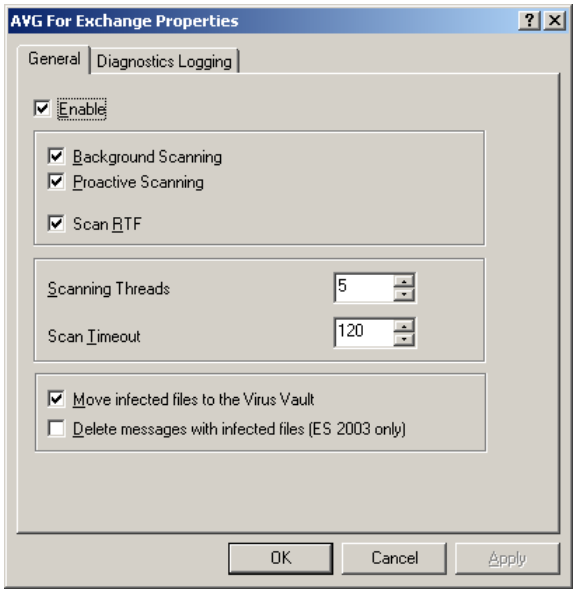
API 2.5 *(VSAPI 2.5 conforme indicado no MS Exchange 2003 Server)* de verificação de vírus também permite a exclusão de mensagens infectadas. Esse recurso pode ser definido na caixa de diálogo de configuração do AVG para MS Exchange 2000/2003 Server.

15.3.3.Propriedades Gerais

Para abrir a janela de configuração do AVG for Exchange 2000/2003 Server, clique com o botão direito do mouse na ramificação ***AVG para Exchange*** e selecione o item ***Propriedades***. Alternativamente, você pode abrir a janela usando o botão ***Ação*** no menu superior.

A janela de configuração de Propriedades do AVG for Exchange ***consiste em duas guias. Você pode alterar a verificação de vírus de e-mail e o comportamento de log aqui.***

Guia Geral



Na guia ***Geral***, você encontrará várias opções predefinidas relacionadas ao desempenho da verificação de vírus de e-mail do AVG para MS Exchange 2000/2003 Server:

- ***Ativar*** – use esta caixa de seleção para ativar ou desativar a verificação de e-mail.
- ***Verificação em Segundo Plano*** – use esta caixa para ativar ou desativar a verificação em segundo plano. Essa verificação é um dos recursos da interface de aplicativo VSAPI 2.0/2.5. Ela oferece verificação encadeada dos bancos de dados de mensagens do Exchange. Sempre que um item que não tenha sido verificado antes for encontrado nas pastas da caixa de correio dos usuários, ele será enviado ao , ele será enviado ao AVG para Exchange 2000/2003 Server para verificação. A verificação e a procura de objetos não examinados são executadas em paralelo.
- Um processo de baixa prioridade específico é utilizado para cada banco de dados, o que garante que outras tarefas (por exemplo, armazenamento de mensagens de e-mail no banco de dados do Microsoft Exchange) sejam sempre executadas com preferência.
- ***Verificação Pró-ativa*** – ative ou desative a função de verificação pró-ativa do VSAPI 2.0/2.5 aqui. A verificação pró-ativa consiste no gerenciamento dinâmico da prioridade dos itens na fila de verificação. Os itens de prioridade mais baixa só serão verificados depois que todos os de prioridade mais alta (fornecidos com mais freqüência por demanda na fila) forem verificados. Entretanto, a prioridade de um item aumentará se um cliente tentar usá-lo; deste modo, a precedência

de um item será alterada de acordo com a atividade dos usuários .

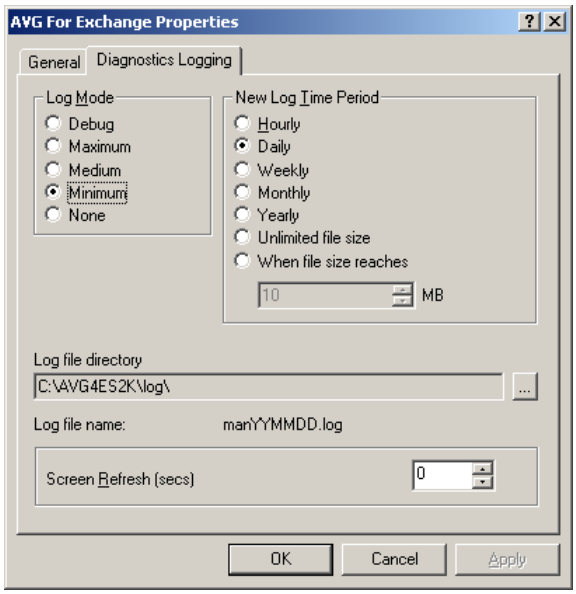
- ***Verificar RTF*** – especifique aqui se o tipo de arquivo RTF deverá ser verificado ou não.
- ***Processos de Verificação*** – o processo de verificação é encadeado por padrão para aumentar o desempenho geral da verificação em um certo nível de paralelismo. Altere a contagem de processos aqui. O número padrão de processos é calculado como 2 vezes o 'número_de_processadores + 1.
- ***Campo Tempo Limite de Verificação*** – o intervalo contínuo máximo (em segundos) para que um processo acesse a mensagem sendo verificada.
- ***Mover arquivos infectados para a quarentena*** – se esta opção estiver marcada, cada arquivo de e-mail infectado será movido para o ambiente de **Quarentena do AVG**.
- ***Excluir mensagens com arquivos infectados (ES 2003 apenas)*** – depois que você marcar este item, as mensagens em que forem detectados vírus serão excluídas. Quando esse item estiver desmarcado, o e-mail infectado será enviado ao destinatário, mas o anexo será substituído por um arquivo de texto contendo informações sobre o vírus detectado. Esta opção estará disponível somente na VSAPI 2.5 no Exchange 2003 Server.

Geralmente, todos os recursos nessa guia são extensões de usuário dos serviços da interface de aplicativo Microsoft VSAPI 2.0/2.5. Para obter informações detalhadas sobre a VSAPI 2.0/2.5, consulte os seguintes links (e também os links acessíveis pelos indicados):

- http://support.microsoft.com:80/support/kb/articles/Q285/6/67.ASP para obter informações gerais sobre a VSAPI 2.0 no Exchange 2000 Server Service Pack 1
- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k para obter informações sobre o Exchange e a interação de software antivírus
- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 para obter informações sobre recursos adicionais da VSAPI 2.5 no aplicativo Exchange 2003 Server.

