AVG File Server 2012

User Manual

Document revision 2012.03 (8/19/2011)

Contents

1. Introduction

This user manual provides comprehensive documentation for **AVG File Server 2012**.

Congratulations on your purchase of AVG File Server 2012!

AVG File Server 2012 is one of a range of award winning AVG products designed to provide you with peace of mind and total security for your server. As with all AVG products **AVG File Server 2012** has been completely re-designed, from the ground up, to deliver AVG's renowned and accredited security protection in a new, more user friendly and efficient way.

AVG has been designed and developed to protect your computing and networking activity. Enjoy the experience of full protection from AVG.

Note: *This documentation contains description of specific File Server Edition features. Should you require information about other AVG features, please consult the user guide to Internet Security edition, which contains all the necessary details. You can download the guide from the http://www.avg.com.*

2. AVG Installation Requirements

2.1. Operation Systems Supported

AVG File Server 2012 is intended to protect workstations/servers with the following operating systems:

- Windows 2003 Server and Windows 2003 Server x64 Edition (Service Pack 1)
- Windows 2008 Server and Windows 2008 Server x64 Edition

(and possibly higher service packs for specific operating systems)

2.2. File Servers Supported

The following file servers are supported:

- MS SharePoint 2003 Server version
- MS SharePoint 2007 Server version
- MS SharePoint 2010 Server version

2.3. Recommended Hardware Requirements

Recommended hardware requirements for **AVG File Server 2012** are:

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

3. AVG Installation Process

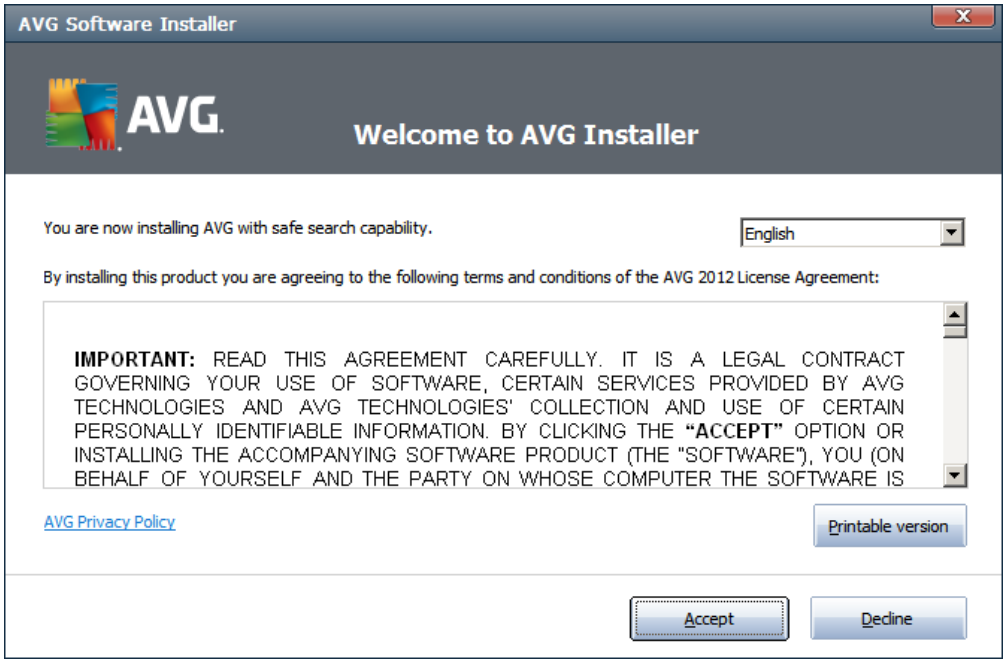
To install AVG on your computer, you need to get the latest installation file. You can use the installation file from the CD that is a part of your box edition but this file might be out-of-date. Therefore we recommended getting the latest installation file online. You can download the file from the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

Note: *There are two installation packages available for your product - for 32bit operating systems (marked as x86) and for 64bit operating systems (marked as x64). Be sure to use the correct installation package for your specific operating system.*

During the installation process you will be asked for your license number. Please make sure you have it available before starting the installation. The number can be found in the CD packaging. If you purchased your copy of AVG on-line, your license number will have been delivered to you via e-mail.

Once you have downloaded and saved the installation file on your hard drive, you can launch the installation process. The installation is a sequence of dialog windows with a brief description of what do at each step. In the following, we offer an explanation for each dialog window:

3.1. Installation Launch



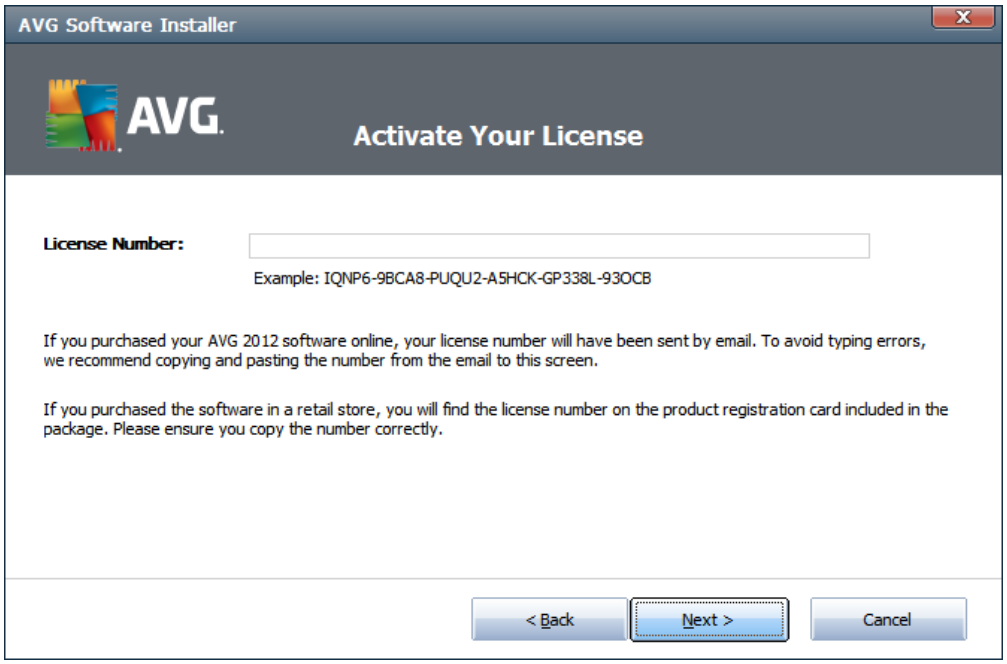
The installation process starts with the ***Welcome*** window. In here you select the language used for the installation process and read the license conditions. Use the ***Printable version*** button to open the license text in a new window. Press the ***Accept*** button to confirm and continue to the next dialog.

