



User Manual

Avira AntiVir Virus Scan Adapter for SAP NetWeaver[®]

SAP[®] Certified
Integration with SAP NetWeaver[®]

Contents

Chapter 1. About this Manual	5
1.1 Introduction	5
1.2 The Structure of the Manual	5
1.3 Signs and Symbols	6
Chapter 2. Product Information	7
2.1 Licensing Concept	8
2.2 Operating Mode of AntiVir VSA (Windows)	8
2.3 System Requirements	9
Chapter 3. Installation	11
3.1 AntiVir VSA Installation (UNIX)	11
3.1.1 Getting the Installation Files	11
3.1.2 Licensing	11
3.1.3 Installing AntiVir VSA	12
3.1.4 Reinstalling AntiVir VSA	14
3.1.5 Background	15
3.2 AntiVir VSA Installation (Windows)	15
3.2.1 Getting the Installation Files	15
3.2.2 Licensing	16
3.2.3 Installing AntiVir VSA	16
3.2.4 Background	18
Chapter 4. Configuration (UNIX)	19
4.1 Overview	19
4.2 Configuration Files	19
4.3 Configuration Script configantivir	23
4.4 Configuring Regular Updates	24
Chapter 5. Configuration (Windows)	29
5.1 Available Entries in SAVAPI.INI	29
5.2 Possible Entry in SAVAPIDL.INI	32
5.3 Immediate Updates	32
Chapter 6. ABAP-Specific Configuration	33
6.1 Setting the Virus Scan Interface	33
6.1.1 Defining Scanner Groups	33
6.1.2 Defining Virus Scan Servers	35
6.1.3 Defining Virus Scan Profiles	45
6.1.4 Implementing a BAfI for Virus Scanners	50
6.2 Problem Analysis for the Virus Scan Server	51
6.3 Testing the Installation of the Virus Scan Server	53
6.4 Commented Example Program	54
Chapter 7. Java-Specific Configuration	55
Chapter 8. Java-Specific Configuration for SAP NetWeaver 2004(s) and KMC	57
8.1 Configuration in the Visual Administrator	57
8.1.1 Define a Scanner Group	57
8.1.2 Define a Virus Scan Provider	60

8.1.3 Define a Virus Scan Profile	63
8.1.4 Check the Configuration	64
8.2 Integration with the Enterprise Portal and the Knowledge Management Center.....	66
Chapter 9. Operation	73
9.1 Reaction to Viruses/ Unwanted Programs Detected.....	73
Chapter 10. Service	74
10.1 Support	74
10.2 Contact.....	74
Chapter 11. Appendix	76
11.1 Glossary	76
11.2 Further Information	77
11.3 Golden Rules for Protection Against Viruses	78

1 About this Manual

In this Chapter you can find an overview of the structure and contents of this manual.

After a short introduction, you can read information about the following issues:

- [The Structure of the Manual](#) – Page 5
- [Signs and Symbols](#) – Page 6

1.1 Introduction

We have included in this manual all the information you need about AntiVir UNIX Server (for SAP Solutions) and it will guide you step by step through installation, configuration and operation of the software.



The full name of the program is Avira AntiVir Virus Scan Adapter (for SAP Solutions). For easier reading, we have shortened the name in this manual to AntiVir VSA.



The term "viruses" is used as a general reference to malware, such as worms, Trojans, hoaxes etc.

For further information and assistance, please refer to our website, to the Hotline of our Technical Support and to our regular Newsletter (see [Service](#) – Page 74).

Your Avira Team

1.2 The Structure of the Manual

The manual of your AntiVir software consists in a number of Chapters, bringing you the following information:

Chapter	Contents
1 About this Manual	The structure of the manual, signs and symbols.
2 Product Information	General information on AntiVir software, its modules, features, system requirements and licensing.
3 Installation	Instructions to install AntiVir UNIX Server on your system – using both the UNIX installation script and the graphical installation routine.
4 Configuration (UNIX)	Directions for optimum settings of AntiVir VSA on your UNIX system.
5 Configuration (Windows)	Directions for optimum settings of AntiVir VSA on your Windows system.
6 ABAP-Specific Configuration	Information on specific ABAP configuration of AntiVir VSA.
7 Java-Specific Configuration	Information on specific Java configuration of AntiVir VSA.

Chapter	Contents
8 Java-Specific Configuration for SAP NetWeaver 2004(s) and KMC	Virus Scan Configuration for Java systems in the Visual Administrator; Integration with the Enterprise Portal and the Knowledge Management Center
9 Operation	Reactions when viruses and unwanted programs are detected.
10 Service	Avira GmbH Support and Service.
11 Appendix	Glossary of technical terms and abbreviations, Golden Rules for Protection against Viruses.

1.3 Signs and Symbols

The manual uses the following signs and symbols:

Symbol	Meaning
✓	... shown before a condition that must be met prior to performing an action.
▶	... shown before a step you have to perform.
↳	... shown before the result that directly follows the preceding action.
	... shown before a warning if there is a danger of critical data loss or hardware damage.
	... shown before a note containing particularly important information, e.g. on the steps to be followed.
	... shown before a tip that makes it easier to understand and use AntiVir VSA.

For improved legibility and clear marking, the following types of emphasis are also used in the text:

Emphasis in text	Explanation
Ctrl+Alt	Key or key combination
<code>/usr/lib/AntiVir/antivir</code>	Path and file name
<code>ls usr/lib/AntiVir</code>	User entries
Choose component Select all	Elements of the software interface such as menu items, window titles and buttons in dialog windows
http://www.avira.com	URLs
Signs and Symbols – Page 4	Cross-reference within the document

2 Product Information

Avira AntiVir Virus Scan Adapter (for SAP Solutions) is the first and until now the only virus scanner for SAP business solutions certified by SAP. It is integrated into the SAP NetWeaver technology platform, monitors the data transfer of SAP applications via SAP Web Application Server and protects them against viruses and unwanted programs.

Using AntiVir VSA, for example, companies whose websites support online job applications and uploads of résumés in Word or PDF format can be certain that there is no malware in their databases. Files such as spreadsheets or pictures that have been processed by various employees can be scanned for malware before they are filed. It is therefore possible to file virus-free objects safely without leaving this important task to the antivirus software on the workstation.

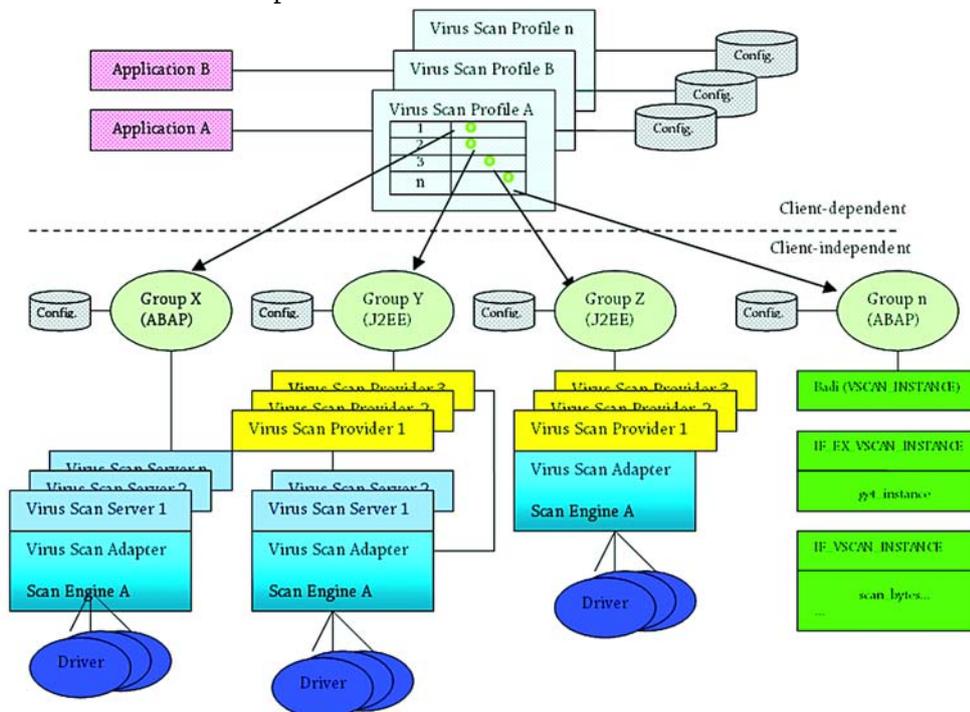
Automatic Internet updates keep the software permanently up to date.

You increase the security of your system by integrating AntiVir VSA into the SAP system with the Virus Scan Interface. In this way, you can scan files or documents processed by applications for viruses and unwanted programs using a high-performance integration solution. This applies both to applications supplied by SAP and to your own processes, for example data transfer via networks or the exchange of documents via interfaces.

The interface has two components:

- an external one, for certification of various antivirus products and
- an internal one, for integrating the virus scanner feature in the application via a Business Add-In.

The figure below shows an integrated ABAP-Java installation. You may also use the Virus Scan Interface on a simple ABAP or Java installation.



First, Application A accesses Group X via the Virus Scan Profile A, then Group Y and in the third step Group Z. Every group covers the antivirus software of a certain provider. Within Group X, a Virus Scan Server supplied by SAP is selected via load balance and access to the antivirus software is achieved via the certified Virus Scan Adapter of the external provider. This software scans the files provided by Application A for viruses.

Group Y has Virus Scan Providers with and without Virus Scan Server, which access the antivirus software via the certified Virus Scan Adapter of the external provider. The Virus Scan Provider in Group Z contains only the certified Virus Scan Adapter of the external provider, which ensures access to the antivirus software.

Alternatively you can implement your current virus scan solution via a Business Add-In (BAI). This is shown as Group n in the above figure and it is also accessed through a Virus Scan Profile.

2.1 Licensing Concept

You must have a license to use AntiVir VSA. You are required to accept the license terms (see http://www.avira.com/documents/general/pdf/en/avira_eula_en.pdf).

The license is contained in a license file named *hbedv.key*. You will receive it by email from Avira GmbH. It contains certain data such as the programs you will use and the period of your license. The same license file may refer to more than one AntiVir product.

The range of Full Version features includes:

- Provision of AntiVir Versions by Internet download
- License file by email
- Complete installation instructions (digital)
- PDF manuals available for Internet download
- Four weeks installation support, starting from acquisition date
- Newsletter service (by email)
- Internet update service for program files and VDF

2.2 Operating Mode of AntiVir VSA (Windows)

The security pack AntiVir VSA consists of 2 modules:

- AntiVir Savapi:
 - Savapi Service: it provides the actual scan and repairing features.
 - Savapi Update Service: ensures that AntiVir VSA is kept up to date via Internet connection. It checks for available updates and it performs the update if necessary.
- Avira AntiVir Virus Scan Adapter (VSA):
Interface for SAP, corresponding to the file *ANTIVIRVSA.DLL*.



You may save *ANTIVIRVSA.DLL* to another location, but you will have to specify the full path to the Adapter in the SAP interface to set the environment variable *VSA_LIB*

2.3 System Requirements

AntiVir VSA asks for the following minimum system requirements on your computer:

SAP

- SAP NetWeaver 6.40 with Support Package 7 or higher;
- ABAP Engine with SAP_BASIS 640 Support Package 11 or higher;
- J2EE Engine with Support Package 13 or higher;
- SAP NetWeaver 2004s (7.0).

UNIX

- Hardware: Pentium III 500 MHz;
- 256 MB RAM;
- 512 MB on hard disk;
- UNIX glibc-2.2.5 or higher.
- Officially supported distributions:
 - Red Hat Enterprise Linux 5 Server
 - Red Hat Enterprise Linux 4 Server
 - Novell SUSE Linux Enterprise Server 10 - 10.2
 - Novell SUSE Linux Enterprise Server 9
 - Debian GNU/Linux 4 (stable)
 - Ubuntu Server Edition 8

SOLARIS

- Hardware: UltraSparc Ili 650 MHz;
- 768 MB RAM;
- 512 MB on hard disk;
- Operating System: Sun Solaris (x86) 8, 9, 10.

Windows

- Hardware: Pentium III 500 MHz;
- 256 MB RAM;
- 20 MB on hard disk;
- Operating System:
 - Windows 2000 Professional, SP3 recommended,
 - Windows 2000 Server, SP3 recommended,
 - Windows 2000 Advanced Server, SP3 recommended,
 - Windows 2003 Server,
 - Windows Server 2008,
 - Windows XP Pro,
 - Windows Vista (32 Bit).
- Administrator rights for installation.



3 Installation

This Chapter describes AntiVir VSA installation for UNIX and Windows systems:

- [AntiVir VSA Installation \(UNIX\)](#) – Page 11
- [AntiVir VSA Installation \(Windows\)](#) – Page 15

3.1 AntiVir VSA Installation (UNIX)

You can find the current version of AntiVir VSA (UNIX) on the Internet or on the AntiVir CD-ROM.

AntiVir VSA is supplied as a packed archive.

You will be guided step by step through the installation procedure:

- [Getting the Installation Files](#) – Page 11
- [Licensing](#) – Page 11
- [Installing AntiVir VSA](#) – Page 12
- [Reinstalling AntiVir VSA](#) – Page 14

3.1.1 Getting the Installation Files

Downloading the Installation Files from the Internet

- ▶ Download the current version file from our website <http://www.avira.com> to your local computer. The file name is *antivir-vsa-prof-<version>.tar.gz*.
- ▶ Save the file in a */tmp* folder on the computer on which you want to run AntiVir VSA.

Getting the Installation Files from CD-ROM

- ▶ On the AntiVir CD-ROM open */en/products/unix/server*.
- ▶ Copy the file *antivir-vsa-prof-<version>.tar.gz* in a directory, for example in */tmp*.

Unpacking Program Files

- ▶ Go to the temporary directory:

```
cd /tmp
```
- ▶ Unpack the archive containing the AntiVir kit:

```
tar -xzvf antivir-vsa-prof-<version>.tar.gz
```


↳ *antivir-vsa-prof-<version>* will then appear in the temporary directory.

3.1.2 Licensing

You must have an AntiVir license in order to use the full product (see [Licensing Concept](#) – Page 8). The license is contained in a file named *hbedv.key*.

This license file contains information regarding the scope and period of the license. Without the license file, AntiVir VSA does not run (not even with restricted features).

Purchasing the License

- ▶ You may contact us by telephone or by email (sales@avira.com) to acquire a license file for AntiVir VSA.
 - ↳ You will receive the license file by email.

Copying the License File

- ▶ Copy the license file *hbedv.key* to the installation directory on your system */tmp/antivir-vsa-prof-<version>*.



You can also perform the installation without having a license key from the beginning. You will then have to copy the license file into the AntiVir program directory */usr/lib/AntiVir*. Without a license, AntiVir will not run.

3.1.3 Installing AntiVir VSA

AntiVir VSA is automatically installed using a script. This script performs the following tasks:

- Checks integrity of the installation files.
- Checks for the required authorizations for the installation.
- Checks for an existing version of AntiVir on the computer.
- Copies the program files. Overwrites existing obsolete files.
- Copies AntiVir configuration files. Existing AntiVir configuration files are inherited.
- Optionally it installs AntiVir Update Daemon.
- Optionally it configures an automatic start for AntiVir Updater on system start-up.

Preparing Installation

- ▶ Login as root. Otherwise you do not have the required authorization for installation and the script returns an error message.
- ▶ Go to the directory in which you unpacked AntiVir:

```
cd /tmp/antivir-vsa-prof-<version>
```

Installing AntiVir VSA

- ▶ Type:

```
./install
```

Please note the dot and slash in the command syntax. Typing the command without this path specification, triggers another command, which is not related to AntiVir installation process and this would result in error messages and unwanted actions. Press q to close the license text view.

