AVG 7.5 Email Server Edition

User Manual

Document revision 75.3 (1.10.2006)

Contents

1. Introduction

Protection against computer viruses is one of the main issues of contemporary global computer security.

This user manual describes the installation, configuration and maintenance of products from **AVG 7.5 Email Server**.

AVG 7.5 Email Server offers many tools for automatic and reliable protection against any form of possible virus infection threatening your e-mail server. Its core function is the scanning of incoming and outgoing messages on your server, as well as scanning of the server's internal folder structures or databases (using the included **AVG 7.5 File Server** edition).

1.1. Anti-Virus and Anti-Spyware Detection Technologies

AVG 7.5 Email Server includes **AVG 7.5 File Server,** and uses its scanning and protection technologies to detect computer viruses and malware. Both products should be installed on the e-mail server so that **AVG 7.5 Email Server** can utilize the functionality of **AVG 7.5 File Server** components.

Note that the e-mail server computer will therefore be fully protected against viruses and malware. For further information on the protection capabilities of **AVG 7.5 File Server**, please refer to the document **AVG 7.5 File Server** User Manual that can be found in the downloads section of the Grisoft website at www.grisoft.com.

1.2. Operating Systems Supported

AVG 7.5 Email Server is intended to protect e-mail servers running under the following operating systems:

- Windows 2003 Server
- Windows 2000 Server
- Windows NT 4.0 Server
- Windows 9x/Me/2000/XP, workstation edition (Lotus Notes/Domino, and Kerio servers)
- Including 64-bit Windows versions

AVG 7.5 File Server must be installed on your computer in order to ensure e-mail antivirus and antispyware protection using the AVG scanning engine!

1.3. E-mail Server Versions Supported

- **AVG for Exchange 5.x Server** – Exchange 5.x Server versions
- **AVG for Exchange 2000/2003 Server** – Exchange 2000/2003 Server versions; for the Exchange 2000 Server Service Pack 1 (or higher) needs to be applied before you can use the AVG engine; AVG 7.5 File Server uses the VSAPI 2.0 (or 2.5 with Exchange 2003 Server) application interface which is covered in this Service Pack
- **AVG for Lotus Notes/Domino Server** – version 4.6 and higher

- **AVG for Kerio MailServer** – version 5.0.0 and higher (all versions available)

1.4. Reasons to Install AVG 7.5 Email Server

AVG 7.5 Email Server provides your system with reliable and comprehensive scanning of processed e-mail messages and server's internal mailbox folder structures. The main features of **AVG 7.5 Email Server** are:

- reliable scanning of incoming e-mail messages and mailbox folders on the server
- easy configuration (using the graphical user interface applications of particular servers or standalone AVG application)

2. Common Installation Steps

2.1. License Number

Please prepare your license/sales number; you will be asked for it during installation. Also, if you decide to download the latest product release you will need to provide your license number online. You received your license/sales number with your purchased copy of AVG product: either via e-mail, or on the registration card with the CD.

Installation of the **AVG for Exchange 5.x Server**, **AVG for Exchange 2000/2003 Server** and **AVG for Lotus Notes/Domino Server** products consists of two steps – first you have to install **AVG 7.5 File Server**, then you can install the AVG plugin for the respective server.

2.2. Latest Installation Files

You can get a product from **AVG 7.5 Email Server** on the CD.

Alternatively, you can download the latest related installation packs from the downloads section of the Grisoft website at www.grisoft.com. Go to the downloads section, follow the ***AVG 7.5 Email Server*** related links and select appropriate server and download all the necessary files (*installation packages of **AVG 7.5 File Server**, in case of Exchange 5.x Server, Exchange 2000/2003 Server and Lotus Notes/Domino Server also installation package of special AVG plugin for respective server*).

Note: *If you have used older AVG version before you decided to install the 7.5 version, you will need to uninstall it manually. You must perform the manual uninstallation for the following products from your previous version of AVG Email Server:*

- ***AVG for Exchange 5.x Server*** *– from the directory with the AVG for Exchange 5.x Server application files, run the uninstallation with **setupes.exe /uninstall** command.*
- ***AVG for Exchange 2000/2003 Server*** *– from the directory with the AVG for Exchange 2000 Server application files, run the uninstallation with **setupes.exe /uninstall** command.*
- ***AVG for Lotus Notes/Domino Server*** *– from the directory with the AVG for Lotus Notes/Domino Server application files, run the uninstallation with **setupln.exe /uninstall** command.*

After uninstalling the older version you can run the installation of the 7.5 version.

2.3. Installation from CD

Follow these steps to perform the installation:

a) Insert CD into the CD-ROM drive. If you have the CD autorun option enabled on your machine, it starts running automatically; then follow the further steps. *(If the installation does not start automatically, you have to launch it manually executing the respective files from your installation CD.)*

b) Select the application language.

***Note**: By default, only two application languages will be installed. The one you select in this dialog and English (the default language). If you select English language, then only English will be installed. You can choose to install additional languages in the **Component selection** dialog (later on in the installation process).*

c) Select what action you want to take – click on the ***AVG Installation*** menu item.

d) Select the product you want to install – click on the ***E-mail Server*** menu item.

e) Select the desired e-mail server from the menu.

f) In the same dialog window choose the ***full version*** of the respective product.

If you do not have the **AVG 7.5 File Server** installed on your computer, you must install it before installing a special AVG plugin for **Exchange 5.x**, **Exchange 2000/2003** and **Lotus Notes/Domino** servers. In case of **Kerio MailServer** it is necessary to install only **AVG 7.5 File Server**, because these servers have internal support of e-mail antivirus control using the AVG scanning engine.

2.4. Installation from the Internet

a) Refer to the downloads section of the Grisoft website at www.grisoft.com for the latest installation pack

b) Select ***AVG 7.5 Email Server*** section, choose the appropriate server, download all the files you need, and save them on your local disk

c) From the folder where you have saved the installation package run the installation executable file(s).

3. AVG for Exchange 5.x Server

3.1. Installation Progress

The setup process will first check versions of all necessary system libraries. If it is needed to install newer libraries, the installer will rename the old ones with a .delete extension. They will be deleted once the system restarts. After pressing the ***Finish*** button to end the successful installation, the system will reboot if you check ***Restart Now*** item in a corresponding dialog window.

a) Setup – Welcome

Execute the installation package, the introduction screen will appear. Press the ***Next*** button to continue with the installation.

b) Setup – License Agreement

The next window provides the full wording of the License Agreement. Please read it carefully, and if you accept all the points, confirm your approval by clicking the ***Accept*** button.

c) Setup – Application Registration

You should fill in your License Number in case you have purchased the **AVG File Server** and **AVG E-mail Server** separately. Otherwise, you will not be asked for it again. Confirm the provided information by clicking the ***Next*** button.

d) Setup – Installation Location

Once you have agreed to the license, you will be prompted to select the target installation folder. Press the ***Browse*** button to select a location other than the default one, though it is recommended to keep the default location. Click on the ***Next*** button to continue.

e) Setup – Start Copying Files

Setup prompts you to trigger copying of the installation files before the installation will be completed. Accept it by clicking on the ***Next*** button.

f) Setup – Service Installation

After installing the application files, the server service for ***AVG for Exchange 5.x Server*** must be installed. In order to perform this you have to be logged in as a system administrator. To verify this you will be asked for the administrator's password once the installation files copying has finished. Enter the password and press the ***Next*** button to complete the installation.

g) Setup – Installation Finished

Once the installation wizard has copied all of the necessary files to your hard drive and the ***AVG for Exchange service*** has been activated, the installation will be completed.

Pressing ***OK*** button in the ***Installation Finished*** window will close the setup dialog. If you check the ***Start configuration of AVG for Exchange Server*** item on, configuration window of ***AVG for Exchange 5.x Server*** application will be opened directly after completing the installation.

3.2. Program Maintenance

After ***AVG for Exchange 5.x Server*** installation your computer is receiving the most complete and reliable protection against computer virus threats.

