

User Manual

 **AntiVir**[®]

SharePoint

Trademarks and Copyright

Trademarks

AntiVir is a registered trademark of Avira GmbH.

Windows is a registered trademark of the Microsoft Corporation in the United States and other countries.

Intel and Pentium are brand names or registered trademarks of the Intel Corporation or its subsidiaries in the United States and other countries.

All other brand and product names are trademarks or registered trademarks of their respective owners.

Protected trademarks are not marked as such in this manual. This does not mean, however that they may be used freely.

Copyright information

The purpose of this information is to acknowledge and recognize the code from third-party suppliers used for Avira AntiVir SharePoint. We would like to thank the copyright owners for allowing us to use their code.

MD5 Code

The MD5 code used for security reasons was written by the Information Science Institute of the University of Southern California and derived from the Message-Digest algorithm from RSA Data Security, Inc.

Copyright (C) 1991-2, RSA Data Security, Inc. Created in 1991.

All rights reserved.

The license to copy and use this software is distributed with the stipulation that it is designated as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all materials mentioned by this software or which refer to this software or these functions..

The license is also granted for the creation of works deriving from this, with the stipulation that these works are designated as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all materials which mention the derived work or refer to it.

RSA Data Security, Inc. provides no warranty whatsoever regarding the marketability of this software or the suitability of this software for a particular purpose. It is provided without any guarantee in its present form. This applies to expressed or implied guarantees.

This information must be contained in every copy of each part of this documentation and/or software.

Table of Contents

1	Introduction	4
2	Symbols and emphases	5
3	Product information.....	6
	3.1 Overview of functions.....	6
	3.2 Delivery scope.....	8
	3.3 System requirements.....	8
	3.4 Licensing	9
4	Installation and uninstallation	10
	4.1 Installation.....	10
	4.2 Uninstallation.....	11
5	User interface and operation	12
6	Virus detection.....	15
7	Updates.....	16
8	Info and Service	17
	8.1.1 Suspicious files	17
	8.1.2 False positive.....	17
9	Configuration options	18
	9.1 Configure AntiVir	18
	9.1.1 Scan.....	18
	9.1.2 Archives	19
	9.2 Configure update	20
	9.2.1 Network.....	20
	9.2.2 Proxy.....	21
	9.2.3 Email.....	21

1 Introduction

Avira AntiVir SharePoint protects SharePoint systems against viruses, malware, adware and spyware, unwanted programs and other dangers. The short form viruses and malware is used in this manual.



Note



The full name of the program is Avira AntiVir SharePoint. To improve legibility, this name is abbreviated to AntiVir SharePoint.

On our website <http://www.avira.de>, you can download the AntiVir SharePoint manual as a PDF, update Avira AntiVir SharePoint or renew your license.

On our website you can also find information such as the telephone number of Technical Support and our newsletter, which you can subscribe to there.

2 Symbols and emphases

The following symbols are used:

Symbol	Explanation
→	Is used in an instruction for navigation before a link that you follow.
✓	Is used before a condition that must be met before carrying out an action.
▶	Is used before an action step that you carry out.
→	Is used before an event that follows the preceding action.
	Is used before a note with very important information or before a tip that facilitates understanding and use of AntiVir for Sharepoint.
	Is used before a warning. Observe warnings to fully ensure the virus protection function of Antivir for SharePoint.

The following emphases are used:

Emphasis	Explanation
<i>Italic</i>	File name or path name.
	Elements of the software desktop that are displayed (e.g. window title, window area or option field).
Bold	Elements of the software desktop that are clicked on (e.g. menu item, index card or button).