Nota: *O comportamento de verificação é controlado pelo AVG File Server Application. No menu principal do aplicativo, selecione Ferramentas/Configurações Avançadas. (Consulte o capítulo Verificador de E-mail).*

15.3.4.Log de Diagnósticos

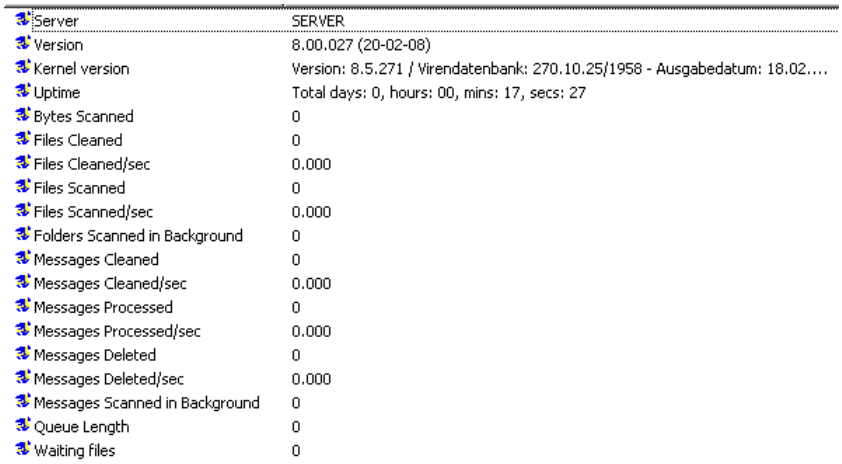


Nesta guia, é possível definir a freqüência do log de verificação e o comportamento geral. Há vários campos predefinidos na guia Log de Diagnóstico:

- ***Modo de Log*** – ajuste aqui a quantidade de informações a serem registradas.
- ***Novo Período de Log*** – defina aqui o período de criação de novo log e possivelmente o tamanho do arquivo de log.
- ***Diretório de arquivos de log*** – altere aqui o local do arquivo de log padrão.
- ***Nome do arquivo de log*** – visualize aqui o nome do arquivo de log padrão.
- ***Atualização de Tela (segundos)*** – especifique a freqüência com que a tela de monitoramento on-line (mostrada na janela de informações do AVG for Exchange 2000/2003 Server) deve ser mostrada.

15.4.Monitoramento do Servidor

15.4.1.Monitoramento On-line



Server	SERVER
Version	8.00.027 (20-02-08)
Kernel version	Version: 8.5.271 / Virendatenbank: 270.10.25/1958 - Ausgabedatum: 18.02....
Uptime	Total days: 0, hours: 00, mins: 17, secs: 27
Bytes Scanned	0
Files Cleaned	0
Files Cleaned/sec	0.000
Files Scanned	0
Files Scanned/sec	0.000
Folders Scanned in Background	0
Messages Cleaned	0
Messages Cleaned/sec	0.000
Messages Processed	0
Messages Processed/sec	0.000
Messages Deleted	0
Messages Deleted/sec	0.000
Messages Scanned in Background	0
Queue Length	0
Waiting files	0

Na janela de informações do AVG para MS Exchange 2000/2003 Server (*consulte o início desta seção para saber como chegar nela*), há diversos campos exibidos:

Os primeiros quatro itens fornecem informações gerais sobre o servidor e o status do AVG for Exchange 2000/2003 Server:

- ***Servidor*** – o nome do servidor
- ***Versão*** – a versão do AVG para Exchange 2000/2003 Server
- ***Versão de kernel*** – a versão do kernel antivírus e seu banco de dados de vírus interno
- ***Tempo de Atividade*** –o tempo total desde a última reinicialização do Exchange 5.x Server

Os outros itens representam determinados contadores do monitor de desempenho da VSAPI 2.0/2.5 relacionados à verificação de vírus do Exchange 2000/2003 Server. Os contadores são descritos da seguinte forma:

- ***Bytes Verificados*** – o número total de bytes em todos os arquivos processados pelo verificador de vírus
- ***Arquivos Limpos*** – o número total de arquivos separados limpos pelo verificador de vírus
- ***Arquivos Limpos/seg*** – a taxa na qual os arquivos separados são limpos

pelo verificador de vírus

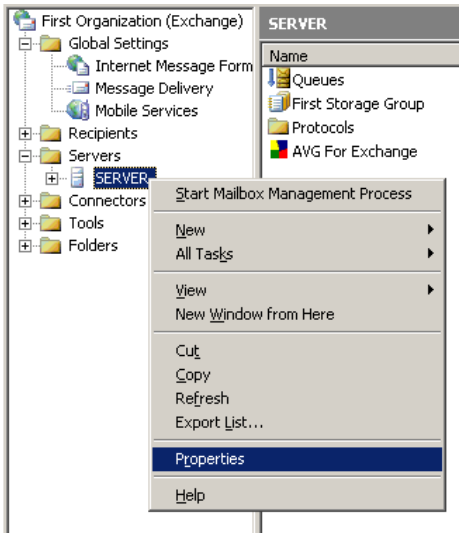
- ***Arquivos em Quarentena*** – o número total de arquivos separados movido para a quarentena pelo verificador de vírus
- ***Arquivos em Quarentena/seg*** – a taxa na qual os arquivos separados são colocados em quarentena pelo verificador de vírus
- ***Pastas Verificadas em Segundo Plano*** – o número total de pastas processadas pela verificação em segundo plano
- ***Mensagens Limpas*** – o número total de mensagens de nível superior limpas pelo verificador de vírus
- ***Mensagens Limpas/seg*** – a taxa na qual as mensagens de nível superior são limpas pelo verificador de vírus
- ***Mensagens em Quarentena*** – o número total de mensagens de nível superior movidas para a quarentena pelo verificador de vírus
- ***Mensagens em Quarentena/seg*** – a taxa na qual as mensagens de nível superior são colocadas em quarentena pelo verificador de vírus
- ***Mensagens Processadas*** – o valor acumulado do número total de mensagens de nível superior processadas pelo verificador de vírus
- ***Mensagens Processadas/seg*** – a taxa na qual as mensagens de nível superior são processadas pelo verificador de vírus
- ***Mensagens Verificadas em Segundo Plano*** – o número total de mensagens processadas pela verificação em segundo plano
- ***Mensagens Excluídas*** – o número total de mensagens suspeitas excluídas pelo verificador de vírus (disponível somente na VSAPI 2.5)
- ***Mensagens Excluídas/seg*** – a taxa na qual as mensagens suspeitas são excluídas pelo verificador de vírus (disponível somente na VSAPI 2.5)
- ***Comprimento da Fila*** – o número atual se solicitações pendentes enfileiradas para verificação de vírus
- ***Arquivos em espera*** – a contagem de arquivos aguardando verificação

15.4.2.Log de Eventos

Com exceção do monitoramento on-line do AVG para MS Exchange 2000/2003 Server, também é possível configurar o log de eventos relacionados ao verificador de vírus no **Log de Eventos**. Os eventos disponíveis cobrem várias questões, como avisos de carregamento de bibliotecas de programa, eventos de arquivos encontrados, avisos de solução de problemas etc.

Você pode configurar o nível de log da VSAPI 2.0/2.5 do Exchange na janela principal do *(conforme mostrado no _início desta seção)*.