You can launch the plugin main configuration window by:

- executing the ***AVG for Exchange 5.x Server*** icon on the Windows desktop
- from a folder, where the ***AVG for Exchange 5.x Server*** installation has been located launch the application file AVG4ESMAN.EXE
- from the ***AVG Control Center/E-mail Scanner*** component of **AVG File Server** by pressing the ***Properties*** button, selecting the AVG for MS Exchange Server plugin, and clicking on the ***Properties*** button in the respective ***AVG Control Center – E-mail Scanner*** window

After launching the ***AVG for Exchange 5.x Server*** application, a new window appears.

In the window's main menu you can save the edited settings using the ***Server*** item. You can customize the application's layout using the ***View*** menu item. Also, you can overview help and program information using the ***Help*** menu item. Below the main menu there is a shortcut toolbar displayed by default. Below the toolbar there is another set of buttons displayed by default; those buttons can be used to execute and/or suspend the ***AVG for Exchange 5.x Server*** service.

You can use the  button from the last mentioned button group for restarting the ***AVG for Exchange 5.x Server*** service. The button will be disabled until the service is running.

Note: *The application checks the service state (and also the buttons state change) every 10-15 seconds, so you may need to wait until the button is actually active again.*

Configuration of the ***AVG for Exchange 5.x Server*** consists of two basic parts. In the left-side panel of the application window there is a control tree; on the right you can see items relevant to the selected tree branch.

In the control tree you can find the following main branches:

a) Info Branch

The Info branch contains three other sub-branches:

- **Statistics**

  contains statistical information about the ***AVG for Exchange 5.x Server*** service state, and number of checked mailboxes, public folders and messages

  You can overview various statistical data here:

- *status* – this item displays the program status
- *version* – AVG for Exchange 5.x Server detailed version specification
- *uptime* – time period since the last AVG for Exchange 5.x Server restart
- *intercepted messages* – number of intercepted messages
- *queued messages* – number of messages ready in the scanning queue
- *messages in process* – number of messages currently being processed
- *processed messages* – number of processed messages
- *scanned mailboxes* – number of scanned mailboxes
- *queued mailboxes* – number of mailboxes ready in the scanning queue
- *monitored mailboxes* – number of mailboxes being monitored
- *scanned folders* – number of scanned folders
- *queued folders* – number of folders ready in the scanning queue
- *monitored folders* – number of folders being monitored

o **Loaded Actions**

contains internal information on the file which provides actions

The offered information describes the action (***AVG for Exchange 5.x Server*** plugin), corresponding version and path to the respective library file.

o **Loaded Restrictions**

contains internal information on conditions and restrictions

You can overview internal information on the file which provides restrictions on mail processing here. The provided information describes action, corresponding program version, and path to respective library file.

b) AVG Settings

The AVG Settings branch contains items related to configuration of user mailboxes and public folders that are scanned.

Two sub-branches are present in the settings branch. Their functionality is similar to each other; the ***Mailboxes*** branch covers scanning mailboxes for possible virus infection; the ***Public Folders*** branch provides the same information for Exchange Public Folders.

Note: *The scanning behavior is controlled from AVG Control Center using the settings of the AVG for MS Exchange Server plugin.*

If you disable scanning of incoming e-mail messages in AVG Control Center, the check will not be carried out by the AVG for Exchange 5.x Server either. You can configure filtering of attachments according to their extensions and

*filtering of encrypted archives and other additional features here after pressing the **Configure** button in the **AVG Control Center – E-mail Scanner** window:*

*Also, the text of e-mail certification can be changed only using the **AVG Control Center / E-mail Scanner** component after pressing the **Properties** button. Then you have to press the **Configure** button in the **Control Center – E-mail Scanner** window and edit the certification text there:*

Refer to the AVG File Server User Manual for further information on the Control Center; the User Manual can be downloaded from the Grisoft website at www.grisoft.com.

o **Mailbox List**

You can select mailboxes to be scanned in the ***Mailbox List*** branch by choosing the appropriate item from ***Type of Selection*** in the dialog shown on the following screenshot. Three items are available for selection:

- *All mailboxes* – no selection is possible; all mailboxes will be scanned
- *All mailboxes except selected mailboxes* – only those mailboxes that are not checked will be scanned
- *Only selected mailboxes* – only checked mailboxes will be scanned

You can also define the program behavior in case a virus infected message is detected. To do so, select the ***AVG for Exchange 5.x Server*** branch.

In this window you can enable/disable the feature of moving infected files to the Exchange 5.x Server folder (specified below). This procedure allows creating a common place where the messages processed by the virus scanner can be stored and further treated:

- You can check on/off the ***Enable moving infected messages to special folder*** to enable or disable this feature respectively.

  When the movement of infected messages option is disabled, all messages detected as infected remain at their original place (but they are copied to **AVG Virus Vault**). When the feature is enabled, infected attachments are moved to the **AVG Virus Vault** quarantine, and information on the infected attachment and detected virus is inserted into the infected message body.

- In the ***Virus Folder*** button group you can specify the special folders' structure. You can select whether you want to have a special virus folder in *each mailbox*, in *public folders,* or in *public folders' individual subfolders* for each user.
- In the ***Mailbox/Public Folder*** field you can change the location of the special virus quarantine folder. However, it is recommended to keep the preset location.

***Note:** The quarantine folder is created as a Public folder, so related "editor" rights are set for each user by default. The folder is created automatically when the first infected message is detected and the corresponding quarantine rule applied. We recommend you to change*

the folder access rights (using MS Exchange Administrator) following these steps:

(i) *In the MS Exchange Administrator control tree select **Folders/Public Folders***

(ii) *Choose a folder among Public folders.*

(iii) *Within the **File** main menu item choose the **Properties** option.*

(iv) *On the **General** tab press the **Client Permissions** button.*

(v) *For default Name select the None role.*

(vi) *Switch the default Folder Visible right off.*

(vii) *Now only users with access granted by MS Exchange 5.x Server Administrator can see and change content of this folder.*

o **Public Folders**

You can select folders to be scanned in the ***Folders*** branch by choosing the appropriate item from ***Type of Selection*** in the dialog shown on the following screenshot. Three items are available for selection:

- *All folders* – no selection possible; all folders will be scanned
- *All folders except selected folders* – only non selected folders will be scanned
- *Only selected folders* – only selected folders will be scanned

You can also define the ***AVG for Exchange 5.x Server*** behavior in case a virus infected message is detected; to do so select the ***AVG for Exchange 5.x Server*** branch:

In this window you can enable/disable the feature of moving infected files to the Exchange 5.x Server folder specified below. This procedure allows creating a common place where the messages processed by the virus scanner can be stored and further treated:

- You can check on/off the ***Enable moving infected messages to special folder*** option to enable or disable this feature respectively. When the infected messages movement option is disabled, all detected infected messages remain in their original place but they are copied to the **AVG Virus Vault**. When the feature is enabled, infected attachments are moved to the **AVG Virus Vault** quarantine, and information on the infected attachment and detected virus is inserted into the infected message body.
- In the ***Virus Folder*** button group, you can specify the special folders' structure. You can select whether you want to have a special virus folder in the *public folders* or in *public folders' individual subfolders* for each user.
- In the ***Mailbox/Public Folder*** field you can specify the location of the special virus quarantine folder.

Note: *The quarantine folder is created as a Public folder, and so related "editor" rights are set for each user by default. The folder is created automatically when the first infected message is detected and the corresponding quarantine rule applied. We recommend you to change the folder access rights (using MS Exchange Administrator) following this guide:*

(viii) In the MS Exchange Administrator control tree choose ***Folders / Public Folders***

(ix) Choose a folder among Public folders

(x) Within the ***File*** *main menu item choose the* ***Properties*** *option*

(xi) On the ***General*** *tab press the* ***Client Permissions*** *button*

(xii) For default Name select the ***None*** *role*

(xiii) Switch the default ***Folder Visible*** *right off*

(xiv) Now only users with access granted by Exchange 5.x Server Administrator can see and change content of this folder

c) Options Branch

The Options branch contains settings of the diagnostic information item. Within the ***Options*** branch there is only one sub-branch present – ***Diagnostic Logging***.

You can edit various logging properties of ***AVG for Exchange 5.x Server*** here.