-
- ↳ The installation script starts and copies the program files, after you accept the license terms. Optionally, the Installer can read an existing license key:

```
Do you agree to the license terms? [n] y
creating /usr/lib/AntiVir ... done
1) installing AntiVir Engine
copying bin/antivir to /usr/lib/AntiVir/ ... done
copying vdf/antivir0.vdf to /usr/lib/AntiVir/ ... done
copying vdf/antivir1.vdf to /usr/lib/AntiVir/ ... done
copying vdf/antivir2.vdf to /usr/lib/AntiVir/ ... done
copying vdf/antivir3.vdf to /usr/lib/AntiVir/ ... done

Enter the path to your key file: [hbedv.key]
copying hbedv.key to /usr/lib/AntiVir/hbedv.key ... done
copying script/configantivir to /usr/lib/AntiVir/ ... done
linking /usr/bin/antivir to /usr/lib/AntiVir/antivir ... done
installation of AntiVir Engine complete
```

- ↳ Then you are asked if you want to install the Internet Update Daemon:

```
2) installing internet update daemon
An internet update daemon is available ...

Would you like to install the internet update daemon? [n]
```



You do not necessarily need the Internet Update Daemon to keep AntiVir up to date. You can perform this operation manually via the Internet. However, for the initial installation it is recommended to install the Update Daemon. You can deactivate it later in the configuration settings.

Installation
with Update
Daemon

If you choose to install the Internet Update Daemon (recommended):

- ▶ Type Y and confirm with Enter.

- ↳ The Internet Update Daemon is installed. Then you are asked if the daemon should start automatically:

```
Would you like to install the internet update daemon? [n] y
copying script/rc.avupdater.SuSE8x to /usr/lib/AntiVir/avupdater ... done
checking for existing /etc/avupdater.conf ... not found
copying etc/avupdater.conf to /etc/ ... done

Would you like the internet update daemon to start automatically? [y]
```

- ▶ Type Y and confirm with Enter. You can later change this setting manually.

- ↳ The automatic system start is configured:

```
Would you like the internet update daemon to start automatically? [y] y
setting up startup script ... done
installation of the internet update daemon complete
```

Installation
without Update
Daemon

If you choose not to install the Internet Update Daemon, or to do this later manually:

- ▶ Type N or press Enter.

Installation of
VSA library

↳ The next step installs VSA library:

```
3) installing VSA library
copying lib/libantivirvsa.so.1.1.0 to /usr/lib/AntiVir/ ... done
linking libantivirvsa.so to libantivirvsa.so.1.1.0 ... done
installation of VSA library complete
checking for existing /etc/avsapvsa.conf ... not found
copying etc/avsapvsa.conf to /etc/ ... done
```

Starting
configuration

↳ Afterwards, you can configure AntiVir:

```
4) configuring AntiVir Updater

Your connection to the internet might require special configuration
settings (such as HTTP proxy settings). You may also want the
updater to log to specific files or send email notification. You
now have the opportunity to set these options.

Would you like to configure the AntiVir updater now? [y]
```



If you answer Y, the configuration script for AntiVir Updater starts. You can make the configuration at any time later. We recommend that you first learn about the configuration options and then perform it.

► End this procedure by answering N.

↳ You will see a report that indicates the completion of the installation:

```
Installation of the following features complete:
AntiVir Engine
AntiVir Internet Update Daemon
AntiVir VSA
```

↳ Finally, the Installer displays information about the update procedure:

```
Note: It is highly recommended that you perform an update now to
ensure up-to-date protection. This can be done by running:

antivir --update

Be sure to read the README file for additional information.
Thank you for your interest in AntiVir VSA.
```

3.1.4 Reinstalling AntiVir VSA

You can always launch the installation script. There are various possible situations:

- Installation of a new version (upgrade). The installation script checks the previous version and installs the necessary new components. The configuration file settings already made are not overwritten (see [Configuration \(UNIX\)](#) – Page 19), but inherited.
- Later installation of some components, e.g. Internet Update Daemon.
- Activation or deactivation of the automatic start of the Internet Update Daemon.

Reinstalling AntiVir VSA

The procedure applies to all these cases:

- ▶ Open the temporary directory where you unpacked AntiVir VSA:
`cd /tmp/antivir-vsa-prof-<version>`
- ▶ Type:
`./install`
 - ↳ The installation script runs more or less as described in [Installing AntiVir VSA – Page 12](#).
- ▶ Make the changes you need during installation procedure.
 - ↳ AntiVir VSA is installed with the required features.

3.1.5 Background

During the installation, please note the following:

- AntiVir VSA Library is copied.
- The administrator can set the environment variable `VSA_LIB` (see system documentation). Otherwise you have to provide the full path in SAP setup:
`/usr/lib/AntiVir/libantivirvsa.so.<version>`
- The administrator has to integrate the SAPCAR tool in `/etc/avsapvsa.conf` (see the given example); without this entry, AntiVir does not scan SAPCAR archives:
`SapCarProgram /usr/bin/SAPCAR`

3.2 AntiVir VSA Installation (Windows)

3.2.1 Getting the Installation Files

Downloading the Installation Files from the Internet

You can find the current program files for AntiVir VSA on our website. They are packed:

- in *ZIP* format (you need a program to unpack it, for example WinZip) or
- in *EXE* format as a self-extracting archive (no unpacking program needed).
- ▶ Download the current version file from our website <http://www.avira.com> to your local computer. The file name is *antivir_vsa_en.exe*.

Getting the Installation Files from CD-ROM

- ▶ On the AntiVir CD-ROM open
`/en/products/vsa/windows`
- ▶ Save the file to the computer on which you want to run AntiVir VSA. The file is currently named *antivir_vsa_en.exe*.

3.2.2 Licensing

You must have an AntiVir license in order to use AntiVir VSA (see [Licensing Concept](#) – Page 8). This license file contains information regarding the scope and period of the license.

Purchasing the License

- ▶ You may contact us by telephone or by email (sales@avira.com) to acquire a license file for AntiVir VSA.
 - ↳ You will receive the license file by email.

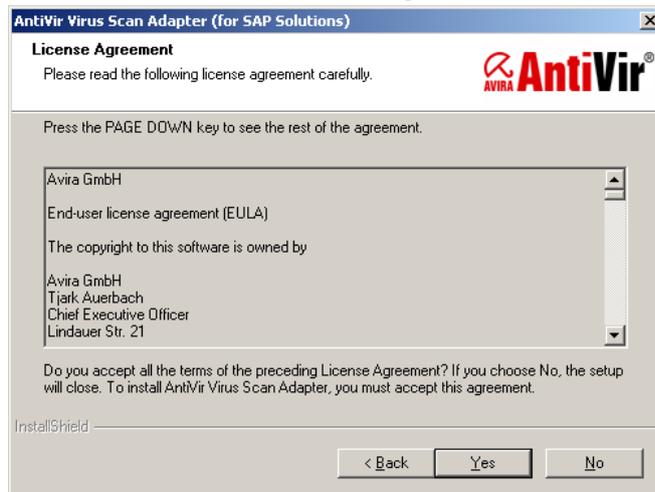
3.2.3 Installing AntiVir VSA

- Requirements
- ▶ Please check the following requirements in order for the software to perform efficiently:
 - ✓ Make sure the [System Requirements](#) are met.
 - ✓ Log in as administrator or as user with administrator rights.
 - ✓ Make sure the Internet connection is available and it allows automatic Updates with the Internet Updater.
 - ✓ Be sure to have the *hbedv.key* license file at hand.
 - ▶ Open the folder containing the downloaded program file *antivir_vsa_en.exe*.
 - ▶ Double-click the file *antivir_vsa_en.exe*.
 - ↳ The setup starts in a dialog window.
 - ▶ Click **Setup**.
 - ↳ AntiVir VSA setup starts.
 - ↳ The welcome window of the Install Shield Wizard appears:



- ▶ Click **Next**.

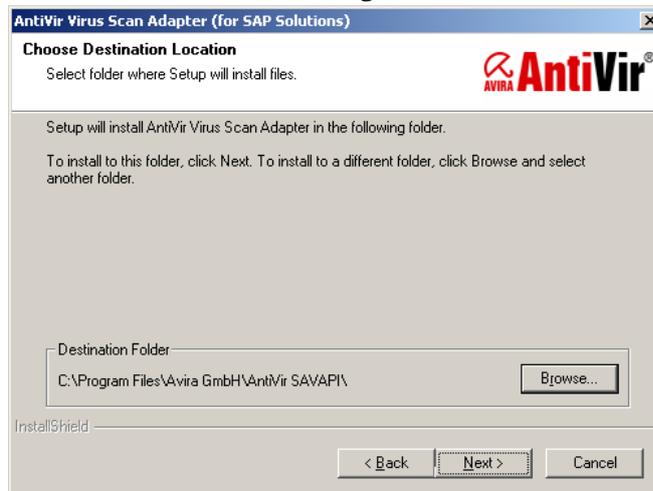
↳ You can read the **License agreement**:



You must agree to these conditions in order to continue the installation.

▶ Confirm with **Yes**.

↳ The window for selecting the **Destination folder** appears:

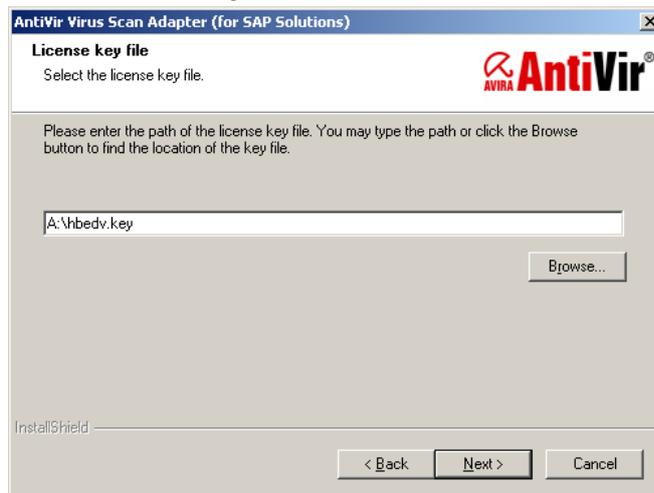


▶ Confirm with **Next** if the path is correct

– OR –

Click **Browse** and select the path, then click **Next**.

↳ The **License file** window follows:



- ▶ Select the folder containing the *hbedv.key* license file and click **Next**.
 - ↳ Then you will see **Install Shield Wizard completed**.
- ▶ Click **Finish**.
 - ↳ The setup program imports and installs the necessary files in the target folder.
 - ↳ AntiVir VSA installation is completed. You do not need to restart your computer.

3.2.4 Background

During installation, the following actions have been performed in the background:

- Copying of the Virus Scan Adapter (VSA) file ANTIVIRVSA.DLL to the installation folder.
- Setting of the environment variable VSA_LIB in the absolute path for VSA; for example:
`VSA_LIB=C:\Program Files\Avira GmbH\AntiVir Savapi\ANTIVIRVSA.DLL`
- Searching for the tool to unpack SAP archives (SAPCAR format); searching for the environment variable PATH of *SAPCAR.EXE* file.
- Adding a parameter in SAVAPI.INI which activates SAPCAR archive scanning; for example:

`SapCarProgram= (empty -> SAPCAR.EXE not found)`

- OR -

`SapCarProgram=C:\SAPCAR\SAPCAR.EXE (program found)`

4 Configuration (UNIX)

You can adjust AntiVir VSA for optimum performance. You can make the most important adjustments immediately after installation. The most common settings are suggested.

You can modify these settings at any time to adapt the product to your requirements.

After a short overview, you will be guided step by step through the configuration process:

- Information on the configuration files:
 - [Parameters in the Configuration File avsapvsa.conf](#) – Page 20 and
 - [Parameters in the Configuration File avupdater.conf](#) – Page 21.If you wish to use the configuration script, you can skip this Section.
- The procedure for using the configuration script: [Configuration Script configantivir](#) – Page 23.
- Specific configuration for AntiVir VSA:
 - [Configuring Regular Updates](#) – Page 24.

4.1 Overview

Configuration files The configuration file *avupdater.conf* defines automatic software updates; the file *avsapvsa.conf* defines the scanning parameters and logging rules when viruses or unwanted programs are detected.



You can make these settings directly in the configuration files. This is not very difficult.

A more convenient way is to use the configuration script included in the program. It intercepts possible errors and restarts the necessary processes.

Configuration script You can use the script *configantivir*, located in */usr/lib/AntiVir*, to edit the settings in *avupdater.conf* (Updater settings).

4.2 Configuration Files

This section describes the structure of AntiVir VSA configuration files *avsapvsa.conf* and *avupdater.conf*. AntiVir reads these files on program start-up. It ignores empty lines and commented lines beginning with #.

The program is provided with default values which are important for many procedures. Some options can be deactivated with a # at the beginning of the line (commented). These can be activated by removing the # character or by changing the values.



You must restart the Internet Update Daemon if you modify any values manually in *avupdater.conf*, without using the configuration script. The changes will only take effect after a restart.

► Type:

```
/usr/lib/AntiVir/avupdater restart
```

Parameters in the Configuration File *avsapvsa.conf*

This section provides a short description of the settings in *avsapvsa.conf*. These settings affect the scanner's behavior.

You can edit most of these parameters using the SAP GUI. SAP NetWeaver applies them to the scanner, via the VSA. When inserting such a parameter in the file *avsapvsa.conf*, the scanner starts with the specified value, but the values in SAP GUI will immediately override it. This means that the settings made in SAP GUI for the AV scanner have a higher priority than those made in the configuration file *avsapvsa.conf*.

- ArchiveScan Scanning archives:
When this option is active (value 1), all archived files are extracted and scanned. The zero value deactivates this option (not recommended).
ArchiveScan 1
- ArchiveMax
Size Maximum unpacked size of archived files:
If the setting is 0, all archived files are unpacked, whatever their size.
If the set value is >0, all archives that do not exceed the given value (in bytes) are unpacked and scanned.
ArchiveMaxSize 1GB
- ArchiveMax
Recursion Maximum archive recursion:
If the setting is 0, recursive (nested) archives are unpacked, whatever their recursion depth.
If the set value is >0, all archives that do not exceed the given recursion depth are unpacked. This saves processing time.
ArchiveMaxRecursion 20
- ArchiveMax
Ratio Blocking "mail bombs":
Blocks so-called "mail bombs" with a very high compression ratio. You can set the maximum difference between packed and unpacked file size.
The zero value deactivates this option (not recommended). The default is 150.
ArchiveMaxRatio 150
- LogFile Logfile:
AntiVir logs all important operations via the *syslog* daemon. It can also create an additional logfile. There is no default setting. You must enter the full path to the logfile in order to use this option:
LogFile /var/log/avsapvsa.log
- EmailTo Email messages:
AntiVir can send emails, when detecting viruses or unwanted programs. There is no default setting. You must specify a recipient in order to send emails:
EmailTo root@localhost
- Syslog... Syslog settings:
AntiVir sends messages for all important operations to the *syslog* daemon. You may specify the facility and priority for these messages. The default setting is:
SyslogFacility user
SyslogPriority notice

Detect...	<p>Detection of other types of unwanted programs: Besides viruses, there are some other types of harmful or unwanted software, described in <i>avsapvsa.conf</i>. You can activate their detection using the following options:</p> <p>DetectADSPY yes DetectAPPL yes DetectBDC yes DetectDIAL yes DetectGAME no DetectHEUR-DBLEXT yes DetectJOKE no DetectPCK no DetectPHISH yes DetectSPR no</p>
Heuristics Macro	<p>Macrovirus Heuristics: Activates the heuristics for macroviruses in office documents.</p> <p>HeuristicsMacro yes</p>
Heuristics Level	<p>Win32-Heuristics: Sets the detection level of Win32-Heuristics. Available values are 0 (off), 1 (low), 2 (medium) and 3 (high).</p> <p>HeuristicsLevel 0</p>
SapCarProgram	<p>Support for CAR/SAR Archives: Avira AntiVir Virus Scan Adapter includes native support for the most popular archive types, such as ZIP, CAB, TAR, etc. You can also scan archives with SAP-specific extensions CAR/SAR, if you use an external "sapcar" tool. Write the full path to the binary of this tool. There is no default path.</p> <p>SapCarProgram /usr/local/bin/SAPCAR</p>

Parameters in the Configuration File *avupdater.conf*

This section provides a short description of the settings in *avupdater.conf*. These settings apply to AntiVir Updater.