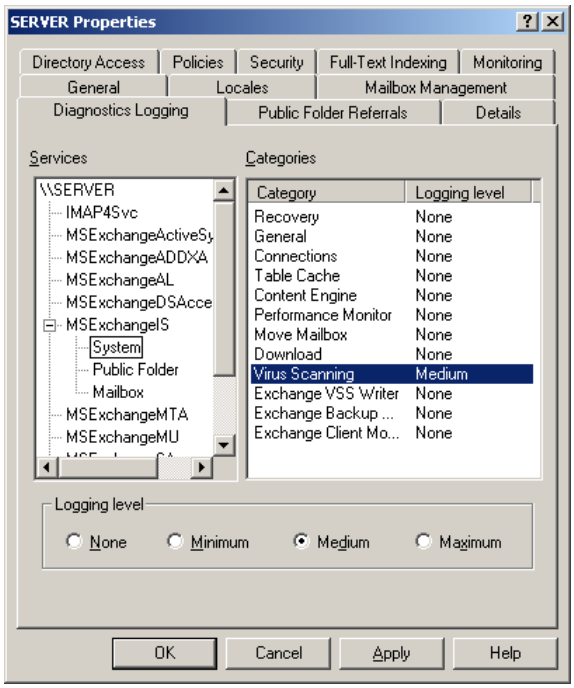
- Clique duas vezes na ramificação Servidores ***na árvore de controle***
- Selecione o servidor em particular (veja um exemplo de nome de servidor realçado na imagem abaixo)
- Clique com o botão direito do mouse no nome do servidor e selecione o item Propriedades ***no menu de contexto***



- A janela Propriedades ***aparecerá.***
- Vá para a guia Log de Diagnóstico
- Na árvore ***Serviços***, selecione a pasta MSExchangeIS / System
- Na lista ***Categorias*** aberta, selecione o item ***Verificação de Vírus*** e escolha o nível de log desejado para o componente Log de eventos do sistema

operacional. Os seguintes níveis são oferecidos:

- Nenhum
- Mínimo
- Médio
- Máximo



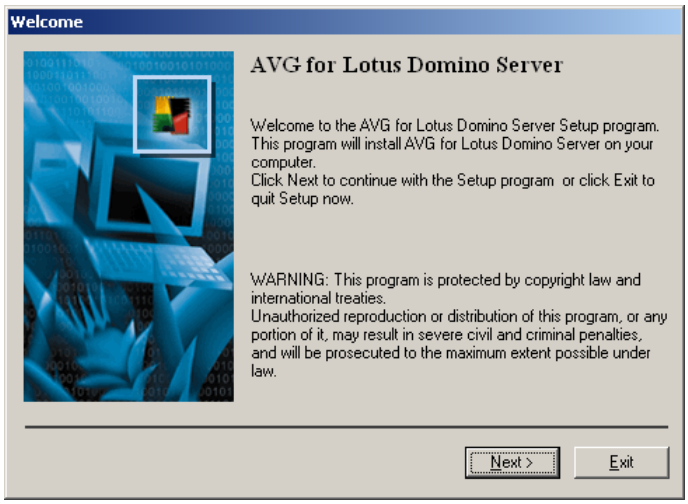
Nota: *você encontrará a descrição completa dos eventos da VSAPI 2.0/2.5 neste link: http://support.microsoft.com/default.aspx?scid=kb;EN-US;294336.*

16. AVG for Lotus Notes/Domino Server

16.1. Instalação

16.1.1. Início da instalação

Execute o pacote de instalação; a tela de introdução será mostrada. Pressione o botão ***Avançar*** para continuar com a instalação.



16.1.2. Contrato de licença

A janela seguinte apresenta o texto completo do ***Contrato de licença***. Leia-o atentamente e se você aceitar todos os pontos, confirme sua aprovação clicando no botão ***Aceitar***.

16.1.3. Registro

Nesta tela, preencha o seu número de licença do **AVG 8.5 File Server**.

Se você usou um número de licença do **AVG 8.5 File Server** durante a instalação do **AVG 8.5 File Server Edition**, esta tela não será exibida. No entanto, se adquiriu o **AVG 8.5 File Server** e o **AVG 8.5 File Server Edition** separadamente, agora deverá inserir o número de licença do **AVG 8.5 File Server**.

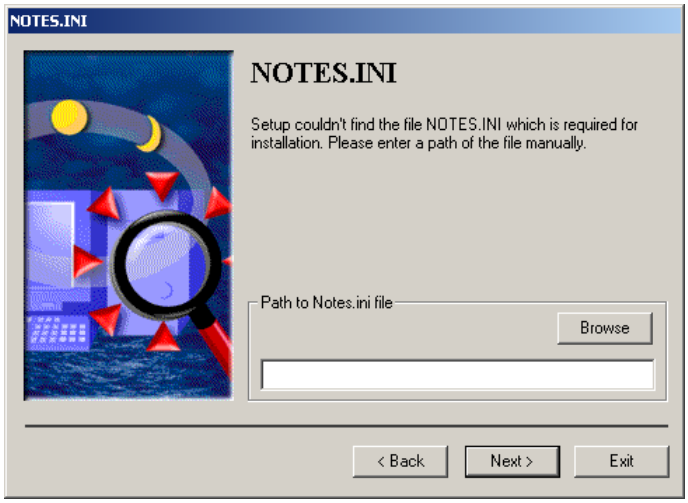
Clique no botão Avançar ***para confirmar as informações fornecidas.***

16.1.4.Localização

Depois que você concordar com a licença, selecione a pasta de destino da instalação. Os dados e os arquivos de programa do **AVG for Lotus Notes/Domino Server** serão instalados diretamente na pasta Lotus Notes/Domino. Pressione o botão Procurar para selecionar um local diferente do padrão, embora seja recomendável mantê-lo. Clique no botão ***Avançar*** para continuar.

16.1.5.Arquivo ini do Notes

Para instalar o **AVG for Lotus Notes/Domino Server** corretamente, é necessário localizar o arquivo de configuração do Lotus Notes/Domino, NOTES.INI. Se o arquivo NOTES.INI não for encontrado imediatamente, você será solicitado a definir o caminho manualmente (pressionando o botão Procurar ou preenchendo o caminho completo diretamente). Clique no botão ***Avançar*** para continuar.



16.1.6.Instalação Concluída

Quando o assistente de instalação tiver copiado todos os arquivos necessários no disco rígido, a instalação será concluída.

16.1.7.Reinicialização do Servidor de E-mail

Para concluir a instalação, reinicie o servidor Lotus Notes/Domino. Isso iniciará automaticamente o AVG para Lotus Notes/Domino Server (serviços de servidor AvgScan e AvgMail) e criará os bancos de dados do AVG (Configuração, Log e Quarentena). Você poderá bloquear todos eles nas seções de configuração apropriadas posteriormente, se necessário.

Agora, o computador está recebendo a proteção mais completa e confiável contra ameaças de vírus.

Os seguintes arquivos foram instalados:

- Diretório de programa do Lotus Notes/Domino:
  - navgscan.exe – aplicativo de servidor para verificação de bancos de dados
  - navgmail.exe – aplicativo de verificação de e-mail antivírus de servidor
  - navghook.dll – biblioteca para armazenamento de e-mails no banco de dados MAIL.BOX até que sejam verificados à procura de vírus
- Diretório de dados do Lotus Notes/Domino:
  - avgsetup.ntf – modelo de banco de dados de configuração
  - avglog.ntf – modelo de banco de dados de log
  - avgvirus.ntf – modelo de quarentena
  - avgsetup.nsf – banco de dados de configuração
  - avglog.nsf – banco de dados de log
  - avgvirus.nsf – banco de dados de quarentena

16.2.Ativação do Programa

AVG for Lotus Notes/Domino Server será ativado automaticamente quando o servidor do Lotus Notes/Domino for reiniciado.