- In the ***Log Mode*** button group you can specify the logging level of detail using following options:
  - *Debug* – detailed diagnostics reports will be logged
  - *Maximum* – all events (including informational messages) will be logged
  - *Medium* – serious events and warnings will be logged
  - *Minimum* – only serious events will be logged
  - *None* – no events to be logged
- In the ***New Log Time Period*** button group you can select the frequency of new log file creation:
  - *Hourly*– new log created each hour
  - *Daily*– new log created each day
  - *Weekly*– new log created each week
  - *Monthly*– new log created each month
  - *Yearly*– new log created each year
  - *Unlimited file size* – one unlimited increasing log file will be used

- *When file size reaches* – in the field below this item you can specify the maximum log file size; when the log file reaches the size, a new file will be created

o In the ***Log file directory*** you can specify the path to log file location.

o The ***Log file name*** field shows the general mask for a log file name.

You can agree to the configuration set in this window by pressing the ***OK*** button. Changes are discarded by pressing the ***Cancel*** button. Finally, changes are applied by pressing the ***Apply*** button.

4. AVG for Exchange 2000/2003 Server

4.1. Installation Progress

Since ***AVG for Exchange 2000/2003 Server*** uses the VSAPI 2.0/2.5 virus scanning interface, you must have the Service Pack 1 (or higher) for Exchange 2000 Server applied on your system. Follow the link below to get the Service Pack 1 for Exchange 2000 Server:

SP 1 for Exchange 2000 Server:
http://www.microsoft.com/exchange/downloads/2000/sp1.asp

For Exchange 2003 Server no additional service pack is needed; however, it is recommended to keep your system as up to date with the latest service packs and hotfixes as possible in order to obtain maximal available security.

At the beginning of the setup, all system libraries versions will be examined. If it is necessary to install newer libraries, the installer will rename the old ones with a ***.delete*** extension. They will be deleted after the system restart.

a) Setup – Welcome

Executing the installation file opens the setup introduction screen. Press the ***Next*** button to continue with the installation.

b) Setup – License Agreement

The next window provides the full wording of the License Agreement. Please read it carefully, and if you accept all the points, confirm your approval by clicking the ***Accept*** button.

c) Setup – Application Registration

You should fill in your license/sales number.

*This screen appears only in case you have purchased **AVG File Server** and **AVG for Exchange 2000/2003 Server** separately. Otherwise, you have already entered your license/ sales number during the AVG File Server installation, and you do not have to re-enter it.*

Confirm the provided information by clicking the ***Next*** button.

d) Setup – Installation Location

In the next window you will be prompted to select the target installation folder. Press the ***Browse*** button to select other location than the default one. If you do not have an actual reason to change the default settings, it is recommended to keep the preset location. Click on the ***Next*** button to continue.

e) Setup – Start Copying Files

Setup prompts you to trigger copying of the installation files before the installation will be completed. Accept it by clicking on the ***Next*** button.

f) Setup – Installation Finished

Once the installation wizard has copied all necessary files to your hard drive, the installation will be completed.

You can view the installation log file by pressing the ***Log*** button.

You can also view the setup log later as the setup.log file in your system temporary directory.

Press the ***OK*** button in the ***Installation Finished*** window to close the setup dialog.

g) Setup – Restarting the Store Service

Having closed the setup dialog you will be prompted to restart the Exchange 2000/2003 Server Store service.

Press the ***Yes*** button to restart the Store service with all ***AVG for Exchange 2000/2003*** components included. Then you can start to use the product.

Note: *Restarting the service will make your server unreachable for some time! You should warn your users before restarting the service because all users online will be automatically disconnected during the restart.*

4.2. Program Maintenance

When the Exchange 2000/2003 Server Store service is restarted after ***AVG for Exchange 2000/2003 Server*** has been installed, no further actions are needed to be taken to launch it.

To view the status of ***AVG for Exchange 2000/2003 Server***, launch the Exchange System Manager application. In the ***Servers*** branch of the control tree *(on the left side of the main window)* select the particular server. There is the ***AVG for Exchange*** branch in the server's sub-tree. Selecting this branch will open the information window showing various data to be overviewed.

The information displayed in the window include server name, application version, database version, and the total time of program run since the last restart. Also, items informing about anti-virus performance are displayed here *(performance monitor counters)*.

AVG for Exchange 2000/2003 Server scans all messages in the databases of private and public folders. If a virus is found, ***AVG for Exchange 2000/2003 Server*** writes a message into the AVG log file and also into the Event Log.

(For details see the 4.3 - AVG for Exchange 2000/2003 Server Monitoring section of this chapter.)

Virus Scanning **API 2.0** (VSAPI 2.0 as provided in Exchange 2000 Server) does not allow the deletion of infected e-mail files. Since the virus infected e-mail message attachment cannot be deleted, its filename is changed: ***AVG for Exchange 2000/2003 Server*** appends the ***.virusinfo.txt*** extension to the original filename. The file content is overwritten with a message about the known virus. If a virus is

found directly in the message, the whole body of the message is overwritten with a note saying a virus was found inside this message.

Virus Scanning **API 2.5** *(VSAPI 2.5 as provided in Exchange 2003 Server)* also allows deletion of messages infected files. This feature can be set up in ***AVG for Exchange 2000/2003 Server*** configuration dialog.

The ***AVG for Exchange 2000/2003 Server*** configuration window can be opened by right clicking on the ***AVG for Exchange*** branch, and selecting the ***Properties*** item. Alternatively, you can open the window using the ***Action*** button, which is right below the Exchange System Manager application main menu.

The ***AVG for Exchange Properties*** configuration window consists of two tabs. You can change the e-mail virus scanning settings and the logging behavior here.

a) General Tab

On the ***General*** tab you will find several preset options related to the ***AVG for Exchange 2000/2003 Server*** e-mail virus scanning performance:

- ***Enable*** checkbox – you can enable or disable mail scanning here.
- ***Background Scanning*** checkbox – you can enable or disable the background scanning process here. Background scanning is one of the features of the VSAPI 2.0/2.5 application interface. It provides threaded scanning of the Exchange Messaging Databases. Whenever an item that has not been scanned before is encountered in the users' mailbox folders, it is submitted to ***AVG for Exchange 2000/2003 Server*** to be scanned. Scanning and searching for the not examined objects runs in parallel.
- ***Proactive Scanning*** checkbox – you can enable or disable the proactive scanning function of VSAPI 2.0/2.5 here. The proactive scanning lies in dynamical priority management of items in scanning queue. The lower priority items are not being scanned unless all the higher priority ones (most frequently supplied on demand in the queue) have been scanned. However, an item's priority rises if a client tries to use it, so the items' precedence changes according to users' activity.
- ***Scan RTF*** checkbox – you can specify here, whether the RTF file type should be scanned or not.
- ***Scanning Threads*** field – the scanning process is threaded by default to increase the overall scanning performance by a certain level of parallelism. You can change the threads count here. The default number of threads is computed as 2 times the 'number_ of_processors' + 1.
- ***Scan Timeout*** field – the maximum continuous interval (in seconds) for one thread to access the message that is being scanned.
- ***Move infected files to the Virus Vault*** – if checked on, every infected e-mail message file will be moved into **AVG Virus Vault** quarantine environment.
- ***Delete messages with infected files (ES 2003 only)*** – after checking this item on, a message where a virus is detected will be deleted. When this item is checked off, the infected e-mail is delivered to recipient, but infected attachment is replaced with a text file containing

information on the virus detected. This option is available only in VSAPI 2.5 in Exchange 2003 Server.

Generally, all the features on this tab are user extensions of the Microsoft VSAPI 2.0/2.5 application interface services. For the detailed information on the VSAPI 2.0/2.5 please refer to the following links (and also the links accessible from the referenced ones):

- http://support.microsoft.com:80/support/kb/articles/Q285/6/67.ASP for general info on the VSAPI 2.0 in Exchange 2000 Server Service Pack 1
- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k for information on Exchange and antivirus software interaction
- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 for information on additional VSAPI 2.5 features in Exchange 2003 Server application.