Attention: *You will be able to choose also additional languages for the application interface later during the installation process.*

3.2. Activate Your License

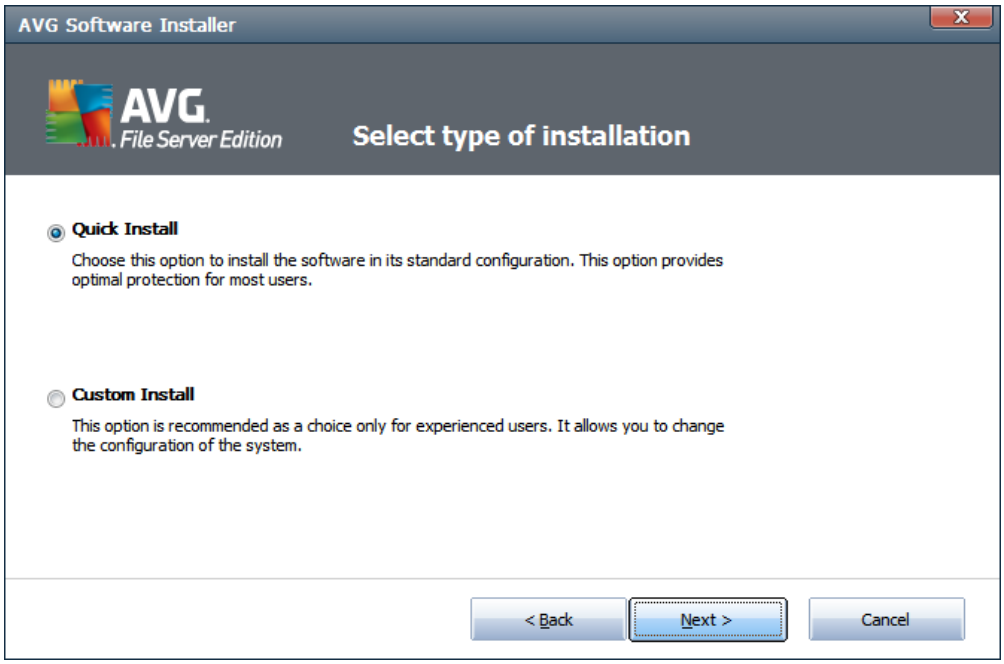
In the ***Activate your License*** dialog you have to fill in your license number.

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



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

3.3. Select Installation Type

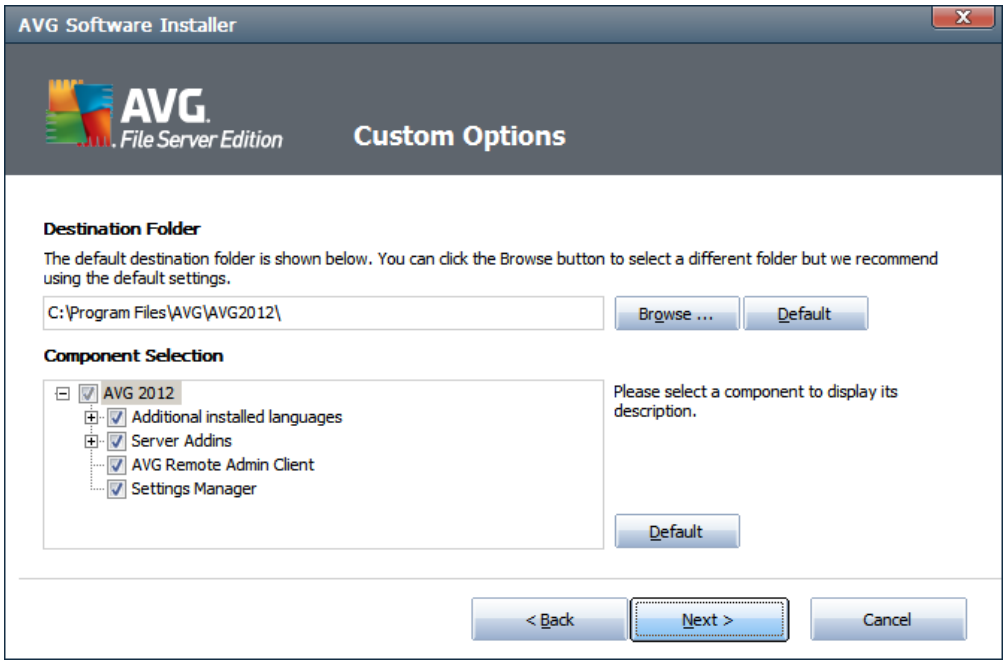


The ***Select type of Installation*** dialog offers the choice of two installation options: ***Quick Install*** and ***Custom Install***.

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

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

3.4. Custom Install - Custom Options



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

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

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

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

  Note: *Only server components available in the list can be managed remotely!*

- ***Settings Manager*** - a tool suitable mainly for network administrators that allows you to copy, edit and distribute AVG configuration. The configuration can be saved to a portable device (USB flash drive etc.) and then applied manually or any other way to chosen stations.

