AVG 7.5 Anti-Virus Network Edition (AVGADMIN 7.5)

User Manual

This product uses RSA Data Security, Inc. MD5 Message-Digest Algorithm, Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991.
This product uses code from C-SaCzech library, Copyright (c) 1996-2001 Jaromir Dolecek <dolecek@ics.muni.cz>.
This product uses compression library zlib Copyright (C) 1995-1998 Jean-loup Gailly and Mark Adler.
This product uses Embedded Firebird SQL Engine without source code modifications in accordance to license conditions InterBase Public License v. 1.0.
(http://www.borland.com/devsupport/interbase/opensource/IPL.html). Firebird SQL Engine is available on project home pages: http://www.firebirdsql.org

All other trademarks are property of their respective owners.

Contents

1. Introduction

This user manual provides comprehensive documentation for **AVG Anti-Virus Network Edition**.

1.1. AVG Network Edition Scheme

Please view the basic scheme of **AVG Network Editions** showing the connection and interaction of remote administration components:
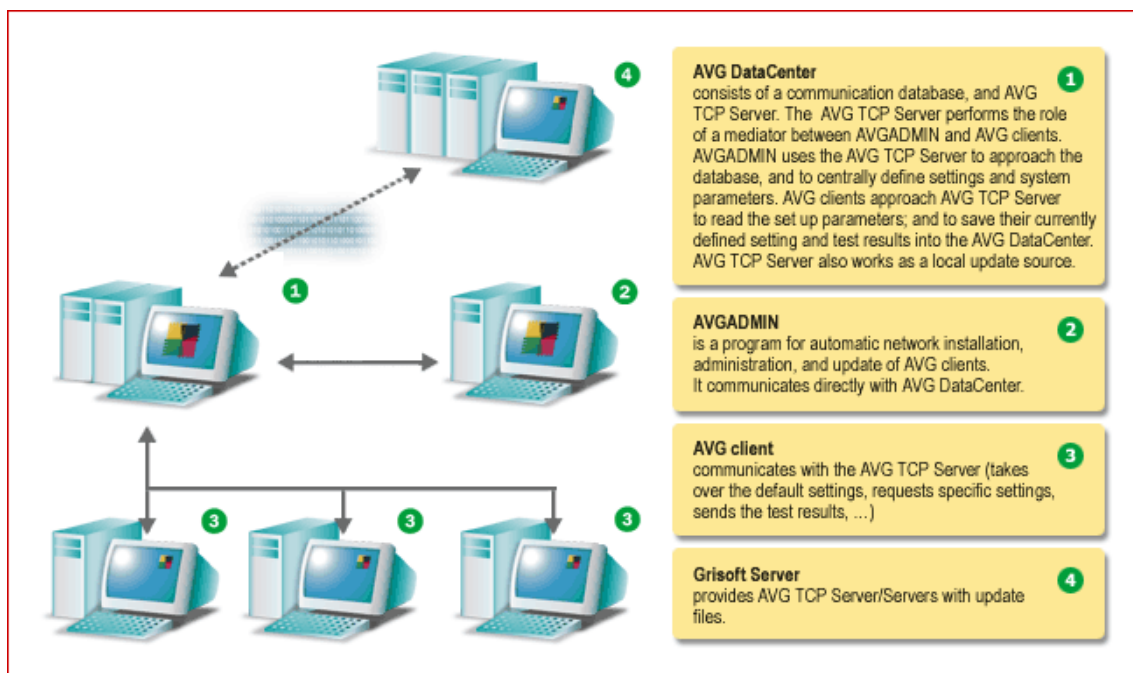
1.2. AVG Anti-Virus Network Edition Functions

AVG Anti-Virus Network Edition offers the following functions:

- **Remote installation**

  Using this function you can easily install AVG on all client workstations in the local network. This remote installation is secured by the **AVG S-Tool** – a program creating an installation script that makes it possible to run the **Setup** installation program on all remote network workstations.

- **Centrally controlled updates**

  All AVG clients in the network can be updated centrally using the **AVGINET Lite** program. This program runs the updates scheduled within the **AVG Scheduler** component.

- **Secured communication**

  Network communication between **AVGADMIN** (**AVG TCP Server**) and workstations is completely encrypted, if both client and server are updated to the current version.

AVG 7.5

AVG Anti-Virus Network

- **_Full remote administration in the network_**

    The full functionality of the **AVG Anti-Virus Network Edition** guarantees:

    o   Automated remote **AVG** installation on all network workstations

    o   Continuous overview of all network **AVG** clients' current status

    o   Central control and administration of **AVG** clients' configuration

    AVG Anti-Virus Network Edition full functionality is provided by the **AVGADMIN** program, and the **AVG DataCenter**.

    (This option is available only for AVG Network Edition users.)

    If you do not need the **AVG Anti-Virus Network Edition** advanced functionality, it is recommended that you install the **AVG S-Tool** only (for installation scripts generation, and remote installation). Neither the **AVGADMIN** nor the **AVG DataCenter** are necessary for automatic installation and/or centrally controlled update.

- In addition to all standard features, **AVG Anti-Virus Network Edition** contains the following component support:

    o   **Firewall** protection and ability to set configuration directly from AVGADMIN

    Please note: AVG Anti-Virus Network Edition _does not support Anti-Malware and Anti-Spam components. All settings dialogs will be available from AVGADMIN, but no Anti-Spam or Anti-Spyware configuration will be synchronized._

1.3. AVG Anti-Virus Network Edition Functions Selection

If you have gone through this documentation and you are still not sure about what level or type of **AVG Anti-Virus Network Edition** functions are best for you, we recommend that you consult the Grisoft technical support department: technicalsupport@grisoft.com.

To help us find the best solution for AVG implementation on your network, please prepare the following information:

- the size of your network (the file server type, number of network workstations)

- operating systems on the client workstations in the network

- average HW parameters of the client workstation (or rather the minimum parameters)

- LAN or WAN, and the connection quality for WAN

- your demands for **AVG Anti-Virus Network Edition** (administrator's requirements, and administration extent)

AVG 7.5

AVG Anti-Virus Network

2. Terminology Definition

Within this User Manual you will find certain terms relating to **AVG Anti-Virus Network Edition** components. Here is an overview of these terms together with brief definitions.

The **AVG Anti-Virus Network Edition** components are then described in detail in the respective chapters of this User Manual.

2.1. AVG DataCenter

The AVG DataCenter is a database that contains the entire configuration for AVG clients, including tests and tasks settings. All client workstations with **AVG** installed, as well as the AVGADMIN program, communicate with the **AVG DataCenter**. Of course communication is possible only if the **AVG Anti-Virus Network Edition** component is properly installed on all workstations connected to the AVG DataCenter.

2.2. AVG TCP Server

The AVG TCP Server enables the **AVG DataCenter** to run: it includes its own SQL database engine. However other standalone SQL database servers can be used, too. Currently, the **AVG TCP Server** can also use the Firebird SQL Server and the Microsoft SQL Server (including the MS SQL Server 2005 Express Edition, formerly known as MS SQL Desktop Engine).

Note: Only the Firebird SQL Server Embedded is part of the AVG Anti-Virus Network Edition installation package. If you want to use the MS SQL Server it needs to be already installed.

AVG TCP Server performs the role of a communication mediator between **AVGADMIN** and AVG clients. **AVGADMIN** uses **AVG TCP Server** to access the **AVG DataCenter**, and to centrally define settings and system parameters. Through **AVG TCP Server** all AVG clients access the **AVG DataCenter** for the preset configuration parameters, and to save their currently defined settings and test results into the **AVG DataCenter**. **AVG TCP Server** also works as a local update source.

AVG clients attached to the **AVG TCP Server** use the standard HTTP communication via the TCP protocol. AVG clients need no extra component or special configuration for communication with the **AVG TCP Server**. AVG clients can even connect to the AVG DataCenter through the proxy server within the WAN.

By default, the **AVG TCP Server** is installed in this directory:

C:\Program Files\Grisoft\AVG TCP Server

Note: Besides using the AVG TCP Server, AVG DataCenter functionality can be supported by other database servers as well. Nowadays you can use the Firebird SQL Server (using the native libraries), or the MS SQL Server (using ODBC).

Should you decide to use one of the above mentioned network administration options, it is crucial that all client workstations have the proper drivers installed. If you decide not to use the AVG TCP Server, it is necessary to create a local web

server for upgrade files mirroring; this server will be used for the network clients scheduled update.

The SQL installation scripts for creating all needed AVG DataCenter tables and data are available for all supported SQL servers.

2.3. AVG TCP Monitor

The AVG TCP Monitor tool is used to control and configure the **AVG TCP Server**. The **TCP Server Monitor** is part of the **AVG TCP Server** installation.

2.4. AVGADMIN

AVGADMIN is a program for automatic network installation, administration, and updating AVG client installations within the network. It communicates directly with the **AVG DataCenter** and controls, processes, and displays separate events. It is regarded as an "administrative console" of the **AVG DataCenter**.

AVGADMIN *can be run in two modes:*

- AVGADMIN Basic interface
- AVGADMIN Advanced interface

The AVGADMIN is installed by default into this directory:

C:\Program Files\Grisoft\AVGADMIN

2.5. AVG S-Tool

AVG S-Tool program helps you create installation scripts and remotely install AVG on target network workstations.

The installation script is a file containing the definition of AVG client installation parameters. The installation script can include license information, component selection, hidden (automatic) installation parameters, etc. Once the installation script is created, you can use the **AVG S-Tool** to schedule the installation's remote launch on the selected network workstations, or you can save the script for later use (e.g. in the login script). Also, **AVG S-Tool** directly supports the generating of scripts and files needed for the creation of an installation CD with preset installation parameters.

The **AVG S-Tool** program can be used to run the remote AVG installation on Windows NT4/2000/2003/XP Professional operating systems. Also, it works as a generator of installation scripts for the automatic installation in the environment of Windows 95/98/Me/XP Home operating systems.

AVG S-Tool *can be run in two modes:*

- AVG S-Tool Basic mode
- AVG S-Tool Advanced mode

By default, the program is installed in this directory:

C:\Program Files\Grisoft\AVGADMIN7

AVG 7.5

2.6. AVGINET Lite

AVGINET Lite is an application that is able to

- recognize the presence of new update files on the internet, and download them

- perform the complete update server structure mirroring for central AVG clients update

- perform AVG update on client workstations

The application can run separately, or using the installed AVG client configuration.

By default, **AVGINET Lite** is installed in this directory:

C:\Program Files\Grisoft\AVG TCP Server

2.7. AVG Client

The term AVG client is used when speaking about a single AVG installation on a workstation within the network. Via **AVG TCP Server**, the AVG client communicates with the **AVG DataCenter**, and takes over the default settings, raises demands for specific settings, sends the test results back to the **AVG DataCenter**, etc.

GRISOFT

AVG 7.5

AVG Anti-Virus Network

3. AVG Anti-Virus Network Edition Installation

3.1. AVG Anti-Virus Network Edition Installation Steps

AVG Anti-Virus Network Edition installation and configuration is divided into these steps:

- **AVG TCP Server** installation

- **AVGADMIN** installation

- **AVGADMIN** connection to the **AVG DataCenter**

It is strongly recommended that you go through the whole documentation first to get a general overview of **AVG Anti-Virus Network Edition** possibilities so that you can set the configuration that best suits your needs.

3.2. AVG Anti-Virus Network Edition Installation Process

AVG Anti-Virus Network Edition can be launched using the exe file within the **AVGADMIN** directory on the installation CD. The latest installation package can always be downloaded from the Grisoft website at www.grisoft.com, in the downloads section.

Before installing AVGADMIN visit the Grisoft website and check for the latest installation file.

Warning: Installation of AVGADMIN to Windows 95 is not supported! Installation of AVGADMIN to Windows NT operating system requires internet Explorer 5.01 or higher to be installed!

On your PC/server create a new directory (e.g. AVGINST), and copy the **AVGADMIN** installation file into it. This directory can then be used for installation of other parts of the network administration. Switch to the directory where your **AVGADMIN** installation file is located, and launch the installation:

a)   Setup language selection

The welcome dialog appears in the language of the operating system to which **AVGADMIN** is being installed. You can switch to another language and confirm your choice by pressing the *Next* button.

b)   License agreement

The new dialog window offers the full wording of the **AVG Anti-Virus Network Edition** license agreement. To approve, press the *Accept* button. Otherwise press the *Don't accept* button, and the installation process will be cancelled.
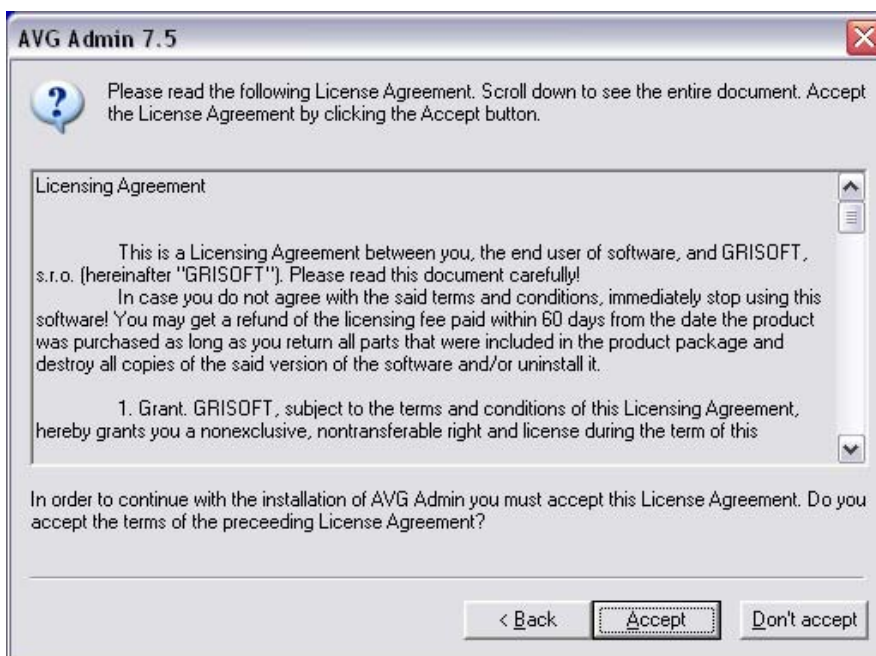
c)   Destination folder

You have to specify the destination folder where **AVGADMIN** (and its components) will be installed. If you want to select another directory, specify the directory path or choose a directory from your local disc by pressing the *Browse* button. To continue the installation press the *Next* button.

AVG 7.5

AVG Anti-Virus Network

d) *Directory confirmation*

If you specified a directory different from the default one, and the specified directory does not exist, a new dialog will pop up asking you whether you want to create the directory. To confirm creating the directory, press the **Yes** button.
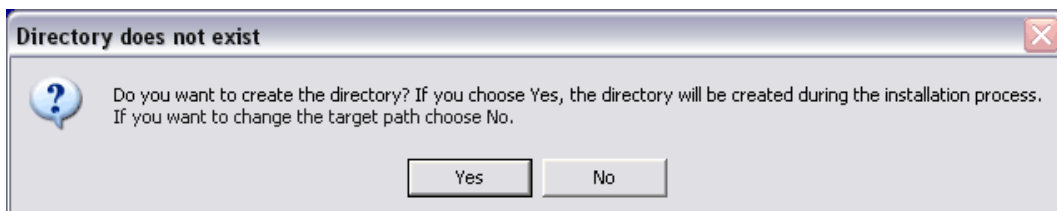
e) *Component selection*

The new dialog window asks you to select those **AVG Anti-Virus Network Edition** components you want to install. Also, you need to specify the type of network communication. By default, the **AVG TCP Server** arrangement is preset. If you decide on another arrangement, mark the respective checkbox. To continue the installation process, press the **Next** button:
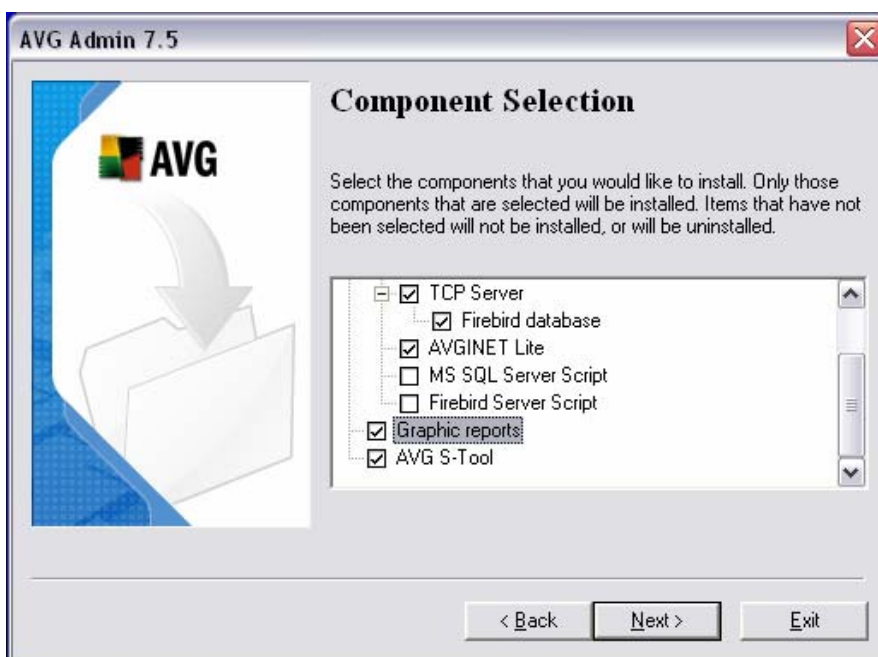
Note: If you want to generate Graphic reports, install the component on the same computer, as AVG TCP Server. Generated reports can be viewed also on stations with only AVGADMIN, but cannot be generated there. The Graphic reports feature is available for Windows NT based systems only (Windows 2000/XP/2003 and compatible).

f) *Installation summary*

This dialog presents a list of all selected parameters. To continue the installation, press the **Finish** button.
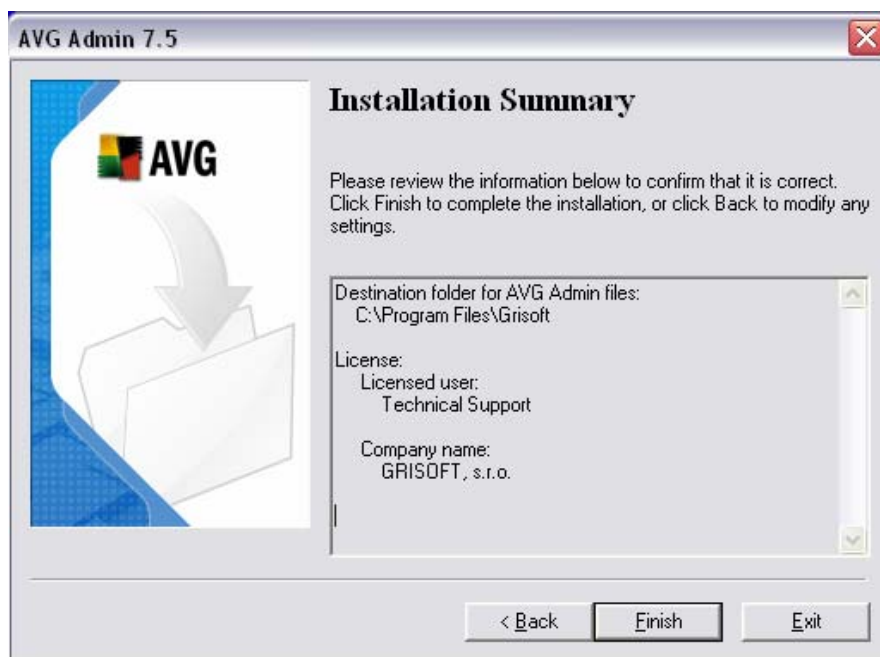
g) Installation complete

The *Installation complete* dialog appears to confirm that **AVGADMIN** and all its components were installed successfully. Press the *OK* button to finalize the installation.

If an error occurred during the installation process, or the installation failed, an error announcement appears. In that case switch to your TEMP directory with the *avg7adm.log* file, and send the file to our technical support department for further analysis. Use the contact e-mail: technicalsupport@grisoft.com

4. AVG Installation on Client Workstations

4.1. Installation Options

For individual stations in your network, that use a personal firewall, you will probably need to allow certain ports and set specific system features in order to be able to correctly use AVG remote installation.

Depending on the firewall type and settings on each station, some of the below mentioned requirements may be already predefined or allowed, or its settings may not be available under the same name and description. We strongly recommend that all changes should be done by well experienced users only! Always consult the User manual or Help guide for your firewall before proceeding to change any settings.

a)   *Ping (ICMP type 0 - Incoming echo request)*

Change this setting only if **AVGADMIN** is not able to detect station(s) in your network, which you are sure are switched ON and fully operational.

In the firewall settings used on the target station allow the incoming **ping** requests within the local network. Often this function can be found under **ICMP type 0** or **Incoming echo request** or similar description. If set correctly, AVGADMIN will be able to find the station in the network.

b)   *File and Printer Sharing for Microsoft Networks*

To allow **AVGADMIN** access to a remote computer over the *Admin$* share, you first need to allow **File and Printer Sharing for Microsoft Network** on the target station. Specifically you must allow TCP ports 139 and 445 and UDP ports 137, 138 and 445. This way **AVGADMIN** can copy the **AvgAgent** to the target computer.

As a first step you should check, whether the **File and Printer Sharing for Microsoft Networks** function is installed on the target computer or not. If you are using Windows 2000 or XP, you can find the settings under **Start/Settings/Network connections. In the properties** window of the Network connections, tick the **File and Printer Sharing for Microsoft Networks**. In case you cannot see such an item, then it is probably not installed yet. In this case, please contact your station administrator or install the component yourself from the installation CD.

If the **File and Printer Sharing for Microsoft Networks** feature is successfully installed, you need to allow the ports mentioned above in the firewall installed on the target station. If for example the built-in Windows XP firewall is used, you can easily allow this feature by clicking the **File and Printer Sharing** item located in the **Exceptions tab**.

c)   *RPC: Remote Procedure Call*

To be able to launch the **AvgAgent** service on the target PC, you need to allow the following ports in the firewall on the station – TCP and UDP port 135.

d) **Communication on TCP port number 6150**

For correct communication between the **AVG S-tool** and the **AvgAgent** component you need to first allow communication on TCP port 6150. Using this port **AVG S-Tool** controls the **AvgAgent** tool and passes it the AVG installation files.

e) **Communication on TCP port number 80 (AVGINET and AVGINET Lite)**

For correct communication between the **AVGINET** (**AVGINET Lite**) and the update servers it is necessary to permit outgoing communication for these components on TCP port 80.

Note: *If you experience any problems with the remote administration/installation, please try to find the proper answer in the FAQ (Frequently Asked Questions) located on Grisoft website at www.grisoft.com.*

AVG Anti-Virus Network can be remotely installed on workstations/servers in several ways (see below), but for most users, we recommend using the AVG DataCenter Setup Wizard for the first time installation.

a) **Direct installation**

Directly, you can install AVG manually on every single workstation/server in the network, and then connect them manually to the **AVG Anti-Virus Network Edition**. This option can be used for *all Windows platforms*.

For a detailed description of AVG installation please refer to the AVG 7.5 Anti-Virus User Manual; for download in the downloads section of the Grisoft website www.grisoft.com.

b) **Remote installation with AVG S-Tool for Windows NT4 and higher**

In the **Windows NT4/2000/2003/XP Professional** operating systems environment mass AVG installation to all network workstations can be performed using the **AVG S-Tool**.

o   Select a workstation in the network and install AVG on it.

o   Define AVG configuration as an example configuration for all other stations in the network.

o   On the same workstation then install **AVG S-Tool.**

o   Based on the configuration of **AVG Anti-Virus Network** installed on the station, **AVG S-Tool** will create a template configuration, and send it to all other network workstations together with the **AvgAgent** program that secures the AVG installation on a single workstation.

o   **AvgAgent** then installs **AVG Anti-Virus Network** with the pre-defined configuration on every network workstation.

Within the Windows NT4/2000/2003/XP Professional operating systems environment the administrator/domain administrator rights are necessary for central AVG installation.

AVG 7.5

AVG Anti-Virus Network

c) Remote installation with AVG S-Tool for Windows 95/98/Me/XP Home

In the **Windows 95/98/Me/XP Home** operating systems environment mass AVG installation to all network workstations can be performed using the **AvgAgent** program that secures running AVG installation on a single workstation.

o Locate the **AvgAgent** executable file on the server.

o Install **AvgAgent** on the Windows 95/98/ME/XP Home workstation.

o Run **AVG S-Tool** on the server and install AVG to the Windows 95/98/ME and Win XP Home workstation where the **AvgAgent** is installed.

See the chapter <u>5.5 AVG Installation on Windows 95/98/ME and Win XP Home</u> for further details.

4.2. Installation Script

The installation script is used to create a configuration template with the example AVG user configuration. The installation script takes over the **AVG Anti-Virus Network** configuration defined on the workstation, where the script is being created. The configuration is then packed and becomes part of the package for automatic installation on other network workstations.

You can influence the installation progress by pre-setting the **SETUP.EXE** command-line parameters. This way you can call the installation process with the preset license number, the specified components to be installed, etc.

a) Installation Parameters

The following table presents a full list of installation parameters. However, we recommend using them only if you have an actual reason to do so! Otherwise, we encourage you to use the <u>AVG S-Tool</u> to create an installation script instead!

Setup installation program parameters can begin with the '/' (slash) character. Some of them are correct only with a value specified; some of them can be specified with no value present. The space character serves as a division between both parameters and values. If the space character is in a value, it has to be enclosed in quotes.

Examples:

SETUP /TARGET_DIR "C:\Program Files\Grisoft\Avg7"

SETUP /QUIT_IF_INSTALLED /COMPANY "Acme Ltd." /HIDE

The following table presents a list of available **Setup** parameters with short descriptions:

Parameter and value name	Meaning
REPAIR	Repair existing installation

Parameter and value name	Meaning
UNINSTALL	Uninstall the program
HIDE	Hidden installation. After entering all the necessary parameters, the installation continues hidden without user intervention.
LOG *path*	The installation log filename and path
SCRIPT_FILE *path*	Loading of parameters from script specified in the path
LICNO *license-number*	Installation license number
LICENSE_DLG	A dialog opens, where license information can be filled in
NAME *name*	User's name
COMPANY *name*	Company's name
LICENSE *user company number*	License information – all three parameters must be specified
MACHINE *name*	Name of AVG installation target computer. Activates remote installation process.
MACHINE_LIST *path*	Path to a file with list of target computers of AVG system installation. There is a single station name on each line of such a file. Activates remote installation process.
RESTART_IF_NEEDED	Reboot will be initiated on a target computer (if needed after the installation has been completed).
USER_ENUM_MODE *mode* ALL CURRENT_ONLY NONE	User enumeration modes. Available values for *mode*: installation is performed for all users (default) installation is performed for user, who is currently logged in no installation of user defined data is performed

Parameter and value name	Meaning
IGNORE_USER *user*	*user* is defined by SID or full name specification *user* is ignored; no installation is performed for him/her. Parameter can be used more times for each single user. It is significant only when USER_ENUM_MODE == ALL

LOG_MODE *mode*
 	
    APPEND
 	
    REWRITE
	Log file records mode. Allowed *mode* values:
	
	appending at the end of the file (default mode)
	
	rewriting the file records

QUIT_IF_INSTALLED	If there is AVG already installed on the target machine, the installation is discarded.
DONT_START_APPS	Suppresses the launching of AVG processes (Control Center, Alert Manager and so on) after a successful installation. When not using this parameter, the processes are launched by default.
NO_WELCOME	After a successful installation and possible reboot there displaying of the welcome dialog and First Run Wizard will be suppressed.
REMOTE_SETUP_PACKAGE *UNC_path*	UNC path to the installation package for remote installation. This path is used by target computer during the installation process.
REMOTE_INSTALL_TYPE {NOW | ON_RESTART}	Remote installation type. The installation can be launched immediately (*NOW*) or after next reboot of target computer (*ON_RESTART*).
REMOTE_LOGIN_AS *account password*	Account and corresponding password to be used by Setup for logging in the remote installation target computer.
LANGID *language_id*	Identification of language to be used for communication with user. Operating system value is used by default. Language ID is the operating system's internal number (e. g. 0x405 for Czech language)

Parameter and value name	Meaning
ADD_FEATURE *component*	Specification of a component to be installed.
REMOVE_FEATURE *component*	Specification of a component not to be installed.
TARGET_DIR *path*	Path to the target installation directory.
DCPATH *path*	AVG DataCenter specification – DSN name of data resource.
NO_CC_STARTUP	Suppresses the registration of AVG Control Center for launching after Windows startup.
NO_AVGW_STARTUP	Suppresses the registration of AVG Test Center for one-shot launching after Windows startup.

You can enter more components by repeating the ADD_FEATURE parameter, as well as for the components not to be installed. If a component is mentioned more than once in a given list, the sequence is also important. Component names and their descriptions are given in the following table:

Component name	Meaning
fea_AVGWin	All of the AVG components. Declaring this component will result in default AVG installation. Particular component selection can be managed using additional REMOVE_FEATURE and ADD_FEATURE parameters.
fea_AVG_ResidentShield	Resident Shield component
fea_AVG_CI	Remote administration installation (only for network edition, not selected by default)
fea_AVG_Bootup	Boot-Up Scanner installation (only for Win9x)
fea_AVG_EmailPlugins	E-mail Scanning installation. Selecting the component will make all of the following components selected by default. You can choose any of the components not to be installed by mentioning it in the REMOVE_FEATURE parameter.
fea_AVG_Office_2000_plugin	MS Office 2000 plugin installation (only when the package is installed)
fea_AVG_Bat_plugin	Plugin for TheBAT! E-mail client

fea_AVG_Exchange_plugin	Plugin for MS Office Outlook.
fea_AVG_Eudora_plugin	Plugin for Eudora e-mail client
fea_AVG_EMC	EMS component for general e-mail clients that use POP3/SMTP protocols for receiving and sending mail.

b)   Example of setup launch

AVG Anti-Virus Network hidden installation will be performed if the application has not been installed on a computer before. User name and license number are entered. All AVG components will be installed, including the **AVG Anti-Virus Network Edition** support but not The Bat! and MS Office 2000 plugins:

SETUP /HIDE /LICNO 70-123-456-ABCD-EFGH /NAME "Josef Novak"

/QUIT_IF_INSTALLED /ADD_FEATURE fea_AVGWin
/ADD_FEATURE fea_AVG_CI
/REMOVE_FEATURE fea_AVG_Bat_plugin
/REMOVE_FEATURE fea_AVG_Office_2000_plugin

AVG hidden installation will be performed if the application has not been installed on a computer before. User name and license number are entered. **AVG Anti-Virus Network Edition** support will be installed. EMS module (but no specific e-mail client plugins) will be installed.

SETUP /HIDE /LICNO 70-123-456-ABCD-EFGH /NAME "Josef Novak"

/QUIT_IF_INSTALLED /ADD_FEATURE fea_AVGWin
/ADD_FEATURE fea_AVG_CI
/REMOVE_FEATURE fea_AVG_EmailPlugins
/ADD_FEATURE fea_AVG_EMC

4.3. Installation File Download

AVG installation files are available for download at the Grisoft website at www.grisoft.com, in the downloads section.

For electronic distribution, some installation files (typically for example additional components for remote administration) are packed into an archive that has to be unpacked before starting the installation process. To do so, you can use the WinRAR program, or any other compression program supporting the RAR format. A free version of the WinRAR compression tool is available for download at www.rarlab.com or in the **Bonus** section of your installation CD.

On the distribution CD you will find the installation files already unpacked in the respective directories.

5. AVG S-Tool

Within the **Windows NT4/2000/2003/XP Professional** operating systems environment, the **AVG S-Tool** program helps you create the installation scripts for mass AVG installation, and for remote AVG installation itself. In the environment of **Windows 95/98/Me/XP Home** operating systems the **AVG S-Tool** can also be used for installation script creation.

5.1. AVG S-Tool Launch

The **AVG S-Tool** program can be started in two ways:

● From the Start menu: **Start/Programs/AVGADMIN 7.5**; or using the prompt from the directory where **AVGADMIN** has been installed

● From the **AVGADMIN** environment select the **Service/Install AVG 7 onto stations or Service/Install AVG 7 onto stations (advanced mode)** menu item.

AVG S-Tool can be run either in the **Basic** or **Advanced** mode. You can select the **Advanced mode** by selecting the option **Advanced mode** in the **Setup mode selection** dialog window. If the option is not selected, the program will run in the **Basic mode** (recommended for most users).

5.2. AVG S-Tool Basic Mode

AVG S-Tool Basic mode is intended for users who prefer the easiest way of configuration and installation. The installation will include **AVG Anti-Virus Network** information and parameters needed for proper and comprehensive AVG functionality.

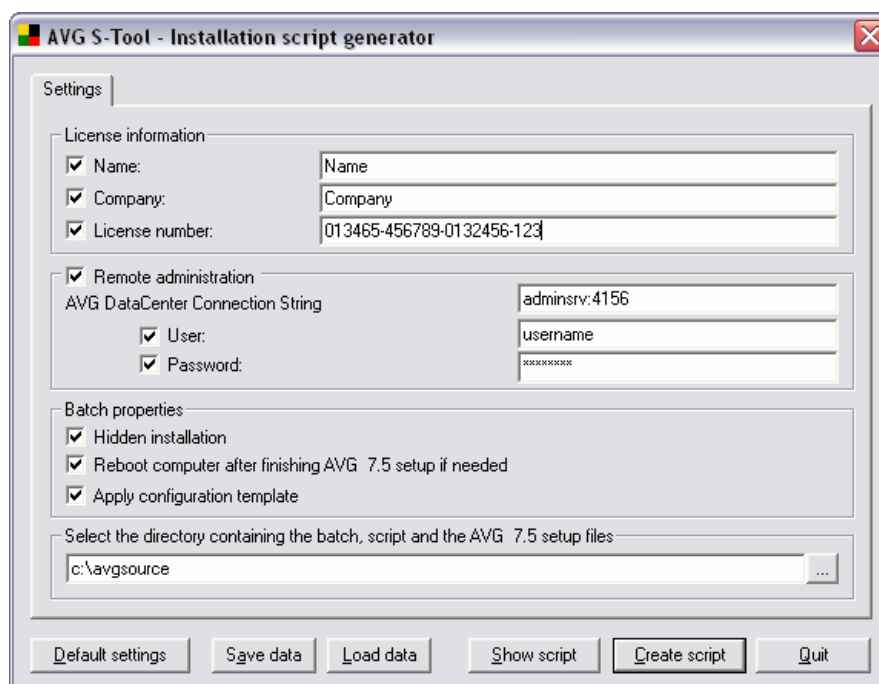To launch the **AVG S-Tool Basic Mode** leave the option **Advanced mode** unselected:
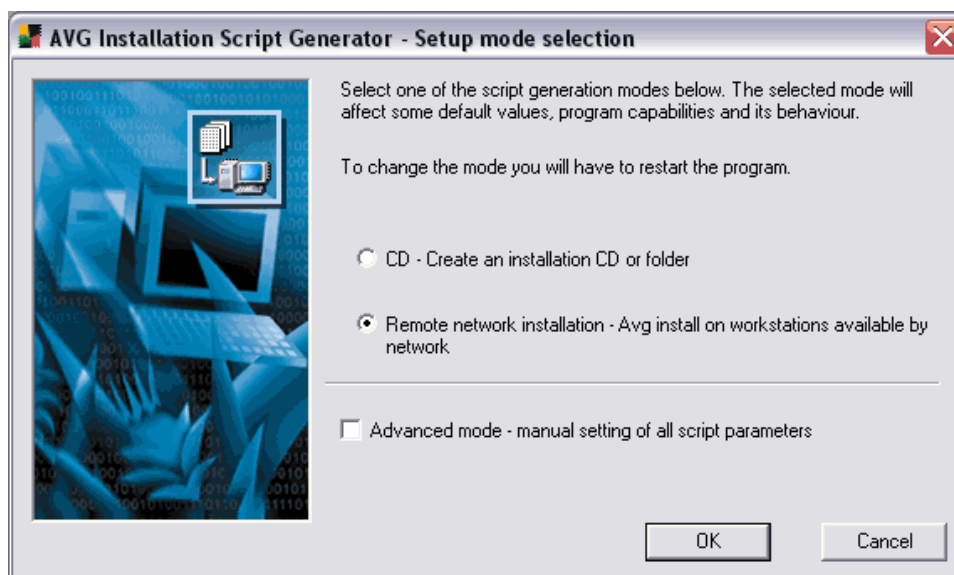
The dialog window offers a selection between two options of creating and use of the installation script:

- **CD or installation script**

- **Remote network installation**

a) **CD or installation script**

Selecting the **CD or installation script** option, **AVG S-Tool** will create an installation script for running the installation into a selected directory. The content of the directory can be then copied to a CD used as an installation CD; or you can use the created files for remote installation.

The selected option does not offer the possibility of remote installation to the network workstations or servers.

In the option CD or installation script dialog window you can define only the basic installation parameters:

o **License information –** type in the license data such as Name, Company, and License number. If you wish to take the Windows username for the **Name** field, do not select the respective check box, and leave the default system settings to be used.

o **Remote administration** – define the **AVG DataCenter** connection string and **username/password**, if applicable *(see chapter 6.7 – Clients Connection to AVG TCP Server when having troubles).*

If you do not want to use the remote administration options and you do not plan to install the **AVG DataCenter** and **AVGADMIN**, leave the respective check box unselected.

o **Batch properties** – offers the selection of Hidden installation/Apply configuration template. Further, you can specify whether the workstation

should reboot after AVG installation is finished (this option is not selected, by default).

o **Select the directory containing the batch, script, and the AVG 7.5 setup files**– Specify the path to the directory where the installation script, the batch and the AVG installation files are located. You can either type in the path manually, or press the button to open a new window; then select the directory from the navigation tree of your local disc.

This dialog provides the following control buttons:

o **Default settings** – returns the dialog parameters to the default settings

o **Save data** – saves the script template in the .stf format to the selected place

o **Load data** – allows you to read data from a previously saved script template

o **Show script** – the installation script content will be displayed in a new window

o **Create script** – compiles and saves the installation script to the selected place

o **Quit** – closes the AVG S-Tool application

b)   Remote network installation

When selecting the **Remote network installation** option, **AVG S-Tool** creates an installation script and performs AVG installation on all accessible local network workstations. This option is available within the **Windows NT4/2000/2003/XP Professional (and higher)** operating systems environment.

Before you run the AVG remote installation using **AVG S-Tool Basic mode**, it is recommended that you set up the full AVG configuration on the workstation from where the **AVG S-Tool** runs (from where the installation will be launched). This configuration will be taken as an example configuration template for all network stations.

Note: The network remote administration can also be launched from the AVGADMIN environment using the menu item Service/Install AVG 7 onto stations (in both the Basic/Advanced modes).
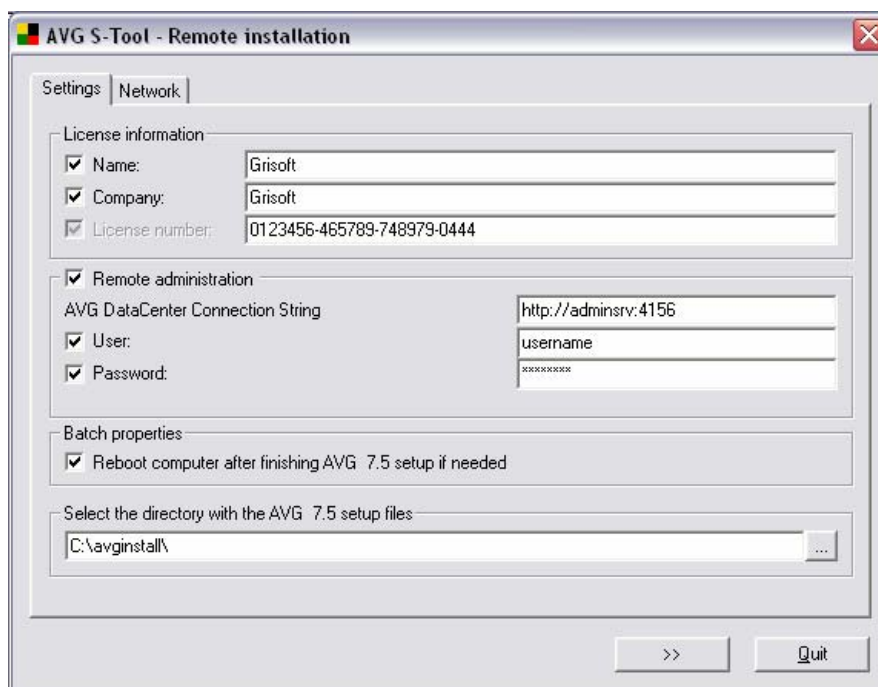
There are the following two tabs within the **Remote network installation** dialog:

o   **Settings Tab**

On the **Settings** tab it is possible to define these installation parameters:

– **License information –** type in the license data such as Name, Company, and License number. If you wish to take the Windows username for the **Name** field, do not select the respective check box, and leave the default system settings to be used.

– **Remote administration** – define the **AVG DataCenter** connection string and **username/password**, if applicable *(see chapter 6.7 – Clients Connection to AVG TCP Server when having troubles).*

If you do not want to use the remote administration options and you do not plan to install the **AVG DataCenter** and **AVGADMIN**, leave the respective check box unselected.

– **Batch properties** –you can specify whether the workstation should reboot after the AVG installation is finished (this option is not selected, by default).

– **Select the directory containing the batch, script, and the AVG 7.5 setup files**– Specify the path to the directory where the installation script, the batch and the AVG installation files are located.

You can either type in the path manually, or press the ⬚ button to open a new window; then select the directory from the navigation tree of your local disc.

AVG 7.5

AVG Anti-Virus Network

The **Settings** tab provides the following control buttons:

- **>>** – switches to the following **Network** tab

- **Quit** – closes the AVG S-Tool application

o **Network tab**

The **Network** tab offers the option of searching the local network for AVG installations on workstations. If there are workstations without AVG installed, the **AVG S-Tool** will install AVG on them. All operations are performed remotely via network communication and using the **AvgAgent** service that is installed automatically on every single network station.

Warning: AVG remote installation can be performed only on stations with the OS Windows NT4/2000/2003/XP Professional installed. Also, you have to be logged in as an administrator. On workstations running the OS Windows 95/98/Me/XP Home the AVG installation must be done manually, or using the login script and the AvgAgent service (for details please refer to chapter 4. AVG Anti-Virus Network Installation on Client Workstations).

On the station where you launch AVG installation from, as well as on all workstations to which you want to install AVG, the option of Microsoft Network Files and Printers Sharing must be enabled. You can enable this option in the Network Connection properties control panel. If the sharing option is disabled, you have to install the AvgAgent manually even on stations running the OS Windows NT4/2000/2003/XP Professional, or you can use the login script.

AVG 7.5
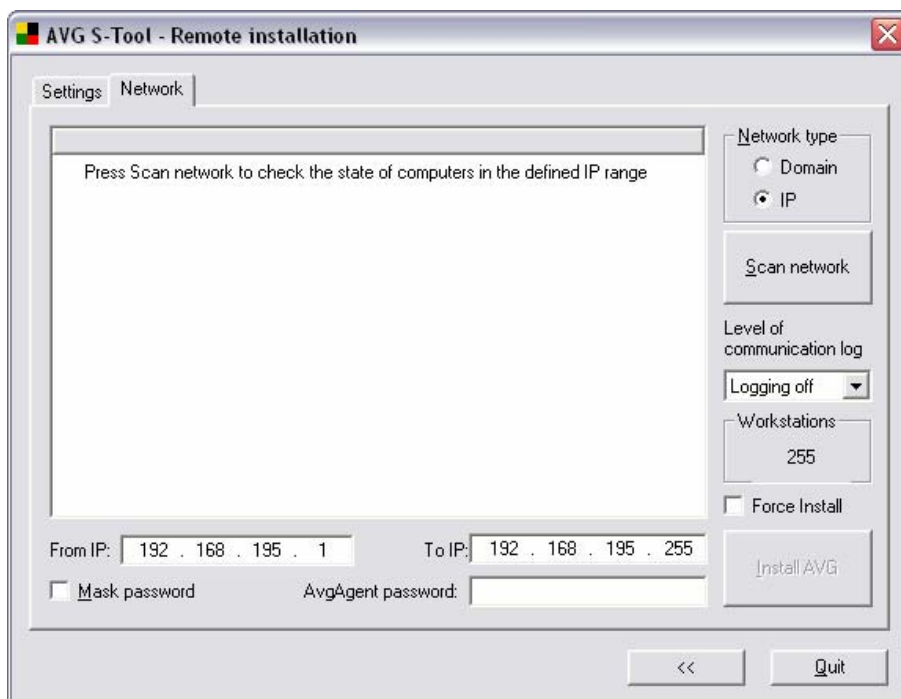
On the **Network** tab you will find the following options:

o **Network type** – **AVG S-Tool** searches for AVG on network stations either in the range of a domain from which the installation is launched (i.e. where the station with **AVG S-Tool** installed is located), or within the range defined by the IP addresses.

o **Level of communication log** - select the preferred level of communication logging.

  – **Logging off** (no logging)

  – **Errors only** (only errors will be logged)

  – **Detailed** (more detailed logs)

  – **Debug** (debug information will be logged)

o **Workstations –** The option displays the current number of stations on which the desired operations should be performed.

o **Force install** – The option specifies that the **AvgAgent** service together with AVG should be installed even on stations where AVG is already installed. This function allows you to perform AVG reinstallation on all network workstations.

o **From IP, to IP** – If you selected the option of searching the network in the range defined by IP addresses, you need to specify the range by entering the IP addresses here.

  Note: When launched for the first time, AVG S-Tool will try to fill in the IP addresses according the network configuration set on the station where the AVG S-Tool application is running. However, if you know the exact IP address range of network stations, adjust the values manually to shorten the time needed for searching the network.

o **Mask password** – Selecting this option will prevent the password from being displayed on your computer's monitor.

o **AvgAgent password** – Enter the password that will protect communication between **AVG S-Tool** and the **AvgAgent** service on remote workstations. Then no operations using the **AVG S-Tool** can be performed on the remote workstations without knowing the password. The password is related to the **AvgAgent** service only, and it does not influence any other remote station settings. This password must be specified BEFORE you launch **AvgAgent** installation on remote workstations!

To change the AvgAgent password, follow these steps:

o Type the new password into the **AvgAgent password** field

o Select the **Force install** option!

o Run AVG remote installation

o A dialog asking for the **AvgAgent** password will be displayed – enter the original password into this dialog!

o After installation, the **AvgAgent** on the station uses the new password already

The *Network* tab control buttons are:

o **Scan network –** After pressing this button, **AVG S-Tool** will start inspecting individual workstations for the **AvgAgent** service and AVG presence. The search results are then displayed using the following icons:

Station found (the station is registered in the domain); the station status has not been inspected yet

Neither **AvgAgent** nor AVG itself are installed on the workstation

AvgAgent is installed on the workstation; AVG itself is not installed

Both **AvgAgent** and AVG itself are installed on the workstation

An error occurred while communicating with the station. Double click to show detailed information. Typically, an error occurs if communication with **AvgAgent** is blocked (e.g. by a firewall), or your password is invalid

While searching the network, **AVG S-Tool** shows a dialog providing information on progress of the required operation. Press the *Cancel* button to stop the operation at any time.

<< – This button will switch to the previous *Settings* tab

Quit – The button will close the AVG S-Tool application

5.3. AVG S-Tool Advanced Mode

AVG S-Tool Advanced Mode is intended for experienced users who want to manually configure the installation script (functionality, parameters, AVG behavior) according to their own needs.

To launch the *AVG S-Tool Advanced Mode* select the option *Advanced mode*:
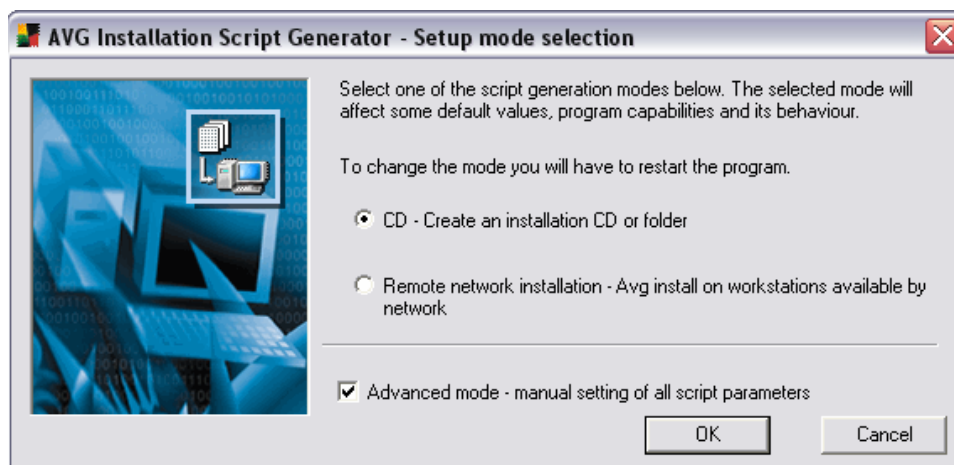
The *Setup Mode Selection* dialog window offers a selection between two options of creation and use of the installation script:

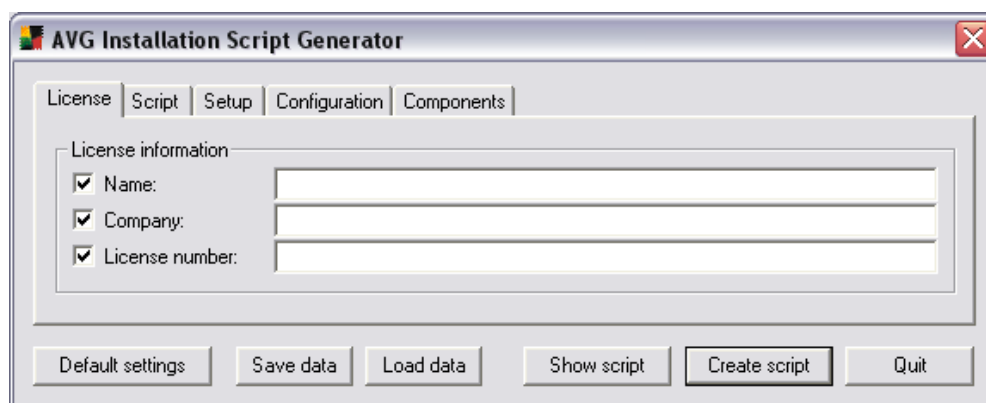- *CD or installation script*

- *Remote Network installation*

a) *CD or installation script*

Selecting the *CD or installation script* option, **AVG S-Tool** will create an installation script for running the installation into a selected directory. The content of the directory can then be copied to a CD used as an installation CD; or you can use the created files for remote installation. The selected option does not offer the possibility of remote installation to the network workstations or servers.

The new dialog window opens with five tabs:

o *License tab*

License information – type in license data such as Name, Company, and License number. If you wish to take the Windows username for the *Name* field, do not select the respective check box, and leave the default system settings to be used.


o *Script tab*

File names definition – You can manually specify the name of the installation file, and the name of the script file with parameters. If you decide to change previously specified parameters and return to the default settings, use the *Default* button to do so.

Setup files location – In this section you need to specify the path to the directories containing the following files:

- Installation script file (to be saved)

- AVG setup file

- AVG setup log file

Also, you have to specify the name of a subdirectory where the AVG installation file should be stored, and decide whether the AUTORUN.INF file (controlling the future CD automatic launch) should be created.
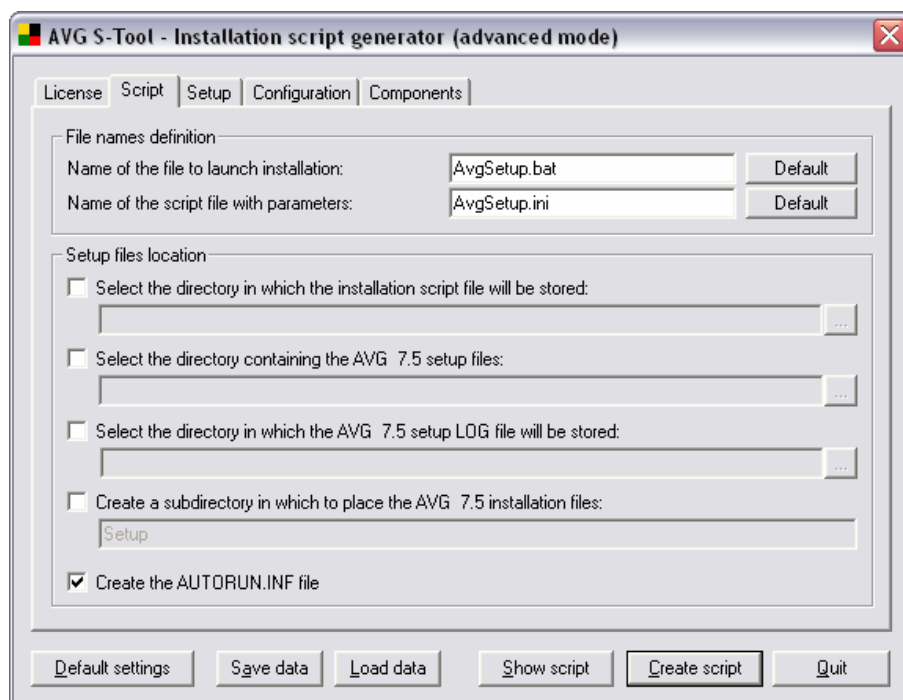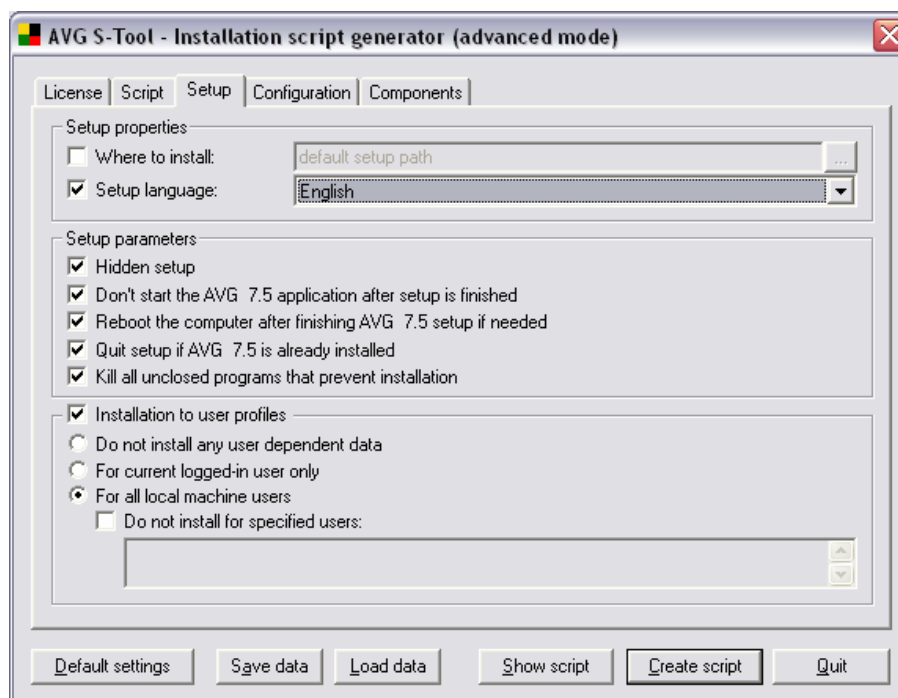
AVG 7.5

o **Setup tab**

Setup properties – Specify where AVG should be installed; you can either type in the path manually or press the ▦ button to locate the directory on your local disc using the navigation tree. Also select the language of the installation.

Setup parameters – Specify the installation parameters selecting the desired option of the following possibilities:

- Hidden setup

- Don't start AVG applications after the setup is finished

- Reboot computer after the AVG setup is finished

- Quit setup if AVG is still installed (the option is selected by default; if you uncheck it, the original AVG will be reinstalled)

Installation to user profiles – Select whether the installation should be performed for all users, for the currently logged-in user, or whether the installation should not reflect any user dependent data. You can also decide to install AVG to all users with specified exceptions – select the **For all local machine users**, and then specify the excepted users manually.

AVG 7.5

AVG Anti-Virus Network

o   ***Configuration tab***

Apply configuration template – Within this section you can specify what AVG configuration parameters should be applied. Parameters are related to the **AVG S-Tool** network search results (***Conditional use of a configuration template***), and divide various configuration templates to be used (***Apply all users common configuration/Apply user dependent configuration***).
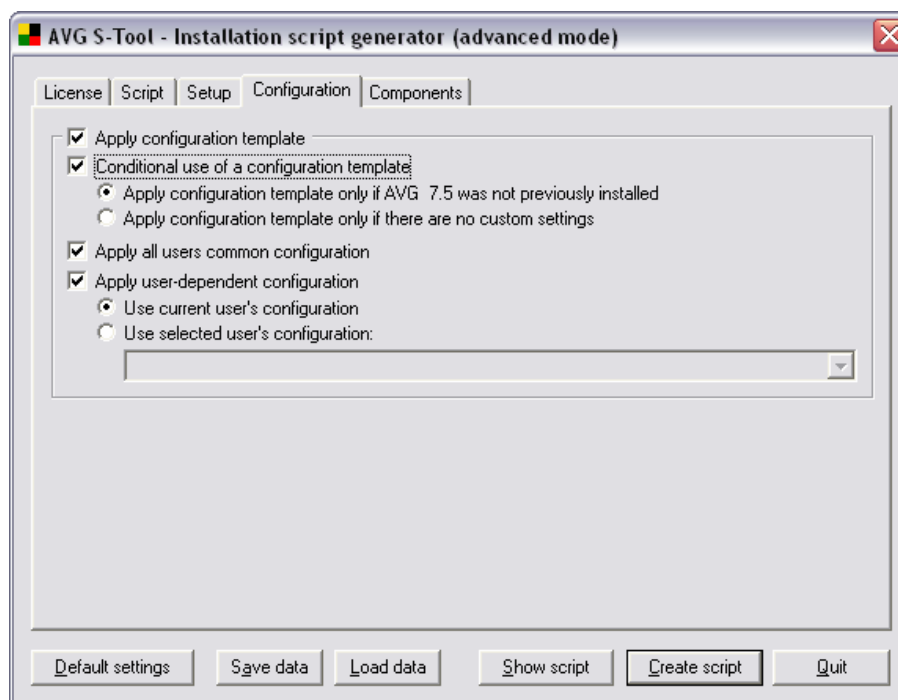
AVG 7.5

AVG Anti-Virus Network

o **Components tab**

Remote administration – Define the **AVG DataCenter** connection string *(see chapter* <u>*6.7 – Clients Connection to AVG TCP Server*</u>*).* If you do not want to use the remote administration options and you do not plan to install the **AVG DataCenter** and **AVGADMIN**, leave the respective check box unselected.

– *User* - specify user name, if applicable.

– *Password* - specify password, if applicable.

– *Add new station into group –* specify a defined group of stations in the AVGADMIN into which the newly added station should be assigned

– *Add new user into group –* specify a defined group of users in the AVGADMIN into which the newly added user should be assigned

– *Install or uninstall components–* In this section, you can see a tree structure offering a list of AVG components that can be either installed or uninstalled. From the list of components select:

– components that should be installed, and mark them like this ☑

– components that should be uninstalled, and mark them like this ☒

The default settings will be used for components that you leave blank (☐).
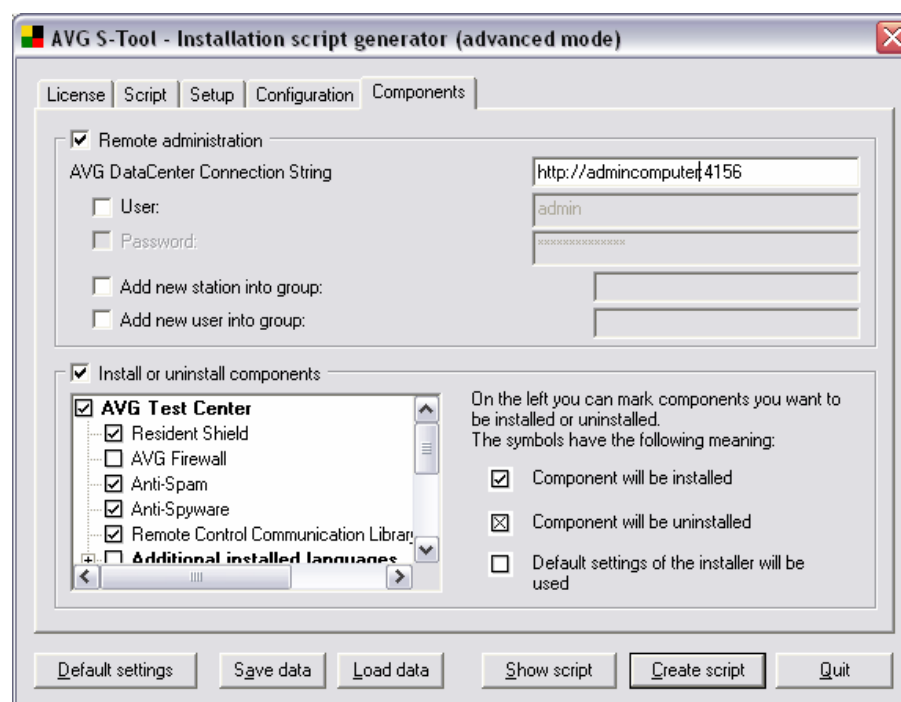
From all tabs you can reach the dialog control buttons:

- *Default settings* – returns the dialog parameters to the default settings

- *Save data* – saves the script template in the .stf format to the selected place on your local disc

- *Load data* – allows you to read data from a previously saved script template

- *Show script* – the installation script content will be displayed in a new window

- *Create script* – compiles and saves the installation script to the selected place on your local disc

- *Quit* – closes the AVG S-Tool application

b) **Remote network installation**

When selecting the **Remote network installation** option, **AVG S-Tool** creates an installation script and performs AVG installation on all accessible local network workstations. This option is available within the **Windows NT4/2000/2003/XP Professional (and higher)** operating systems environment.

Note: Network remote administration can also be launched from the AVGADMIN environment using the menu item Service/Install AVG 7 onto stations (in both the Basic/Advanced modes).