Note: *The scanning behavior is controlled from AVG Control Center using the settings of AVG for MS Exchange Server plugin:*

If you disable scanning of incoming e-mail messages in AVG Control Center, the check will not be performed by AVG for Exchange 2000/2003 Server either. You can also configure filtering of attachments according to their extensions and filtering of encrypted archives and other additional features here:

For details on AVG Control Center please refer to the AVG File Server User Manual document in the downloads section of the Grisoft website at www.grisoft.com.

b) Diagnostics Logging Tab

On this tab you can define the virus scanning logging frequency and general behavior here. Several fields are preset on the ***Diagnostics Logging*** tab:

- ***Log Mode*** radio button group – you can adjust the amount of information to be logged here.
- ***New Log Time Period*** radio button group – you can define the period of new log file creation, and possibly the log file size here.
- ***Log file directory*** field – you can change the default log file location here.
- ***Log file name*** field – you can see the default log filename here.
- ***Screen Refresh*** field – you can specify how often the online monitoring screen (shown on the ***AVG for Exchange 2000/2003 Server*** information window) should be refreshed.

4.3. AVG for Exchange 2000/2003 Server Monitoring

a) Online Monitoring

In the ***AVG for Exchange 2000/2003 Server*** information window (*Refer to the beginning of this section to see how to get there.*), there are several fields displayed:

The first four items provide general information on the server and ***AVG for Exchange 2000/2003 Server*** status:

- ***Server*** – server name
- ***Version*** – version of AVG for Exchange 2000/2003 Server
- ***Kernel version*** – version of the Anti-Virus kernel, and its internal virus database
- ***Uptime*** –total time since the last Exchange 5.x Server restart

The other items represent particular VSAPI 2.0/2.5 performance monitor counters related to virus scanning of Exchange 2000/2003 Server. Counters are described as follows:

- ***Bytes Scanned*** – total number of bytes in all files processed by the virus scanner
- ***Files Cleaned*** – total number of separate files cleaned by the virus scanner
- ***Files Cleaned/sec*** – rate at which separate files are cleaned by the virus scanner
- ***Files Quarantined*** – total number of separate files moved to quarantine by the virus scanner
- ***Files Quarantined/sec*** – rate at which separate files are put into quarantine by the virus scanner
- ***Folders Scanned in Background*** – total number of folders processed by background scanning
- ***Messages Cleaned*** – total number of top-level messages cleaned by the virus scanner
- ***Messages Cleaned/sec*** – rate at which top-level messages are cleaned by the virus scanner
- ***Messages Quarantined*** – total number of top-level messages moved to quarantine by the virus scanner
- ***Messages Quarantined/sec*** – rate at which top-level messages are put into quarantine by the virus scanner
- ***Messages Processed*** – cumulative value of the total number of top-level messages processed by the virus scanner
- ***Messages Processed/sec*** – rate at which top-level messages are processed by the virus scanner
- ***Messages Scanned in Background*** – total number of messages processed by background scanning
- ***Queue Length*** – current number of outstanding requests that are queued for virus scanning
- ***Waiting Files*** – count of files waiting to be scanned
- ***Messages Deleted –*** total number of suspect messages deleted by virus scanner (available only in VSAPI 2.5)
- ***Messages Deleted/sec –*** rate at which suspect messages are deleted by virus scanner (available only in VSAPI 2.5)

b) Operating System Event Log

Except for the online monitoring of ***AVG for Exchange 2000/2003 Server*** you can also setup the virus scanner related events logging within the **Event Log**. Available events cover many issues, such as program libraries loading notes, virus-found events, troubleshooting warnings, etc.

You can set up the logging level of Exchange VSAPI 2.0/2.5 in the Exchange System Manager's main window *(as shown in the beginning of this section)*.

- Double-click the ***Servers*** branch in the control tree
- Select the particular server *(see an example server name highlighted in the picture below)*
- Right-click the server name, and select the ***Properties*** item from the context menu
- The ***Properties*** window appears.
- Switch to the ***Diagnostics Logging*** tab
- From the ***Services*** tree select the ***MSExchangeIS / System*** folder
- From the opened ***Categories*** list select the ***Virus Scanning*** item, and choose the desired logging level for the operating system Event Log component. The following levels are offered:
  - *None*
  - *Minimum*
  - *Medium*
  - *Maximum*

Note: *You will find the complete description of the VSAPI 2.0/2.5 events on this link: http://support.microsoft.com/default.aspx?scid=kb;EN-US;294336.*

5. AVG for Lotus Notes/Domino Server

5.1. Installation Progress

Make sure none of the e-mail server applications is running before you start ***AVG for Lotus Notes/Domino Server*** installation! When all the server processes and services are shut down, you can follow the installation instructions below.

The setup process will first check versions of all necessary system libraries. If it is needed to install newer libraries, the installer will rename the old ones with a .delete extension. They will be deleted once the system restarts. After pressing the ***Finish*** button to end the successful installation the system will reboot if you check the ***Restart Now*** item in a corresponding dialog window displayed.

a) Setup – Welcome

Execute the installation package; the introduction screen will appear. Press the ***Next*** button to continue with the installation.

b) Setup – License Agreement

The next window provides the full wording of the License Agreement. Please read it carefully, and if you accept all the points, confirm your approval by clicking the ***Accept*** button.

c) Setup – Application Registration

In this screen you should fill in your ***AVG for Lotus Notes/Domino Server*** license number.

You will only be asked to provide your license number in case you have purchased **AVG File Server** (or **AVG Anti-Virus**) and ***AVG for Lotus Notes/Domino Server*** separately. Otherwise, you have already provided the license number during the **AVG File Server** or **AVG Anti-Virus** installation, and you will not be asked for it again.

Confirm the information provided by clicking the ***Next*** button.

d) Setup – Installation Location

Once you have agreed to the license agreement, you will be prompted to select the target installation folder. The ***AVG for Lotus Notes/Domino Server*** data and program files will be installed directly into the Lotus Notes/Domino folder. Press the ***Browse*** button to select a location other than the default one, though it is recommended to keep the default location. Click on the ***Next*** button to continue.

e) Setup – NOTES.INI

In order to install ***AVG for Lotus Notes/Domino Server*** correctly it is necessary to locate the Lotus Notes/Domino server configuration file NOTES.INI. If NOTES.INI is not found automatically, you will be prompted to set its path manually (by pressing the ***Browse*** button or by filling in the complete path directly). Click on the ***Next*** button to continue.

f) Setup – Installation Finished

Once the installation wizard has copied all of the necessary files to your hard drive, the installation is completed.

5.2. Program Maintenance

Your computer is now receiving the most complete and reliable protection against computer virus threats.

The following files were installed:

- ***Lotus Notes/Domino program directory:***
  - navgscan.exe – server application for checking databases
  - navgmail.exe – server anti-virus mail checking application
  - navghook.dll – library for holding mail in the MAIL.BOX database until it has been scanned for viruses
- ***Lotus Notes/Domino data directory:***
  - avgsetup.ntf – configuration database template
  - avglog.ntf – log database template
  - avgvirus.ntf – virus vault template
  - avgsetup.nsf – configuration database
  - avglog.nsf – log database
  - avgvirus.nsf – virus vault database

In order to complete the installation, the Lotus Notes/Domino server must be restarted. This will automatically launch ***AVG for Lotus Notes/Domino Server*** (server services AvgScan and AvgMail) and create the AVG databases (Configuration, Log and Vault). All of these can be blocked in the appropriate configuration sections later if needed.

After correct installation of ***AVG for Lotus Notes/Domino Server*** and Lotus Domino server restart there are no further actions needed for efficient mail protection. The default ***AVG for Lotus Notes/Domino Server*** settings for are as follows:

- scan all e-mails with attachments
- a certification message will be added to any e-mail which is virus-free, does not include a signature attachment, and has not been encrypted
- incoming files that are considered infected are sent to the recipient with a message containing file and virus details
- outgoing e-mail containing infected attachments will be returned to the sender with information about the infected objects and corresponding viruses; the infected e-mail will not be delivered to the recipient

You can easily change the default configuration of ***AVG for Lotus Notes/Domino Server*** using the Domino Administrator utility. After selecting the ***Files*** tab in the initial window, you will see three AVG related files (Lotus databases literally) among all the files to administer:

- ***AVG Log*** (see section 5.4 AVG Log File)
- ***AVG for Lotus Notes*** (see section 5.2 Program Maintenance)
- ***AVG Virus Vault*** (see section 5.3 AVG Virus Vault)

Double click the ***AVG for Lotus Notes*** in the administrator utility main window / ***File*** tab to open the ***AVG for Lotus Notes – Configuration*** window.