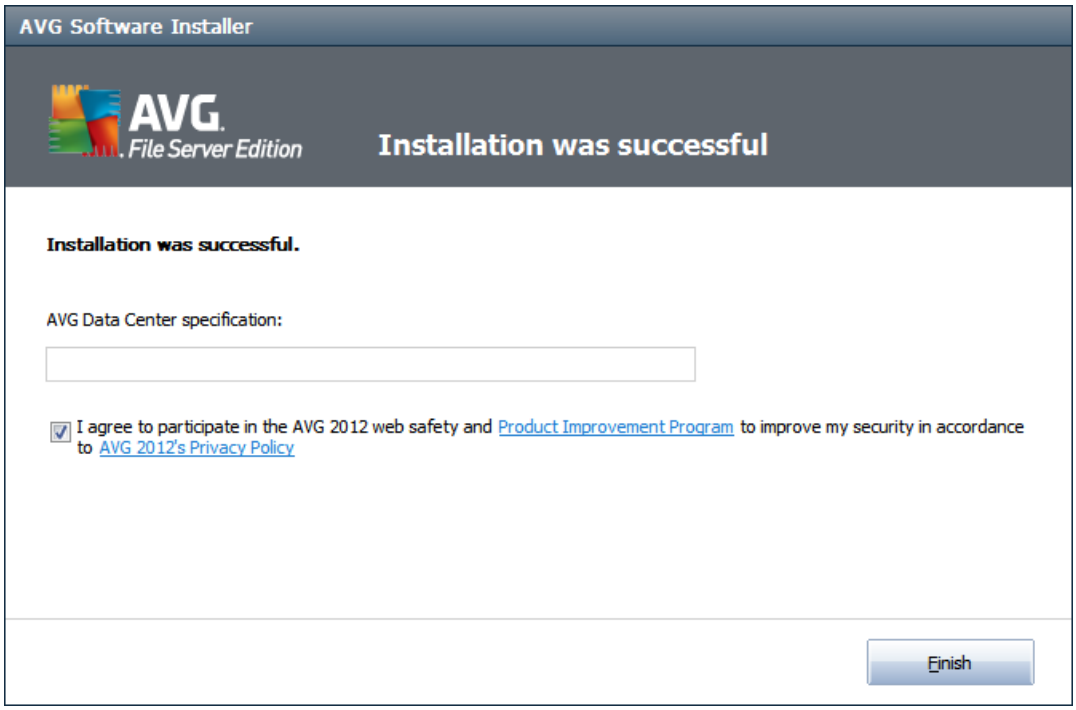
- ***Additional Installed Languages*** - you can define which language(s) AVG should be installed in. Check the ***Additional installed languages*** item and then select the desired languages from the respective menu.

- ***Server Addins*** - only ***Document Scanner for MS SharePoint*** server component is available in this AVG edition. It scans documents stored in MS SharePoint and removes all viruses detected.

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

3.5. Installation Completion

If you selected the ***Remote Administration Component*** module during module selection, then the final screen will allow you to define the connection string for connecting to your AVG DataCenter.



AVG is now installed on your computer and fully functional. The program is running in the background in fully automatic mode.

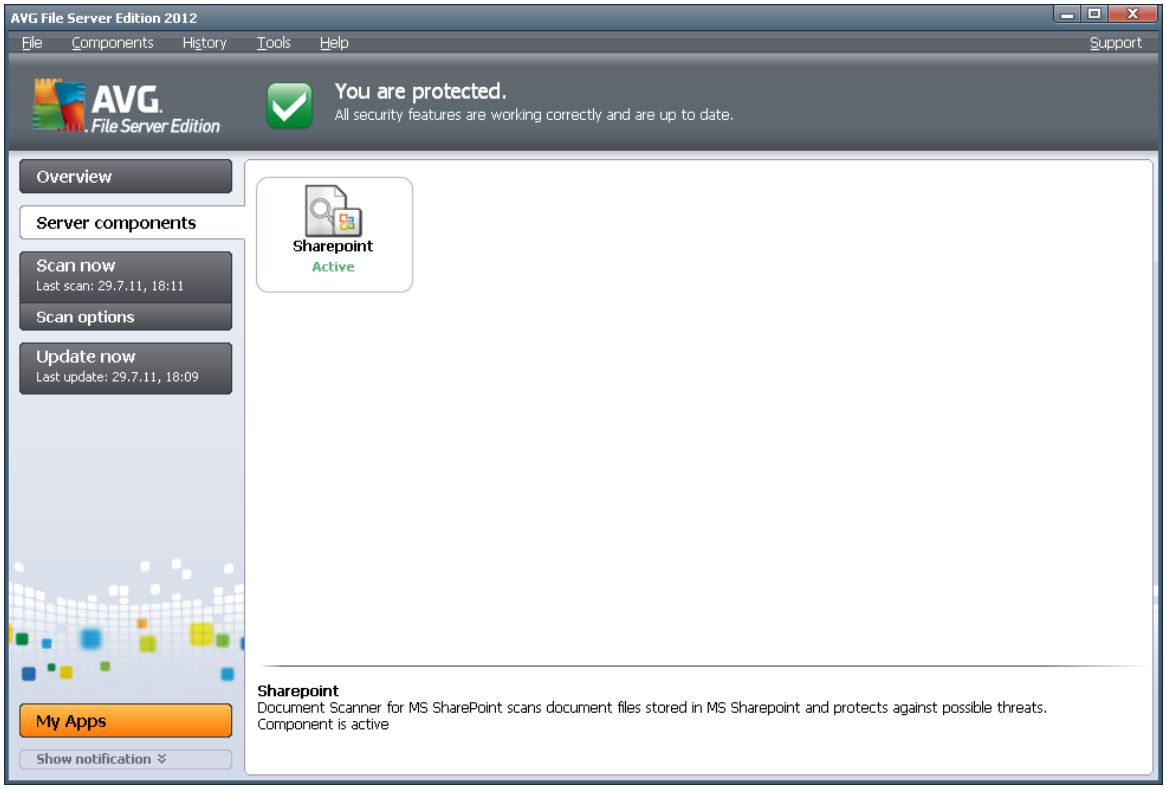
To individually setup protection for your e-mail server, follow the appropriate chapter:

- ***Document Scanner for MS SharePoint***
- ***AVG for SharePoint Portal Server***