The new dialog window opens with six tabs:

o **License tab**

License information – type in the license data such as Name, Company, and License number. If you wish to overtake the Windows username for the **Name** field, do not select the respective check box, and leave the default system settings to be used.
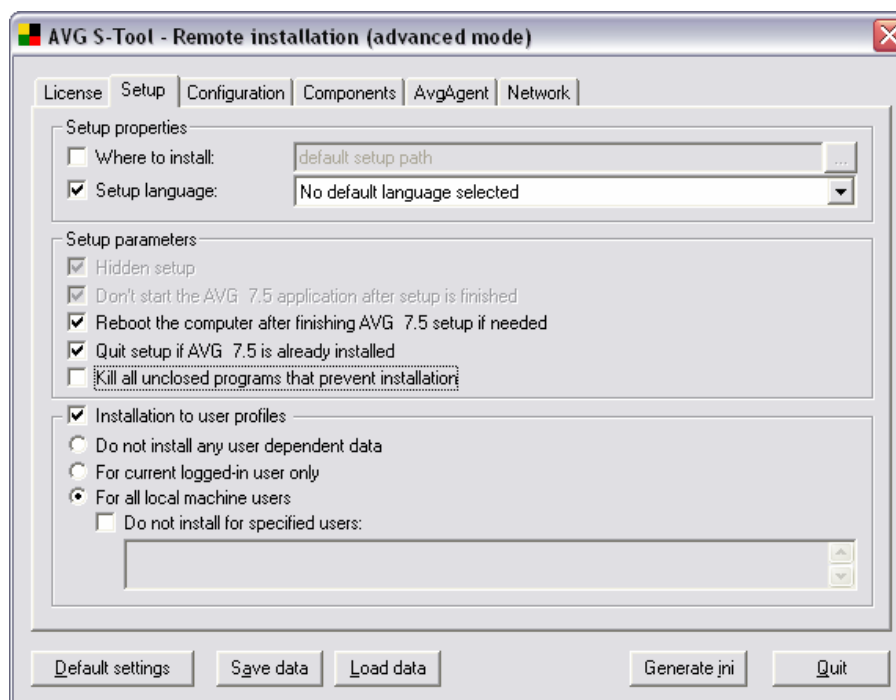
AVG 7.5

AVG Anti-Virus Network
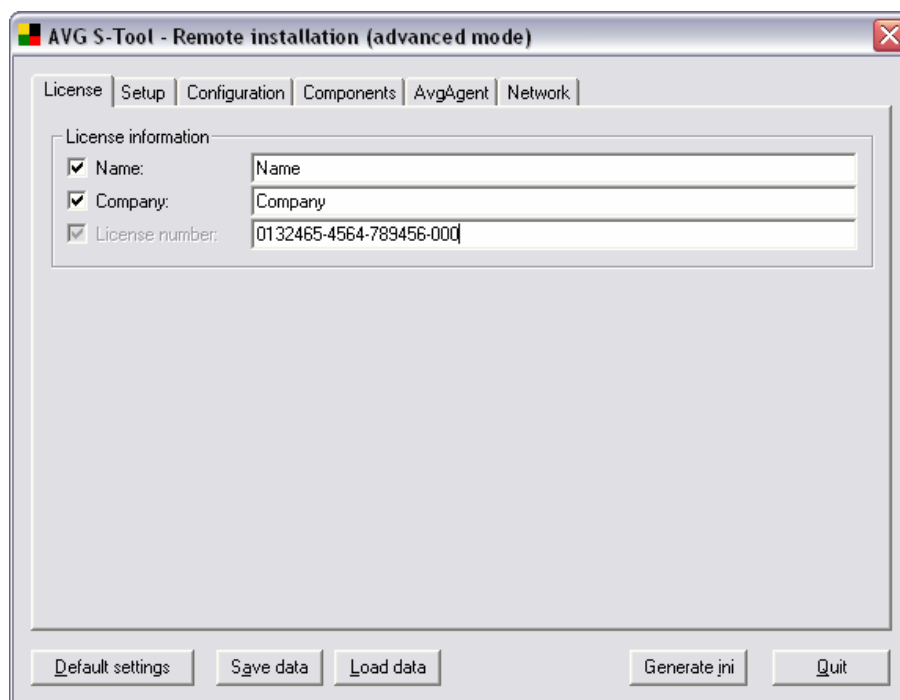
o **Setup tab**

Setup properties – Specify where AVG should be installed; you can either type in the path manually or press the ▨ button to locate the directory on your local disc using the navigation tree. Also select the language of the installation.

Setup parameters – Specify the installation parameters selecting the desired option from the following possibilities:

– Reboot computer after the AVG setup is finished

– Quit setup if AVG is still installed (the option is selected by default; if you uncheck it, the original AVG will be reinstalled)

Installation to user profiles – Select whether the installation should be performed for all users, for the currently logged-in user, or whether the installation should not reflect any user dependent data. You can also decide to install AVG to all users with specified exceptions – select the **For all local machine users**, and then specify the excepted users manually.

o **Configuration tab**

Apply configuration template – Within this section you can specify what AVG configuration parameters should be applied. Parameters related to the network search results (**Conditional use of a configuration template**). The configuration will be performed automatically for all users.
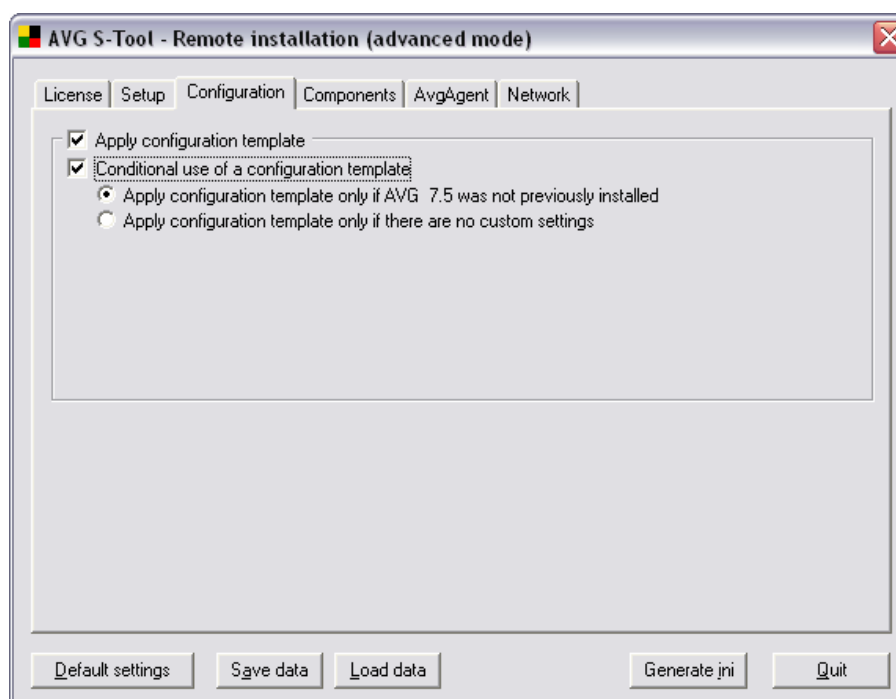
o **Components tab**

Remote administration – Define the AVG DataCenter connection string *(see chapter 6.7 – Clients Connection to AVG TCP Server)*. If you do not want to use the remote administration options and you do not plan to install the **AVG DataCenter** and **AVGADMIN**, leave the respective check box unselected.

Add new station into group – specify a defined group of stations in the **AVGADMIN** into which the newly added station should be assigned

Add new user into group – specify a defined group of users in the **AVGADMIN** into which the newly added user should be assigned

Install or uninstall components– In this section, you can see a tree structure offering a list of AVG components that can be either installed or uninstalled. From the list of components select:

– components that should be installed, and mark them like this ☑

– components that should be uninstalled, and mark them like this ☒

The default settings will be used for components that you leave blank (☐).
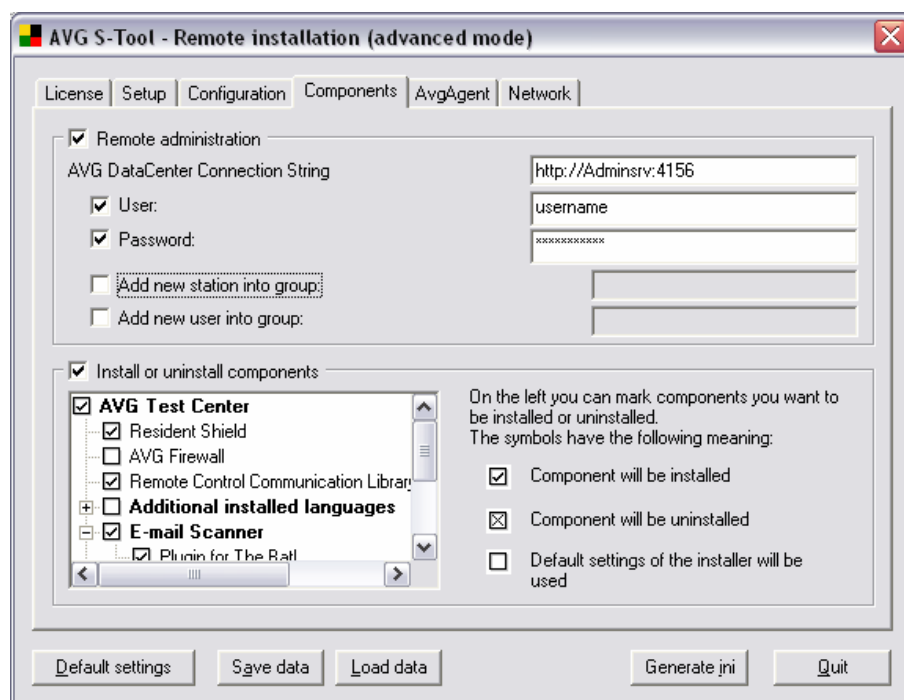
o **AvgAgent tab**

Select the directory containing the batch, script, and the AVG 7.5 setup files – Specify the path to the directory where the installation script, the batch and the AVG installation files are located. You can either type in the path manually, or press the ▦ button to open a new window; then select the directory from the navigation tree of your local disc.

IP addresses – If you selected the option of searching the network in the range defined by IP addresses, you need to specify the range by entering the IP addresses here.

Note: When launched for the first time, AVG S-Tool will try to fill in the IP addresses according the network configuration set on the station where the AVG S-Tool application is running. However, if you know the exact IP address range of network stations, adjust the values manually to shorten the time needed for searching the network.

AvgAgent settings – This group is intended to set up some parameters of the **AvgAgent** service. This service is installed on the remote stations and supports AVG remote installation and other AVG utility operations.

All changes will make an impact on the remote stations only after (re)installation of the **AvgAgent** service on them. Therefore it is necessary to reinstall **AvgAgent** service on the stations after changing some of the settings here. You can do this by checking on the *Always install* option on the *Network* tab. This holds also for the *AvgAgent password* item on the *Network* tab!

Attention: Automatic AvgAgent service installation is available only for the Windows NT4/2000/2003/XP Professional operating systems. On the Windows 95/98/Me/XP Home stations you have to firstly install AvgAgent manually or by login script. Reinstallation of AvgAgent service on the stations, which are running the service already, can be performed remotely using AVG S-Tool.

Enable AvgAgent log – switched off by default. Once you have switched this item on, the **AvgAgent** service generates a log file on stations with a newly installed **AvgAgent** service. For usual **AvgAgent** running, there is no need to create the log files.

Log level – you can specify the logging files detail level here:

- *Errors only –* only application's run related errors are logged – such as unauthorized connection attempts, network timeouts and so on.

- *Detailed –* information on the operations requested and performed by the service on a station.

- *Debug –* very detailed records covering the program diagnostics. After selecting this level, the log files will be very large.

Log file name – fill in the name of the log file. **AvgAgent** service will store the log files under the selected name on remote stations, where the service should be installed. If you do not enter the absolute path (e.g. C:\avgagent.log), the directory containing the AvgAgent.exe file (typically the C:\Windows or C:\WinNT directory) will be used for storing the log file.

Note: Log files are not deleted or decreased automatically! If you use them, you have to analyze them and then delete manually.

– **Port –** TCP/IP communication port, where the **AvgAgent** service listens for the **AVG S-Tool** connection. The default value is 6150 and usually there is no need to change this.

– **Timeout –** the **AvgAgent** and **AVG S-Tool** communication timeout value in milliseconds. When there is no response within the specified value in the **AvgAgent** and **AVG S-Tool** communication process, the connection is terminated with an error. If you have a very busy network or the stations with AVG installed are very slow, you can increase this timeout value to prevent connection timeout errors.

o **AVG S-Tool parameters**

AVG setup type – you can specify the type of installation files located in the directory selected in the **Select the directory with the AVG setup files** field. Selecting the wrong type will result in discarding of the installation.

Inet – the installation is performed from the single file in avg7*.exe form as it was downloaded from the web pages of Grisoft. There is no need to unpack the file, you can keep it packed. If there are more versions of the file in an installation folder, the most recent (according to date of creation) file will be used.

– **CD** – the content of the installation CD is in an installation directory or there is the unpacked content of a single installation file, which has been downloaded from the internet. You can use a freeware WinRAR application for unpacking a single file.

– **Ping –** number of Ping operations used while detecting availability of a remote station is specified here. If **AVG S-Tool** does not receive a response to any of the Ping queries, it will consider the station to be unavailable and will not offer it for further operations.

Other dir for ini files – If this item is checked on, **AVG S-Tool** will store the generated ini files into a specified directory. These files are needed to perform AVG and **AvgAgent** remote installation. Leaving this item unchecked, the default path for ini files is **Documents and Settings\user_name\Application data\AVG7**. Pressing the button will open a window, where you can choose the desired directory. Ini files are created automatically at the beginning of each installation of AVG program and **AvgAgent** (the **Install AVG** button on the **Network** tab). Ini files can be created on demand after pressing the **Generate ini** button.

AVG 7.5

AVG Anti-Virus Network
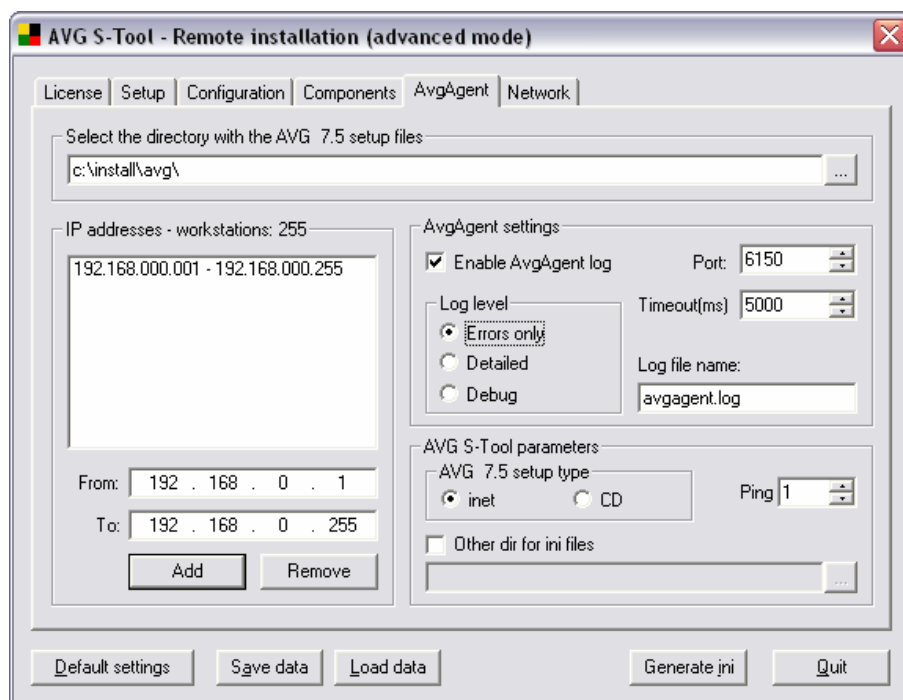
o **Network tab**

   Network type – **AVG S-Tool** searches for AVG on network stations either in the range of a domain from which the installation is launched (i.e. where the station with **AVG S-Tool** installed is located), or within the range defined by the IP addresses (on the previous **AvgAgent** tab).

   – **Level of communication log** - select the preferred level of communication logging.

     Logging off (no logging)

     Errors only (only errors will be logged)

     Detailed (more detailed logs)

     Debug (debug information will be logged)

   Scan network – After pressing this button, **AVG S-Tool** will start inspecting separate network workstations for the AvgAgent service and AVG program presence. The search results are then displayed using the following icons:

   Station found (the station is registered in the domain); the station status has not been inspected yet

   Neither **AvgAgent** nor AVG are installed on the workstation

   AvgAgent is installed on the workstation; AVG is not installed

   Both **AvgAgent** and AVG itself are installed on the workstation

AVG 7.5

AVG Anti-Virus Network

❌ An error occurred while communicating with the station. Double click to show detailed information. Typically, an error occurs if communication with **AvgAgent** is blocked (e.g. by a firewall), or your password is invalid

While searching the network, **AVG S-Tool** shows a dialog providing information on progress of the required operation. Press the *Cancel* button to stop the operation at any time.

Workstations – The option displays the current number of stations on which the desired operations should be performed.

Force install – The option specifies that the AvgAgent service together with AVG should be installed even on stations where AVG is already installed. This functionality allows you to perform AVG reinstallation on all network workstations.

Mask password – Selecting this option will prevent the password from being displayed on your computer's monitor.

AvgAgent password – Enter the password that will protect communication between **AVG S-Tool** and the **AvgAgent** service on remote workstations. If the password is specified, no operations using the **AVG S-Tool** can be performed on the remote workstations without knowing it. The password is related to the **AvgAgent** service only, and it does not influence any other remote station settings. This password must be specified BEFORE you launch **AvgAgent** installation on remote workstations!

AVG 7.5

AVG Anti-Virus Network

To change the AvgAgent password, follow these steps:

– Type the new password into the ***AvgAgent password*** field

– Select the ***Force install*** option!

– Run AVG remote installation

– A dialog asking for the **AvgAgent** password will be displayed – enter the original password into this dialog!

– After the installation, the **AvgAgent** on the station uses the new password already
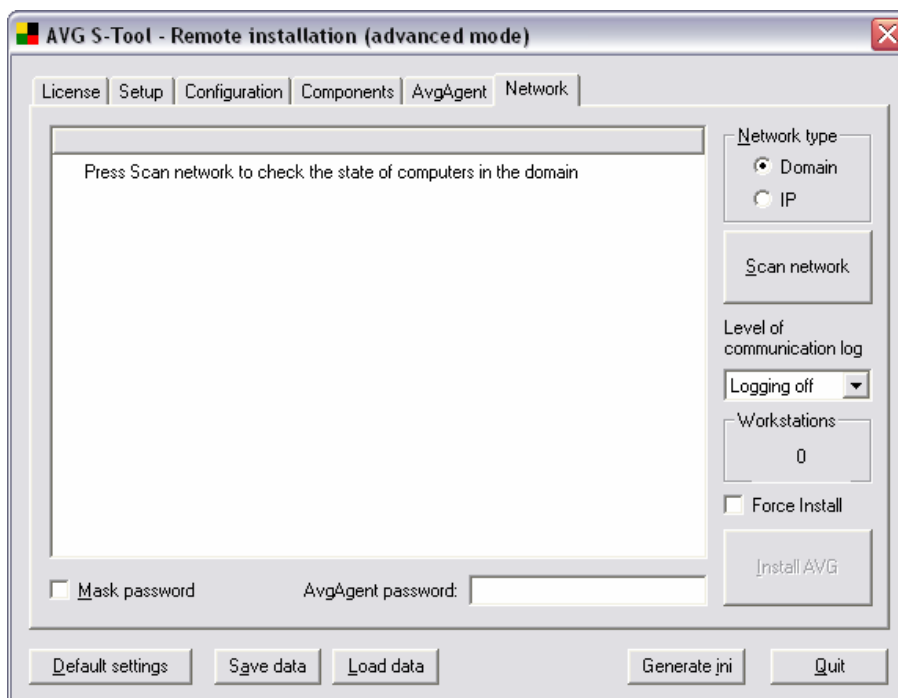
From all tabs you can reach the dialog control buttons:

o ***Default settings*** – returns the dialog parameters to the default settings

o ***Save data*** – saves the script template in the .stf format to the selected place

o ***Load data*** – allows you to read data from a previously saved script template

o ***Generate ini*** – allows you to create the configuration settings defining INI file

o ***Quit*** – closes the AVG S-Tool application

Warning: *Within the Windows NT4/2000/2003/XP Professional operating systems environment it is possible to run AVG remote installation only on network workstations/servers where you are logged in as an administrator.*

5.4. AVG Installation on Windows NT4/2000/2003/XP Professional

Having searched the network and specified the network workstations status, you can install AVG to the network workstations. If you select some workstations from

the list, AVG installation will be performed on these workstations only. Otherwise installation will be performed on all listed workstations.

If your access rights do not suffice for **AvgAgent** service installation on the remote workstation, you will be asked for the domain administrator's login/password during installation.

If there is no common administrator account for all workstations (with the same login name and password) you will be asked separately for every workstation.

Pressing the *Cancel* button will cause the current workstation installation to be skipped, and the **AVG S-Tool** will continue installation on the following workstation in the list.

5.5. AVG Installation on Windows 95/98/ME and XP Home

The installation process on workstations with these operating systems is the same as installation on workstations running the Windows NT4/2000/2003/XP Professional OS. However, due to the restrictions of these older operating systems it is not possible to run the automatic installation of the **AvgAgent** service. Therefore, before you start AVG installation on all workstations with the Windows 95/98/Me/XP Home operating system, it is necessary to install the **AvgAgent** service manually, or using the login script.

For manual **AvgAgent** installation it is necessary to generate the avgagent.ini file. At the beginning of remote installation this file will be automatically generated into the user's data directory – typically *Documents and Settings\user_name\Application Data\AVG7*. The file can also be generated on demand from the *AVG S-Tool Advanced mode*.

To perform manual **AvgAgent** service installation, copy the avgagent.exe, avgagent.lng, and avgagent.ini files into one directory. Then run the command line: *Start menu/Programs/Accessories/Command Prompt*; using the *cd* command switch to the directory with the copied **AvgAgent** service files, and run the command *avgagent.exe /install /start*.

Once the **AvgAgent** service is installed on the workstations, you can run all **AVG S-Tool** operations on these workstations, including AVG installation and **AvgAgent** service upgrade.

6. AVG TCP Server

AVG TCP Server is used to secure communication between the **AVG clients** on workstations, and the **AVG DataCenter** on the server. Through the **AVG TCP Server** the AVG clients connect to the **AVG DataCenter** using the TCP protocol (or the HTTP protocol, to be exact) that is a part of each Windows operating system installation. Therefore, the AVG clients do not need any other third party component to be able to connect to the remote administration system.

Besides this elementary function, the **AVG TCP Server** can also provide update distribution within the local network. **AVG TCP Server** can work as a very simple web server offering the update files to AVG clients. The update files are downloaded from the Grisoft central update servers just once, which significantly decreases the internet connection link load, especially in larger networks.

6.1. AVG TCP Server Installation and Launch

By default, the **AVG TCP Server** is installed into this directory:

C:\Program Files\Grisoft\AVG TCP Server

If you select another destination folder for the network administration, the **AVG TCP Server** will be installed into the **AVG TCP Server** subdirectory within the selected directory.

In the *Windows NT4/2000/2003/XP Professional* environment the **AVG TCP Server** launches automatically on operating system start up.

In the *Windows 98/Me* environment the **AVG TCP Server** launch is defined by the register key record *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices.*

6.2. AVG TCP Server as a Local Web Server Update Source

Using the web server implemented into the **AVG TCP Server** it is possible to perform a centrally controlled AVG update within the local network.

The main advantage of this option consists of the fact that AVG clients on separate workstations do not have to download the update files from the internet but can update from the local network update source. This way the connection load is significantly decreased, and the download time shortened. This function can be provided by any web server. **AVG TCP Server** secures the service if there is no local web server in the network.

All workstations download their updates based on a preset schedule using the HTTP protocol. The web server (**AVG TCP Server**, or any other web server) address used for the local update can be specified directly on the workstation, in the *AVG Control Center/Update manager component/Configuration/URL tab*. If the workstation is connected to the network administration you can also control the updates within the AVGADMIN application.

The easiest way to download the update files from the internet to the local web server is using the AVGINET Lite application.

AVG 7.5

AVG Anti-Virus Network

The **AVGINET Lite** program is a part of the **AVGADMIN** installation. Automatically, it is able to mirror all update files, to remove all redundant files, and to download new ones. For this purpose, we recommend running **AVGINET Lite** with these parameters:

AVGINETL.EXE /URL="http://update.grisoft.cz/softw/70/update" /DIR="C:\AVGUPDATE" /PRI=5

The */DIR* parameter must correspond to the **AVG TCP Server** configuration value, Local HTTP Server Root item!

On a computer with **AVG TCP Server** running, you can launch the **AVGINET Lite** either manually, or you can schedule its launch using the operating system scheduled tasks option.

For further **AVGINET Lite** program and its components description see chapter 14. AVGINET Lite.

Step by step network updates settings procedure:

This example will lead you step by step through the procedure of

● downloading update files to the **AVG TCP Server**

● updating from this local server

a) On your server create a new folder named *C:\AVGupdate*

b) Run *C:\Program files\Grisoft\AVG TCP Server\avgtcpmon.exe* to open the **AVG TCP Monitor**. Use the *Configuration* button to open the *AVG TCP Server Settings* dialog, and then press the *To advanced* button in the bottom left corner of the screen. In the newly opened dialog fill in the further listed text fields as follows:

    o In the *License number* field replace the string *AB-CDEF-GHIJ-1234-5678* with your actual license number.

    o Write *c:\AVGupdate* in the *Local HTTP Server Root* field

    o Write */avgupdate* in the *HTTP Server Root* field

    o Write *c:\AVGupdate\avgtcp_http.log* in the *HTTP Log Path* field

c) Switch to the *Inetlite* tab of the *AVG TCP Server Settings* dialog, and fill in the *Update URL* field with this URL: *http://update.grisoft.cz/softw/70/update*. If you use any proxy server you need to specify its name in the *Proxy* field. Also, you can select the required type of update in the bottom section of the *Inetlite* tab.

d) Switch to the *Scheduler* tab to specify the update schedule time period.

e) Save all configuration changes and you will be prompted to restart the **AVG TCP Server**.

GRISOFT

f)   From the **AVG TCP Monitor** start the **AVG TCP Server** again.

To make sure that the **AVG TCP Server** is running properly create a new file named *C:\avgupdate\test.txt*, and write a testing text *Test of TCP Server* inside this file. Then, try to run the *http://<IP address of your server>:4156/avgupdate/test.txt* address in your web browser. You should be able to see the *Test of TCP Server* text if the web server over **AVG TCP Server** is set properly.

Note that update files are downloaded to your local server by a utility named *avginetl.exe* located in the **AVG TCP Server** directory. On the **AVG TCP Monitor**'s *Scheduler* tab you can specify the update files should be downloaded automatically, or you can run *avginetl.exe* manually and use many other parameters that are available *(Run C:\Program files\Grisoft\AVG TCP Server\avginetl.exe to be able to see all the parameters).*

Example:

The command

AVGINETL.EXE /URL="http://update.grisoft.cz/softw/70/update" /DIR="C:\avgupdate

will download all update files into the C:\avgupdate folder. Put this command into the batch file, and then schedule this batch file in Windows scheduler.

g)   Open **AVGADMIN**, and from the top menu select *Settings/Shared settings for stations* to open a new *Station.SHARED.STATION* dialog where you can specify the server parameters. Double click to the *internet connection/Server* item to open the *URL* dialog. Select the appropriate server from the list; you can edit its parameters (*Edit* button) or add a new server (*Add* button) in the *Edit URL* dialog. Enter the server name into the *Server* field (*you can call the server any name you like; this name only helps you recognize the server in the list of other servers*); the *URL* field requires a full **AVG TCP Server** address in the form of http://server:4156/avgupdate.

Please note, that both the **http://** and the **:4156/avgupdate** are necessary for the update to work properly!

6.3. AVG TCP Server Control

To control and configure **AVG TCP Server** you can use the **AVG TCP Monitor** tool.

In the **Windows9x/Me** operating system environment, the **AVG TCP Monitor** also works as an elementary tool for status monitoring, launching and stopping **AVG TCP Server**. In the **Windows NT4/2000/2003/XP Professional** operating system environment you can also control **AVG TCP Server** with the standard operating system tools. Within these operating systems the **AVG TCP Server** uses the Application Event log to create the log files.

The **TCP Server Monitor** is a part of the **AVG TCP Server** installation. **TCP Server Monitor** displays an icon on the system tray, and the icon's color indicates the **AVG TCP Server** status. Double click on the icon to open the **AVG TCP Server Monitor** dialog with the basic information on the server activities:

AVG 7.5

AVG Anti-Virus Network

The **AVG TCP Server Monitor** dialog Windows contains the following control buttons:

Pause server – allows you to pause the AVG TCP Server, and continue its running

Stop server – allows you to stop the AVG TCP Server

Configuration – allows you to set up the *AVG TCP Server configuration*

Hide monitor – hides the AVG TCP Monitor dialog window

Quit monitor – closes the AVG TCP Monitor service

You can also overview the login data recorded in the **Application Event log** – only for the **Windows NT4/2000/2003/XP Professional** operating system.

6.4. AVG TCP Server Configuration

Note: The **AVG TCP Server** can also be remotely configured from AVGADMIN (AVG TCP Server must be already started) by selecting the **AVG TCP Server settings** item from the **Settings** top menu.

The **Configuration** button opens the server configuration dialog. The configuration dialog can run in two modes:

- AVG TCP Monitor Simple mode
- AVG TCP Monitor Advanced mode

When you launch **AVG TCP Server Monitor** for the first time, the configuration dialog automatically opens in the simple mode.

AVG 7.5

AVG Anti-Virus Network

The **AVG TCP Server** configuration is stored in the file AVGTCPSV.INI, which is located in the **AVG TCP Server** program folder. The most comfortable way of changing the configuration is using the **AVG TCP Monitor** application. However, the configuration file is a raw text file, so it can be edited by any usual text editor (such as NOTEPAD). Each parameter is on a separate line and the # (hash mark) starting lines are ignored, as well as empty lines.

Attention! *AVG TCP Server is case sensitive; therefore it is crucial to distinguish upper/lower case letters. For example, if the URL is specified as follows* http://server:port/ADDRESS, *the link* http://server:port/address *will not work!*

Attention! *All the comments will be erased after using the configuration dialog in the AVG TCP Monitor application!*

A list of the most important parameters and information on how and when to use them follows:

a) **Port**

If you want to change the number of the communication port to 4444 for example, delete the '#' character before the Port=80 value and enter the desired new port number, 4444. If you want to use another port of connection, e.g. port 80, be sure that there is no other application running on this port (for example a web server). This port is also used for reduced http protocol functionality, which offers update features for clients in the local network.

Attention! *While changing the port number in the configuration file, you also have to change it in the communication string, which defines the connection between AVG clients and AVG DataCenter!*

Note: *Default port number is 4156.*

AVG TCP Server configuration file
Specifies the port that AVG TCP Server will use for incoming connections
Default value is 4156

Port=4444

b) **LocalAddr**

If there is more than one network card installed on a system hosting **AVG TCP Server**, all the cards are used for receiving by default. This can be undesirable, for example when the computer is on internet gateway as well. **LocalAddr** parameter allows entering a local address to be used exclusively for the **AVG TCP Server** connection. After entering this address (in domain form or by number in A.B.C.D form), the **AVG TCP Server** will receive connections only at this address.

Specifies local address that the AVG TCP Server will use for incoming
connections. Default value is empty, meaning any local address
If the specified name resolves to more than one address then first
available address is used (the server tries each of them)

LocalAddr=10.10.10.7

c)   Databasepath

If you want to move the **AVG DataCenter** database to another place, for example to the folder D:\AVGData, delete the '#' character before Databasepath= value and enter a new absolute path to the avgdb.fdb (including the filename), that is Databasepath= D:\AVGData\avgdb.fdb. Changing this value can be useful, for example when connecting to another database server (such as Firebird SQL server itself). For further details please refer to the given database type documentation.

Attention! *Do not use quotation marks in the path string; the program will use the entire string till the end of the line.*

The configuration file will look like this:

```
# Full path to the database file. For relative paths, current directory
#   is the AVG TCP server executable directory
#   Default value is AVGDB.GDB - i.e. the database file is stored in the same
#   directory as the executable file

Databasepath= D:\AVGData\avgdb.fdb
```

d)   Verbose

If you need the application to produce more verbose (diagnostic) output, set the Verbose value to 1. In that particular case, delete the "#" character before Verbose=1 value. Default value is 0, which means, that no excessive diagnostic output will be produced.

```
# If set to 1, more verbose (diagnostic) output is produced.
#   Default value is 0, producing no excessive diagnostic output

Verbose=1
```

e)   DCrequestloglevel

These two configuration options define the logging level of **AVG DataCenter** requests that were accepted and processed by **AVG TCP Server**. The logging is not active by default. Setting the **DCrequestloglevel** to value 1 will activate normal logging level, which records all the requests resulting in error into the log file. The records are provided with the client's IP address, timestamp and literal text of database server response. Setting the **DCrequestloglevel** to value 2 will activate detailed logging. In this mode, all the client requests are recorded into the log file. This mode should be applied only when detailed diagnostics are needed. A huge log file is generated which occupies a lot of disk space.

f)   License

If you uncomment this parameter, a full license number for **AVG Anti-Virus Network Edition** needs to be entered. Some **AVG TCP Server** functions are supported only after entering your AVG license number.

AVG 7.5

AVG Anti-Virus Network

g) FBConsTrans

This parameter controls the transaction mode used when accessing Firebird SQL server. By default, AVG TCP Server uses the "concurrency" transaction mode. If FBConsTrans is set to 1, then more conservative "consistency" mode is used. Set this only if the AVG TCP Server reports errors in SQL commands.

```
# This parameter controls the transaction mode used when accessing
#   Firebird SQL server. By default, AVG TCP Server uses the "concurrency"
#   transaction mode. If FBConsTrans is set to 1, the more conservative
#   "consistency" mode is used. Set only if the AVG TCP Server reports

#   errors in SQL commands

FBConsTrans=1
```

h) Username and Password

These two values represent Username and password that the clients will have to use in order to access the DataCenter. If these values are empty, clients don't have to authenticate. If the values are set, clients are obliged to use them. By default no authentication is necessary. It is recommended that if you change these parameters, you should use values different from the default ones!

```
# Username and password that the clients will have to use in order to
#   access the DataCenter. If these values are empty, clients don't have
#   to authenticate. If the values are set, clients are obliged to use them
#   By default no authentication is necessary
#   It is recommended that if you change these parameters, you use values
#   different from the default ones

Username=ExampleOfUserName

Password=ExampleOfUserPassword
```

i) DBAUsername and DBAPassword

Username and password for accessing the database engine itself. These should hardly be used for the embedded database engine, but could come handy if AVG TCP Server connects to a standalone database server

```
# Username and password for accessing the database engine itself. These
# should hardly be used for the embedded database engine, but could come
# handy if AVG TCP Server connects to a standalone database server

DBAUserName=SYSDBA

DBAPassword=masterkey
```

j) WebUIURL

AVG TCP Server publishes basic information on its state also on a web page. This feature is active by default. It is accessible on the remote administration port for implicit document query. If the default 4156 port is used, you can

enter an address http://server:4156/ in any web browser and the server displays basic information on its state. You can change this address by editing the WebUIURL parameter. You can fully disable this feature by defining the WebUIURL parameter with an empty value.

k) **LocalHttpServerRoot**

If this parameter is uncommented and also valid remote administration license number is used, reduced functionality of web server is activated. Clients can then utilize updates from their computer with **AVG TCP Server** installed (and running). No other components or shared folders for the update distribution in local network are needed.

The **LocalHttpServerRoot** parameter defines a folder, which is accessible through the web server functions (that means the GET requests). Clients can access only this one directory and only after the path specified in the request agrees with the **HttpServerRoot** parameter value.

l) **HttpServerRoot**

If a simple web server support is active, this parameter defines the path to be used in user requests for file operations. This path then corresponds to the folder given in the **LocalHttpServerRoot** parameter.

In the specified folder the AVG update files must be accessible, including the correct update controlling file AVG7INFO.CTF. You can easily guarantee this by the regular mirroring of update files with the AVGINET Lite application.

Supposing the update files are stored in the C:\AVGUpdate folder on a computer which is running **AVG TCP Server**, the parameter values are then defined as follows:

LocalHttpServerRoot= C:\AVGUpdate

HttpServerRoot=/avg7upd

If a HTTP client poses a request for C:\AVGUpdate\AVG7info.ctf, a query in http://<server_name>/avg7upd/AVG7info.ctf form will be used.

In update configuration (**AVG Control Center**) it is possible to define a new local server with URL http://server:4156/avg7upd after specifying the parameters as above.

Attention! Note that in the previous example there is a port number specified! The web server is active on a port with the number specified in the AVG TCP Server configuration (see paragraph a) above). The default number is therefore 4156!

m) **HttpLogPath**

This parameter specifies the absolute full path to the HTTP protocol GET requests log file. The file is in an Apache Combined log file format for maximum portability.

n) **UpdateURL**

If an update control feature is activated, this parameter specifies the address to be used for downloading the update files. The recommended value is http://update.grisoft.cz/softw/70/update.

o) **Proxy**

If an update control feature is activated, this parameter specifies a server and an account for proxy server connection during the downloading of update files (e. g. http://user:password@server:port)

p) **CheckMode, CheckPeriod, CheckTime**

The *CheckMode*, *CheckPeriod* and *CheckTime* parameters relate to the Scheduler tab of the **AVG TCP Monitor**.

The *CheckMode* parameter specifies the frequency mode of the **AVGINET Lite** scheduled launch using the **AVG TCP Server** (values 0-4 in the example AVG TCP Server configuration file). If the parameters are specified within the configuration dialog you can only select from the modes: never, at startup, every N minutes, every N hours, at specific times. By default, the value is set to the *every N hours* option.

The *CheckPeriod* parameter is an additional parameter that is activated only if you have set the *CheckMode* parameters value to *every N hours* or *every N minutes*. The *CheckPeriod* parameter represents the *N* value. By default, the value is set to 2.

The *CheckTime* parameter defines the times when the **AVGINET Lite** should be launched if you selected the *at specific times* option within the *CheckMode* parameter.

q) **Inetliteplatform (Download updates for operating system)**

This parameter defines, for which operating system(s) will be updates downloaded.

inetliteplatform=winall – only MS Windows updates will be downloaded.

inetliteplatform=linux – only Linux updates will be downloaded.
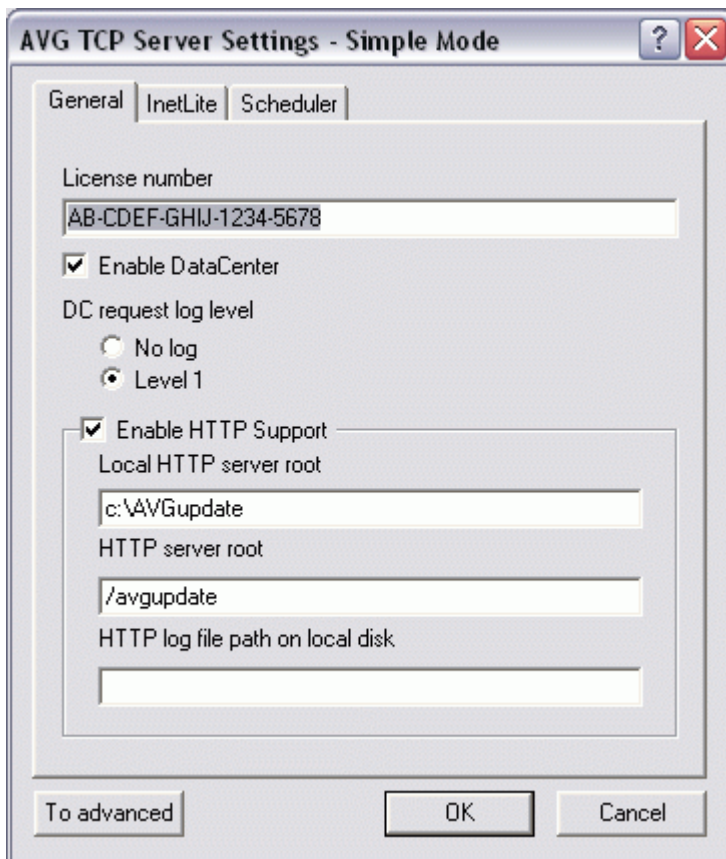
If you leave the parameter unset (i.e. delete it from the INI file), default settings will be used and both MS Windows and Linux updates will be downloaded.

6.5. AVG TCP Monitor Simple Mode

AVG TCP Monitor opens in the simple mode on the **General** tab. Within the **AVG TCP Monitor** simple mode you can enter your license number, and activate the web server simple mode intended for local network updates.

The other two tabs stay inactive until you mark the *Enable HTTP Support* item check box.

AVG 7.5

AVG Anti-Virus Network

a) **General Tab**

o   *License number*

Enter your AVG license number. This license number must correspond to the network license, i.e. the remote administration support must be active. Some AVG TCP Server functions are supported only if a proper AVG Anti-Virus Network Edition license number is specified.

o   *DC request log level*

Within this section you can specify the extent and particularity of the request log records. By default *Level 1* is activated; at this level all error-causing requests sent to the AVG DataCenter are recorded into the request log. It is also possible to suppress the logging completely by selecting the *No log* option. In the advanced mode you will be allowed to activate higher levels of the request log.

o   *Local HTTP Server Root*

If the parameter is active, and a valid AVG license number is used, the limited web server function is activated. In this way the AVG clients can update from a computer with the AVG TCP Server installed. No other components are required, and no directory sharing is necessary for local network update distribution.

The value of the parameter defines the directory made accessible by the web server functions. Only this directory is open to AVG clients, and only

if the path specified in the file request corresponds to the parameter's value.

To activate this function we recommend that you create a local directory **C:\AVGUPDATE**, and set the value of the parameter to **c:\avgupdate**. This directory content will then be open for the AVG clients' updates. The AVG update files must be available in the specified directory, including the update-controlling file AVG7INFO.CTF. To reach this status make sure you perform regular update files mirroring.

If you use the possibility of updating from the local web server implemented in the AVG TCP Server, and you have checked this option, the two remaining dialog tabs are activated – the *InetLite* tab, and the *Scheduler* tab.

o *HTTP Server Root*

If the simple web server support is activated, the *HTTP Server Root* parameter defines the path that AVG clients must use in their requirements for update files. This path then responds to the directory set up in the Local HTTP Server Root parameter.

We recommend setting this parameter to the */avgupdate* value, for instance.

Within the update configuration (in the **AVG Control Center**) it is possible to define a new local server. If you keep to the above-mentioned parameters, the new server URL should be as follows: http://server:4156/avgupdate.

Attention! Please keep in mind that in the previous example a port number is defined! The web server is active on a port with the number set in the AVG TCP Server configuration (Port parameter). The default value is then 4156!

o *HTTP Log File Path on Local Disk*

If the **HTTP Log Path** parameter is specified, it defines the full path to the AVG clients' requirements on the web server log file (e.g. update requirements). For the local update function it is not necessary to create the file; it only serves for diagnostics or server requirement recording.

AVG 7.5

AVG Anti-Virus Network

b)   InetLite Tab
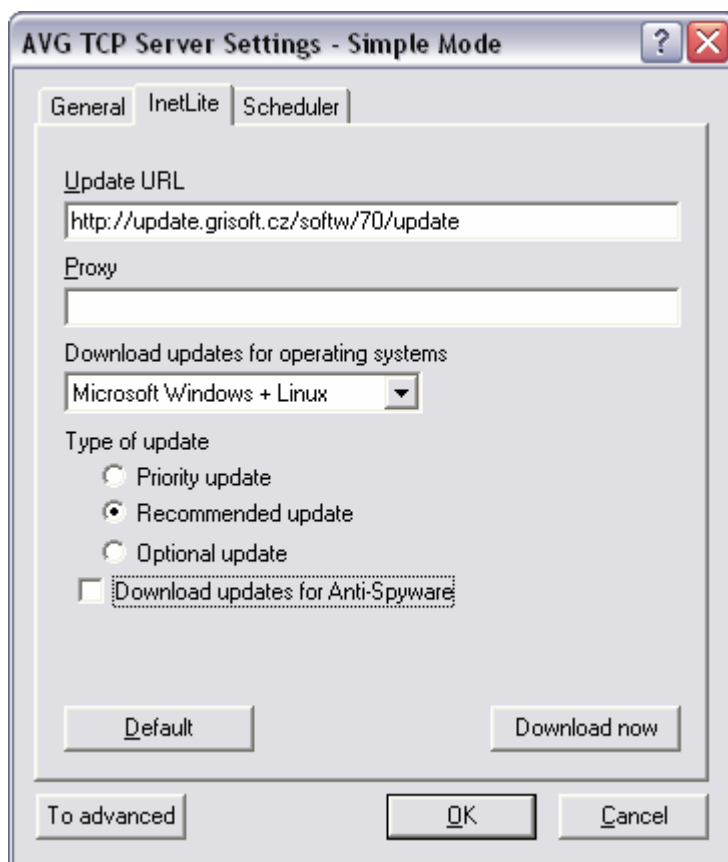
By default, the primary update source is defined on this tab and the item value is preset to the **Grisoft** server URL at http://update.grisoft.cz/softw/70/update. From this server the update files are downloaded to the local web server. If you use a proxy server, specify its location as well.

You can choose the priority level of the InetLite update in the **Type of update** field. Three options are available (*priority*, *recommended* and *optional*), corresponding to the particular update's importance. The levels are described in the following overview:

o   **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**.

o   **Recommended update**

A recommended update contains various program changes, fixes and improvements.

o   **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.

From the **Download updates for operating systems** drop down menu choose the operating system(s) that you require updates for.

The checkbox *Download updates for antispyware* when checked, allows you to download updates for antispyware database as well.

There is also the *Download now* button in the bottom right corner of the tab – you can initiate immediate check of available updates by pressing the button.

The detailed update parameter settings are described in the 14.2 - AVG Client Update Using the AVGINET Lite chapter.

Note: *If you do not enable the download of updates for antispyware, you may experience this dialog during AVGADMIN startup:*

c)   **Scheduler Tab**
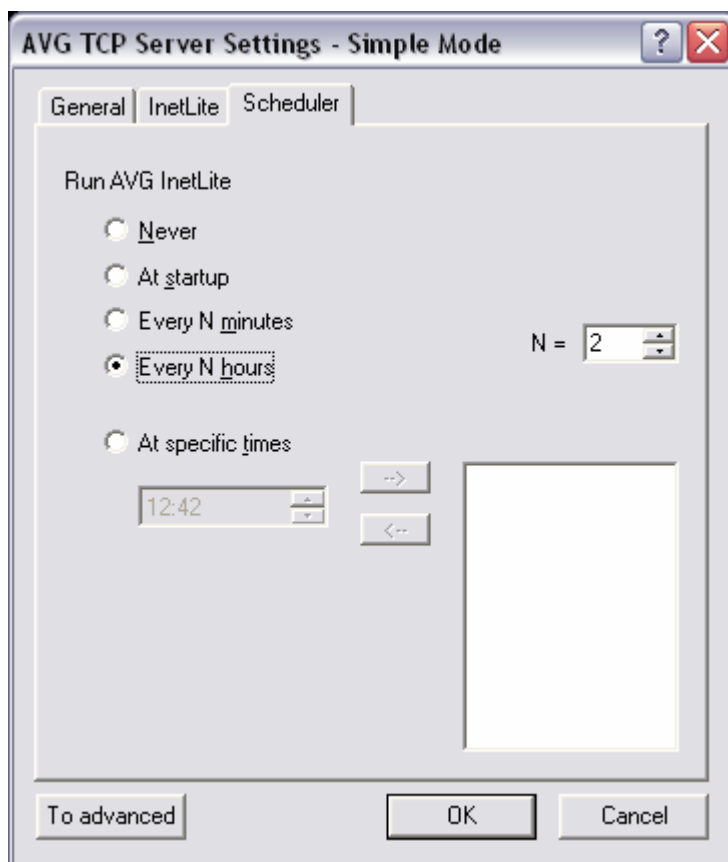
This tab allows you to specify the **AVGInet Lite** time period for new update files existence examinations. If new update files are found, the **AVGInet Lite** downloads them to the local web server.

The available options are offered in the **Run AVG InetLite** section of the window:

o   **Never** – never check for updates

o   **At startup** – check for updates at every startup of **AVG TCP Server**

o   **Every N minutes** – check for updates every N minutes; N can be set in the field on the right

o   **Every N hours** – check for updates every N hours; N can be set in the field on the right

o   **At specific times** – check for updates at times specified in the field below; more times can be specified and set by moving them into the box on the right side, using the [-->] button (use the [<--] button to exclude the selected time from the set of update-check times)
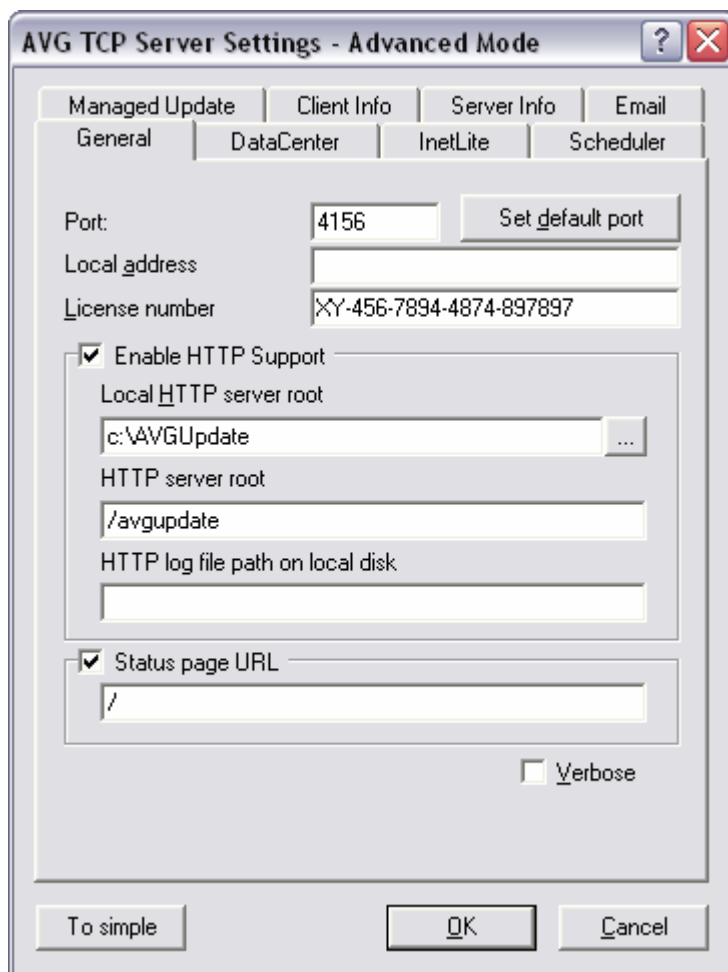
6.6. AVG TCP Monitor Advanced Mode

The **AVG TCP Monitor** Advanced mode is activated from the Simple mode by pressing the **To advanced** button. To switch back to the Simple mode press the **To simple** button.

AVG 7.5

The advanced mode allows you to set up further and extended **AVG TCP Server** function configuration, e.g. scheduling of the automatic launch of update files mirroring in the local network, diagnostics level configuration, setting up the connection to other database servers, etc.

a) **General Tab**

The Advanced mode opens in this tab as well, but it slightly differs from the same tab in the Simple mode:

The *License number* and *Enable HTTP Support* sections are identical to the respective ones in Simple mode. Other three fields are added in the Advanced mode:

o **Port**

If basic *HTTP support* is active, the HTTP server uses the port specified in this field for updates, too. The default port value is 4156. You can reset the default value any time by pressing the *Set default port button*.

o **Local address**

Specifies the local address for incoming connections. The default value is empty, meaning any local address. If the specified name resolves to

more than one address, then the first available one is used (the server tries all of them).

o **Status page URL**

AVG TCP Server status can also be checked using a web browser. By default, requesting root document will return the server status (in the form of http://address:port/ - http://127.0.0.1:4156 with default settings). The text field in this section can be used to change the URL to be used for querying the status. The default value ∕ corresponds to the default root document. When the string is empty, status display functionality over a web page is disabled.

b) **DataCenter Tab**
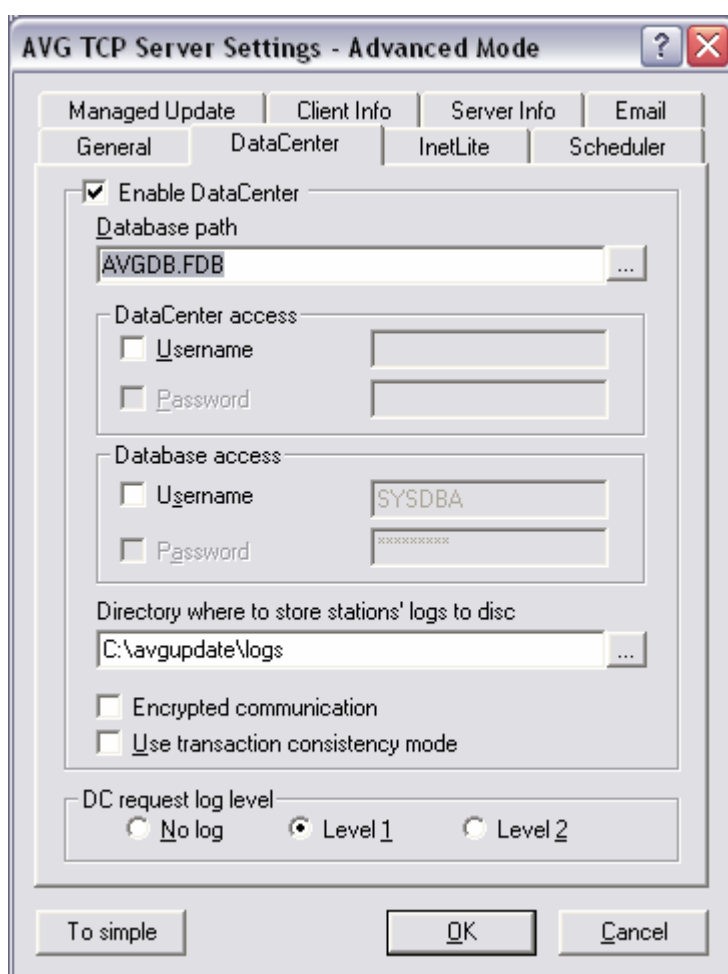
The tab is one of the enhancements of Advanced mode. If you check the *Enable DataCenter* box on, the **AVG DataCenter** database is then used. In the respective section of this tab, you can adjust parameters related to database access:

o **Database path**

You can specify the path to the **AVG DataCenter** database – either by filling in the exact path, or by browsing your system using the button.

o **DataCenter access**

The user name and password can be set for access to **AVG DataCenter**. The values are optional, but we recommend setting them up in order to increase security.

o **Database access**

The username and password for accessing the database engine itself can be set here.

o **Directory for storing station log files**

By default, all log files are stored in the AVG TCP Server installation directory, *stored_logs* subfolder. If you prefer a custom location, specify it here.

Note: Firewall Logs will not be processed during Export/Import, because they are stored outside the database (due to performance reasons).

Note: The browsing icon will not be available if you run AVG TCP Server settings from AVGADMIN.

o **Encrypted communication**

Tick this checkbox to disallow all unsecured network communication between the AVG TCP Server and workstations.

Please note! Make sure that all your workstation clients are up-to-date (AVG build 395 or newer) before ticking this checkbox. Once the encrypted communication is set, workstations with outdated AVG versions will not be able to communicate properly with the AVG TCP Server!

If you are not sure that all of your workstations in the network are properly updated, we suggest to leave this box unchecked.

The AVG TCP Server will be restarted once the change is confirmed.

o **Use transaction consistency mode**

The database transaction (read, write and other data manipulation operations) consistency checking is activated after checking on this option.

o   The *DC request log level* section defines the logging level of **AVG DataCenter** requests that were accepted and processed by **AVG TCP Server**. The logging is not active by default. *Level 1* will activate normal logging level, which records all the requests resulting in an error into the log file. The records are provided with the client's IP address, timestamp and literal text of database server response. *Level 2* will activate detailed logging. In this mode, all the client requests are recorded into the log file. This mode should be applied only when detailed diagnostics are really needed. A huge log file is generated which occupies a lot of disk space (the disk can be filled up in extreme case – this may happen when you do not wipe off the old versions of the rotating log file regularly).

c)   InetLite Tab

This tab is identical to the same tab in the Simple mode.

d)   Scheduler Tab

This tab is identical to the same tab in the Simple mode as well.

e)   AVG Managed Update Tab

Detailed description of this tab can be found in chapter 13.1 AVG Managed Update tab

f)   Client Info Tab

Detailed description of this tab can be found in chapter 13.2 Client Info

g)   Server Info Tab

Detailed description of this tab can be found in chapter 13.3 Server Info

AVG 7.5

AVG Anti-Virus Network

h) Email tab

To be able to send Graphic reports by e-mail, you need to configure this tab first.

*Note: The crucial fields to be filled are located in the **Server for sending e-mail (SMTP)** section (see below). You will be allowed to select other fields (**To/Subject/Body**) during the **Report Schedule Definition Wizard** as well. All values you will fill in now will be considered as default.*

The **Header of message** section contains these fields:

www.grisoft.com

o **To** - specify one or more e-mail addresses that the report(s) will be sent to. Separate individual items by a comma. This field can also be filled during Report Schedule definition.

o **Copy** - *An optional value.* Specify one or more e-mail addresses that the report(s) will be sent to. Separate individual items by a comma.

o **Blind copy** - *An optional value.* Specify one or more e-mail addresses that the report(s) will be sent to as a blind copy (no other recipients will see these addresses). Separate individual items by a comma.

o **From** - *An optional value.* Specify the sender's e-mail address and/or sender's name and e-mail address in angle brackets <user@address.com>

o **Reply to** - *An optional value.* Specify a reply e-mail address.

o **Subject** - enter some text to recognize the reports.

The **Server for sending e-mail (SMTP)** section contains these customizable fields:

o **SMTP server** - insert your SMTP server address (can be an IP address or domain name).

o **SMPT port** - specify the SMTP server port number. Default value is 25.

If your SMTP server requires authentication for sending e-mails, enter the login details below:

o **SMTP Login** - specify username

o **SMTP Password** - specify password

Confirm all changes of the server configuration by the **OK** button. However, the changes are applied after the server launches again with new configuration. If the **AVG TCP Server** is running, the following window will prompt you to restart the server (note that the server will be **inaccessible** for some time during the restart):
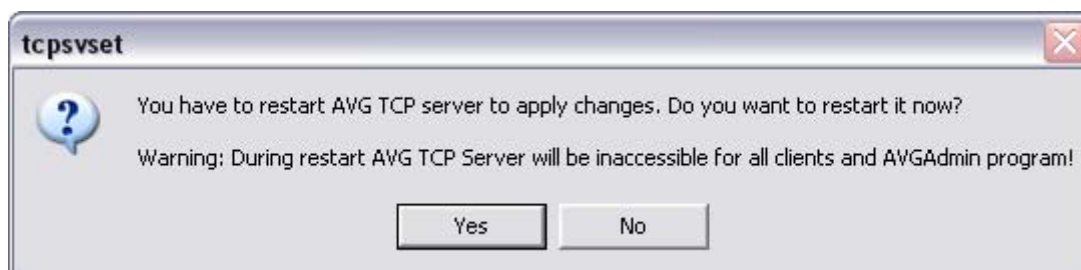
Confirm the restart of **AVG TCP Server** by pressing the **Yes** button.

6.7. Clients Connection to AVG TCP Server

AVG clients using the **AVG TCP Server** can easily connect to the **AVG DataCenter** by employing the proper URL as a communication string. The URL should be in the following form:

[http://]<address>[:port]

where

- **<address>** is the address of the server where AVG DataCenter is installed. This address can be in the form of server name or IP address/pc with the AVG TCP Server installed.

- **[:port]** is a voluntary port number. The default port number is 4156, and that refers to the default AVG TCP Server configuration.

For example if you install the **AVG TCP Server** to a computer named *myserver*, and you use the server's default configuration, the string will be in this form:

http://myserver:4156

Any valid **AVG TCP Server** address can be used; all the following syntax examples are applicable:

http://server.acme.com:4156

http://192.168.1.123:4156

http://NETWORKSRV

192.168.1.123:4156

COMPUTER:4156

COMPUTER

If you have changed the port settings to 4444 within the **AVG TCP Server** configuration *(see the previous example)*, it is necessary to change the port number in the URL set up on a client. The new URL setting will be:

http://server.acme.com:4444

http://192.168.1.123:4444

http://NETWORKSRV

192.168.1.123:4444

COMPUTER:4444

Example: *Using the installation program, the AVG TCP Server has been installed to the network computer called NETWORKSRV. After installation, no changes were carried out in the configuration file, and all settings are default. The AVG clients will connect to the AVG DataCenter by setting the remote administration connection string in the form of:* http://NETWORKSRV:4156. *No other configuration is required; the network administration has been activated by this link.*

If the AVG client has already been installed to a workstation, but is not connected to the AVG DataCenter *(e.g. because the AVG DataCenter connection string has changed)*, it is possible to change the communication string using the **AVGW** program with the **/CONNECT** parameter set in the command prompt.

If you define this parameter, the **AVGW** program will only set the new connection value, and quit. Due to this function the administrator can reconnect all AVG clients

to the new AVG DataCenter by including the following command into the login script:

AVGW /CONNECT="<connection>"

where

<connection> is the string defining the connection. The string is in the same form as the connection string set up interactively through the AVG Control Center. This string must always be inserted into quotation marks!

Applicable command examples:

AVGW /CONNECT="http://server.firma.cz:4156"

AVGW /CONNECT="http://192.168.1.123:4156"

AVGW /CONNECT="http://NETWORKSRV"

6.8. AVG TCP Server Command Line Parameters

If you need some advanced diagnostics, it is also possible to launch **AVG TCP Server** in an interactive mode (not as an operating system service). In this mode, you can use command line parameters for additional configuration settings. It is also the only accessible mode for **Windows 9x/Me** operating systems.

Command line parameters are denoted by '/' or '-' character. When a value is part of a parameter, it is typed right behind the parameter specification; space then acts as a separator. The available parameters are as follows:

install - service installation (WinNT4/2k/XP Professional only)

remove - service uninstallation (WinNT4/2k/XP Professional only)

stop - service shutdown (WinNT4/2k/XP Professional only)

ini <path> - absolute path to configuration file. File AVGTCPSV.INI in AVG TCP Server's program folder is used by default

interactive - AVG TCP Server execution in interactive mode (not as an OS service). In the Win9x/Me environment this is the default mode of execution.

Verbose - detailed output messages (makes sense only for the interactive mode)

Examples:

AVGTCPSv /ini c:\avg7DataCenter\avgtcpsv.ini

AVGTCPSv -interactive -verbose

AVGTCPSv –install

7. AVG DataCenter

The **AVG DataCenter** is a database that all **AVG clients** as well as the **AVGADMIN** program communicate with. **AVGADMIN** accesses the **AVG DataCenter** to centrally define AVG settings and system parameters. **AVG clients** connect to the **AVG DataCenter** to read the set up parameters; and to save their currently defined setting and test results.