In this window, select the server, on which you want to have the AVG configuration database. Double click on the server field, or simply press the ***Edit*** button that is right above the servers list. A new untitled window opens then within the Lotus administrator utility environment.

You can fully control the scanning and infected e-mail management behavior of ***AVG for Lotus Notes/Domino Server***. Also you can schedule multiple Lotus database scans. To save the performed configuration changes, press the ***Save and close*** button in the upper area of the window.

All the configuration options fully corresponding to the fields presented on the screenshots above are as follows:

a) Global Settings

- ***Server name*** – the current server specification
- ***Certify mail*** – select whether ***AVG for Lotus Notes/Domino*** should certify e-mails or not
- ***Certify text*** – edit the certification text (e. g. “The message is virus-free...”)

b) Mail Scan

- ***Scan mail*** – enable/disable the automatic e-mail anti-virus scan

c) Incoming Mail Settings

- ***Attachments*** – the option enables defining file extensions of e-mail attachments that should be automatically removed from the e-mail. Attachments with user-defined extensions will be automatically removed from an incoming e-mail message, no matter whether the identified file has been infected by a virus or not. The possible actions are:
  - *No action* - incoming attachments will not be filtered or removed
  - *Remove* - user defined attachments will be removed from virus-detected e-mail message, and then deleted
  - *Remove and store in Virus Vault* - user defined attachments will be deleted from virus-detected e-mail, and moved to the Virus Vault

  You will be allowed to choose the attachment file extensions from the list of keywords (or you can type a new one if the desired extension is not in the list) in a new ***Extensions*** field when the *Remove* or *Remove and store...* actions are selected.

- ***Virus found action*** – you can specify action to be taken if a virus is found in an incoming e-mail:

- *Deliver mail to the recipient* - the infected e-mail will be delivered to the recipient with a warning about the virus and infected file added; additional settings will define whether the infected attachments are removed from the email message and/or moved to the ***AVG Virus Vault***. The ***Infected files*** field allows you to specify the action to be taken for virus infected files. Possible actions are:

  Remove – the infected files are removed from the e-mail

  Remove and store in Virus Vault – the infected files are removed from the e-mail and stored in the local Virus Vault

  Store in Virus Vault and deliver to recipient – the infected files are kept in the e-mail, and their copies are also stored in the local Virus Vault

  Deliver to recipient – the infected files will be kept in the e-mail, and delivered to recipient

- *Return mail to sender* - the infected e-mail will be returned to the sender as undeliverable with an option to add a warning about the virus found
- ***Send warning to recipient/sender*** – you should select this field if you wish to warn the recipient/sender (depending on whether you choose *Deliver mail to the recipient* or *Return mail to the sender* action) of virus-infected e-mail.
- ***Text of warning*** – here you can edit the default message text included in the virus-infected email (if you have previously selected the ***Send warning to recipient/sender*** option).
- ***Send warning to administrator*** – when this field is selected, a warning will be sent to administrators specified in the ***Administrators*** field after an incoming e-mail is detected as virus-infected. You can edit the text of the warning message in the corresponding ***Text of warning*** field.

d) Outgoing Mail Settings

- ***Virus found action*** – you can specify what action is to be taken if a virus is found in an outgoing e-mail message:

  - *Deliver mail to the recipient* - the infected e-mail message will be delivered to the recipient with a warning about the virus and infected file added; additional settings will define whether the infected attachments are removed from the email message and/or moved to the ***AVG Virus Vault***. The ***Infected files*** field allows you to specify the action to be taken for virus-infected files. Possible actions are:

    Remove – the infected files are removed from the e-mail

    Remove and store in Virus Vault – the infected files are removed from the e-mail and stored in local Virus Vault

    Store in Virus Vault and deliver to recipient – the infected files are kept in the e-mail, and copies are also stored in local Virus Vault

    Deliver to recipient – the infected files will be kept in the e-mail, and delivered to recipient

- *Return mail to sender* - the infected e-mail message will be returned to the sender as undeliverable with an option of adding a warning about the virus found
- ***Send warning to recipient/sender*** – select this field if you wish to warn the recipient/sender (depending on whether you choose *Deliver mail to the recipient* or *Return mail to the sender* action) of virus-infected e-mail.
- ***Text of warning*** – here you can edit the default message text included in the virus-infected email message if you have previously selected the ***Send warning to recipient/sender*** option.
- ***Send warning to administrator*** – with this field selected, a warning will be sent to administrators specified in the ***Administrators*** field after an outgoing e-mail is detected as virus-infected. You can edit the text of the warning message in the corresponding ***Text of warning*** field.

e) Scheduled Database Scan

You can plan the scanning of server databases in this area of the ***AVG for Lotus Notes/Domino Server*** configuration form. Various fields are available:

- ***Scan at times*** – specify a time interval and/or exact time to tell ***AVG for Lotus Notes/Domino Server*** when it should run the databases scanning
- ***Repeat interval of*** – specify a time period (in minutes) defining the frequency of scans during the intervals specified in the Scan at times field
- ***Days of the week*** – you can select the days when database tests are run
- ***Scan*** (the attachments related field) – here you can define whether to check all the attachments or only those with extensions specified in the ***Extensions*** field
- ***Infected files*** - here you can specify the action to be taken for virus-infected files. Possible actions are:
  - *Remove* – the infected files are removed from the document
  - *Remove and store in Virus Vault* – the infected files are removed from the document, and stored in the local Virus Vault
  - *Leave in the document* - the infected files are kept in the document
- ***Scan*** (the databases related field) – here you can define whether to scan all the server databases or only those specified in the ***List of databases*** (files to scan) field
- ***Send warning to administrator*** – with this field selected, a warning will be sent to administrators specified in the ***Administrators*** field after a virus is detected during the database scan. You can edit the text of the warning message in the corresponding ***Text of warning*** field. You can define the subject line of the message. In the message body, a list of infected files (with links) and found viruses will be included.

Note: *The scanning engine performance and the attachment filter are controlled from AVG Control Center. Please remember that the plugin settings in general*

cannot be configured in the AVG Control Center. Features like e-mail scanning enabling/disabling, and e-mail certification can be configured only via AVG for Lotus Notes/Domino Server databases.

5.3. AVG Virus Vault

AVG for Lotus Notes/Domino Server Virus Vault is special server database where you can place the virus-infected files for safe further treatment (deletion or recovery) without risk of affecting the rest of your system resources.

In the Lotus Notes/Domino Server administration environment you can access the Virus Vault via the **AVG Virus Vault** database. Note that this database has nothing to do with the **AVG Virus Vault** application! It is a special Lotus Notes/Domino Server database. Double click the corresponding field in the Lotus administrator utility main window / ***File*** tab to open and a new window will be opened.

You can examine the viruses stored in the Virus Vault according the following grouping parameters:

a) Grouped by virus infected database files detected during database scans:

There are four fields present by default:

- *Created* – the database creation timestamp
- *Modified* – the database modification timestamp
- *Files* – the infected files
- *Viruses* – the viruses found identification

b) Grouped by viruses found in databases during database scans:

There are four fields present by default:

- *Created* – the database creation timestamp
- *Modified* – the database modification timestamp
- *Files* – the infected files
- *Viruses* – the viruses found identification

c) Grouped by the date of infected message detected in e-mail scan:

There are five fields present by default:

- *Time* – the infected e-mail delivery time
- *For* – the recipient info
- *From* – the sender info
- *Files* – the infected files identification
- *Viruses* – the viruses found identification

d) Grouped by the recipient of infected message detected in e-mail scan:

There are four fields present by default:

- *Time* – the infected e-mail delivery time
- *From* – the sender info
- *Files* – the infected files identification
- *Viruses* – the viruses found identification

e) Grouped by the virus in infected message detected in e-mail scan:

There are five fields present by default:

- *Time* – the infected e-mail delivery time
- *For* – the recipient info
- *From* – the sender info
- *Files* – the infected files identification
- *Viruses* – the viruses found identification

5.4. AVG Log File

Information on ***AVG for Lotus Notes/Domino Server*** events recorded during the server's run is stored in the AVG Log file. Here you can review and further examine various events, such as initialization progress, viruses findings, etc.