4. Document Scanner for MS SharePoint

4.1. Overview

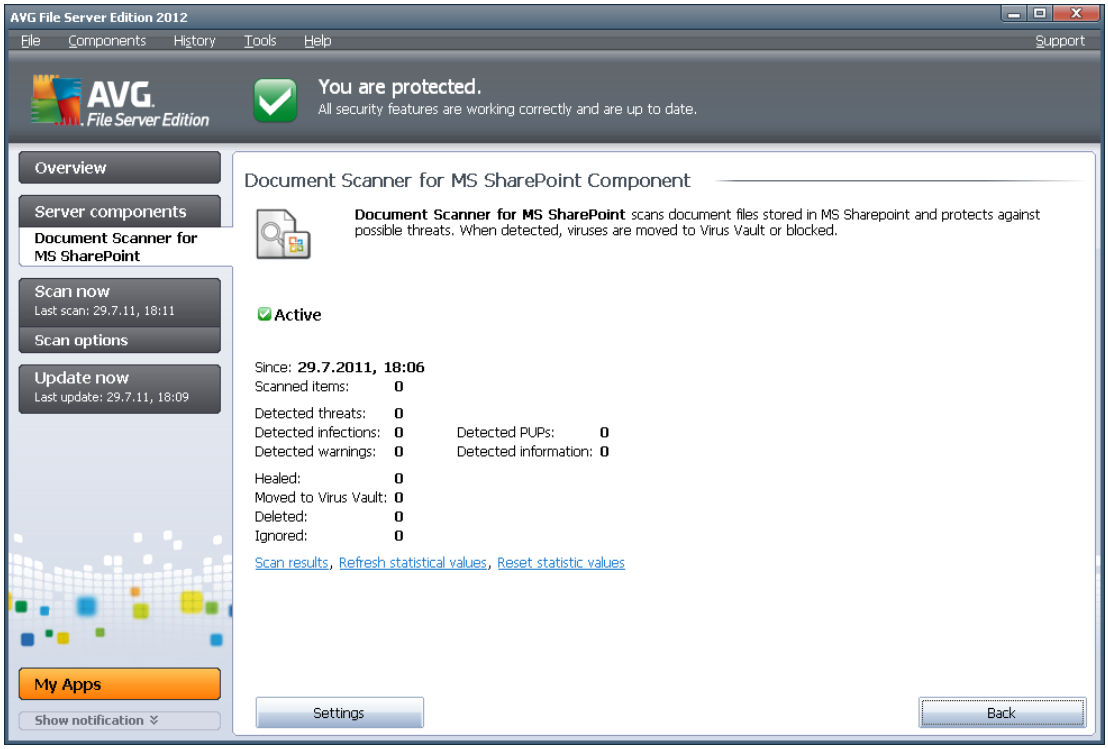
The AVG for MS SharePoint Server 2003/2007/2010 configuration options are fully integrated within the AVG File Server 2012 via the server components screen.



The purpose of the ***Document Scanner for MS SharePoint*** server component (it is the only one available in this AVG edition) is to scan documents stored in MS SharePoint. If any viruses are detected, they are moved to the Virus Vault, or completely removed.

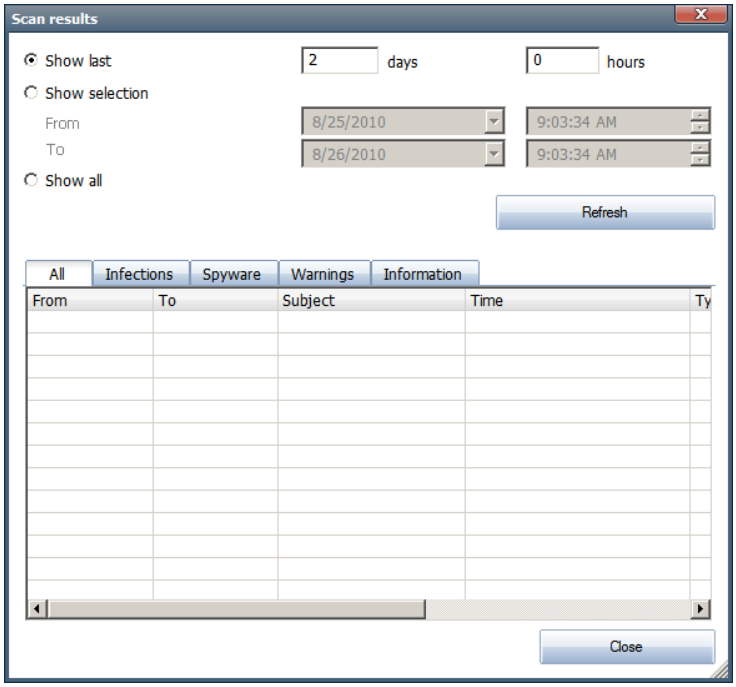
Microsoft SharePoint is a collection of products and software elements that includes, among a growing selection of components, Internet Explorer–based collaboration functions, process management modules, search modules and a document-management platform. SharePoint can be used to host web sites that access shared workspaces, information stores and documents.

Click the component icon to open its interface:



- ***Scan Results***

  Opens a new dialog where you can review scan results:



  Here you can check messages divided into several tabs according to their severity. See configuration of individual components for amending the severity and reporting.

By default there are displayed only results for the last two days. You can change the displayed period by amending the following options:

- ***Show last*** - insert preferred days and hours.
- ***Show selection*** - choose a custom time and date interval.
- ***Show all*** - Displays results for the whole time period.

Use ***Refresh*** button to reload the results.

- ***Refresh statistical values*** - updates stats displayed above.
- ***Reset statistical values*** - resets all the stats to zero.