The communication is possible only if the **AVG Anti-Virus Network Edition** component is properly installed on all workstations, and connected to the **AVG DataCenter**.

AVG DataCenter contains an implemented SQL database, or it can be attached to a separate database server running either on the same or another computer within the local network.

*Attention: Particular database engines can serve only limited number of computers connected. For example, the **Firebird** database integrated into the **AVG Anti-Virus Network Edition** installation package can server up to 150 computers. If you want to manage more computers, you have to install **Microsoft SQL Server** or **Microsoft SQL Server 2005 Express Edition** – they can server over or up to 1000 stations respectively. Use the* [AVG DataCenter Setup Wizard](#) *then to configure the selected database engine.*

7.1. AVG DataCenter Modes

The **AVG DataCenter** can run in two modes:

a)   **AVG DataCenter Monitoring Mode**

If you select the **AVG DataCenter Monitoring mode**, all centrally defined configuration settings specified by the administrator are transferred to the **AVG clients** only once (however, the shared settings are always transferred, and the end user has no possibility of editing them). Then, all **AVG clients** are allowed to modify their own configuration settings, and the configuration modifications are transferred back to the **AVG DataCenter**. The administrator is thus able to view the current configuration of all **AVG clients**. If necessary, the administrator can change the configuration at any time. Any configuration change carried out by the administrator is always prior to the **AVG client** user configuration change. However, once the administrator's new configuration is transferred to the **AVG client**, the end user is allowed to change it again.

b)   **AVG DataCenter Mandatory Mode**

If you select the **AVG DataCenter Mandatory mode** then all users are prevented from performing any changes in the **AVG client** configuration. All configuration settings defined by the administrator (using the **AVGADMIN**) are automatically transferred to the **AVG client**, and these settings overrule any user settings. The administrator can also use the **this mode** and specify exact values that will be taken as "voluntary", i.e. the end user will be allowed to change these values.

7.2. AVG DataCenter Setup Wizard

The **AVG DataCenter Setup Wizard** is launched after the installation of **AVGADMIN 7.5.** It can also be launched any time later using the *setupdc.exe* command in the **AVG TCP Server** program directory.

The *AVG DataCenter Setup Wizard* guides you through the configuration process of **AVG DataCenter** database on a selected database engine. Using the wizard, you can also configure **AVG TCP Server** in order to mirror the AVG updates in a local network. The wizard leads you through the configuration process in a few steps listed in the following overview.

Note: Navigation in the wizard is as usual:

- *The **Back** button takes you one step back in the wizard.*

- *The **Next** button takes you one step forward and also performs all actions selected in the current stage.*

- *The **Skip** button allows you to skip the action imposed by the current screen – but only when is it possible to skip an action (the button is disabled otherwise).*

- *By pressing the **Quit** button, you can cancel the wizard at any stage, discarding the changes performed so far.*

a) **Welcome**

The welcome dialog explains the main purpose of the setup wizard, and briefly describes the process of the **AVG DataCenter** configuration.

AVG 7.5
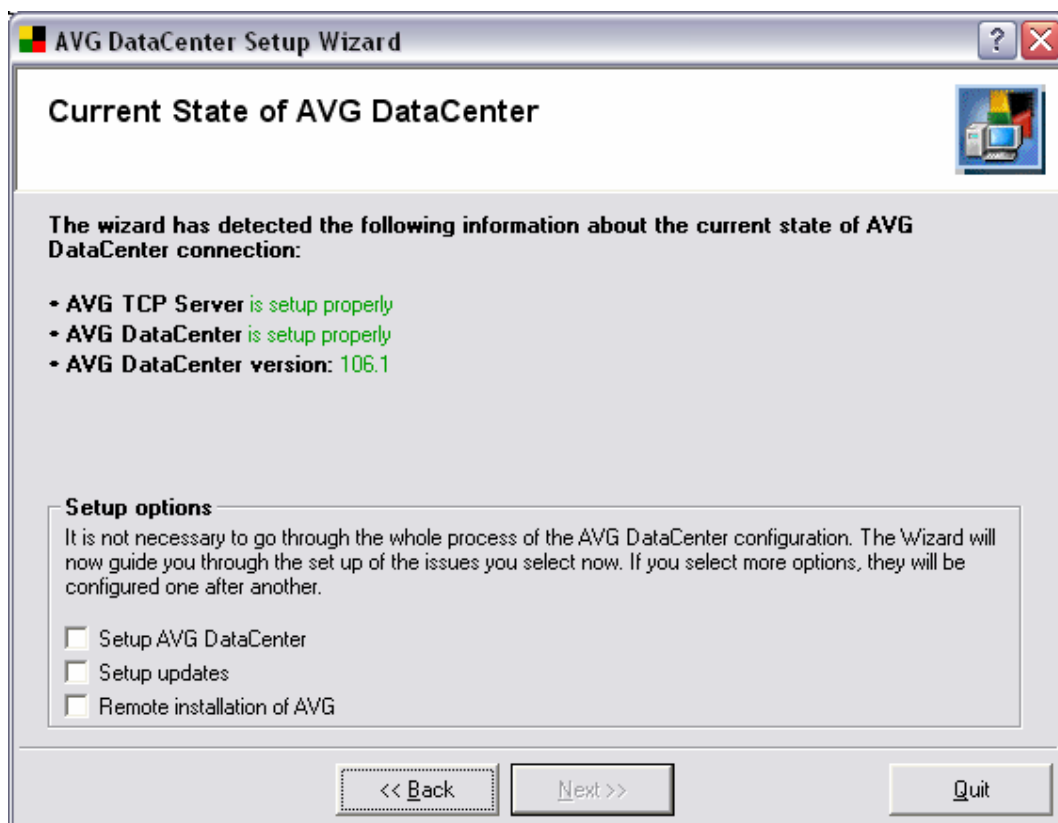
b) Current State

This screen displays information on the **AVG DataCenter** and **AVG TCP Server** current state. When everything is correct, the respective information is displayed in green color together with the **AVG DataCenter** version number.

In such case, there is no need to go through the **AVG DataCenter** configuration process again. Nevertheless the Setup Wizard will allow you to go through all processes that you choose in the **Setup options** section. If you mark several checkboxes, the Setup Wizard will configure them successively. Configuration of each step is described in the following points.

If there is any configuration problem, you will be briefly informed about the reasons, as you can see in the following picture:
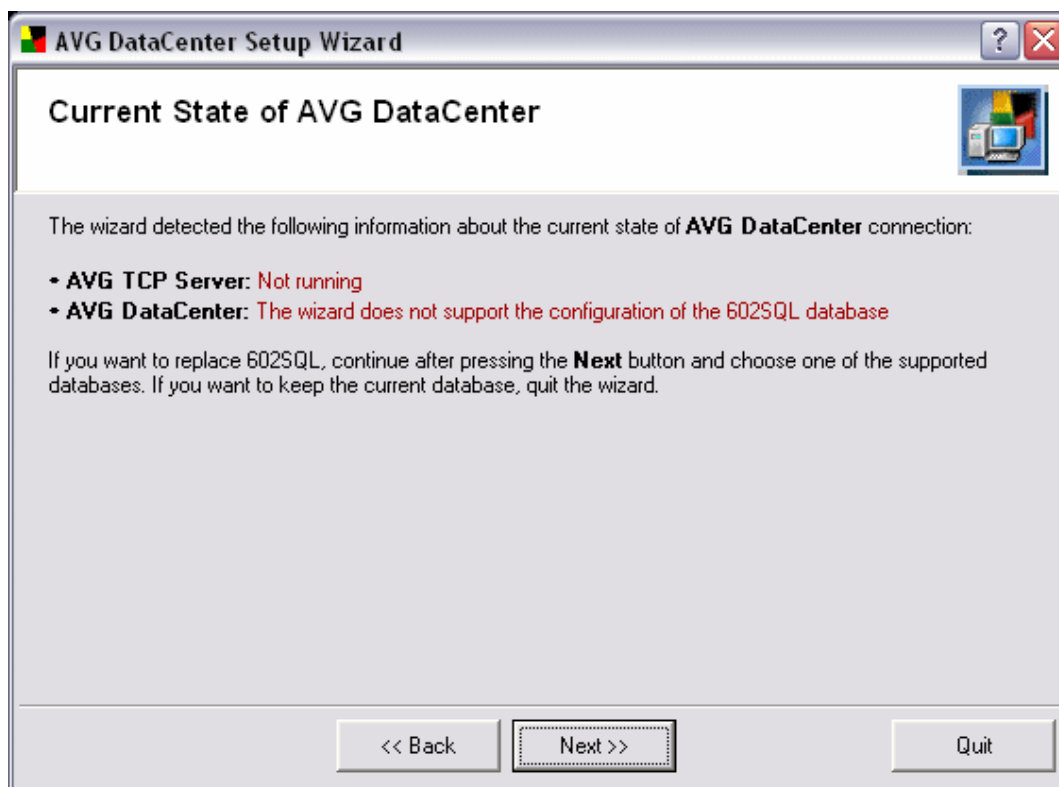
Note: *When you are using the* ***602SQL*** *database engine, which is no longer supported by* ***AVG Anti-Virus Network Edition****, it will be detected in this particular step of the configuration process. You cannot configure the unsupported database using the wizard. However, you can still keep the current settings (if functional) and terminate the wizard by pressing the* ***Quit*** *button here. If you want to replace the database, in the next step you may choose one of the supported engines.*

If **AVG DataCenter** is set up properly and you are content with the performance of **AVG Anti-Virus Network Edition**, you can quit the wizard here (using the *Quit* button). Otherwise continue by pressing the *Next* button.

Alternatively you may experience for example the following dialog:
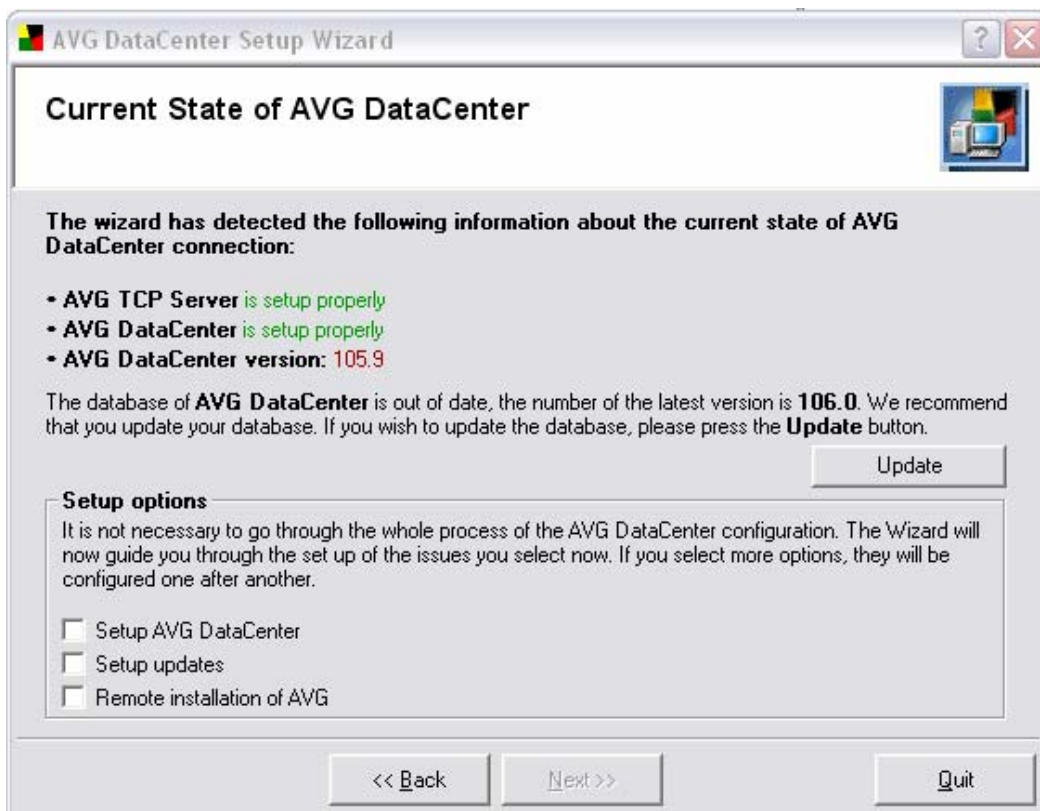
In this case we recommend to click the *Update* button to get the **AVG DataCenter** automatically updated. The update process is done instantly.

AVG 7.5

AVG Anti-Virus Network

c) AVG DataCenter Selection
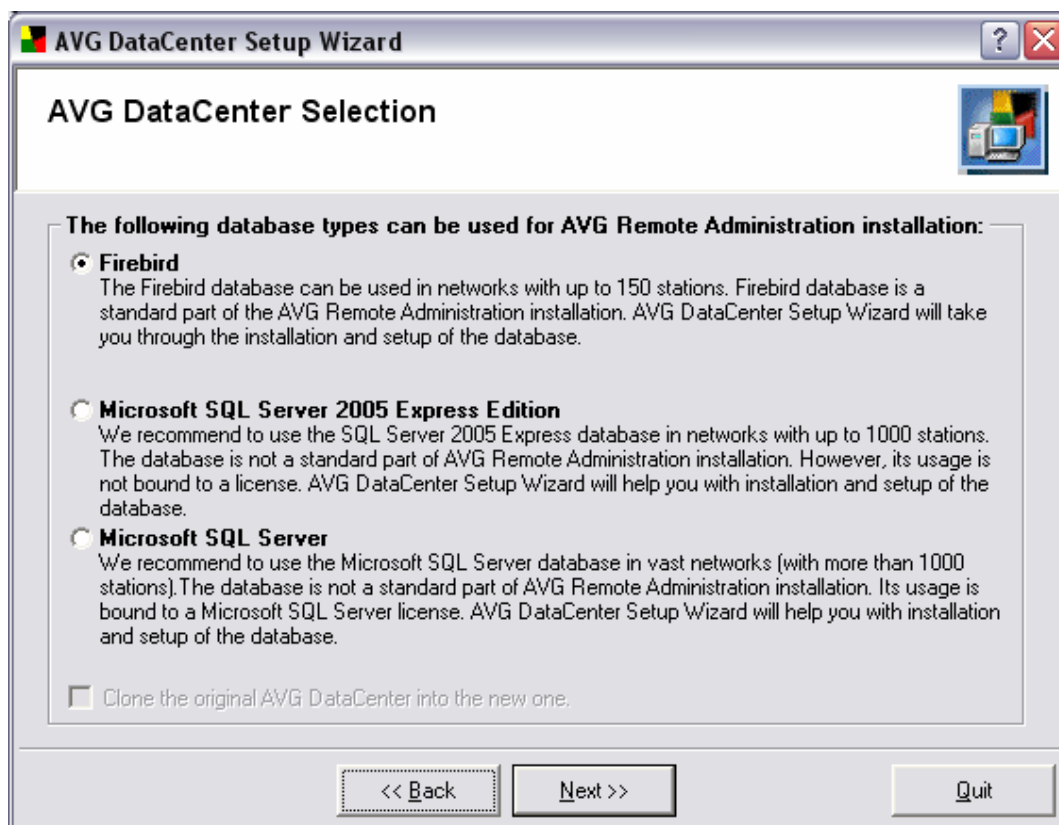
Select the database corresponding to your needs. Three options are available:

o   ***Firebird***

The solution is appropriate for smaller networks with up to 150 computers. The database is a standard part of **AVG Anti-Virus Network Edition**.

o   ***Microsoft SQL Server 2005 Express Edition***

A reduced version of the **Microsoft SQL Server**, it can serve up to 1000 computers. The product is not a standard part of **AVG Anti-Virus Network Edition**. Its usage is not limited by any license.

o   ***Microsoft SQL Server***

This engine can serve over 1000 computers in large networks. It is not a standard part of **AVG Anti-Virus Network Edition** and its usage is bound to the Microsoft SQL Server license.

If you choose a database type other that is different to the one you have been currently using, the Setup Wizard can automatically convert the contents of the current AVG DataCenter into the newly chosen database type.
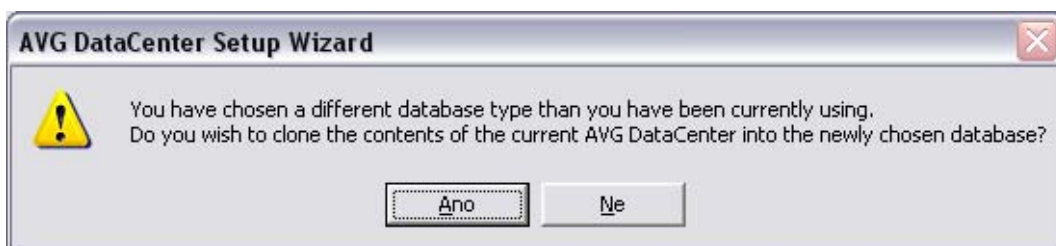
*Note: If you have not checked the **Firebird database** component during the installation of the **AVGADMIN 7.5** product, the **Firebird** option in this window is disabled. If you want to configure Firebird database, you must quit the wizard and reinstall **AVGADMIN 7.5** with the Firebird database support!*

When the number of computers exceeds the server limit, it is suitable to split the load among several isolated **AVG DataCenters** running on more computers.

If you have selected the ***Firebird*** option, continue to another stage of the wizard.
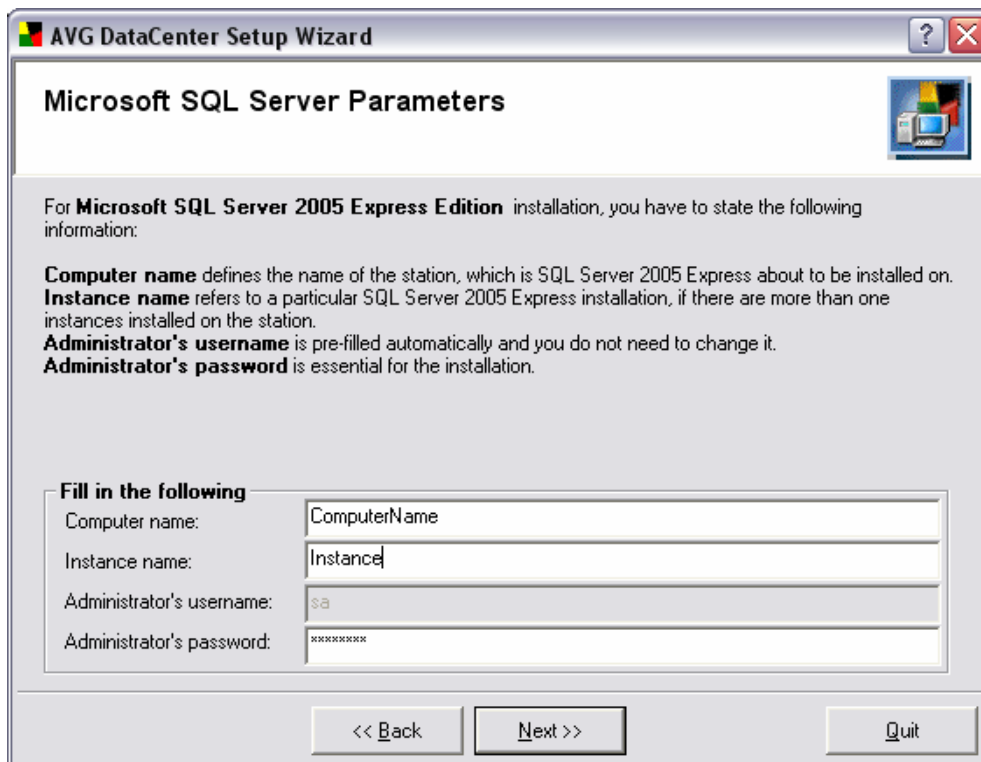
If you have selected the **Microsoft SQL Server** or **Microsoft SQL Server 2005 Express Edition** option, you will be prompted to perform additional actions according to the following:

o   **Installation/Configuration of SQL Server 2005 Express**
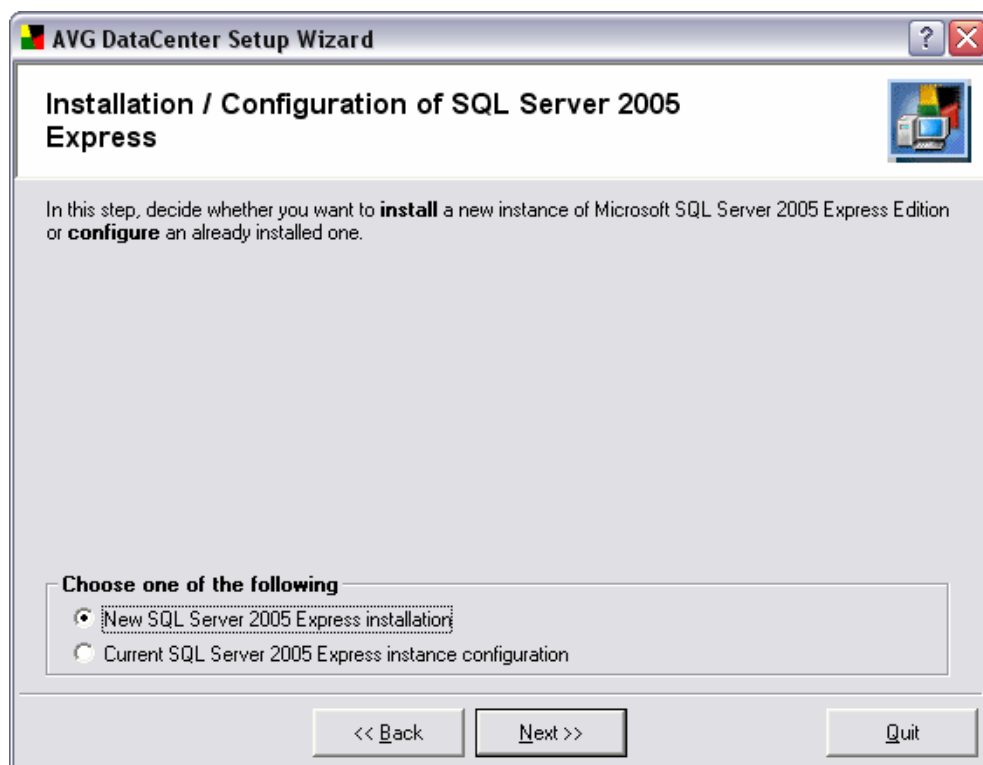
Choose whether you want to *install* **AVG DataCenter** on a new instance of Microsoft SQL Server, or to *configure* an already installed instance of Microsoft SQL Server. Select the respective option in the ***Choose one of the following*** section of the dialog window, and continue by pressing the ***Next*** button.

AVG 7.5

**AVG Anti-Virus Network**

o **Microsoft SQL Server Parameters**

If in the previous dialog you chose **New SQL Server 2005 Express Edition installation**, you will be asked to fill in the following information:

– *Computer name* – defines the name of the station, which is SQL Express Edition about to be installed on

– *Instance name* –refers to a particular SQL Express Edition installation, if there are more than one instances installed on the station.

– *Administrator's username* – predefined automatically, you do not need to change it

– *Administrator's password* – password for the database administrator

Continue to the next screen by pressing the *Next* button

AVG 7.5

AVG Anti-Virus Network

o   **Microsoft SQL Server 2005 Express Edition Installation**
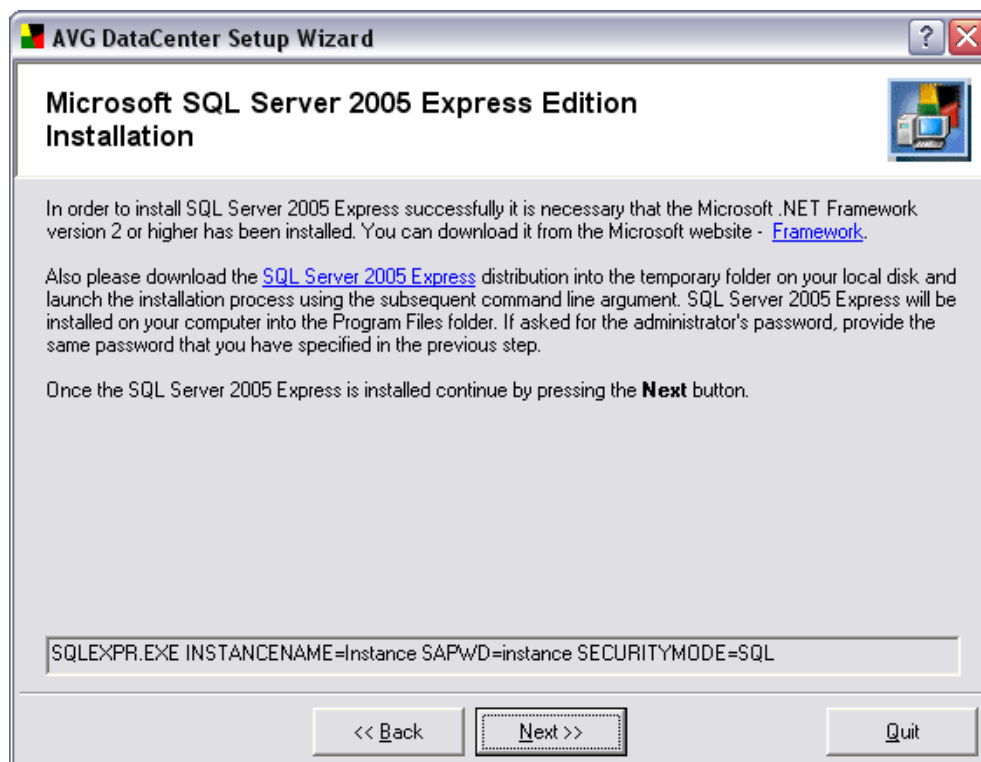
If you do not have **Microsoft SQL 2005 Express Edition** installed on your computer yet, you will need to install it now. In order to install SQL Server 2005 Express Edition properly, you need to download and install Microsoft .NET Framework version 2.0 or higher. You can download it from the Microsoft web site.

After successful installation of .NET Framework, please download the installation package of SQL Server Express Edition from the Microsoft web site:
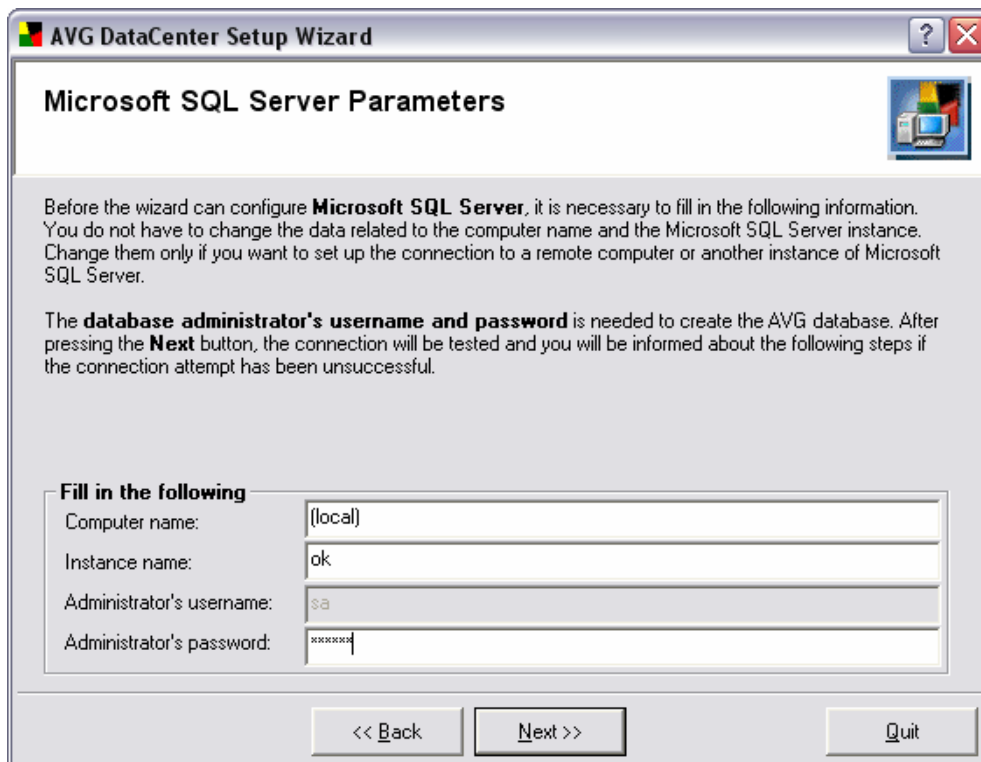
http://www.microsoft.com/downloads/details.aspx?familyid=220549b5-0b07-4448-8848-dcc397514b41&displaylang=en and save it to some temporary directory. Then launch the installation using the command indicated below (example)

SQLEXPR.EXE INSTANCENAME=Instance SAPWD=instance SECURITYMODE=SQL

The above string is only an example of such a command. For correct installation please copy the string displayed in your specific Setup Wizard window!

As soon as the MS SQL Server Express installation is finished, continue to the next step - Preparing AVG DataCenter - by pressing the **Next** button.

o **Microsoft SQL Server parameters**

If you have chosen in dialog <u>Installation / Configuration of SQL Server</u> <u>2005 Express</u> **Current SQL Server 2005 Express instance configuration**, you will be asked to fill in the following details:

In this stage of the wizard, you have to fill in the correct parameters needed to perform administration actions on an instance of Microsoft SQL Server:

– *Computer name* – the name of the computer where the database engine is running

– *Instance name* – the name of the engine instance that is supposed to host **AVG DataCenter**

– *Administrator's name* – the database administrator's name

– *Administrator's password* – the database administrator's password

Continue by pressing the *Next* button.

AVG 7.5

AVG Anti-Virus Network

d) Preparing AVG DataCenter
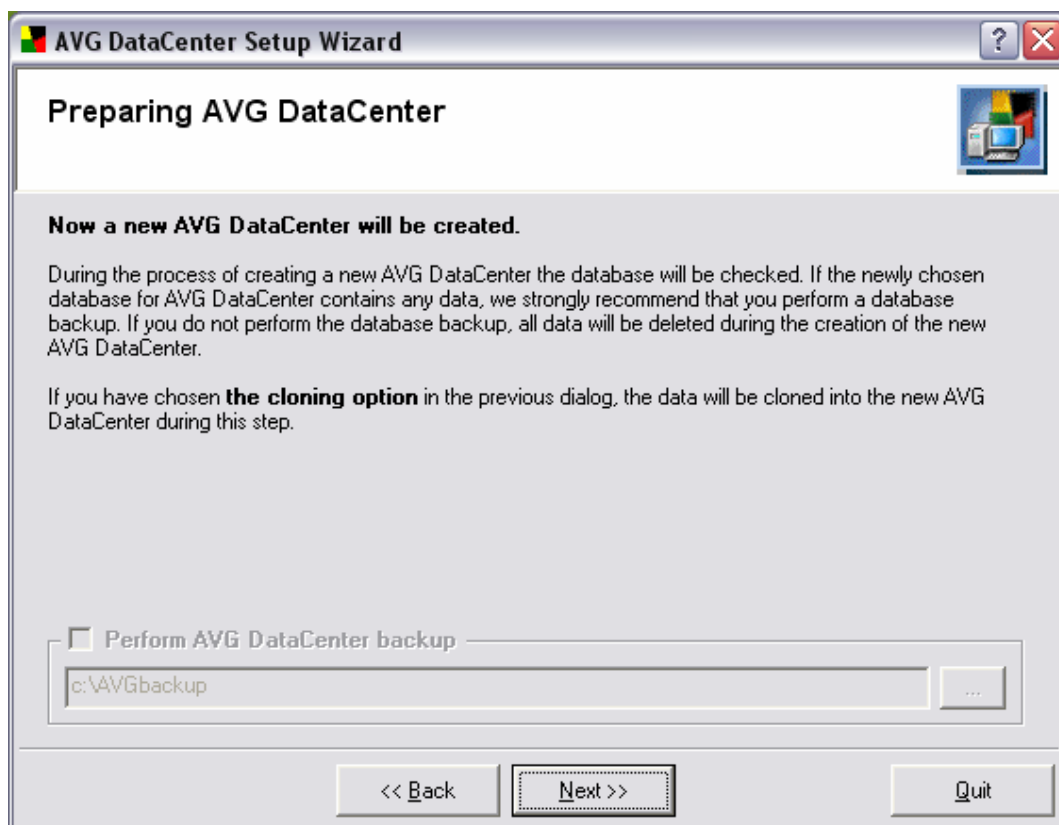
This dialog informs you that an empty **AVG DataCenter** database will be created using the selected database engine. If it does exist, the old database will be replaced.
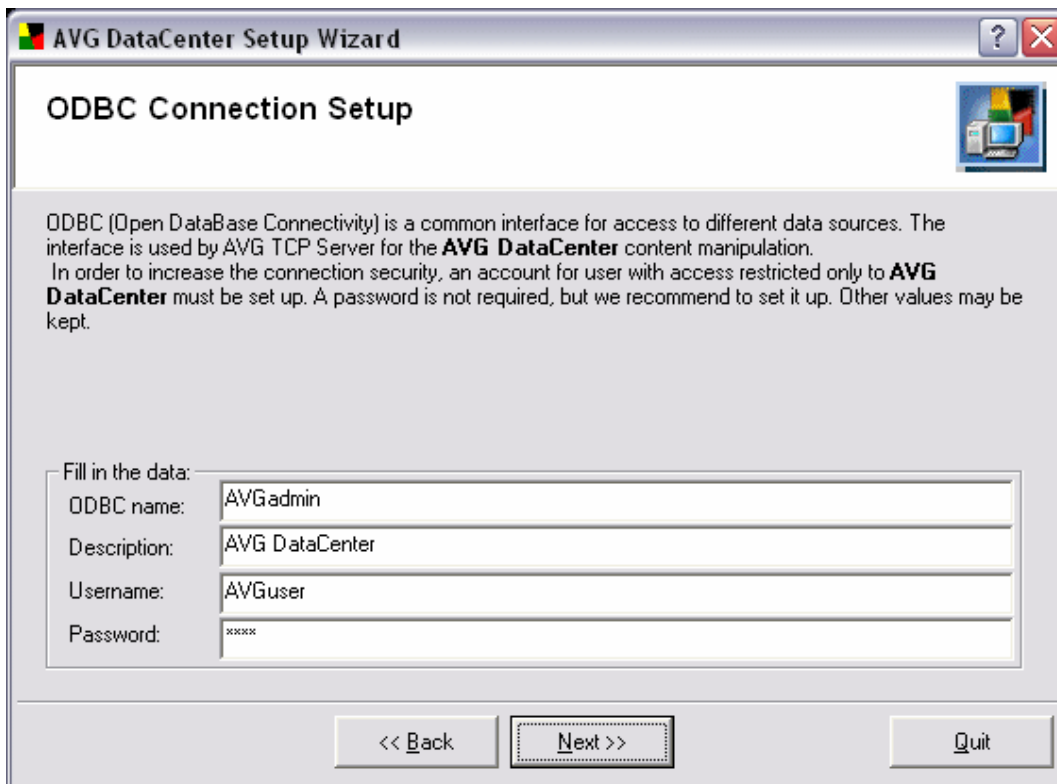
When an existing **AVG DataCenter** *modified* database has been detected on the computer, this dialog window of the wizard prompts you to create a backup of the database. When there has been no **AVG DataCenter** database detected, or when the database is clear (this means that neither **AVGADMIN** nor an **AVG client** have accessed the database) the Backup part of the screen will not be accessible.

You may lose important data when replacing the old database, so it is recommended *not to skip* the backup!

In the **Perform AVG DataCenter backup** field you can optionally specify any directory (other than default) for the database data backup. Either enter the path directly, or browse your disk to select the desired directory using the

[...] button on the right side of the editing field.

If you want to keep the present version of **AVG DataCenter** in the current database, you can leave this step out - use the *Skip* button. If you want to create a new empty database continue by pressing the *Next* button.

e)   ODBC Connection Setup

Note: *This dialog comes after you have chosen* **Current SQL Server 2005 Express instance configuration** *or* **New SQL Server 2005 Express installation** *on an instance of Microsoft SQL Server.*

You have to fill in the correct parameters for ODBC connection here:

o   *ODBC name* – the name of the **AVG DataCenter** connection

o   *Description* – the description of the connection

o   *Username* – the username for the **AVG DataCenter** database access

o   *Password* – the password for the **AVG DataCenter** database access

Continue by pressing the *Next* button.

f) Mirroring of Update Files
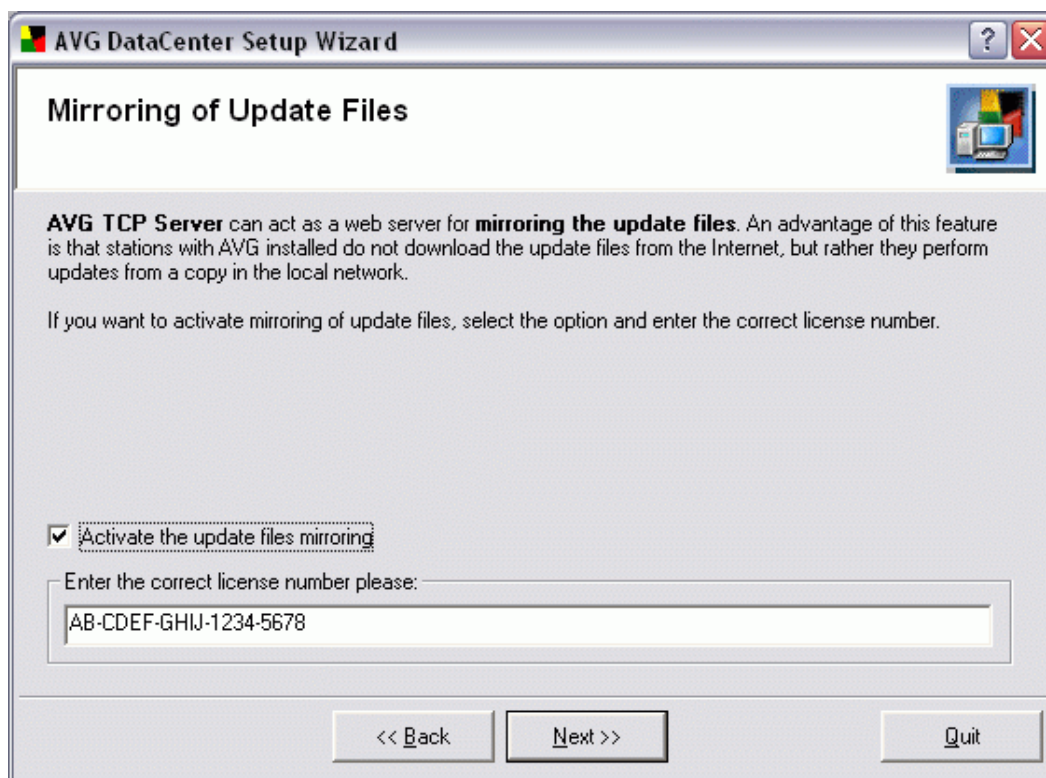
In this dialog you can switch on the update files mirroring feature – mark the **Activate the update files mirroring** option. Then you have to provide a valid **AVG Anti-Virus Network Edition** license number.

If you decide to mirror update files, your **AVG TCP Server** will be able to download the update files at once and distribute them from a folder in your local network directly to your AVG clients.

Note: We have some recommendations regarding update mirroring – for mission critical systems we suggest to distribute the recommended level updates after they have been successfully tested in a secure environment. For other systems we recommend to distribute an update when it is available.

If you switched the update files mirroring on, you will have to specify a few things in the next two steps after pressing the **Next** button.

If you do not want to mirror updates, do not check the respective field and continue to this dialog by pressing the **Next** button.

AVG 7.5

AVG Anti-Virus Network

o **Update Files Folder**
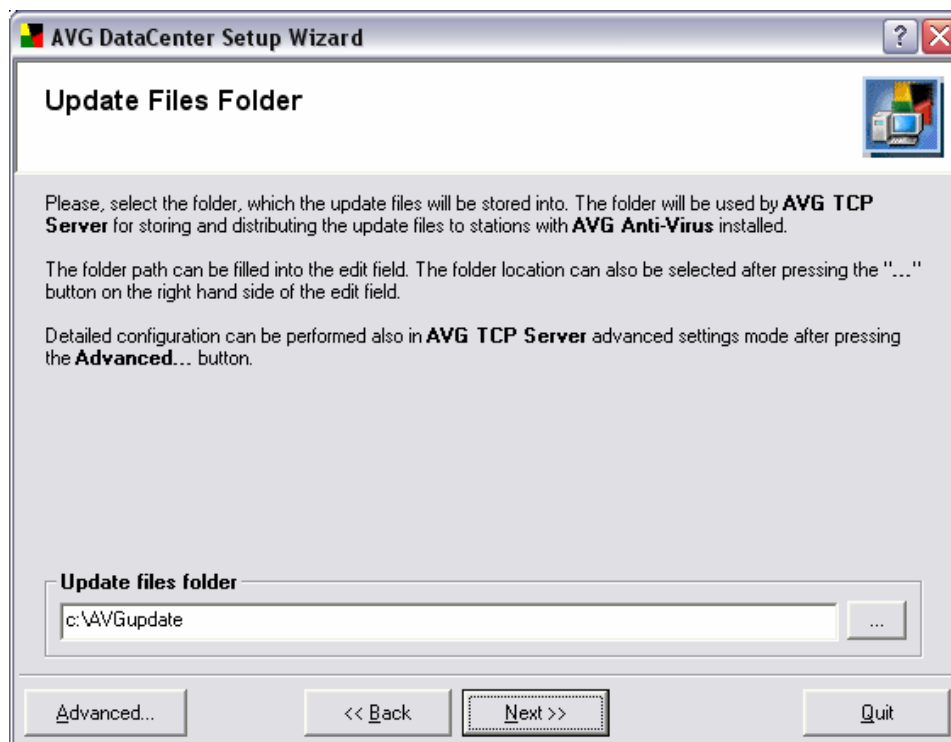
Select the local folder where the downloaded update files will be stored.

Enter the full path to **Update files folder field**, or use the [...] button to locate the appropriate folder in your hard drives' directory structure.

Continue by pressing the **Next** button.

AVG 7.5

AVG Anti-Virus Network

o **Interval of New Update Availability Checks**
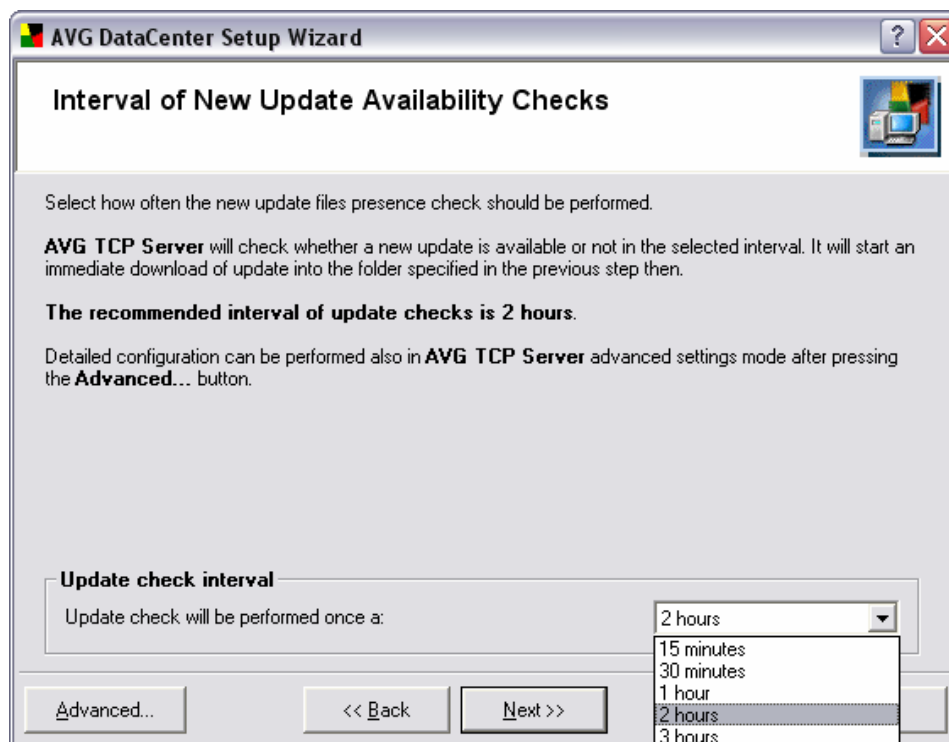
You can select an interval for **AVG TCP Server** to verify whether there are new updates available. Choose the period in menu of the *Update check interval* item.

Note: *The recommended interval of update checks is 2 hours in general.*

More specific options regarding the update check period can be specified in the Advanced mode – press the *Advanced...* button in the left down corner of the dialog to open the following new window:

AVG 7.5
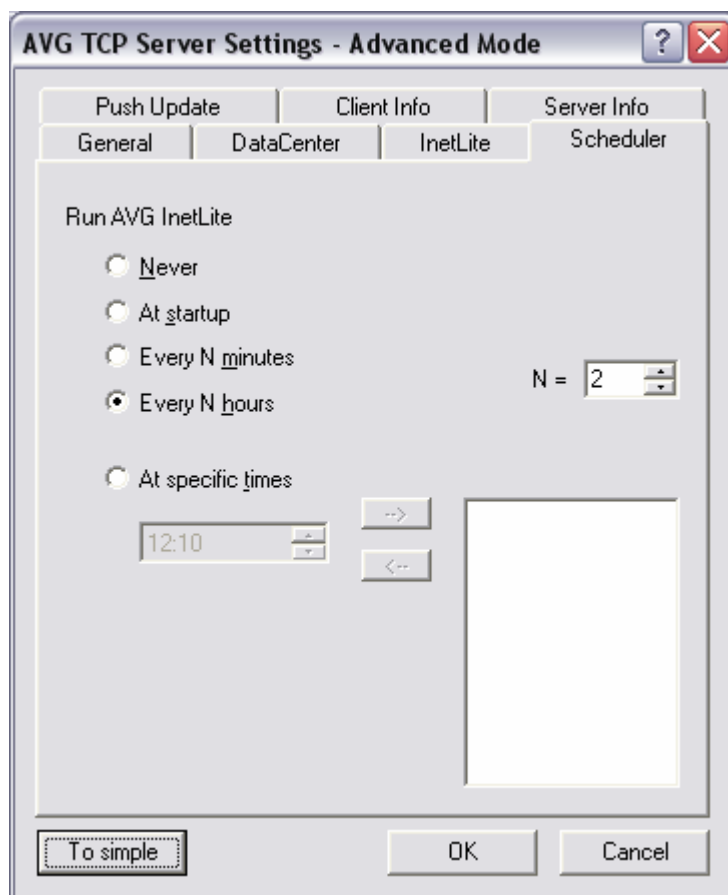
You can choose from these update interval options in the window:

- *Never* – never check for updates

- *At startup* – check for updates at every startup of **AVG TCP Server**

- *Every N minutes* – check for updates every N minutes; N can be set in the field on the right

- *Every N hours* – check for updates every N hours; N can be set in the field on the right

- *At specific times* – check for updates at times specified in the field below; more times can be specified and set by moving them into the box on the right side, using the [-->] button (use the [<--] button to exclude the selected time from the set of update-check times)

Confirm your choice and close the window by pressing the **OK** button here. The selected interval option is now present in the *Update check interval* combo box, so you can choose it there (if it is has not been selected automatically yet).

AVG 7.5

o   **Update servers setup**
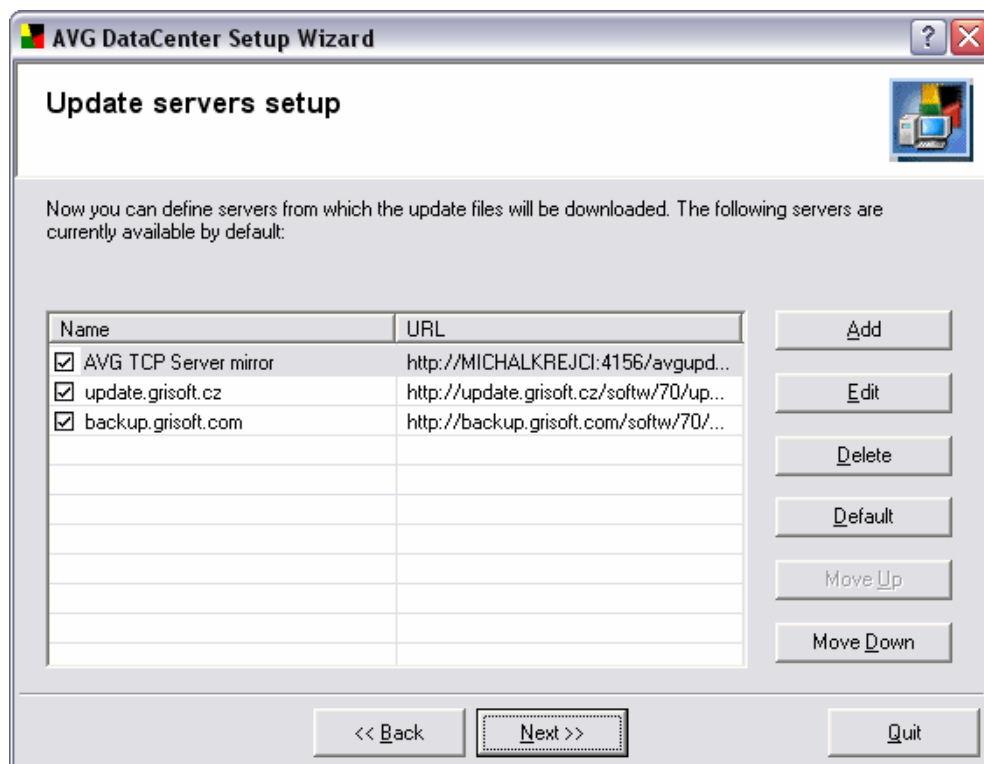
In this window you can define update server addresses from which the update files will be downloaded.

Press the **Add** button to define additional update servers.
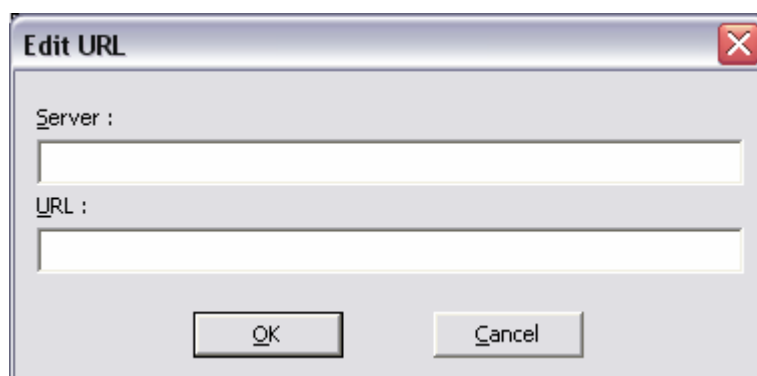
The following buttons are available too:

–   **Edit –**for changing the address or name of the selected server

–   **Delete** – for deleting selected server address

–   **Default** – for setting the server addresses to default values

Move up/Move down– will move the chosen server address one field up or down. **AVG DataCenter** will contact the servers in the selected order.

GRISOFT

g)   Remote AVG install
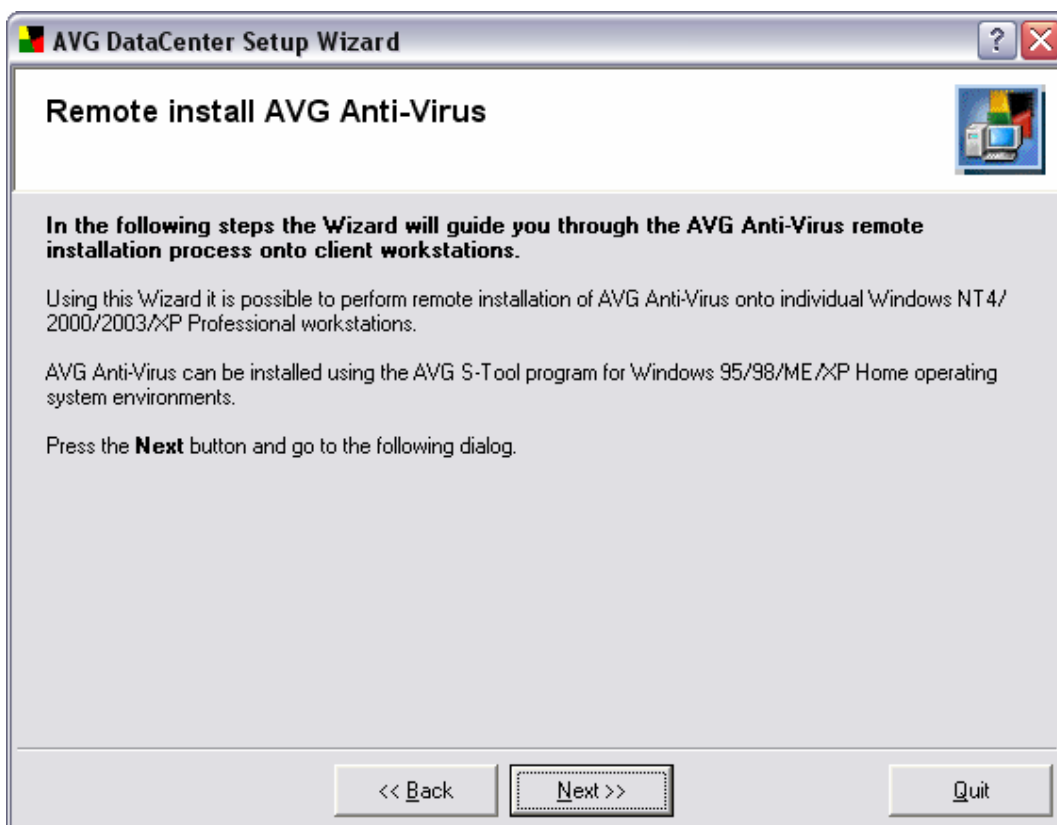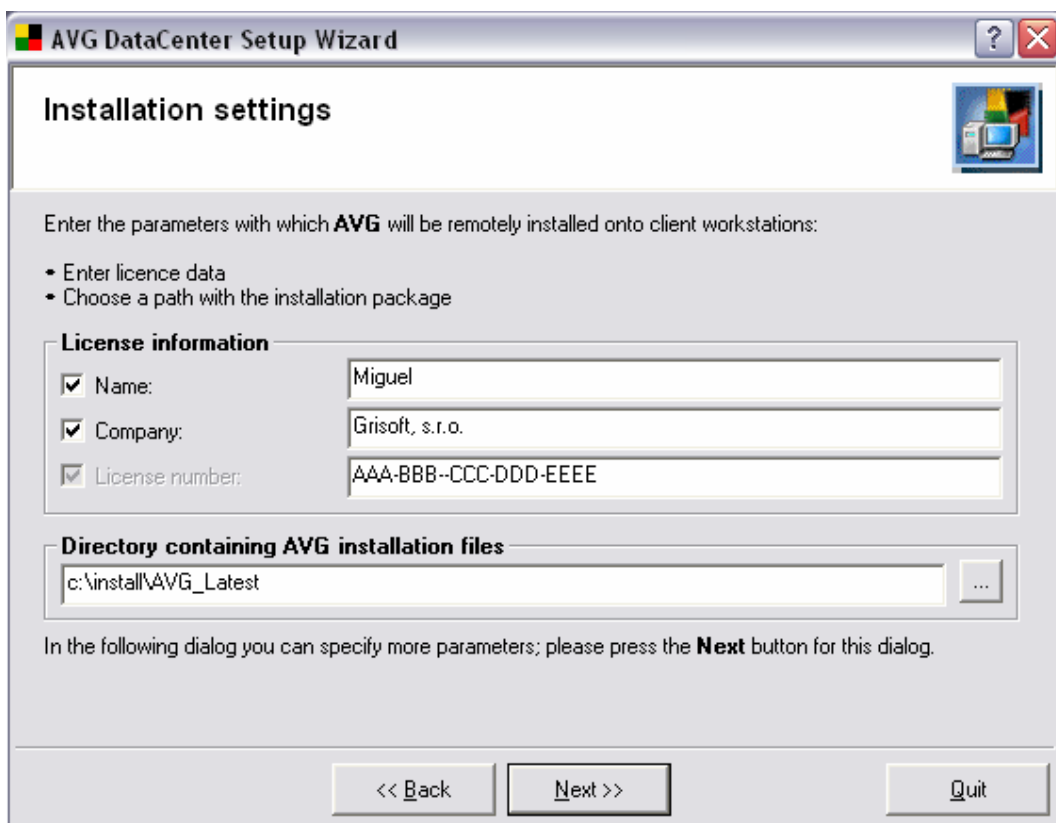
In the following steps the Wizard will guide you through the AVG remote installation process onto client workstations/servers.

Using this Wizard it is possible to perform remote AVG installation onto individual Windows NT4/2000/2003/XP Professional workstations.

If you use Windows 95/98/ME or XP Home operating system, you can use the AVG S-Tool application for installation.

Press the **Next** button to continue to the next step.

h)   Installation settings

In this dialog, please fill in the requested fields – **Name**, **Company** and **License number**. Also choose the Directory containing AVG Installation files (these will be used for installation on the target stations).

AVG 7.5

AVG Anti-Virus Network
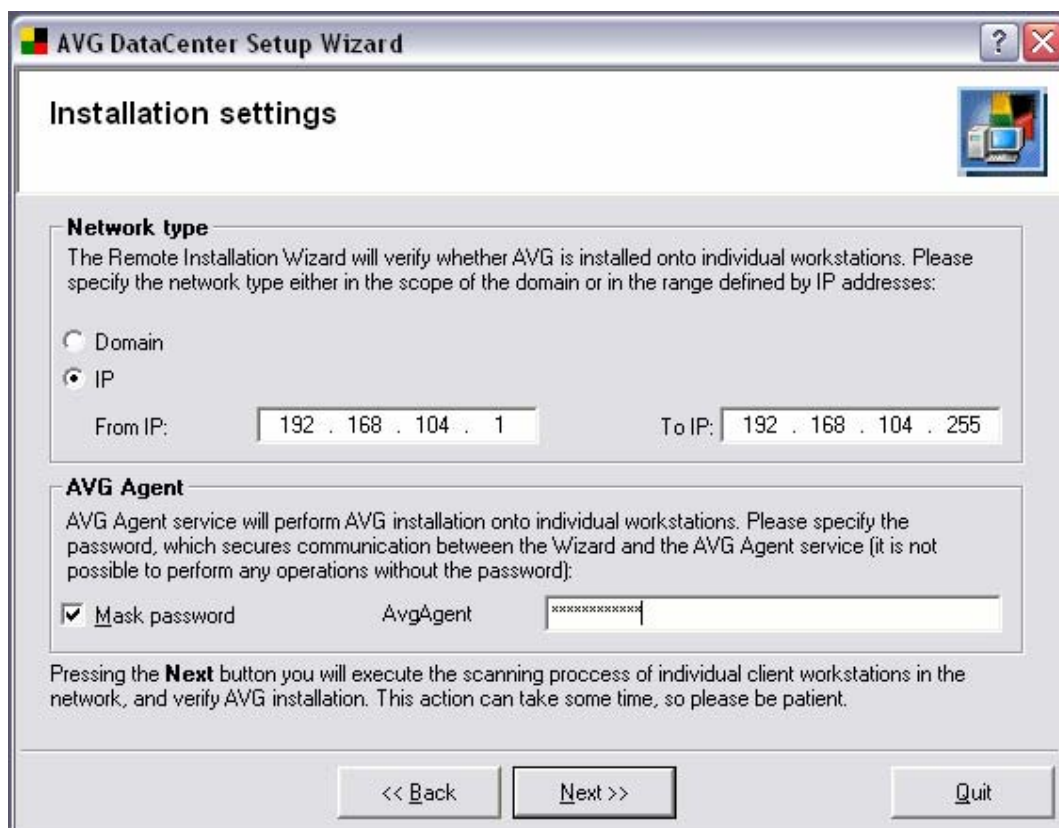
The AVG DataCenter Setup Wizard will now verify whether the AVG application is installed on the individual stations in the network.

In the **Network type** section choose which kind of network you are actually going to check. You can choose either all stations inside the **Domain** or a specific **IP** range.

AvgAgent is a service allowing AVG installation onto individual workstations. We recommend choosing a password, which will secure communication between the Wizard and the AvgAgent service (as it is not possible to perform any operations without the password).

Press the **Next** button to start scanning selected client workstations in the network. Please note that this action may take some time.
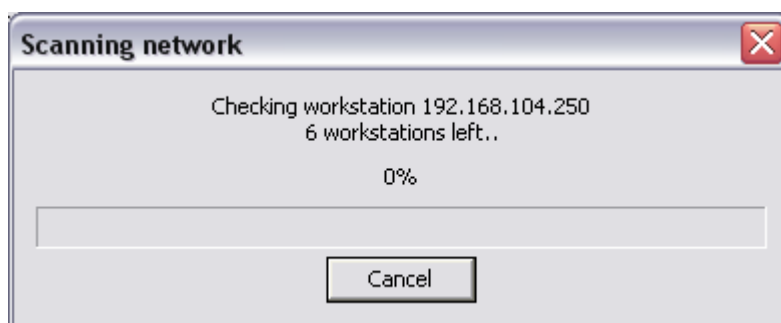
System will check during the network scanning process, whether there is AVG installed on the found stations or not.

i)   Installation
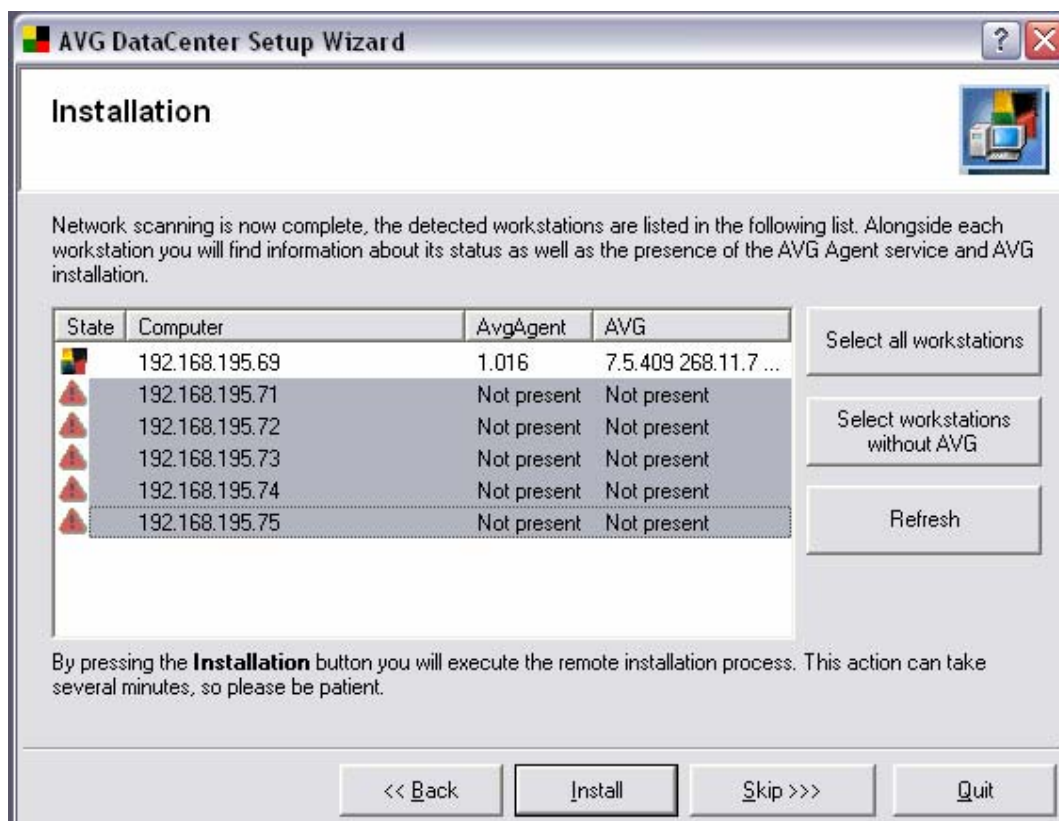
As soon as the scanning process is finished, the list of checked stations will be displayed. You can see details about every station – if **AvgAgent** service and AVG are installed including the exact version information.