In the Lotus Notes/Domino Server administration environment you can access the AVG Log file via the AVG Log database. Double click the corresponding field in the Lotus administrator utility main window/ ***Files*** tab to open new window.

There are two fields present for both the Databases and Mail folders. Those are:

- *Date* – the timestamp of the logged record
- *Text* – the text of the log information

6. AVG for Kerio MailServer

The anti-virus protection mechanism is integrated directly into the Kerio MailServer application. In order to activate e-mail protection of Kerio MailServer by the Anti-Virus scanning engine, launch the Kerio Administration Console application. In the control tree on the left side of the application window choose the ***Content Filter*** sub-branch in the ***Configuration*** branch.

Click the ***Content Filter*** item to open the dialog window. There are three items in the window:

- ***Spam Filter***
- ***Antivirus*** (see section 6.1 – Antivirus Item)
- ***Attachment Filter*** (see section 6.2 – Attachment Filter Item)

All changes made can be saved by pressing the ***Apply*** button in the bottom area of this configuration window. You can also return to the previously saved state by pressing the ***Reset*** button.

6.1. Antivirus Item

To activate ***AVG for Kerio MailServer*****,** select the ***Use external antivirus*** checkbox and choose the **AVG Email Server** edition from the external software menu on the ***Antivirus usage*** frame of the configuration window.

In the following section you can specify what to do with an infected or filtered message:

a) If a virus is found in a message

This frame specifies the action to be carried out when a virus is detected in a message, or when a message is filtered by an attachment filter:

- ***Discard the message*** – when selected, the infected or filtered message will be deleted.
- ***Deliver the message with the malicious code removed*** – when selected, the message will be delivered to the recipient, but without the possibly harmful attachment.
- ***Forward the original message to administrator address*** – when selected, the virus infected message is forwarded to the address specified in the address text field
- ***Forward the filtered message to administrator address*** - when selected, the filtered message is forwarded to the address specified in the address text field

b) If a part of message cannot be scanned (e.g. encrypted or corrupted file)

This frame specifies the action to be taken when part of the message or attachment cannot be scanned:

- **Deliver the original message with a prepared warning** — the message (or attachment) will be delivered unchecked. The user will be warned that the message may still contain viruses.
- **Reject the message as if it was virus** — the system will react the same way as when a virus was detected (i.e. the message will be delivered without any attachment or rejected). This option is safe, but sending password protected archives will be virtually impossible.

Note: *Scanning engine performance and behavior is controlled from the AVG Control Center. If you disable scanning of incoming e-mail messages in AVG Control Center, the scanning will not be carried out by the AVG for Kerio MailServer either. For details on AVG Control Center please refer to the AVG File Server (or AVG Anti-Virus) User Manual in the downloads section of the Grisoft website at www.grisoft.com.*

6.2. Attachment Filter Item

In the ***Attachment Filter*** menu there is a list of various attachment definitions:

You can enable/disable filtering of mail attachments by selecting the ***Enable attachment filter*** checkbox. Optionally you can change the following settings:

- **Send a warning to sender that the attachment was not delivered**

  The sender will receive a warning from Kerio MailServer, that he/she has sent a message with a virus or blocked attachment.

- **Forward the original message to administrator address**

  The message will be forwarded (as it is — with the infected or forbidden attachment) to a defined email address, regardless of whether it is a local or an external address.

- **Forward the filtered message to administrator address**

  The message without its infected or prohibited attachment will be (apart from the actions selected below) forwarded to the specified e-mail address. This can be used to verify the correct functioning of the antivirus and/or attachment filter.

In the list of extensions, each item has four fields:

- ***Type*** – specification of the kind of attachment determined by the extension given in the ***Content*** field. Possible types are *File name* or *MIME type*. You can select the respective box in this field to include/exclude the item from attachment filtering.
- ***Content*** – an extension to be filtered can be specified here. You can use operation system wildcards here (for example the string '*.doc.*' stands for any file with the .doc extension, and any other extension following).
- ***Action*** – define action to be performed with the particular attachment. Possible actions are *Accept* (accept the attachment), and *Block* (block the attachment as defined in the ***Action*** tab dialog).
- ***Description*** – description of the attachment is defined in this field.

An item is removed from the list by pressing the ***Remove*** button. You can add another item to the list by pressing the ***Add...*** button. Or, you can edit an existing

record by pressing the ***Edit...*** button. A window with the following items then appears:

- In the ***Description*** field you can write a short description of the attachment to be filtered.
- In the ***If a mail message contains an attachment where*** field you can select the type of attachment (*File name* or *MIME type*). You can also choose a particular extension from the offered extensions list, or you can type the extension wildcard directly.
- In the ***Then*** field you can decide whether to block the defined attachment or accept it.

7. Program Updates

Anti-virus system can ensure reliable protection only when it is updated regularly. **AVG 7.5 Email Server** edition provides a reliable and fast update service with quick response times. Modern viruses spread very quickly and infect huge numbers of workstations in almost no time. Therefore, it is necessary that servers in particular are updated as soon as possible so that the threat is stopped before end-user machines can be infected.

7.1. Update Levels

AVG offers three update levels to select from:

- **Priority Update**

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

- **Recommended Update**

  A Recommended Update contains various program changes, fixes and improvements.

  For mission-critical systems, it is recommended that such updates are not applied automatically when available, but rather that they are tested in a testing environment first.

  Note: *Generally, if your system policy is not to apply operating system patches and updates on production servers without testing them first in a test environment, you should not apply recommended updates on such servers either. If you apply OS patches on servers directly without any further testing, you can do the same with recommended updates.*

- **Optional Update**

  An Optional Update reflects changes that are not necessary for program functionality – texts, updates of the setup component, etc. Optional updates can be downloaded and applied together with recommended updates but their importance is rather low.

When scheduling an update, it is possible to select which priority level should be downloaded and applied. Higher update levels automatically include more critical ones.

The recommended update periods for an e-mail server are as follows:

- Priority update – every 2 hours
- Recommended update – on demand, or once a day

7.2. Update Types

You can distinguish between two types of update:

- **On Demand Update**

An On Demand Update is an immediate update that can be performed any time when the need arises.

- **Scheduled update**

  Within **AVG File Server** or **AVG Anti-Virus** it is also possible to preset an update plan. The planned update is then performed periodically according to the set up configuration. If new update files are available, they are downloaded from the Internet.

7.3. Update Schedule

The update files can be downloaded directly from the Internet. To make sure you always get the latest version of update files it is recommended to create an update schedule that checks for critical updates directly from the Internet at regular intervals.

To set up the update schedule follow these steps:

a) Update – Control Center

In AVG Control Center select the ***Test Center*** item from the left menu, and in the bottom part of the dialog window press the ***Scheduled task*** button.

b) Update – Scheduled Tasks

In the new ***Scheduled tasks*** dialog window press the ***New schedule*** button.

c) Update – Scheduled Task Properties / Task

In the new ***Scheduled task properties*** dialog window stay on the ***Task*** tab, and select from the list of possibilities available for the ***Schedule*** item.

Note: *Remember that in the case of AVG 7.5 Email Server the schedule should be planned for all users and not for the current user only!*

d) Update – Scheduled Task Properties / Perform Task

For both update types you can then configure the regular update time on the ***Perform task*** tab.

You can select the periodicity setting from a list – item ***Periodicity***. Depending on the Internet connection available, an interval of 2 to 6 hours may be appropriate for such a task on an e-mail server. However, you can set up the periodicity otherwise according to your own needs, and then you can also configure other timing parameters appropriately.

e) Update – Scheduled Task Properties / Action to Take, If Missed

On the tabs ***Action to take*** and ***If missed*** you can define what is to be done if none of the server users responds to the update, or if the regular update time is missed for some reason.

8. FAQ and Technical Support

Should you have any problems with your AVG, either business or technical, please refer to the FAQ section of the Grisoft website at www.grisoft.com.