You can conveniently edit this file using [Configuration Script configantivir](#) – Page 23, which also restarts the affected processes, if necessary.

AutoUpdate...	<p>Update scheduler: The security software can check regularly for updates online using the Internet Update Daemon and, if available, it performs the update. By default, the possible options are deactivated; the program therefore does not start automatic updates. In order to keep AntiVir up to date, please set the appropriate HTTP proxy parameters and use one of the two methods to run the updates: set an update schedule and start the Internet Update Daemon; or create an update job using cron daemon.</p> <p>For updates every 2 hours, you must activate the following option: AutoUpdateEvery2Hours</p> <p>For daily updates, activate the option below: AutoUpdateDaily</p> <p>In the case of daily updates, you may also set the time for this action in HH:MM format: AutoUpdateTime 04:23</p>
---------------	--

EmailTo	<p>Email messages:</p> <p>AntiVir can send email notifications with details regarding the performed updates. There is no default setting. You must specify a recipient in order to send emails:</p> <pre>EmailTo root@localhost</pre>
LogTo	<p>Logfile:</p> <p>AntiVir logs all important operations via the <i>syslog</i> daemon. It can also create an additional logfile. There is no default setting. You must enter the full path to the logfile in order to use this option:</p> <pre>LogTo /var/log/avupdater.log</pre>
HTTPProxy...	<p>Proxy server:</p> <p>If your computer is connected to the Internet via an HTTP proxy server, you must specify this, so that the automatic Internet Updater functions properly. By default, the settings are deactivated; a direct connection to the Internet is assumed. You must specify:</p> <ul style="list-style-type: none"> • HTTP proxy server • Port • Username and password for the HTTP proxy server if necessary. <p>Example:</p> <pre>HTTPProxyServer proxy.domain.com HTTPProxyPort 8080 HTTPProxyUsername username HTTPProxyPassword password</pre>
Updater Keeps Backups	<p>The Internet Updater replaces installed files with newer versions when updates are available. Even if the program is testing the new files, you might want to keep backups of earlier versions.</p> <p>When activating this option, your existing files will be moved to the newly created subdirectories of <i>/usr/lib/AntiVir</i>, named <i>updater-backup-YYYYmmd-HHMMSS</i>.</p> <hr/> <div style="display: flex; align-items: center;">  <p>If you activate the backup function of the Internet Updater, you should check this directory regularly and manually delete old versions as the size increases.</p> </div> <hr/> <pre>UpdaterKeepsBackups</pre>
GnuPG...	<p>GnuPG settings:</p> <p>The Updater can check the updates for authenticity using GnuPG. For more information, see Verifying Updates Authenticity with GnuPG – Page 28. If you use GnuPG, you have to enter the path to GnuPG executable, for example:</p> <pre>GnuPGBinary /usr/local/bin/gpg</pre> <p>You can also add other options using <code>GnuPGOptions</code>, depending on the specific GnuPG installation. This is usually not necessary. Both settings are deactivated by default.</p>
Syslog...	<p>Syslog settings:</p> <p>AntiVir sends messages for all important operations to the <i>syslog</i> daemon. You may specify the facility and priority for these messages. The default setting is:</p> <pre>SyslogFacility user SyslogPriority notice</pre> <p>These values apply even if the option is not active.</p>

4.3 Configuration Script configantivir

You can conveniently configure AntiVir Internet Updater using the configuration script *configantivir*, which is able to intercept possible invalid entries and restart the necessary processes.

The script for configuring AntiVir Updater edits the parameters in *avupdater.conf*.

The procedure for using the script is very easy:

- ▶ Type:

```
/usr/lib/AntiVir/configantivir
```

The script reads the current settings in *avupdater.conf* and systematically asks if you want to enter new values. It displays all possible parameter values, while the current ones are shown as default.

If you want to keep one of the current settings:

- ▶ Press Enter.

If you want to change a setting:

- ▶ Type the new value and confirm with Enter.

↳ Finally, a summary of the configuration settings is displayed. For example:

```
AntiVir Configuration
=====
Here are the configuration settings you have specified. Look them over
to make sure they are correct.

email notification:    no
specific logfile:     /var/log/avupdater.log
update frequency:    every 2 hours (if update daemon is running)
http proxy server:    none

available options: y n
Save configuration settings? [y]
```

If you do not agree with all displayed options:

- ▶ Type N to restart the configuration script and correct the values.

If all settings correspond to the configuration you require:

- ▶ Confirm with Y or Enter to save the configuration file with the new values.

↳ The script informs you about saving the configuration file. It displays details about running the Internet Update Daemon:

```
* SUCCESS *

Configuration successfully saved to.
/etc/avupdater.conf

Press <ENTER> to continue.

Running Internet Update Daemon
=====
In order for the Internet Update Daemon to be active ...

available options: y n

Would you like to apply the new configuration? [y]
```

- ▶ Confirm with Y or Enter, to start the Update Daemon.
 - ↳ The Internet Update Daemon starts. If already running, it will automatically restart in order to apply the new settings. Then the configuration is complete.

```
Starting AntiVir: avupdater
...
AntiVir Status: avupdater running      [ running ]
Here are some commands that you should remember...

configure updater: /usr/lib/AntiVir/configantivir
start update daemon: /usr/lib/AntiVir/avupdater start
stop update daemon: /usr/lib/AntiVir/avupdater stop
update daemon status: /usr/lib/AntiVir/avupdater status
```

4.4 Configuring Regular Updates

The performance and effectiveness of an antivirus software depends on its being up to date. This is why AntiVir offers the possibility to download current updates via HTTP from the AntiVir webservers and even to schedule them automatically at regular intervals.

These updates ensure that AntiVir components, which provide security against viruses and unwanted programs, are always kept up to date.

There are two methods to configure AntiVir updates:

- You can use the Internet Update Daemon provided with AntiVir, which is easy to configure. This is recommended if you have little UNIX knowledge and if you only want to make small adjustments.
- You may use AntiVir with cron daemon. This is recommended if you have extensive UNIX knowledge. You have to carry out the configuration yourself, but it gives you more flexibility.

Configuring the Internet Connection for Updates

- ✓ Check that your Internet connection is functioning correctly. In most cases, the connection is already configured. If not, refer to your UNIX documentation for the information you need.

Proxy server If your AntiVir VSA computer is connected to the Internet via HTTP proxy server, you must make the necessary settings for AntiVir:

- ▶ Run *configantivir*:
/usr/lib/AntiVir/configantivir
- ▶ Confirm all settings with Enter until you reach the proxy server option:

```
HTTPProxyServer/HTTPProxyPort      (4 of 4)
=====
If this machine is sitting behind an HTTP proxy server, you will need to configure
AntiVir with the appropriate proxy settings. Internet access is required in order to
make updates.

available options: y n

Does this machine use an HTTP proxy server? [n]
```

- ▶ Type Y.
- ▶ You are then asked for the name and the port of the proxy server:

```
What is the HTTP proxy server name? []
```

- ▶ Type its name (example):
proxy.domain.com
- ▶ Then you are asked for the port of the proxy server. Type in the data:

```
What is the HTTP proxy server name? [] proxy.domain.tld
Which port number does the HTTP proxy server use? [] 3128
```

- ↳ You are then asked if you need a username and password for the proxy server:

```
HTTPProxyUsername/HTTPProxyPassword          (4-2 of 4)
=====
Proxy servers may be configured to require a username and password. If
the HTTP proxy server for this machine requires a username and password
AntiVir needs to be appropriately configured.

available options: y n
Does the HTTP proxy server require a username/password? [n]
```

If this is the case:

- ▶ Type Y.
 - ↳ Then you are asked for the username and password.
- ▶ Enter the username and password.
 - ↳ The configuration script displays the configuration summary and asks for confirmation, to write the configuration file.

The Internet update connection is now configured.

Configuring Automatic Updates via Internet Update Daemon

The Internet Update Daemon is a very simple service which performs the following command at fixed intervals:

```
antivir --update
```



To enable the following settings, you must first install the Internet Update Daemon, i.e. if you have installed AntiVir VSA with Update Daemon as described in [Installing AntiVir VSA](#) – Page 12. Otherwise you have to run the installation script again, see [Reinstalling AntiVir VSA](#) – Page 14.

You can define the following settings:

- Update intervals. It is possible to:
 - update every two hours
 - update daily
- Time settings for updates (for daily updates). You can:
 - set the time yourself
 - let the daemon choose a random time. The script chooses the time once and keeps it as the update time. In this case, the computer has to be online at the set hour.
- ▶ Run *configantivir*:

/usr/lib/AntiVir/configantivir

↳ Confirm every setting with Enter, until you reach the question about update frequency:

```
AutoUpdateEvery2Hours/AutoUpdateDaily          (3 of 4)
=====
AntiVir is equipped with an Internet Update Daemon. At specified
intervals, AntiVir will connect to an update server to check for newer
versions of the AntiVir engine or the data files. If a newer
version is available, AntiVir will automatically download and install
the updates without requiring any special attention. This allows AntiVir
to be kept current against attacks and problems.

AntiVir can be configured to check for updates every 2 hours (2) or
once a day (d). You can also choose to disable the Internet Update
Daemon (n).

Note: Updates can also be done manually from the command line:
    antivir --update
You may prefer to disable the Internet Update Daemon and
instead perform regular updates using a cron(8) job.

Using the startup script for the Internet Update Daemon when
it is disabled will result in an error.

available options: 2 d n
How often should AntiVir check for updates? [2]
```

▶ Type:

- n, if you do not want to perform automatic updates
- 2 for updates every two hours
- d for daily updates

↳ If you select daily updates, you have to set the time:

```
AutoUpdateTime                                  (3-2 of 4)
=====
The AntiVir Updater can be set to always check for updates at a
particular time of day. This is specified in a HH:MM format
(where HH is the hour and MM is the minutes). If you do not have a
permanent connection, you may set it to a time when you are usually
online. You may also let AntiVir choose a random time (r).

If you have a permanent connection then a random time may be preferred
because it will help to disperse the times when other users are
getting updates.

available options: HH:MM r
What time should updates be done? [RANDOM]
```

▶ Type the time in HH:MM format

- OR -

type R for a random time.

▶ Confirm all other configuration questions with **Enter**.

-
- ↳ The automatic updates via the Internet Update Daemon are now configured. The Daemon will automatically start (if not running already) or it restarts (if already running).

Starting and Stopping Internet Updater Manually

If you want to start Internet Update Daemon manually:

- ▶ Type:
`/usr/lib/AntiVir/avupdater start`

If you want to stop Internet Update Daemon manually:

- ▶ Type:
`/usr/lib/AntiVir/avupdater stop`

If you want to check the current status of the Internet Update Daemon:

- ▶ Type:
`/usr/lib/AntiVir/avupdater status`

Performing Cron Updates



Performing updates with cron is recommended!

If you are an experienced UNIX user, you can use cron daemon to perform automatic AntiVir updates.

Cron daemon is used to run regular system processes. For more details, refer to your UNIX documentation.

Using cron for updates, you have more configuration possibilities than with the Internet Updater.

- Example:
- ▶ Enter the following cron job in `/etc/crontab`:
`45 */2 * * * root /usr/lib/AntiVir/antivir --update -q`
 - ↳ This command activates updates every 2 hours, but performs them 15 minutes ahead of the set time: 0:45, 2:45, 4:45 and so on. The `-q` parameter states that no report will be given.

Starting Internet Updater Automatically

If you do not want to use cron, you can work with the Internet Update Daemon. If you have performed the installation as described in [Installing AntiVir VSA – Page 12](#), your system is correctly configured.

If the Internet Update Daemon has not yet been automatically activated on system start-up:

- ▶ Reinstall AntiVir with the necessary settings (see [Reinstalling AntiVir VSA – Page 14](#)).

Verifying Updates Authenticity with GnuPG

GnuPG is a free alternative to the encryption program PGP (Pretty Good Privacy). Using GnuPG you can verify the authenticity of the AntiVir Updates.



It is highly recommended to use GnuPG.

However, this procedure requires extensive knowledge of UNIX and GnuPG. In the event of configuration errors, there is the danger of deactivating AntiVir updates.

The user running updates on the computer has to perform these steps. Usually it has to be a user with administrator rights.

You can find more details of GnuPG at <http://www.gnupg.org>

Follow these steps to activate GnuPG support:

- ▶ Download GnuPG from the website <http://www.gnupg.org>. Here you can also find the manual with further information on GnuPG and its features.
- ▶ Generate your own PGP key pair, as described in the documentation.
- ▶ Import the AntiVir public PGP key to your key-ring:

```
gpg --import antivir.gpg
```

– OR –

Import the AntiVir public key directly from the key server:

```
gpg --keyserver=wwwkeys.pgp.net --recv-keys 0F821C2E
```
- ▶ Display the fingerprint of the key to check if it really is the AntiVir PGP key:

```
gpg --fingerprint build@avira.com
```

↳ The 40-character fingerprint is displayed.
- ▶ Check whether the fingerprint corresponds with the one on the AntiVir website (<http://www.avira.com>).
- ▶ Sign the AntiVir public key in order to certify its validity:

```
gpg --sign-key build@vira.com
```
- ▶ Change to the */bin* sub-directory of the AntiVir installation directory (example):

```
cd /tmp/antivir-vsa-prof-<version>/bin
```

↳ Here you can find the files *antivir* and *antivir.asc*.
- ▶ Check the signature with:

```
gpg --verify antivir.asc antivir
```

↳ If you do not get any error message, you can use GnuPG for AntiVir updates.
- ▶ Activate GnuPG for AntiVir. In */etc/avupdater.conf* enter the path to GnuPG binaries, using the option *GnuPGBinary*:

```
GnuPGBinary /usr/local/bin/gpg
```



You can only edit this option in *avupdater.conf* manually. Setting in the configuration script is not possible in order to avoid the danger of configuration errors.

- ▶ Restart Internet Update Daemon to activate the new settings in *avupdater.conf*:

```
/usr/lib/AntiVir/avupdater restart
```

↳ From now on, GnuPG authenticates the updates.

5 Configuration (Windows)

Savapi 2 has two components: Savapi Service and SAVAPI.DLL. You can configure both using their .INI files.



Please note that you do not normally need to carry out any special configuration for SAVAPI 2. The default settings are usually sufficient.

The Savapi Service initially runs with secure default values. It automatically creates the file *SAVAPI.INI*.

You can change most of the parameters while Savapi Service is running. A restart is only necessary for the following parameters:

- Port number
- Temporary directory
- Updates directory
- License file name
- Logfile name

If you want to stop Savapi Service:

- ▶ Start the services applet under **Start\Administrative Tools\Services**
- ▶ Select Savapi Service.
- ▶ Stop Savapi Service.
- ▶ Change the parameters.
- ▶ Restart Savapi Service.
- ▶ If necessary, restart the program that uses *SAVAPI.DLL*.