To quickly select all stations, onto which you want to install AVG to, you can use the following buttons:

o   **Select all workstations –** will automatically choose all workstations.

o   **Select workstations without AVG –** will automatically choose all workstations without AVG installed.

o   **Refresh –** will scan the whole network again and display the results. This may take a while.

You can also manually select stations for installation also by clicking one or more items in the list.

After selecting all stations requested for installation, click the **Install** button.

If you are not going to install AVG right now, choose the **Skip** button to skip the process.

AVG 7.5

AVG Anti-Virus Network

j)   Configuration summary

In the last dialog of the **AVG DataCenter Setup Wizard**, there is an overview of all specified settings. You can change the configuration of any parameter in the respective dialog window that you may enter via the *Back* button.

If the configuration is correct press the *Finish* button to complete the wizard.

7.3. AVG DataCenter Mode Configuration Wizard

This can be run within the **AVGADMIN** environment by selecting the menu option *Program/DataCenter mode*.

When you first use the *Program/DataCenter mode* option, the **AVG DataCenter Configuration Wizard** is launched automatically. From the **AVG DataCenter Configuration Wizard** you can switch to the customized **AVG DataCenter** settings dialog using the *Custom settings* button *(for further information on the Custom settings dialog please refer to chapter).*

Then, you can get back to the **AVG DataCenter Configuration Wizard** by pressing the *Wizard* button.

The **Wizard's** control buttons (accessible from every dialog Windows) are as follows:

www.grisoft.com

AVG Anti-Virus Network

- **Custom Settings** – opens the <u>AVG DataCenter Mode Settings</u> dialog

- **Next** – go on in **AVG DataCenter** configuration

- **Cancel** – close the Wizard without applying the set parameters

- **Back** – return to the previous screen

a) **Welcome Screen**

AVG 7.5

AVG Anti-Virus Network
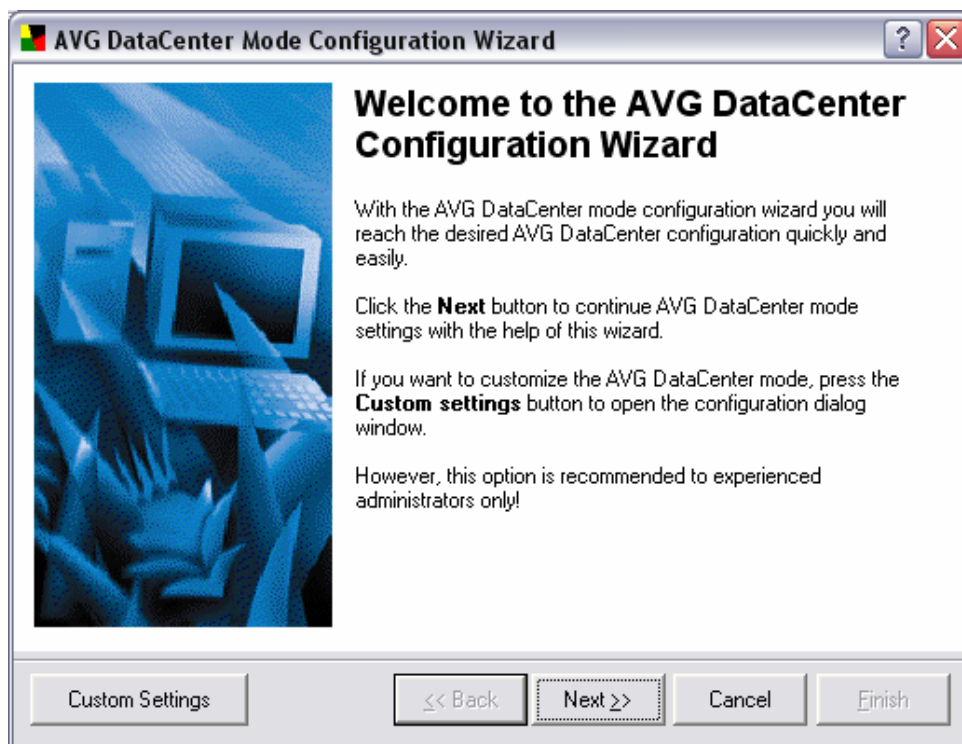
b)   Select AVG DataCenter Mode
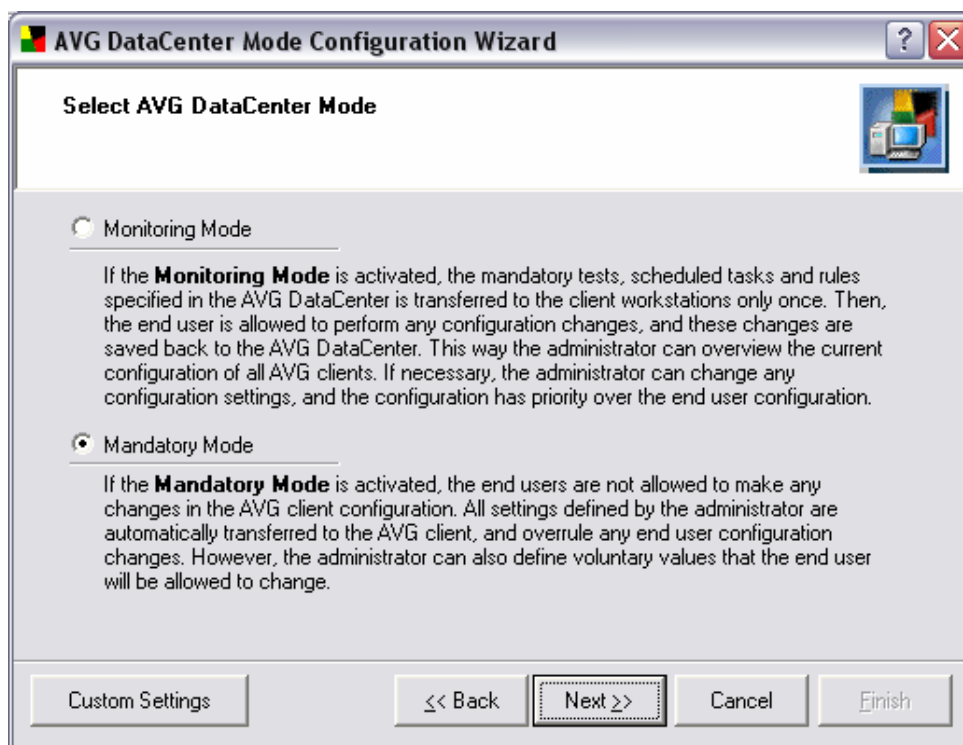
o   The *Monitoring Mode* allows the users to change the AVG client configuration after the initial transfer of administrator configuration specified in the AVG DataCenter has been performed. All changes made by users are then saved back into the AVG DataCenter.

o   The *Mandatory Mode* does not allow the end users to make any changes in the AVG client configuration – any user configuration settings are always overridden by the administrator settings. However, the administrator can define voluntary values that can be changed by the end users as well.

c)   After Selecting the AVG DataCenter Mode

o   If you have selected the **_Monitoring Mode_**, the following screen is
shown in the wizard:
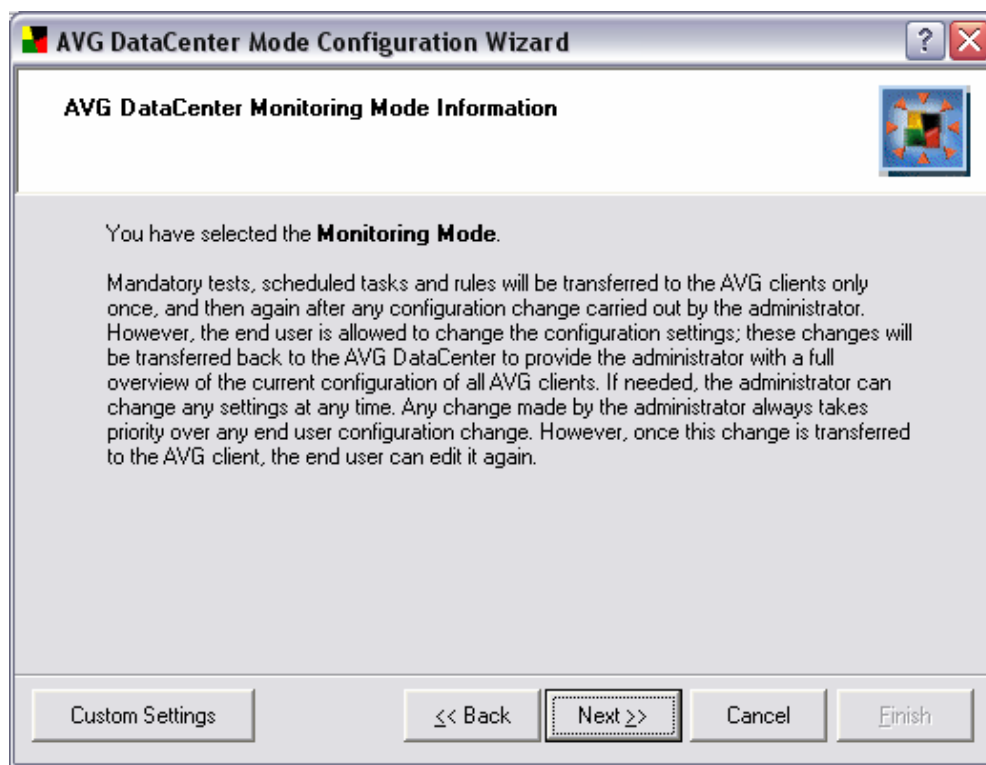
In the screen you will find additional information about the **Monitoring
mode**. Press the **_Next_** button to continue the wizard – you will get to
screen d) - Deleted Records Display. From that section on the wizard
progress is the same for both AVG DataCenter modes.

o   If you have selected the *Mandatory Mode*, the following screen is shown in the wizard:
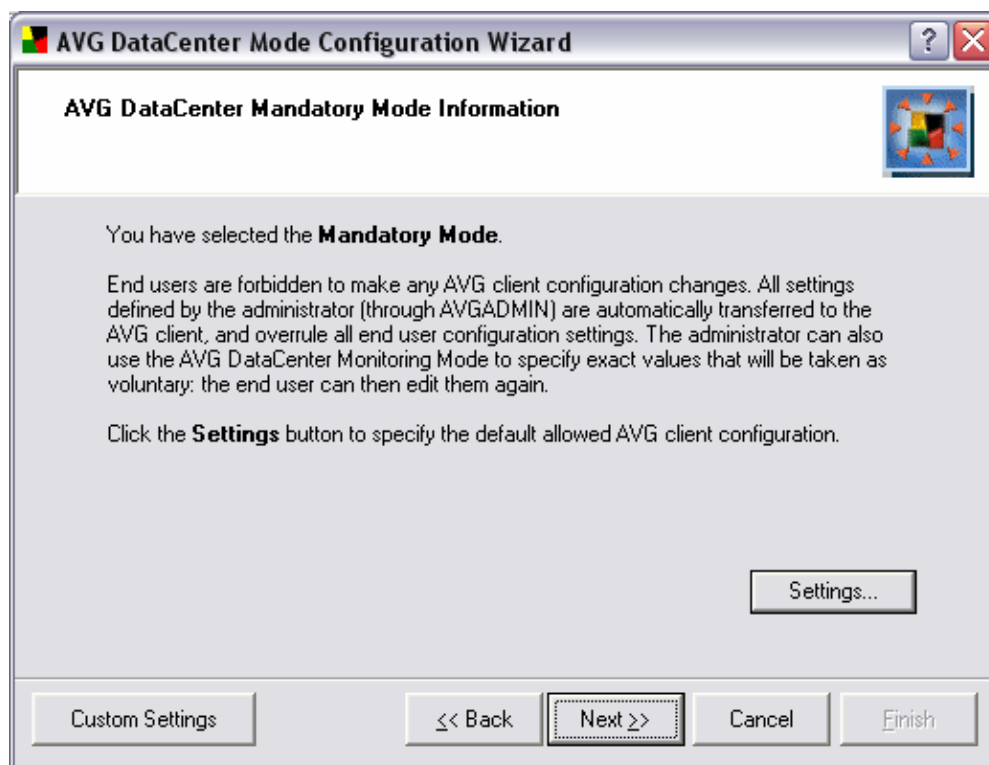
In the screen you will find additional information about the **Mandatory mode**. Press the *Settings* button to open the *Administrator options* window:
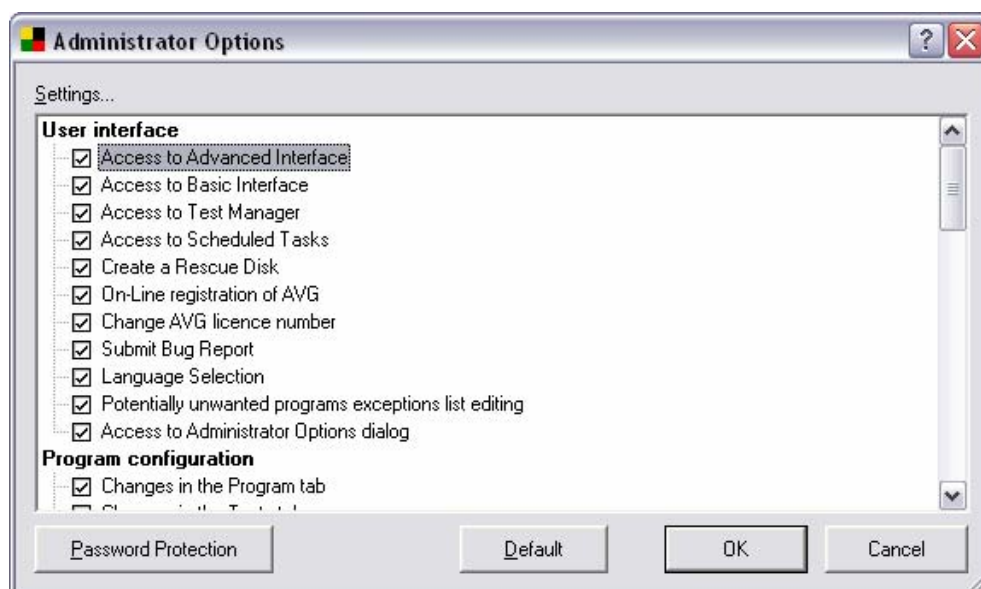
You can allow or restrict (or password protect) the particular AVG client settings options to be edited by the end users.

Press the **Next** button in the **AVG DataCenter Mandatory Mode Information** window to continue with the wizard onto the following **Configuration Reset** window:
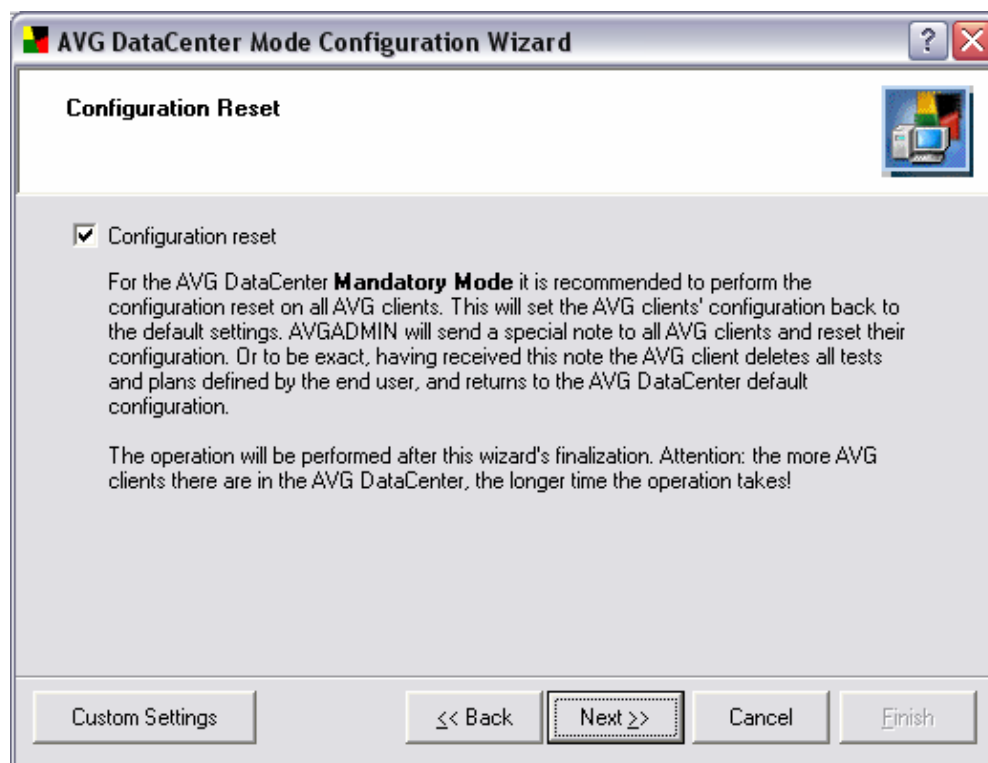
If you select the **Configuration reset** option, all AVG client settings will be reset and returned to the default configuration specified in the AVG DataCenter. This option is recommended within the Mandatory Mode.

Press the **Next** button to continue with the wizard as described in the following paragraphs. From now on the progress is common for both AVG DataCenter modes.

d)   Deleted Records Display

In this dialog you can enable or disable the option of hiding records marked as deleted. If this option is activated (by default), then plans/tests marked as **to be deleted** (X parameter) will not show up. That of course does not mean that plans/ tests marked as **to be deleted** do not exist – they are only hidden!

(For details on this option configuration you may want to see chapter 7.3 – AVG DataCenter Mode Setting – In the configuration dialog.)

AVG 7.5

AVG Anti-Virus Network

e) **Station and User Names Saved As …**

The **Station and User Names Saved As** dialog allows you to enable or disable converting user names to uppercase.

The user names can be saved in the AVG DataCenter in the exact form every single user uses to log in, or they can be transferred to uppercase. By selecting this option, all user names are automatically transferred to capital letters. Then, if there is a user name saved in the AVG DataCenter several times with the only difference of lower/uppercase, through selecting this option you can discover such duplication, and remove it. Finally every username will be saved just once.

(For details on this option configuration you may want to see chapter 7.3 – AVG DataCenter Mode Setting – User Administration.)
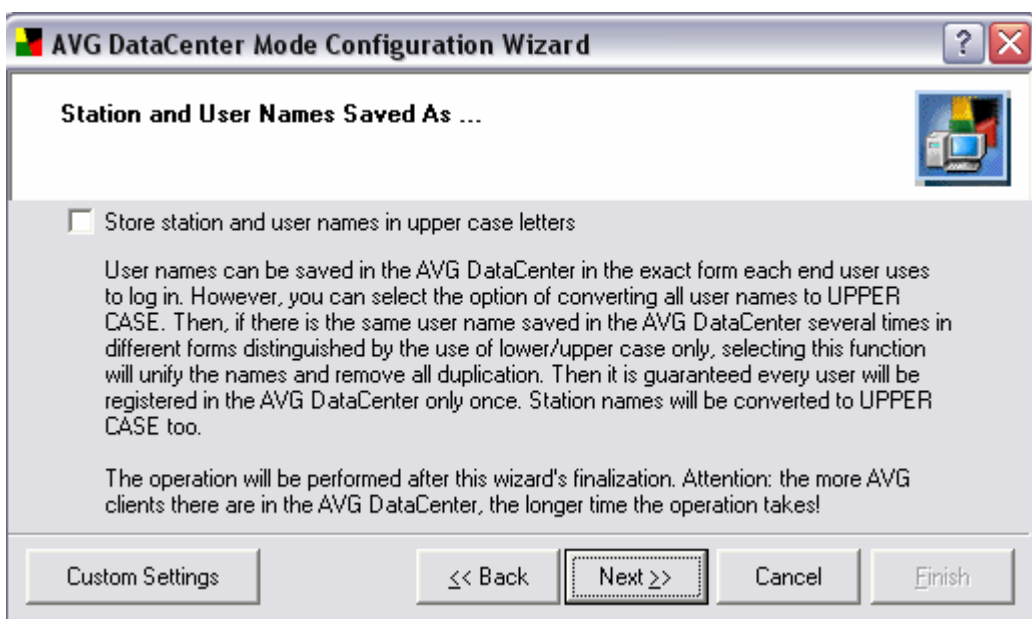
f) **Distinguish Users by Computer/Domain Name**

You can also distinguish users by their computer or domain name.

GRISOFT

If the option is not active (by default), a username is saved in the database. If activated, every username is saved with the name of its respective computer name/domain name. Under the condition that all AVG DataCenter accessing users in the network have their own unique name, it is not necessary to apply this option. Otherwise (if there are at least two users with the same name, and they can only be distinguished by their respective domain), you should apply this function.

(For details on this option configuration you may want to see chapter 7.3 – AVG DataCenter Mode Setting – User Administration.)
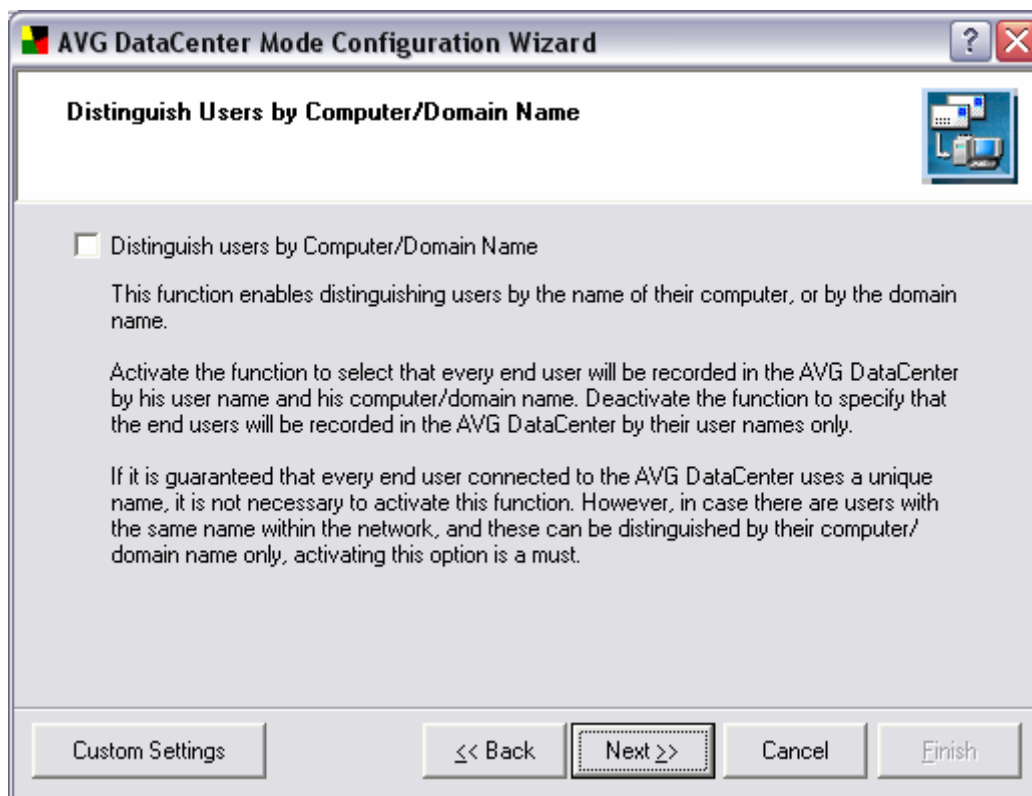
g) User Plans/Tests Settings

This option controls whether the tests/plans are scheduled for stations only (the option is inactive) or both for stations and users (the option is active).

Generally, for a network with strict administration rules, e.g. the administrator wants to have a comprehensive overview of the AVG clients' settings, it is recommended to maintain the test/plan schedules for workstations only. If the network rules are more benevolent, you may want to maintain the test/plan settings for stations and users.

If you activate the mode with neither user tests nor the plans included into the remote administration, the default preset test/plan schedules will automatically be forbidden on all workstations. If you decide to define tests/plans for workstations only, it is of course necessary to define the respective tests/plans for all workstations. The easiest way is to define the tests/plans within the shared settings, so that all workstations newly

connected to the AVG DataCenter will automatically take this obligatory configuration.

(For details on this option configuration you may want to see chapter 7.3 – AVG DataCenter Mode Setting – User Administration.)

h)   Test Results

The ***Test Results*** dialog allows you to define whether negative test results (no virus was found) should be also stored in AVG DataCenter, or not. You can also specify the number of days for which the test results are kept in the AVG DataCenter before they are deleted.

Settings of both options listed in this dialog section significantly affect the data volume transferred to the AVG DataCenter, and the AVG DataCenter size itself. For most users we therefore recommend selecting the option of not transferring negative test results and automatic removal of test results after 30 days.

Attention! *This configuration specifies that all test results older then 30 days will be removed. That applies for the positive test results (virus detected) as well!!*

(For details on this option configuration you may want to see chapter 7.3 – AVG DataCenter Mode Setting – Test Results.)

AVG 7.5

AVG Anti-Virus Network
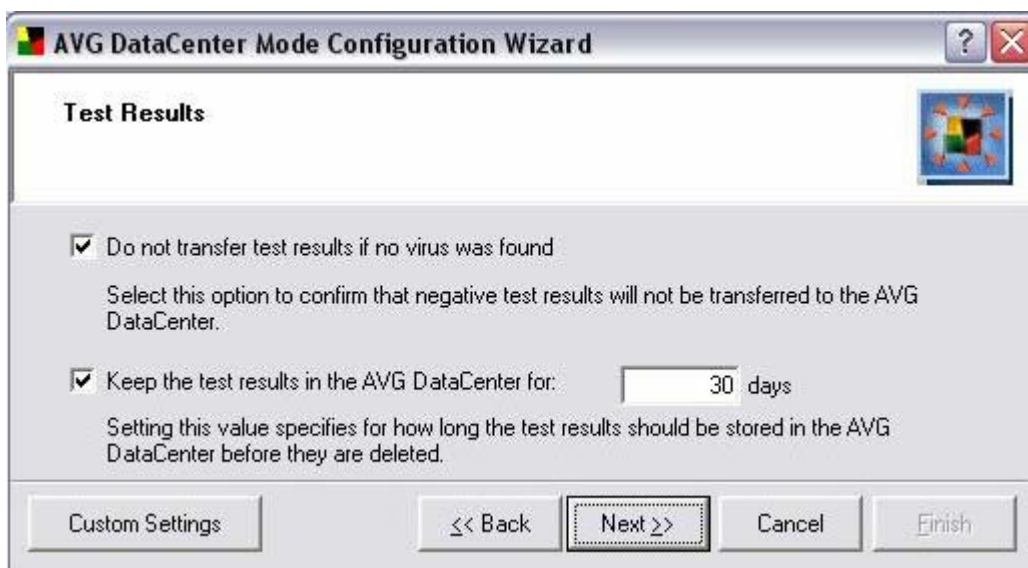
i) **Summary**

You can overview the AVG DataCenter mode settings summary before finishing the wizard and applying the settings.

Press the **Back** button to change the settings if necessary. Press the **Finish** button to complete the wizard and apply the settings.

AVG 7.5

AVG Anti-Virus Network
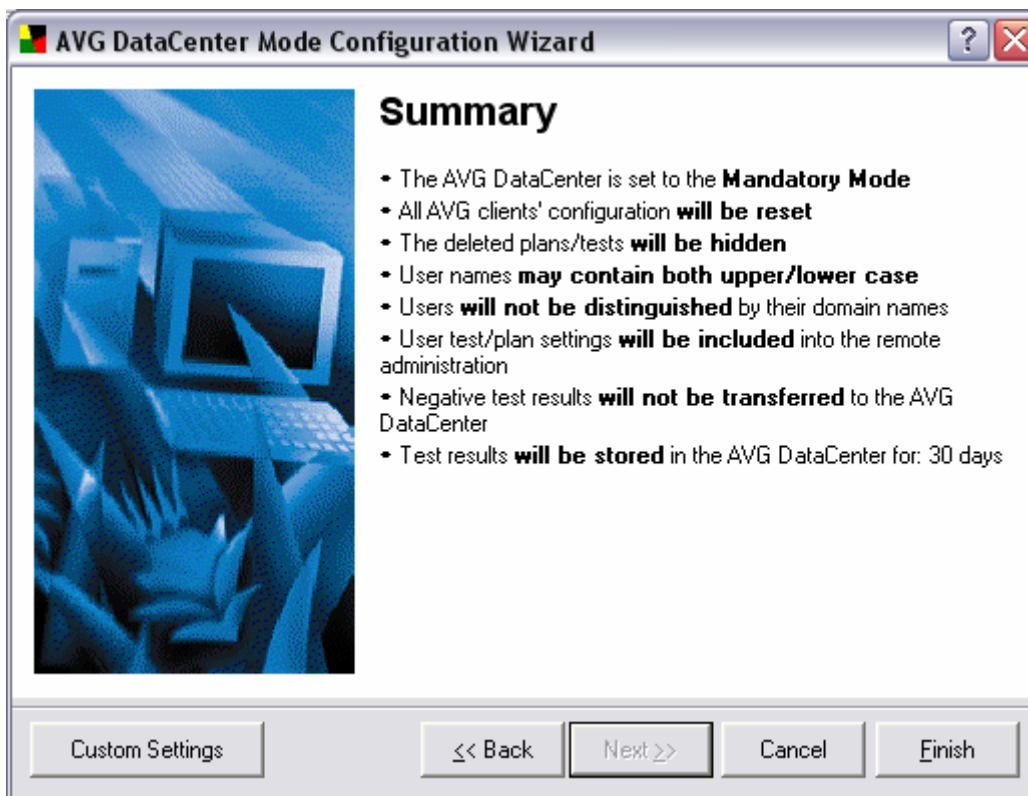
7.4. AVG DataCenter Mode Settings

The **AVG DataCenter** mode configuration can be carried out either using the AVG DataCenter Mode Configuration Wizard, or can be performed manually (using the **Custom Settings** button in the AVG DataCenter Configuration Wizard).

This dialog controls the **AVG DataCenter** elementary settings, and the remote administration settings. The administrator can switch between the **Monitoring** and the **Mandatory mode**:
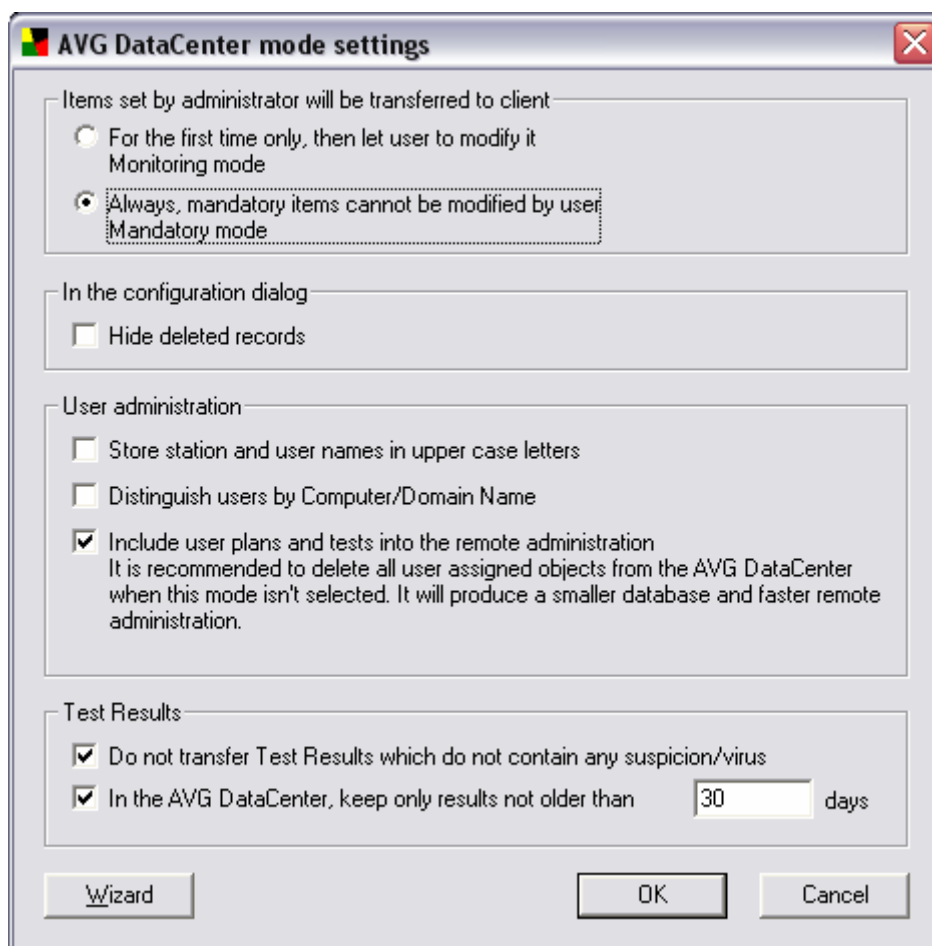
The dialog Windows is structured into four sections:

a)   Items set by administrator will be transferred to client

In this section you define the rules for transfer of administrator's settings to **AVG clients**. This option in fact relates to the selection of one of the two optional **AVG DataCenter** modes:

GRISOFT

AVG 7.5

o **_For the first time only, then let user to modify it_** (Monitoring mode)

o **_Always; mandatory items cannot be modified by user_** (Mandatory mode)

b) **In the configuration dialog**

In this section it is possible to either allow or forbid the **Hide records marked as deleted** option. If this option is activated (by default), then plans / tests marked as "to be deleted" (X parameter) will not show up. This option does not mean that plans/tests marked as "to be deleted" do not exist – they are only hidden! To be able to work with them uncheck the **Hide records marked as deleted** option.

c) **User administration**

o **_Store station and user names in uppercase letters_** - The user names can be saved in the AVG DataCenter in the exact form every single user uses to log in, or they can be transferred to uppercase. By selecting this option, all user names are automatically transferred to capital letters. Then, if there is a user name saved in the AVG DataCenter several times with the only difference of lower/uppercase, through selecting this option you can discover such duplication, and remove it. Finally every username will be saved just once.

o **_Distinguish users by computer/ domain name_** - If the option is not active (by default), a username is saved in the database. If activated, every username is saved with the name of its respective computer name/domain name. Under the condition that all AVG DataCenter accessing users in the network have their own unique name, it is not necessary to apply this option. Otherwise (if there are at least two users with the same name, and can only be distinguished by their respective domains), you should apply this function.

o **_Include user plans/tests into the remote administration_** – This option controls whether the plans and tests are scheduled for stations only (option inactive) or both for stations and users (option active).

Generally, for a network with strict administration rules, e.g. the administrator wants to have a comprehensive overview of the AVG clients' settings, it is recommended to maintain the test/plan schedules for workstations only. If the network rules are more benevolent, you may want to maintain the test/plan settings for stations and users.

If you activate the mode with neither user tests nor the plans included in the remote administration, the default preset test/plan schedules will be automatically forbidden on all workstations. If you decide to define tests/plans for workstations only, it is of course necessary to define the respective tests/plans for all workstations. The easiest way is to define the tests/plans within the shared settings, so that all workstations newly connected to the AVG DataCenter will automatically take this obligatory configuration.

d) **Test Results**

Do not transfer Test Results which do not contain any suspicion/virus

In the DataCenter keep only results not older than xxx days

Settings of both options listed in this dialog section significantly affects the data amount transferred to the AVG DataCenter, and the AVG DataCenter size itself. For most users we therefore recommend selecting the option of not transferring negative test results and automatic removal of test results after 30 days.

Attention! *This configuration specifies that all test results older then 30 days will be removed. That applies for positive test results (virus detected) as well!!*

7.5. AVG DataCenter User/Station Settings

It is also important to decide whether the **AVG DataCenter** settings should include test/plan configurations both for users and stations, or if these are defined for stations only.

Both user and station settings maintenance is suitable in network where users do not share stations, and they are allowed to change the **AVG client** configuration settings

Station settings maintenance is generally useful for situations when a large number of users share a smaller number of workstations, e.g. in school computer labs or training centers. Saving and maintenance of such a huge number of tests/plans can easily turn into a nightmare and may significantly reduce the communication speed as well as increase the **AVG DataCenter** file. In these cases it is recommended that the **AVG DataCenter** does not work with the user test/plan settings at all.

Using **AVGADMIN 7.5**, the configuration records in the **AVG DataCenter** are not defined as default objects (*.DEFAULT.xxxx*) any longer. Instead, a new type of shared object (*.SHARED.xxxx*) is implemented. The configuration given by shared objects is not copied, but shared. Each record is then stored in the **AVG DataCenter** only once. Every station (or user) takes such a record as a part of its own settings.

This solution prevents database growth caused by multiple storage of a large number of similar records that only differ in their owner.

We can speak of:

- shared settings of stations
- shared settings of users
- shared settings of groups

All records (tests, plans and rules) under shared configuration are passed automatically to all stations and users as a part of their own configuration.

The preset records can exist both in the AVG client and shared configuration. In that case the following hierarchy is applied: the mandatory configuration in shared settings take priority over the shared settings in general; furthermore, the shared settings take priority over the AVG client (workstation, user) settings.

7.6. AVG DataCenter Update

If a new **AVGADMIN** version supporting new functions is installed, or if the data processing changed, it is necessary to perform an **AVG DataCenter** update. Usually

the administrator is allowed to keep the database in its original format. However, we recommend transferring the database to the new format as soon as possible so that you can fully use all functions and features of the new **AVGADMIN** version.

From time to time, the **AVG DataCenter** structure changes significantly; then it is necessary to update the **AVG DataCenter** before using the new **AVGADMIN** version in order to secure the correct performance. In that case, **AVGADMIN** will inform the user that it is not possible to continue working until the **AVG DataCenter** updates.
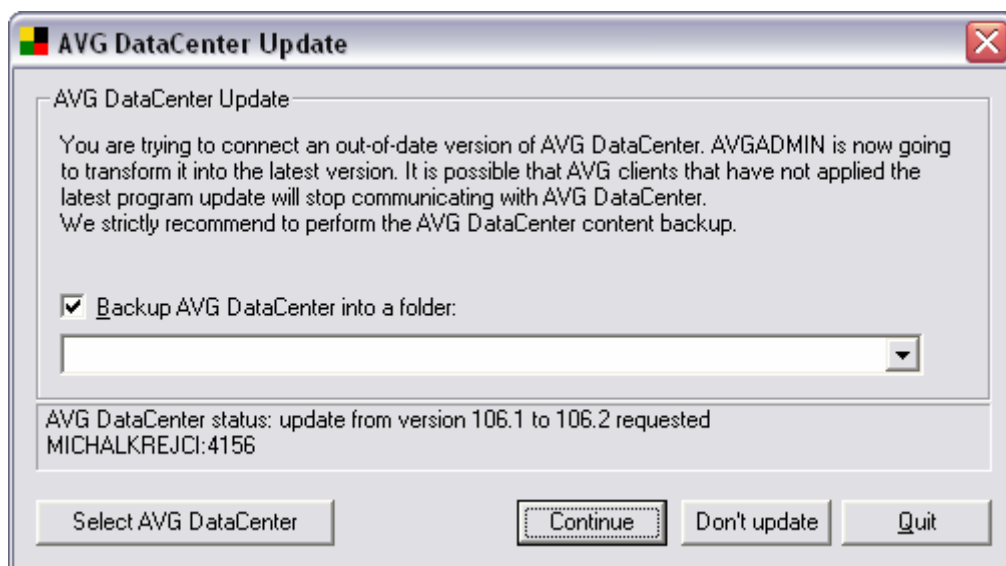
The update dialog always offers the option of exporting the **AVG DataCenter** content before the actual update process starts. We strongly recommend creating a backup before starting the update.

7.7. AVG DataCenter Maintenance

After a considerable period of **AVG Anti-Virus Network Edition** use (i.e. **AVGADMIN** use), some inconsistencies or duplication in the **AVG DataCenter** may appear. Such a situation makes increasing demands on the network load, and the maintenance options are aggravated. For easy **AVG DataCenter** maintenance we have prepared several scripts that will help you perform the frequently required maintenance operations. During maintenance (when a script is active) the **AVG DataCenter** is locked, and users cannot access it.

AVG 7.5

AVG Anti-Virus Network
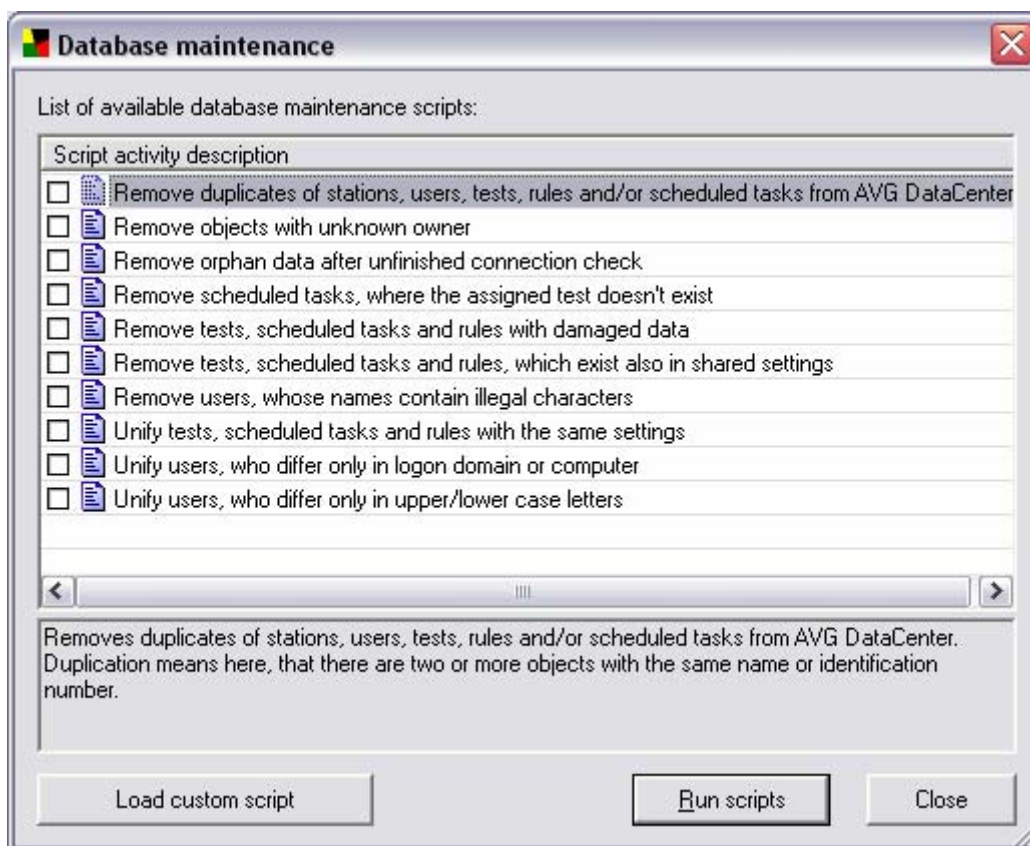
The following scripts are available:

- **Remove duplicates of stations, users, tests, rules and/or scheduled tasks from AVG Datacenter**

  Removes duplicates of stations, users, tests, rules and/or scheduled tasks from AVG DataCenter. Duplication means here, that there are two or more objects with the same name or identification number.

- **Remove objects with unknown owner**

  Removes from AVG DataCenter all settings, tests, rules and scheduled tasks belonging to stations or users, that don't exist in AVG DataCenter.

- **Remove orphan data after unfinished connection check**

  Removes orphan data after unfinished connection check. This data may occupy and waste database space.

- **Remove scheduled tasks, where the assigned test doesn't exist**

  Removes scheduled tasks, where the assigned test doesn't exist.

- **Remove tests, scheduled tasks and rules with damaged data**

  Removes tests, scheduled tasks and rules with damaged data. Such objects are totally or partially functionless.

AVG 7.5

AVG Anti-Virus Network

- **Remove tests, scheduled tasks and rules, which exist also in shared settings**

    Removes tests, scheduled tasks and rules belonging to particular stations and users, if the same tests, scheduled tasks and rules also exist as mandatory in shared settings.

- **Remove users, whose names contain illegal characters**

    Removes users, whose names contain illegal characters.

- **Unify tests, scheduled tasks and rules with the same settings**

    Recalculate checksum of tests, scheduled tasks and rules. Objects with identical checksum will be displayed in the Global settings on one row.

- **Unify users, who differ only in logon domain or computer**

    Remove duplicate users, whose names differ only in logon domain or computer. In case of duplication in config sets the most recent one will be kept. AVG DataCenter mode Distinguish users by Computer/Domain Name will be switched off.

- **Unify users, who differ only in upper/lower case letters**

    This script identifies all user names that differ by upper/lower case letters only, and it will find all duplication. Except for the most recently specified name all other names will be removed. For instance, if there are users named Jameson, JAMeson, and JAMESON in the AVG DataCenter, running this script will delete two of these names, and leave the last of them - JAMESON. This script runs automatically if the network administrator selects the ***Store user names in uppercase letters*** option in the AVG DataCenter Mode Settings.

It is also possible to read and run a script preset by **Grisoft** (the script must be digitally signed so that **AVGADMIN** accepts it) using the ***Load custom script*** button.

To perform the complete AVG DataCenter maintenance process, it is recommended to:

- Run the database maintenance scripts.

- Examine all tests/plans in the overview. Some tests and plans with the same name may easily be unified by selecting the ***Edit*** function. Click ***OK*** to confirm, and the tests/plans will be unified.

- Sometimes it may be useful to mark the unwanted tests/plans as ***to be deleted***, or to remove them from the **AVG DataCenter** completely – in the ***Tests/Plans marked as deleted*** tab.

- Newly created tests/plans can be assigned to specific users/stations.

7.8. AVG DataCenter Password Protection

The access to the **AVG DataCenter** can be password protected, and the password is saved directly in the **AVG DataCenter**. If **AVGADMIN** finds out that the **AVG DataCenter** is password protected, it will require the password to be entered at every connection, i.e. at startup, and also at connecting from **AVGADMIN** through the main menu ***Program/Select AVG DataCenter*** option.

If you want to activate the **AVG DataCenter** access password protection, you can do so using the **AVGADMIN** main menu option *Program/Protect DataCenter with password*, and type the new value of the access password. The password can be changed this way any time, or you can decide to deactivate the password protection by leaving the fields empty.

7.9. Number of Clients Connected to AVG DataCenter

Based on the number of client stations with installed AVG that are connected to the **AVG DataCenter** it is necessary to select the appropriate database type considering the following limitations:

a)   **Embedded Firebird** – is a standard part of the **AVG Anti-Virus Network Edition** installation (no extra license is required); this database is recommended for maximum of 150 client stations

b)   **Firebird SQL Server** – requires an extra license; this database is recommended for maximum of 150 client stations

c)   **MS SQL Server** – requires an extra license; the number of connected client stations is limited by the server's hardware equipment only

d)   **MS SQL 2005 Server Express Edition** – is the free version of MS SQL server and you need no extra license to use it; up to 1000 client stations can be connected to this server

7.10. AVG DataCenter on Microsoft SQL Server 7.0/2000/2005

Creation and configuration of AVG DataCenter is completely managed by **AVG DataCenter Setup Wizard** that is automatically launched after the successful installation of AVG Anti-Virus Network Edition. It can also be launched any time later using the **AVGADMIN** program folder.

More information on this topic can be found within chapter 7.2. AVG DataCenter Setup Wizard.

AVG 7.5

AVG Anti-Virus Network

7.11. AVG DataCenter on Firebird SQL Server

By default, the **AVG TCP Server** uses a special embedded version of the Firebird SQL Server database engine. If there is a standalone Firebird SQL Server already installed in the network, it is also possible to connect to it, using existing infrastructure and tools. **AVG TCP Server** can connect to the Firebird server.

The default AVG database AVGDB.FDB can be used in this mode too. This database is created during **AVG TCP Server** installation. On the other hand, you can create all needed tables with SQL scripts included in your AVG distribution. This way you can create tables also within an existing database. Firebird database installation script is created during the installation (once this option is activated). For script execution and corresponding tables creation, any SQL client applications (such as ISQL) can be used. We recommend restricting **AVG TCP Server's** (or clients') access rights for the database part containing the **AVG DataCenter** only.

For **AVG TCP Server** to connect to an existing Firebird server it is necessary to modify the database path in the **AVG TCP Server** configuration. Open the configuration within the **AVG TCP Monitor** using the *Configuration* button, and modify the Database path to:

<server_name>:<database_path>

where *server_name* is name of the server with Firebird SQL Server and *database_path* is full path to the database file. Please note that Firebird SQL Server requires the path specification without spaces. Generally, the so-called "short pathname" should be used.

For example, if the Firebird SQL Server is running on a server named **dbserver**, and the database file is in **c:\avgdb\avgdb.fdb**, the database path string would be

dbserver:c:\avgdb\avgdb.fdb

If the Firebird SQL server runs on a same computer as the **AVG TCP Server**, a special server name **localhost** can be used, too:

localhost:c:\avgdb\avgdb.fdb

If all workstations have the Firebird SQL client library installed, **AVG clients** can also connect directly to the Firebird SQL Server. In this case it is only necessary to change the connection string in **AVG clients** to

direct=firebird;dbq=*<server_name>:<database_path>*

where

● **server_name** stands for the name or IP address of the database server

● **database_path** stands for the absolute location of the database file

Example:

direct=firebird;dbq=dbserver:C:\AVG7DC\AVGDB.FDB

In order to allow all the clients to access the database, you have to change their connection string respectively. You can use the AVGW/CONNECT parameter for the connection of already installed clients.

AVG Anti-Virus Network

7.12. Converting the AVG DataCenter to a Different Database

AVG TCP Server installation does not automatically convert any existing **AVG DataCenter** to a different database format. If the database engine is changed, it is usually desirable to convert all existing settings and results to the new database.

It is always possible to convert the **AVG DataCenter** from one **AVG DataCenter** to another using the *Export/Import* functions. From within **AVGADMIN** it is possible to export the **AVG DataCenter** to a portable text format, and then (having switched to the new **AVG DataCenter**) import the data using the **AVGADMIN** *Import* function.

AVG TCP Server also comes with a tool named *CloneDC* that can be used for a fast and efficient **AVG DataCenter** conversion. This tool can be found in the **AVG TCP Server** program directory. *CloneDC* directly copies all the necessary data from one database to another. It does not use the **AVG TCP Server** but rather accesses both the source and the target database server directly. Therefore it is necessary for the **AVG TCP Server** to be stopped during this conversion, and that both the source and the target database engine are accessible via its native methods (e.g. Firebird engine and ODBC data source). *CloneDC* also requires that both the source and the target database contain the **AVG DataCenter** database structure and that the versions are the same. Therefore it may be necessary to upgrade the source **AVG DataCenter** using the **AVGADMIN** program before running the conversion.

CloneDC can be launched with two parameters:

CloneDC *<source_DC> <target_DC>*

where the source and the target DC specify full direct connection strings to the respective **AVG DataCenter**. Some samples of *CloneDC* command line follow:

CloneDC direct=firebird;dbq=avgdb.fdb

 "Driver={SQL Server};Server=*dbserver*;Database=AVG;Uid=sa;Pwd="

this command launches conversion from the default Firebird SQL database (using the default embedded engine) to MS SQL Server. The name of the server with MS SQL is dbserver, the user name is *sa* and there is no password set for this account

CloneDC direct=firebird;dbq=localhost:avgdb.fdb

"Driver={SQL Server};Server=*dbserver*;Database=AVG;Uid=sa;Pwd="

this is the same conversion, only using a local standalone Firebird SQL database engine rather than the embedded one. Note that the standalone Firebird requires that the server name *localhost* is specified because the client libraries can generally connect to a different computer across the network.

8. AVGADMIN

8.1. What is AVGADMIN

AVGADMIN is an entrance gate to **AVG DataCenter**. It helps the network administrator to maintain the network configuration, to monitor the **AVG clients'** status, and to remotely call various operations on **AVG clients**. **AVGADMIN** can help you perform:

● **AVG clients monitoring**

All AVG clients connected to the AVG DataCenter report their AVG program version, the operating system version, workstation IP address, and other important data.

● **AVG client settings display and configuration**

AVGADMIN is connected to the AVG DataCenter. The AVG DataCenter keeps information about all AVG clients' configuration settings. With the use of AVGADMIN, the network administrator is able to control the current AVG clients' configuration, and change any required value.

● **Test results and virus infection control**

All test results and virus infection reports from the Resident Shield are saved in the AVG DataCenter. AVGADMIN allows the administrator to review the reports, analyze the possible virus attack reasons, discover the virus source, and take protective steps to prevent such events.

● **Test/update remote launch on AVG clients**

From the AVGADMIN console you can remotely run tests, or check for available update files directly on workstations.

● **AVG remote installation launch**

From AVGADMIN you can call the AVG remote installation on workstations. For this type of installation we recommend using the AVG S-Tool component

● **Update file distribution within the local network**

There are several ways to download and distribute update files in the local network. One of them is using the AVGADMIN function for downloading update files. AVGADMIN then asks the AVG client to update.

Note: If you want to use this function it is essential that the AVG 7.5 client is installed on the same station where AVGADMIN runs. For further information on the update files distribution in the local network please refer to the 12. Centrally Controlled Update chapter.

8.2. AVGADMIN Launch

You can start AVGADMIN in several ways:

- from the Windows menu:
  Start/Programs/AVGADMIN 7.5/AVGADMIN 7.5

- from the desktop: double click the *AVGADMIN 7.5* icon

- from the **AVGADMIN** program folder run the *AVGADMIN.exe* file

At startup, **AVGADMIN** automatically tries to connect to the last used **AVG DataCenter**. If the connection fails, or if you are launching **AVGADMIN** for the first time, a dialog window will appear and you will be asked to specify the communication string for the **AVG DataCenter** connection. The communication string uses the same form as the **AVG client's** communication string – for details refer to chapter 6.7 Clients connection to the AVG TCP Server.

Typically, if **AVGADMIN** is installed on the same computer as the **AVG DataCenter**, it is possible to use this communication string: http://localhost.

The general communication string structure is http://server_address:port, where:

- *server_address* is the name/address of a server where the **AVG TCP Server** runs

- *port* is the **AVG TCP Server** port number. The default port value is 4156. If the **AVG TCP Server** uses this default number, it is not necessary to include the number into the communication string.
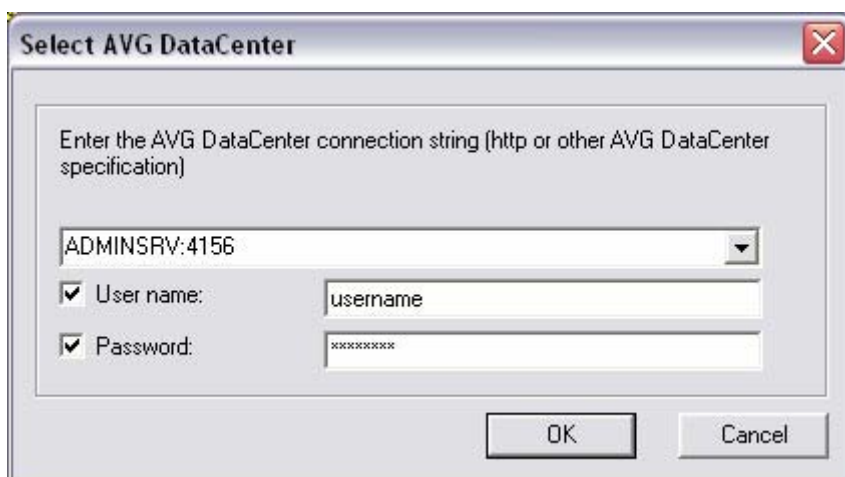
If the **AVG DataCenter** is password protected, **AVGADMIN** will ask you to supply the password after connecting to the **AVG DataCenter**. If the password provided is wrong, you can try to connect to another **AVG DataCenter**. Otherwise the program quits.

## 8.3. AVGADMIN Command Line Parameters

When starting **AVGADMIN**, it is possible to use some command line parameters that affect the application's standard behavior. The following parameters are available:

Parameter	Meaning

AVG 7.5

AVG Anti-Virus Network

/LNG=*xxxx*	Selection of the user interface communication language. If the required language version is available, it will be used. Otherwise the application will choose the language according to the operating system language. The possible values are: **CSY** – Czech user interface **ENU** – English user interface *number* – the language code (internal Windows encoding)
/DC="connections_string"	AVGADMIN will try to connect to the specified AVG DataCenter instead of the recently used AVG DataCenter. The communication string must be typed in quotation marks. /DC="http://tcpsv:4156"
/IMPORT=*path*	Calls the database import from the specified directory.
/EXPORT= *path*	Export the AVG DataCenter database to the specified (existing) directory. This parameter can be used for the database back up, for instance.
/LOG=file	Activates the database export/import functions logging. This parameter is intended for diagnostics only.
/UPDATE=*path*	Asks the stations to update from the specified directory. *Path* stands for the exact path to the directory with the update files (could be UNC, e.g. including the server name). This directory must be accessible to all clients.
/LIST=list	Specifies a list of stations that will be asked to update; single stations are separated by a semicolon. If the /LIST parameter is not specified, the update call is sent to all registered stations. The parameter can be used together with the /UPDATE parameter.

8.4. AGADMIN Modes

Having specified the **AVG DataCenter** communication string, **AVGADMIN shows the following** dialog window:

AVG 7.5

AVG Anti-Virus Network
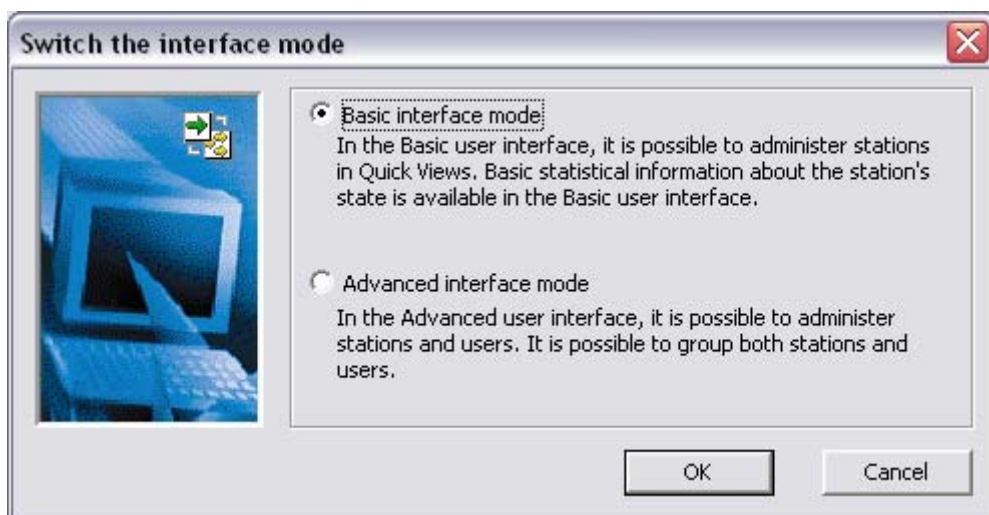
Within this dialog you can decide whether what **AVGADMIN** mode you want to run:

Basic User Interface

Advanced User Interface

9. AVGADMIN Basic Interface

AVGADMIN Basic Interface is a environment with user friendly interface for easier administration. However, the functionality available within the **AVGADMIN Basic Interface** is the same as the Advanced interface functionality. The **AVGADMIN Basic Interface** is intended rather for smaller networks.

The **AVGADMIN Basic Interface** opens in this environment:
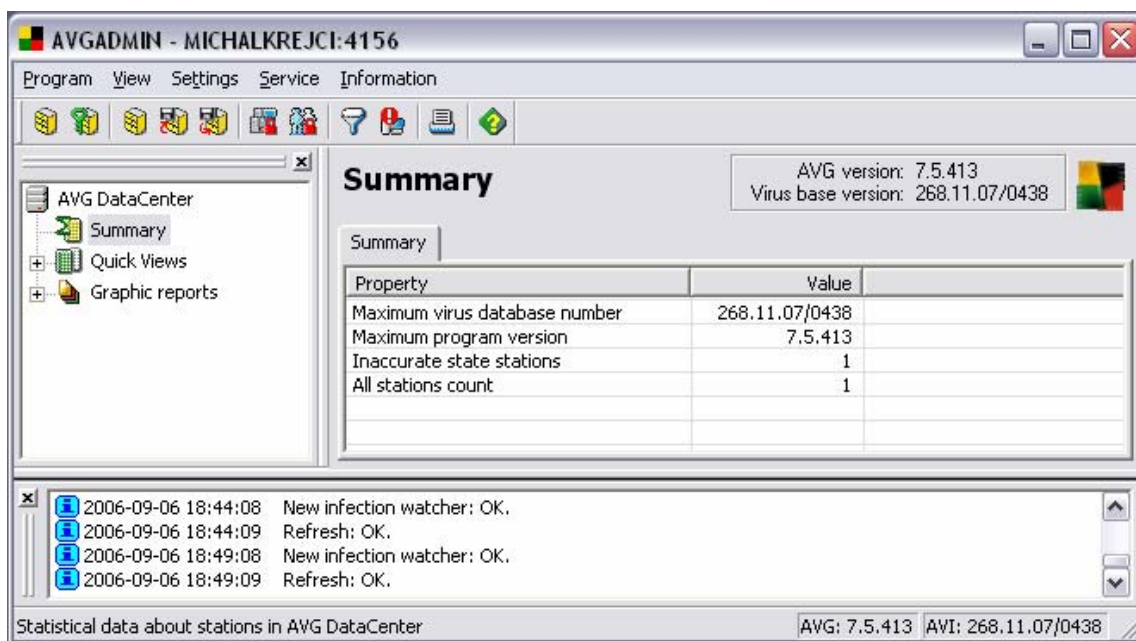
The window is divided into four sections:

- [Program main menu](#) (upper part)
- [Navigation tree](#) (left panel)
- [Records section](#) (central part)
- [Status window](#) (bottom part)
- [Other control component](#)

9.1. Program Main Menu

The program main menu offers the following options; these options are available both from the Basic and Advanced interface of the **AVGADMIN** program:

a)   Program

- o   **Select AVG DataCenter** – allows you to select a connection to another **AVG DataCenter**

- o   **Protect AVG DataCenter with password**... – the **AVG DataCenter** can be password protected; **AVGADMIN** will ask you to supply the password at every connection to the **AVG DataCenter**.