The working buttons are as follows:

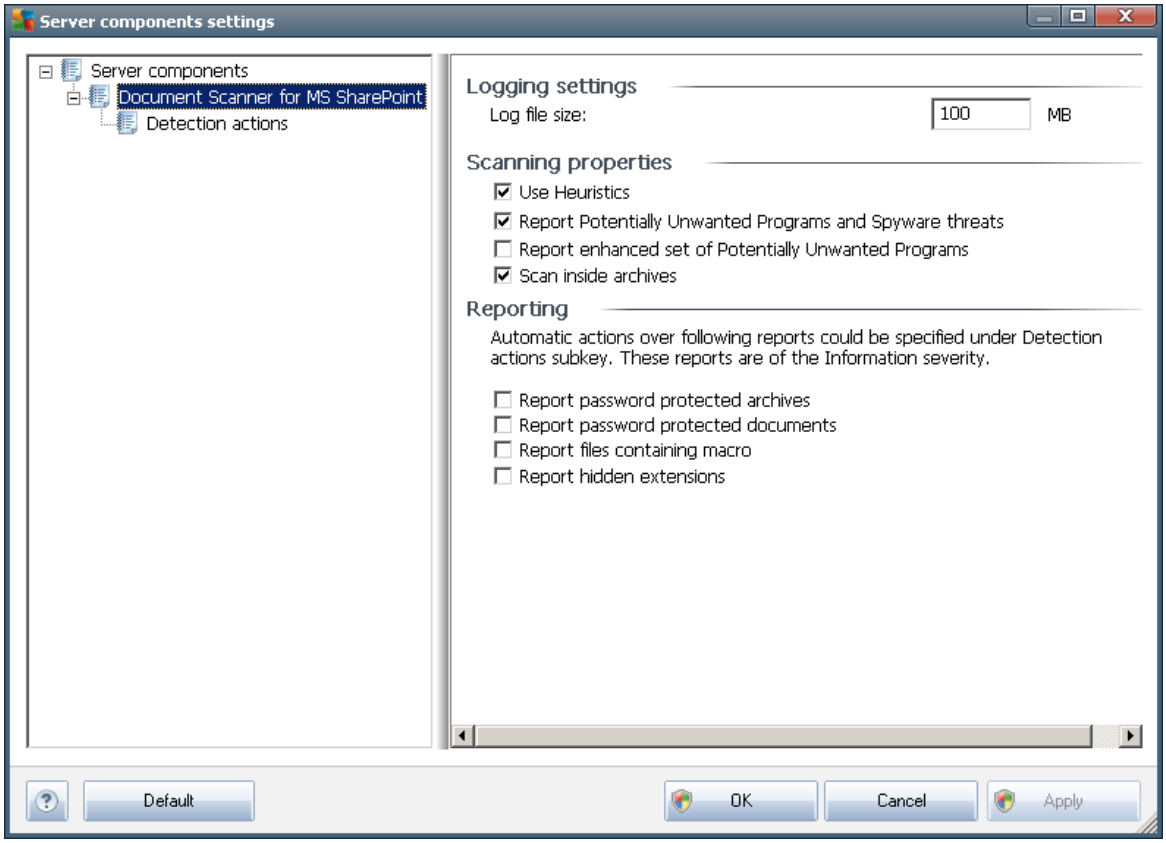
- ***Settings*** - use this button to open settings of the component.
- ***Back*** - press this button to return to the Server components overview.

You will find more information on more advanced settings of this component in the chapters below.

4.2. Document Scanner for MS SharePoint

To open the settings of **Document Scanner for MS SharePoint**, select the ***Settings*** button from the interface of the component.

From the ***Server components*** list select the ***Document Scanner for MS SharePoint*** item:



The ***Logging settings*** section:

- ***Log file size*** - choose a preferred size of the log file. Default value: 100 MB.

The ***Scanning properties*** section:

- ***Use Heuristics*** - check this box to enable heuristic analysis method during scanning.
- ***Report Potentially Unwanted Programs and Spyware threats*** - check this option to report the presence of potentially unwanted programs and spyware.
- ***Report enhanced set of Potentially Unwanted Programs*** - check to detect extended package of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later, or programs that always harmless but might be unwanted (various toolbars etc.). This is an additional measure that increases your computer security and comfort even more, however it can possibly block legal programs, and is therefore switched off by default. Note: This detection feature is additional to the previous option, so if you want protection from the basic types of spyware, always keep the previous box checked.
- ***Scan inside archives*** - check this option to let the scanner look also inside archived files (zip, rar, etc.)

The ***Reporting*** section allows you to choose which items should be reported during scanning. This

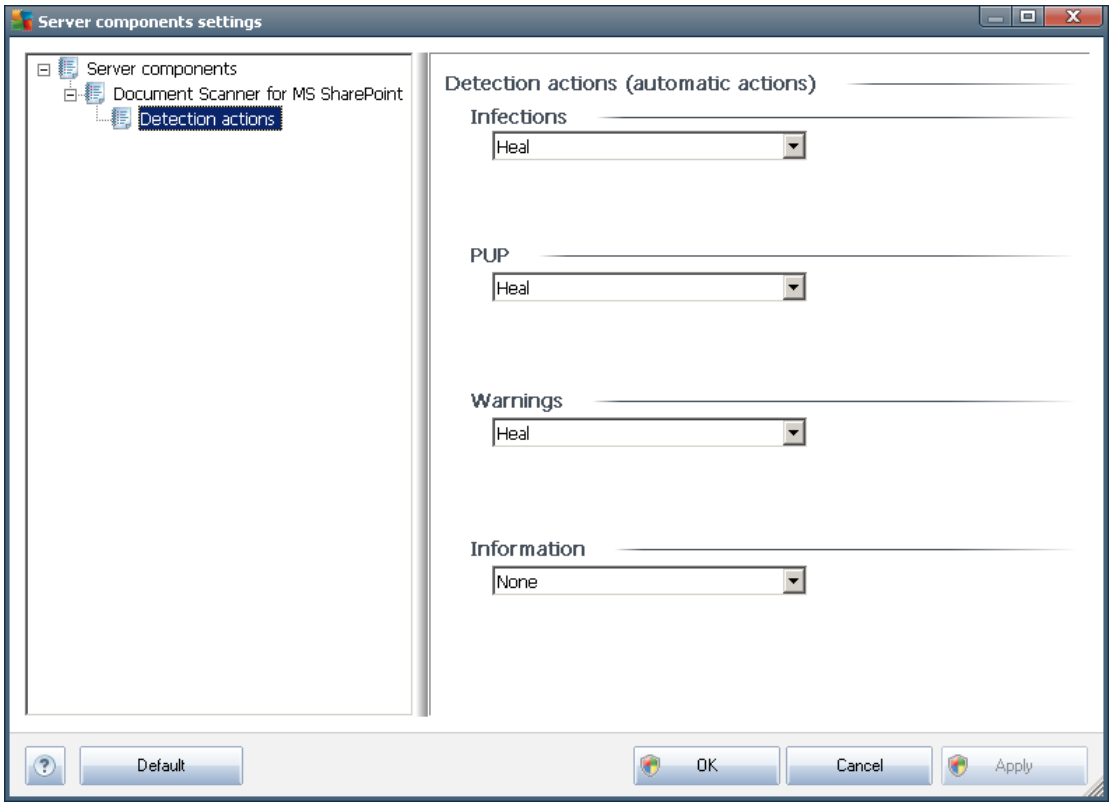
is the default configuration which can be easily amended in the ***Detection actions* section**, part ***Information*** (see below).