5.1 Available Entries in SAVAPI.INI

You can change the following parameters of *SAVAPI.INI*:

Port Number

This value indicates the number of the TCP/IP port used for communication between Savapi Service and SAVAPI.DLL. If this port is already assigned, you can change it. Do not forget to specify it in *SAVAPIDL.INI* (see [Possible Entry in SAVAPIDL.INI](#) – Page 32).

Example `PortNumber=18370`

Temporary Directory

It specifies the directory to which Savapi Service writes its temporary files. The location is usually the sub-folder *\temp* of the installation directory. You may, however, use another location – but ensure there is enough memory space.

Example `TempDirectory=C:\Program Files\Avira GmbH\AntiVir SAVAPI\temp\`

Update Directory

Savapi Service saves the downloaded updates to this directory. It is a so-called working directory for the Updater (Savapi Update Service). The directory should not be modified. Ensure that Savapi Update Service has write access to this directory.

Example `UpdateDirectory=C:\Program Files\Avira GmbH\AntiVir SAVAPI\update\`

License File Name

This parameter defines the name of the license file to be copied to the SAVAPI installation folder.

Example `KeyFileName=C:\Program Files\Avira GmbH\AntiVir SAVAPI\hbedv.key`

Logfile Name

This value indicates the name of the Savapi Service logfile. You can move the logfile to another location on your hard disk. The Service requires write access to this directory. The default logfile is located in the installation directory and its name is *SAVAPI.LOG*.

Example `LogFileName=C:\Program Files\Avira GmbH\AntiVir SAVAPI\savapi.log`

Maximum Logfile Size

It sets the maximum size of the logfile (in kB). When this value is exceeded, the oldest entries are deleted automatically.

If the value is 0, there is no restriction for the logfile size.

Example `LogFileSize=1000`

Updates Server Name

Savapi Service downloads its updates (new virus signatures) from the specified URL. If you want to use another server (e.g. via Internet Update Manager), you can change the URL.

Example `UpdateUrl=http://dl.antivir.de`

If you want to perform updates from a shared directory, you must specify the path to this directory for `UpdateUrl`. In the case of authentication, you have to write the username and password for `NetworkUserName` and `NetworkPassword`. Please note that Savapi Update Service must run under a user account (default, Local System Account) and access the shared directory through it.

Example `UpdateUrl=file://computername/sharedfolder
NetworkUserName=fmeier
NetworkPassword=password`

Updates Interval

This value sets the time interval for the Internet Updater to search for available updates on the server specified as `UpdateURL`. The value is given in minutes. Default: every 120 minutes. Savapi Service automatically performs an update of the engine and virus

signatures after the first action (scan for viruses and other malware). The zero value deactivates the search for updates.

Example `UpdateInterval=120`

Proxy Server for Updates

If the option is activated (1), Savapi Service downloads the updates via the specified proxy server. By default, the Updater does not use a proxy.

Example `ProxyEnabled=0`

Proxy Server Address

Type the full name or IP address of the server you use for updates. This value is applied only if `ProxyEnabled` is active.

Example `ProxyUrl=proxy.mydomain.com`

Username and Password for Proxy Server (Proxy Authentication)

Type the username and password that the Internet Updater should use to access the proxy server. These values are applied only if `ProxyEnabled` is active.

Example `ProxyUserName=fmeier`
 `ProxyPassword=password`

Email Notifications

If `SmtMailEnabled` is active (1), Savapi Service sends email notifications to the address specified for `SmtRecipientAddress`. The notifications can be sent in the event of errors or successful updates.

Make sure that the parameters `SmtMailMode`, `SmtHostName`, `SmtSenderAddress` and `SmtRecipientAddress` are correctly set.

`SmtMailEnabled` is by default inactive.

`SmtMailMode` parameter sets the case for sending emails.

Example `SmtMailEnabled=0`
 `SmtMailMode=0`

0 = sending emails only by update errors.

1 = sending emails in every case (Update successful or not).

SMTP Server Name

Type the full name or IP address of your SMTP server. This value is used only if `SmtMailEnabled` is active.

Example `SmtHostName=smtp.domain.net`

Sender Email Address

Type the email address you want to use when sending notifications. This value is used only if `SmtMailEnabled` is active.

Example `SmtSenderAddress=sender@domain.net`

Recipient Email Address

Type the email address to which you want to send the notifications. This value is used only if `SmtMailEnabled` is active.

Example `SmtRecipientAddress=recipient@domain.net`

5.2 Possible Entry in SAVAPIDL.INI

The .INI file for *SAVAPI.DLL* is *SAVAPIDL.INI*. It enables the communication between AntiVir VSA and the engine. This file is not available by default and the program runs with default settings.

In order to change the default port for communication with Savapi Service, you have to create a file named *SAVAPIDL.INI* in the directory of *SAVAPI.DLL*.

It only contains the following entries:

```
[ SAVAPI2DLL ]
PortNumber=18370
```

Port Number

This is the number of the TCP/IP port used for communication between Savapi Service and *SAVAPI.DLL*. If this port is already assigned, you can change it.

Do not forget to change this value in the corresponding entry of the Savapi Service .INI file (*SAVAPI.INI*) (see [Available Entries in SAVAPI.INI](#) – Page 29).

Example `PortNumber=18370`

5.3 Immediate Updates

AntiVir VSA is set by default to perform automatic updates every two hours.

Updates can be carried out via the Internet, via Intranet from any computer in your network or from a shared directory.

Using *StartUpdate.exe* Savapi Service searches immediately for updates. This does not depend on the update interval settings. In the event of errors, the application returns the `Errorlevel 1` (very useful for batch files). Successful updates are logged in *SAVAPI.LOG*. The application itself has no output.

Background

Immediate updates are useful, for example, to test the settings in *SAVAPI.INI*.

You can also control updates entirely via the SAP environment (if supported). In this case, you should set the update interval to 0.

6 ABAP-Specific Configuration

This Chapter describes the Virus Scan Interface configuration for ABAP systems. The texts are taken from the SAP website.

6.1 Setting the Virus Scan Interface

In order to use the SAP Virus Scan Server, you have to observe the implementation guide (IMG) files. Follow these steps:

- [Defining Scanner Groups](#) – Page 33
- [Defining Virus Scan Servers](#) – Page 35
- [Defining Virus Scan Profiles](#) – Page 45
- [Implementing a BAdI for Virus Scanners](#) – Page 50

6.1.1 Defining Scanner Groups

A scanner group combines multiple virus scanners of the same type to allow load balancing. Since you select the virus scan server using the scanner group when maintaining the virus scan profile, you must assign each virus scan server to a scanner group.

Maintain a scanner group for each product class of virus scanners that are connected to the system using the virus scan server. If you include your own virus scanners with the BAdI `VSCAN_INSTANCE`, create a scanner group for each implementation of your own scanner and identify these as BAdI implementations.

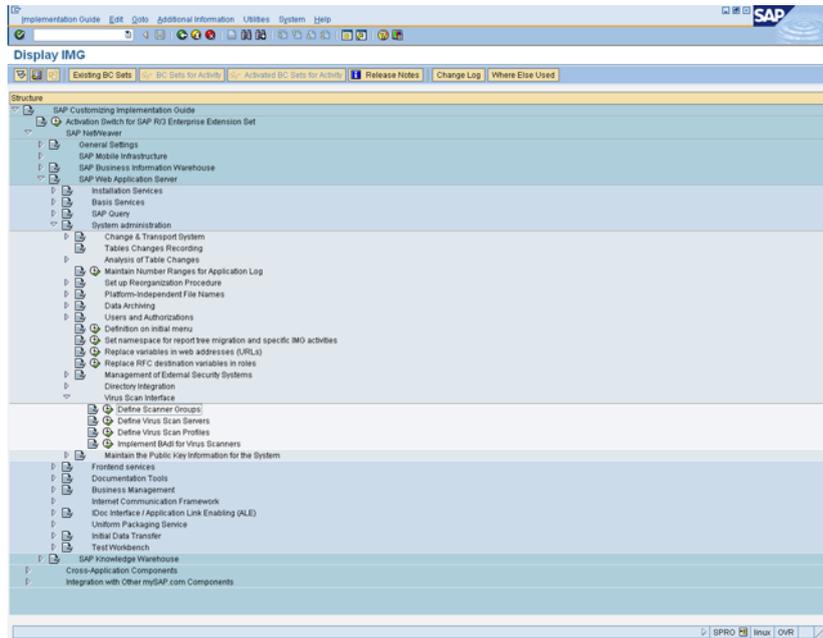
You can store configuration parameters for each scanner group. These are divided into initialization parameters and scan parameters:

- Initialization parameters are transferred to the virus scan server when it is started, and are required to be able to start the virus scan server. If you use the Business Add-In, these parameters for the method of creating the scan instance are transferred. The parameters contain, for example, the path to the virus signatures.
- Scan parameters are transferred for each scan process and control the behavior of the individual request, such as yes/no for activating the scanning of macros.

SAP does not supply any scanner groups.

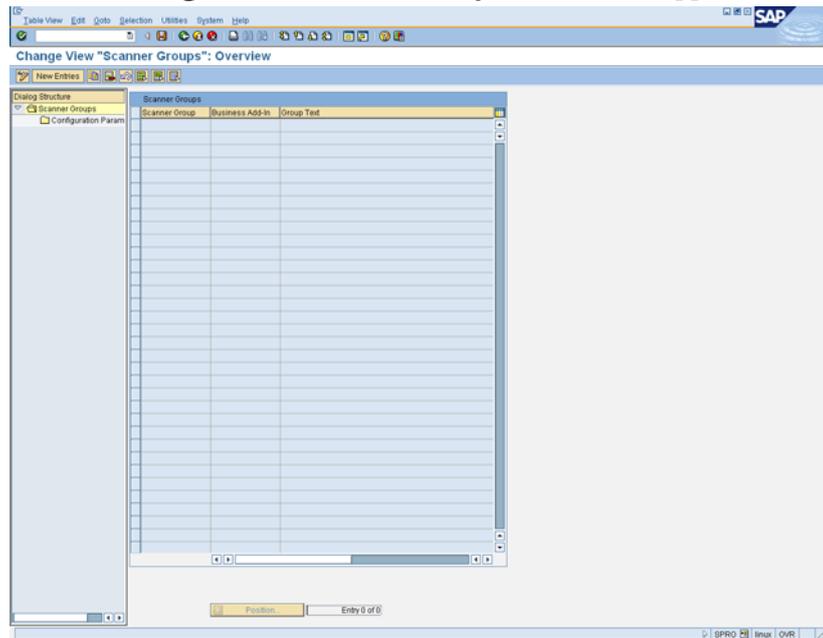
- ▶ Type the transaction number ***spro*** (upper-left field).

- ▶ In the Implementation Guide, choose (IMG) **SAP Web Application Server/System Administration/Virus Scan Interface:**



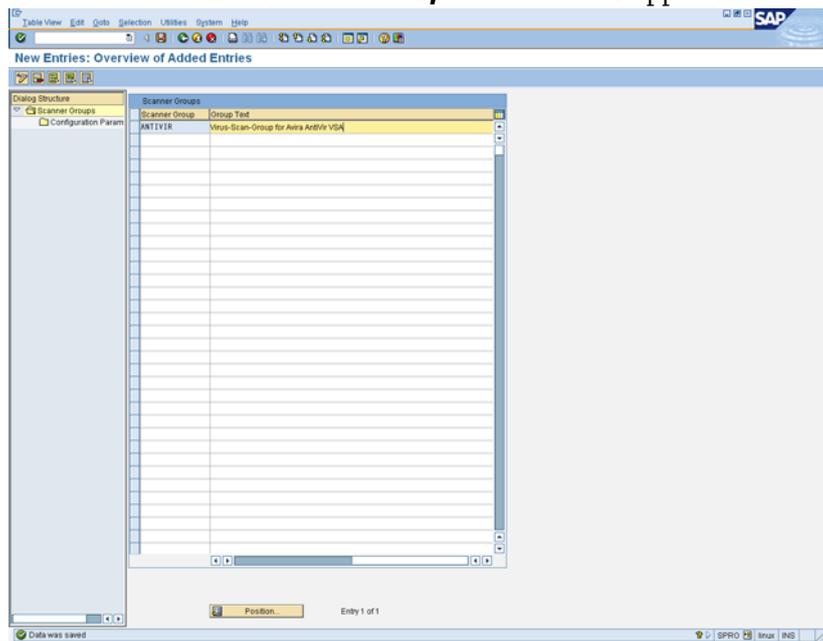
- ▶ Choose the **Execute** option next to **Define Scanner Groups**.

↳ The screen **Change View "Scanner Groups": Overview** appears



- ▶ Choose **New Entries**.

↳ The screen **New Entries: Overview of Added Entries** appears.



► Specify the data for the scanner group (see table below).

Field	Notes
Scanner Group	Freely definable name of the scanner group.
Business Add-In	If this indicator is set, the program transfers the request for a virus scan instance for this scanner group to the Business Add-In VSCAN_INSTANCE, with which customers can include their own virus scanners. If this option is not set, the program searches for a suitable virus scan server among the set of virus scan servers maintained in Customizing that have this scanner group.
Group Text	Explanation of the scanner group.

► Save your entries.

6.1.2 Defining Virus Scan Servers

The SAP Virus Scan Server is an executable program that includes virus scanners from certified vendors using an interface and provides scan services to the application servers of the system as a registered RFC server.

The application server controls tasks such as starting, stopping and monitoring the virus scan server. You configure the data required to do this in this step.



- Use this procedure to create an entry for each virus scan server that you want to set up. For performance reasons, we recommend that you set up at least one virus scan server on each application server.
SAP does not provide any configuration data for virus scan servers.

-
- ✓ You have created at least one scanner group.
 - ✓ You have decided whether you are creating the virus scan server as an application-server-starter or as a self-starter (see [Application-Server-Starter or Self-Starter](#) – Page 40).
 - ▶ In transaction SM59, create an RFC connection with the connection type T.



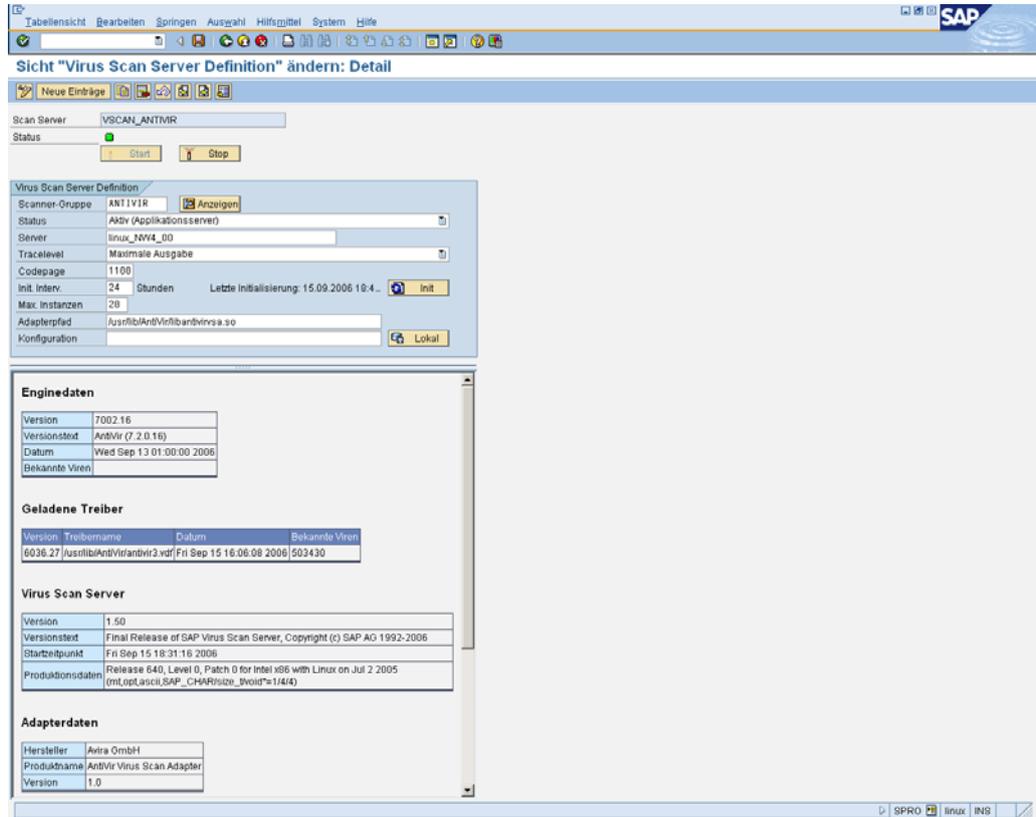
Since the configuration of the virus scan server requires the following naming convention, you must use it for the RFC destination of a virus scan server:

- VSCAN_<host name>, if you only want to start one virus scan server on the host.
- VSCAN_<host name>-<number>, if you want to start multiple virus scan servers on the host. The number is a sequence number, which is separated from the host name with a hyphen.