3 Product information

3.1 Overview of functions

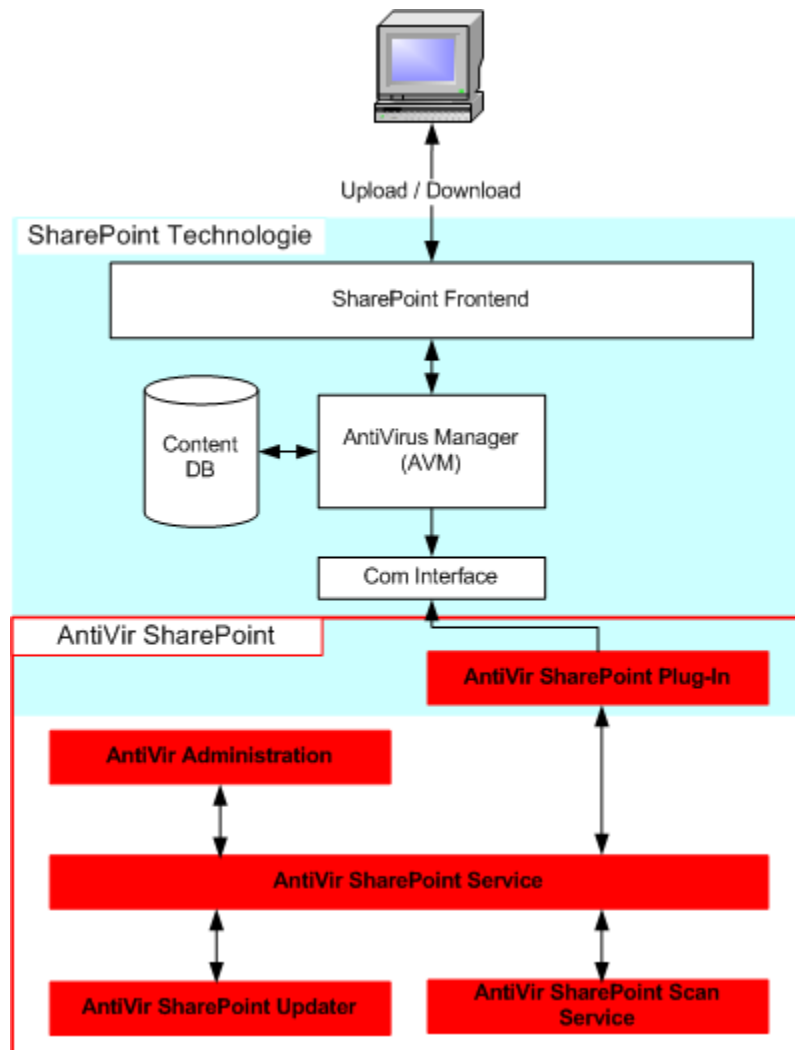
AntiVir SharePoint is an anti-virus solution specially developed for Microsoft SharePoint and supports the following SharePoint technologies.

- Microsoft Office SharePoint Server 2007
- Microsoft Windows SharePoint Services 3.0
- Microsoft Office SharePoint Portal Server 2003
- Microsoft Windows SharePoint Services 2.0

Microsoft SharePoint technologies make company documents available to users at a central point and manage these with a version control utility. Documents are accessed via a web desktop – the SharePoint Team pages - via upload and download. The documents or files are stored centrally in an MS SQL database. This represents a serious security problem, as the data cannot be protected against virus protection with a conventional anti-virus solution such as an on-demand or on-access virus scanner: on-demand and on-access virus scanners require the data to be scanned to be available as files in the file system.

According to the configuration, AntiVir SharePoint scans documents for viruses and malware when uploading and downloading to and from the SharePoint Team pages. In the event of a virus detection, transfer is prevented if a repair of the document is not possible.

Architecture:



In the SharePoint technologies, use of external anti-virus programs is controlled via the Antivirus Manager (AVM). Virus protection functions can be enabled in the SharePoint anti-virus settings. If the virus functions are enabled, AVM transfers the data requested for upload or download to an external anti-virus program.

AntiVir is integrated in the Sharepoint technologies via a plug-in. The AntiVir SharePoint plug-in processes requests for scanning for viruses by SharePoint and forwards these to the AntiVir SharePoint service. The AntiVir SharePoint service forwards requests for scanning to the AntiVir SharePoint scan service, starts the AntiVir update service and processes the AntiVir administration settings. AntiVir Administration is a snap-in of the Microsoft Management Console (MMC). The scan for viruses and malware is carried out by the AntiVir SharePoint scan service.

3.2 Delivery scope

AntiVir SharePoint offers comprehensive anti-virus protection for company data that you manage and provide with SharePoint technologies. AntiVir SharePoint offers comprehensive anti-virus protection for company data that you manage and provide with SharePoint technologies. In this way you also protect the computer systems used for SharePoint. AntiVir SharePoint is easy to install and has the following configuration possibilities:

Settings to scan for viruses and malware:

- OLE heuristic and Win32 file heuristic
- Archive scan

Settings for automatic update (update of the scanning engine and of the virus definition file):

- Update of webserver or fileserver possible
- Update via proxy server possible
- Email notification function

3.3 System requirements

Avira AntiVir SharePoint supports the SharePoint technologies:

- Microsoft Office SharePoint Server 2007
- Microsoft Windows SharePoint Services 3.0
- Microsoft Office SharePoint Portal Server 2003
- Microsoft Windows SharePoint Services 2.0

The following system requirements exist:

- Executable SharePoint technology: SharePoint Server 2007 or SharePoint Services 3.0 or SharePoint Portal Server 2003 or Windows SharePoint Services 2.0
- Server with processor speed of 2.5 gigahertz (GHz) or higher, 32-bit or 64-bit processor
- At least 1 GB RAM, 2 GB RAM recommended
- 130 MB of available hard disk drive space
- At least 100 MB temporary memory on the hard disk

3.4 Licensing

You require a license to use Avira AntiVir SharePoint. The license is available in the form of a digital license key, the file hbedv.key. You can obtain the license file by email from Avira GmbH. The license file contains the license for all products that you have ordered in an order process.

With the license file hbedv.key you can activate your license for Avira AntiVir SharePoint. During installation you are asked to download this license file. To extend your license to download the license after installation, save the license file to the installation directory.

4 Installation and uninstallation

4.1 Installation

Before installing AntiVir SharePoint, check the following conditions:

- ✓ Ensure that the system requirements are met (see System requirements).
- ✓ Ensure that you are logged in on the computer as an administrator or as a user with administrator rights.
- ✓ Ensure that an Internet connection or a network connection to a download server exists for updating AntiVir SharePoint. If you use a fileserver, you may require a user name and a password for serve login.
- ✓ Ensure that a valid license file hbedv.key exists and is stored in a local directory on the server.

How to install Avira AntiVir SharePoint:

- ▶ To start the installation program, double click on the installation file you downloaded from the Internet, or insert the program CD.
 - ↳ After a security message from the software publisher, the installation program dialog box appears.
- ▶ Click **Accept**.
- ▶ The setup program for Avira AntiVir SharePoint starts.

Follow the instructions of the installation assistant:
- ▶ Confirm stoppage of the WWW publishing service and continue the installation by clicking **Next**.
- ▶ Confirm that you accept the license agreements and click **Next**.
- ▶ Specify a user account or select the *Log in as local system user* option. Continue the installation by clicking **Next**.

When an update is performed, the AntiVir update module for the specified user account is started. If you wish to acquire the update directly from the internet, the specified user account must be authorized to use an internet connection (LAN or dial-up).
- ▶ Select the directory in which you saved the license file hbedv.key and confirm by clicking **Next**.
- ▶ Start the installation by clicking **Install**.
- ▶ Complete installation with **Finish**.

After installation, the anti-virus function of SharePoint AntiVirus Manager is enabled, AntiVir SharePoint is configured with default settings.



Note

Settings in SharePoint AntiVirus Manager can be modified in the SharePoint central administration under **SharePoint central administration :: Security configuration :: Configure anti-virus settings**.



Warning

Please note with regard to settings in the SharePoint central administration: In order for Avira AntiVir Sharepoint to check documents uploaded to the SharePoint Team pages or downloaded from the SharePoint Team pages, anti-virus protection must be enabled when uploading and downloading documents.



Note

You can modify the AntiVir SharePoint default settings in the AntiVir administration and define other settings: Configuration of update via a proxy server or fileserver, configuration of email notification function.

4.2 Uninstallation

Carry out uninstallation via the control panel of the operating systems:

- Under **Control panel :: Software** search for Avira AntiVir SharePoint and click on the option **Remove**.
- Confirm uninstallation.

During uninstallation the AntiVir services are stopped, all program and report files are deleted.