As configurações padrão do **AVG for Lotus Notes/Domino Server** são as seguintes:

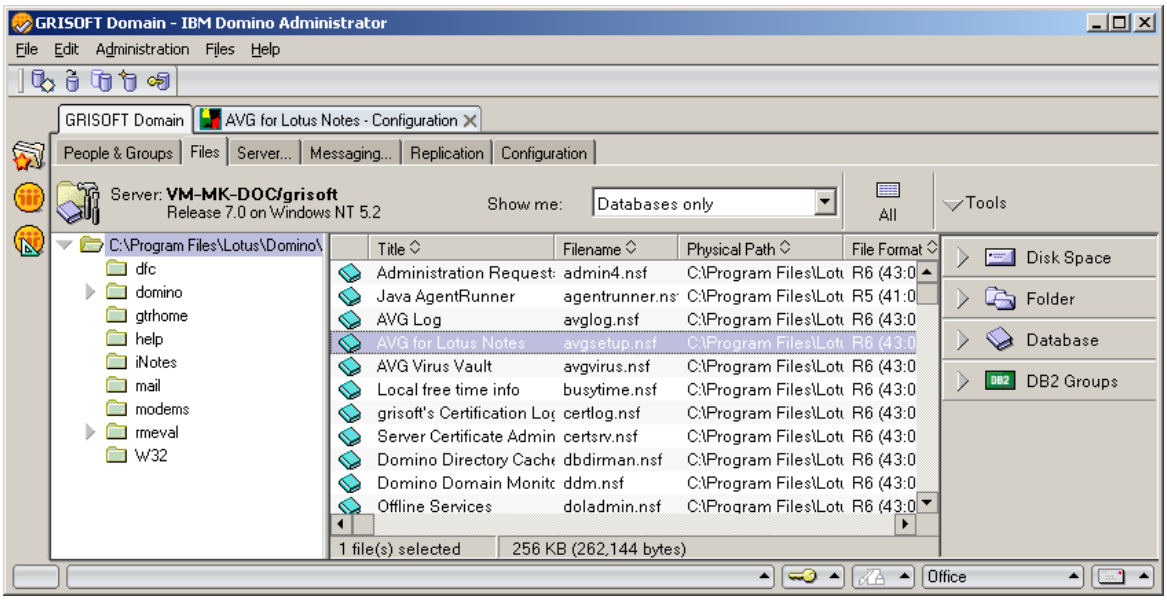
- verificar todos os e-mails com anexos
- uma mensagem de certificação será adicionada a qualquer e-mail que não tenha vírus, não possua um anexo de assinatura e não tenha sido criptografada
- os arquivos recebidos considerados infectados serão enviados ao destinatário

com uma mensagem contendo detalhes do vírus e do arquivo

- os e-mails enviados contendo anexos infectados serão devolvidos ao remetente com informações sobre os objetos infectados e os vírus correspondentes; o e-mail infectado não será entregue ao destinatário.

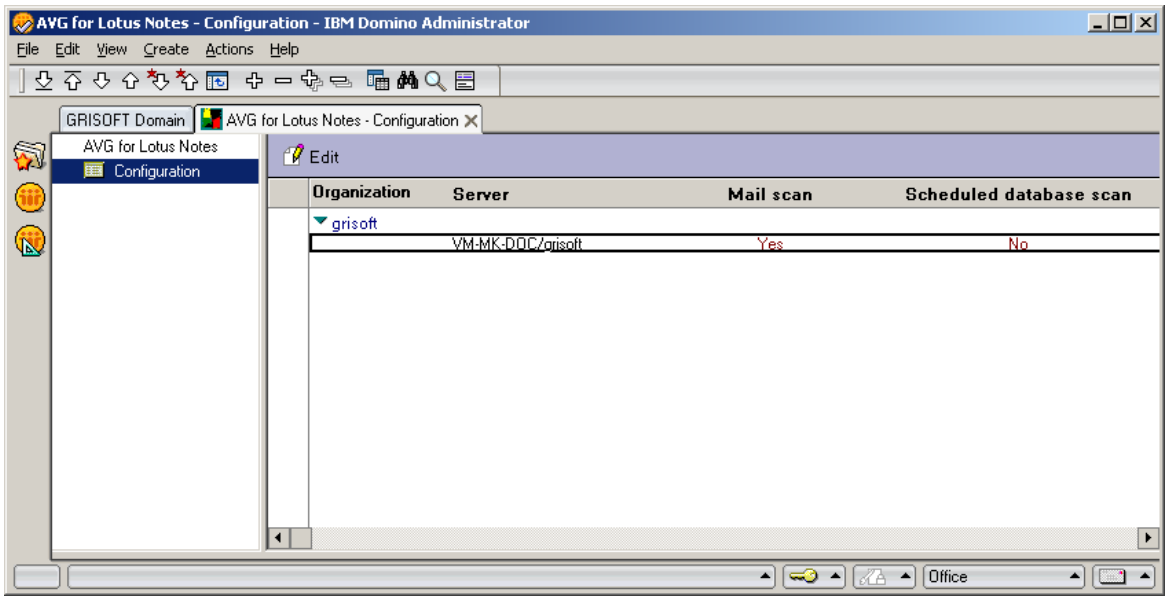
Você pode alterar facilmente a configuração padrão do **AVG for Lotus Notes/ Domino Server** com o utilitário Domino Administrator. Selecione a guia ***Arquivos*** na janela inicial e você verá três arquivos relacionados do AVG (bancos de dados do Lotus) entre todos os arquivos a administrar:

- ***Log do AVG*** (consulte a seção Arquivo de log do AVG)
- ***AVG para Lotus Notes*** (consulte a seção Ativação do Programa)
- ***Quarentena do AVG*** (consulte a seção Quarentena do AVG)

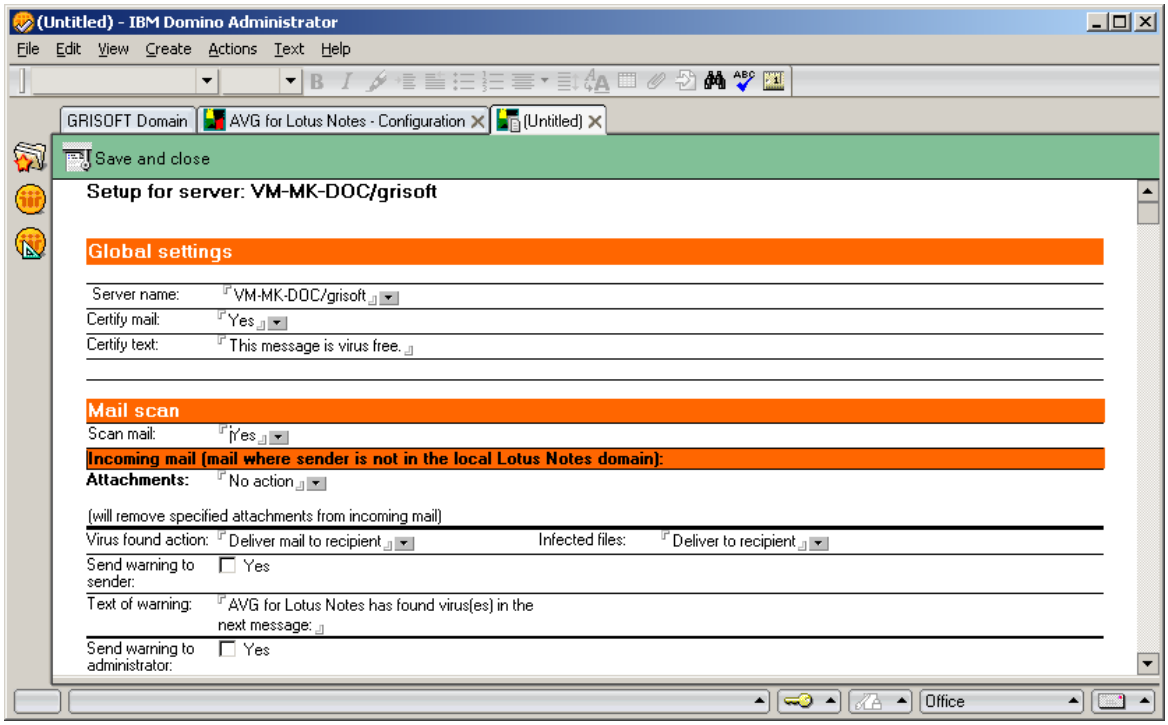


16.3.Configuração

Clique duas vezes em ***AVG for Lotus Notes*** na janela principal do administrador / guia ***Arquivo*** para abrir a janela ***AVG for Lotus Notes – Configuração***.