Possible names would therefore be: VSCAN_HOST123 , VSCAN_HOST345-1 , VSCAN_HOST345-2, and so on.

- ▶ Choose the activation type **Registered Server Program**.
- ▶ Use the name of the RFC destination as the program ID.
- ▶ Enter the address of the gateway of the system as the gateway host and gateway service. If you are starting the virus scan server on an application server using the Computing Center Management System, choose the gateway of that application server.
- ▶ In the Implementation Guide, choose (IMG) **SAP Web Application Server/System Administration/Virus Scan Interface**.
- ▶ Choose the **Execute** option next to **Define Virus Scan Servers**.
 - ↳ The screen **View: Change "Virus Scan Servers": Overview** appears.
- ▶ Choose **New Entries**.
 - ↳ The screen **New Entries: Details of Added Entries** appears.

- In the **Scan Server** field, enter the name of the virus scan server. The name must be the same as the name of the RFC destination that contains the technical connection to the virus scan server.



- Under **Virus Scan Server Definition**, enter the data for the virus scan server (see table below).

Field	Possible Values	Comment
Scanner Group	All previously created scanner groups, which you can display using the input help.	<p>The scanner group combines multiple virus scan servers or allows the use of a BAdI implementation.</p> <p>If you create multiple virus scan servers in a scanner group, you achieve load balancing.</p> <p>All of the virus scan servers of a scanner group have the same set of configuration parameters and will therefore use the same scan engine.</p>
Status	<p>-ACTS (Active as a self-starter): Although the CCMS monitors the virus scan server (if it is not available, an error status is triggered), it does not start or stop the virus scan server. This status is suitable for virus scan servers that are, for example, started as a service at operating system level.</p> <p>-ACTV: Active (Application Server) The CCMS monitors the virus scan server and, if necessary, starts it on the specified application server.</p> <p>-INAC (Inactive on an Application Server) The CCMS monitors the virus scan server and, if necessary, stops it on the specified application server.</p> <p>-NONE: No monitoring: The CCMS does not monitor the virus scan server.</p>	<p>Monitoring status of the virus scan server in the CCMS.</p> <p>If the status is NONE or INAC, the system's automatic server selection can no longer find this virus scan server.</p>
Server	The input help provides a list of the existing servers. Do not specify a different server name.	Application server on which the virus scan server is to be started and/or monitored.
Trace Level	<p>-Errors only</p> <p>-Errors and warnings</p> <p>-Errors, warnings and information</p> <p>-Maximum output</p>	<p>Specifies the trace level for the virus scan server, which is to be transferred to the CCMS at operating system level when the virus scan server is started.</p> <p>We recommend that you only use one of the first two levels Errors Only or Errors and Warnings in production systems. The two other trace levels are available for finding errors during test operation in the test system.</p>

Field	Possible Values	Comment
Codepage	<p>Enter the codepage valid for the virus scan server. It must correspond to the codepage of the application server that is communicating with the virus scan server:</p> <ul style="list-style-type: none"> -If you are only using one codepage in your application servers, enter this codepage. -If you have application servers in different codepages, set up a virus scan server on each application server and specify the valid codepage in each case. -If your system uses UNICODE, do not enter anything. 	Codepage that the CCMS sets when the virus scan server is started.
Init.Interv.	<p>0 or <empty>: no automatic reinitialization</p> <p>If the vendor of your virus scanner uses the interface provided by SAP with which an initialization from outside the system can be performed, you can leave the field empty. This interface is available to certified vendors of virus scanners.</p> <p><n>: Interval in hours</p>	<p>Specifies the number of hours after which the virus scan server is to be regularly reinitialized.</p> <p>For the virus scan server to load new virus definitions from the virus scan server, you must reinitialize it.</p> <p>The automatic reinitialization is performed during the periodic monitoring of the virus scan servers by the CCMS.</p>
Max. Instances		<p>Specifies the maximum number of scan instances provided by the virus scan server.</p> <p>A virus scan server may provide multiple scan instances.</p> <p>You can use the maximum number specified here to determine how many of these instances are provided. If this number is exceeded, the virus scanner is no longer available for scan requests. The number of instances should correspond to the number of work processes.</p>

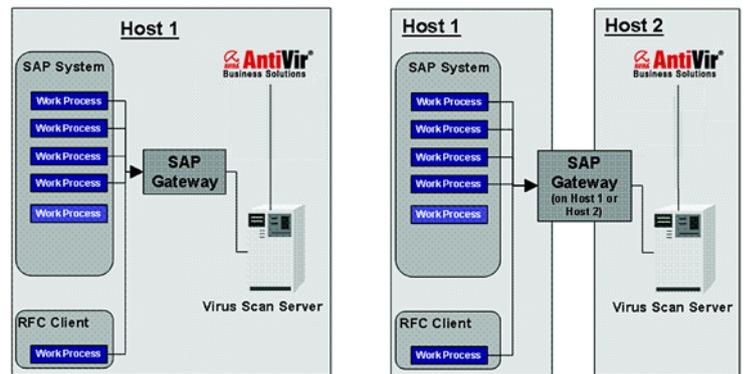
Field	Possible Values	Comment
Adapter Path	Full path of the library that contains the virus scan adapter.	Specifies the full path of the virus scan adapter. If you do not fill the field, the virus scan server uses the content of the environment variable VSA_LIB.
Configuration	Full path to the configuration file of the virus scan server.	Specifies the full path to the configuration file of the virus scan server. The configuration file can contain optional parameters of the virus scan server. For externally-started virus scan servers, the configuration file has already been defined at the virus scan server command line and you cannot therefore change it here.

► Save your entries.

Application-Server-Starter or Self-Starter

When configuring a virus scan server for ABAP systems, instead of an application-server-starter (started by the application server) you can install a self-starter (for example, started externally as a service under Microsoft Windows NT or a daemon under UNIX). In the case of application-server-starters, all components are on the same host. On the other hand, in the case of self-starters, the virus scan server and the SAP Web AS can be on different hosts. This means that you can use a virus scan server that is only available for a particular platform, even if the SAP Web AS is installed on a different platform.

Virus Scan Server on One or Two Hosts:



During operation, this division into application-server-starters and self-starters primarily affects the Computing Center Management System (CCMS). You can monitor the virus scanners in the CCMS (transaction RZ20), in the monitor Virus Scan Servers in the monitor set SAP CCMS Monitors for Optional Components (for more details see SAP Website). The following differences exist in this case:

- Application-Server-Starters:
In this case, the CCMS data collector automatically checks whether a configured virus scan server is available. If this is not the case, the CCMS triggers an alert, and starts the virus scan server again as an auto-reaction.
- Self-Starters:
In this case, although the processes are monitored by CCMS, they are not

automatically stopped or started. There is, however, a separate MTE class in CCMS for these self-starters. You can assign an auto-reaction method to this MTE class yourself to react to alerts. You can, for example, use the MTE class `CCMS_OnAlert_Email` to send an e-mail or an SMS (see "Defining Automatic Alert Notification" and "Forwarding Alerts to Alert Management (ALM)" on the SAP website).



Ensure that you safeguard your RFC connections with Secure Network Communications (SNC) as described in the SNC manual. You can find the SNC manual on the SAP Service Marketplace under <http://service.sap.com/security> **Security in Detail/Secure System Management**.

For more information about application-server-starters and self-starters, see:

- Virus Scan Server as an Application Server Starter
- Installing a Virus Scan Server as a Self-Starter

Virus Scan Server as an Application-Server-Starter

With this use of the virus scan server, all required components are in the working directory of the SAP Web AS kernel on one host. The virus scan server is included in the standard system. This means that you only have to ensure that the prerequisites for the operation of the application-server-starter are fulfilled:

- You have installed the external anti-virus product and the associated virus scan adapter in accordance with the instructions provided by the vendor.
- The kernel directory contains the following components:
 - `vscan_rfc.exe` (Microsoft Windows NT) or `vscan_rfc` (UNIX)
 - The current RFC library or `LIBRFC` (see SAP Note 413708)
 - `sapcpp45.dll` (Microsoft Windows NT) or `sapcpp45.<shared ext.>` (UNIX)
 - `xml63d.dll` (Microsoft Windows NT) or `xml63d<shared ext>` (UNIX)

Installing a Virus Scan Server as a Self-Starter

The self-starter is available to you as an alternative if you cannot use the application-server-starter, for example in the following cases:

- The SAP Web AS kernel uses 64 bits and the external anti-virus product or the external virus scan adapter (VSA) uses 32 bits.
- The SAP Web AS and the external anti-virus product support different architectures. For example, the SAP Web AS is installed on an AIX platform, but the anti-virus product is only available for Microsoft Windows.
- ✓ The self-starter starts the virus scan engine using a local XML configuration file. This is usually the file `vscan_rfc.xml`, which contains the parameters required by the virus scan adapter. The server must be started, or, if necessary, restarted using operating system resources.
 - ▶ Copy the relevant variant of the virus scan server from the CD or the SAP Service Marketplace to a start directory.
 - ▶ Create the configuration file using the commands listed in the table below, with which you can later also change the existing configuration.

Example

The following call generates both the server and the VSA configuration for `savapi.dll` (Windows) or `libantivirvsa.so.<version>` (UNIX):

To set new parameters to overwrite existing parameters, execute additional commands and options in a new call. These are then set in the XML configuration.

Windows: vscan_rfc get_config -V <drive:>\vsa\savapi.dll -cfg
<drive:>\vsa\vscan_rfc.xml

UNIX: vscan_rfc get_config -V <drive:>/usr/local/AntiVir/libantivirvsa.so.<version> -cfg
<drive:>/usr/local/AntiVir/vscan_rfc.xml

In this example, you can change the call as follows:

Windows: vscan_rfc get_config -V <drive:>\vsa\savapi.dll -cfg
<drive:>\vsa\vscan_rfc.xml -a VSCAN_LOCAL -g <Hostname of SAP Gateway> -x
<Servicename of SAP Gateway> -c <SAP Codepage>

UNIX: vscan_rfc get_config -V <drive:>/usr/local/AntiVir/libantivirvsa.so.<version> -cfg
<drive:>/usr/local/AntiVir/vscan_rfc.xml -a VSCAN_LOCAL -g <Hostname of SAP
Gateway> -x <Servicename of SAP Gateway> -c <SAP Codepage>

Configuration commands for the Self-Starter:

Command	Platform	Notes
help	all	Calls the online help for the commands and options.
regonly	all	Registers the virus scan server only at the gateway without starting the underlying engine. The CCMS uses this command to then call the RFC function VSCAN_RFC_INIT. Note that if you use this command outside the CCMS, the server is not ready for use.
get_config	all	Receives the CSA and separate server configuration and stores them in a local XML configuration. (Option -cfg <file> is mandatory for this). The options received using the command line are stored as the server configuration in this case. If you do not specify any command line options, the predefined values are set. Use this command to start the setup of a self-starter. If the file specified using the option -cfg does not exist, a new file is created.
install	NT	Installs a "new" VSCAN_XX service in the Microsoft Windows NT Service Control Manager (SCM). The -cfg option with a specification of a local configuration is mandatory for this command. The service is installed if the VSA is successfully initialized. If you specify additional options, these are only stored in the XML file used. The -srcv option specifies the number of the service; that is, you can install up to 100 services on a host. The default value for -srcv is 00.
remove	NT	Deletes an existing VSCAN_XX service in the Microsoft Windows NT Service Control Manager (SCM). You can specify the service more exactly using the -srcv option. Example: vscan_rfc remove -srcv 1 deletes the existing service VSCAN_01.
start	NT	Starts an installed VSCAN_XX service. This command starts the service with the specified options. The Microsoft Windows NT command "net start VSCAN_XX" starts the previously installed service only if the local configuration is used.
stop	NT	Stops a running VSCAN_XX service. This command corresponds to the Microsoft Windows NT command "net stop ...".

In addition to the commands, you can specify the following options:

Option	Platform	Notes
-a	all	Program ID of the RFC destination, such as VSCAN_LOCAL.
-g	all	Host name of the SAP gateway.
-x	all	Service name of the SAP gateway, such as sapgw00.
-cfg	all	Complete path specification of the XML configuration file.
-f	all	Path specification of the trace file to be used.
-l	all	Trace level of the trace file: 0 := Errors 1 := Errors and warnings (such as virus infections) 2 := Errors, warnings, and virus scan engine calls 3 := Additional information, all RFC calls, and memory operations.
-c	all	SAP codepage for NON-UNICODE virus scan servers.
-V	all	Path specification of the virus scan adapter to be used. If you do not set this option, the environment variable VSA_LIB is used.
-p	all	Profile name (Default: VSA_CONFIG) for the current VSA configuration. This option allows differentiation if you are using multiple (different) VSA configurations in one XML file.
-T	all	Maximum number of threads that the server can use. Possible values: 1 to 999.
-m	all	Minimum number of threads that the server should use. Note: The mean value of -m and -T is always used for the number of threads that are held open.
-L	all	Path specification for an SNC library.
-S	all	The SNC name of this instance. Note: Setting -L, -S, or -Q activates SNC for the server.
-Q	all	SNC security level Possible values 1:=Authentication 2:=Integrity protection 3:=Encryption 7:=Minimum level 8:=DEFAULT 9:=Maximum level.
-P	all	The SNC name of the SAP instance. Caution: If you set this name, only requests from SAP instances with this SNC identity are accepted.
-I	all	Timeout in seconds for the internal instances operations RELOAD and SHUTDOWN.
-n	all	Maximum number of trace lines for the memory trace. Default value: 10000
-h	all	Retention period in seconds for the memory trace: Default value: 86400 seconds.

Option	Platform	Notes
-srvc	NT	Service number of the Microsoft Windows NT commands install remove start stop
-daemon	UNIX	Starts the virus scan server as a daemon process with fork().

Operating the Self-Starter

You can operate the self-starter as a service under Microsoft Windows NT or as a daemon under UNIX.

Operation as a Service: You can use the Microsoft Windows Service Control Manager (SCM) to install the virus scan server as a service. You can install up to 100 services of this type (numbered from 00 to 99).

Operating the virus scan server as a service means that operating system resources such as the Event Log are available to you for monitoring. You can also use the SCM to restart the virus scan server service after a termination. You can also use the Microsoft Management Console (MMC) to remotely monitor and control the installed service.

Example ► Installation of a service:

```
vscan_rfc install -cfg <drive:>\vsa\vscan_rfc.xml
```

► Installation of additional services (VSCAN_<xx>):

```
vscan_rfc install -cfg <drive:>\vsa\vscan_rfc.xml -srvc 1
```



You must specify the local configuration file (option -cfg). The service is only installed after successful initialization of the virus scan adapter and checking of the SAP gateway.