5 User interface and operation

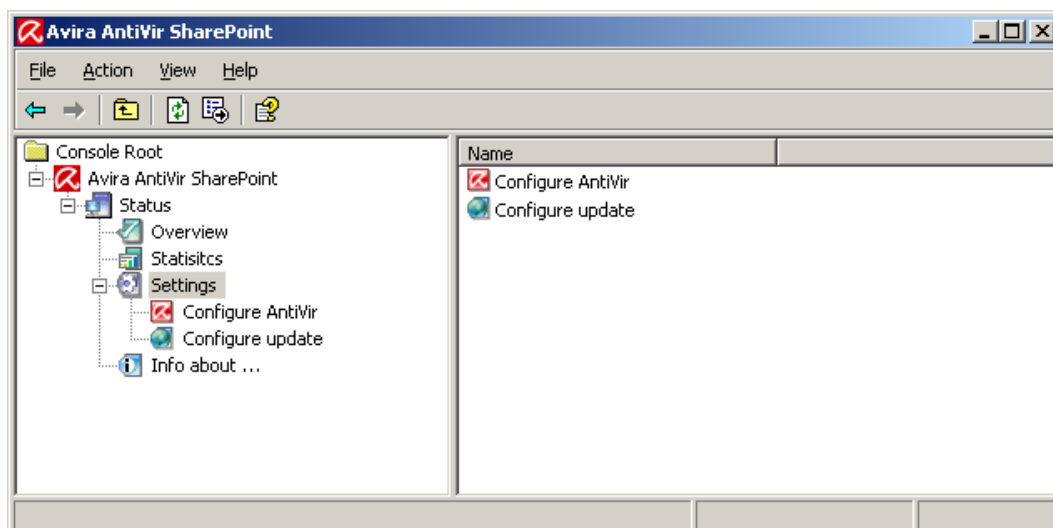
The virus protection function of Avira AntiVir SharePoint can be controlled, i.e. enabled or disabled, using the SharePoint AntiVirus Manager. You will find the settings for SharePoint AntiVirus Manager in the SharePoint central administration under **Security configuration :: Configure anti-virus settings**. After installation the anti-virus function is enabled by default.



Warning

Please note with regard to settings in the SharePoint central administration: In order for Avira AntiVir Sharepoint to check documents uploaded to the SharePoint Team pages or downloaded from the SharePoint Team pages, anti-virus protection must be enabled when uploading and downloading documents.

AntiVir SharePoint is configured via AntiVir Administration. AntiVir Administration is a snap-in of the Microsoft Management Console (MMC).



Note

Please note that only the proprietary elements of AntiVir Administration are documented in this Help Information on the MMC and the manual installation of a snap-in can be found in the operating system's user manual or Online Help.

Starting and ending AntiVir Administration

Start AntiVir Administration via the link under Programs::Avira::AntiVir SharePoint::Avira AntiVir SharePoint User Interface. You can also load AntiVir Administration directly into the MMC. The AntiVir console file can be found in the AntiVir SharePoint installation directory. To exit AntiVir Administration, you must close the MMC.

Operation

- Use the console structure in the left-hand window of the MMC to navigate. Navigation elements are also displayed as objects in the right-hand detail window. Double-click these objects in the detail window to open. The AntiVir SharePoint configuration can be accessed under the node **Settings**. You can select different configuration sections in the detail window: The *Configure AntiVir* window opens in which you can configure the appropriate section.
- Commands and actions can be accessed via links in the detail window.
- When configuring AntiVir SharePoint, you must click the **OK** button in the *Configure AntiVir* window to confirm your information and accept the new settings. Click on the **Cancel** button to discard your information.

Accessing the product version of AntiVir SharePoint

You can access the product version of AntiVir SharePoint in the MMC Help menu under **Info on Avira AntiVir SharePoint...**

Accessing Help

You can access Help via the Help icon in the MMC or by pressing F1.

AntiVir Administration overview

Avira AntiVir SharePoint

Status

- Display of status of AntiVir Administration connection to AntiVir SharePoint services
- Actions: **Connect server** when connection to AntiVir SharePoint services is interrupted

Overview

- Display of status of AntiVir SharePoint services: AntiVir SharePoint service and AntiVir SharePoint scan service
- Display of system status: Last update, VDF and search engine version
- Actions: Start update (VDF/search engine)

Statistics

- Display of statistical data from virus scan
- Actions: reset statistics

Settings

- **Configure AntiVir:** Heuristic and archive search options
- **Configure update:** Download methods (via webservice or fileserver), configuration of connection to download server, email notification function

Info on..

- Display of contact and support information
- Display of license information, licensee, serial number, validity

6 Virus detection

During upload or download of documents to or from SharePoint Team pages, AntiVir SharePoint scans these documents for viruses and malware. If AntiVir finds viruses or malware in a document, SharePoint is informed. The transfer of the document is prevented by SharePoint. The user of the SharePoint Team page receives a message:



Note

You can specify behavior in the event of a virus detection in the SharePoint central administration under **Security configuration :: Configure anti-virus settings**. In this way, for example, you can permit the download of infected files to allow users to scan infected documents on their own computer system for viruses and malware.