    (For details please refer to chapter [7.7 – AVG DataCenter Password Protection](#))

AVG 7.5

AVG Anti-Virus Network

o   **AVG DataCenter mode** – launches the **AVG DataCenter** mode configuration wizard that will help you set the **AVG DataCenter** information processing parameters

    (For details please refer to chapter 7.2 – AVG DataCenter Mode Configuration Wizard)

o   **Lock AVG DataCenter** – the **AVG DataCenter** automatically locks during maintenance operations, e.g. updates. Users cannot access the database at that time. Using this option enables you to lock the **AVG DataCenter** manually.

o   **Export** – exports the **AVG DataCenter** contents into a file; can be used for data backup

o   **Import** – imports the **AVG DataCenter** contents from a file; can be used to restore the **AVG DataCenter** data from a backup file

o   **Print** – prints the currently selected data (main panel content)

o   **Exit** – quits the **AVGADMIN** application

b)   View

o   **Interface mode** – allows you to switch from the **AVGADMIN** Basic User Interface to the Advanced User Interface

o   **Stations visible in Quick Views**

–   *Filter settings* – opens a window where you can specify parameters limiting the display of stations in Quick Views

–   *Inaccurate state conditions* – opens a window, where you can define the inaccurate state stations parameters *(see Quick Views - Inaccurate state stations)*

o   **Firewalls visible in Quick Views** - opens a window where you can specify parameters limiting the display of Firewall-enabled stations within *Quick Views*.

o   **Panels**

–   **Toolbar** – shows/hides the *Toolbar*

–   **Navigation tree** – shows/hides the *Navigation tree*

–   **Navigation bar** – shows/hides the *Navigation bar*

–   **Version information** – shows/hides the *Version information*

–   **Status window** – shows/hides the *Status window*

–   **Status bar** – shows/hides the *Status bar*

–   **Show errors only** – shows only errors within the *Status window*

o   **Options –** allows you to customize font styles for specific information types displayed

o   **Refresh** – refreshes all records displayed in the **AVGADMIN** records section.

c) Settings

o **Shared settings for stations –** opens a dialog for editing the shared configuration for stations *(For detailed information on stations shared settings please refer to chapter 7. AVG DataCenter)*

o **Shared settings for users –** opens a dialog for editing the shared configuration for users *(For detailed information on users shared settings please refer to chapter 7. AVG DataCenter)*

o **Periodic tasks –** allows you to specify a time period for regular periodic tasks launch. *(For detailed information on periodic tasks settings please refer to chapter 11.1 – AVGADMIN Periodic Tasks)*

o **AVG TCP Server settings** - allows you to start the *AVG TCP Server* configuration dialog directly from AVGADMIN. The *AVG TCP Server* must be already running.

d) Service

o **Install AVG 7 onto stations** – launches **AVG S-Tool** Basic mode for AVG remote installation on workstations

o **Install AVG 7 onto stations (advanced mode)** – launches **AVG S-Tool** Advanced mode for AVG remote installation on workstations

o **Ask to download update files** – downloads the update files into the selected directory. Works only if AVG is installed on the same computer as AVGADMIN. Only incremental updates will be downloaded, based on the current status of installed AVG.

o **Ask stations to update** – asks **AVG clients** on workstations to update AVG

o **Reset configuration on all stations** – sends a special note to all **AVG clients** and resets their configuration (when **AVG clients** receive the note, all tests and plans set up by the end user are removed, and the **AVG client** returns to the default configuration set up in the **AVG DataCenter**)

o **Licenses Administration -** A configuration dialog for managing license numbers. It shows license numbers that have expired, or that are incorrect and allows you to easily monitor all existing license numbers, and add or update license number for individual or multiple stations.

More information on this topic can be found in chapter 10.7 Licenses Administration

o **Database maintenance** – allows running of various up-keeping and correcting scripts for the **AVG DataCenter** maintenance

e) **Information**

o **About...** - displays the copyright information, and the application/database version number

o **What is new** – displays step-by-step summary of important news in the AVGADMIN 7.5 application.

o **Check for updates** - AVGADMIN automatically, during startup, checks if a newer version of AVGADMIN is available. But you can also open this dialog and immediately see if a new version is available.

To disable the startup checking feature, check the *Do not check for updates at start* checkbox.

o **Check for Report viewer** - AVGADMIN automatically, during startup, checks if the Graphic viewer for the Graphic reports is installed or not.

To disable the startup checking feature, check the *Do not check for Report viewer on startup* checkbox.

9.2. Navigation Tree

The **Navigation Tree** contains all groups arranged in a hierarchical manner. A group is a data structure review, e.g. a list of workstations with their configuration, or test results table, etc. The group content itself displays in the *Records section*, in the central table.
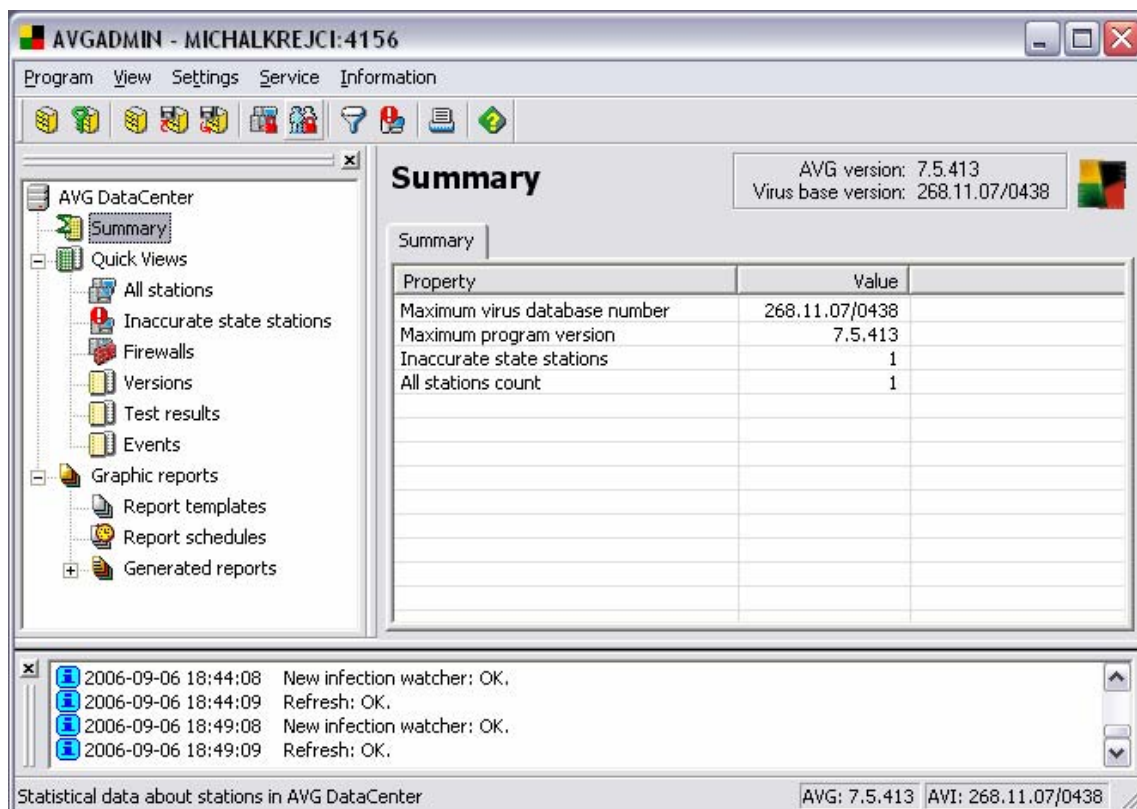
The **AVGADMIN Basic Interface** Navigation tree offers the following sets:

AVG 7.5

- [Summary](#)

- [Quick Views](#)

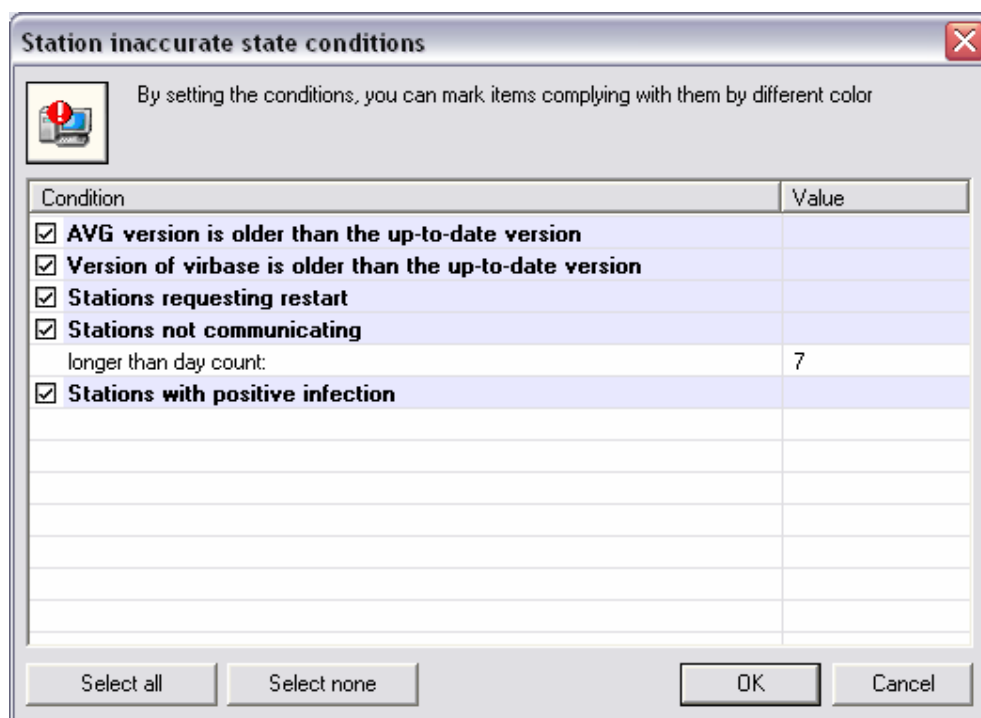- [Graphic reports](#)

a)   Summary

The **Summary** group offers an overview covering:

o   Inaccurate state stations *(see [Quick Views – Inaccurate State Stations](#))*

o   All stations count

o   Maximum virus database number

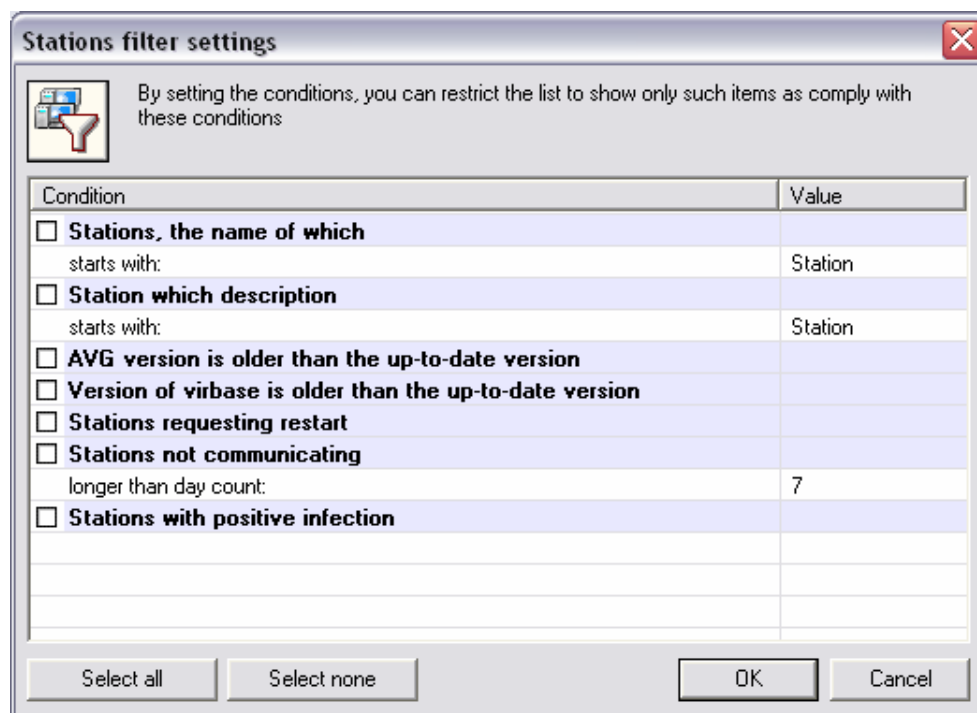o   Maximum program version

b)   Quick Views

The **Quick Views** group provides the administrator with structured information divided into the following categories:

o   **All stations** – An overview of all stations in the network accompanied with information on station description, version of AVG installed on a specific station, the Anti-Virus database version, etc.

o   **Inaccurate state stations** – The station is taken for an **Inaccurate state station** if at least one of the administrator specified inaccurate state conditions holds good for that station. These conditions can be defined by the administrator within the **Station Inaccurate state conditions** dialog:

GRISOFT

The *Inaccurate state conditions* dialog can be accessed from the application's main menu selecting the option *View/Stations visible in Quick Views/Inaccurate state conditions*

If there are more stations reported as inaccurate state stations, the administrator can use the *Filtering* function to structure the overview and to make it easier to observe. From the main menu select the *View/Stations visible in Quick Views/Filter settings* to open the following dialog window:

The administrator can then select parameters from the list to define which of the inaccurate state stations should be displayed.

The group records can also be filtered according a selected item in the central table. There are to options of filter settings using the keyboard shortcut:

– *ALT + left mouse button* – AVGADMIN displays only records that have the same value recorded for the selected item parameters

– *ALT + right mouse button* - AVGADMIN displays only records that have a different value recorded for the selected item parameters

Switching into another set of records shows all stations again. This filtering option can be used for all **AVGADMIN** sets.

o **Firewalls**

See chapter – <u>Firewalls</u>.

AVG Anti-Virus Network

o **Versions**

The **Versions** group offers an overview of operating system versions and AVG versions installed on a specific workstation. The group uses the following two tabs:

− **Windows** – an overview of OS Windows versions installed on workstations, and number of respective OS version installations

− **AVG** – an overview of AVG versions installed on workstations, and number of respective AVG version installations

o **Test results**

The **Test results** group offers an overview of all test results on workstations together with detailed information related to specific tests. The other two tabs of the central table the divide the test results into two groups:

− **Infected** – positive test results

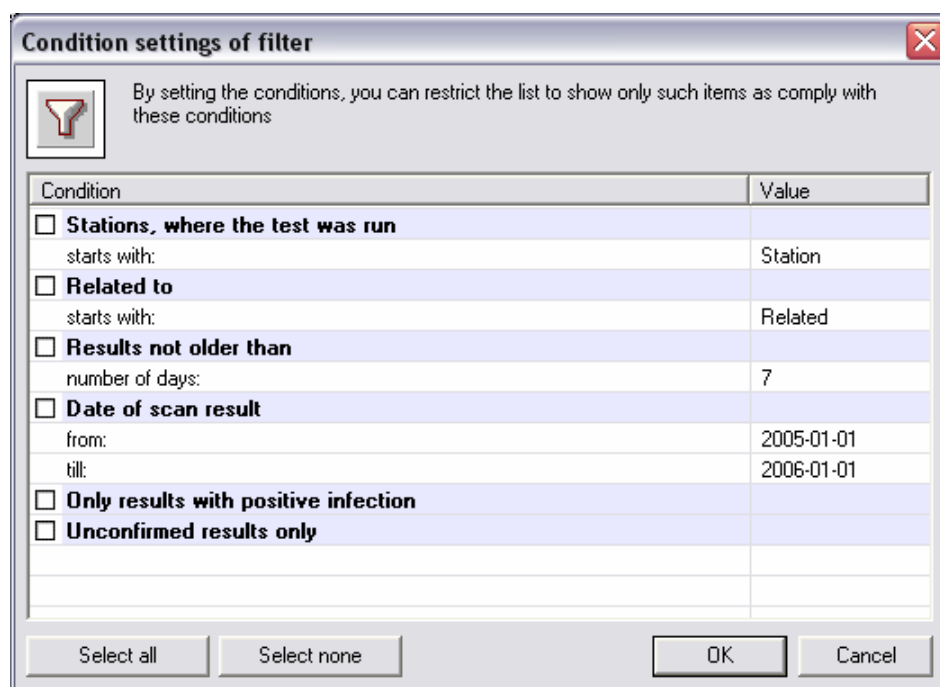− **Resident shield**– test results reported by the **Resident Shield**

Clicking the right mouse button within the list of test results will open a new menu containing these options:

− **Show result details**

Displays dialog window with test result details.

− **Filter settings**

Displays dialog window with filtering options:

By defining one or more parameters you can filter out the requested results.

– **Delete** – deletes marked test results.

– **Delete reports with no infection** – deletes only test results containing no infection.

– **Delete all** – deletes all test results.

– **Acknowledge**

Marks the selected test result as accepted and in the column named as *Time Acknowledged* you will see date and time of the confirmation. At the same time, you will not find the number of infections from the accepted test within the other reports.

Double clicking your mouse on any row will display a dialog window containing details of the selected test result – i.e. list of infections.
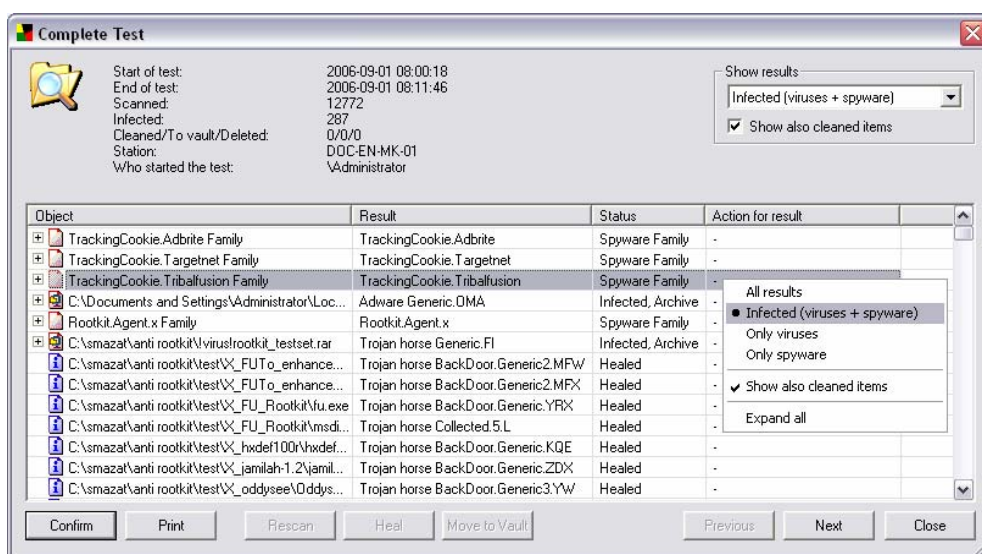
Using the top right menu or using the right mouse button (and choosing from the menu) select which results should be listed:

– **All results** – Displays all results.

– **Infected (viruses + spyware)** – Displays virus infected results and also Potentially Unwanted Programs (like spyware, cookies and similar malware).

– **Only viruses** - Displays only virus infected results.

– **Only spyware** - Displays only Potentially Unwanted Programs (such as spyware, cookies and similar malware).

– To also display cleaned items, check the **Show also cleaned items** checkbox.

– *Expand all* - available only from the right-clicking menu. Will expand all items' details.

Confirm - If you click the **Confirm** button, you will mark the test result as accepted and in the column named as *Time Acknowledged* you will see date and time of the confirmation. At the same time, you will not find the number of infections from the accepted test within the other reports.

If there are listed one or more infections within the results, you can select one or more of such findings and by clicking the appropriate buttons performing these actions:

– **Rescan** – will ask the station to rescan the selected finding(s).

– **Clean** – will ask the station to clean the selected finding(s).

– **Move to Vault** - will ask the station to remove the selected finding(s) to AVG Virus Vault on the station.

If the station is active, the operation(s) will be done immediately after request. If the station is not currently active (i.e. is not connected to the AVG Datacenter), all pending operations will be processed upon next station connection.

More information about all possible actions can be found in chapter 9.6 Processing infections in the Test results.

Previous and **Next** buttons can be used to browse through the test results, therefore it is not necessary to close the window, if you need to move to next or previous result.

You can print the whole report by clicking the **Print** button (you will be offered with a standard MS Windows print dialog where you can select printing options and a specific printer).

If there is an archive listed within the infected results, you may display the infections inside by simply clicking the plus symbol located on the left side of the row.

clicking the plus symbol in the left side of the row or using the right mouse button and choosing from the displayed menu the appropriate selection.

o *Events*

The *Events* group offers an overview of all events divided into the categories of messages, warning, errors, and critical events. On specific category-related tabs you can then find more detailed information related to the actual event.

c) **Graphic reports**

This group offers graphic reports. It allows users to quickly and easily generate well arranged reports. Reports may show a summary of stations managed by AVGADMIN, top infected stations, top virus occurrences and similar statistics.

Users can select from pre-defined templates and produce the reports by simply double-clicking, schedule report creation at a customized time period, send generated reports to e-mail addresses or print reports to PDF file or printer.

To learn more about Graphic reports and its configuration, see chapter 9.7 Graphic Reports.

AVG 7.5

AVG Anti-Virus Network

9.3. Records Section

Within the central table in the ***Records Section*** of the screen you can view data of the group specified within the navigation tree. Some sets may contain a considerable amount of data for a specific record (e.g. workstation/user information); that is why the relevant data is arranged into groups, and every group can be displayed when you select the corresponding tab.

To select a record from the central table you need to perform a mouse click over the desired record. You can select more records at the same time: press the ***CTRL*** key (adding a new record to the current selection), or the ***SHIFT*** key (selecting all records between the first and the last highlighted record). Click the mouse right button over the selected record to open the ***Context menu***. It is possible to call various actions related to the current selection from the ***Context menu***.

Within the central table of the records section you can use the ***quick search*** option: the option allows searching for records according to the record value specified in the central table first column. The search is activated by the ***CTRL+F*** keyboard shortcut; to confirm the search keyword hit the ***Enter*** key. The ***Esc*** key will cancel the search. The search identifies all records that correspond to the specified search parameter, and the first search result of the search results list will be highlighted – to switch among the search results use the ***F3*** key.

9.4. Status Window

In this part of the **AVGADMIN** main window you can find various system notices and information on the application functionality, communication with **AVG clients**, detected problems, positive test results warnings, etc.

9.5. Other Control Components

a) Navigation bar

The Navigation bar can be found in upper part of the Records section above the central table with records.

b) Tool bar

The Tool bar can be found under the application main menu; the icons represent specific main menu options and act as quick links for selected operations.

c) Status bar

The Status bar can be found at the very bottom of the screen; the status bar displays the help file for specific menu items, and application status information.

d) Context menu

The Context menu can be opened from any selected item listed in the central table by a right mouse-button click; the context menu items differ according to the content of the item to which the context menu relates.
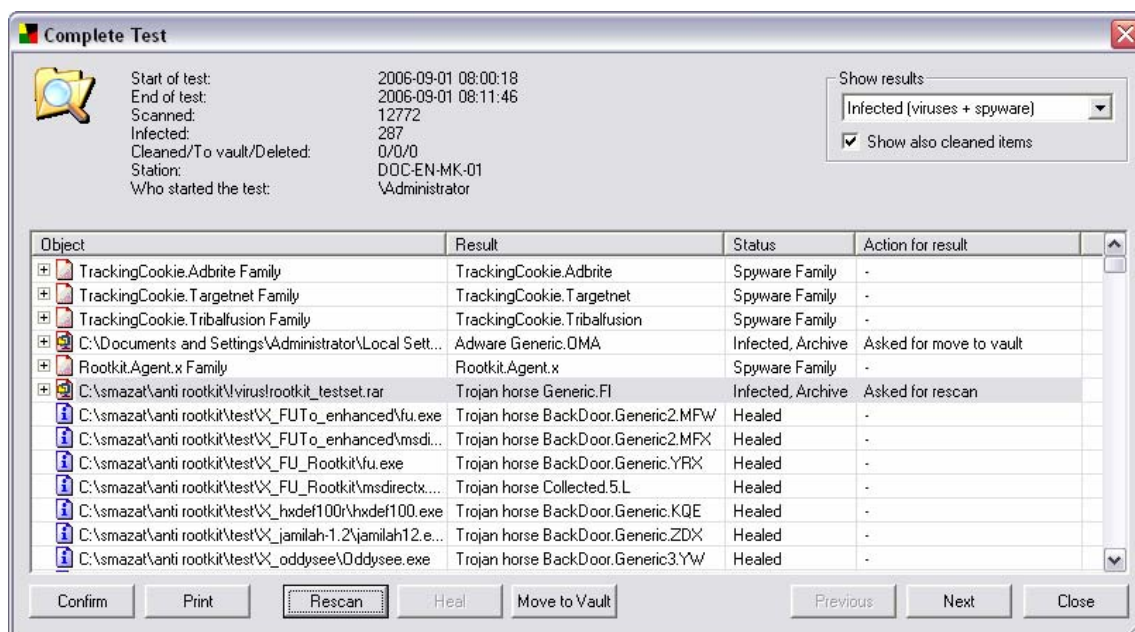
9.6. Processing infections in the Test results

There are three main actions, that can be performed on the infected results:

- **Rescan** – will ask the station to rescan the selected finding(s).

- **Clean** – will ask the station to clean the selected finding(s).

- **Move to Vault** - will ask the station to remove the selected finding(s) to the AVG Virus Vault on the station.

Each action can be performed in every test result, that contains one or more infections in the list. You can select one or more infected objects and then click the appropriate button – **Clean/Rescan/Move to Vault**.

If the station is not currently active (i.e. is not connected to the AVG Datacenter), all pending operations will be processed the next time the station connects.

Once you request an action, then if the AVG station is active, it will either try to find the requested test result and process all selected infections or, if the test result cannot be found, it will try to process the infection anyway, since the full path to the file is always known.

In both cases one of the *action result states,* listed below, will be displayed in the **Action for result** column. The possible states are as follows:

- **Asked for clean** – the station will try to heal the infected file.

- **Asked for move to vault** – the station will try to move the infected file to the AVG Virus vault.

- **Asked for rescan** – the station will scan the file again.

- **Successfully cleaned** – the file was successfully cleaned.

- **Successfully moved to vault** – the file was moved to the AVG Virus vault on the station.

- **File was rescanned** – the file was successfully scanned again on the station.

- **Cleaning is not available** – the file cannot be cleaned.

- **Moving to vault is not available** – the file cannot be moved to the AVG Virus Vault.

  Several other error states exist that should not occur under normal circumstances:

- **Error during deletion** – an error happened during the cleaning process.

- **Error during moving to vault** – an error occurred when moving infected file(s) to the AVG Virus vault.

- **Error during rescanning** – an error occurred when rescanning the infected file(s).

- **File is not infected** – the file to be processed is no longer infected, the requested action cannot be done.

- **File doesn't exist anymore** – the file to be processed is no longer available on the station, the action cannot be completed.

- **Access to file denied** – Access to the requested file was denied (probably because it is being used by another application or process), the action cannot be completed.

- **Unknown error** – an unknown error occurred during the action.

9.7. Graphic reports

Note: As *Graphic reports are generated by the **AVG TCP Server**, the generation will only work if installed on computer with **AVG TCP Server***.

The **Graphic reports** allows users to quickly and easily generate well arranged reports. Reports may show various summaries and statistics. Graphical reports are accessible from the main AVGADMIN navigation tree.

The reports are always generated in the language that has been chosen during installation of the **AVG TCP Server**.

Note: Generated reports are physically saved to a temporary location on your hard drive, usually under your SystemRoot/Temp (e.g. Windows/temp). Each generated report will consume some hard drive capacity (from 0,1 to 0,5 MB approximately, but can be even more, if you have lots of stations). Therefore if you suffer from insufficient disk space, we recommend to only create a reasonable amount of reports or delete the old ones accordingly.

*During Export/Import (available through **Program/Export** or **Import**) of AVGADMIN data, only Report schedules will be processed. Templates and generated reports will not be exported or imported!*

*Once you import your former exported data, Graphic reports will not be available until you restart the **AVG TCP Server**!*

- **Report templates**

  There are some predefined templates that can be quickly used for report generation. Some templates allows you to set additional parameters for more precise reports.

  To create a report directly from this menu, right-click on the report you want to generate and select the **Generate report** menu item. If you prefer only to display a preview of the report layout, select **Template preview**.

  o **All stations** - shows all stations registered in AVGADMIN

     Available parameters:

     – **Min count of infected** - type in the minimum count of infected objects on station. 0 = disable this parameter.

     – **IP address starts with** - specify a beginning part of the IP address.

  o **Stations by AVG Version** - shows all stations sorted by AVG version.

  o **Top N infected stations** - shows top infected stations.

     Available parameters:

     – **N stations count in report** - limit the number of stations in report. 0 = unlimited.

  o **Top N viruses** - This report shows the top viruses of all stations.

     Available parameters:

     – **N - viruses count in report** - limit the number of viruses in report. 0 = unlimited.

     – **Time interval** - specify the time interval for selecting data (last day, last month, last year).
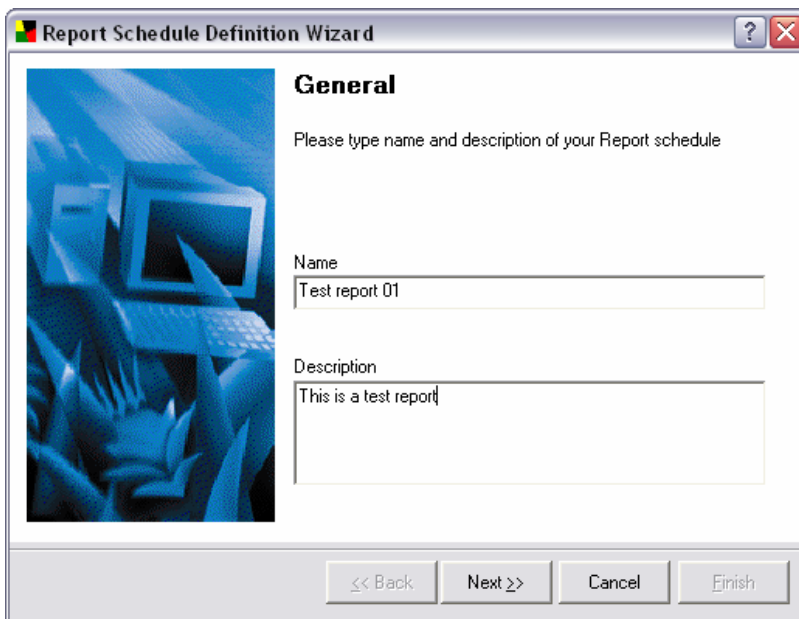
- **Report schedules**

  In this group, you can create, edit and view graphic reports. There are two tabs available:

o   **Reports Schedules** - contains list of all schedules. See more details below.

o   **Report schedules marked as deleted** - this tab contains a list of all reports that have been marked as deleted. If you right click on a report in this tab, you can select from the following choices:

–   **Edit** - opens an edit dialog for the selected schedule.

–   **Restore report schedule(s)** - you can select one or more items and restore them by using this function.

–   **Completely remove from AVG Datacenter** - select one or more items and delete them by using this function. Alternatively press the **Delete** keyboard button.

By default, there are no schedules available. To prepare a new scheduled report, right-click in the **Report schedules** tab area and select **Define new schedule** item from the menu.
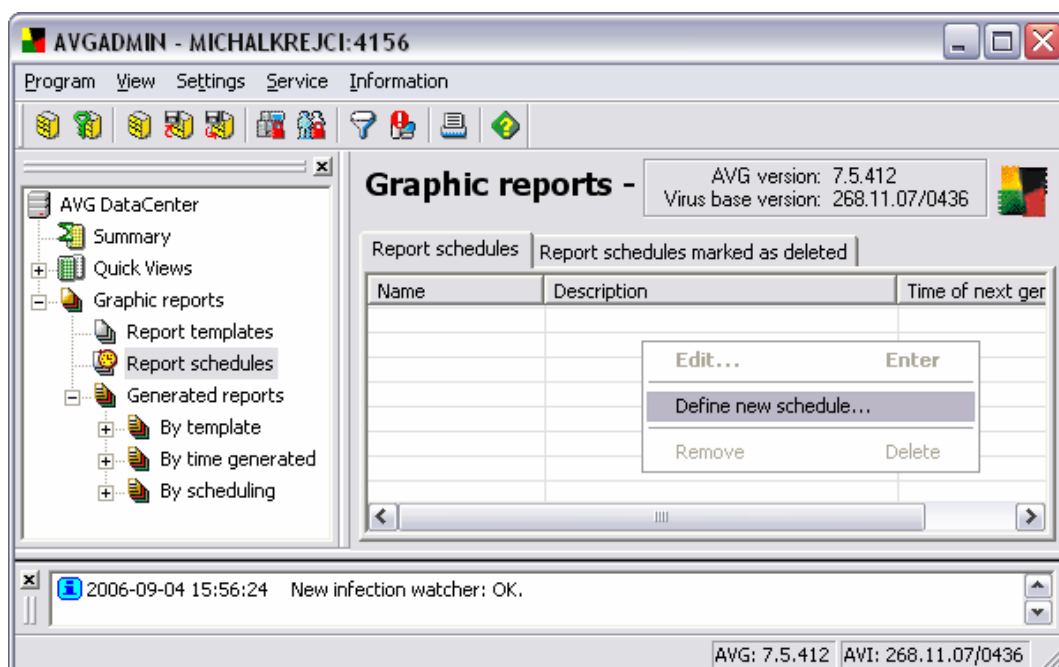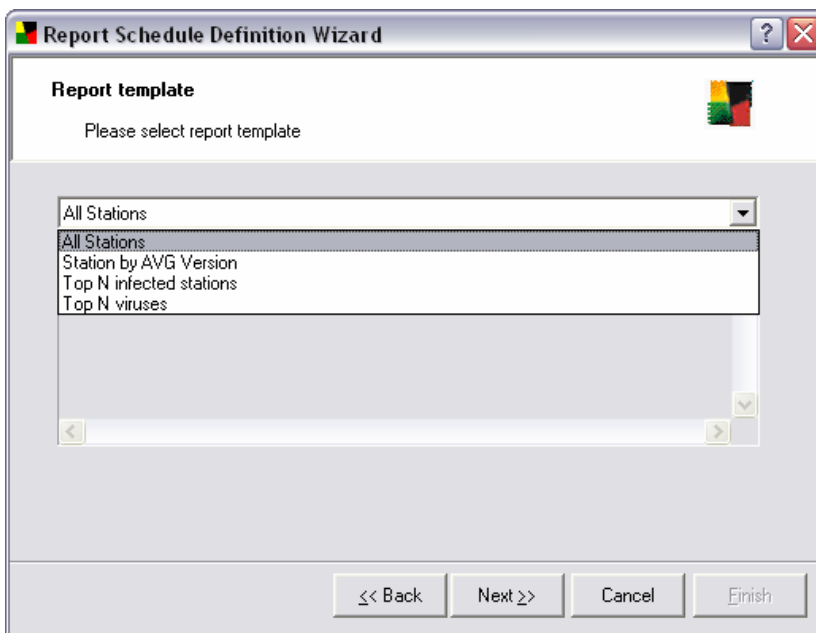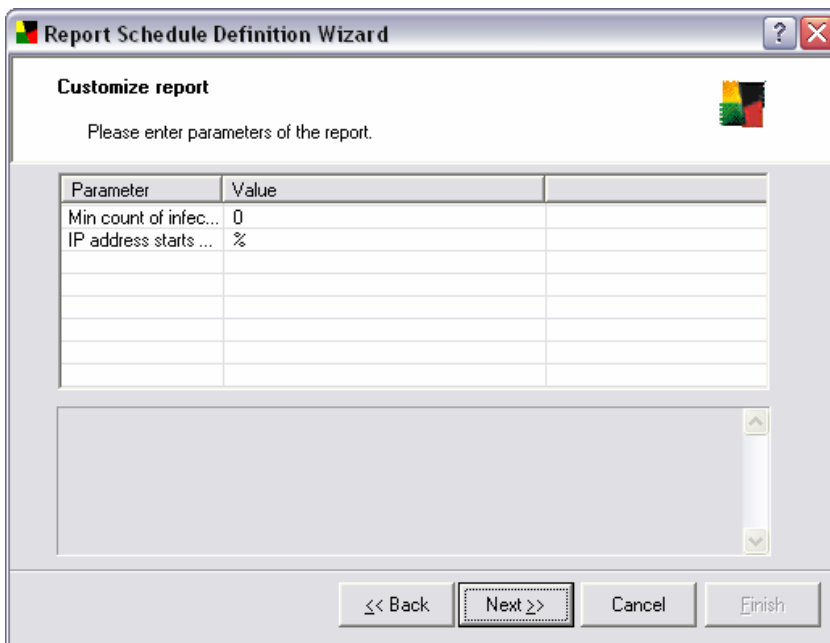

A new dialog will come up:

AVG 7.5

Fill in some **Name** and **Description**. Proceed to the next dialog by pressing the **Next** button.

From the rollover menu select which template do you want to use for your scheduled report.
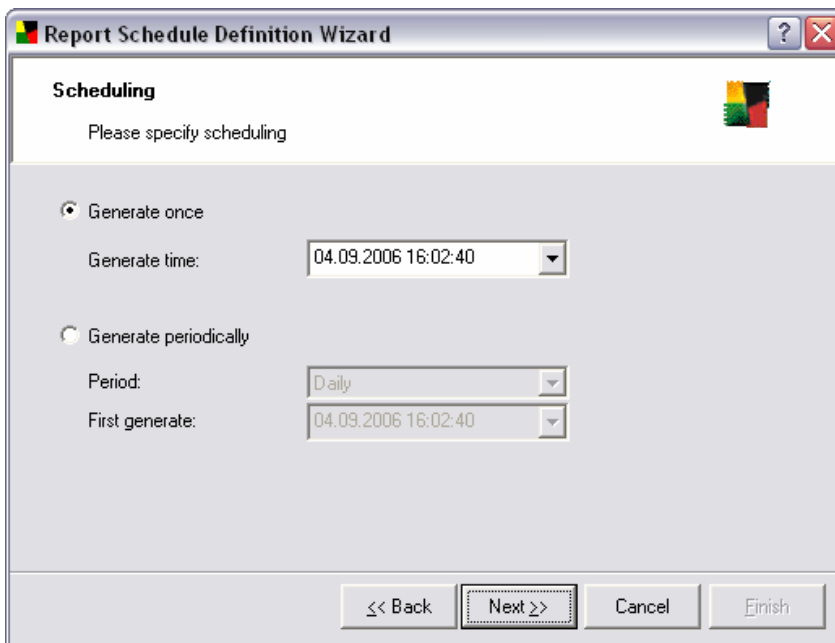
If there are additional parameters available for the selected report, fill in the requested values. You can leave it with default values as well. For more information on templates, see the templates section above. Once ready, press the *Next* button.
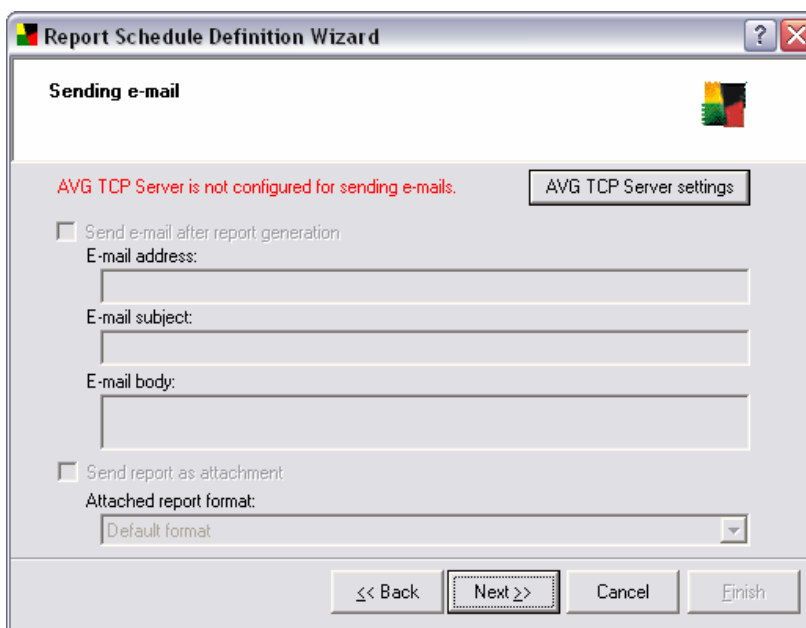
In this dialog, choose whether you want to generate the report only once in the selected time, or to generate the report periodically:

o **Generate once** - Choose the exact *Generate time* and date.

o **Generate periodically** - Choose *Period* (daily, weekly, monthly) for generation and *First generate* time and date.

Press *Next* to proceed to the next part:

AVG 7.5

AVG Anti-Virus Network

If you have already configured **Email** tab in the AVG TCP Server settings dialog, then you can skip this step and proceed to the next part. Otherwise, click the **AVG TCP Server settings** button to open AVG TCP Server configuration dialog.

To learn more about configuring **AVG TCP Server settings** for sending Email, see **Email tab** section in chapter 6.6. AVG TCP Monitor Advanced Mode.

If you want to send the report or notification by e-mail message when it is generated, enable the **Send e-mail after report generation** checkbox.

If you have already previously configured *Email* tab in the AVG TCP Server configuration, you should see predefined values already in the proper fields. If not, please check the AVG TCP Server settings or fill in your custom values.
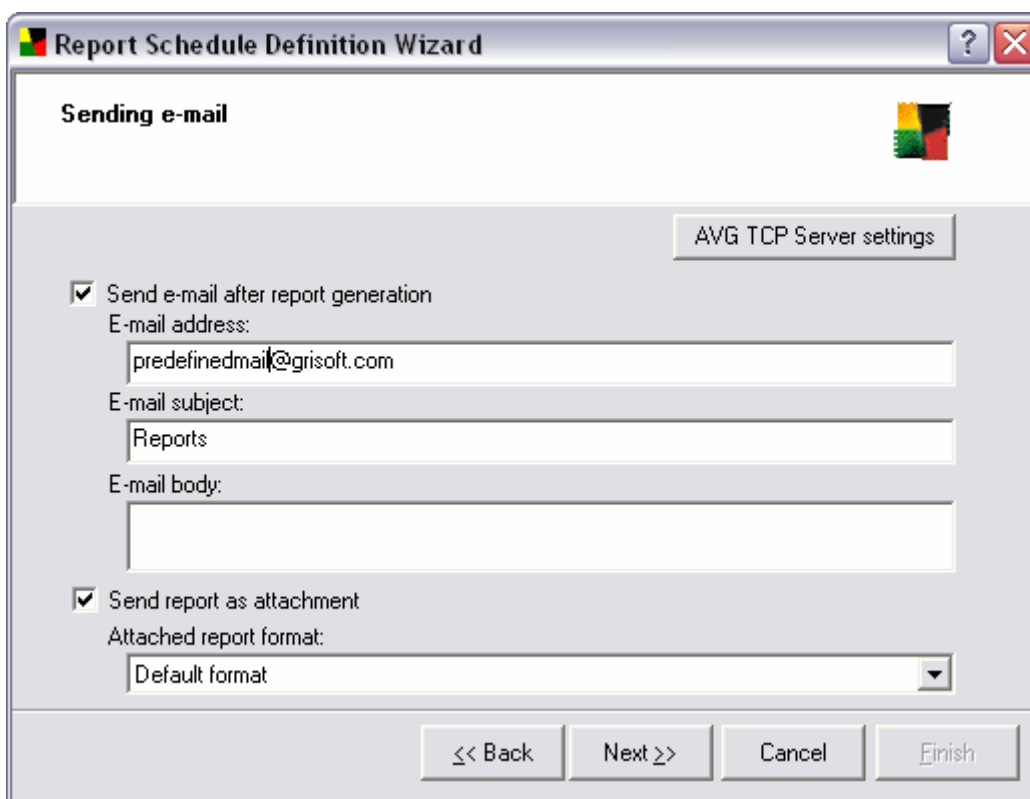
If you want to receive reports directly as an attachment, enable the *Send report as attachment* checkbox and from the rollover menu select, which format do you prefer for delivery of your report(s).

If you will not select to receive the report as an attachment, you will receive only notification e-mail and will have to review the report in AVGADMIN manually.

Once ready, proceed to the final screen by pressing the *Next* button. Here you can check if all settings are correct. Finalize the process by pressing the *Finish* button.

● **Generated reports**

This group contains list of all so far generated reports. The reports can be browsed:

o   *By template* - reports are sorted according to the predefined templates.

o   *By time generated* - reports are sorted according to a generation time.

o   *By scheduling* - reports are sorted according to a schedule type.

To work with individual reports, navigate to the chosen category. The list of generated reports will be displayed in the right section. You can double-click any report to open it, or select one or more reports and press *Delete* keyboard button to remove them.

If you open one of your generated reports, you can then print or save it as well.
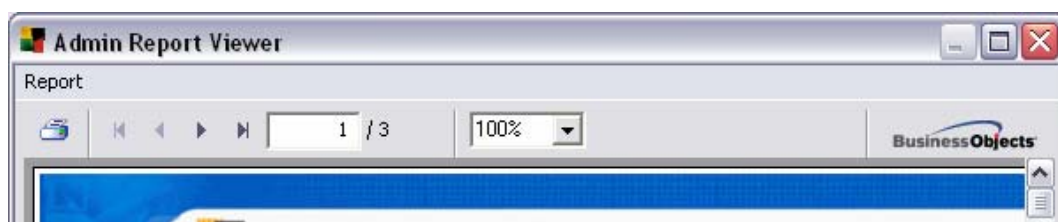
The report contains more than one page. To navigate through pages, use the left and right buttons at the top of the screen.

By clicking the printer 🖨 icon located in the top-left corner, you will open standard Windows print dialog, where you can choose to print the report on a printer(s) or produce a PDF file.

If you prefer to export the report to a file, use the *Report/Save* menu item. The confirmation dialog will appear where you can choose which output format do you prefer (Adobe Acrobat PDF, Comma Separated Values CSV, MS Excel XLS)

AVG 7.5

AVG Anti-Virus Network

10. AVGADMIN Advanced Interface

AVGADMIN Advanced Interface follows up the former **AVGADMIN 7.5** interface. The functionality available from the **AVGADMIN Advanced Interface** is the same as in the Basic Interface; however the reports used in the **AVGADMIN Advanced Interface** are more comprehensive and detailed compared to the Basic Interface. **AVGADMIN Advanced Interface** is intended for experienced administrators.

The **AVGADMIN Advanced Interface** opens in this environment:
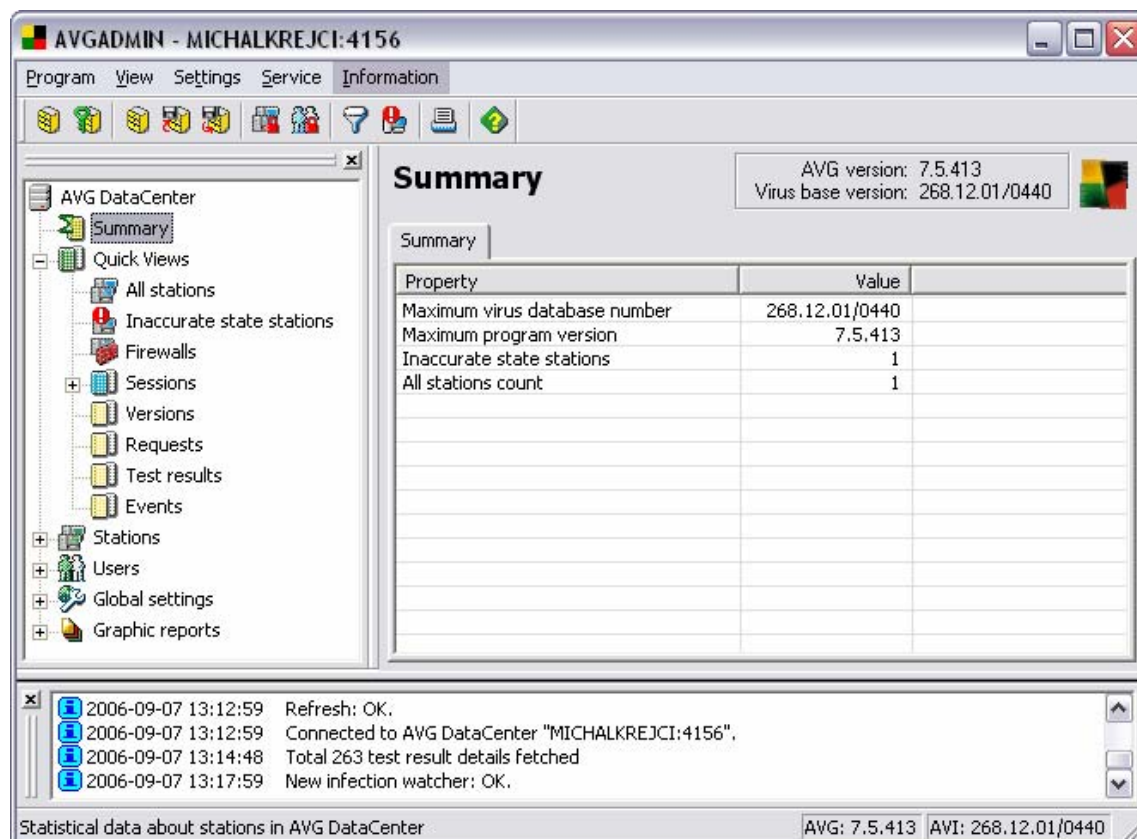
The window is divided into four sections:

● Program main menu (upper part)

● Navigation tree (left panel)

● Records section (central part)

● Status window (bottom part)

● Other control components

10.1. Program Main Menu

The program main menu offers the same options in both the Basic and Advanced interface of the **AVGADMIN** program.

For detailed information about menu items please see chapter 9.1. Program Main Menu.

10.2. Navigation Tree

The **Navigation Tree** contains all sets arranged in a hierarchical manner. A group is a data structure review, e.g. a list of workstations with their configuration, or test results table, etc. The group content itself is displayed in the *Records section*, in the central table.
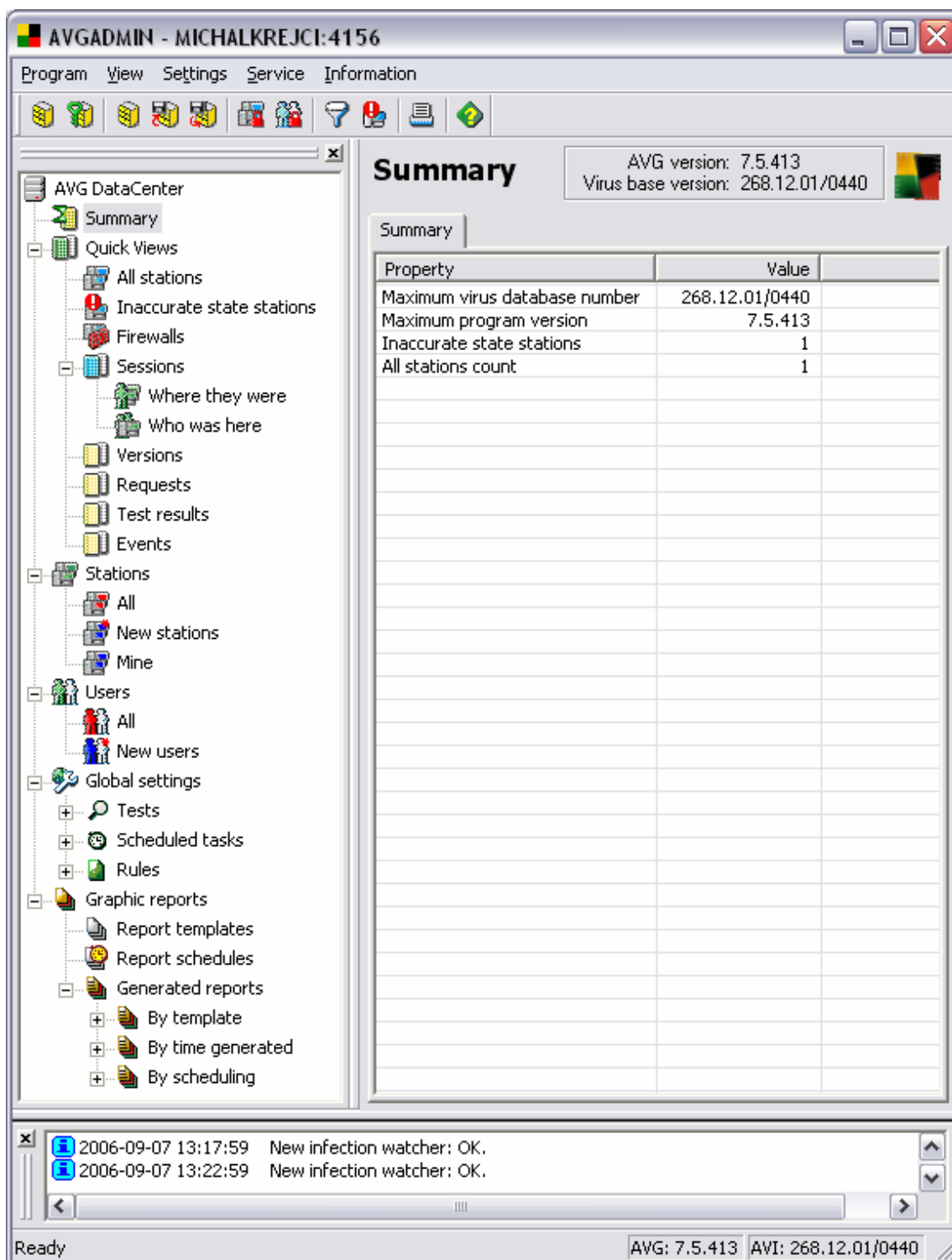
The **AVGADMIN Advanced Interface** Navigation Tree offers the following sets:

AVG 7.5

AVG Anti-Virus Network

- Summary

- Quick Views

- Stations

- Users

- Global Settings

- Graphic reports

a)   **Summary**

The *Summary* group offers an overall general information overview covering:

o   Maximum virus database number

o   Maximum program version

o   Inaccurate state stations *(see Quick Views – Inaccurate State Stations)*

o   All stations count

b)   **Quick Views**

The *Quick Views* group provides the administrator with structured information divided into the following categories:

o   **All stations** – An overview of all stations in the network accompanied by information on station description, version of AVG installed on a specific station, the Anti-virus database version, etc.

o   **Inaccurate state stations** – The station is taken for an **Inaccurate state station** if at least one of the administrator specified inaccurate state conditions holds good for that station. These conditions can be defined by the administrator within the **Inaccurate state conditions** dialog:

The **Inaccurate state conditions** dialog can be accessed from the application's main menu selecting the option **View/Stations visible in Quick Views/ Inaccurate state conditions**

If there are more stations reported as inaccurate state stations, the administrator can use the **Filtering** function to structure the overview and to make it easier to observe. From the main menu select the **View/Stations visible in Quick Views/Filter settings** to open the following dialog window:

The administrator can then select parameters from the list to define which of the inaccurate state stations should be displayed.

The group records can also be filtered according a selected item in the central table. There are two options of filter settings using the keyboard shortcut:

– **ALT + left mouse button** – AVGADMIN displays only records that have the same value recorded for the selected item parameters

– **ALT + right mouse button** - AVGADMIN displays only records that have different value recorded for the selected item parameters

Switching into another set of records shows all stations again. This filtering option can be used for all **AVGADMIN** sets.

o **Firewalls**

The **Firewalls** group contains a list of all network stations with firewall enabled.

Double click your mouse or press the **Enter** key to open Firewall configuration Dialog. Only certain settings are allowed to change because of safety precautions.

To review all settings and conditions in detail, see chapter 10.6 Firewall.

o **Sessions**

The **Sessions** group offers a structured overview of information on relations between stations, users, and specific AVG applications installed on workstations. The central table works with the following three tabs:

– **All** – an overview of all AVG applications running on all network workstations accompanied with the information on application user, the respective station, its IP address, etc.

– **Stations** – an overview of all AVG applications related to network workstations

– **Users** - an overview of all AVG applications related to users

Within the **Navigation Tree** the **Sessions** section further branches into the following two subsections:

– **Where they were** – Click this branch to open a new window with an overview of all users. Select a user from the list, and in the central table find the information on stations to which the selected user was/is logged in.

– **Who was here** - Click this branch to open a new window with an overview of all stations. Select a station from the list, and in the central table find the information on users that were/are logged in to the selected station.

o **Versions**

The **Versions** group offers an overview of operating system versions and AVG versions installed on a specific workstation. The group uses the following two tabs:

– **Windows** – an overview of OS Windows versions installed on workstations, and number of respective OS version installations

– **AVG** – an overview of AVG versions installed on workstations, and number of respective AVG version installations

o **Requests**

The **Requests** group offers an overview of all requests divided into categories of completed and uncompleted requests. On specific category-related tabs you can then find more detailed information related to the actual message.

o **Test results**

The **Test results** group offers an overview of all test results on workstations together with detailed information related to specific tests. The other two tabs of the central table the divide the test results into two groups:

– **All**- displays list of all test results.

– **Infected** – displays only positive test results.

– **Resident shield**– test results reported by the **Resident Shield**

Other **Test results** settings and control features are identical with the Basic interface.

o **Events**

The **Events** group offers an overview of all events divided into categories of **Requests**, **Warnings**, **Errors**, and **Critical events**. On specific

AVG 7.5

category-related tabs you can then find more detailed information related to the actual event.
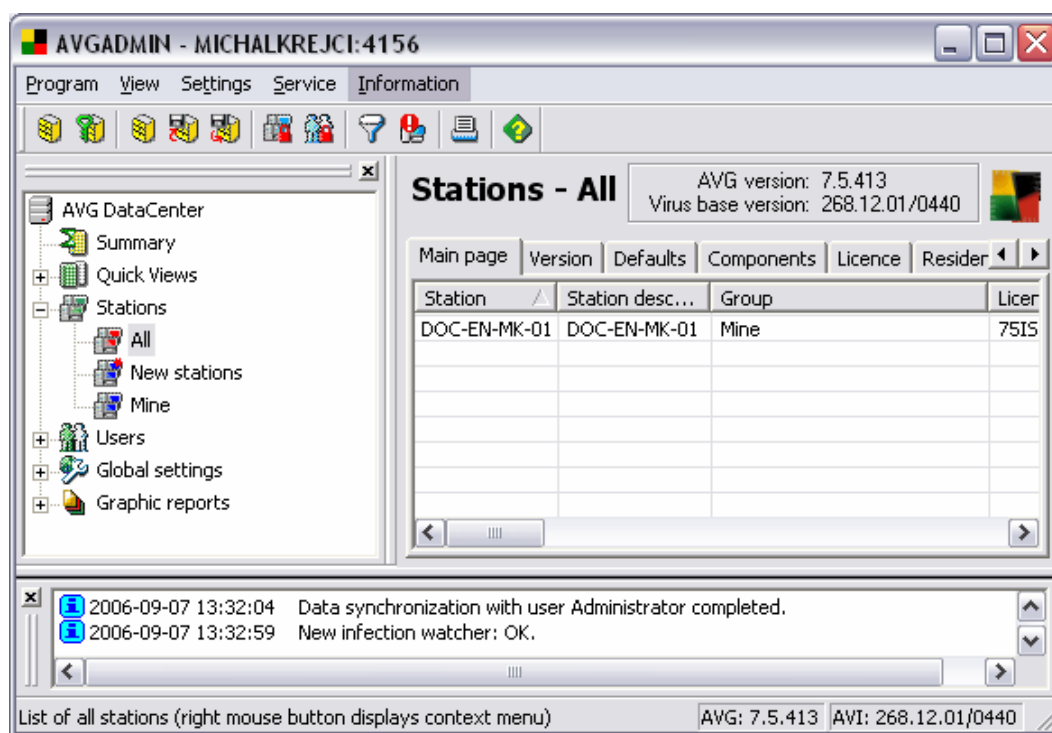
c)   Stations

The **Stations** group offers an overview of all stations known in the **AVG DataCenter**. The record of a station is created once the station first logs in to the **AVG DataCenter** or it can be created manually by the administrator.

The administrator is allowed (using the context menu over the table of groups of stations displayed in the **Records section**) to create groups of stations, and to assign a separate station into specific groups.

By default, the stations are divided into two groups:

o   **All** – automatically includes all stations connected to the **AVG DataCenter**

o   **New stations** – contains only stations that have not been assigned to any administrator defined group yet

In the **Records section** you can then find information related to specific stations. Using the tabs, the information is divided into several categories – see the screenshot:
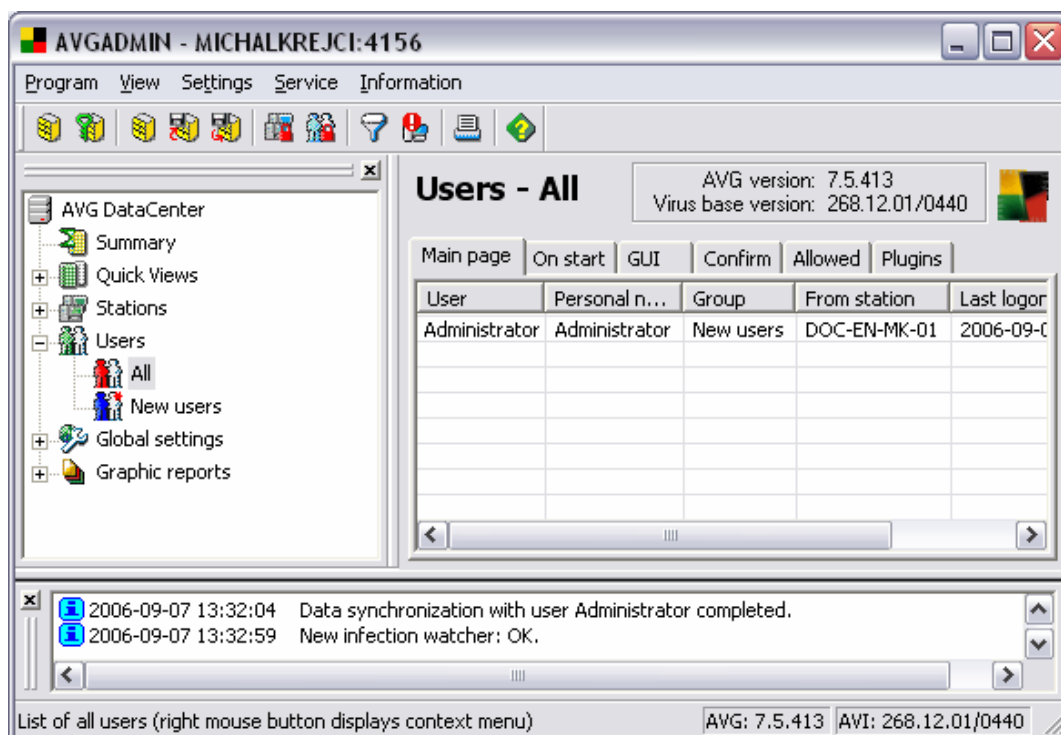

d)   Users

The **Users** group offers an overview of all users known in the **AVG DataCenter**. The record of a user is created once the user first logs in to the **AVG DataCenter** or it can be created manually by the administrator.