The following options are available:

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

There are also ***Detection actions*** sub-item available in the following tree structure (see the chapter below).

4.3. Detection actions



In this dialog you can configure how the ***Document Scanner for MS SharePoint*** component should behave, when it detects a threat. The threats are divided into several categories:

- ***Infections*** – malicious codes that copy and spread themselves, often unnoticed until the damage is done.
- ***PUP (Potentially Unwanted Programs)*** – such programs, in general, vary from positively serious to only potential threats to your privacy.
- ***Warnings*** – detected objects unable to be scanned.
- ***Information*** – includes all detected potential threats that cannot be classified as any of the above categories.

Use the roll-down menus to select an automatic action for each of them:

- ***None*** – a document containing such threat will be left alone.
- ***Heal*** - tries to heal the infected file/document.
- ***Move to Vault*** – every infected document will be moved into Virus Vault quarantine environment.
- ***Remove*** – a document where a virus is detected will be deleted.

5. AVG for SharePoint Portal Server

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

5.1. Program Maintenance

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

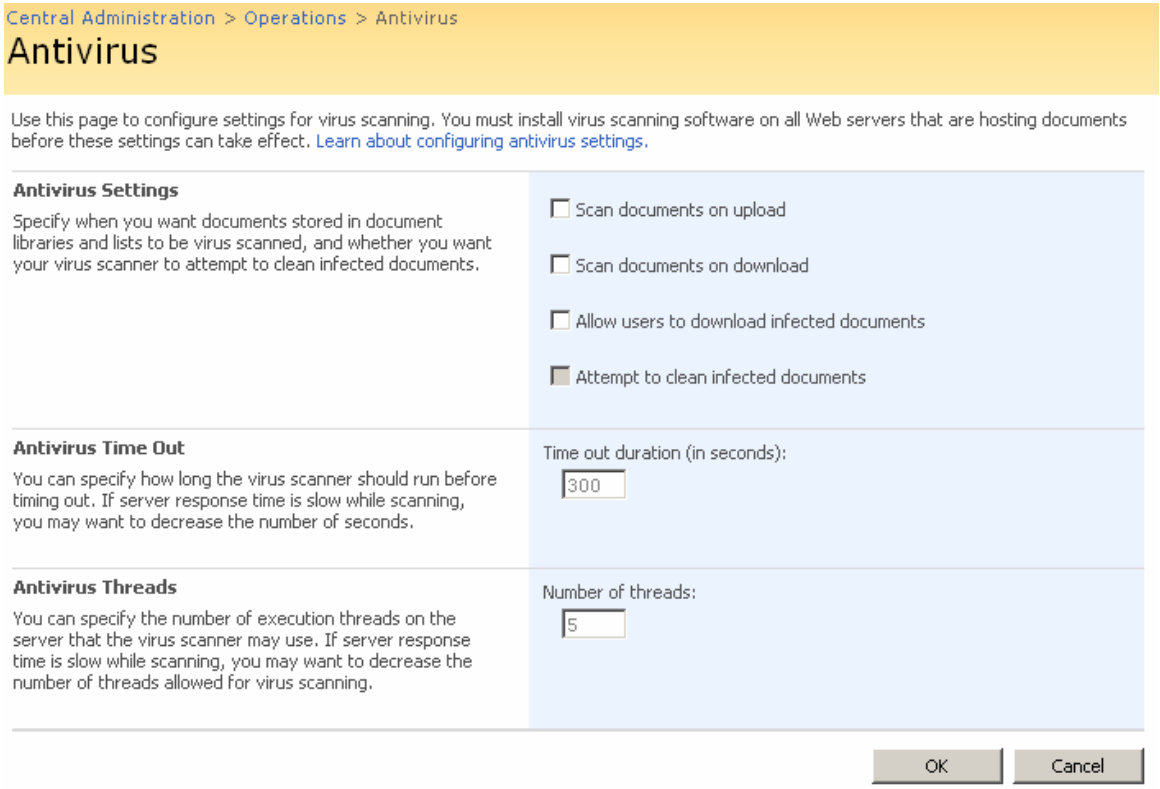
You can launch the ***SharePoint Portal Server Central Administration*** when you are logged in on the computer that your server is running on. The administration interface is web-based (*as well as the user interface of the SharePoint Portal Server*) and you can open it using the ***SharePoint Central Administration*** option in the ***Programs/Microsoft Office Server*** folder (depending on your version also ***SharePoint Portal Server***) of the Windows ***Start*** menu, or by navigating to ***Administrative Tools*** and selecting ***Sharepoint Central Administration***.