Operation as a Daemon (UNIX): You can start the virus scan server as a daemon directly on operating system start-up.

Example ► Starting a daemon:

```
vscan_rfc -cfg /vsa/vscan_rfc.xml -daemon
```

You can monitor the daemon with operating system resources (CRONTAB, INITTAB).

Configuring the Self-Starter

You have the following options for configuring the self-starter:

- Call `get_config` again and use additional commands and options as in [Installing a Virus Scan Server as a Self-Starter](#) – Page 41.
- Edit the XML configuration file directly.
- Synchronize the settings using the IMG activity Define Virus Scan Servers (transaction VSCAN) (see [Defining Virus Scan Servers](#) – Page 35).
With this configuration option, the parameters for trace level (option -I), codepage (option -c), max. threads or max. instances (option -T), and VSA_LIB (option -V) are saved to the specified configuration using the Local button. If you leave the

Configuration field empty for a self-starter, the values are saved to the XML configuration in use.



The values are only saved if an XML file already exists.

6.1.3 Defining Virus Scan Profiles

Application programs use virus scan profiles to check data for viruses. A virus scan profile contains a list of scanner groups that check a document. You can also use a virus scan profile to assign configuration parameters for the virus scanner. If you scan for viruses with this virus scan profile, the virus scanner receives the parameters.

A virus scan profile specifies steps that are to be run during a virus scan. A step is either a virus scanner, which is found using the scanner group, or a step specifies, in turn, a virus scan profile, which is then performed as part of the enclosing virus scan profile.

A virus scan is performed under the name of a virus scan profile. The system administrator can use the profile to activate or deactivate the virus scan for each component.

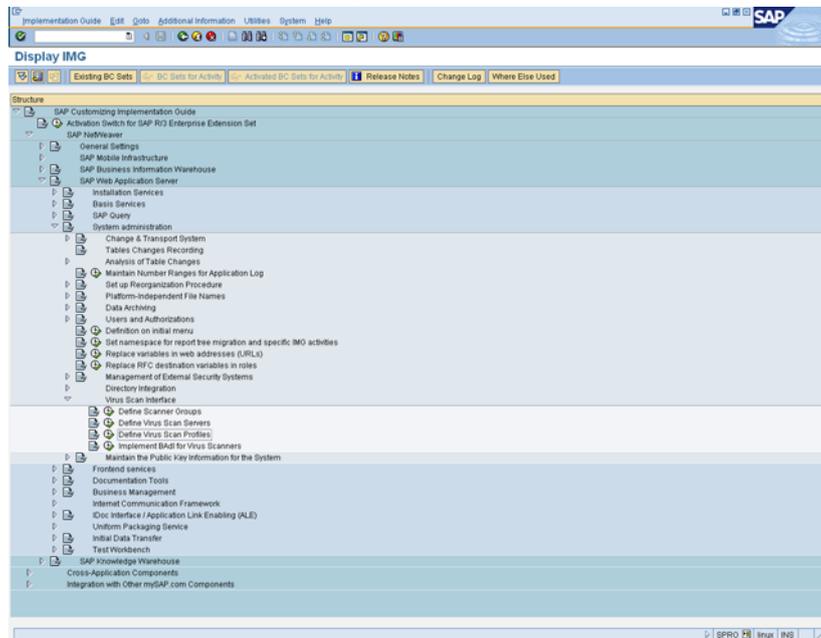
By default, each SAP application that integrates a virus scan provides a virus scan profile. The names of these virus scan profiles are constructed as follows /<Name of the package of the application>/<Name of the function>.

Check the virus scan profiles provided by SAP and determine for which components you are activating or deactivating the virus scan.

If you want to create your own virus scan profiles, you can use the namespaces Y* and Z*.

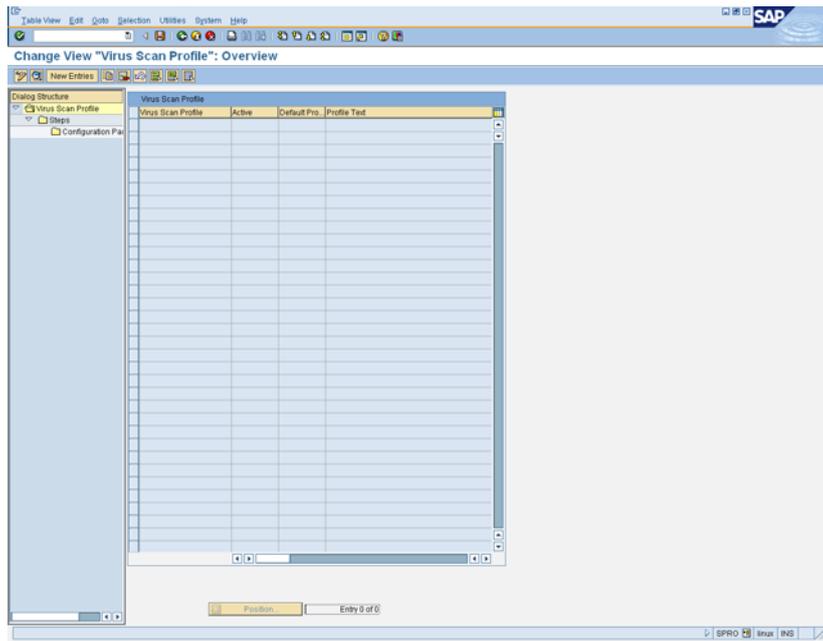
✓ You have created scanner groups.

► In the Implementation Guide, choose (IMG) **SAP Web Application Server/System Administration/Virus Scan Interface**.



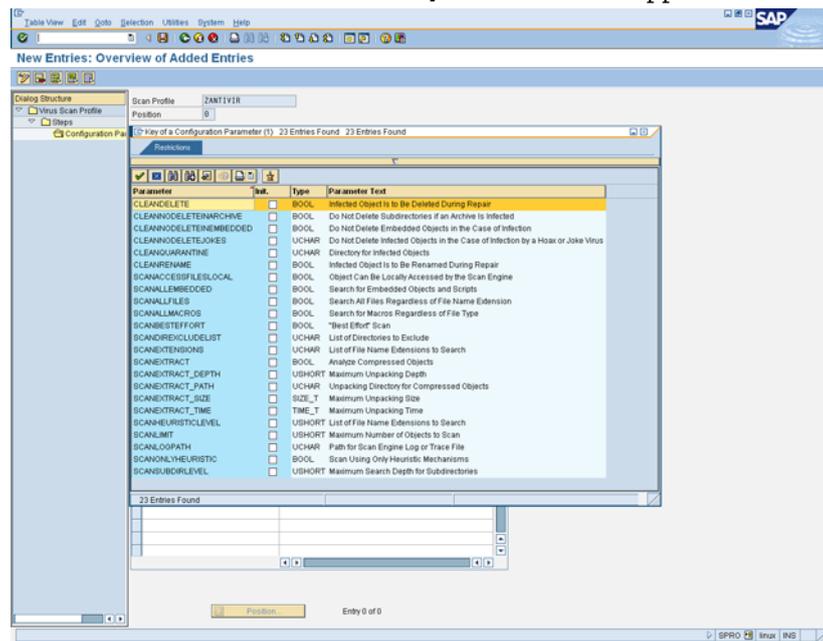
► Choose the **Execute** option next to **Define Virus Scan Profiles**.

↳ The screen **Change View "Virus Scan Profile": Overview** appears.

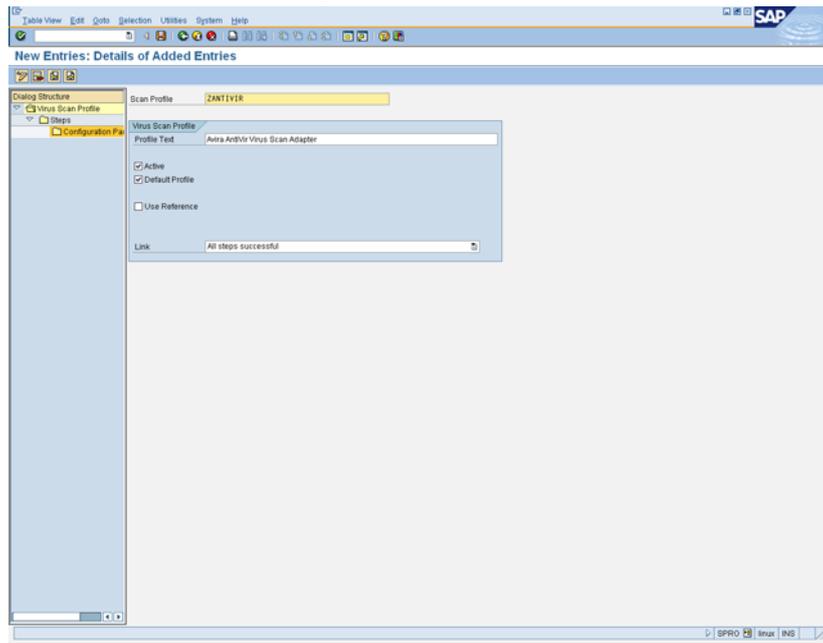


▶ Choose **New Entries**.

↳ The screen **New Entries: Overview of Added Entries** appears.



- Specify the data for the scanner profile (see the table below):

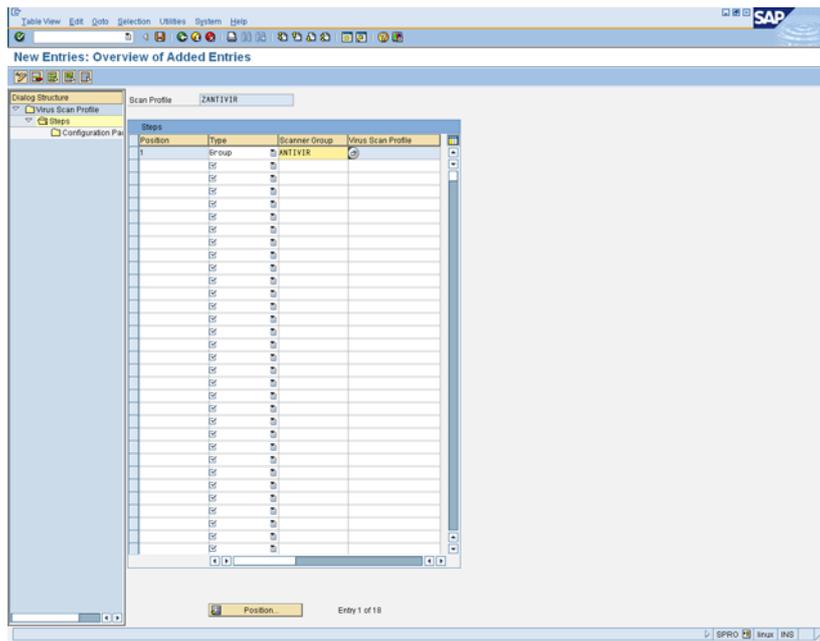


Field	Possible Values	Note
Scan Profile		Specifies the name of a virus scan profile.
Profile Text		Explanatory text for a virus scan profile.
Active		<p>Specifies that this virus scan profile is active.</p> <p>The virus scan profile can only be used if this indicator is set.</p> <p>SAP applications can use fixed profile names that are delivered. By default, these profiles are not active, meaning that the application program works without a virus scan.</p> <p>You can activate the virus scan for each application by setting this indicator.</p>
Default Profile		<p>Indicator that this virus scan profile is the default profile.</p> <p>You can set this indicator for a maximum of one virus scan profile. This virus scan profile is used in the following cases:</p> <ul style="list-style-type: none"> -If an application requests a virus scanner without specifying a virus scan profile. -If a virus scan profile is requested for which the Use Reference Profile indicator is set, and the Reference Profile is empty.
Use Reference		To operate multiple applications using the same virus scan profile, set the Use Reference indicator and specify the reference profile.

Field	Possible Values	Note
Reference Profile	<p>The input help provides a list of all of the profiles that have already been defined.</p> <p>If you leave the field empty, the system uses the default profile.</p>	<p>Specifies the name of the reference profile.</p> <p>Since a virus scan profile can use another virus scan profile as a reference profile, you can operate multiple applications using the same virus scan profile.</p> <p>If the Use Reference Profile indicator is set in the virus scan profile, this field specifies the name of the reference profile to be used. Instead of the settings of the current virus scan profile, the settings of the reference profile are then used. This means that several virus scan profiles can use the settings of a shared reference profile, such as the scanner groups to be used.</p>
Relationship	<p>All steps successful : The virus scan must have performed all steps without errors.</p> <p>At least one step successful : It is sufficient if one step of the virus scan was successfully performed.</p>	<p>Specifies the type of logical linkage for the steps in the virus scan profile.</p> <p>If multiple steps that are to be performed during the virus scan with a virus scan profile are defined for a profile, you can use this field to control how the overall result of the virus scan is to be evaluated.</p> <p>Using multiple steps allows you to scan documents with scan engines from different vendors at the same time.</p> <p>The program interprets a virus scan as error-free only if the scan engine returns the value <code>Check performed successfully</code> or (in the case of cleanups) <code>Cleanup performed successfully</code>.</p> <p>All other return values are regarded as unsuccessful virus scans. This also includes situations such as:</p> <ul style="list-style-type: none"> -The program did not check the document because the file name extension is categorized as non-critical. -The program could not check the document because the document is a password-protected archive. -The scan engine is obsolete.

- ▶ Save your entries.
- ▶ To define steps for the profile, select the **Steps** node in the dialog structure by double-clicking it.

- Choose **New Entries**.

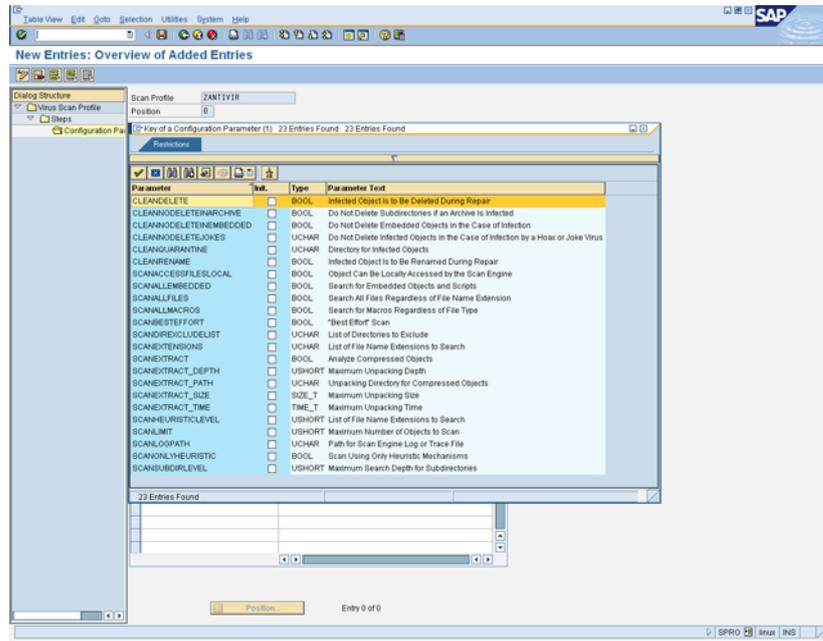


- Enter the following data for the definition of the step:

Field	Possible Values	Notes
Position	<integer value>	Specifies the position of the scanner group in the virus scan profile. If a virus scan profile uses multiple scanner groups, place these in the desired sequence by assigning a position number.
Type	Group or Profile	Specifies whether a step in the virus scan profile refers to a scanner group or another virus scan profile. If you choose Group , the system uses a virus scan server from this group (or a BAdI implementation) for the virus scan. If you choose Profile , the program processes the specified virus scan profile instead of this step. You can define any conditions by combining the steps of the virus scan profile with the linkage type of the steps (AND/OR).
Scanner Group	The input help provides a list of all existing scanner groups.	Combines multiple virus scan servers or allows the use of a BAdI implementation. All of the virus scan servers of a scanner group have the same set of configuration parameters and will therefore use the same scan engine.
Virus Scan Profile	The input help provides a list of all existing profiles.	Specifies the name of a virus scan profile that you can include as a step in the profile that you are currently processing.