The administrator is allowed (using the context menu over the table of groups of users displayed in the **Records section**) to create groups of users, and to assign each user to a specific group.

By default, the users are divided into two groups:

o   ***All*** – automatically includes all users connected to the **AVG DataCenter**

o   ***New users*** – contains only users that have not been assigned to any administrator defined group yet

In the **Records section** you can then find information related to specific users. Using the tabs, the information is divided into several categories – see the screenshot:

e)   **Global settings**

The ***Global settings*** group includes the possibilities of global tests, plans, and rules maintenance. The administrator usually needs to create a group of tests/plans/rules and to assign them to individual users/stations/groups. The ***Global settings*** group contains an overview of all tests/plans/rules registered in the **AVG DataCenter**. The administrator can then easily change their configuration, create new tests, plans, or rules, delete the old ones, and assign them to their respective owners.

f)   **Graphic reports**

This group offers graphic reports. It allows users to quickly and easily generate well arranged reports. Reports may show a summary of stations managed by AVGADMIN, top infected stations, top virus occurrences and similar statistics.

Users can select from pre-defined templates and produce the reports by simply double-clicking, schedule reports creation at a customized time period, send generated reports to e-mail addresses or print reports to PDF file or printer.

To learn more about Graphic reports and its configuration, see chapter 9.7 Graphic Reports.

10.3. Records Section

Within the central table in the *Records Section* of the screen you can view data of the group specified within the navigation tree. Some sets may contain a considerable amount of data for a specific record (e.g. workstation/user information); that is why the relevant data are arranged into groups, and every group can be displayed when you select the corresponding tab.

To select a record from the central table you need to perform a mouse click over the desired record. You can select more records at the same time: press the *CTRL* key (adding a new record to the current selection), or the *SHIFT* key (selecting all records between the first and the last highlighted record). Click the mouse right button over the selected record to open the *Context menu*. It is possible to call various actions related to the current selection from the *Context menu*.

Within the central table of the records section you can use the *quick search* option: this option allows searching for records according to the record value specified in the central table first column. The search is activated by the *CTRL+F* keyboard shortcut; to confirm the search keyword hit the *Enter* key. The *Esc* key will cancel the search. The search identifies all records that respond to the specified search parameter, and the first search result of the search results list will be highlighted – to switch among the search results use the *F3* key.

10.4. Status Window

In this part of the **AVGADMIN** main window you can find various system notices and information on the application functionality, communication with **AVG clients**, detected problems, positive test results warnings, etc.

10.5. Other Control Components

a)   Navigation bar

The Navigation bar can be found in the upper part of the Records section above the central table with records.

b)   Tool bar

The Tool bar can be found under the application main menu; the icons represent specific main menu options and act as quick links for selected operations.

c)   Status bar

The Status bar can be found at the very bottom of the screen; the status bar displays the help file for specific menu items, and application status information.

d) **Context menu**

The Context menu can be opened from any selected item listed in the central table by a right mouse-button click; the context menu items differ according to the content of the item to which the context menu relates.

10.6. Firewall

The Firewall configuration dialog contains the following tabs:

- General

- Profile

- Profile switch

- Applications

- System

- Networks

- Log

Note: If you have older (7.1) versions of AVG installed on some workstations which are connected to the AVG Datacenter, configuration editing and synchronization of the Firewall is still possible from the most current version of AVGADMIN. However, such actions must be applied on an individual basis (i.e. not via shared station settings).

As many new features were introduced in the AVG 7.5 Firewall version, these settings will not be applicable for 7.1 workstations, but the rest of the settings will work fine.

*If you are going to edit **Shared settings for workstations** and there are still 7.1 AVG versions in your network, you will see a message box with information about converting Firewall settings to the most current version (reflecting AVG 7.5). If you convert the settings to the newest version, then your older workstations with AVG 7.1 will not be able to synchronize their Firewall settings until you upgrade them to 7.5 versions.*

Even though the compatibility works as described, we still recommend that you keep all workstations up to date and install the latest AVG version on all workstations.

General note about Firewall synchronization background:

If the Firewall configuration is not set as mandatory in AVGADMIN, a copy of the whole local configuration is transferred to the DataCenter (including areas, interfaces, rules assigned to a physical interface, etc,) The station's current settings are therefore visible in AVGADMIN.

If the Firewall configuration is set as mandatory in AVGADMIN and editing is being done from AVGADMIN on the stations-level (i.e. not in the shared settings), then the complete configuration is transferred to the client. However, interface and area objects are omitted from the configuration as these are not changed on the client, they are only merged to the DataCenter. Activation of a profile remotely using

AVGADMIN is only possible when the *Area detection and profile switch* feature is disabled.

It is not possible to assign profiles to interfaces, because this feature is dependant upon the hardware fitted to the individual workstation, and AVGADMIN cannot evaluate the station's hardware. Assigning applications to only a specific interface is possible. However, if hardware changes are made, such settings will now point to non-existent connections, and the new connections will thus be given the default connection settings rule as defined by AVG.

If the configuration is set as mandatory in AVGADMIN, and editing is being done via shared settings, all interfaces are removed from the configuration and all references to them are removed from the rules. Further, all area objects are also removed.

Assigning profiles to areas is not possible either. Physical interfaces will be visible on the client, but rules will be set for the configuration as a whole.

If the configuration is copied from one station to another, all interfaces and areas are adjusted according to the current ones during the next synchronization.

a) General
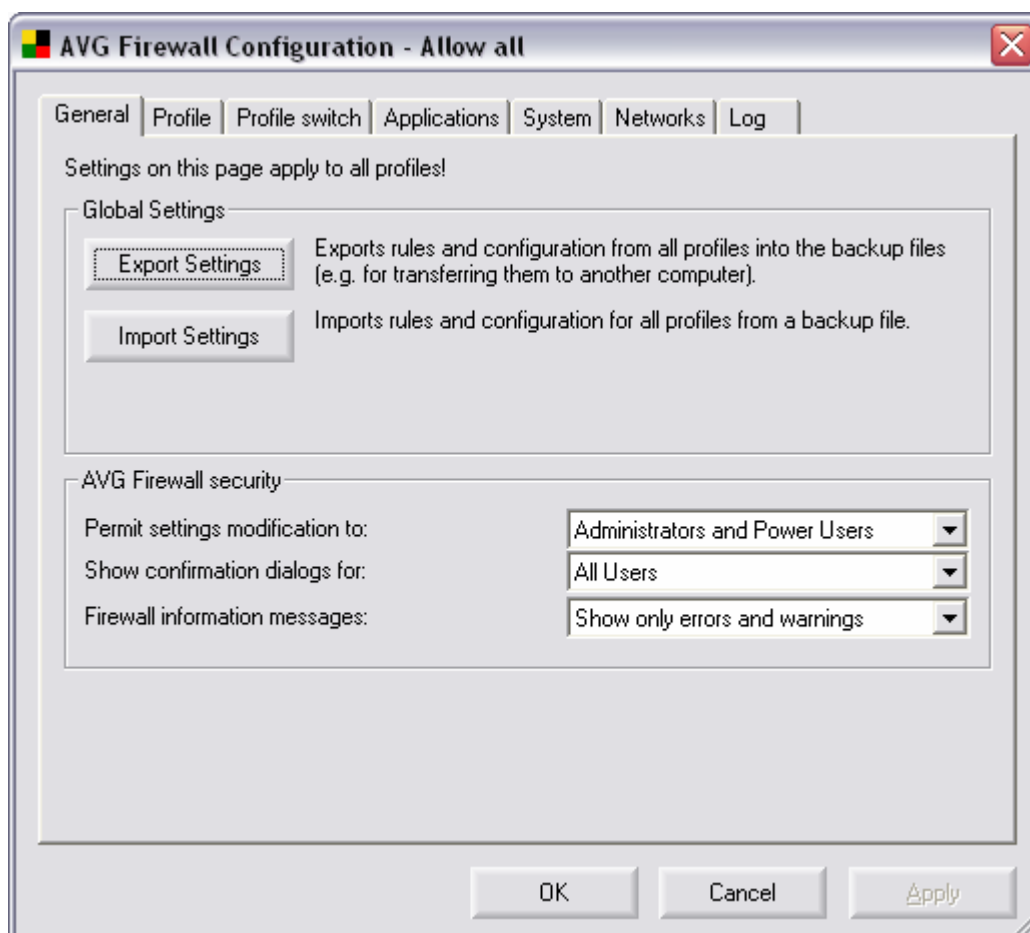
The *General* tab offers an overview of the **Firewall** settings parameters that apply to all profiles. The tab is divided into three sections:

o **Global settings** – using the *Export settings* / *Import settings* buttons you can export the defined **Firewall** rules and settings to the back-up files, or on the other hand to import the entire back up file.

o **Firewall Security** – in this section you can define rules for the **Firewall** configuration rights. Specify who should be allowed to modify the **Firewall** settings, and to whom the confirmation dialogs and Firewall information messages should be shown. You can select from the following three categories with a different authority level:

- *Administrator* – controls the PC completely and has the right of assigning every user into groups with specifically defined authorities

- *Administrator and Power User* – the administrator can assign any user into a specified group (Power User) and define authorities of the group members

- *All Users* – other users not assigned into any specific group

b) Profile
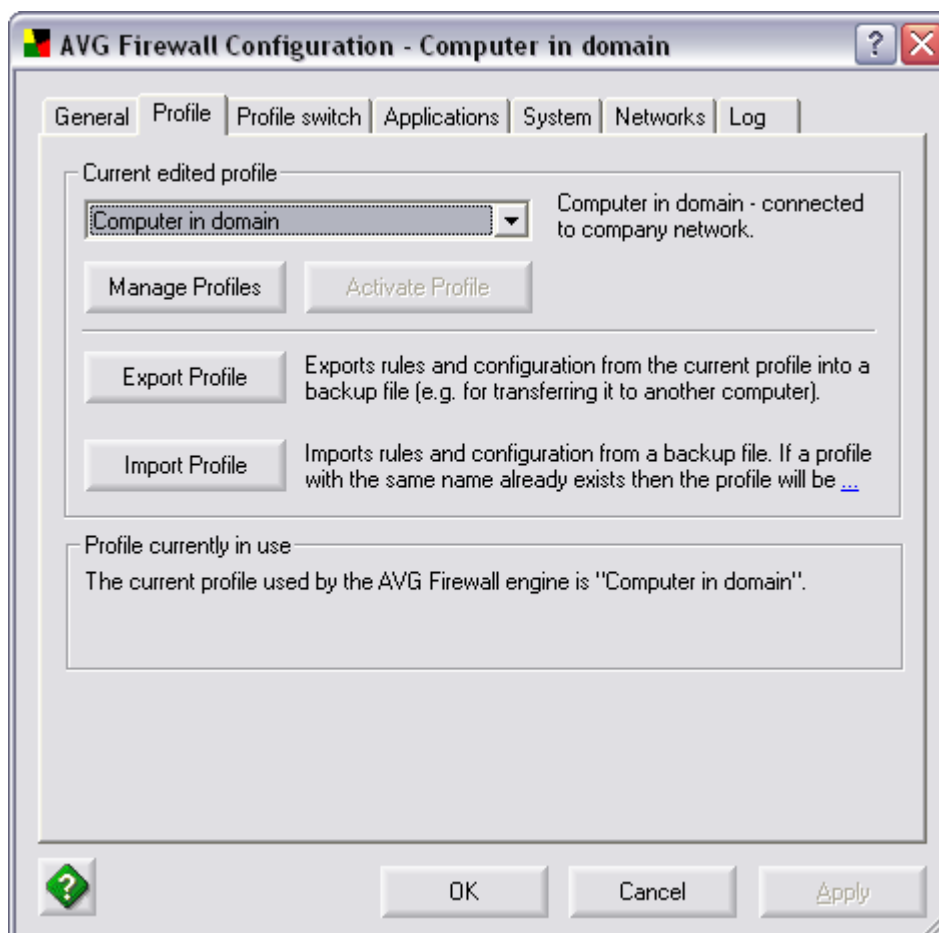
On the *Profile* tab you can select the desired **Firewall** profile (profile specification option is available on the following operating systems only: Windows NT/Win2K/WinXP). The main principle of *Profile* selection is the possibility to set different **Firewall** security levels.

For example, consider the two following profiles – *Computer on the move* and *Computer in domain*. During a business trip, you may wish to connect your notebook to the internet from a hotel or at the airport. Here the risk to your computer will be significantly higher than while connecting to the company network. For this reason, we recommend that you define, and set up, a specific *Computer on the move* profile - with parameters that will ensure a higher protection level. However, the *Computer in domain* profile could be defined with a lower security level. In addition, the *Computer in domain* profile could allow some services that would not be required or desired while you are on a business trip (e.g. file sharing).

Typically you can select among the following profile options:

o   Allow All

o   Block All

o   Computer in domain

o   Computer on the move

o   Standalone computer

By default, the profile generated based on parameters that you have specified within the **Firewall Automatic Configuration Wizard** will be used.

*Note: You cannot use **Automatic Configuration Wizard** from AVGADMIN, but the predefined configuration already contains rules for AVG applications and components. Other rules must be created either manually (see part d), or on a sample workstation by using **Automatic Configuration Wizard** and then copy this configuration where needed.*

Each profile covers specific settings of your PC, and an adequate **Firewall** security level is assigned to each of the profiles. The proper profile option can be selected from the drop-down menu; then confirm your choice using the **Set active profile** button.

Setting the **Firewall** profile you can use the following two operating buttons:

o   *Manage profiles* – opens a new **Manage profiles** dialog where you can edit each specified profile and add new custom profiles.
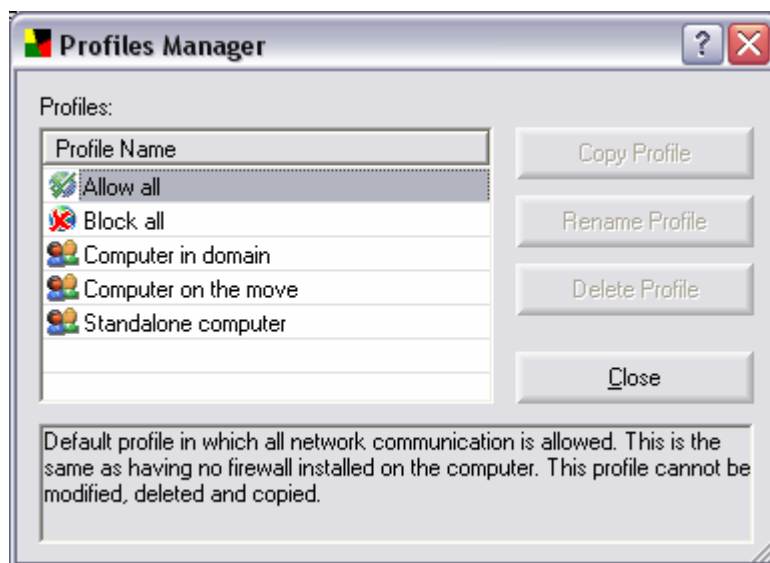
The following buttons can be used:

–   *Copy profile* – makes creating a new profile easier and more comfortable for you: To use this option, highlight a profile in the list of profiles and press the *Copy profile* button. A new profile will be created with predefined parameters taken from the definition of the cloned profile. Then you can easily edit the parameters for the new profile.

–   *Rename Profile* – press this button to enable editing of the selected profile name

–   *Delete Profile* – press this button to delete the selected profile from the list (unless the profile is currently used)

–   *Close* – closes the **Manage profile** dialog

o   *Activate profile* – use this button to confirm the profile selection, or any changes made to the profile settings

In the bottom part of the **Profile** tab you will find the *Export profile/Import profile* buttons that allow you to export the defined **Firewall** profiles into the back-up files, or on the other hand import the entire back-up profiles.

c)   Profile switch

On the *Profile switch* tab you can manage network areas and local network interfaces. You can assign specific profiles to local interfaces and network areas.

Note: *You will not experience the below described dialogs from within AVGADMIN. These will be displayed only on workstations. You can use AVGADMIN only to configure the areas.*

AVG 7.5

AVG Anti-Virus Network

Whenever you connect to a new (unrecognized) connection, the **New area** dialog will appear. Here you should select the most appropriate profile for the current network connection, then click on **Assign Profile**.
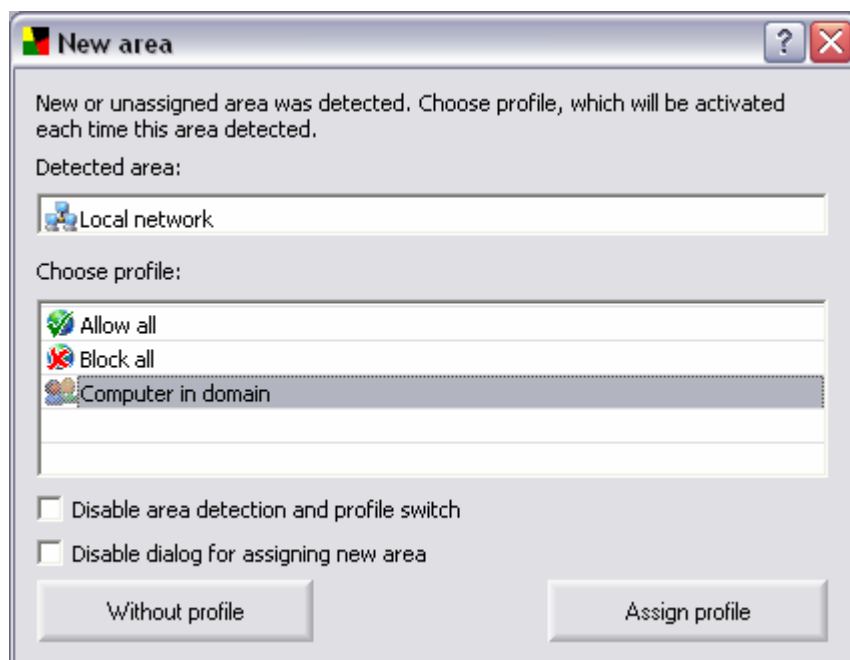

o   **Detected area** - indicates the type of network connection that has been detected. You can rename the area, by clicking the text field to make it more convenient for remembering if you are using more connections on a regular basis.

o   **Choose profile** - contains a list of available profiles. Choose the most suitable profile.

o   **Disable area detection and profile switch** - tick this checkbox to disable the whole Profile detection feature.

o   **Disable dialog for assigning new area** - tick this checkbox if you prefer not to display the **New area** dialog anymore. The default profile will then be automatically assigned.

Working buttons are as follows:

o   **Assign profile** - Once you have clicked on this button, the selected profile will always be automatically associated with this connection, and in the future, this dialog will not be displayed when connecting to this connection.

o   **Without profile** - press this button to keep the connection type without a profile. The Firewall will ask you again, each time when this connection type is found. To disable this window, (before confirming your choice) tick either **Disable area detection and profile switch** checkbox to disable the entire area detection system, or **Disable dialog for assigning new area** checkbox to disable the confirmation dialog (profile will be assigned automatically).

**Note:** The above dialog is visible only on stations.
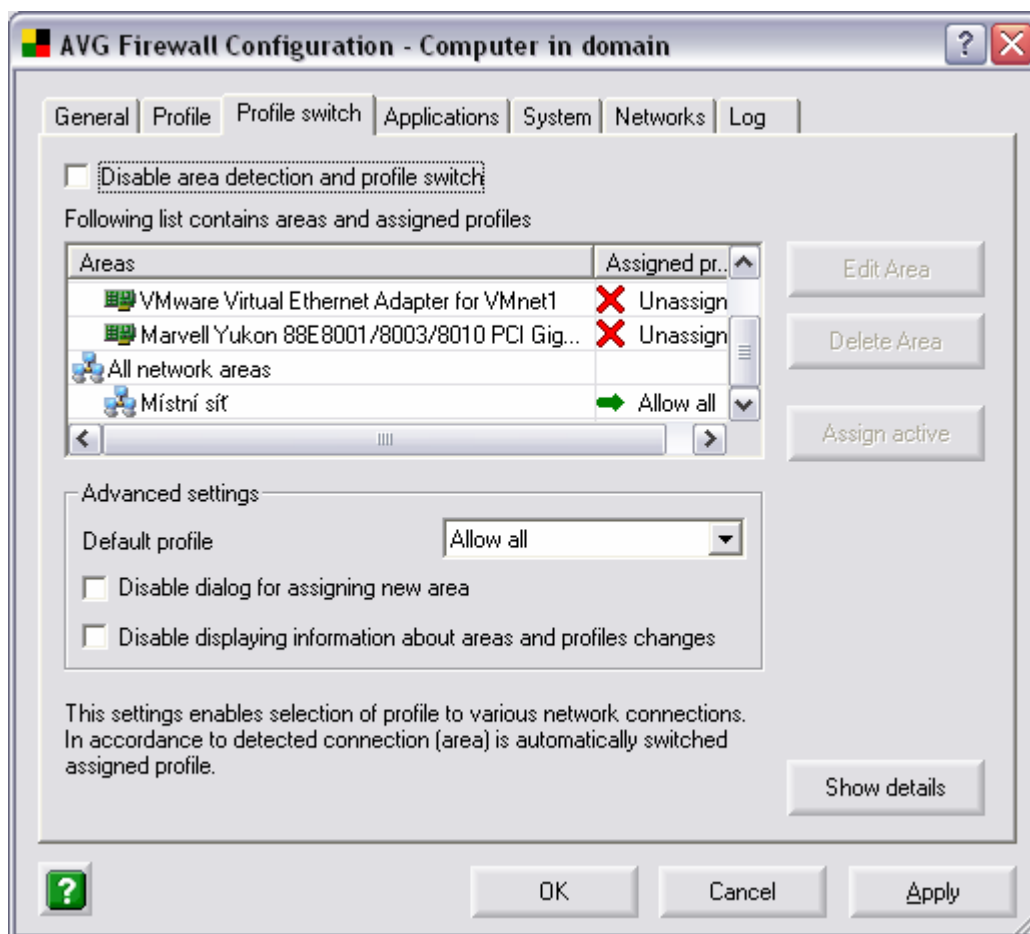
Users on workstations can setup separate profiles for each connection type and/or network interface and then assign them as preferred.

Note: Only limited configuration options are available from the AVGADMIN! Most of the settings are hardware-dependent and cannot be changed from within the AVGADMIN.

To disable this feature, simply tick the **Disable area detection and profile switch** checkbox.

To view more details about selected network area, click the **Show details** button.

The main list contains areas and assigned profiles.
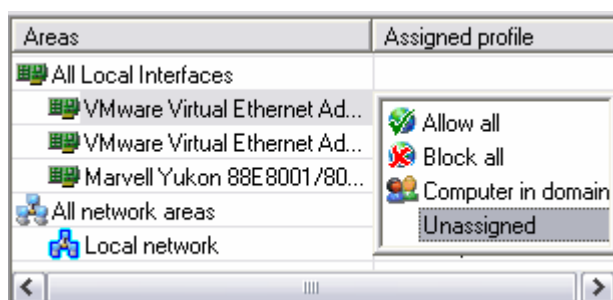
AVG Anti-Virus Network

If you do not want to specify a profile for a specific interface or area, simply leave the option as *Unassigned*.

o   To change the network area name, select the area you want to rename and click the *Rename* button.

o   To delete the network area, select the desired area and click the *Delete* button.

> *Please note: If you delete all network areas, or when there is no network area present in the list, a new button* **Assign active** *will appear. By clicking this button, you will simply assign the currently active network area.*
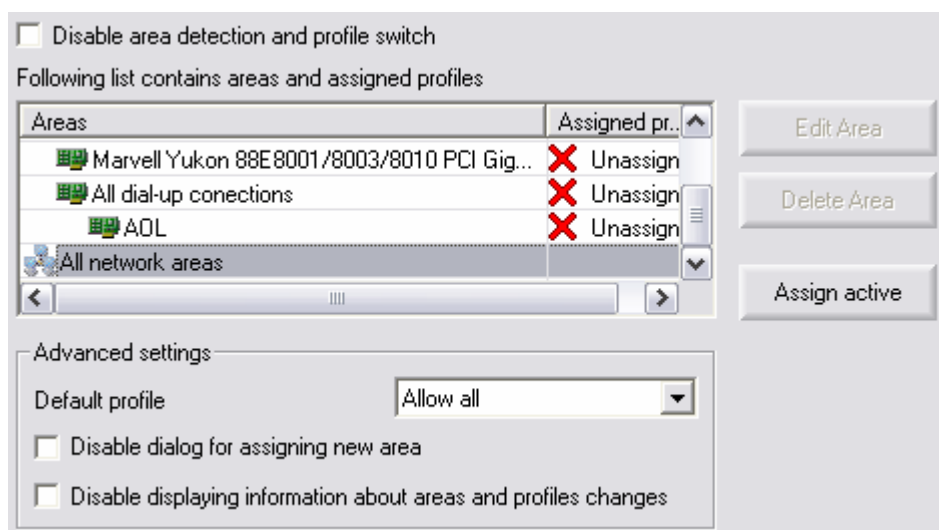
Advanced settings:

o   *Default profile* - this profile will be automatically activated when:

–   A new area is detected.

–   An error occurs during new area detection (for example when there is no active connection type).

–   An area with no assigned profile is active.

o   *Disable dialog for assigning new area* - tick this checkbox if you prefer not to display the *New area* dialog. The default profile will then be automatically used.

o   *Disable displaying information about areas and profiles changes* - tick this check box to disable displaying information about areas or profiles changes in the tray area.

Please note:

AVG Anti-Virus Network

(i) Assigning a profile to a network interface has a higher priority than to a network area. This means that once you assign a profile to your network interface, it will be always used regardless of the network area.

(ii) When in safe mode, automatic profiles will be disabled.

d) Applications – Basic Settings
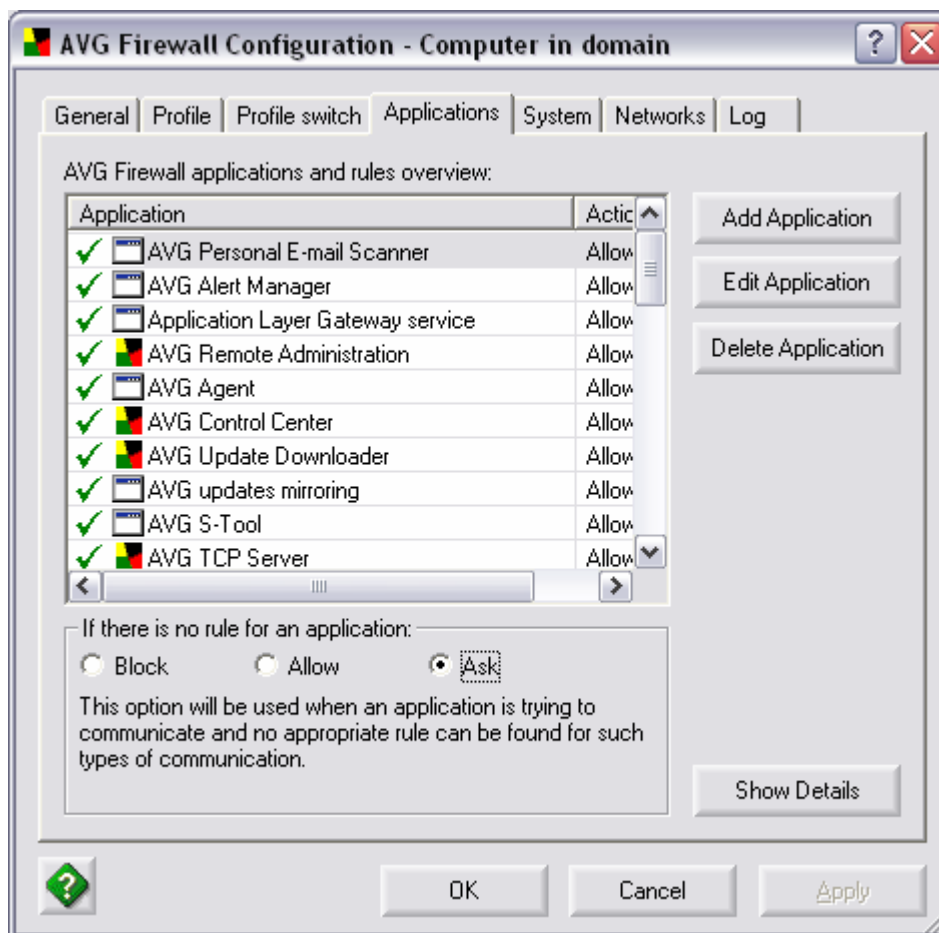
In the main section of the **Applications** tab you can see the list of all applications, and the list of rules that have been created for each application. In the list of applications, there is always one of the following signs displayed left to the icon and the name of the respective application:

o ✔ Allow

o ✘ Block

o ❓ Ask

o ⚙ Advanced settings

*For detailed information on specific actions please refer to chapter*

Click this sign to change the rule assigned to the currently highlighted application by selecting another action from the newly opened context menu:

AVG 7.5

Press the **Enter** key to confirm your choice, or the **Esc** key to cancel it.

The **Applications** tab offers the following operating buttons:

o **Add/Edit Application** – these buttons open a new **Application Properties** dialog window where you can create (edit) a new rule for a specific application. Within the dialog you need to provide the application's name, the path to the application's current location on your hard disk, and you must assign the relevant action to the application (e.g. an action to be taken when the application attempts to communicate on any network port).
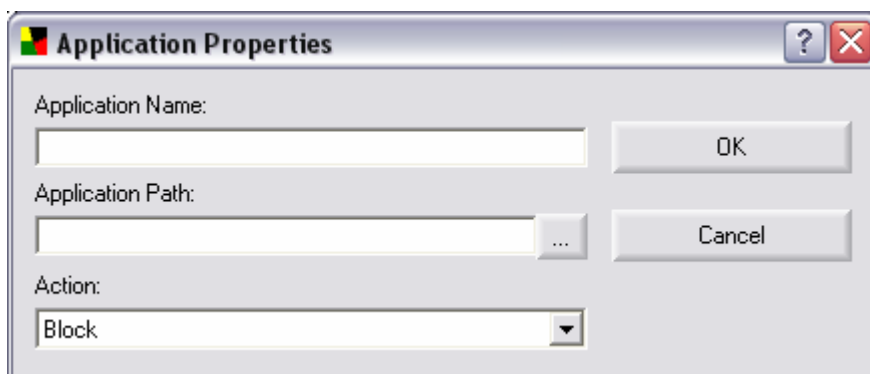
o **Delete Application** – this button deletes the rule defined for a specific application, and removes the application and its relevant action from the list within the **Applications** tab of the **Firewall Configuration** dialog window.

o **Show/Hide Details** – in the same dialog window, this button provides a brief overview of detailed information referring to the application currently highlighted in the list of applications:

- **Application** – name of the application

- **File path** – current location of the respective application

- **Action** – action assigned to the respective application
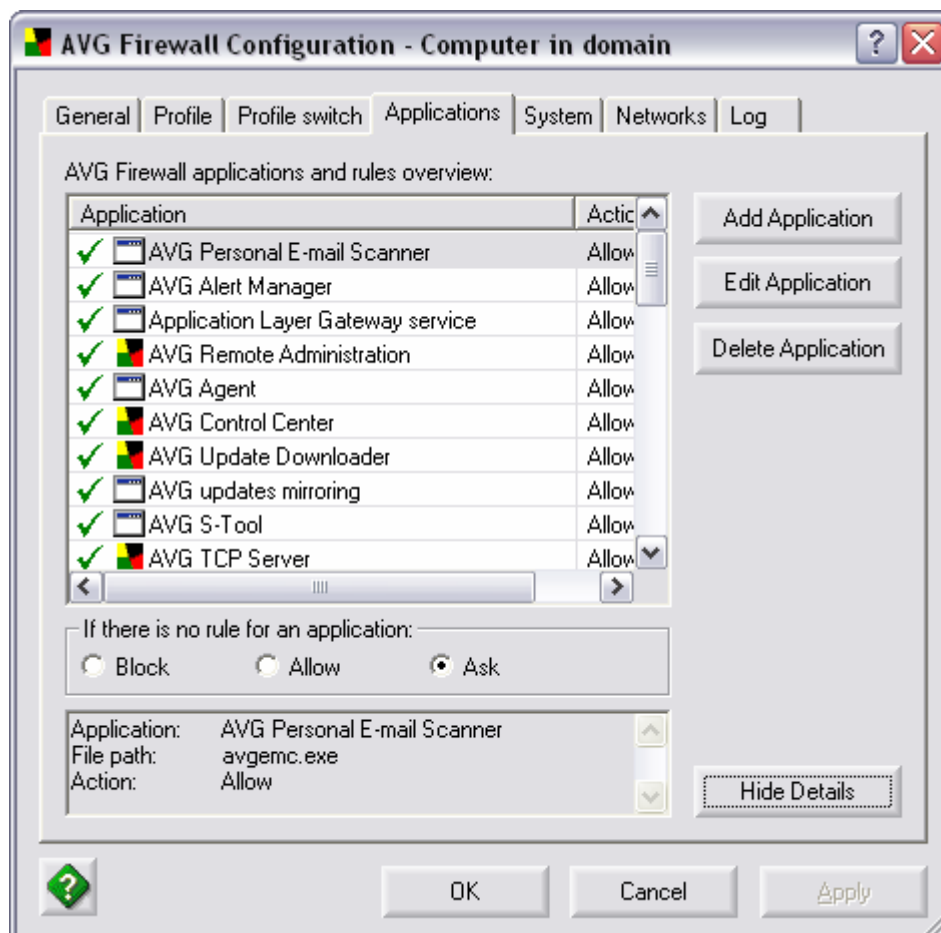
On the **Application** tab you can also find a section named **If there is no rule for an application**; here you should specify what action should be performed in case a new application attempts to communicate over the network and there is no rule specified for this application in the **Firewall** yet.

e) **Applications – Advanced Settings**

Note: Use of the Advanced Settings can be recommended to well experienced users only!

The **Applications** tab also allows you to configure advanced settings for specific application. For a new application, use the **Add Application** button

and in the newly opened **Application Properties** dialog select the **Advanced configuration** option within the **Action** section.

If you have already selected an application with the advanced settings from the list of applications in the **Applications** tab, the **Application Properties** dialog opens with the following extended interface:
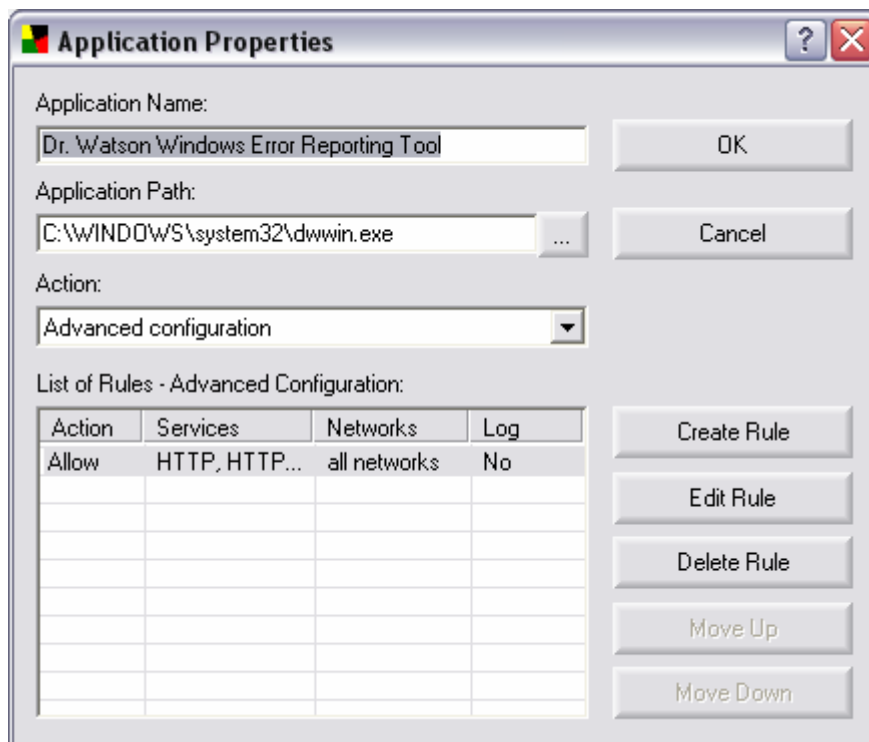
The following control buttons are available in the extended **Application Properties** dialog:

o **Create Rule/Edit Rule** – opens the same **Application Rule** dialog where you can define parameters for a new application rule, or edit parameters of an existing application rule.

o **Delete Rule** – removes the currently selected rule from the list of rules.

o **Move Up** – moves the rule one position up in the list of rules.

o **Move Down** - moves the rule one position down in the list of rules.

In the bottom part of this dialog you can see a new section named **List of Rules – Advanced Configuration**. This section contains information divided into four columns:

o **Action** – brings information on an action type assigned to the selected application

o **Services** – brings information on a network service assigned to which the application rule relates

o **Networks** – brings information on a network to which the application rule relates

o **Log** – provides information about whether the selected application events are being recorded into the log file

The following control buttons are available:

o **Create Rule** – opens a new **Application Rule** dialog where you can define a new rule for the selected application:
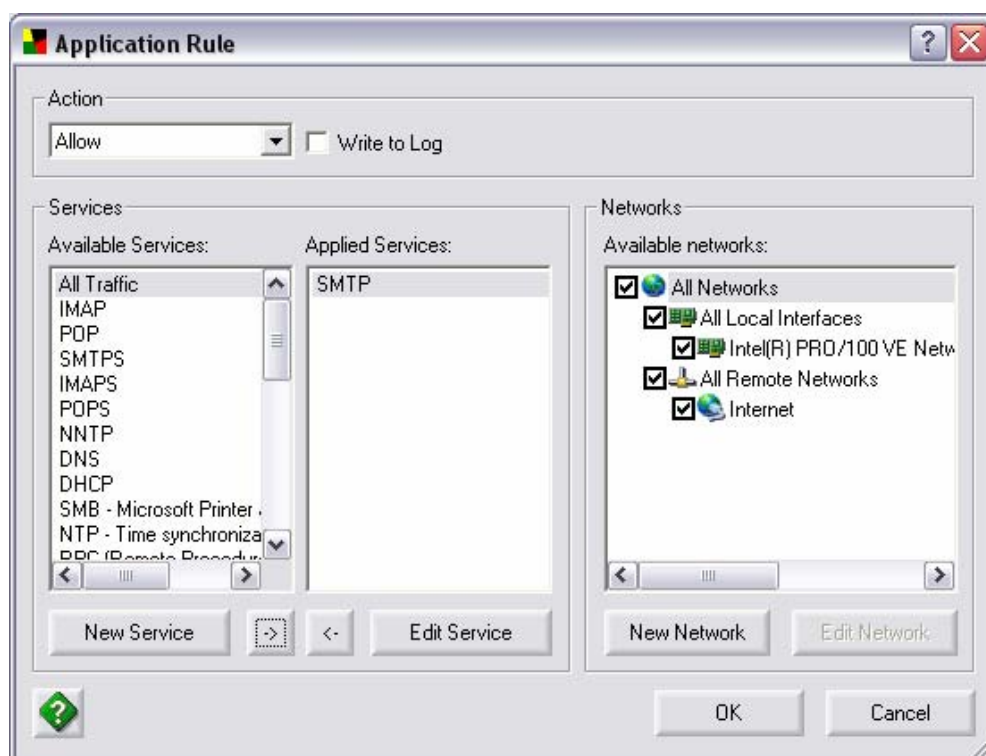
The dialog is divided into three sections:

o **Actions** – from the drop-down menu select an action that should be performed in case all network communication conditions (as defined I the bottom part of this dialog) are met. The available action types are Block / Allow / Ask.

The **Actions** section also contains the **Write to Log** item – mark this option if you want the application's communication to be recorded in the **Firewall** log file.

o **Services** – this section offers two lists of services:

– **Available Services** – list of services defined for the application in the default configuration, and services that have already been defined by the user

– **Applied Services** – list of services covered by the defined application rule. This list is a subset of the Available Services list.

You can move items between both of the lists using the **->** or **<-** buttons respectively. Moving an item from the list of **Available Services** to the **Applied Services** list means the service will be considered for the respective application when applying this rule.

There are two control buttons in the **Services** section:

- New Service/Edit Service – opens a new **Service Properties** dialog where you can specify the new service parameters/edit parameters of already defined service:
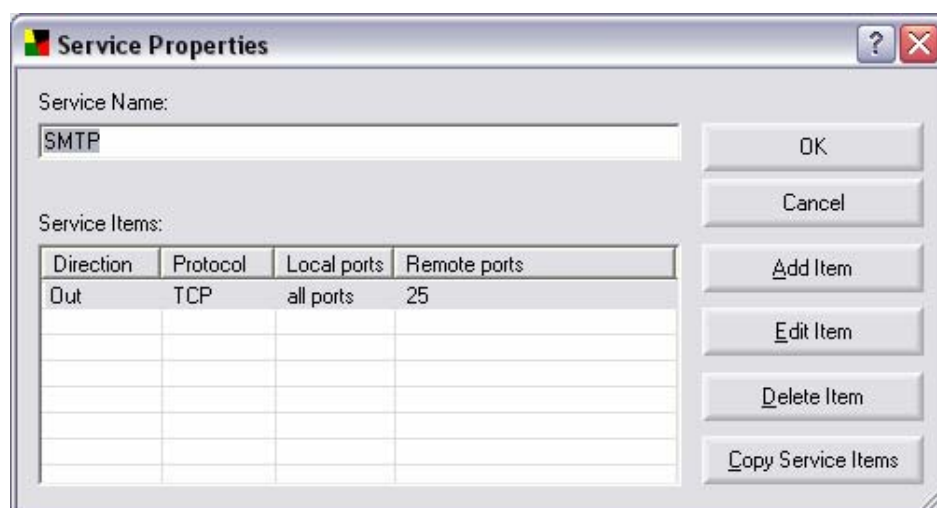

In the **Service Properties** dialog specify the service name in the **Service Name** field. The dialog contains the following control buttons:

- Add Item/Edit Item - opens a new **Service Item** dialog where you can define (edit) parameters of specific service items (Protocol, Direction of communication, Local Ports, and Remote Ports):

AVG Anti-Virus Network
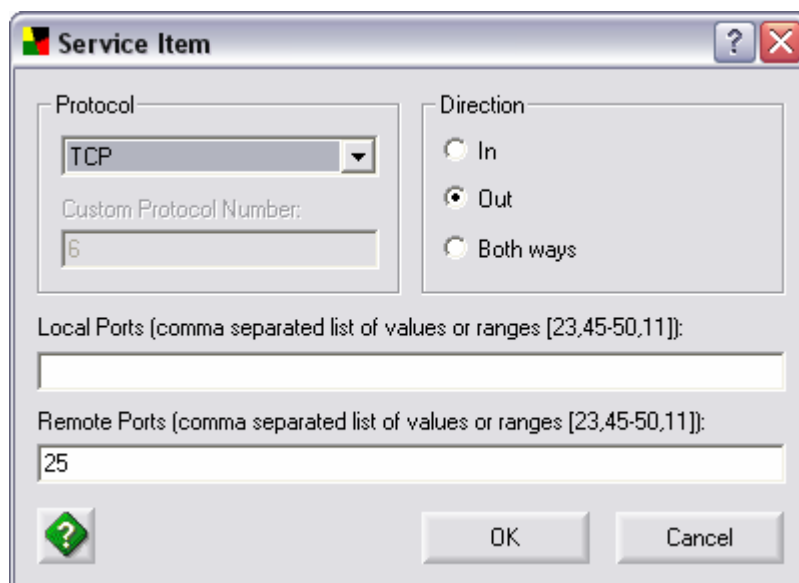
- **Protocol** – select a predefined protocol from a drop down menu, or select the option of **Custom protocol** and then provide the standard protocol number in the **Custom Protocol Number** field (the "0" value stands for all protocols).

  - Direction – define the service direction

  - Local Ports – list all local ports or define a range

  - Remote Ports - list all local ports or define a range

- **Delete Item** – removes the selected item from the **Service Items** list.

- **Copy Service Items** – makes it easier to create a new service item record using the possibility of copying the already defined parameters of an existing item. The button opens a new **Select Service** dialog where you are offered a list of services; select a service whose items you want to copy:
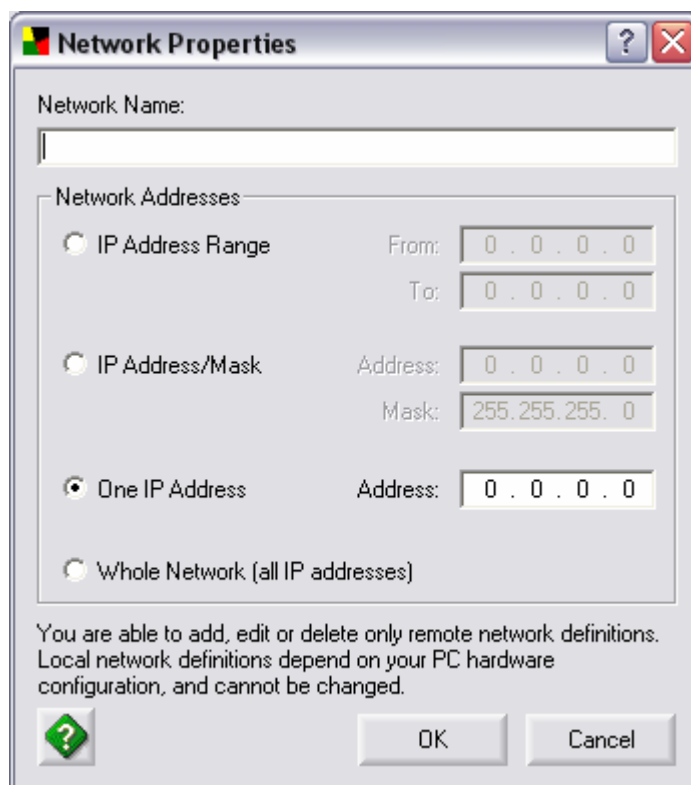
AVG 7.5
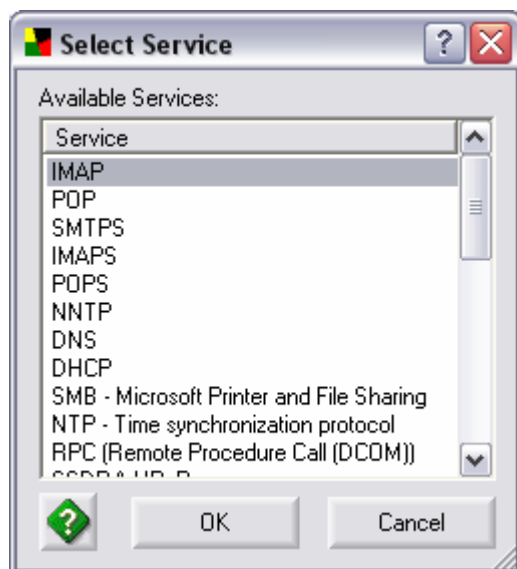
AVG Anti-Virus Network

o   ***Networks*** – this section offers a control tree providing a list of available networks. Mark the check box for each network to which the respective application rule should be assigned.

There are two control buttons in the ***Networks*** section:

–   ***New Network / Edit Network*** – opens a new **Network Properties** dialog where you can define (edit) new network parameters: ***Network Name*** and ***Network Addresses*** (specified by the IP address range):

f)   System

Any editing of the System tab parameters is recommended to experienced users only!

The ***System*** tab opens an overview of rules specified for system services that need to communicate over the network. Compared to the applications, there are only two kinds of actions that can be assigned to a system service:

o   ***Allow*** – signed by the green check mark before the system service's
      name

o   ***Block*** - signed by the red cross mark before the system service's name
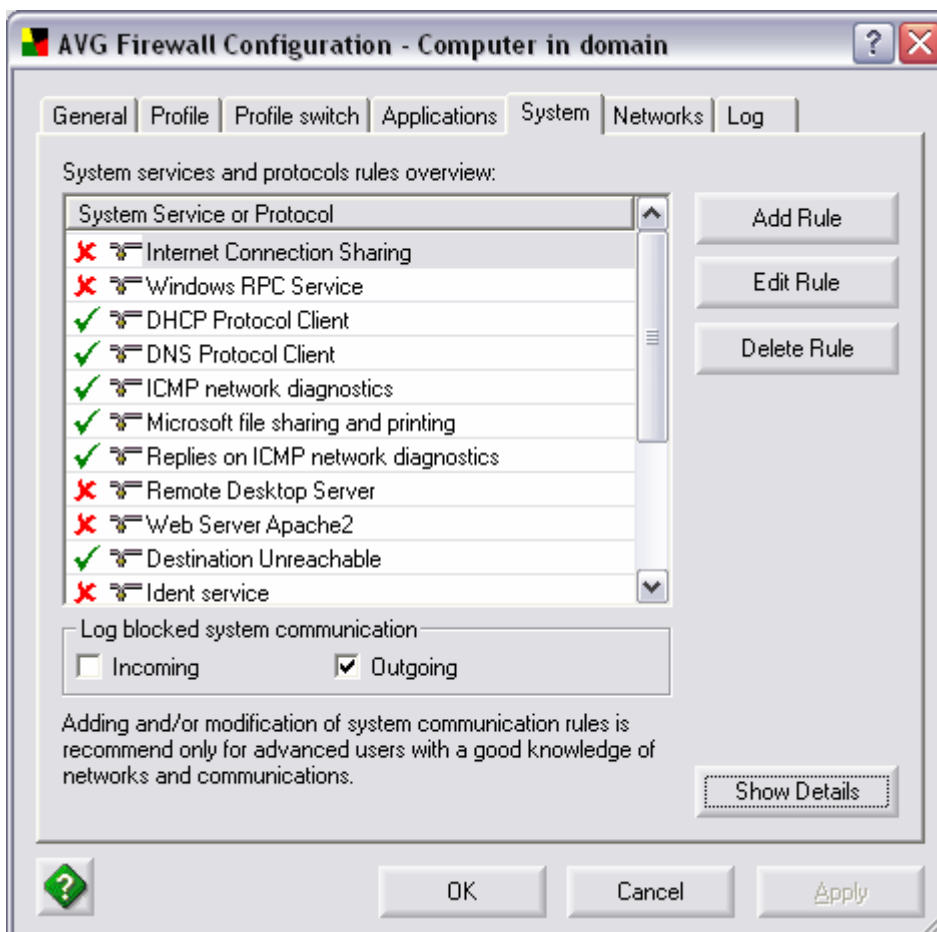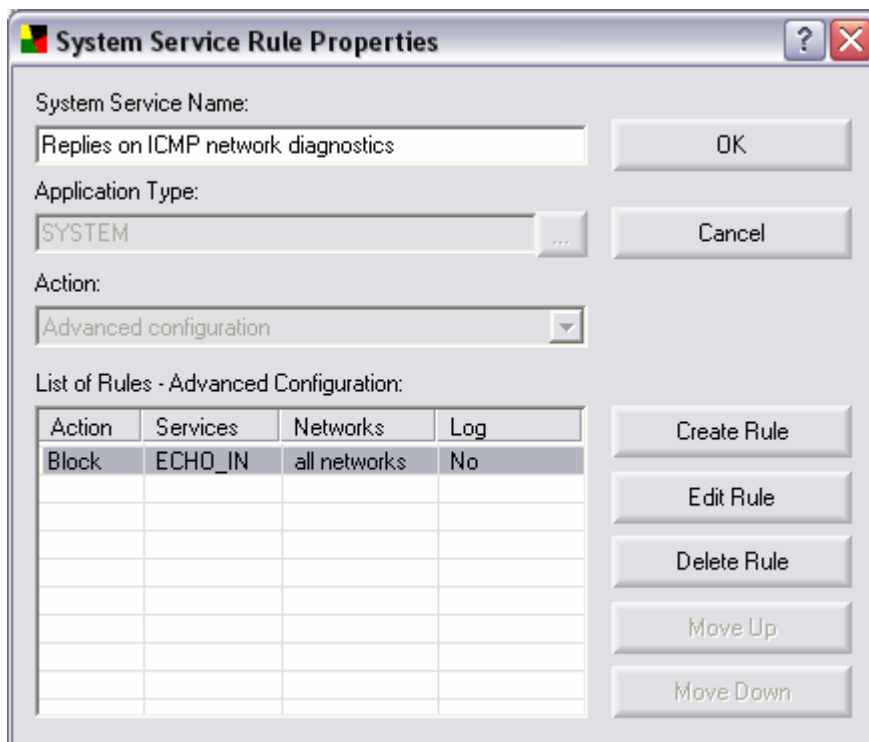
If you want to change the rule assigned to a specific system service, click the
color sign (green check mark / red cross mark) displayed in the list of services
and the sign switches to the opposite one automatically (the rule is changed).

In the ***Log blocked system communication*** section you can specify whether
you want to log the incoming / outgoing blocked communication, or
communication in both ways.

The ***System*** tab further offers the following operating buttons:

o   **Add/Edit Rule** – opens a new dialog where you can add a new system service rule, or edit the current one:

o   **Delete Rule** – deletes the rule defined for the selected system service

o   **Show Details** – in the bottom section of the dialog window, this button displays an information overview referring to the system service currently selected in the list of system services and protocols:

–   **Service** – name of the system service (or protocol)

–   **Rule** – rule assigned to the respective system service (or protocol)

Having selected the **Show Details** option, a new button labeled **Services** appears in the **System** tab:
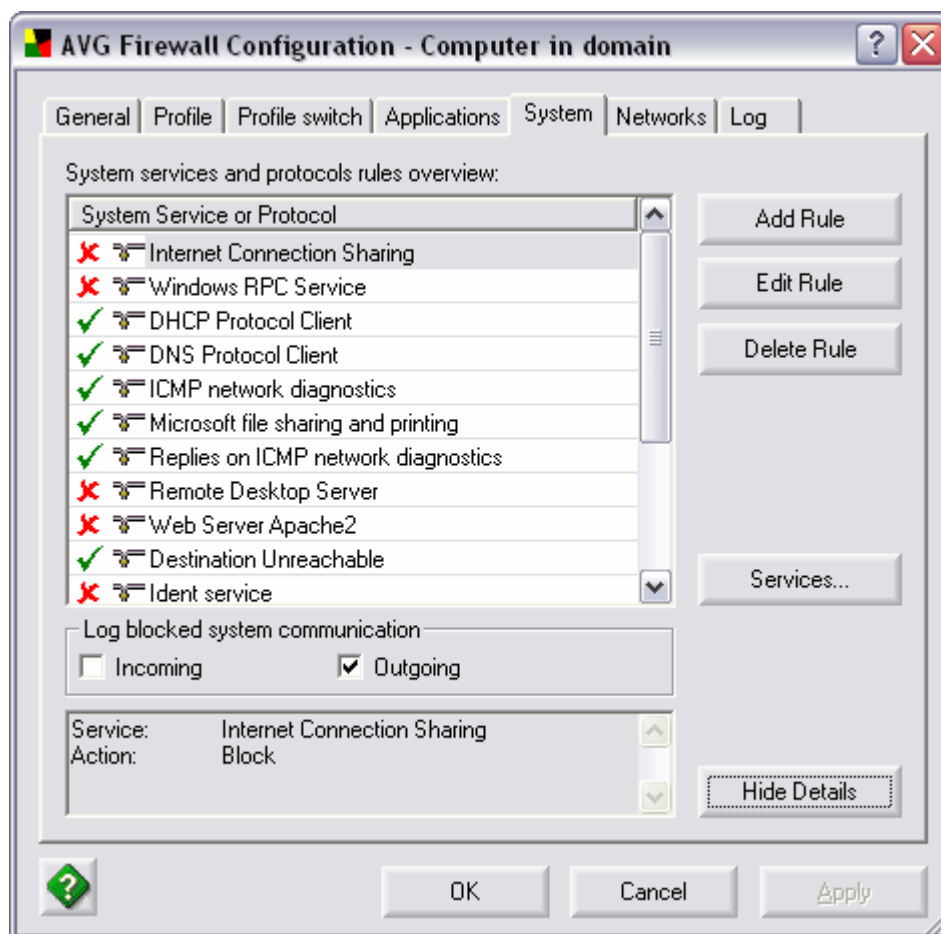
The **Services** button opens a new **Services** dialog that displays a detailed overview of system services and brings the option of editing parameters of respective system services:
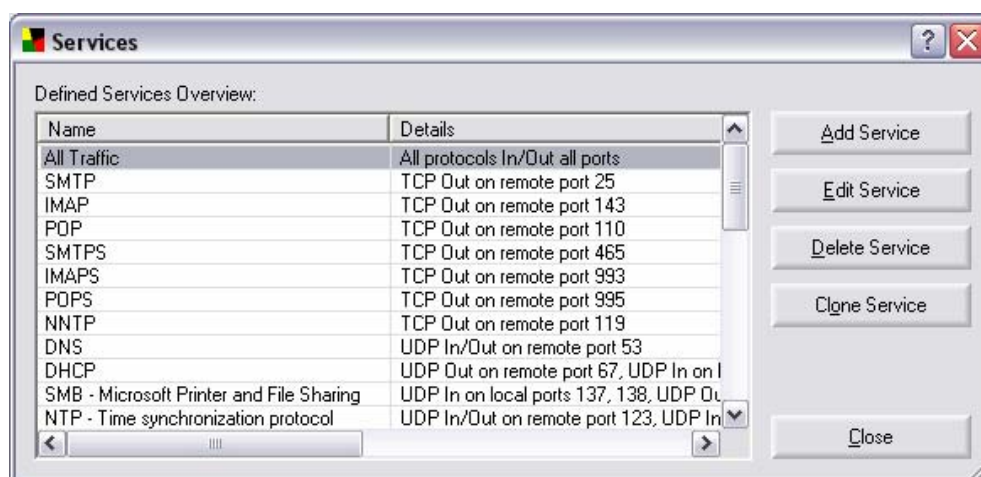
The **Services** dialog window provides the following operating buttons:

– **Add Service** – opens a new **Service Properties** dialog where you can define the new service name and set specific parameters for this service (direction, protocol, local ports, remote ports)
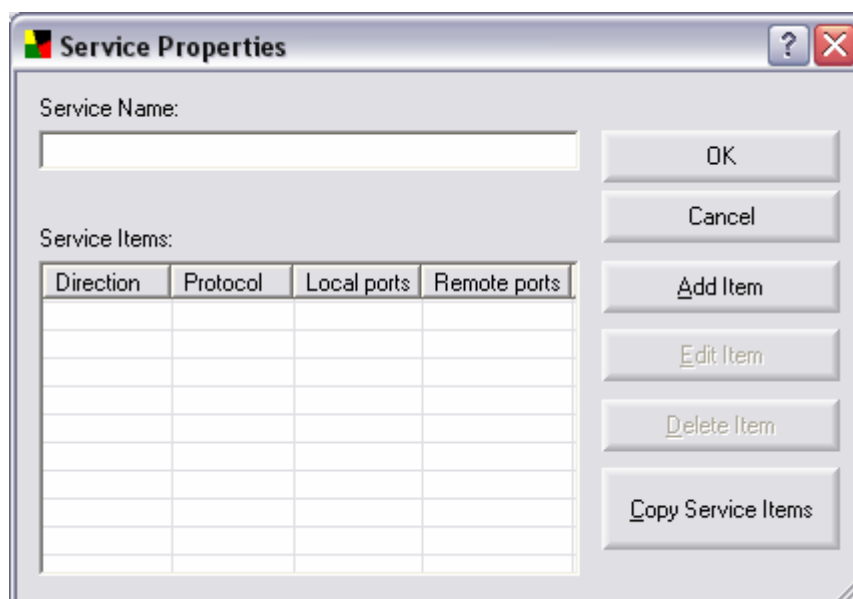
– **Edit Service** – opens the **Service Properties** dialog window where you can edit the existing parameters defined for a specific service.

– **Delete Service** – deletes the defined service (and removes the information about the service from the list of services)

– **Clone Service** – makes creating a new service record easier and more comfortable for you: To use this option, highlight a service in the list of services (**Services** dialog) and press the **Clone Service** button. A new service record will be created with predefined parameters taken from the definition of the cloned service. Then you can easily edit the parameters for the new service.

g) **Networks**

*Note: Once you change these Firewall Network settings in the **Shared settings for stations**, all network interfaces' settings will be deleted. This feature cannot be set from the AVGADMIN, because individual workstations in the network will always have different network interfaces.*

On the other hand, it is possible to manage user-defined networks (defined by IP range etc.).

When editing individual stations, assigning rules to interfaces will be possible as well.