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

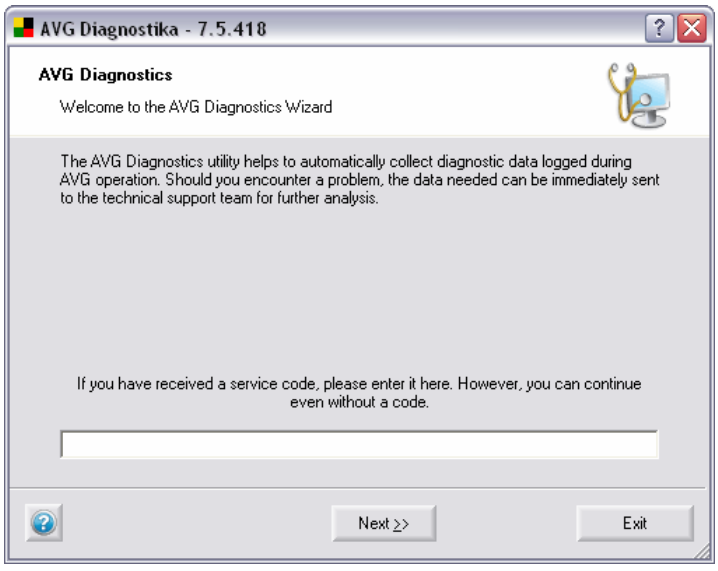
However, we recommended contacting the Grisoft technical support from the dialog window accessible from all **AVG** applications (e.g. **AVG Test Center**, **AVG Control Center** ...). To open this dialog, select ***Technical support by e-mail*** option from the ***Information*** folder of the application main menu. Then proceed to chapter 8.1 AVG Diagnostics utility for more information how to process the technical support request.

8.1. AVG Diagnostics utility

AVG Diagnostics is a supportive diagnostic utility distributed by AVG Technical Support. Its main purpose is to obtain information from the host computer. This information helps the Technical Support team to solve your problem with AVG by analyzing the collected logs, error reports, system information, suspicious files, your own comments and other data.

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

a) **AVG Diagnostics** starts with the following screen asking for a service code:



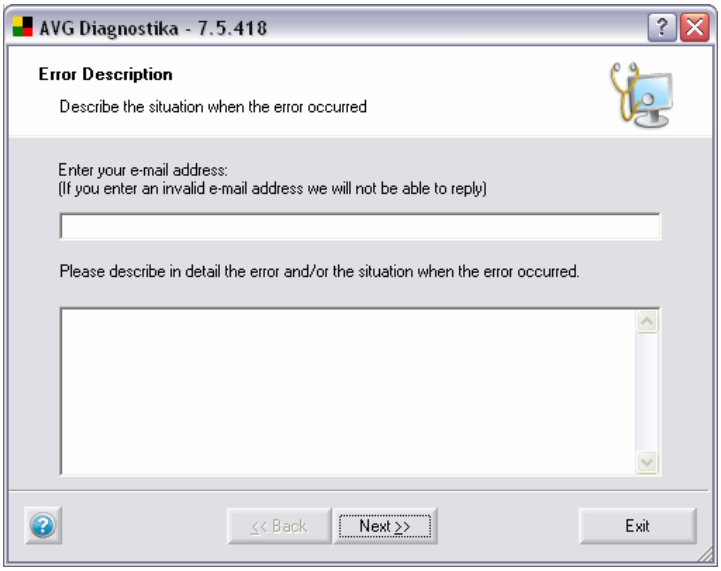
If you have received a service code, please type it into the text field, or use the copy/paste method. The code will automatically set up the correct ***AVG diagnostics mode*** which ensures that only the required (and no redundant) data is collected during the **AVG Diagnostics** session.

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

- Contact AVG Technical Support and ask for an ***AVG Diagnostics*** service code. We strongly recommend this option if you are an inexperienced user.
- Click ***Next*** and run the **AVG Diagnostics** utility in full (default) mode. In this case continue to step b - Error description.
- If you are well experienced computer user you can shut down **AVG Diagnostics** and follow instructions in step d) Advanced settings - AVG Diagnostics Modes.
-

b) Error description

This dialog allows you to add your comments and contact information to the data that will be sent to Grisoft technical support team.

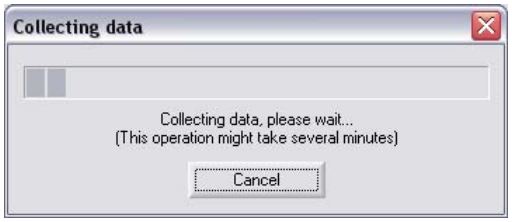


Try your best to describe in detail what the problem with your AVG installation is, and in what circumstances it occurs; you are welcome to provide any information that might help the technical support team solve the problem.

Above, you can also enter your e-mail address where the technical support team can contact you.

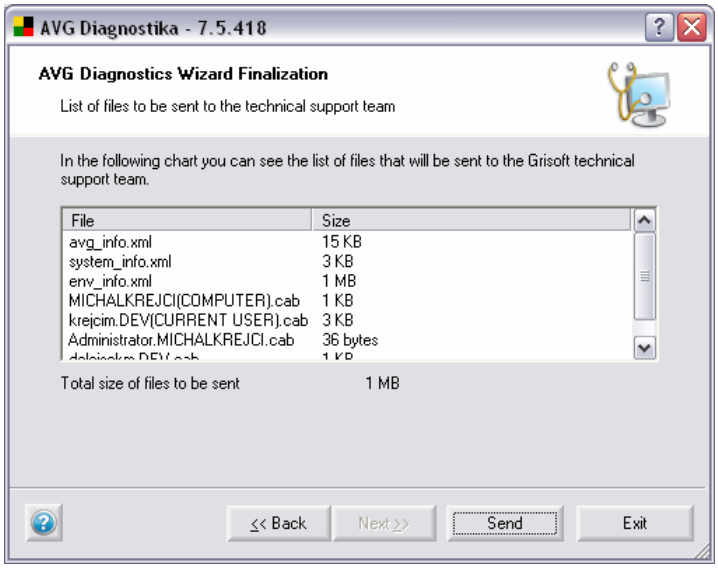
Note: *In this dialog, the Back button is disabled; if you want to enter a different AVG Diagnostics Service code, you have to shut down the current AVG Diagnostics session and run AVG Diagnostics again.*

When done with selecting, click ***Next*** button. **AVG Diagnostics** utility will start collecting data. This process may take some time to process.



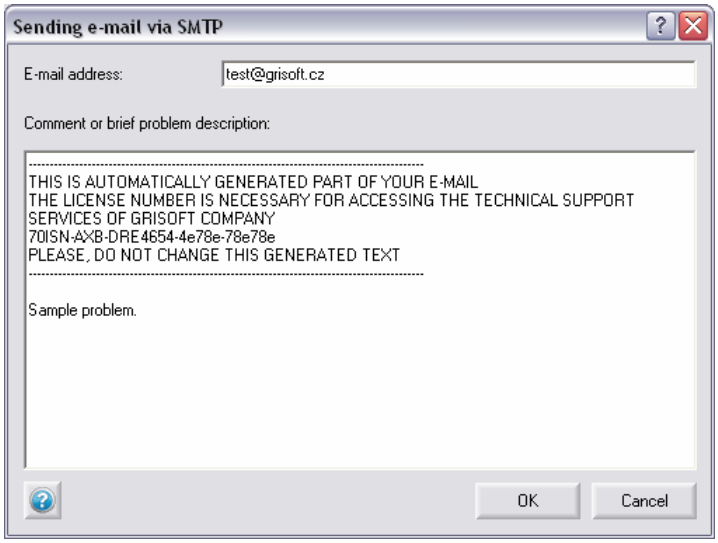
c) *AVG Diagnostics Wizard Finalization*

This dialog displays an overview of the data (file name and size) that is going to be sent to Grisoft technical support team. Below this, the total size of the data is given.



Confirm the process by clicking the ***Send*** button. A new dialog will appear with previously entered data and your license number.

Note: *If you change the automatically generated part of the e-mail body containing your license number, you might not receive an answer from the Grisoft technical support team!*



To send the data to the Grisoft technical support team, click the ***OK*** button. AVG Diagnostics will then try to automatically send the collected data.