- Save your entries.

- To create configuration parameters for a step, double-click the **Configuration Parameters** node.



- Choose **New Entries**.
- Enter the following data for the definition of the configuration parameters:

Field	Possible Values	Notes
Parameters	The input help provides a list of all existing constants.	Specifies the key of a configuration parameter. A virus scanner requires configuration data. The set of possible configuration parameters is defined by SAP as a predetermined set of symbolic constants.
Value	<Value>	Specifies the value given by the vendor for a configuration parameter.

- Save your entries.
 - ↳ You have defined a virus scan profile and therefore performed the last configuration step for the virus scan server. Finally you can check the configuration (see [Problem Analysis for the Virus Scan Server](#) – Page 51).

6.1.4 Implementing a BAdI for Virus Scanners

You can use the Business Add-In VSCAN_INSTANCE to include your own virus scanners in the virus scan interface.

To integrate the BAdI implementation, use the **BAdI Implementation** indicator when creating the scanner group. If you then perform a virus scan with this scanner group, the program calls your implementation of the BAdI as a filter value for the group name and you can transfer an instance of your scanner implementation.

Create an implementation for each scanner group that is to use the BAdI implementation. You can use an implementation for multiple filter values (group names).

SAP does not provide a default implementation. Instead, with the virus scan server, there is a separate component available that integrates the scan engines of certified vendors into the virus scan interface.

- ✓ You have created a scanner group that is to address your implementation.
- ▶ In the Implementation Guide, choose (IMG) **SAP Web Application Server/System Administration/Virus Scan Interface**.
- ▶ Choose the **Execute** option next to **Implement BAdI for Virus Scanners**.
 - ↳ The dialog screen **BAdI Builder: All Implementations for Definition VSCAN_INSTANCE** appears.
- ▶ Choose **Create**.
 - ↳ The dialog screen **BAdI Builder: Create Implementation** appears.
- ▶ Enter a name in the **Implementation Name** field.
 - ↳ The screen **BAdI Builder: Change Implementation <Implementation Name>** appears.
- ▶ Enter a short description in the **Short Text for Implementation** field.

To specify filter characteristics:

- ▶ Choose the **Insert Row** button under **Defined Filters** and specify your group using the input help.
- ▶ Save your entries.
 - ↳ You have created an implementation for the scanner group. For the rest of the procedure, see the documentation for the interface IF_EX_VSCAN_INSTANCE.

6.2 Problem Analysis for the Virus Scan Server

The virus scan server either outputs errors, warnings or additional information to a file or writes them on the server's memory. You can use the VSCANTRACE analysis tool to query and output this memory content to analyze all registered virus scan servers for errors during their production operation.

When the server is started, the trace is deactivated for memory output. Activate it only if problems occur, since it affects the performance of the server. The settings for memory output are only valid for a particular length of time (the default value is 24 hours). They are then deactivated.

- ✓ For you to be able to use the memory trace, at least one virus scan server must be active.
- ▶ Start transaction VSCANTRACE.
- ▶ Choose the server either using the input help that displays all defined virus scan servers from table VSCAN_SERVER, or specify it directly. To do this, it must have been started at the SAP gateway using an RFC destination defined in transaction SM59.
- ▶ Confirm your entry with **ENTER**.
 - ↳ The connection to the virus scan server is created. If the connection to the server is made, the traffic light is green.
- ▶ Choose **Memory**.
 - Otherwise the trace is output to a file, which you can display using the developer traces (transaction ST11, file name dev_VSCAN_<Hostname>.trc).
 - ↳ The current trace level is displayed.

-
- ▶ To set a new value for the trace level, select the desired trace components and then choose **Activate**.



You can completely deactivate the memory trace with the **Deactivate** button, but not the error output to the trace file. You can therefore not suppress the output of errors by setting the trace level for the file to the value **0**.

If you change the selection from **Memory** to **File** or vice versa, you can display the trace level already selected for this option for the individual components with the **Copy** button. The selection option is activated for each active component when you do this.

- ▶ To display the memory trace, choose the **Execute** option.
 - ↳ The overview appears. It shows the availability of the anti-virus engine used, the utilization of the virus scan server, the current trace level for the memory and an HTML output of the current trace information.

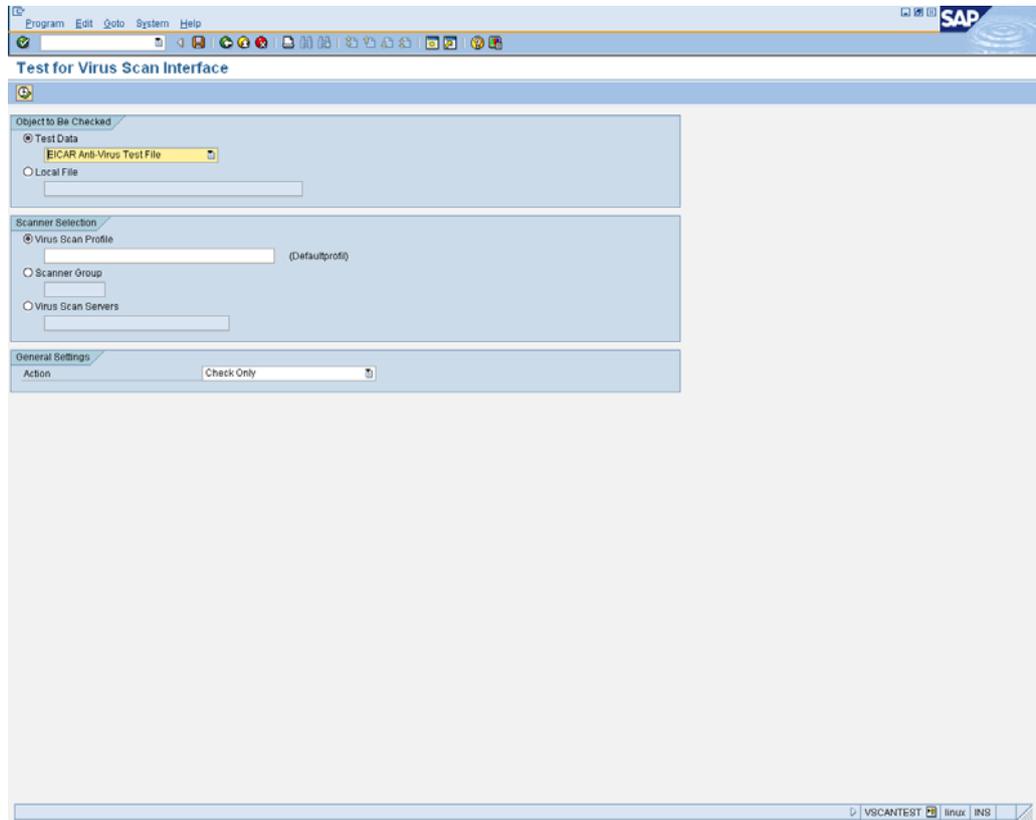
You have the following options in the overview:

- Refresh: Refreshes the list.
- Delete: Deletes the trace output.
- Export: Exports the list to a local file.
- Status: Displays the current status of the virus scan server used, even if the memory trace is deactivated. In addition to technical information on the virus scan server, this output also contains the configuration of the virus scan server and information on the loaded virus scan adapter including the anti-virus engine.
- Stop: Stops the virus scan server.
- Configuration: Branches to the display mode of the IMG activity Define Virus Scan Servers.
- Test: Branches to the transaction VSCANTEST.

6.3 Testing the Installation of the Virus Scan Server

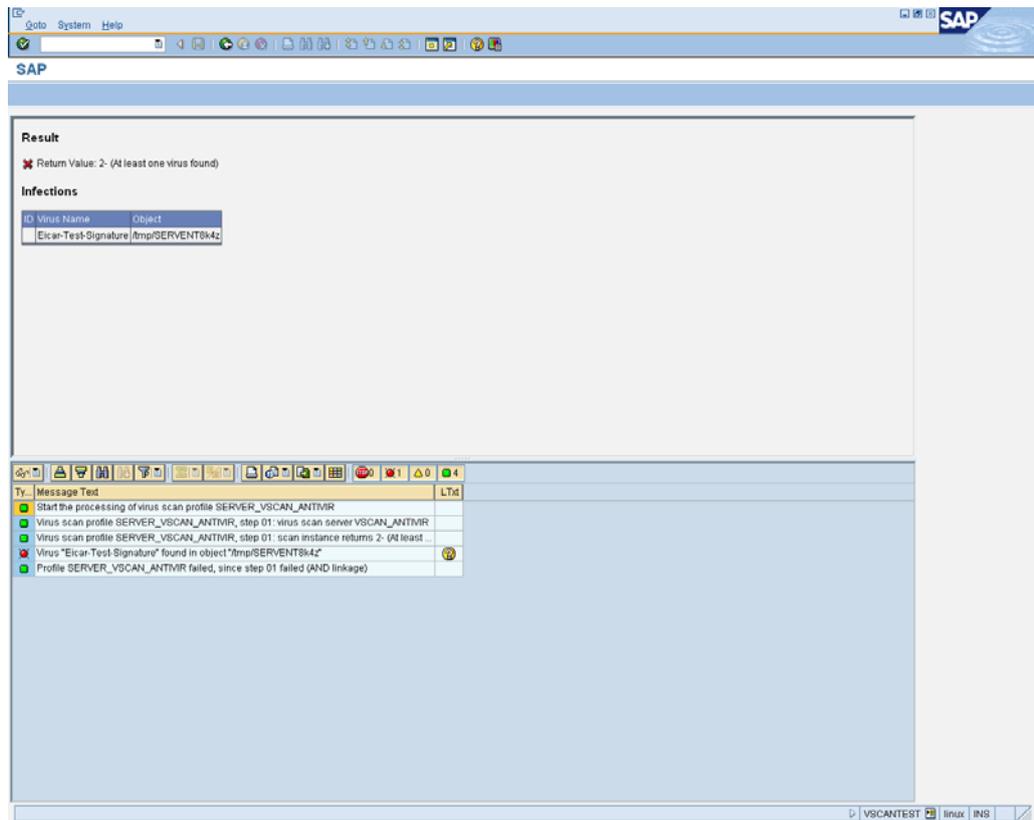
You can use this procedure to check that your configured virus scan server is functioning correctly.

- ▶ Start transaction VSCANTEST.
- ▶ Specify the object to be checked, using either the test data provided or your own local file.



- ▶ Select the virus scan profile, scanner group, or the virus scan server to be tested.
- ▶ Select an action.

- If you choose **Check Only**, the anti-virus product that you specified scans the data for viruses and displays a result:



- If you choose **Check and Clean**, the product also attempts to clean the data if a virus infection is diagnosed.

6.4 Commented Example Program

You can also find a Commented Example Program on the SAP website.

7 Java-Specific Configuration

This Chapter describes the Virus Scan Interface Configuration for Java systems. The texts were taken from the SAP website.

The virus scan provider is the service of the J2EE Engine that makes the `tc/sec/vsi/` interface available to the SAP applications of the Engine.

Select an installation type for the virus scan provider, depending on your system prerequisites:

- **Virus scan adapter for a purely-Java installation:**
This procedure describes the normal case in which you are using a local virus scan adapter. The virus scan adapter is a native dynamic library from a third-party vendor, which can be loaded directly into the process environment of the J2EE Engine. This means that you can check memory contents directly for viruses, which enables higher performance.
- **Virus scan server for a purely-Java installation:**
This procedure describes the special case in which the platform or process architecture does not allow the direct inclusion of a virus scan adapter. This is the case, for example, if the required operating system for SAP NetWeaver is not compatible with the external anti-virus product. In this case, use a virus scan server. The virus scan server communicates with the J2EE Engine using TCP/IP (SAP RFC protocol) and accesses the external anti-virus product using a virus scan adapter.
- **Virus scan adapter or virus scan server for an integrated installation (Java and ABAP):**

Both purely-Java installations provide the same interface to `instancejava` from the package `com.sap.security.core.server.vsi.api`.

The configuration of the virus scan provider service is stored in the Configuration Manager of the J2EE Engine. You can use the Visual Administrator for graphical administration.

Prerequisites: You are an administrator of the J2EE Engine.

Virus Scan Adapter for a Purely-Java Installation

After you have installed an external anti-virus product including a certified adapter, you only need to enter the path to the adapter specified in the documentation for the partner product in the `VSA_LIB` field.

Virus Scan Server for a Purely-Java Installation

- ▶ Start the standalone gateway.
- ▶ Start the virus scan server with the options `-a`, `-x`, and `-g`, as described in [Installing a Virus Scan Server as a Self-Starter](#) – Page 41. For option `-a`, specify the program ID using the naming convention (case-sensitive; prefix `VSCAN_`).
- ▶ In the Visual Administrator, set up the virus scan provider as a virus scan server, as described in [Define a Virus Scan Provider](#) – Page 60.
 - Specify exactly the program ID that you defined above under option `-a` as the name. However, you must omit the name prefix `VSCAN_`, since this is added automatically.
 - Specify server settings that match those of the provider defined above. Specify `-g` and `-x` as defined under step 2.

Virus Scan Adapter or Virus Scan Server for an Integrated Installation (Java and ABAP)

Follow the steps explained in the next Chapter:

- [Define a Scanner Group](#) – Page 57
- [Define a Virus Scan Provider](#) – Page 60
- [Define a Virus Scan Profile](#) – Page 63

8 Java-Specific Configuration for SAP NetWeaver 2004(s) and KMC

This Chapter describes the Virus Scan Configuration for Java systems in the Visual Administrator, as well as the integration with the Enterprise Portal and the Knowledge Management Center.