The **Networks** tab offers a list of networks that the application communicates with. You can add new networks, edit parameters of the currently defined networks, and delete a defined network:
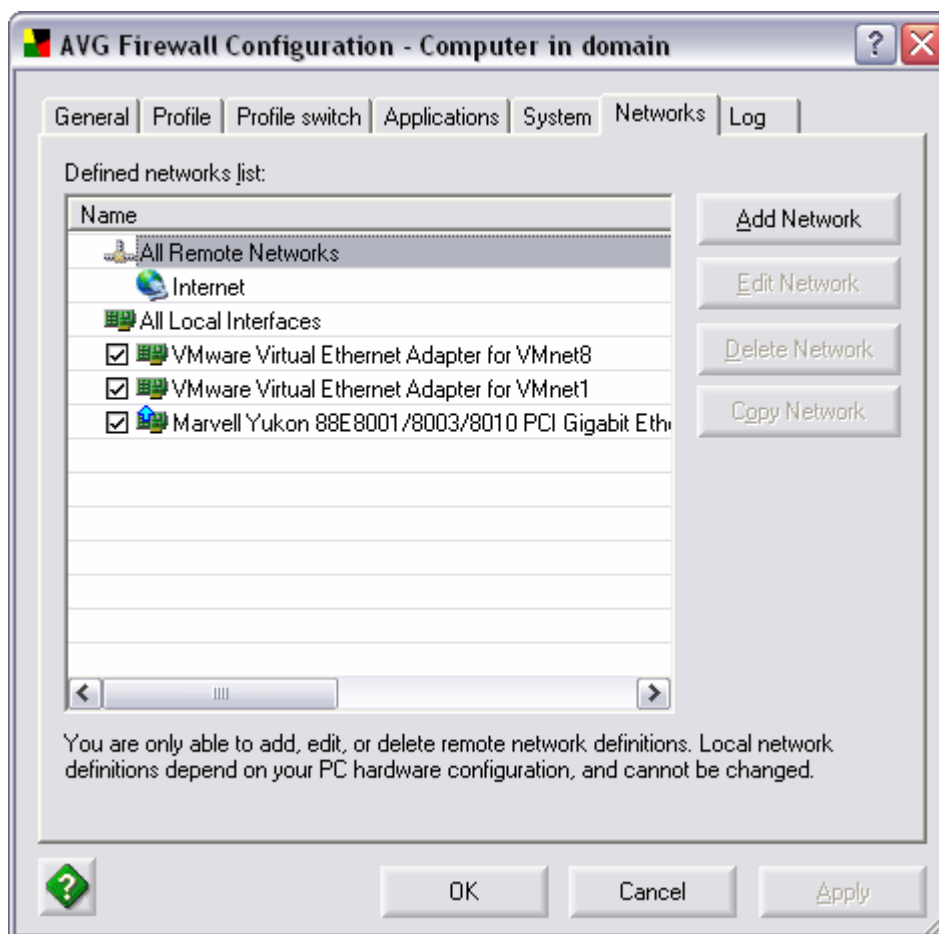
One or more network interfaces may be listed within the Defined networks list. If you wish Firewall to stop filtering traffic coming through one of the interfaces, simply uncheck the required check box located to the left of the network interface's name.

Stopping traffic filtering for a particular network interface can be useful in the following situation: If your computer is connected to the internet by one network interface and to the Local Area Network (LAN) by another interface, it is possible to select traffic filtering for the internet interface and leave the LAN connection unfiltered, (as the LAN has a lower risk of potential threats).

The dialog window additionally provides the following operating buttons:

o **Add Network** – opens a new **Network Properties** dialog where you can define the new network name and set its parameters:
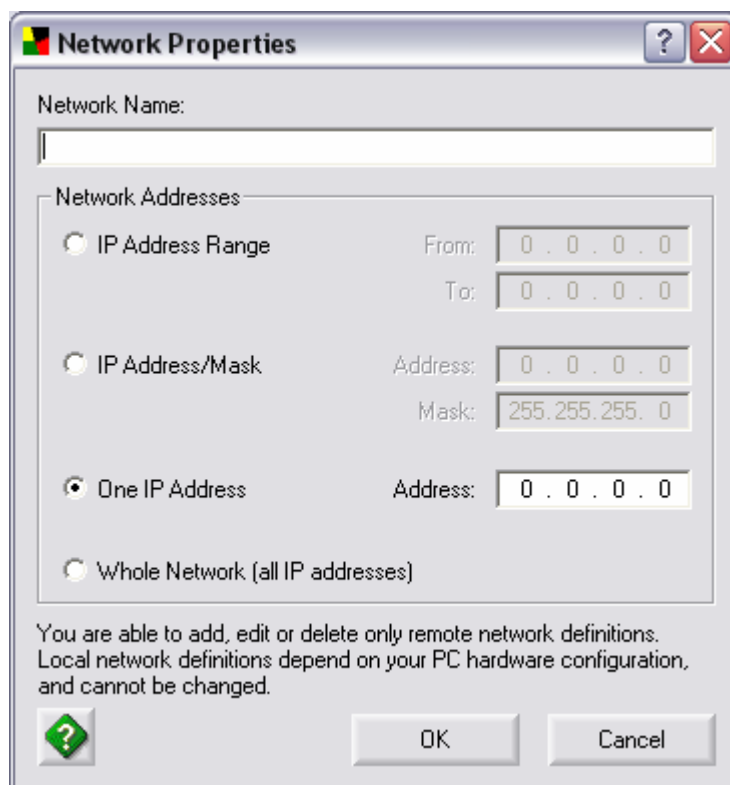
o **Edit Network** – opens the **Network Properties** dialog window with parameters already set for a specific network, and allows you to edit them

o **Delete Network** – deletes the defined network from the list of networks

o **Copy Network** – makes creating a new network record easier and more comfortable for you: To use this option, highlight a network in the list of networks (**Networks** dialog) and press the **Copy Network** button. A new network record will be created with predefined parameters taken from the definition of the cloned network. Then you can easily edit the parameters for the new network.

AVG 7.5

AVG Anti-Virus Network

h)   Log
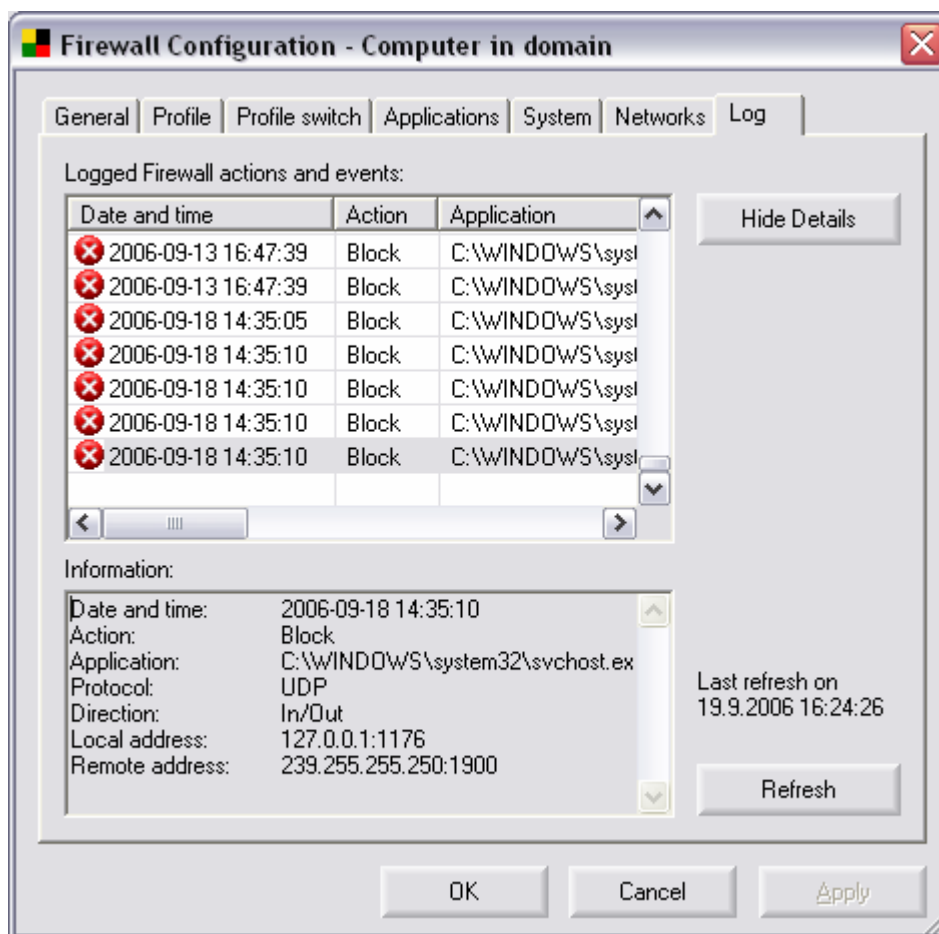
Within the *Log* tab you are able to review the list of all logged **Firewall** actions and events with a detailed description of relevant parameters.

The Firewall logs are usually quite big, therefore by default there are no Logs stored. User can request logs at anytime by pressing the *Refresh* button. The request status will be indicated in the Status section of the main AVGADMIN workspace.

If there are no logs available on the station, warning dialog will be displayed.

By default, all log files are stored in the AVG TCP Server installation directory, *stored_logs* subfolder.

You can customize the download folder in the AVG TCP Server configuration (for more details see chapter 6.6. AVG TCP Monitor Advanced Mode, DataCenter tab).

Once the logs are loaded, you can see the overview in the dialog window. The main part of the *Log* tab is divided into two sections:

o   **Logged Firewall Actions and Events Section**

This section offers an overview of all actions and events that were performed by **Firewall** with their parameters recorded within the log file.

By default, the *Log* tab opens in the standard mode with the following parameters provided for each of the logged actions:

- *Date and Time* – exact date and time when the event was encountered
- *Action* – type of action performed
- *Application* – name of the process to which the logged event refers

If you find the provided parameters insufficient, and want to see more, use the *Show Details* button to switch to the advanced log file overview:

Then you will be able to review the following parameters:

- *Date and Time* – exact date and time when the event was encountered
- *Action* – type of action performed
- *Application* – name of the process to which the logged event refers
- *User* – name of the user of the application
- *Direction* – the application's communication direction (in/out, or both ways)
- *Protocol* – type of protocol used
- *Local Address* – the local address of the connection related to the logged event
- *Remote Address* – the remote address of the connection related to the logged event

In both the standard/advance *Log* tab mode you can always use the option of sorting the logged parameters according to a selected attribute: you can sort the data chronologically (press the header of the *Date and Time* column), by type of action (press the *Action* column header), etc.

o **Information Section**

The *Information* section provides a comfortable and easy to view list of parameters logged for a specific event that is currently highlighted in the above *Logged Firewall Actions and Events* section.

o **Log Tab Operating Buttons**

The *Log* tab offers this operating button:

- *Show/Hide Details* – switch between the standard/advanced mode of the log file display (as described above)

10.7. Licenses Administration

A configuration dialog for managing license numbers. It allows you to easily monitor all existing license numbers, and add or update license number for individual or multiple stations.

Individual license numbers are distinguished by different font colors:

AVG 7.5

● **Black color** indicates assigned license numbers that are up to date.

● **Red color** indicates license numbers that are either expired, will expire in seven days or where the number of stations using the license number exceeds the license number quantity.

● **Blue color** indicates license numbers that are currently set, but that have not yet synchronized with workstation(s).

Therefore it may also occur, that certain license numbers could be listed more than once with different colors. For example after setting a new license number, some stations could synchronize and accept the new settings (line marked as black), but several may not yet have synchronized (line marked as blue).
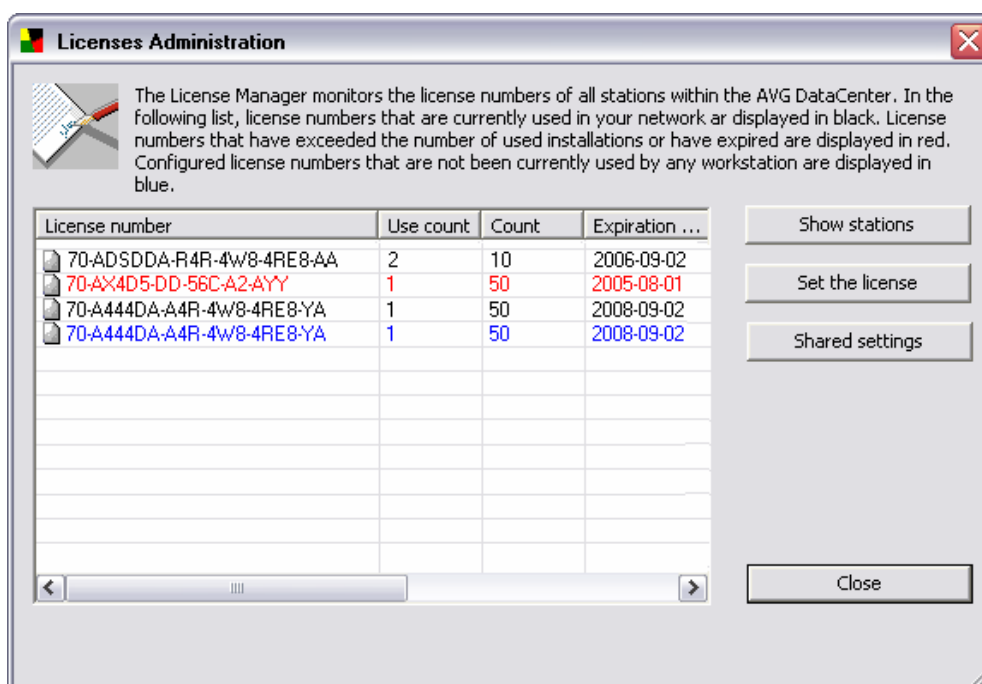
Operating buttons are:

● **Show stations** - shows stations that are using the selected license number. Select the desired license number for which you want to see the list of stations using it and then press the **Show stations** button. If there is an 🔒 icon displayed within the row, then the workstation is included in the shared station settings and therefore the license number cannot be changed.

● **Set the license -** allows the user to set a new license number for one or more stations. Select one or more rows that you would like to change and then press the **Set the license** button.

● **Shared settings** - displays license numbers that are used for Shared stations settings.

11. AVGADMIN Configuration

11.1. AVGADMIN Periodic Tasks

Periodic tasks are scheduled actions which run repeatedly in time periods defined by the network administrator. The dialog window for periodic tasks editing can be accessed from the **AVGADMIN** main menu selecting the *Settings/Periodic tasks* option:
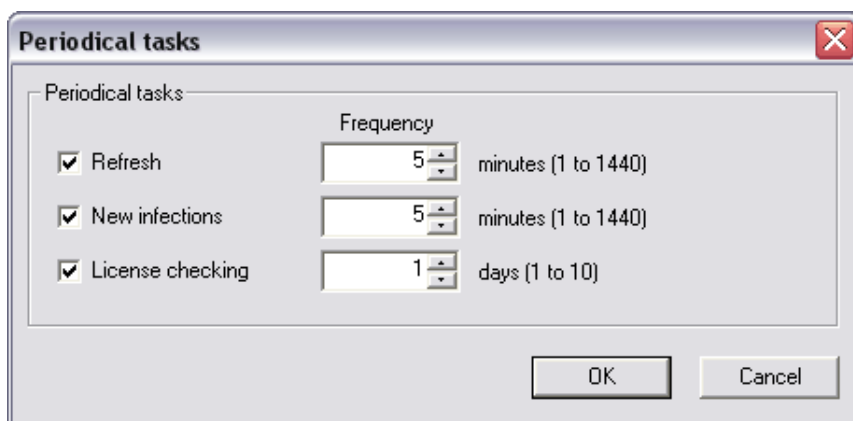
In this dialog window you can specify the time interval for performing the following tasks:

● *Refresh* - In the specified time period **AVGADMIN** refreshes the information displayed in the central table.

● *New infections -* Every workstation sends its test results to the **AVG DataCenter**. **AVGADMIN** regularly checks the test results table, and every new virus appearance is immediately reported in the status window.

● *License checking -* **AVGADMIN** goes through all AVG license numbers used on separate workstation's and reports any discrepancy with the license policy. The report on a possibly discovered problem is displayed to the network administrator via the status window entry.

11.2. AVG DataCenter Update

It may happen that **AVGADMIN** asks for the database update. This situation occurs if you install a newer **AVGADMIN** version supporting new functions, or if the data processing changed. Usually the administrator is allowed to keep the database in its older format. However, we recommend transferring the database to the new format as soon as possible so that you can fully use all functions and features of the new **AVGADMIN** version.

From time to time, the **AVG DataCenter** structure changes significantly; then it is necessary to update **AVG DataCenter** before using the new **AVGADMIN** version in order to secure the correct performance. In that case, **AVGADMIN** will inform the user that it is not possible to continue working until the **AVG DataCenter** updates.
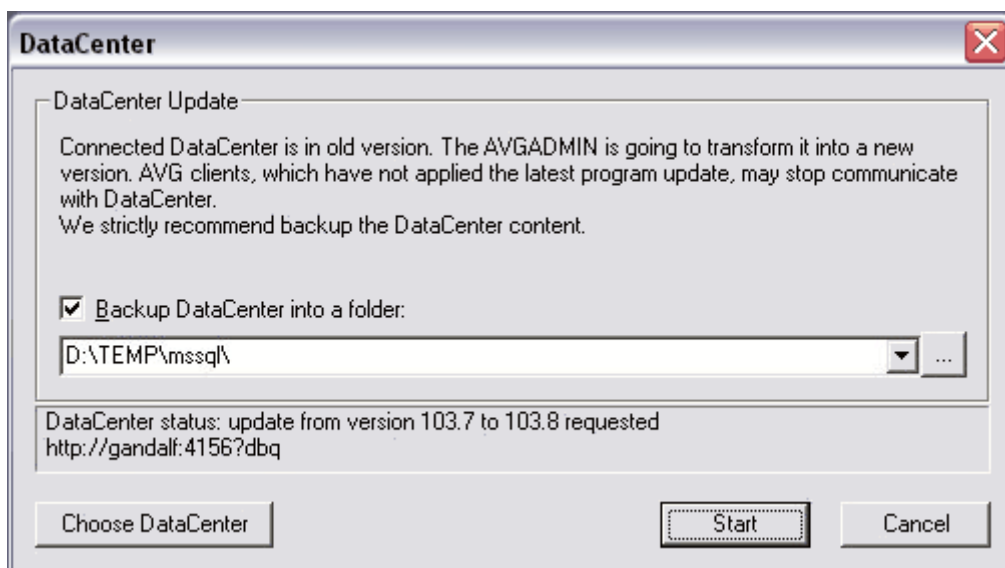
The update dialog always offers the option of exporting the **AVG DataCenter** content before the actual update process starts. We strongly recommend creating a backup before starting the update.

11.3. Workstation/User Groups

The administrator can define workstation/user groups as the need arises. All objects included in the group then take the configuration set up for this group.

This way the administrator can define the group configuration, and change the configuration previously set for a specific workstation/user by simply assigning the workstation/user into a group. Workstation/user assignments into groups makes administration much easier, and should be used if the number of workstations/users exceeds the number of records for one screen (i.e. approximately 20-25 objects).

The procedure of creation and administration of workstation/user groups is the same in both cases. The following text describes the respective procedure for workstations:

a)   **Create a new group**

To create a new group, follow these steps:

o   In the navigation tree select the **Stations** group

o   A list of all existing groups appears in the central table

o   Click the mouse right button anywhere in the central table to open the context menu

o   From the context menu select the **Create new group** item, and specify its name

o   Press the **Enter** button to confirm the creation of the group

Immediately after creating the group, a new shared settings object is created in the **AVG DataCenter** that can be further edited (for details please refer to chapter 11.5 – Configuration Editing). All members of the new group then automatically share this object's configuration.

AVG 7.5
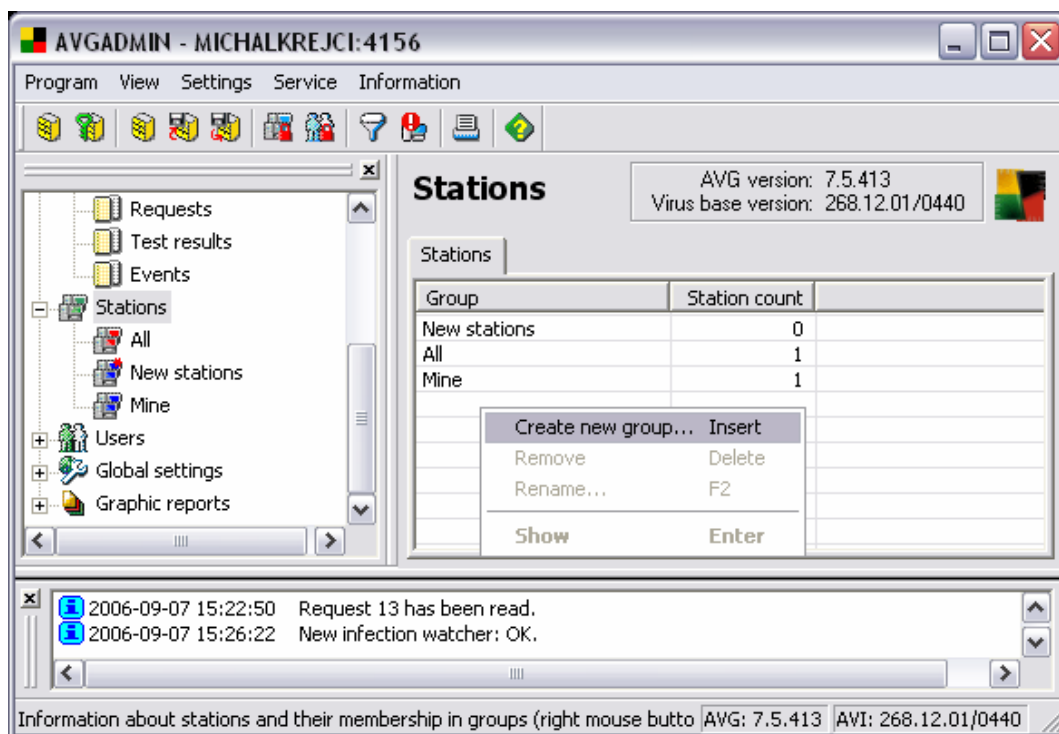
b)   Delete a Group

The **Delete group** procedure is analogical to the group creating:

o   Click the right mouse button over the name of the group that you want to delete

o   From the newly-opened context menu select the **Delete** item

Using the same context menu you can also **Rename** groups.

Stations can be assigned into a station group using the context menu **Assign to group** item. You can highlight and assign more stations at once:

o   Find a station that should be assigned into another group; newly-connected stations are listed in the **New stations** group

o   Select one or more stations that you want to work with

o   Click the mouse right button over any of the selected objects to open the context menu

o   From the context menu, select the **Assign to group** item

o   A new window with the list of all available groups appears

o   Select the target group

o   The stations will be assigned to this group, and automatically inherit the configuration defined for this group
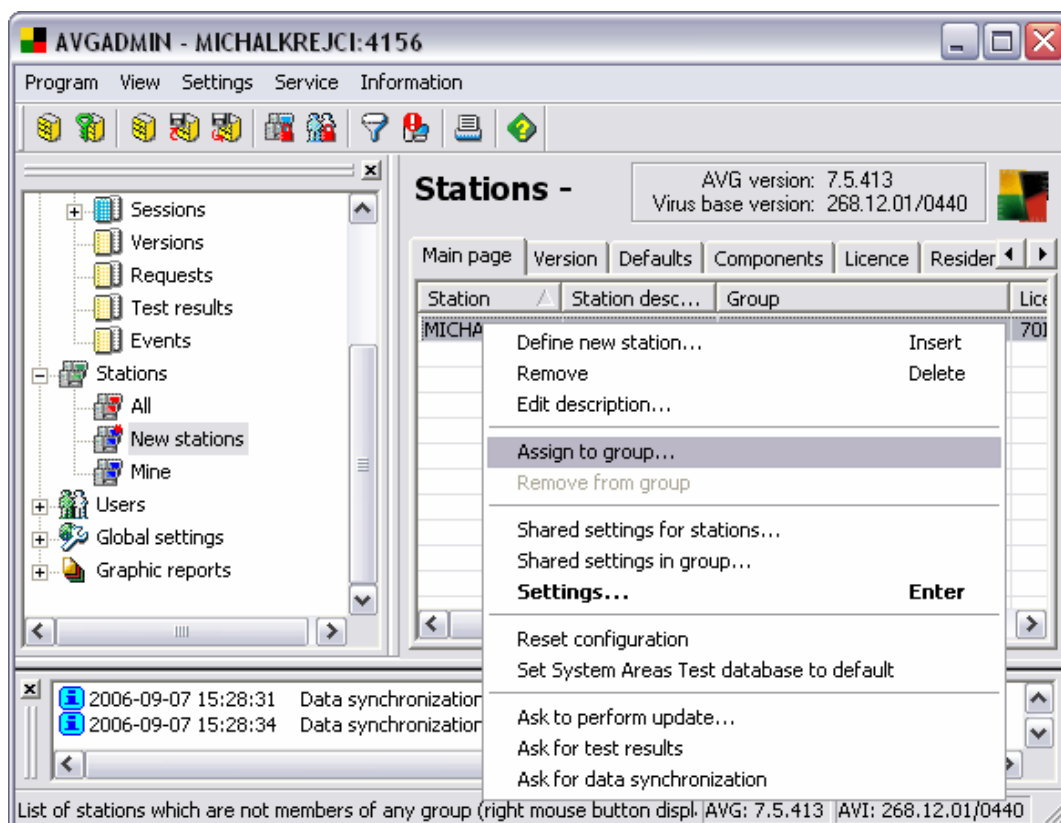
Groups *All* and *New stations* are specific system groups that cannot be deleted. Stations/users are automatically assigned to these groups. The *All* group contains all existing stations connected to the **AVG DataCenter**. The group *New stations* automatically contains all stations that have not yet been assigned to any specific user group.

11.4. Configuration and Display Management

a) Client configuration

The **AVG client** configuration is divided into two main parts – workstation configuration, and user configuration. This separation is extremely important for the whole AVG administration.

o **Workstation configuration** is not transferable, and it is intended for a specific workstation. Besides other parameters, it contains information about the list of installed components, the **Resident Shield** configuration, the last update version and date, etc.

o **User configuration** on the other hand can be transferred – it will be copied to every workstation to which the user logs on. This configuration contains mainly the user interface parameter settings.

The workstation configuration is saved separately from the user configuration, although it is not quite obvious on a workstation where AVG is installed. After AVG start-up, both configurations combine automatically, and the user does not even notice. However, **AVGADMIN** keeps the user configuration unchanged, because it is not specified on which station the user will log in next time.

The workstation receives its configuration information automatically after its first logging into the **AVG DataCenter**. Users then receive their configuration after log-in from a workstation that they have never used before. If a user or workstation is not yet registered in the **AVG DataCenter**, the default configuration is used, using the *.DEFAULT.SET* object (accessible from the Global settings branch of the **AVGADMIN** application navigation tree).

The administrator can use **AVGADMIN** to predefine new clients' accounts, assign them into specific groups, and prepare the suitable default configuration for them. If these accounts are not predefined, the workstation/user account will be created automatically at the first login, and its configuration can be changed later.

b) Tests and plans

Tests and plans can also be defined both for users and/or stations. In some networks, it is better to keep tests/plans defined for workstations only. This applies especially for networks where strict security rules are required for AVG installation.

The administrator can activate this mode selecting the *Program/AVG DataCenter Mode* item from the **AVGADMIN** main menu.

Even this option does not guarantee the administrator to have the needed overview of the stations/users configuration within the network. That is why it is recommended to use the *Global settings* section for test/scheduled tasks administration. In the Global settings section the administrator controls all tests/tasks defined for all users/workstation.

11.5. Configuration Editing

The configuration window helps to modify the user/workstation configuration. The window can be opened by double clicking on the user/workstation record, or by the mouse right button click and selecting the *Settings* from the context menu:
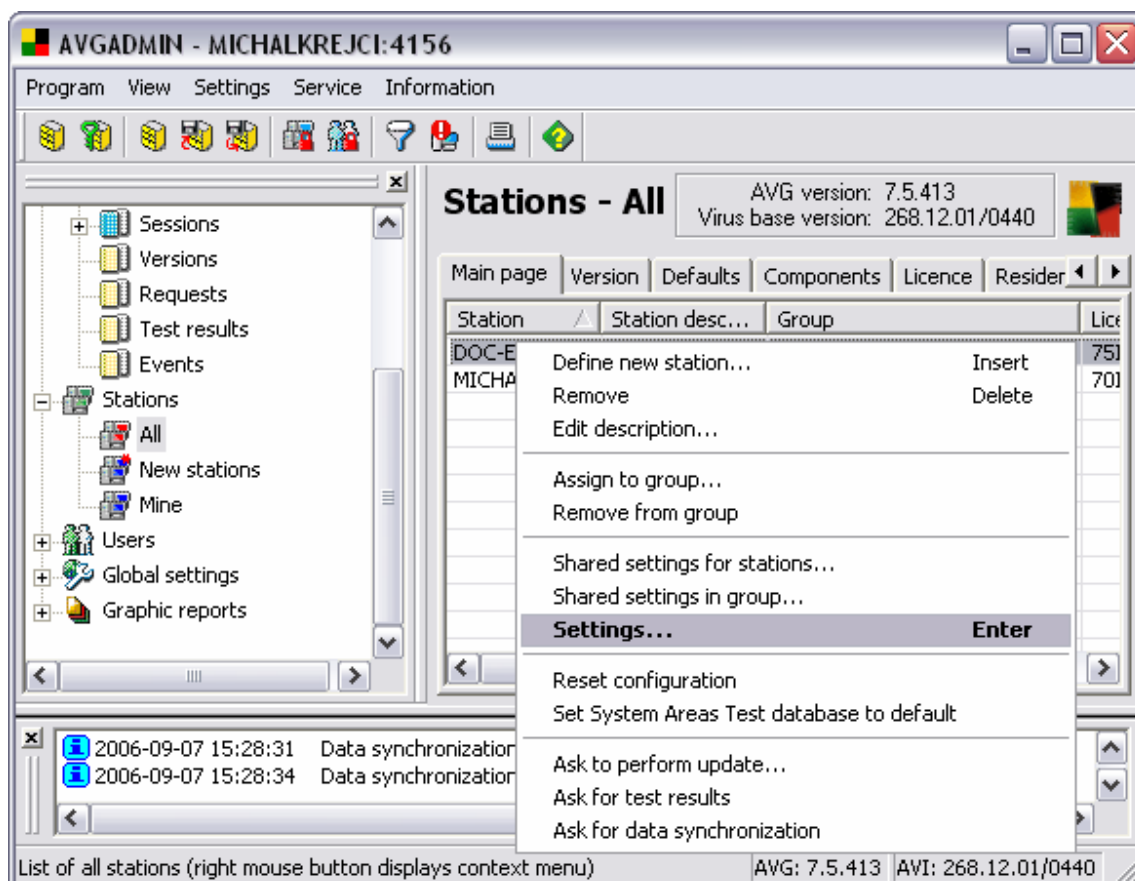
The configuration window itself contains the following tabs:

General settings

- **Tests** – the Windows Explorer labeled button
- **Scheduled tasks** – the calendar labeled button
- **Rules** (for workstation only) – configuration of rules for event processing
- **E-mail**
- **Firewall** *(for workstations only)*

For example, the following window displays the configuration dialog for a particular station:

AVG 7.5
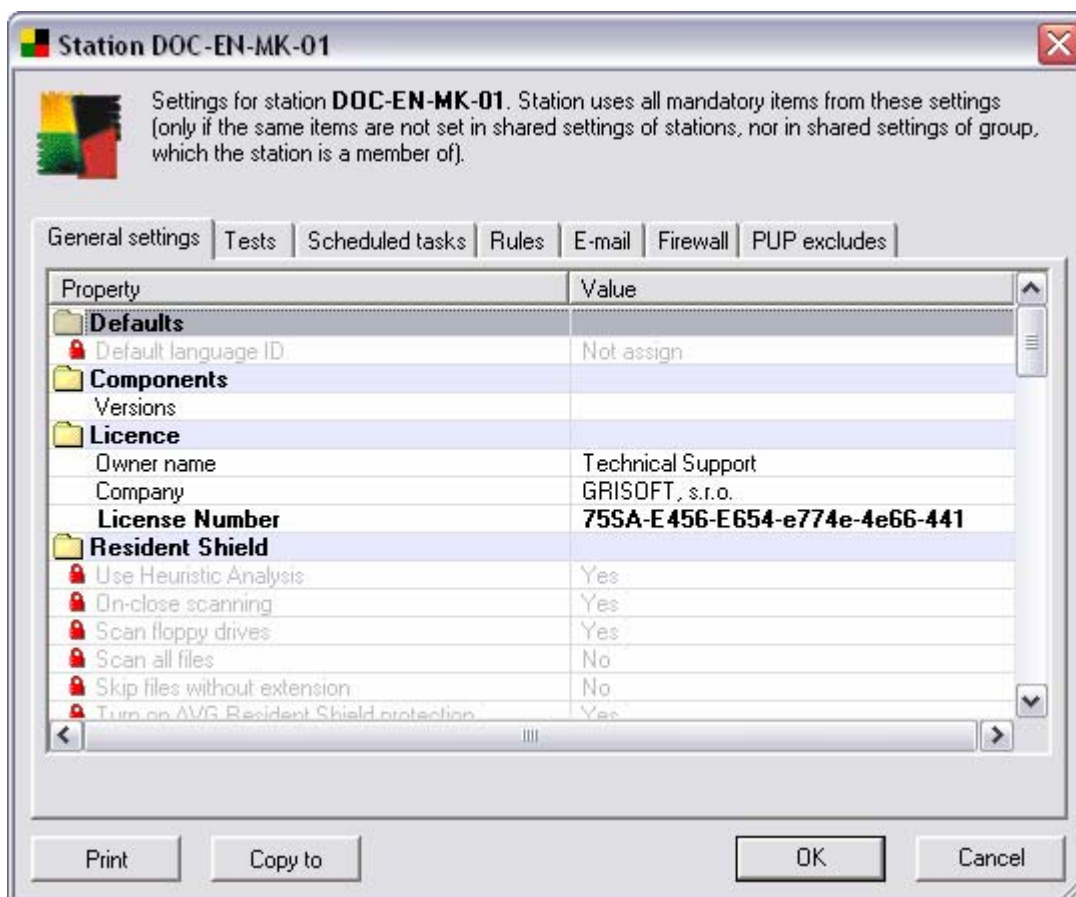
The layout of configuration windows is analogous for settings of particular users, shared settings of stations, users and group of stations or users.

a)   General Settings Editing

The general properties are divided into several logical groups separated by a color ruler with the highlighted headline. Under the general properties panel you can find two buttons that enable you to print or copy the whole configuration.

o   ***Print*** – Prints the configuration on the selected printer. A standard window with the printer choice and the print confirming dialog will be displayed.

o   ***Copy*** – Copies the configuration to other workstations or users. The configuration value set can be copied to one or more stations/users, but also to a station/user group.

Any value can be defined as a **mandatory value** or as an **optional value** (default setting). A value can be changed from mandatory to optional from its context menu (right mouse button). To specify a value's format and font distinguishing the mandatory/optional values, use the ***Settings/Options*** main menu item. The basic settings are distinguished by the ***AVG DataCenter mandatory/monitoring mode*** use.

For common objects the ***mandatory/optional values*** mean rather ***active/inactive values***. This option is intended to discriminate between the

AVG Anti-Virus Network

temporarily unused tests/plans/rules, and the used ones without deleting the former.

Any configuration value can be edited. To open the value editing dialog, click your mouse on the selected value. A small editing window is displayed; the window appearance depends on the item nature (text field, selection box, etc.). Within this window you can specify the new item value: press the **_Enter_** key to confirm, and the **_Esc_** key to cancel the editing (the previously defined value will be used then).
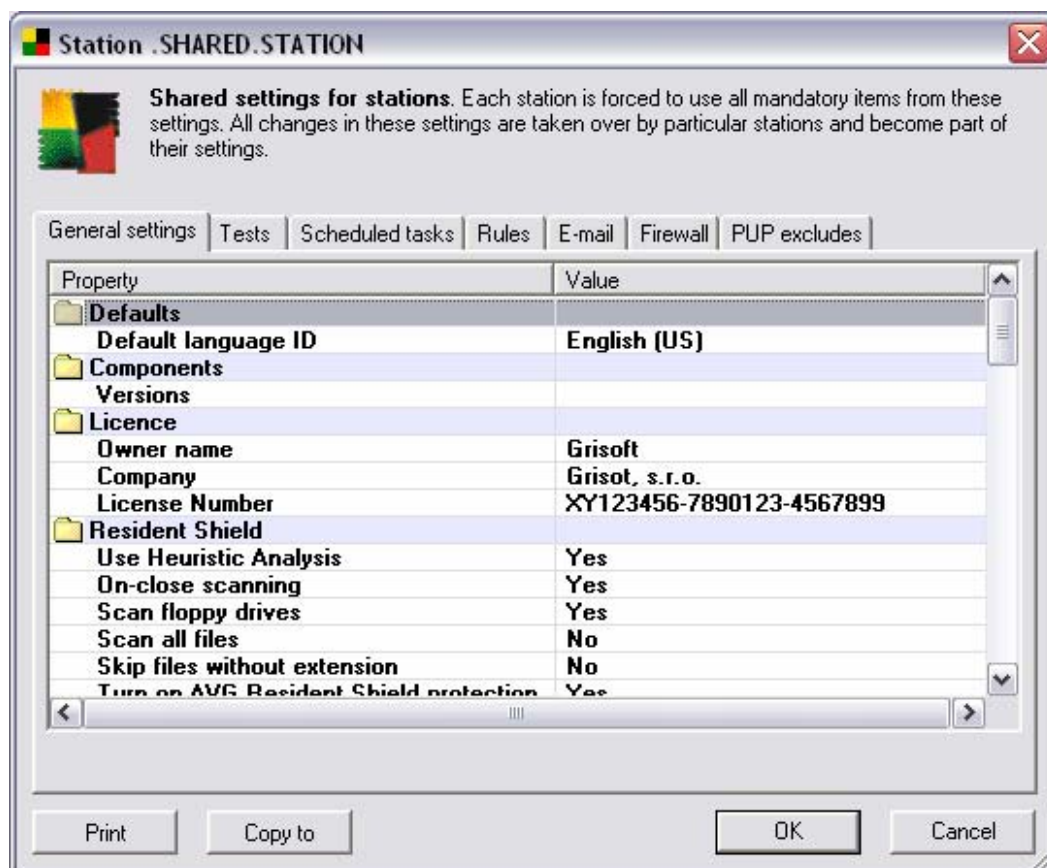
The configuration editing window is always displayed in the same manner, although there can be differences according to whether you are editing the user, station, or group configuration:

o   If there is a mandatory record defined in shared user/station settings, its value is prior to the value defined in the configuration of the station or user. Also, it is not allowed to edit it. There is a red lock sign displayed on the left side next to the record.

o   If there is a record defined as optional in shared user/station settings, but it exists as mandatory in the shared settings of the respective group, its value for group takes priority over the station/user settings. The difference in the graphical display is the same as in the previously described case expect for the color of the lock – it is blue for group mandatory settings.

Certain items can be configured also using the standard dialogs (which are mostly the same as in the AVG application)

Resident shield - Configuration

To display **Resident shield** configuration window, double click any of the Resident shield section items.
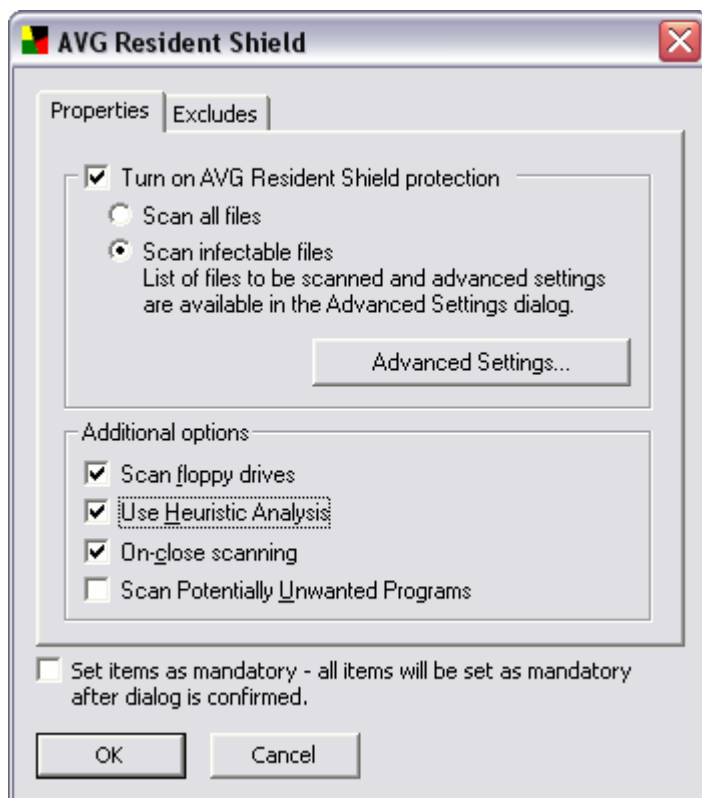
o   *Properties*

The tab offers a range of possible **Resident Shield**'s scanning options to select from:

Advanced Settings – opens the dialog window **Resident Shield - Advanced Settings**, where it is possible to configure scanning of infectable files and selected types of documents (specific extensions), or define exceptions. According to these settings **Resident shield** will skip or include the chosen extension in the scanning process.
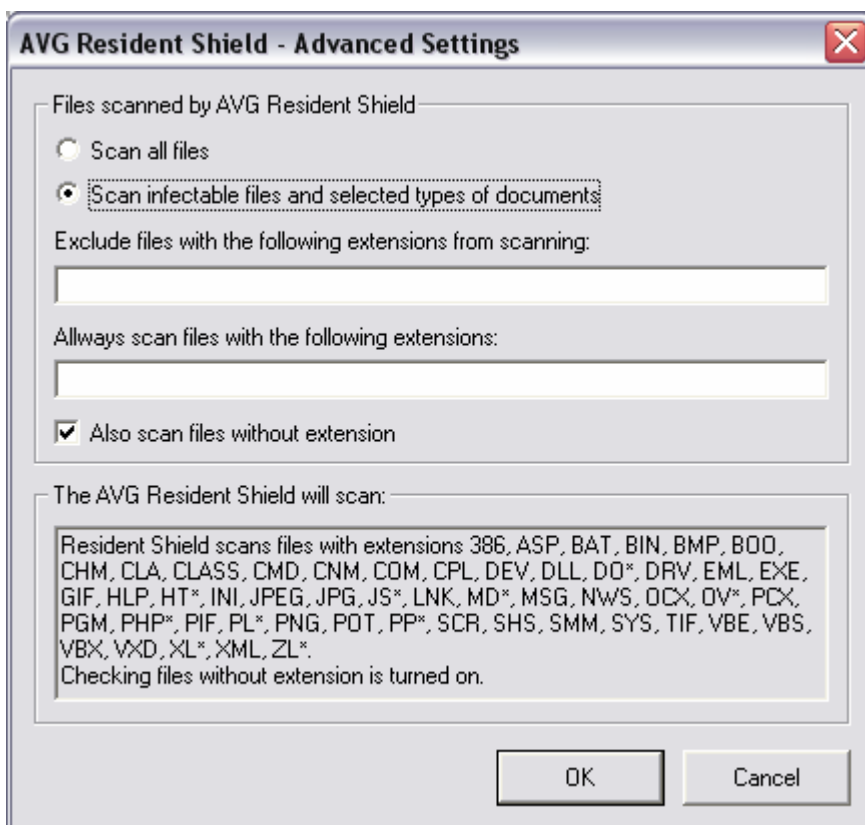
o   *Excludes*

The *Excludes* tab offers a possibility of defining folders that should be excluded from the **Resident Shield** scanning. If this is not a must, we strongly recommend not excluding any directories! If you decide to exclude a folder from **Resident Shield** scanning, mark the *Use excludes in Resident Shield* check box.

AVG 7.5

AVG Anti-Virus Network

Use the *Edit Excludes* button to open a new dialog where you can directly specify the folders to be excluded from scanning:
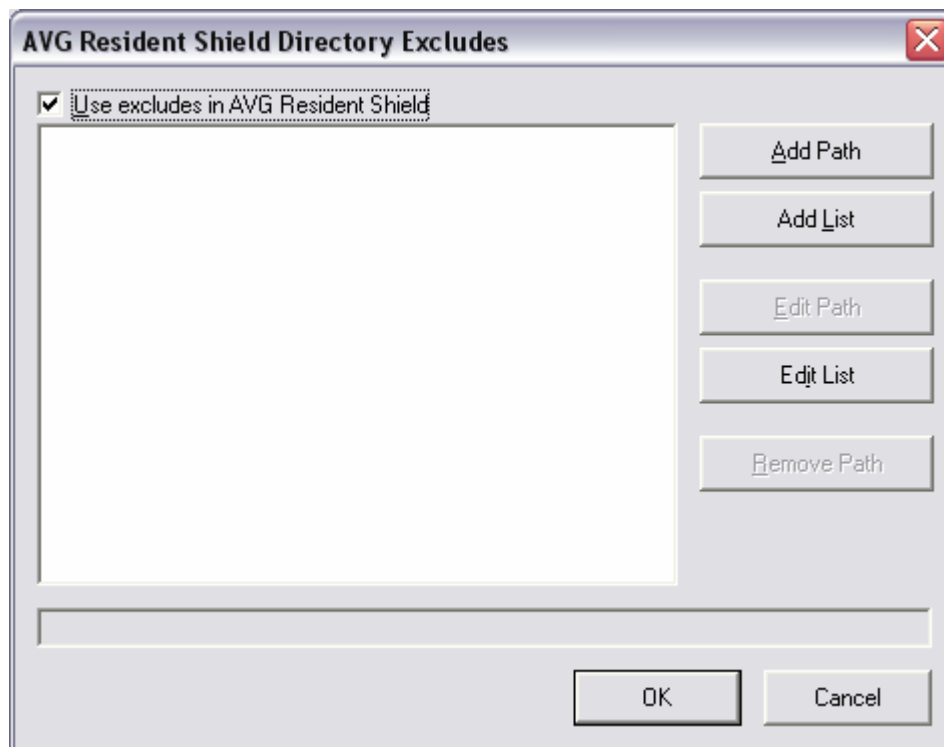
This dialog provides the following control buttons:

- *Add path* – offers you to 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 the 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

- *OK* – accepts all new settings, and closes the dialog window

- *Cancel* – closes the dialog window without accepting the changes

o   All items can be also set as *Mandatory* by ticking the **Set items as mandatory** checkbox.

o **Firewall – basic settings**
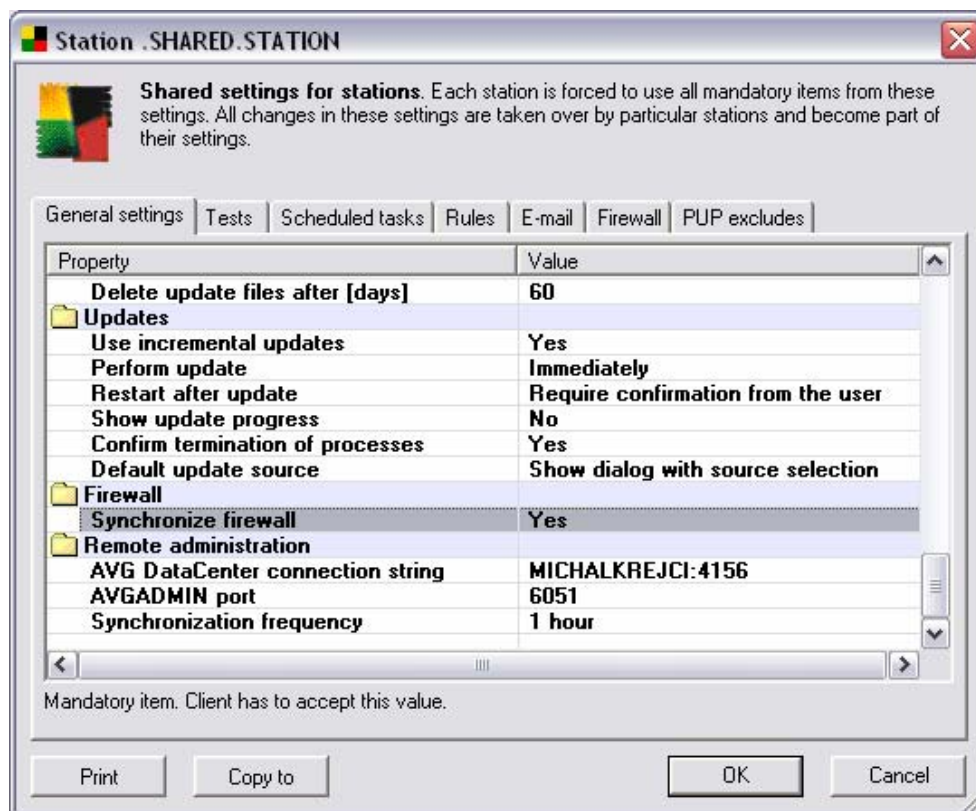
If you need to change firewall settings on individual stations, set the **Synchronize firewall** setting to *Yes* value.

*Note: By default, this setting is set to **No**. Because in larger networks, the synchronization of large number of workstations could affect database performance. Besides, in most of LAN/WAN networks, security should be usually maintained not by firewalls on individual stations, but with some reliable hardware firewall protecting the whole network.*

More detailed description on firewall settings can be found in Firewalls chapter.

b) **Tests and Scheduled Task Configuration Editing**

We recommend performing all test/task configuration editing within the Global settings section. However, if the administrator only wants to overview the current user/station configuration, or to change a specific user/station configuration, a test/task configuration window can be used.

Select the *Tests* tab to get to the tests configuration dialog:

AVG 7.5

AVG Anti-Virus Network
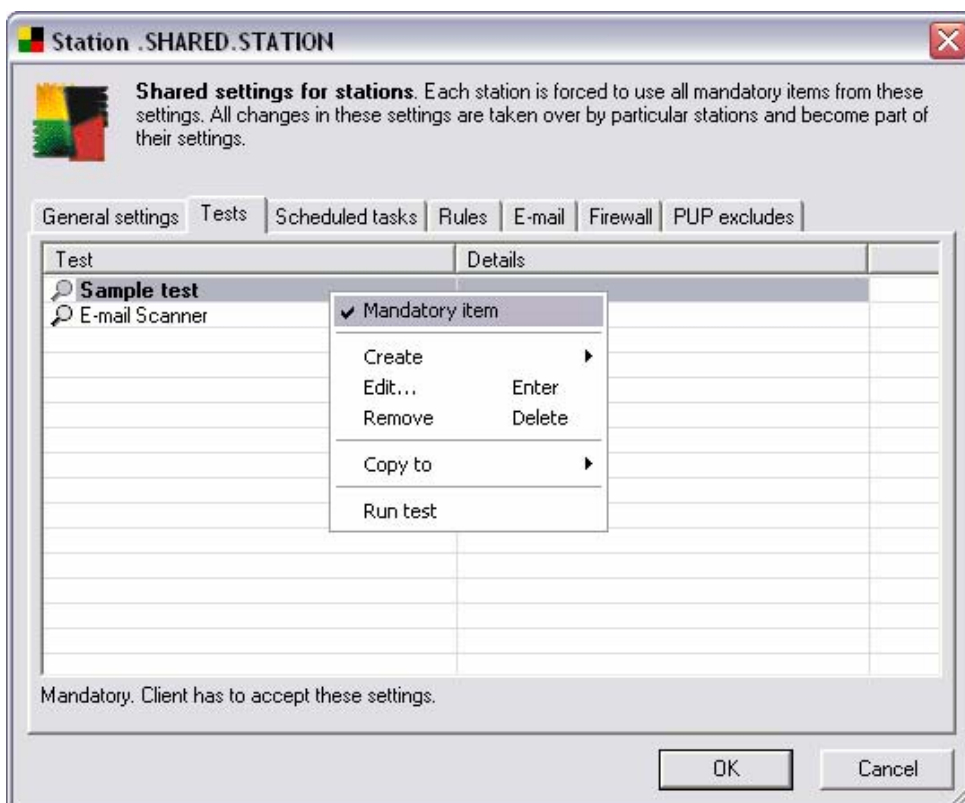
Select the **Scheduled tasks** tab to get to the scheduled tasks configuration dialog:
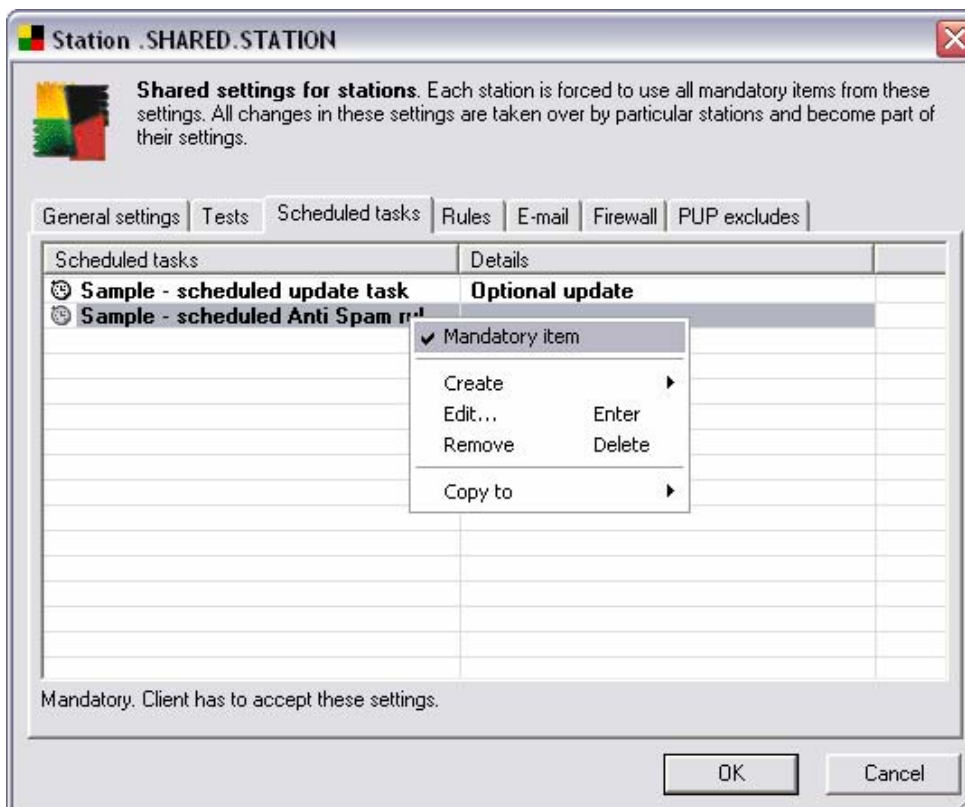
Generally, double click the specific test/scheduled task to open a dialog window for configuration editing. The mandatory tests/plans are not only displayed with a different font or color but in the "*A*" column they are also signed with an exclamation mark "*!*".

If it is allowed to display <u>tests and plans assigned as to be deleted</u>, these records are marked with the "*X*" sign. Otherwise, the **AVG DataCenter** mode default settings specify these records as hidden.

Test/plans operations can be called from the context menu as well:

o **Mandatory configuration** – this option marks the settings as mandatory. The mandatory settings (tests and plans) is copied to the AVG client, and overrules any changes the end user previously made to the settings.

o **Create –** the option creates a new test/plan according to the default settings (if this is possible: e.g. it is not possible to duplicate specific tests)

o **Edit** – this option opens the test/plan configuration editing dialog

o **Remove** – this option removes the settings, or rather marks it as "to be removed". The settings will actually be removed at the next synchronization (e.g. at the connection to the AVG DataCenter, if the client is not connected). Some sets cannot be removed at all.

o **Copy** – this option copies sets of parameters to other stations or users. The settings can be copied to a station/user, or to a selected group. The group of parameters can also be copied to the default settings. The default settings is then used when the administrator creates a new test/plan that does not take any specific configuration from an existing defined settings.

o **Run test** – the option starts the test (applies to tests only). The test will run on a respective station in the invisible mode, and when the test is over the test results will be saved to the AVG DataCenter. If the station is off, the test will run automatically, immediately after the station start up.

c) **Rules tab**

More information on this topic can be found in the <u>Events in the AVGADMIN application</u> chapter.

d) **E-mail tab**

This tab offers to setup E-mail scanner settings and configure Anti-Spam options. To review Anti-Spam configuration possibilities, see to chapter <u>16. Anti-Spam</u> for more details.

Clicking the **Configure** button will show up the following Personal E-mail Scanner Setup window.

o **Properties**
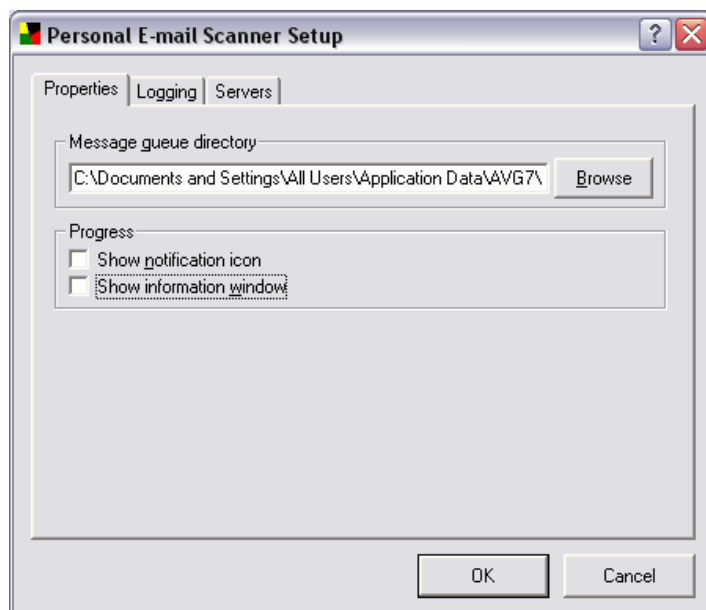
The **Message queue directory** textbox points to the folder where incoming and outgoing messages are stored and checked for viruses.

o **Logging**
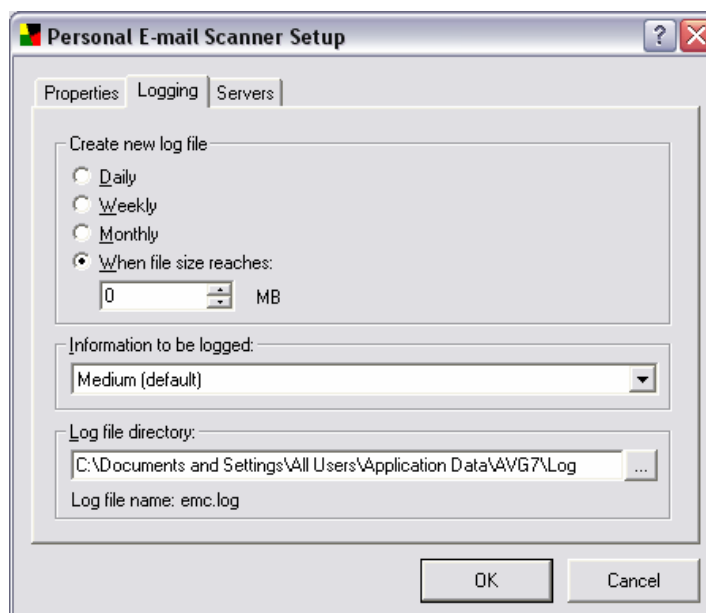
Under **Create new log file** you can select how often new log files are created. Remember that data in the old log file will be lost.

You can either select a time limit (**Daily**, **Weekly**, **Monthly**) or a size limit in Megabytes.

The **Information to be logged:** section has four options to choose from – Minimum (basic connection information), Low (small file size), Medium (default) or High (all traffic).

The **Log files directory** textbox points to the folder where log files are stored.

o   **Servers**
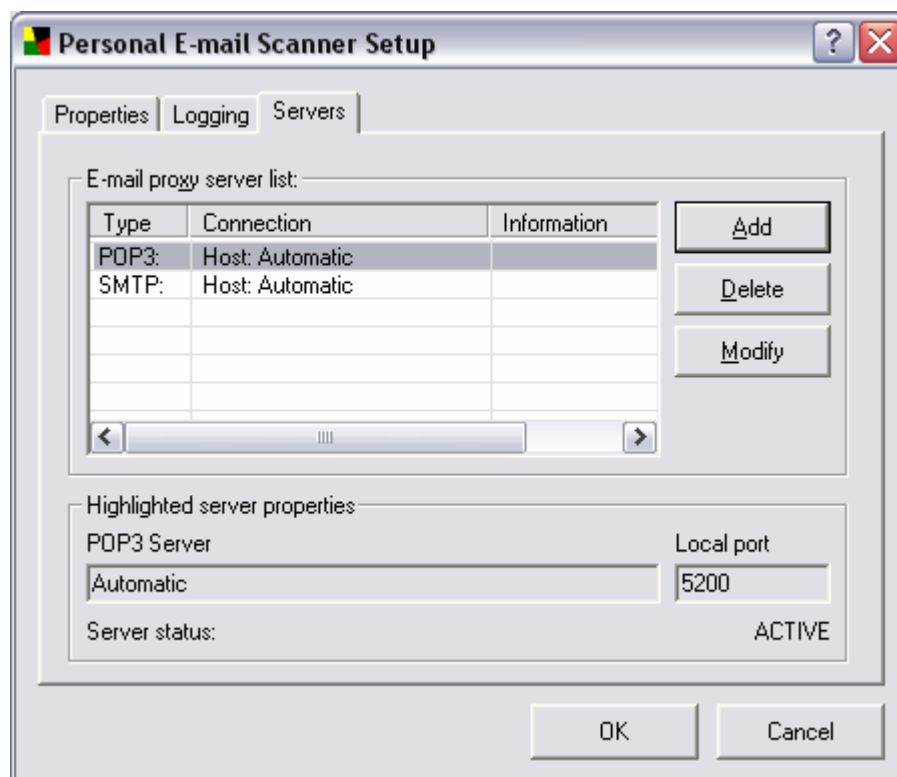
Use this tab to view and modify the list of E-mail servers handled by the AVG Personal E-Mail Scanner.

The **E-mail proxy servers list** box lists all currently defined servers.

– Click the **Add** button to create a new server.

– Click the **Delete** button to delete the selected server.

– Click the **Modify** button to modify the select server properties.

Under **Highlight server properties** lists the parameters the selected server.

The first label shows the server type (for example POP3, SMTP), and the textbox underneath shows the login for POP3 servers or server names for SMTP servers.

The Local port textbox shows which port is used for communication with the given server.