Nesta janela, selecione o servidor no qual deseja que o banco de dados de configuração do AVG seja instalado. Clique duas vezes no campo do servidor ou pressione o botão Editar logo acima da lista de servidores. Uma nova janela sem título será aberta no ambiente do utilitário de administrador do Lotus.



Você pode controlar totalmente o comportamento de verificação e gerenciamento de e-mails infectados do AVG for Lotus Notes/Domino Server. Além disso, é possível programar várias verificações de bancos de dados Lotus. Para salvar as alterações de configuração executadas, pressione o botão Salvar e fechar na área superior da janela.

Todas as opções de configuração correspondem totalmente aos campos apresentados nas capturas de tela acima, da seguinte forma:

- Configurações Globais - Aqui você pode especificar os detalhes do servidor
- Verificação de e-mail - Aqui você pode especificar as configurações de e-mail de entrada/saída
- Verificação Planejada do Banco de Dados - Aqui você pode especificar a freqüência e profundidade da verificação do banco de dados

16.3.1.Configurações Globais

- ***Nome do servidor*** – a especificação de servidor atual
- ***Certificar correio*** – selecione se o AVG for Lotus Notes/Domino deve ou não

certificar e-mails

- ***Certificar texto*** – edite o texto de certificação (por exemplo, "A mensagem não contém vírus…")

16.3.2.Verificação de E-mails

- ***Verificar e-mails*** – ativa ou desativa a verificação antivírus automática
- ***E-mail de entrada*** (um e-mail cujo remetente não está no domínio local do Lotus Notes)
  - ***Anexos*** – a opção ativa a definição de extensões de arquivo de anexos de e-mail que deverão ser removidos automaticamente do e-mail. Anexos com extensões definidas pelo usuário serão completamente removidos de um e-mail recebido, quer o arquivo identificado tenha sido infectado ou não por um vírus. As ações possíveis são:
    - ***Nenhuma ação*** - os anexos recebidos não serão filtrados ou removidos
    - ***Remover*** - os anexos definidos pelo usuário serão removidos do e-mail com vírus detectado e depois excluídos
    - ***Remover e armazenar na Quarentena*** - os anexos definidos pelo usuário serão excluídos do e-mail com vírus detectado e movidos para a Quarentena

    Você poderá escolher as extensões de arquivo de anexo na lista de palavras-chave (ou poderá digitar uma nova extensão se a opção desejada não estiver na lista) em um novo campo Extensões quando as ações Remover ou Remover e armazenar... estiverem selecionadas.

    Além disso, você pode digitar um texto personalizado que será inserido no corpo da mensagem de e-mail quando a ação desejada for processada. Preencha um texto opcional no campo Texto informativo no e-mail.
  - ***Ação de vírus encontrado*** – você poderá especificar a ação a ser executada se um vírus for encontrado em um e-mail recebido:
    - ***Entregar e-mail para o destinatário*** - o e-mail infectado será enviado para o destinatário com um aviso sobre o vírus e arquivo infectado adicionado.

- ***Devolver e-mail ao remetente*** - o e-mail infectado será devolvido ao remetente como indesejável, com uma opção para adicionar um aviso sobre o vírus encontrado.

- ***Arquivos infectados*** - configurações adicionais definirão se os anexos infectados serão removidos da mensagem de e-mail e/ou movidos para a Quarentena do AVG. O campo Arquivos infectados permite especificar a ação a ser executada para arquivos infectados. As ações possíveis são:

  Remover – os arquivos infectados são removidos do e-mail

  Remover e armazenar na Quarentena – os arquivos infectados são removidos do e-mail e armazenados na quarentena local

  Armazenar na quarentena e entregar ao destinatário – os arquivos infectados são mantidos no e-mail e suas cópias também são armazenadas na quarentena local

  Entregar ao destinatário – os arquivos infectados serão mantidos no e-mail e entregues ao destinatário

- ***Enviar aviso ao destinatário/remetente*** – selecione este campo se quiser avisar o destinatário/remetente (dependendo se você escolher a ação Entregar e-mail ao destinatário ou Devolver e-mail ao remetente) do e-mail infectado com vírus.

- ***Texto do aviso*** – edite aqui o texto da mensagem padrão incluído no email infectado com vírus (caso você tenha selecionado anteriormente a opção Enviar aviso ao destinatário/remetente).

- ***Enviar aviso ao administrador*** – quando este campo estiver selecionado, um aviso será enviado aos administradores especificados no campo Administradores após a detecção de um e-mail recebido infectado com vírus. Edite o texto da mensagem de aviso no campo Texto do aviso correspondente.

- ***Configurações de E-mails Enviados***

  - ***Ação de vírus encontrado*** – você poderá especificar a ação a ser executada se um vírus for encontrado em um e-mail enviado:

    - ***Entregar e-mail para o destinatário*** - o e-mail infectado será enviado para o destinatário com um aviso sobre o vírus e arquivo infectado adicionado.

- ***Devolver e-mail ao remetente*** - o e-mail infectado será devolvido ao remetente como indesejável, com uma opção para adicionar um aviso sobre o vírus encontrado

- ***Arquivos infectados*** - configurações adicionais definirão se os anexos infectados serão removidos da mensagem de e-mail e/ou movidos para a Quarentena do AVG. O campo Arquivos infectados permite especificar a ação a ser executada para arquivos infectados. As ações possíveis são:

  Remover – os arquivos infectados são removidos do e-mail

  Remover e armazenar na Quarentena – os arquivos infectados são removidos do e-mail e armazenados na Quarentena de Vírus

  Armazenar na quarentena e entregar ao destinatário – os arquivos infectados são mantidos no e-mail e suas cópias também são armazenadas na quarentena local

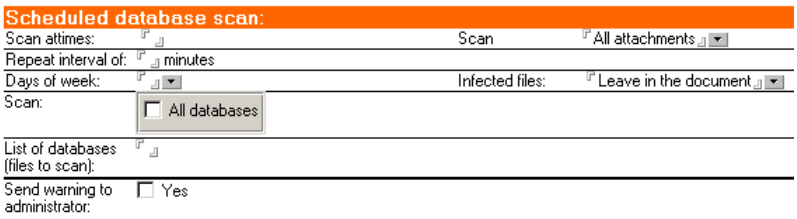
  Entregar ao destinatário – os arquivos infectados serão mantidos no e-mail e entregues ao destinatário

- ***Enviar aviso ao destinatário/remetente*** – selecione este campo se quiser avisar o destinatário/remetente (dependendo se você escolher a ação Entregar e-mail ao destinatário ou Devolver e-mail ao remetente) do e-mail infectado com vírus.

- ***Texto do aviso*** – edite aqui o texto da mensagem padrão incluído no email infectado com vírus (caso você tenha selecionado anteriormente a opção Enviar aviso ao destinatário/remetente).