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

5.2. AVG for SPPS Configuration - SharePoint 2007

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

The following window will then be displayed:

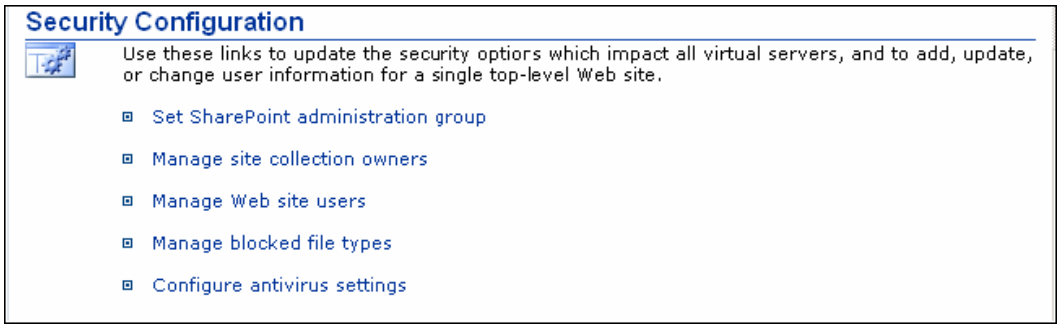


You can configure various **AVG for SharePoint Portal Server** anti-virus scanning actions and performance features here:

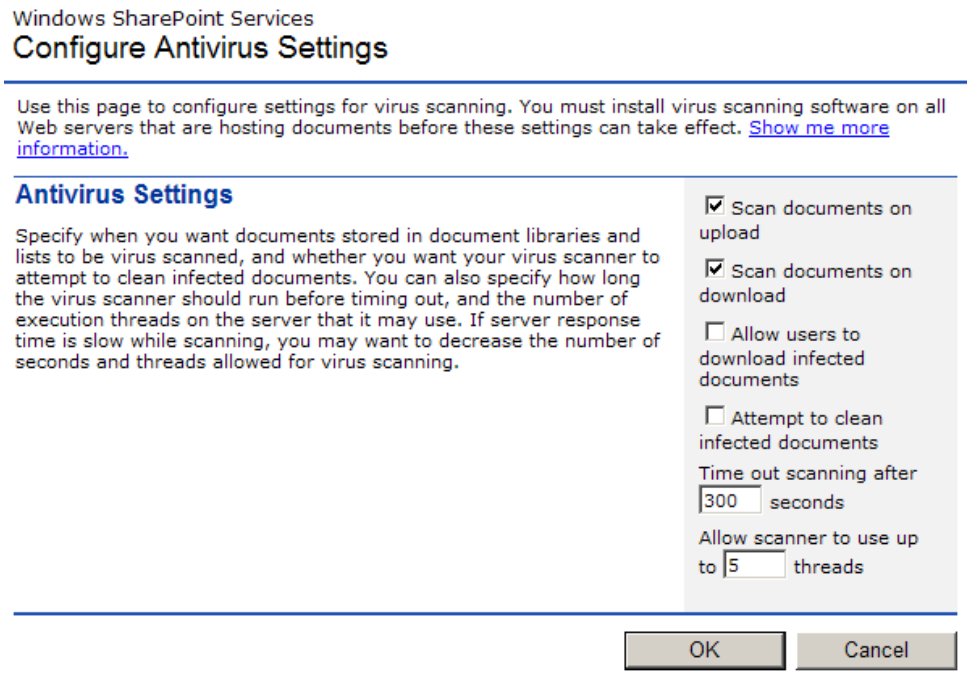
- ***Scan documents on upload*** – enable/disable the scanning of documents being uploaded
- ***Scan documents on download*** – enable/disable the scanning of documents being downloaded
- ***Allow users to download infected documents*** – allow/disallow users to download infected documents
- ***Attempt to clean infected documents*** – enable/disable automatic healing of infected documents (when possible)
- ***Time out duration*** (*in seconds*) – the maximum number of seconds the virus scanning process will run after single launch (decrease the value when the server's response seems to be slow when scanning the documents)
- ***Number of threads*** – you can specify the number of virus scanning threads that can run simultaneously; increasing the number may speed up the scanning due to the higher level of parallelism, but it can increase the server's response time on the other hand

5.3. AVG for SPPS Configuration - SharePoint 2003

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



The following window will then be displayed:



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

- ***Scan documents on upload*** – enable/disable the scanning of documents being uploaded
- ***Scan documents on download*** – enable/disable the scanning of documents being downloaded
- ***Allow users to download infected documents*** – allow/disallow users to download infected documents

- ***Attempt to clean infected documents*** – enable/disable automatic healing of infected documents (when possible)

- ***Time out scanning after ... seconds*** – the maximum number of seconds the virus scanning process will run after single launch (*decrease the value when the server's response seems to be slow when scanning the documents*)

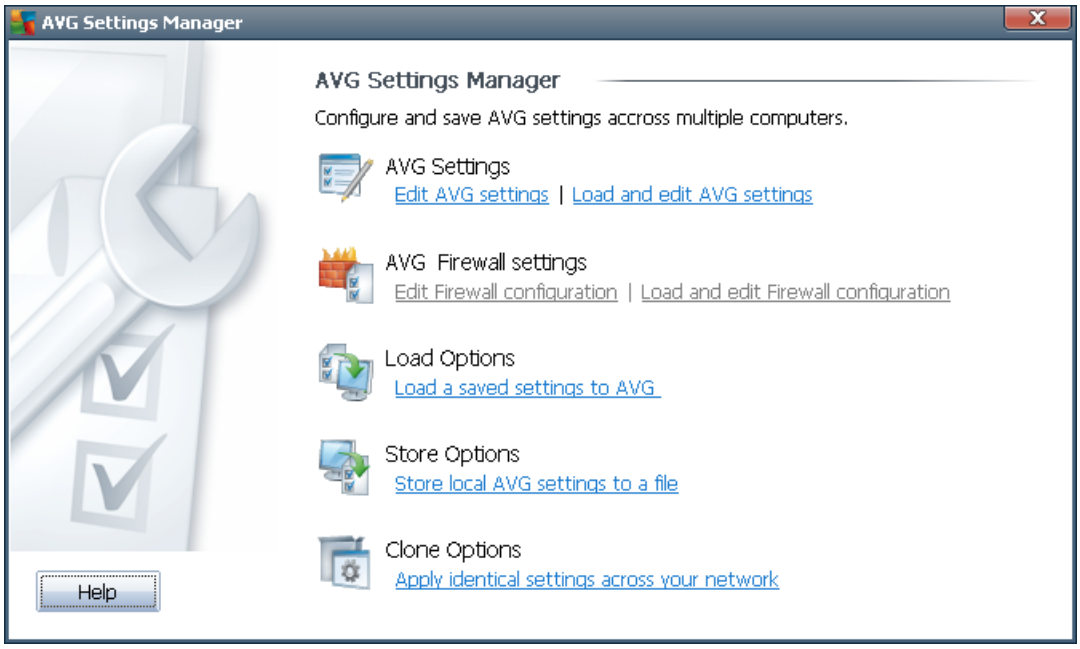
- ***Allow scanner to use up to ... threads*** – the value specifies the number of virus scanning threads that can run simultaneously; increasing the number may speed up the scanning due to the higher level of parallelism, but it can increase the server's response time on the other hand