Server status indicates whether the server is active or not.

e)   **Firewall tab**

All **Firewall** settings can be found within this section.

f)   **PUP Excludes tab**

This tab contains a list of defining exceptions for *Potentially Unwanted Programs (PUP).*

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 station, you can define it as a **Potentially Unwanted Program Exception.**

From the AVGADMIN interface you can list, edit, or delete the existing Potentially Unwanted Programs exceptions or define new one.
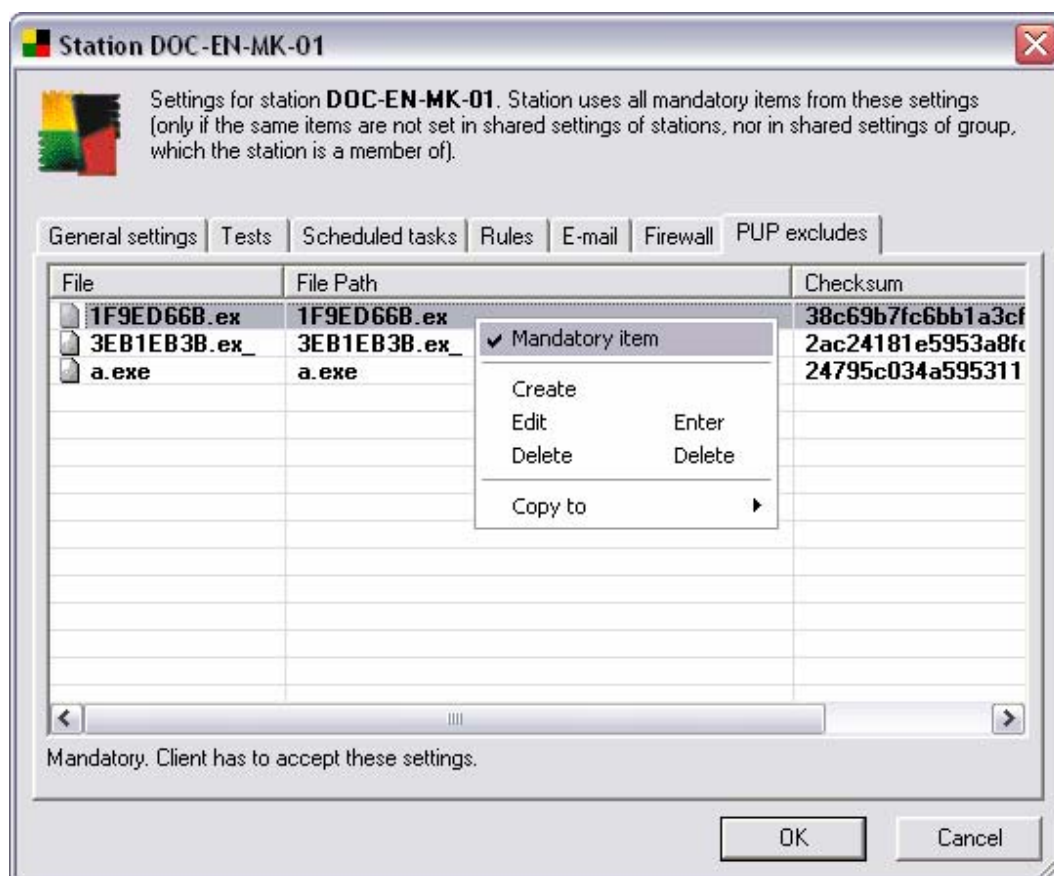
(i) Defining a new exception for Potentially Unwanted Program

Use the mouse to right-click on the table and select the **Create** option to manually define new exception:
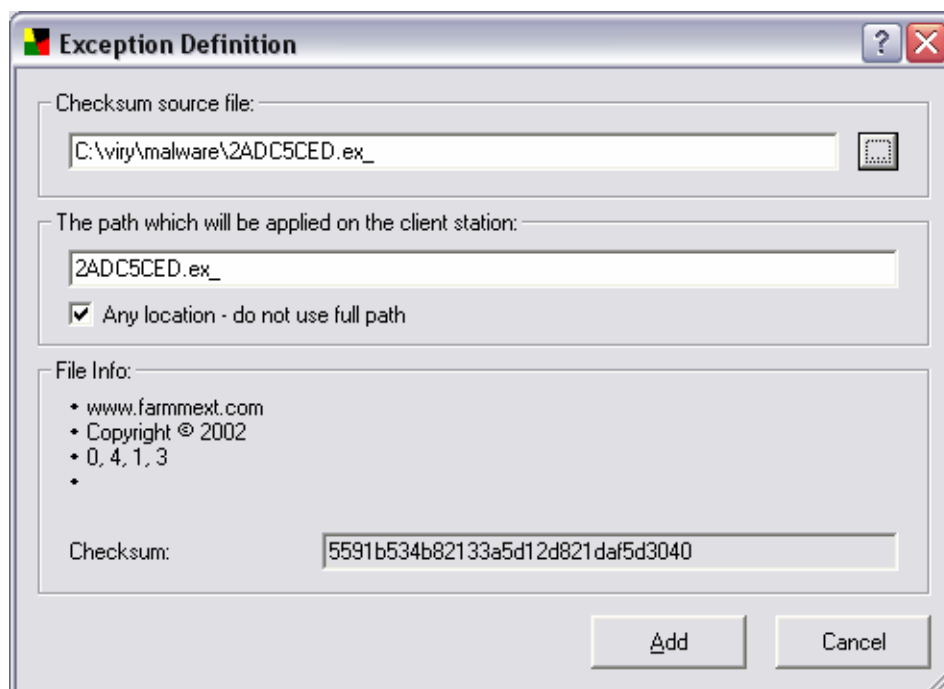
In the **Checksum source file** field, type the full path to the file that you want to mark as an exception. If you want to define this file as an exception only for the specific location, then leave the checkbox **Any location – do not use full path** unchecked.

If you tick the checkbox, then the selected file (and any copies of the file) will be defined as an exception, no matter where they are actually located. You still need to fill in the full path to the specific file, since this will be used as the sample file (just in case more than one 'different' file with the same filename exists on your computer).

You can alternatively click this button to open a standard explorer dialog for easier location of the desired file.

If there is any additional information available about the file (license/version information etc.), it will be displayed within the *File info* section.

The **Checksum** field 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.

To confirm and save the new exception, click the **Add** button.

(ii)   Editing an existing Potentially Unwanted Program exception

To edit an existing exception, choose the row you want to edit and press Enter, or alternatively use mouse to right-click on the row to be changed and select **Edit** option from the menu.
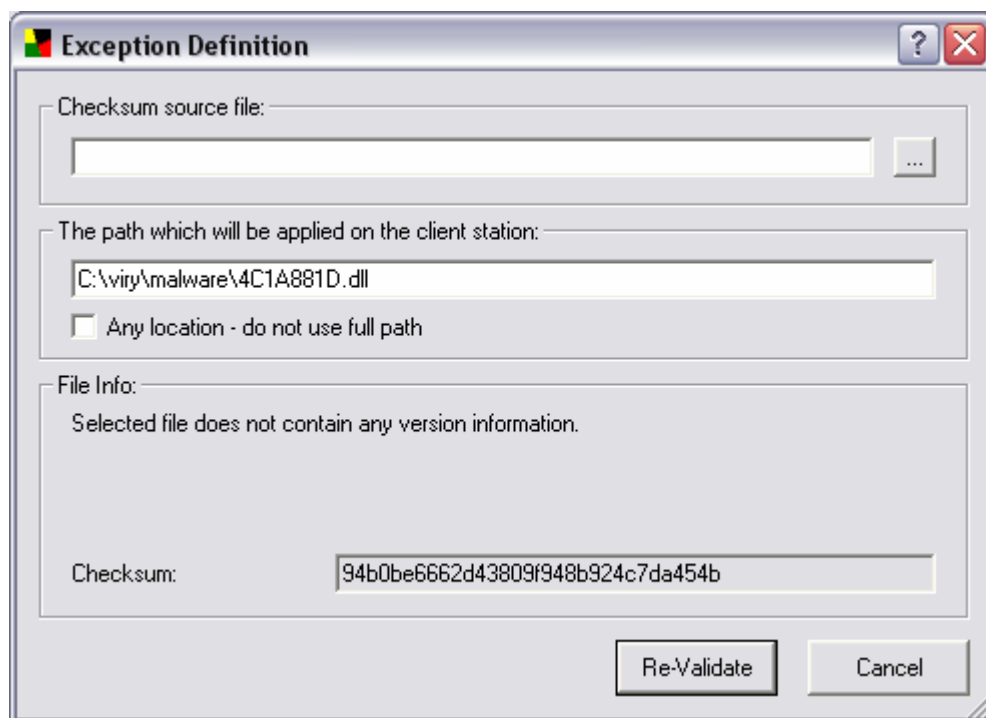
To finish and save your changes, press the **Re-Validate** button.

(iii)   Deleting existing exceptions

To delete any of the existing exceptions, simply select one or more rows and press **DELETE** button, or use mouse to right-click on the selection and from the menu choose **Delete** option.

AVG Anti-Virus Network

12. Centrally Controlled Update

12.1. Update Levels

AVG offers three update levels to select from:

- **Priority update**

  The priority update contains changes necessary for a 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**

  The recommended update contains various program changes, fixes and improvements.

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

- **Optional update**

  The 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. Every update of higher extent (e.g. Optional update) automatically includes all available update types (Priority, Recommended update).

12.2. Update within the Local Network

AVG clients can perform an update directly from **GRISOFT** web servers. Also, it is possible to download the update file onto a LAN server, and configure the **AVG clients** for local update.

For smaller networks (20-25 workstations typically) it is recommended to update directly from the internet. AVG update files are designed so that the smallest available needed files are always being downloaded.

If the network consists of more than 50 workstations, it is better to maintain mirroring of all the available update files within the local network. All the update files (that could be used for all the previous AVG versions update) must be downloaded this way to allow **AVG clients** to use the current file to perform the program/virus database update.

Generally, there are two options of update files local mirroring. The recommended option is using the local web server. **AVG TCP Server** provides limited web server functionality, and it can be used for mirroring. Update files can be downloaded on the **AVG TCP Server** using the **AVGINET Lite** application (a part of the **AVGADMIN** installation package). **AVG clients** then search for the update files on the computer with the **AVG TCP Server** running. This option is considered the preferred way of update file distribution within the local network.

Note: For further information on AVG TCP Server settings please refer to chapter *6.2 - AVG TCP Server as a Local Web Server Update Source*.

However, it is possible to use any other web server for this kind of update. The server only has to share one isolated folder accessible by **AVG clients**. When you are using Microsoft Information Server for example, the root of all the accessible folders is usually *C:\InetPub\wwwroot*. Supposing *C:\InetPub\wwwroot\avgupdate* folder, which is accessible by web interface, is present on the web server called *localweb*. Web (HTTP) clients can access documents and files in this directory by the URL http://localweb/avgupdate. Following these steps, **AVG clients** will use the same URL http://localweb/avgupdate for updates.

Update files can be downloaded using the **AVGINETL** application, which has been launched on the web server with following parameters:

AVGINETL.EXE /URL="http://update.grisoft.cz/softw/70/update" /DIR="C:\InetPub\wwwroot\avgupdate" /PRI=5

This command mirrors all the update files (default settings) from **GRISOFT** main server (the URL parameter) and saves them into the *C:\InetPub\wwwroot\avgupdate* folder. All the update file alternatives (including the optional update) will be downloaded after setting the PRI parameter to the 5 value, as in the example above.

12.3. AVGADMIN Controlled Update

Update files download and **AVG client** updates can also be launched directly from the **AVGADMIN** application. **AVGADMIN** uses AVG modules for the update download, i.e. you need to have AVG installed on the same machine where **AVGADMIN** runs. Only incremental updates will be downloaded, based on the current status of installed AVG.

You can launch the update files download directly from **AVGADMIN** by selecting the *Service / Ask to download update files* item in the main menu. Also, you can ask selected workstations to check possible new files presence in the specified location (URL of web server or a network directory) immediately. To do so, select *Service/Ask stations to update* item in **AVGADMIN** main menu.

AVG 7.5

AVG Anti-Virus Network

13. AVG TCP Server AVG Managed Update Service

Please Note: AVG *Managed Update service and all its settings is available only if you use a proper license!*

The **AVG Managed Update** is a service for our clients that enables forced AVG updates invoked by the **Grisoft** Corporation. Using the service, a registered **AVG TCP Server** can be told by an external incentive (a special TCP/UDP packet sent by a program residing at the **Grisoft** server) that a new update is available. The update files are downloaded then and an update notification is distributed to the defined AVG clients instantly (see the description of the <u>Client info</u> tab for details).

Thus you can obtain and distribute the update immediately after its release. This is another security enhancement, which helps to keep your system even more up-to-date than regular scheduled update checking. But note that the scheduled update does not lose its sense – on the other hand, we recommend you do not neglect the proper setup of scheduled updates, for they can serve as a reserve when the **AVG Managed Update** feature is not functional for any reason.

Note: Only a server with a public IP address can receive update notification packets. And for a server in a firewall-protected network, the respective port (4157 by default) must be allowed for incoming connections.

The **AVG Managed Update** feature is controlled using two tabs in the **AVG TCP Monitor** Advanced Mode settings. The application is accessible from the **AVGADMIN 7.5** folder of the **Programs** folder in the Windows **Start** menu.
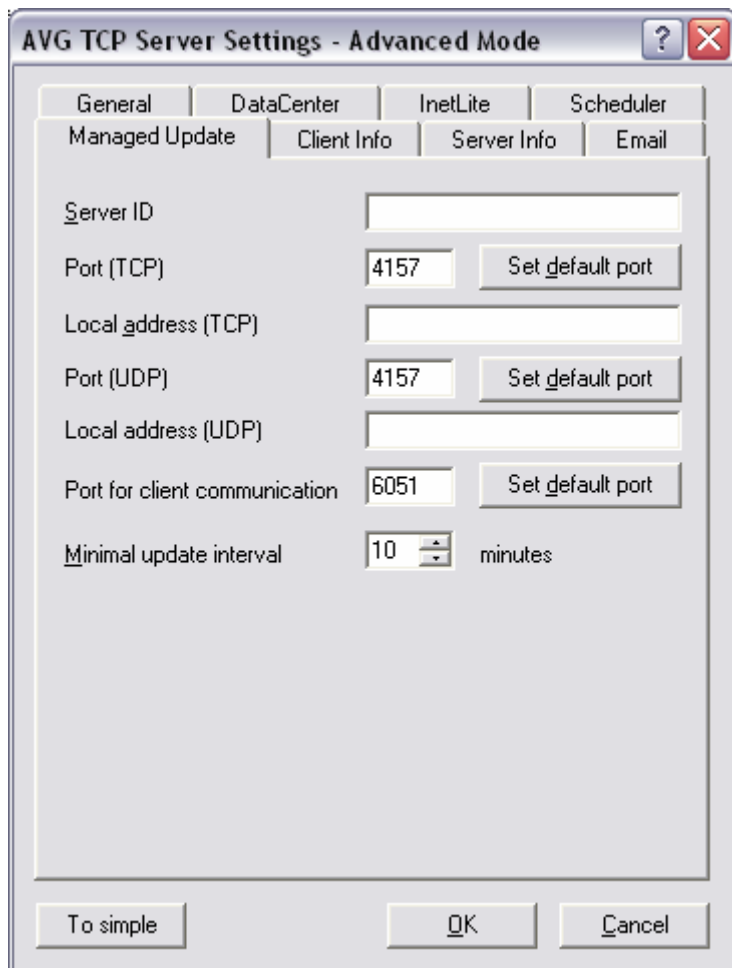
Press the **Configuration** button in the **AVG TCP Server Monitor** interface:

*Note: When the Simple mode of configuration is displayed, press the **To advanced** button. For complete description of the **AVG TCP Monitor** interface and function please refer to <u>6.6 – AVG TCP Monitor Advanced Mode</u> section of this document.*

The tabs of **AVG TCP Monitor** advanced configuration that are designed to set up the **AVG Managed Update** feature are described in the following two sections.

13.1. AVG Managed Update Tab

This tab in the **AVG TCP Monitor** Advanced Mode is the place where you can manage reception parameters of your **AVG TCP Server** with respect to the **AVG Managed Update** feature. The following fields are present within the tab:

● **Server ID**

Identification of your server, obligatory parameter. It must be the same as your *AVG Managed Update* service ID registered by **Grisoft** corporation.

● **Port (TCP)**

The field defines the TCP port where **AVG TCP Server** listens to the incoming commands.

● **Local address (TCP)**

The address where **AVG TCP Server** listens to the TCP encoded incoming commands.

- **Port (UDP)**

  The field defines the TCP port where **AVG TCP Server** listens to the incoming commands.

- **Local address (UDP)**

  The address where **AVG TCP Server** listens to the UDP encoded incoming commands.

- **Port for client communication**

  Enter the number of the port for **AVG Managed Update**-related communication between **AVG TCP Server** and AVG clients.

  *Note: The port must be the same as the **AVG Anti-Virus Network Edition** port number set on the client stations.*

- **Minimum update interval**

  When more commands regarding updates come over the network in a short time, **AVG TCP Server** does not act immediately. It waits for the time specified (in minutes) in this field before another check for updates. This protects your server from becoming overloaded by excessive requests.

  *Note: You can set the default port values for any above field by pressing the respective **Set default port** button.*

AVG 7.5

AVG Anti-Virus Network

13.2. Client Info Tab
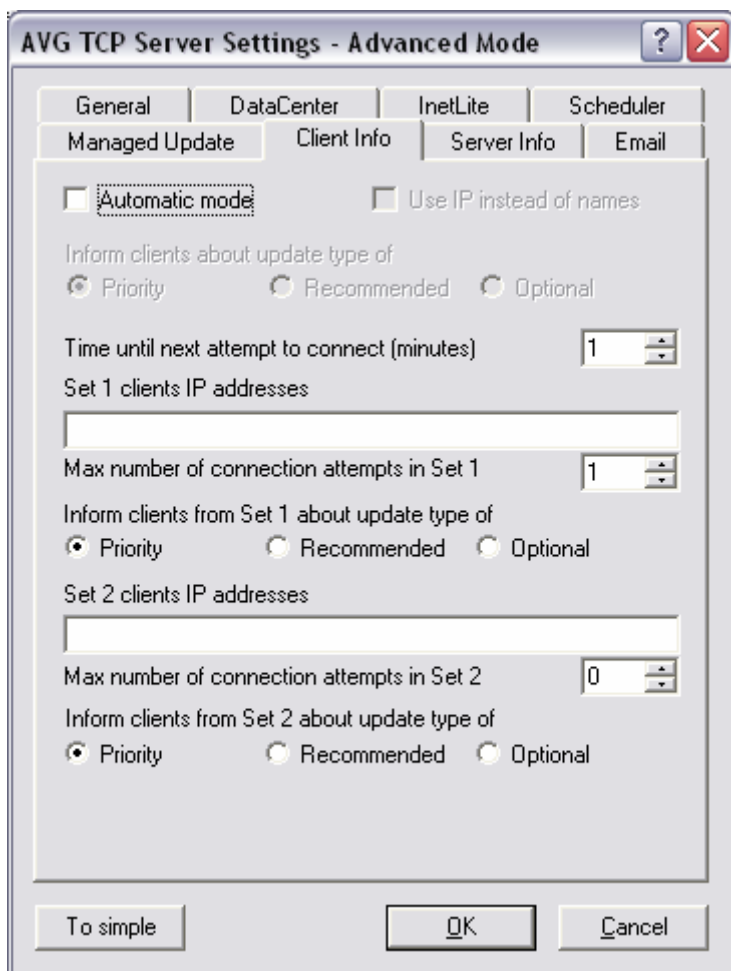
This tab is designed to set up the parameters of the update distribution from **AVG TCP Server** to clients, or between **AVG TCP Servers**. Two modes of update distribution are available – the automatic and manual:

● **Automatic Mode** (the *Automatic Mode* field is checked)

This mode requires **AVG DataCenter** support (so the mode is not accessible when **AVG TCP Server** is used only for update management).

AVG TCP Server gets the clients' (or their IP addresses') list from **AVG DataCenter** in the automatic mode and sends the update command to them. The principle is the same as for the **AVGADMIN** application – the command is stored in **AVG DataCenter** and a notification is send to the station. When a station cannot be reached, it will process the command within the next synchronization with the **AVG DataCenter** database.

● **Manual Mode** (the *Automatic Mode* field is not checked)

Define specific IP addresses of AVG clients for update distributions in the manual mode. You can divide your clients into two groups, when you want to define different rules for particular clients. This mode can be used even if there is no **AVG DataCenter** support.

The fields for each group are as follows (the **X** stands for the group number):

o **Set X clients IP addresses** – the list of clients' IP addresses; available form of values are: *full IP address*, *station name, IP address range* (using the start and the end address of range, divided by dash) or *address combined with network mask.* Examples of address specification follow:

- 122.64.200.216 (IP address)

- 122.64.200.125-122.64.200.133 (IP address range)

- station26 (station name)

- 10.10.2.0/255.255.255.0, 122.64.200.173 (subnet mask and address)

o **Max. number of connection attempts in Set X** – the maximum number of connection attempts for the given set; if set to 0, an unlimited number of attempts is allowed. The default values are 1 for the first set and 0 for the second.

o **Inform clients from Set X about type of update** – select one of the update priority levels (*Priority*, *Recommended* or *Optional*) using the respective radio button.

Note: When you put a station into both of the sets, it is taken as if it were in the second one (the second set has higher priority). Thus you can define all your stations in the first set and the stations with special rules to be applied in the second one.

For the **Manual Mode**, there is one field common for both sets – the **Time until the next attempt to connect**. Specify the time (in minutes), after which the server should try to contact clients that have not been responding during the previous attempts. It will try to connect to all clients until all of them are informed about the update or the allowed number of connection attempts is exceeded.

Note: Any **AVG Managed Update** *related changes performed in the* **AVG TCP Monitor** *configuration interface are saved after pressing the* **OK** *button in the* **Advanced Mode** *window (refer to 6.6 – AVG TCP Monitor Advanced Mode section of this document for details).*

AVG 7.5

13.3. Server Info Tab
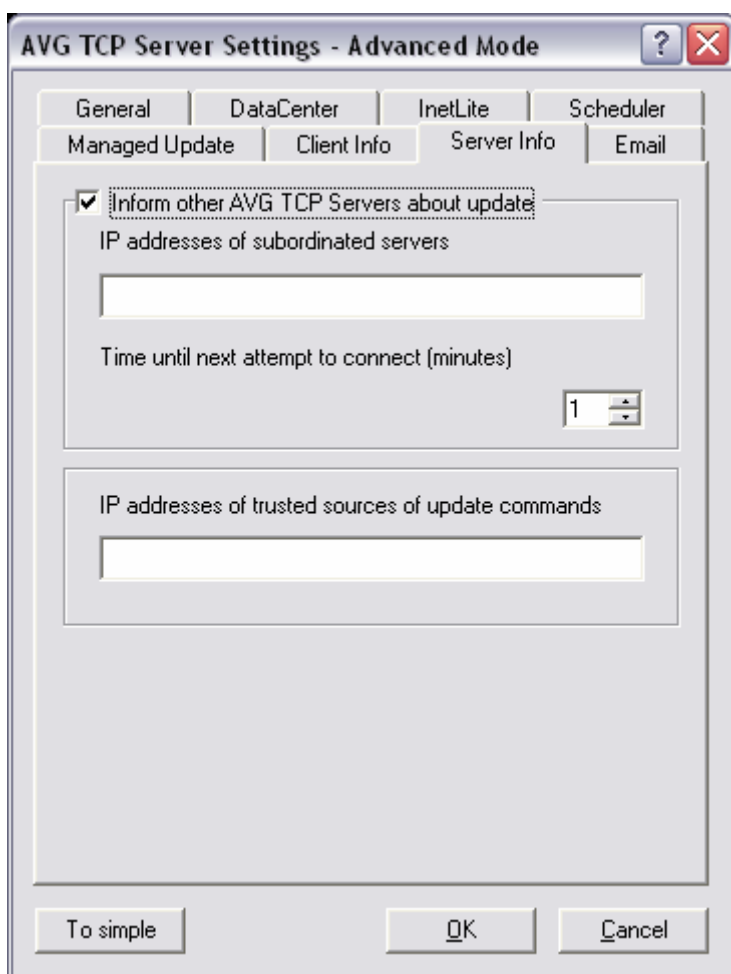
- **Inform other AVG TCP Servers about update**

  By ticking this checkbox you will allow the application to inform about newly downloaded updates also other defined AVG TCP Servers.

  Enter the appropriate server IP value(s) to the **IP addresses of subordinated servers** field. AVG Managed Update updating command will be then send to these addresses. As a part of this command is information about URL, which is to be used for updating (defined by IP address, port accepting HTTP requests and parameter **Http Server Root** – all can be set in the General Tab).

  Time until next attempt connect

  If **AVG TCP Server** does not receive a confirmation of AVG Managed Update command acceptance from one of the defined servers, it will repeat the attempt later. Choose the requested time interval (in minutes).

- **IP addresses of trusted sources of update commands**

  If you need **AVG TCP Server** to accept unsecured AVG Managed Update commands from different AVG TCP Servers, it is necessary to define IP addresses of trusted servers into this field.

Fill this field only on servers, which are subordinated to AVG TCP Servers accepting AVG Managed Update commands from Grisoft, s.r.o. company.

All server addresses on this tab is possible to insert in the same way as addresses in the Client Info Tab (i.e. as an full IP address, station name, IP address range, IP address and mask or combination of all mentioned methods).

14. Alert Manager

14.1. Events and Actions

Anytime the **Resident Shield** has detected a virus, when a scheduled test has ended, when an update has been finished, and on many other occasions, an **event** is shown by AVG. The event is processed by the **Alert Manager** component that executes an **action** according to defined **rules**. An event message can be displayed to the user, or the information can be sent to the **AVG DataCenter**.

Note: The Alert Manager component panel is therefore accessible from the AVG Control Center only if you have installed any AVG network edition.

All AVG installations implement this event management system. Furthermore, network edition users can **change the default rules** and **define new rules** as well.

They can also use additional types of action that are not included in the default settings. It is possible to write event messages into the operating system Event Log, to send a special message to the **AVG DataCenter**, and even to write an e-mail message to the specified address. Some of the standard actions can be edited. A typical example is the **automatic action** option in the dialog with information on the finding of a virus by **Resident Shield** - moving the infected file into **AVG Virus Vault**, etc.

14.2. Alert Manager Rules

The rules define relations between an action and the corresponding event. Every rule defines:

- An event to which it responds.

- The source component of the event; some of the events can be reported by more than one component, a rule can include restrictions to the selected ones.

- An action to be executed; within each rule more actions can be specified (e.g. Event Log recording, and sending a message to the **AVG DataCenter** simultaneously).

After AVG installation there are a few default rules defined without the possibility of editing the event and source component definition. But you can edit actions as needed. In case of a new user defined rules, it is possible to change both the event and source component definitions, as well as the actions.

The default settings of the rules are as follows:

Event	Shown	Action
Virus detection by Resident Shield	When Resident Shield detects a virus	Opens a virus detected message dialog, the user must choose an action. It is possible to configure automatic behavior of the dialog (infected file movement into Virus Vault and so on)

Resident Shield dialog action	In the moment a user selects an action in the Resident Shield dialog (see the previous rule) or when the action is executed automatically	Sending detection information and action selected to AVG DataCenter. It is possible to define, for example, a record to be written into Event Log
Finished test notification	After a scheduled or manually launched test has been finished	Sending information on the test results to the AVG DataCenter

Besides these default rules there are some internal system rules which are hidden from the user.
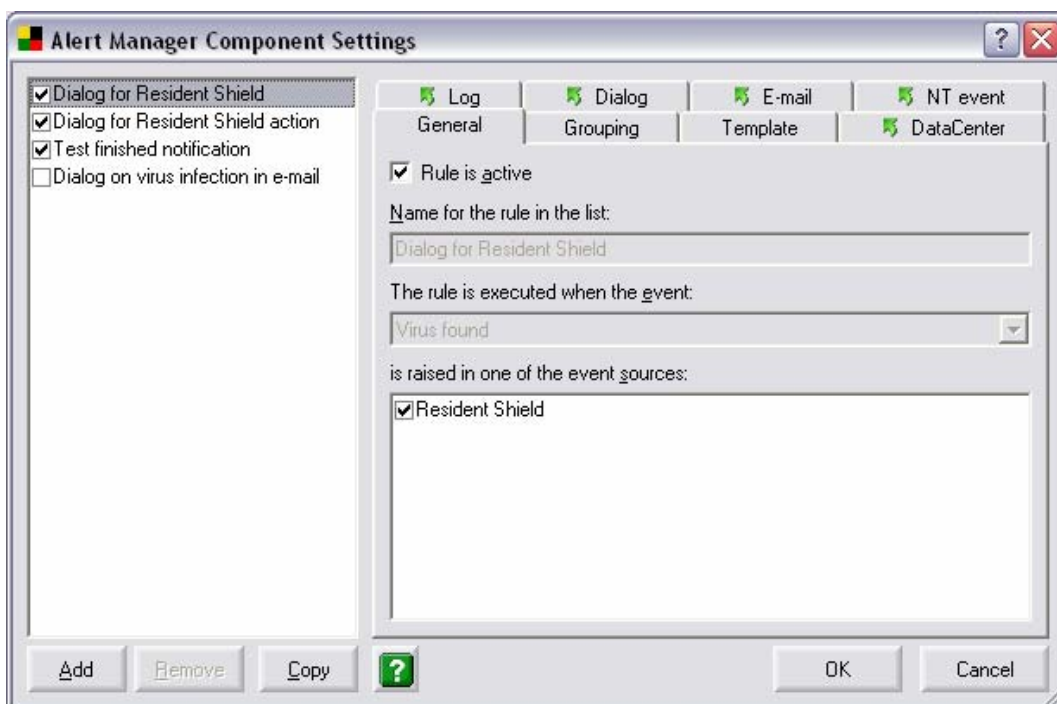
14.3. Rules Configuration

a)   AVG Client Rules Configuration

Within the client part of AVG, the event management configuration window is accessed from the **AVG Control Center/Alert Manager** component:

Press the *Settings* button to open the *Alert Manager Component Settings* dialog:

AVG Anti-Virus Network

On the left side of the window, there is a list of rules with active rules being marked. On the right side you can manage the selected rule settings. Default rules with automatic settings cannot be changed (neither the rule nor the respective action).

General properties, such as the rule name, or rules grouping are common for all rules. Tabs with an action definition included are marked with green arrows. For each rule it is possible to define more actions.

The next screenshot shows an example of **Display dialog to user** action definition for the **Dialog for Resident Shield** rule. This rule is launched if the **Resident Shield** detects a virus.

AVG Anti-Virus Network
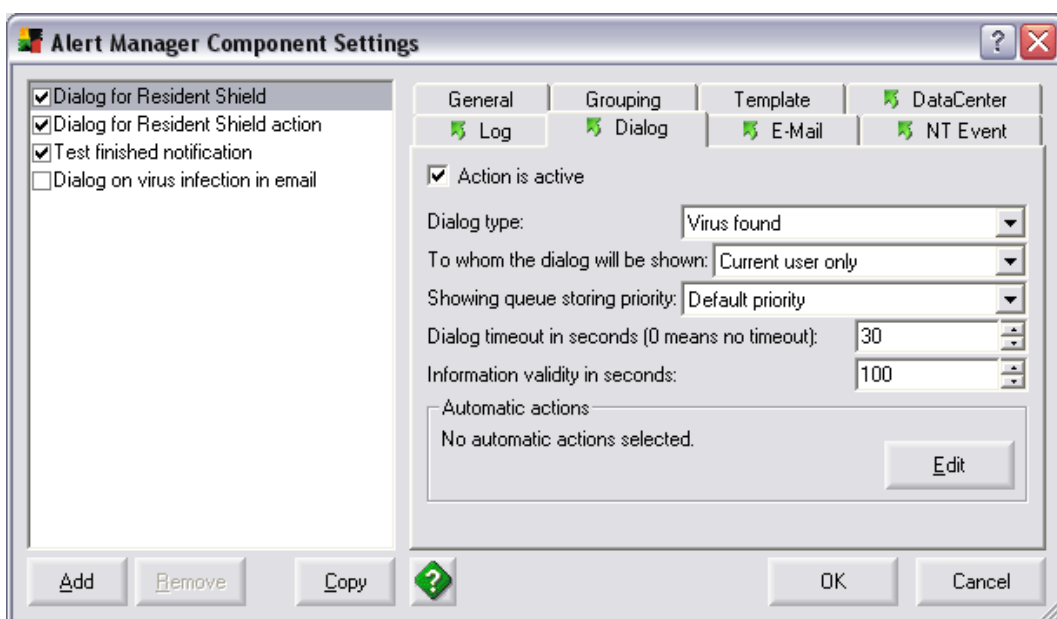
Mind the *Edit* button within the screenshot. Using this button you can define automatic actions to be taken. As an example, all of the available actions are selected on the next screenshot:

o   *Try to heal infected files* – AVG will try to heal and recover the infected files

o   *Wipe infected files* – AVG will delete the infected files

o   *Display notification when automatic actions failed* – a notification message will be displayed to the user if the automatic action failed
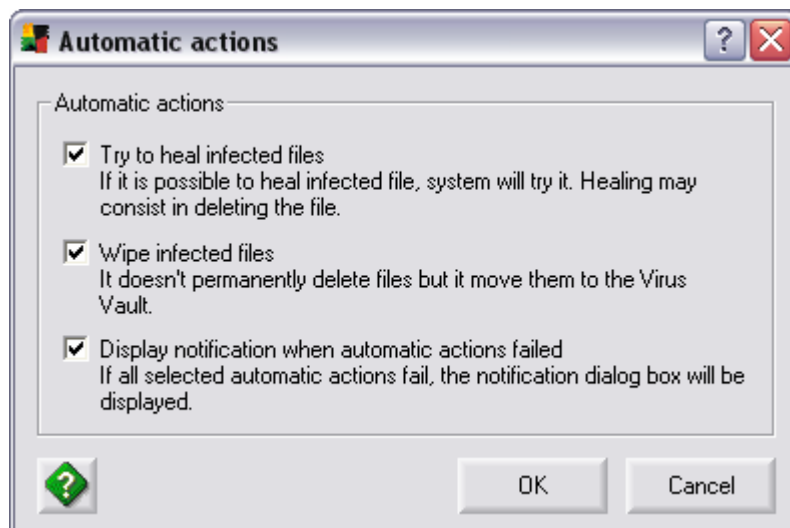
Based on the defined actions, AVG first tries to heal the infected file. If the healing is not successful, AVG tries to delete the file: of course, if the infected file is about to be deleted, it is always moved to the **AVG Virus Vault** first. Then in case even deletion has failed, AVG eventually displays the appropriate notification to the user.

After any of the automatic actions mentioned above have been performed, a *Found virus reported* event is generated. This event is passed to another default rule – *Dialog for Resident Shield action*:
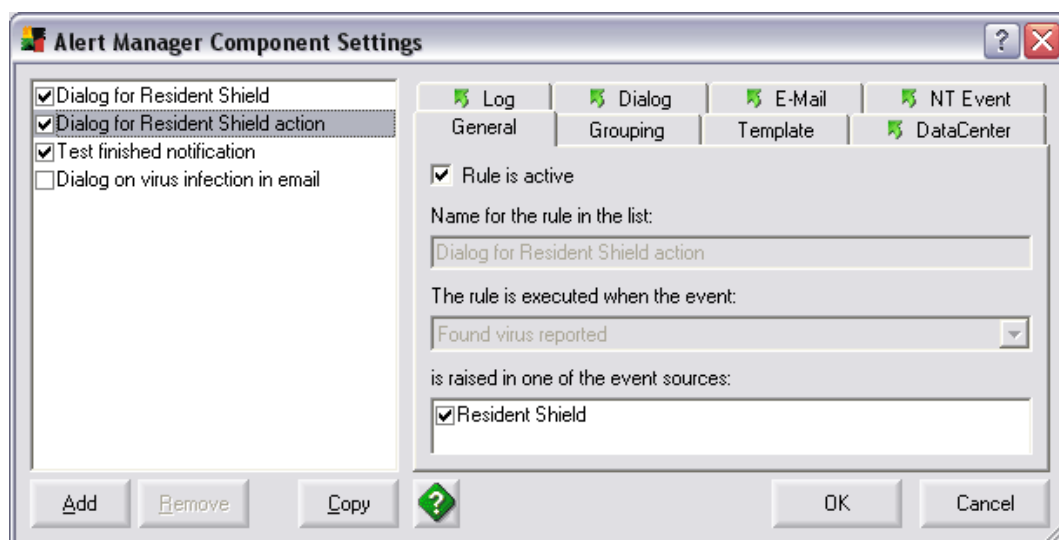
The ***Dialog for Resident Shield action*** rule has the default configuration set up to take the ***Send Message to AVG DataCenter*** action.

For some exceptional situations it may be appropriate to send an e-mail message as well – you can specify this option on the ***E-mail*** tab:
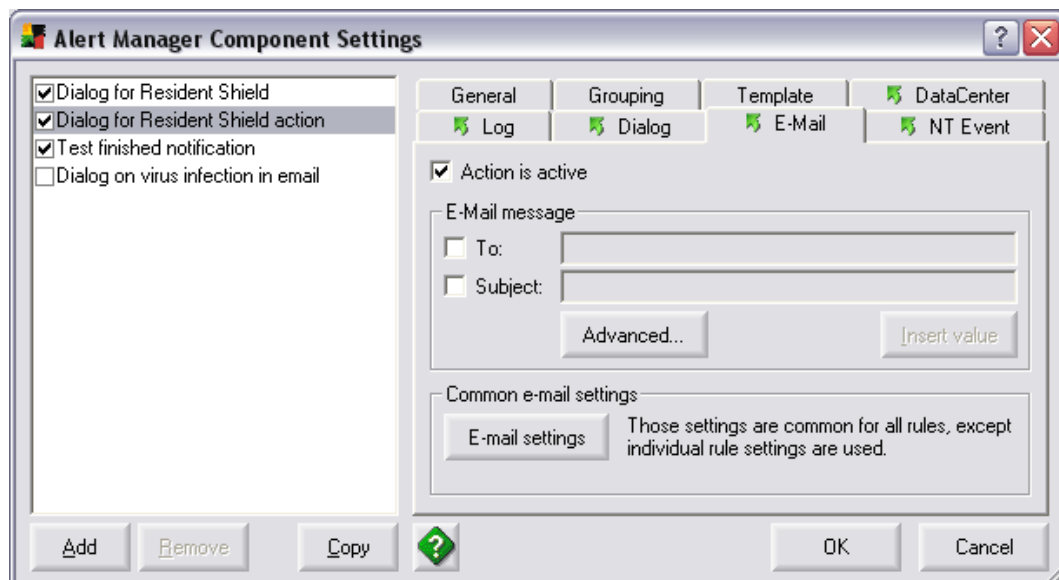
The ***E-mail Settings*** button open a new dialog where you can edit the common e-mail settings shared by all other rules (sender's name, address of mail server, etc.).

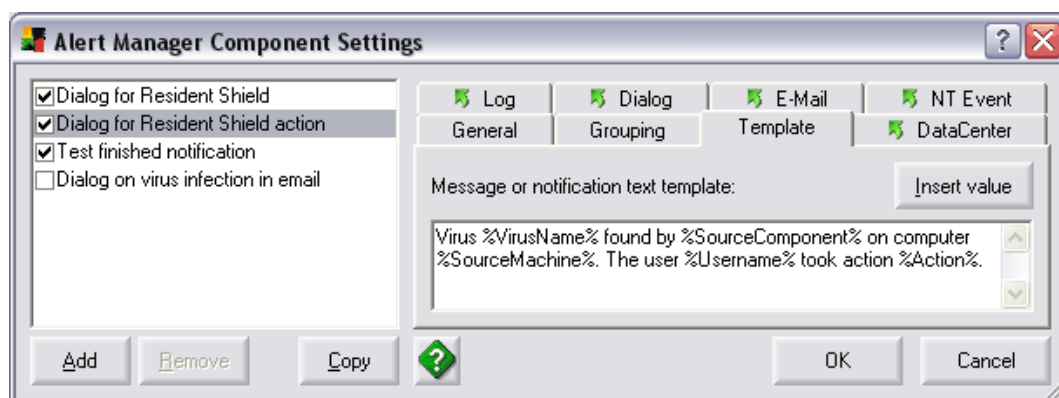Text to be used after an action has been triggered (e.g. the e-mail body text) is predefined on the ***Template*** tab. The message text can be supplemented by special values related to the event properties. Those values are typed inside ***%*** characters for further internal processing. To add a new value, press the ***Insert value*** button:

Default rules specify sending messages on selected important issues to the **AVG DataCenter**. These messages project to their respective overviews. For example, a test result report is further processed according to the conditions specified in the **AVG DataCenter** mode (enable/disable negative test results passing). Besides that you can send a general event message to the **AVG DataCenter**. These messages are recorded in the event overview.

Only generic text message sending is enabled on the screenshot below:
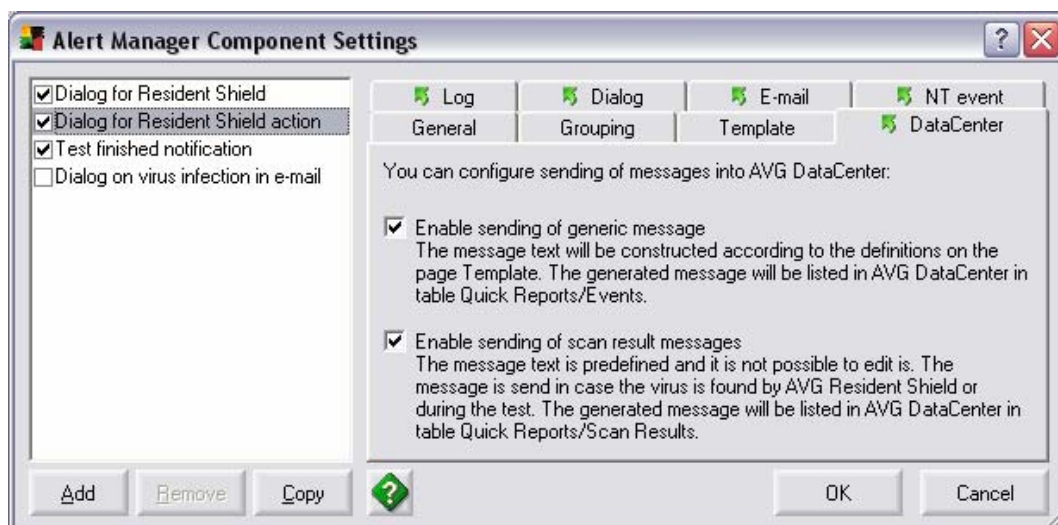
Attention!

*For proper AVG Anti-Virus Network Edition functioning it is recommended to keep the **Enable sending of generic message** option specified for the default rules! You are encouraged to disable this action only if you have an actual reason to do so! For sending a generic text notification we recommend creating a new rule!*

b)   Events Grouping

In case of a huge virus epidemic, the e-mail messaging frequency can be very high. If the **E-mail message sending** action had been activated for a virus found event, the addressee mailbox and mail server may be overloaded very quickly. To prevent an excessive number of shown events you can define event grouping conditions for each rule.
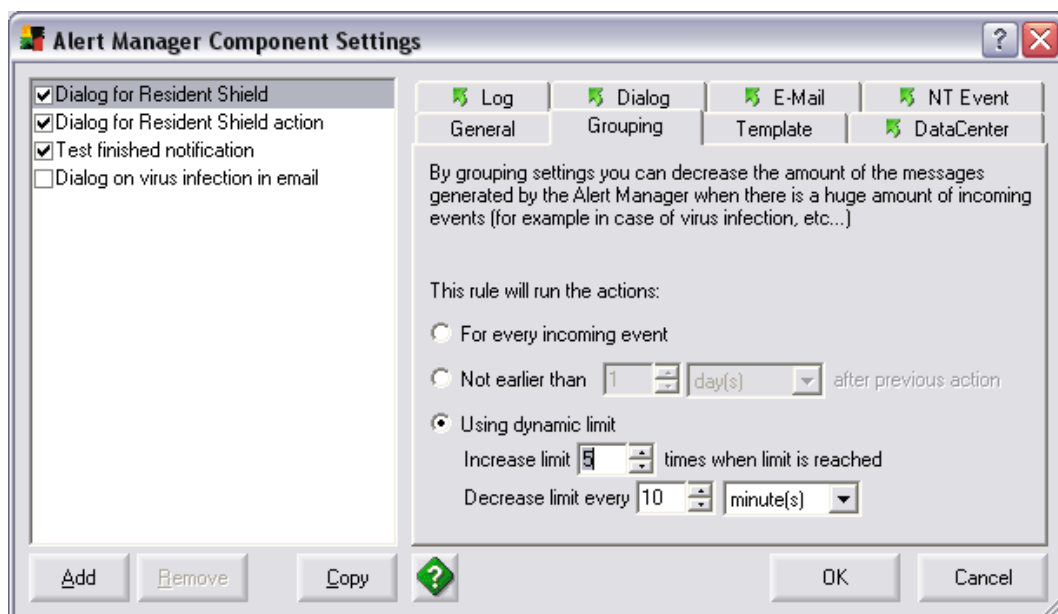
o   ***For every incoming event*** - By default, an action is triggered for each event occurrence.

o   ***Not earlier than ... after previous action*** - It is possible to delay the next action launch by setting a minimum time interval for which the same event is ignored. All the events shown in this interval will then be joined into a group. The next action (e. g. the next e-mail message) will cover an overview of all the grouped events.

o   ***Using dynamic limit*** - In this mode, any triggered action will increase the limit of grouped events n-times. The first virus detection will trigger an action. The same following event will execute no action, it will be grouped instead. On the screenshot above the limit is set to 5, so the next action will be triggered after five successive virus detections. In case of a sixth detection, the limit would be increased 5-times again. After the specified period of time the limit will decrease automatically.

This feature allows flexible adaptation to the current situation. It helps to ensure that the administrator is warned immediately in case of a single event; on the other hand it minimizes the chance of network overload in case of an epidemic.

c)   Events in the AVGADMIN application

The administrator can define rules for particular events centrally in the **AVG DataCenter** using the **AVGADMIN** application – to reach this dialog, please follow the steps:

o   **AVGADMIN**

o   ***Settings*** menu item

o   ***Shared settings for stations*** item

o   ***Alert Manager*** option

o   ***Rules*** tab
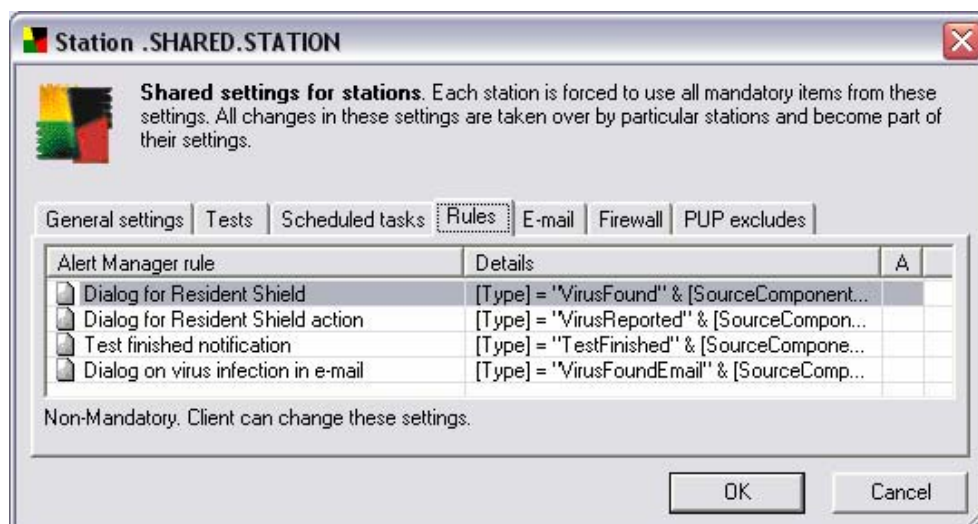
A list of rules for stations is displayed in the dialog together with some detailed rule information. Double-click the selected rule to open a new rule configuration dialog similar to the client rule configuration dialog.

Again, the default rules send special messages relating to some important events to the **AVG DataCenter**. These messages are reflected in the respective dedicated overviews. For example, a test result message is further processed according to conditions defined in the **AVG DataCenter** mode (enabled/disabled passing of negative test results).

Besides this, it is possible to send a generic event message to the **AVG DataCenter**. These events are recorded in the event log.

14.4. Configuration Suggestions

Please pay attention to the following suggestions for rules configuration. Ignoring these main principles can result in serious problems, such as network congestion, Denial of Service error occurrence on application servers, etc.

- For the proper **AVG Anti-Virus Network Edition** functionality we recommend that you keep the specific notifications sending action in default rules. If you want to disable this action you should have an actual serious reason to do so. For generic text notification sending we recommend creating a new rule!

- Using the **E-mail** action is recommended only for exceptional situations, such as virus detection by the **Resident Shield** on a mission critical system. Otherwise, the load generated by **E-mail sending** action can congest a recipient's mailbox and overload the mail server. The final damage can then be greater than the potential one caused by a successfully captured virus.

- Generally, use of automatic actions is not recommended in the **Dialog for Resident Shield** option. Deletion of system-essential files can result in unwanted system or application failures without informing the user of possible reasons for such a situation. Moreover, the user is not informed in case a virus epidemic is caused by dangerous or irresponsible behavior, such as browsing untrustworthy websites or the launching of unknown applications.

- Before implementing a rule in a larger network we recommend testing the rule in a testing environment first. Particularly, it is necessary to evaluate the potential impact of a newly-created rule on the network resources – mail servers, free disk space, number of event records in operating system Event Log and so on.

15. AVGINET Lite

AVGINET Lite is an application, which is able to detect new AVG update files presence, download them, and also perform the AVG update itself. **AVGINET Lite** can work in standalone mode or use a configuration of the installed **AVG client**. The name of the application's executable file is AVGINETL.EXE.

15.1. Update Files Mirroring

The most frequent use of the **AVGINET** application is mirroring of the update files in a local network. In this mode it is necessary to specify at least the URL of the update server (update files source). Usually the location of the target directory is also specified. The full syntax of the AVGINET command is as follows:

AVGINETL.EXE   /URL=<url>   [/DIR=<dir>]   [/PRI=<pri>]

[/FULL_ONLY | /NO_DIFF]   [/NO_DELBIN]   [/SILENT]
[/PROXY="http://user:password@server:port"] [/TYPEOS=winall/all/linux]

AVGINET Lite application downloads the update files from the URL specified in **<url>** parameter into the directory specified in **<dir>** parameter. When the target directory is not specified, the update files are downloaded into the directory, which the **AVGINET Lite** was launched from. /URL parameter is compulsory; all the others are optional. The parameters description is covered below.

If a proxy server is needed to perform the update download, you can define its address and accessible account in /PROXY or /HTTP_PROXY parameter.

Example:

AVGINETL.EXE /URL="http://update.grisoft.cz/softw/70/update"
/DIR="C:\UPDATEAVG" /PRI=5 /TYPEOS=winall

In this case, the **AVGINET Lite** application downloads all the available update files only for MS Windows (with the *.bin extension), which are specified in an update control file AVG7INFO.CTF. Downloaded files will be stored in the directory C:\UPDATEAVG. **AVGINET Lite** does not need an **AVG client** installed on a station where AVGINETL.EXE is running.

15.2. AVG Client Update Using AVGINET Lite

AVGINET Lite can also be used for updating of already installed AVG on client workstations. You can manage the hidden AVG update using the /UPDATE_AVG parameter. The process executed in this way employs the update tool of AVG. **AVGINET Lite** can use the client's parameters in this mode for all the unspecified ones. The full syntax of the command is:

AVGINETL.EXE   /UPDATE_AVG   [/URL=<url>]   [/PRI=<pri>]

[/FULL_ONLY | /NO_DIFF | /CTF_ONLY]   [/PREINSTALL]   [/SILENT]
[/PROXY="http://user:password@server:port"][/TYPEOS=winall/all/linux]

Example:

AVGINETL.EXE /UPDATE_AVG /PRI=3

AVG 7.5

AVG Anti-Virus Network

In this case AVG has to be installed on a station where the **AVGINET Lite** application is running. The application downloads all essential update files according to priority level 3 (recommended update). The update process itself is then executed.

15.3. List of Available Parameters

Parameter and value name	Meaning
/URL="<url>"	Defines URL, which shall be used for downloading the update files. The recommended value is: "http://update.grisoft.cz/softw/70/update"
/DIR="<path>"	Defines the target directory for the update files download.
/PRI=<id>	Defines the update files priority (the default value is 3 – recommended update).
/NO_DIFF	No differential update files will be used for AVG update.
/FULL_ONLY	Only full update files will be used.
/CTF_ONLY	Only the control file (AVG7INFO.CTF) will be downloaded.
/NO_DELBIN	The unnecessary files will not be deleted after a successful download.
/UPDATE_AVG	Activates the update mode – AVG installation on a computer, on which the AVGINET Lite application is running, will be updated. If there is no such installation on the computer, AVGINET Lite will be closed.
/PREINSTALL	Downloads the update control file AVG7INFO.CTF, analyzes it and if necessary, will download available update files. After the download, the AVG update will be prepared. All the processes will be finished after the next execution of AVG.
/SILENT	All error reports will be deactivated.
/PROXY= "http://user:password@server:port"]	Defines the proxy server connection and account.
/TYPEOS=	Defines operating system for which updates will be downloaded. Possible parameter values

	are:
	winall – MS Windows
	linux – Linux
	all – Both Linux and MS Windows
	Default value is **all**.
/HELP or /?	Basic help will be displayed.
/HELPU	AVG update related help will be displayed.
/HELPM	Mirroring of the update files related help will be displayed.
/HELPE	Return values description will be displayed.

Return values of AVGINET Lite application	
0	Update/mirroring of update files was finished successfully.
1	No new update files found.
2	New update files found.
3	New update files found and successfully downloaded.
4	Reboot is needed to finish the update.
5	The downloaded update control file AVG7INFO.CTF is damaged (this is caused by wrong URL specification in most cases).
6	Update was finished due to a damaged update file.
7	There was an error detected when checking URL.
8	There was an error detected when processing the command line parameters.
9	There was an error detected during the update.
10	Update or download of update files was interrupted.
11	Only help was shown.

16. Anti-Spam

Note: *The Anti-Spam component is available only in* **AVG Internet Security Network Editions**. *For more information about this product visit Grisoft website at* www.grisoft.com.

AVG 7.5

AVG Anti-Virus Network

17. 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 17.1 AVG Diagnostics utility for more information how to process the technical support request.

17.1. AVG Diagnostics utility

Note: This utility can be started only from AVG applications!

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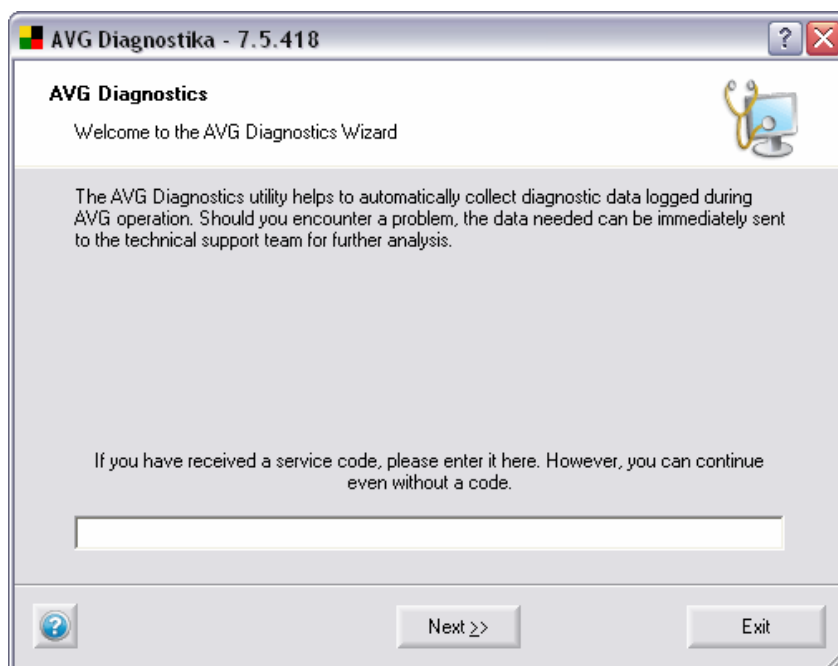
If you have received a service code, please type it into the text field, or use the copy/paste method. The code will automatically set up the correct **AVG diagnostics mode** which ensures that only the required (and no redundant) data is collected during the **AVG Diagnostics** session.

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

o   Contact AVG Technical Support and ask for an **AVG Diagnostics** service code. We strongly recommend this option if you are an inexperienced user.

o   Click **Next** and run the **AVG Diagnostics** utility in full (default) mode. In this case continue to step b - Error description.

o   If you are well experienced computer user you can shut down **AVG Diagnostics** and follow instructions in step e) Advanced settings - AVG Diagnostics Modes.

o

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.
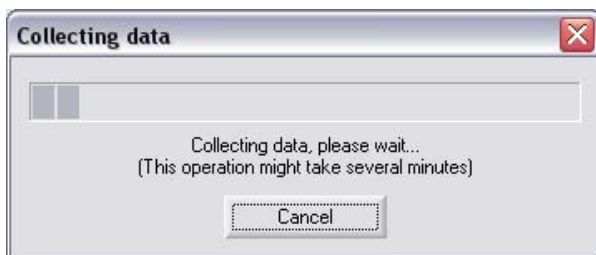

c) AVG Diagnostics Wizard Finalization

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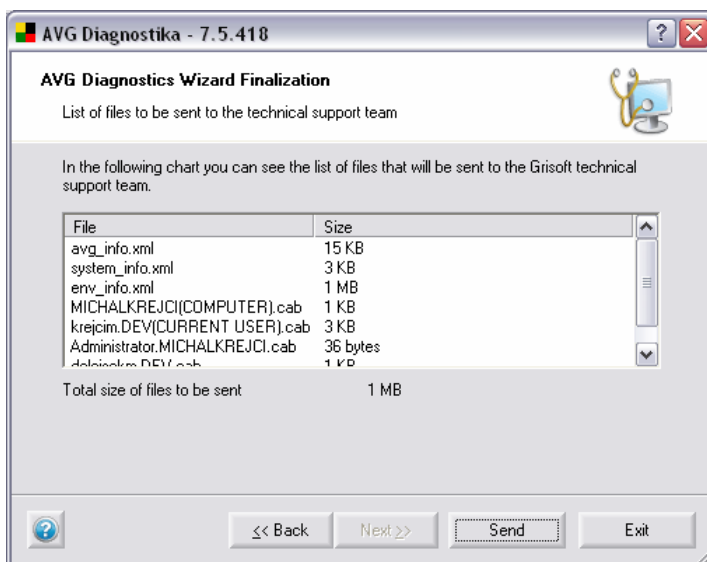
Confirm the process by clicking the **Send** button. A new dialog will appear with previously entered data and your license number.

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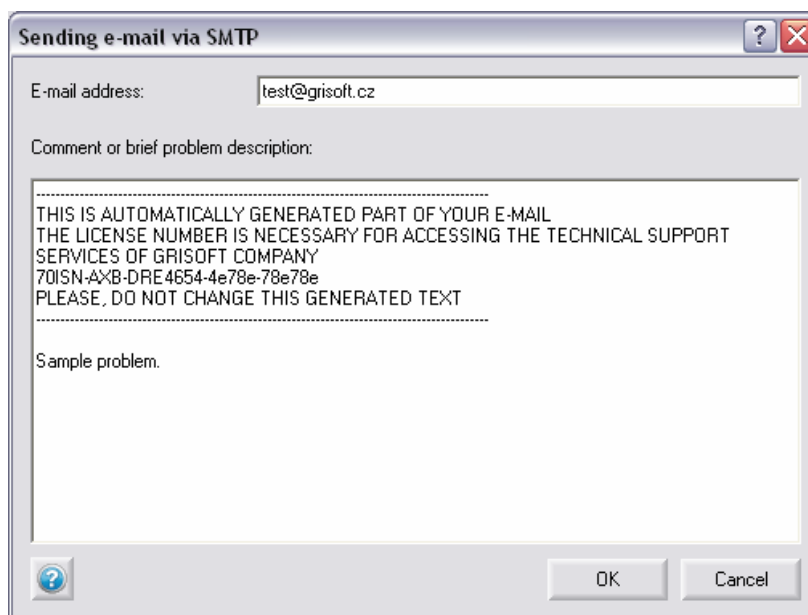
To send the data to the Grisoft technical support team, click the **OK** button. AVG Diagnostics will then try to automatically send the collected data.

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:

o   automatically by an **AVG Diagnostics Service code** (supplied by AVG Technical Support along with the **AVG Diagnostics** utility),

o   by running **AVG Diagnostics** from the command line with the respective parameter.

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

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

o   **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*

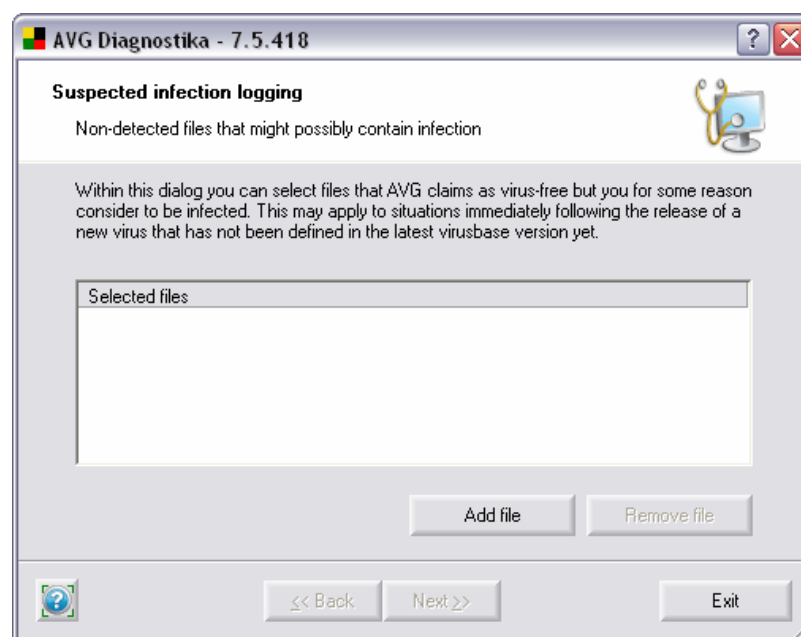o ***Sending a suspect file for analysis***

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 Anti-Virus.

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.

o   ***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>

o   ***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

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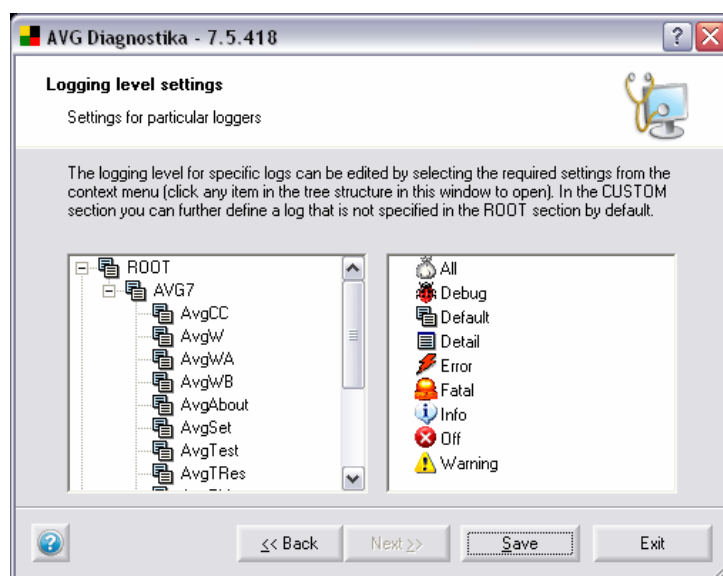
The left section displays an expanded logger tree. The AVG7 branch contains all default AVG loggers; the CUSTOM branch allows you to define a new logger (double-click <new item>). To specify a path for the logger, use dots, e.g. AVG7.AvgWB.MyLogger.

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.
/LNG=<lng>	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>