- ***Enviar aviso ao administrador*** – quando este campo estiver selecionado, um aviso será enviado aos administradores especificados no campo Administradores após a detecção de um e-mail enviado infectado com vírus. Edite o texto da mensagem de aviso no campo Texto do aviso correspondente.

16.3.3.Verificação Programada de Banco de Dados



É possível planejar a verificação de bancos de dados do servidor nesta área do formulário de configuração do AVG for Lotus Notes/Domino Server. Há vários campos disponíveis:

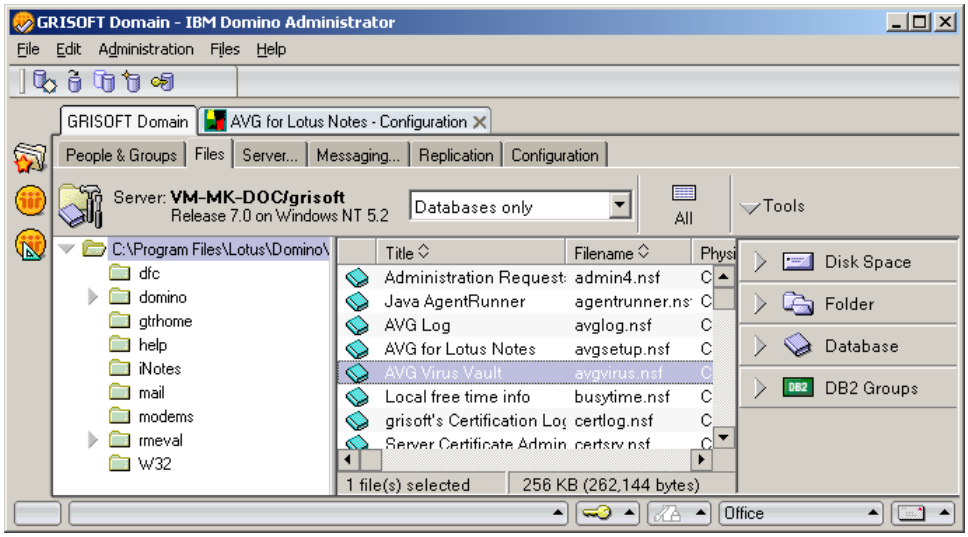
- ***Verificar em horários*** – especifique um intervalo e/ou a hora exata para dizer ao AVG para Lotus Notes/Domino Server quando a verificação de bancos de dados deve ser executada
- ***Intervalo de repetição de*** – especifique um período (em minutos) para definir a freqüência das verificações durante os intervalos especificados no campo Verificar em horários
- ***Dias da semana*** – selecione os dias em que os testes do banco de dados serão executados
- ***Verificar*** (campo relacionado aos anexos) – defina aqui se todos os anexos devem ser verificados ou somente aqueles com as extensões especificadas no campo Extensões
- ***Arquivos infectados*** - especifique aqui a ação a ser executada para arquivos infectados com vírus. As ações possíveis são:
  - ***Remover*** – os arquivos infectados são removidos do documento
  - ***Remover e armazenar na Quarentena*** – os arquivos infectados são removidos do documento e armazenados na Quarentena de Vírus
  - ***Deixar no documento*** - os arquivos infectados são mantidos no documento
- ***Verificar*** (campo relacionado aos bancos de dados) – defina aqui se todos os bancos de dados do servidor devem ser verificados ou somente aqueles especificados no campo Lista de bancos de dados (arquivos a serem verificados)

- ***Enviar aviso ao administrador*** – com este campo selecionado, um aviso será enviado aos administradores especificados no campo Administradores após a detecção de um vírus durante a verificação de banco de dados. Edite o texto da mensagem de aviso no campo Texto do aviso correspondente. Defina a linha do assunto da mensagem. No corpo da mensagem serão incluídos uma lista de arquivos infectados (com links) e os vírus encontrados.

Nota: *o desempenho do mecanismo de configuração e o filtro de anexos são controlados pelo AVG. Lembre-se de que as configurações do plug-in geralmente não podem ser definidas no AVG. Recursos como a ativação/desativação da verificação de e-mail e a certificação de e-mail podem ser configurados somente por meio de bancos de dados do AVG for Lotus Notes/Domino Server.*

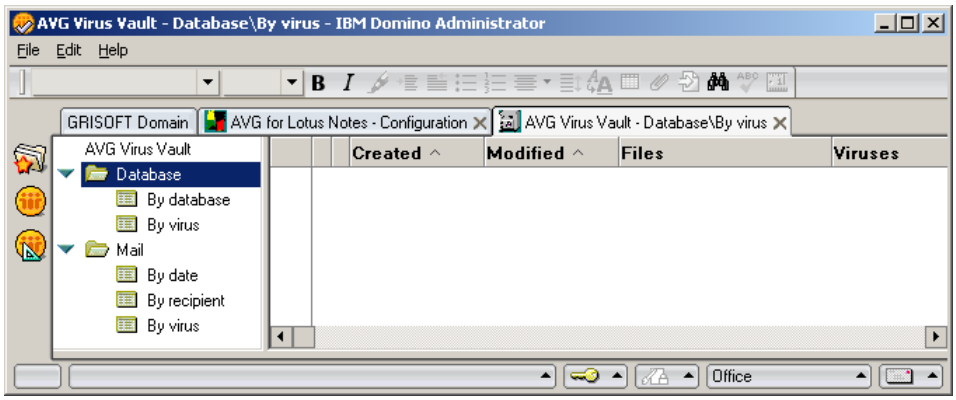
16.4.Quarentena de Vírus do AVG

AVG for Lotus Notes/Domino Server A Quarentena é um banco de dados de servidor especial em que você pode colocar os arquivos infectados para um tratamento seguro (exclusão ou recuperação), sem o risco de afetar o restante dos recursos do sistema.



No ambiente de administração do Lotus Notes/Domino Server, você pode acessar a Quarentena por meio do banco de dados ***Quarentena do AVG***. Observe que este banco de dados não tem nada a ver com o aplicativo Quarentena do AVG! É um banco de dados especial do Lotus Notes/Domino Server. Clique duas vezes no campo correspondente na janela principal do utilitário de administrador do Lotus / guia ***Arquivos*** e uma nova janela será aberta.

Examine os vírus armazenados na Quarentena de acordo com os seguintes parâmetros de agrupamento:



- ***Agrupados por bancos de dados*** (arquivos de bancos de dados infectados por vírus detectados durante verificações de banco de dados)

A classificação adicional é dividida em duas categorias:

- Por banco de dados
- Por vírus

Em cada categoria, há quatro campos presentes por padrão:

  - ***Criação*** – o carimbo de data/hora de criação do banco de dados
  - ***Modificação*** – o carimbo de data/hora de modificação do banco de dados
  - ***Arquivos*** – os arquivos infectados
  - ***Vírus*** – a identificação de vírus encontrado

- ***Agrupados por e-mail***

A classificação adicional é dividida em três categorias:

- Por data
- Por destinatário

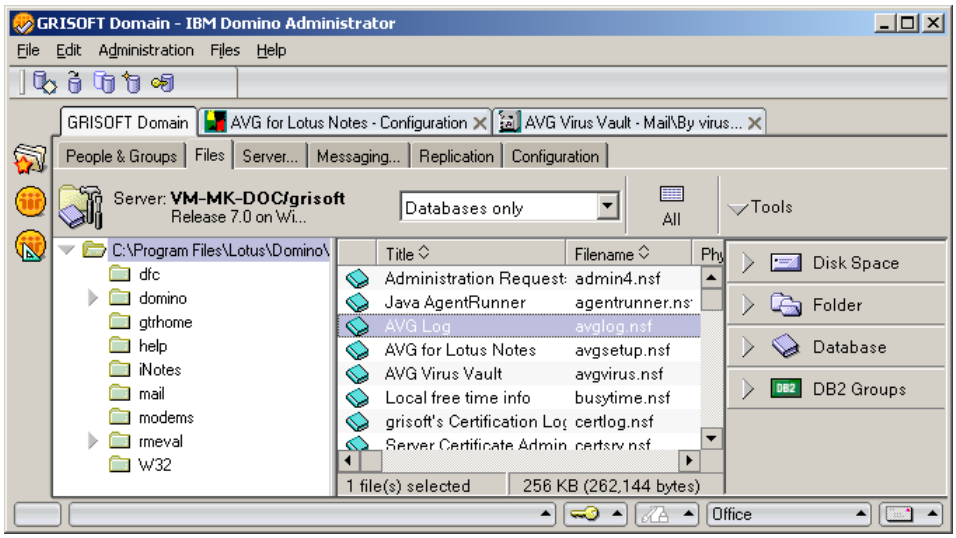
- Por vírus

Em cada categoria, há cinco campos presentes por padrão:

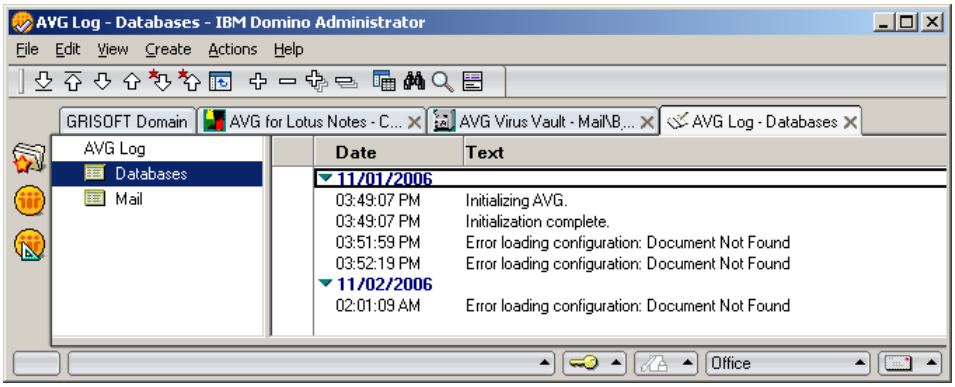
- **Hora** – a hora de entrega do e-mail infectado
- **Para** – as informações do destinatário
- **De** – as informações do remetente
- **Arquivos** – a identificação dos arquivos infectados
- **Vírus** – a identificação de vírus encontrado

16.5.Arquivos de Log do AVG

As informações sobre os eventos do **AVG for Lotus Notes/Domino Server** registrados durante a execução do servidor são armazenadas no arquivo de ***Log do AVG***. Nele é possível revisar e examinar mais ainda vários eventos, como o andamento da inicialização, as descobertas de vírus etc.



No ambiente de administração do Lotus Notes/Domino Server, você pode acessar o arquivo de ***Log do AVG*** por meio do ***banco de dados de Log do AVG***. Clique duas vezes no campo correspondente na janela principal do utilitário de administrador do Lotus / guia ***Arquivos*** para abrir uma nova janela.

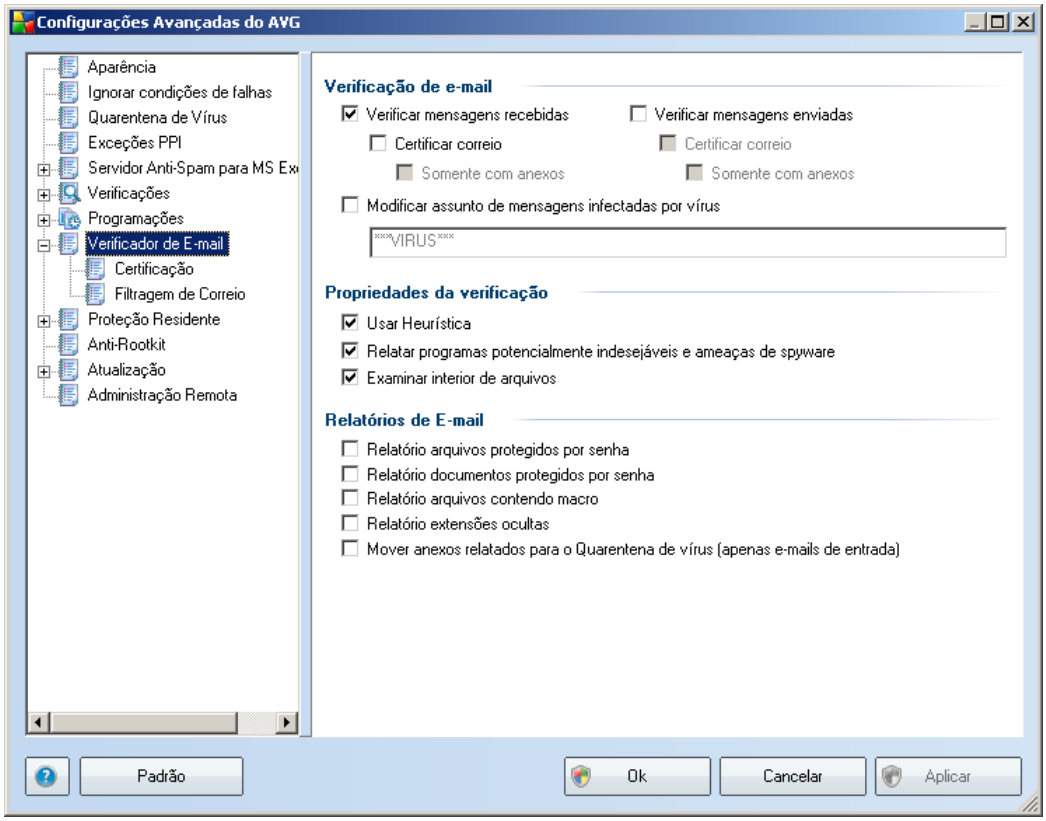


Há dois campos presentes para as pastas ***Bancos de dados*** e ***E-mail***. São eles:

- ***Data*** – o carimbo de data/hora do registro no log
- ***Texto*** – o texto das informações do log

17. Verificador de e-mail

As configurações do ***Verificador de e-mail*** são definidas no AVG File Server Edition. No menu principal do aplicativo, selecione***Ferramentas/Configurações Avançadas*** . No menu esquerdo, na caixa de diálogo **Configurações Avançadas**, selecione o item **Verificador de E-mail**.