Warning

Please note with regard to settings in the SharePoint central administration: In order for Avira AntiVir Sharepoint to check documents uploaded to the SharePoint Team pages or downloaded from the SharePoint Team pages, anti-virus protection must be enabled when uploading and downloading documents.

7 Updates

The effectiveness of anti-virus software depends entirely on the status of the scanning engine and virus definitions. For this reason, regularly download updates for Avira AntiVir SharePoint from our download servers. To carry out regular updates, the AntiVir SharePoint updater service is integrated in AntiVir SharePoint. The update service updates the following program components:

- Virus definition file
- Scanning engine

Create update jobs to be performed at predefined intervals by the update service in AntiVir Administration under *Configure update*. For every update job, the virus definition file and the scanning engine are checked for their status and updated if necessary. You can start an update manually in AntiVir Administration under **Overview :: Last update**. After an update, AntiVir SharePoint does not have to be restarted.

You can obtain updates via the following servers:

- directly from the Internet via a webserver of Avira GmbH. The following update webservers are available:
dl.antivir.de
<http://dl1.pro.antivir.de>
<http://dl2.pro.antivir.de>
<http://dl3.pro.antivir.de>
<http://dl1.antivir.net>
<http://dl2.antivir.net>
<http://dl3.antivir.net>
- via a webserver or fileserver in the Intranet, which downloads the update files from the Internet and supplies them to other computers in the network. This is useful if you want to update AntiVir SharePoint on more than one computer in a network. This ensures that AntiVir SharePoint on the computer systems to be protected is up to date in a resource-saving way.

If a webserver is used, the download is carried out via HTTP protocol. If a file server is used, the update files are accessed via the network. Configure the update on the AntiVir Administration under the update configuration.



Note

You can use AntiVir Internet Update Manager (file- or webserver under Windows) or AntiVir Mirror Script (fileserver under Linux) as web- or fileserver in the Intranet. These programs mirror download servers of AntiVir products (e.g., AntiVir SharePoint) and are available in the Internet at <http://www.avira.com>. However, you can also update AntiVir SharePoint on the computer systems to be protected in the network by cascading via a central fileserver.

8 Info and Service

Information on our contact and support addresses can be found in AntiVir Administration under the node *Info on...* Please feel free to send us your ideas concerning product improvements. In particular in the case of undetected, suspicious files and false positives, you can contribute to optimising the virus protection of the AntiVir products.

8.1.1 Suspicious files

You can send viruses to us that may not yet be detected or removed by our products. We provide several ways of doing this.

- Send the requested file packed (WinZIP, PKZip, Arj etc.) in an email attachment to virus@avira.com. As some email gateways work with anti-virus software, you should also assign a password to the file(s) (please do not forget to inform us of the password).
- Alternatively, you can send the suspicious file to us via our website.

8.1.2 False positive

If you believe that AntiVir indicates detection in a file which is however very probably "clean", please send this file packed (WinZIP, PKZIP, Arj etc.) with reference to a false positive in an email attachment to virus@avira.com. As some email gateways work with anti-virus software, you should also assign a password to the file(s) (please do not forget to inform us of the password).

9 Configuration options

Configure Avira AntiVir Sharepoint in the AntiVir Administration under *Settings*. The following configuration options are available:

- **Configure AntiVir:** Heuristic and archive scan options
- **Configure update:** Download methods (via webservice or fileserver), configuration of connection to download server, email notification function

9.1 Configure AntiVir

You can configure the heuristic search and archive search under **Configure AntiVir**.

9.1.1 Scan

You can enable heuristic options under **Scan**. Avira AntiVir SharePoint contains very powerful heuristics that can detect even unknown (new) viruses, worms and trojans. This is done by analyzing the relevant code for functions typical of viruses, worms or trojans. If the scanned code fulfils these characteristic features, it is flagged as suspicious. This means that the code may or may not actually contain a virus, worm or trojan. False positives can occur.

OLE Heuristic

AntiVir contains a very powerful macro-virus heuristic. If this option is enabled, documents are scanned for unknown macro-viruses. In an affected document, all macro-viruses are deleted if repair is possible.

Win32 File heuristic

AntiVir contains a very powerful heuristic for Windows file viruses, worms and Trojans that can also detect unknown viruses, worms and Trojans. If this option is enabled, you can define here how "strict" this heuristic should be:

Low detection level

If this option is enabled, AntiVir detects fewer viruses, worms and Trojans, the risk of possible false positives is low here.

Medium detection level

This setting is enabled by default if you have selected application of this heuristic.