Note: *If you are not able to dispatch the report, please make sure that your firewall is not blocking the transmission.*

d) Advanced settings - AVG diagnostics modes

Note: *Follow these instructions only if you are fully familiar with AVG Diagnostics advanced features.*

If **AVG Diagnostics** is already running, shut it down and launch it again from the command line with the respective AVG diagnostics mode parameter.

The AVG diagnostics modes serve to collect only the required and no redundant diagnostic data. Each mode affects the utility behavior so that it only performs the necessary actions, and only displays the necessary dialog boxes to the user, which also speeds up the whole process considerably.

The AVG diagnostics mode can be set:

- automatically by an ***AVG Diagnostics Service code*** (supplied by AVG Technical Support along with the **AVG Diagnostics** utility),
- by running **AVG Diagnostics** from the command line with the respective parameter.

For running **AVG Diagnostics** from a command line, see also step e) AVG Diagnostics - Complete Parameter Overview.

For parameters and more info on each individual AVG Diagnostics mode, see the respective topic:

- ***Full Diagnostics***

  This is the basic AVG Diagnostics mode.

  AVG Diagnostics in full mode creates a complete set of information about the PC: logs, system info, configuration, license, network environment, and other important information that might be useful for solving a problem with AVG.

  Parameter: /MODE=FULL, *or no parameter*

- ***Sending a suspect file for analysis***

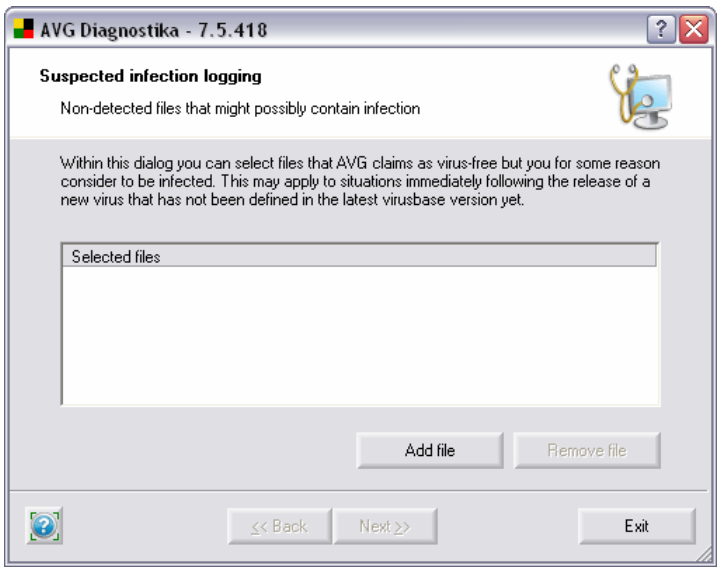
  This ***AVG Diagnostics Mode*** allows you to send a suspect file (or more files) for analysis to the Grisoft technical support team.

  A *suspect* is typically a file that is not being detected by AVG but you think, for some reason, that it could be infected, or an unwanted program.

  Parameter: /MODE=VIRUS

  To locate the suspect file directly: /FILE=<file>

The following dialog ***Suspected Infection Logging*** will appear:



This dialog allows you to add a file to the report which will be sent to Grisoft technical support team.

You can add a file that you believe is infected but has not been detected by AVG.

Click ***Add file*** to open the browse dialog and locate the file you want to attach. You can repeat this step as many times as needed.

Click ***Remove file*** to remove the highlighted file from the list.

When done, click ***Next*** button.

- ***Sending a false alarm file for analysis***

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

  A false alarm means a file that has been detected by AVG but you believe that it does not contain any viruses.

  Parameter: /MODE=FALSE

  To locate the false alarm file directly: /FILE=<file>

- ***Customer Feedback***

  This ***AVG Diagnostics Mode*** allows you to send your comments to Grisoft technical support team.

  AVG settings and system info will be attached to your message.

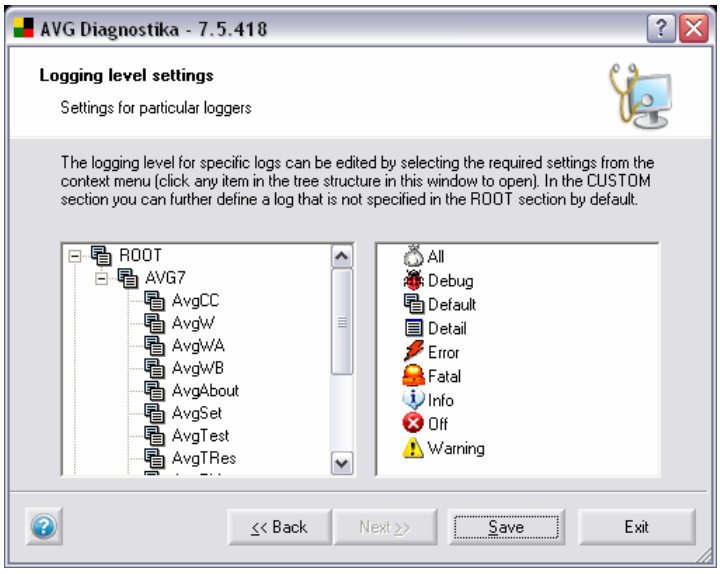
  Parameter: /MODE=FEEDBACK

- ***Log Level Setting***

Basically, this ***AVG Diagnostics Mode*** allows you to set the required logging level for the AVG software, so that only the required information is logged when working with AVG and Grisoft technical support team will be able to deal with it effectively.

Parameter: /MODE=LOGLEVEL

Recommended to experienced users only!



The left section displays an expanded logger tree. The AVG7 branch contains all default AVG loggers; the CUSTOM branch allows you to define a new logger (double-click <new item>). To specify a path for the logger, use dots, e.g. AVG7.AvgWB.MyLogger.

To remove a user-defined logger, right-click it and select ***Remove logger***.

You can set a specific logging level for any item in the tree - available logging levels are shown in the right section of the dialog. Right-click an item and select the desired logging level from the context menu. If you want to apply your selection to all subordinate loggers, select ***Apply to all*** first.

When finished, click ***Save*** button to confirm and save the settings. (The ***Next*** button is disabled in this dialog.)

Then click ***Exit*** to shut down the ***AVG Diagnostics*** application.

o ***AVG Failure Detection***

This ***AVG Diagnostics Mode*** allows you to detect and send for analysis any ERR and DMP files (only present if your AVG installation has previously broken down). Absence of these files indicates that there has been no AVG failure.

If an AVG failure is detected, a confirmation dialog with the error files overview appears and you are asked whether you wish to send them for analysis.

When running **AVG Diagnostics** in the ***Failure Detection Mode*** next time, only newly detected error files will be reported.

Parameter: /MODE=ERRDUMP

e) AVG Diagnostics - Complete Parameter Overview

In the list below you will find complete overview of all **AVG Diagnostics** parameters.

Parameter	Description
No parameter	Launches AVG Diagnostics in the full (default) mode.
/CODE=<code>	Allows you to enter the AVG Diagnostics Service code you obtained from AVG Technical Support. The code automatically sets up the required AVG Diagnostics mode.
/MODE=FULL	Launches AVG Diagnostics in the full (default) mode.
/MODE=VIRUS	Launches AVG Diagnostics in the Sending a suspect file for analysis mode.
/MODE=FALSE	Launches AVG Diagnostics in the Sending a *false alarm* file for analysis mode.
/MODE=FEEDBACK	Launches AVG Diagnostics in the Customer Feedback mode.
/MODE=LOGLEVEL	Launches AVG Diagnostics in the Log Level Setting mode.
/MODE=ERRDUMP	Launches AVG Diagnostics in the AVG Failure Detection mode.
/LOGROOT=<level>	Automatically sets up the Log Level Setting mode and allows you to directly select logging level.
/FILE=<file>	In the Sending a suspect file for analysis and Sending a "false alarm" file for analysis modes, it allows you to locate the respective file(s) directly. In the full (default) mode, it allows you to attach an additional file to the report.
/CLEARUPD	Deletes any obsolete update and temporary files.
/NOUI	Minimizes the number of displayed dialog windows.

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

Available languages and their codes:

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