A caixa de diálogo ***Verificador de E-mail*** é dividida em três seções:

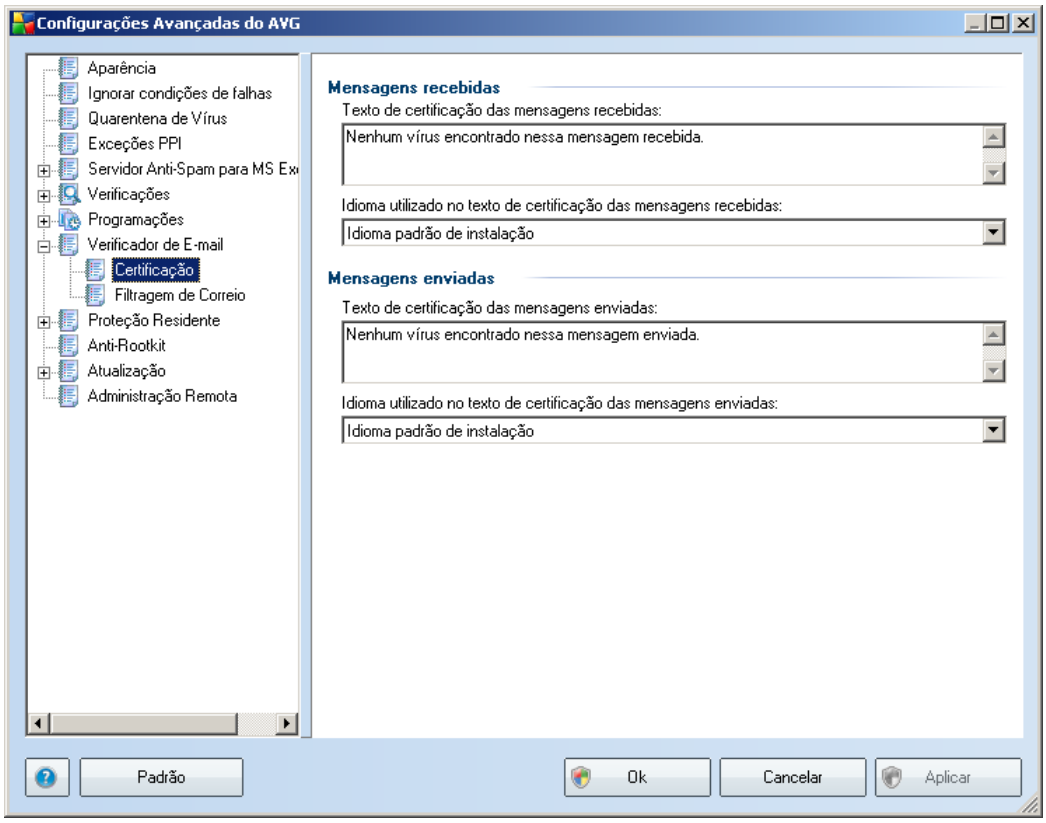
- ***Verificação de e-mail*** - nessa seção, selecione se deseja verificar as mensagens de e-mail enviadas/recebidas e se todos os e-mails devem ser certificados ou somente os que contêm anexos (*a certificação de e-mails sem vírus não tem suporte no formato HTML/RTF*). Além disso, você poderá escolher se deseja que o AVG modifique o assunto das mensagens que contêm vírus potenciais. Marque a caixa de seleção ***Modificar assunto das mensagens infectadas por vírus*** e altere o texto (*o valor padrão é ***VIRUS****).

- ***Propriedades da verificação*** - especifique se o método de análise heurística

deve ser usado durante a verificação (***Usar heurística***), se deseja verificar a presença de programas potencialmente indesejados***(Verificar Programas Potencialmente Indesejados***) e se os arquivos devem ser verificados também (***Verificar interior dos arquivos***).

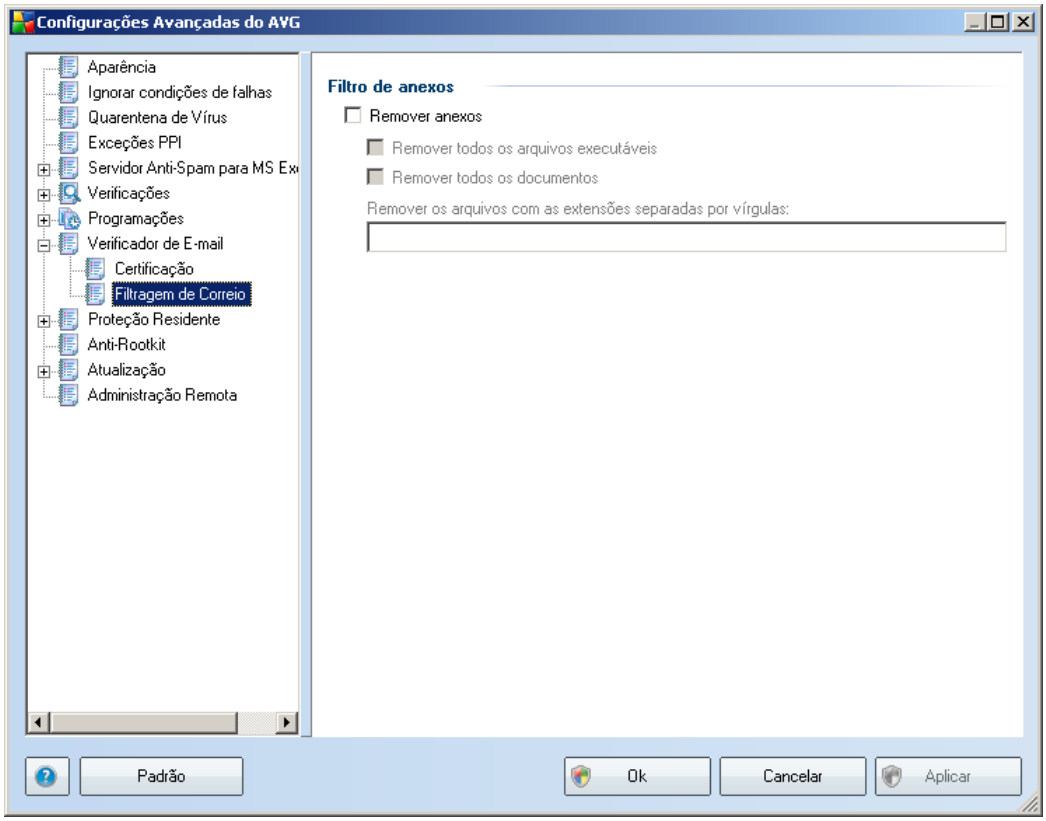
- ***Relatório de e-mail*** - especifique se você deseja ser notificado por e-mail sobre arquivos protegidos por senha, documentos protegidos por senha, arquivos contendo macros e/ou arquivos com extensão oculta detectados como anexo da mensagem de e-mail verificada. Se uma mensagem desse tipo for identificada durante a verificação, defina se o objeto infectado detectado deve ser movido para a ***Quarentena***.

17.1.Certificação



Na caixa de diálogo ***Certificação*** é possível especificar o texto que a nota de certificação deve conter e em que idioma. Essa especificação deve ser separada para as ***Mensagens recebidas*** e ***Mensagens enviadas***.

17.2.Filtragem de correio



A caixa de diálogo ***Filtro de anexo*** permite configurar parâmetros para a verificação de anexos de mensagens de e-mail. Por padrão, a opção***Remover anexos*** é desativada. Se você desejar ativá-la, todos anexos de mensagens de e-mail detectados como infectados ou potencialmente perigosos serão removidos automaticamente. Se você desejar especificar os tipos de anexo que devem ser removidos, selecione a opção apropriada:

- ***Remover todos os arquivos executáveis*** - todos os arquivos *.exe serão excluídos.
- ***Remover todos os documentos*** - todos os arquivos *.doc serão excluídos.
- ***Remover arquivos com estas extensões*** - removerá todos os arquivos com as extensões definidas.