High detection level

If this option is enabled, AntiVir detects a very large number of unknown viruses, worms and Trojans, but you must also expect false positives.

9.1.2 Archives

You can configure the archive scan under **Archives**. As the archive scan may require more computer resources, you have further options to limit scanning in archives or to configure the behavior of the scan in archives.

Scan archives

If this option is enabled, archives are scanned. The archives are unpacked and scanned. The archive scan is enabled by default and is recommended.

Smart extensions

If this option is enabled, AntiVir SharePoint detects whether a file is a packed file format (archive), even if the file extension differs from usual extensions, and scans the archive. Each file must be opened to check the file formats. This slows down the scanning speed. This setting is enabled by default and is recommended.

Limit recursion depth

When scanning in archives, AntiVir SharePoint uses a recursive scan: archives in archives are unpacked and scanned for viruses and unwanted programs. Limit the recursion depth. Permitted values are 1 to 99. The default value for the recursion depth is 5 and is recommended. Example: the recursion depth is 2. All archives located directly in the main archive are unpacked and scanned.

Maximum compression rate [ratio]

You can prevent the transfer of deeply nested archives. Deeply nested archives, so-called 'archive bombs', are a popular method of concealing viruses and infiltrating systems. The transfer of archives that are more deeply nested than the specified value is prevented on the SharePoint Team pages. Permitted values are 1 to 300. The default value is 150 and is recommended.

Maximum size of archives to be scanned

Restrict the scan to a maximum size of archive to be unpacked. Permitted values are 1 to 600 MB. The default value is 300 MB and is recommended.

9.2 Configure update

Under **Configure update** you can define the network settings and if necessary proxy settings for updating AntiVir SharePoint. You can also configure an email message by SMTP.

9.2.1 Network

Configure the network settings for the AntiVir SharePoint update under **Network**. You can obtain updates via a webserver or via fileserver / share from the internet or intranet (see Ch. Updates).

Network settings

Update URL

Specify the URL or the IP address of the server from which you want to download the updates. You can specify more than one webserver, separated by commas. AntiVir SharePoint uses the first available webserver for the update:

```
http://dl1.pro.antivir.de, http://dl2.pro.antivir.de
```

If you want to obtain the updates from a fileserver via a share directory, specify the UNC path for the share directory:

```
\\<server>|<IP address>\<share>\<path>
```

Update interval in minutes

Specify an update interval in minutes. AntiVir SharePoint checks at the predefined intervals whether updates are available for AntiVir SharePoint on the specified update server, and where appropriate, starts the update process. The default setting is 120 minutes and is recommended.

Network access

If you are using a share directory on a fileserver for the update, specify the user name and password.

User name

Specify a user name for authentication.

Password

Specify a password for authentication.

9.2.2 Proxy

If you are using a webserver for the AntiVir SharePoint update, you can specify a proxy server to establish the connection to the webserver under **Proxy**

Proxy server

Connect via proxy server

If this option is enabled, AntiVir SharePoint connects to the webserver via a proxy server, which is used to update AntiVir SharePoint. This option is disabled as the default setting.

Address

Enter the URL or IP address of the proxy server via which AntiVir SharePoint is connected to the webserver.

Port

Enter the port number of the proxy server via which AntiVir SharePoint is to connect to the webserver.

User name

Enter your login name on the proxy server.

Password

Enter the relevant password to log in to the proxy server.

9.2.3 Email

You can define settings for email notification via SMTP under **Email**. You have the option of being notified by email of every update or only in the event of a defective update. The email message contains the following information:

- Computer name of AntiVir SharePoint
- Date and time of the update
- Status of the update

Email messages

Activate email notification

If this option is enabled, an email notification is sent either with every update or only in the event of a defective update. This option is disabled as the default setting.

Event selection

Select the event of which you wish to be notified when it occurs:

Notification when an update has failed

An email is only sent after a defective update.

Notification of every update

An email notification is sent after every update in which new files are installed or an error occurs. No email is sent if no new files are installed during the update process, as AntiVir SharePoint already has access to the current files.

Configuration options

SMTP server

Enter the name of the SMTP server you wish to use to send the notifications.

User name:

Specify a user name for authentication on the SMTP server.

Password

Specify a password for authentication on the SMTP server.

Sender address

Specify a name or an email address as the sender of the email notification.

Recipient address

Specify the email address of the recipient of the email notification. You can also specify more than one recipient address, separated by commas.