6. AVG Settings Manager

The ***AVG Settings Manager*** is a tool suitable mainly for smaller networks that allows you to copy, edit and distribute AVG configuration. The configuration can be saved to a portable device (USB flash drive etc.) and then applied manually to chosen stations.

The tool is included in the installation of AVG and available via Windows Start menu:

All Programs/AVG 2012/AVG Settings Manager

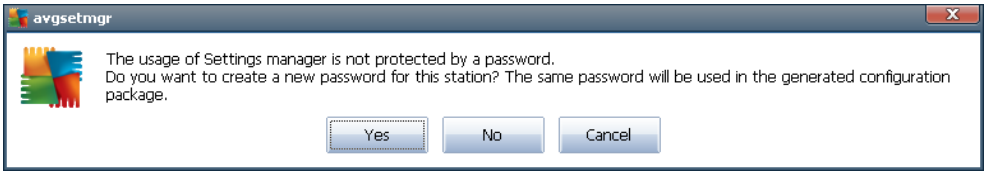


- **AVG Settings**
    - ***Edit AVG Settings*** - use this link to open dialog with advanced settings of your local AVG. All changes made here will be reflected also to the local AVG installation.
    - ***Load and edit AVG settings*** - if you already have an AVG configuration file (.pck), use this button to open it for editing. Once you confirm your changes by the ***OK*** or ***Apply*** button, the file will be replaced with the new settings!
- **AVG Firewall settings**

    This section would allow you to make changes to Firewall settings of your local AVG installation, or to edit Firewall settings in already prepared AVG configuration file (.pck). However, since your AVG File Server 2012 doesn't include the Firewall component, both links are grayed out and functionless.
- **Load Options**
    - ***Load a saved settings to AVG*** - use this link to open an AVG configuration file (.pck) and apply it to the local installation of AVG.

- **Store Options**

  - ***Store local AVG settings to a file*** - use this link to save the AVG configuration file (.pck) of the local AVG installation. If you did not set a password for the Allowed actions, you may experience the following dialog:



    Answer ***Yes*** if you wish to set the password for access to Allowed items now and then fill-in the required information and confirm your choice. Answer ***No*** to skip the password creation and continue to save the local AVG configuration to a file.

- **Clone Options**

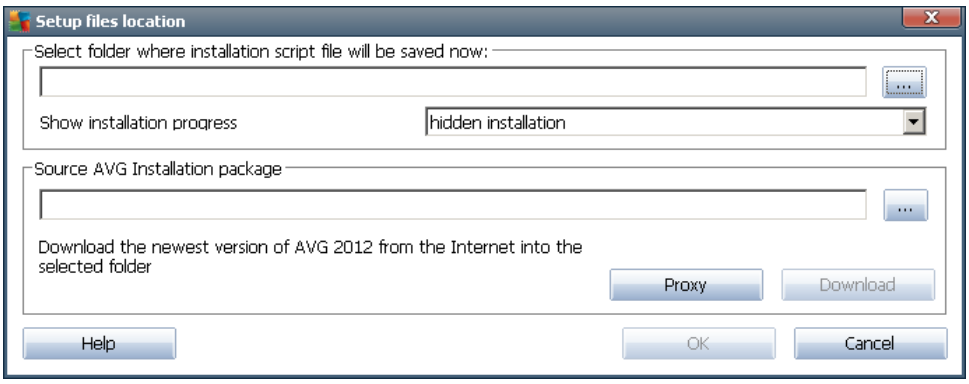
  - ***Apply identical settings across your network*** - clicking this link allows you to make a copy of the local AVG installation by creating an installation package with custom options. The clone includes most of the AVG settings with the exception of the following:

    ✓ *Language settings*

    ✓ *Sounds settings*

    ✓ *Allowed list and potentially unwanted programs exceptions of the Identity protection component.*

    To proceed first select folder where the installation script will be saved.



    Then from the drop-down menu select one of the following:

    ✓ *Hidden installation* - no information will be displayed during the setup process.

    ✓ *Show installation progress only* - the installation will not require any user attention, but the progress will be fully visible.

- ✓ *Show installation wizard* - the installation will be visible and user will need to manually confirm all steps.

Use either the ***Download*** button to download the latest available AVG installation package directly from the AVG website to the selected folder or manually put the AVG installation package into that folder.

You can use the ***Proxy*** button to define a proxy server settings if your network requires this for a successful connection.

By clicking ***OK*** the cloning process begins and should shortly finish. You may also experience a dialog asking about setting password to Allowed items (see above). Once finished, there should be ***AvgSetup.bat*** available in the chosen folder along with other files. If you run the ***AvgSetup.bat*** file, it will install AVG according to the parameters chosen above.

7. FAQ and Technical Support

Should you have any problems with your AVG, either business or technical, please refer to the ***FAQ*** section of the AVG website at http://www.avg.com.

If you do not succeed in finding help this way, contact the technical support department by email. Please use the contact form accessible from the system menu via ***Help / Get help online***.