8.1 Configuration in the Visual Administrator

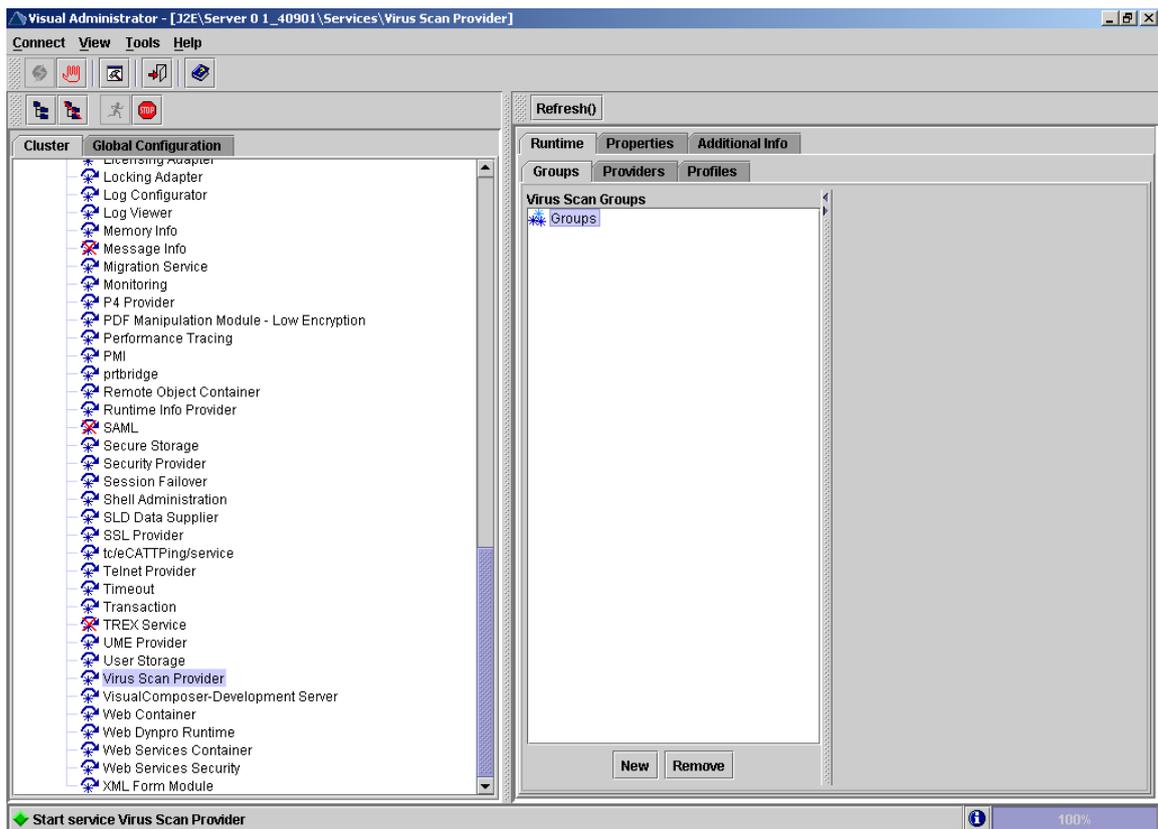
The steps of the configuration are:

- [Define a Scanner Group](#) – Page 57
- [Define a Virus Scan Provider](#) – Page 60
- [Define a Virus Scan Profile](#) – Page 63

8.1.1 Define a Scanner Group

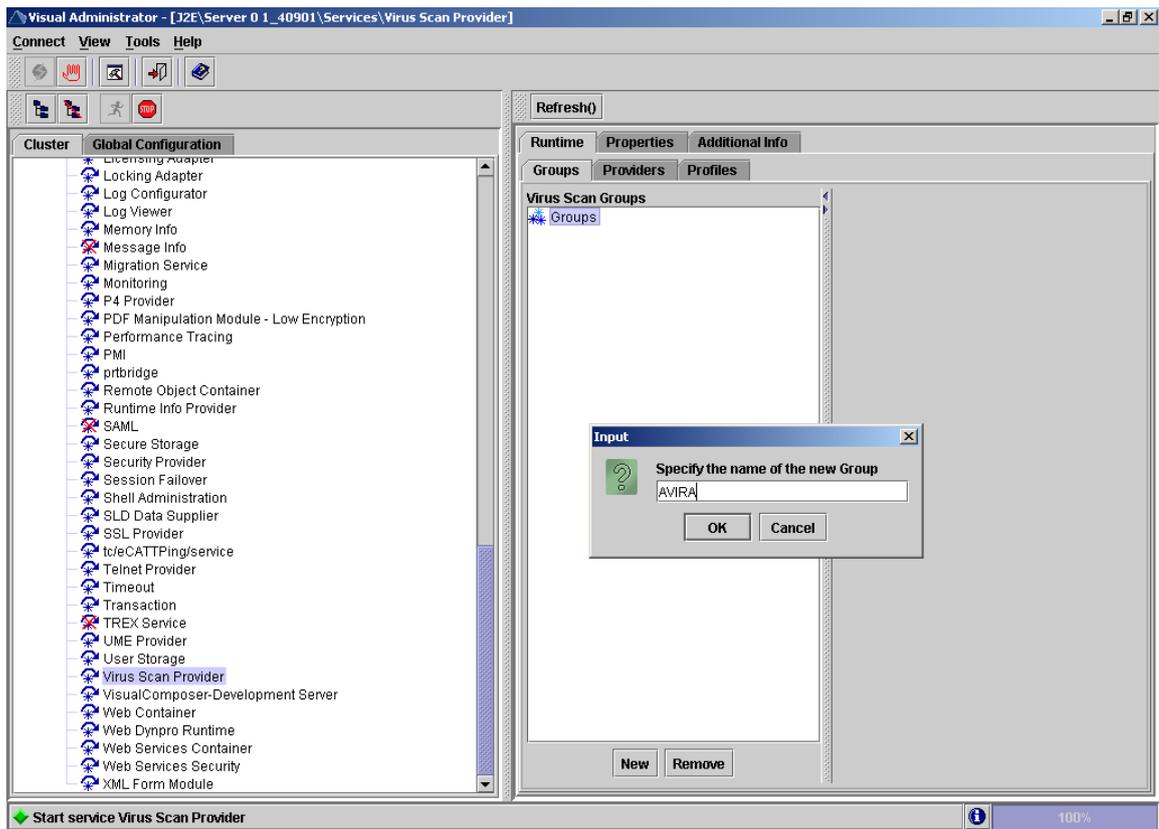
A scanner group combines multiple virus scanners of the same type. You require the groups to specify virus scan profiles later. SAP does not supply any scanner groups.

► In the Visual Administrator, choose the cluster **Virus Scan Provider**.



If the service is not started, click the **Start** button (or right-click on Virus Scan Providers and select **Start**).

- ▶ On the **Groups** tab, create a scanner group by pressing the **New** button.

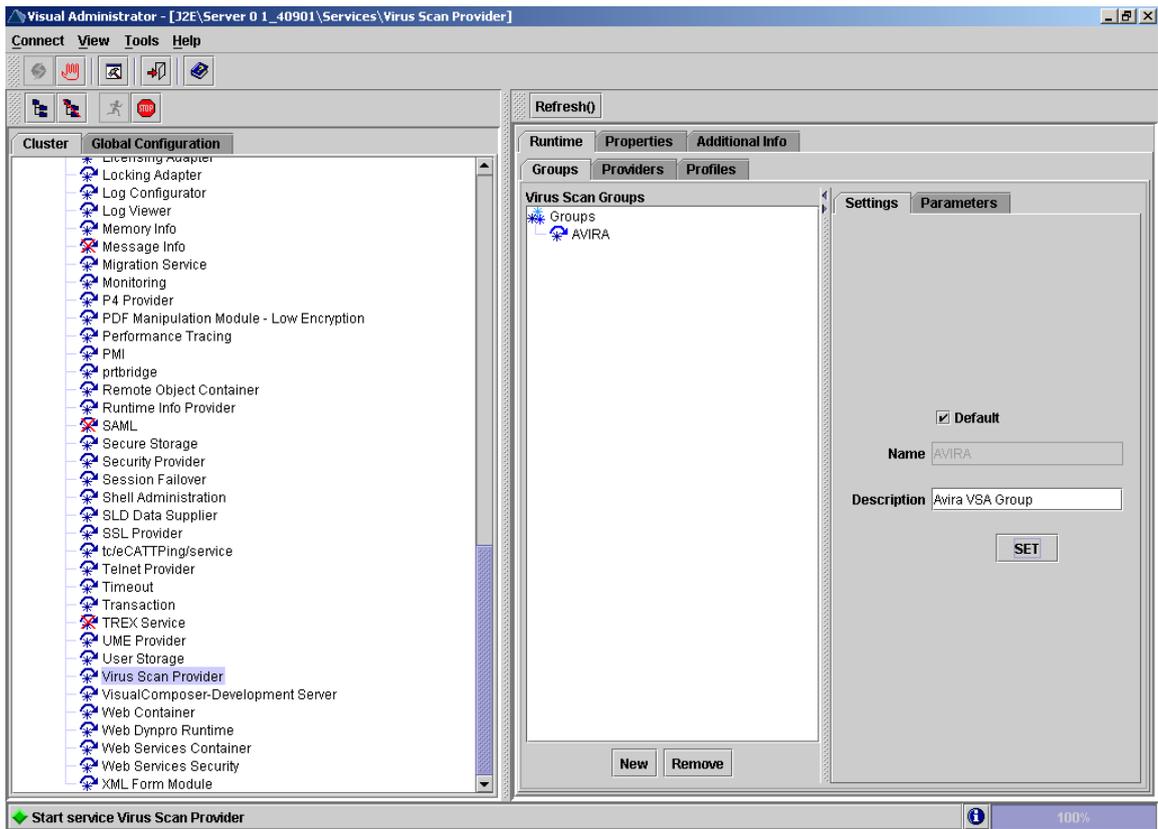


- ▶ Specify the name of the new group (AVIRA) in the dialog box and confirm your entry with **OK**.



The group names are case sensitive. You have to use the same names later in the KMC.

- ▶ Select the node for the newly created group.



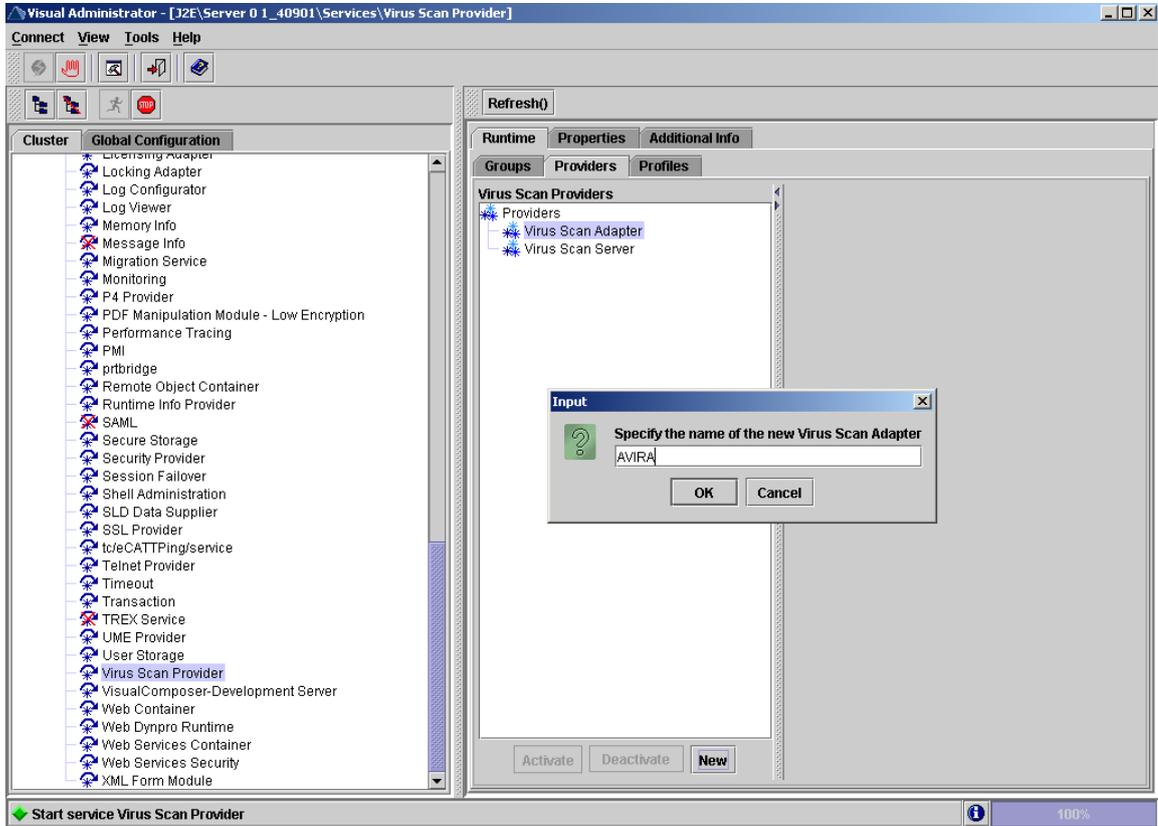
- ▶ On the **Settings** tab, activate the **Default** option, to set the group as default.
- ▶ Enter a description of the group in the **Description** field.
- ▶ To save your entries, press **Set**.

You do not have to make any configuration on the **Parameters** tab at this point.

As the next step, [Define a Virus Scan Provider](#) – Page 60.

8.1.2 Define a Virus Scan Provider

- ▶ In the Visual Administrator, choose the cluster **Virus Scan Provider**.
- ▶ On the **Provider** tab page, select the **Virus Scan Adapter** node and press the **New** button, to create a new virus scan provider.

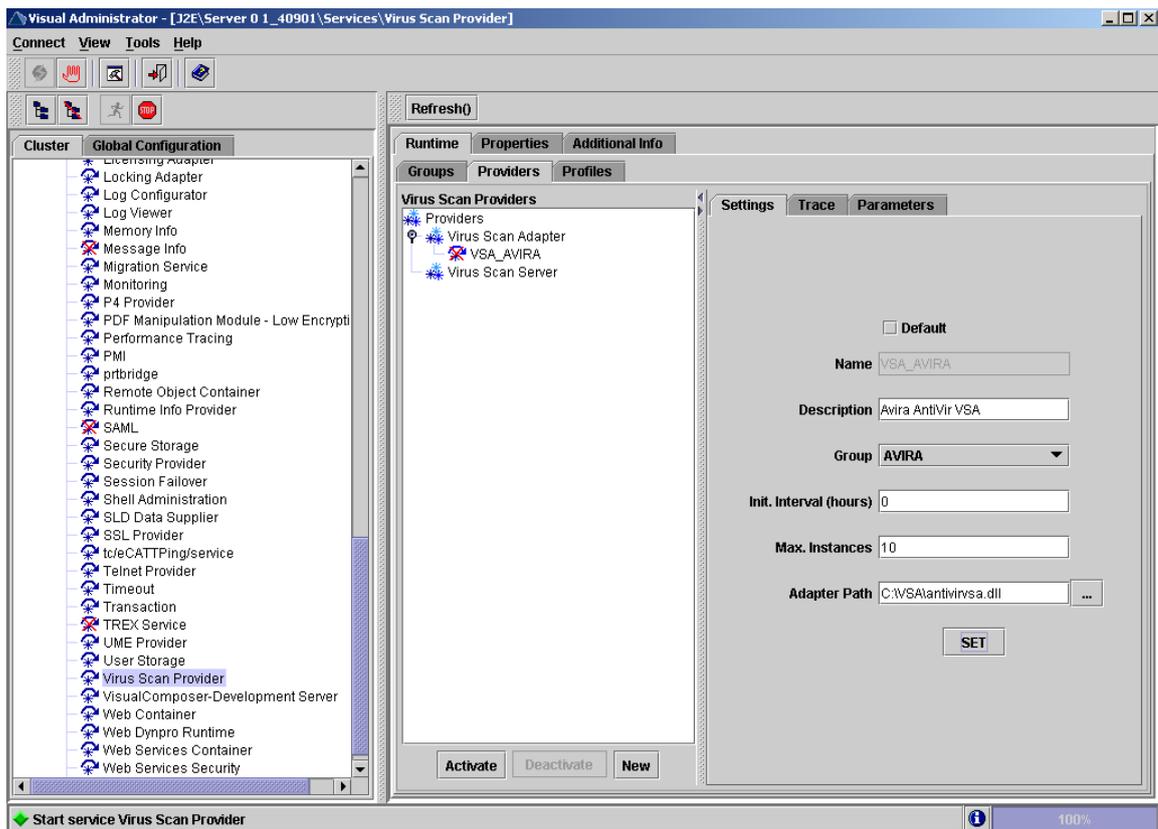


- ▶ Specify the name of the new provider (AVIRA) in the dialog box and confirm your entry with **OK**. The name entered is automatically saved with the prefix “VSA_”.



The names are case sensitive. You have to use the same names later in the KMC.

- ▶ Select the node for the newly created provider.



- ▶ On the **Settings** tab, activate the **Default** option, to set the provider as default and eventually adjust the values described in the table below.

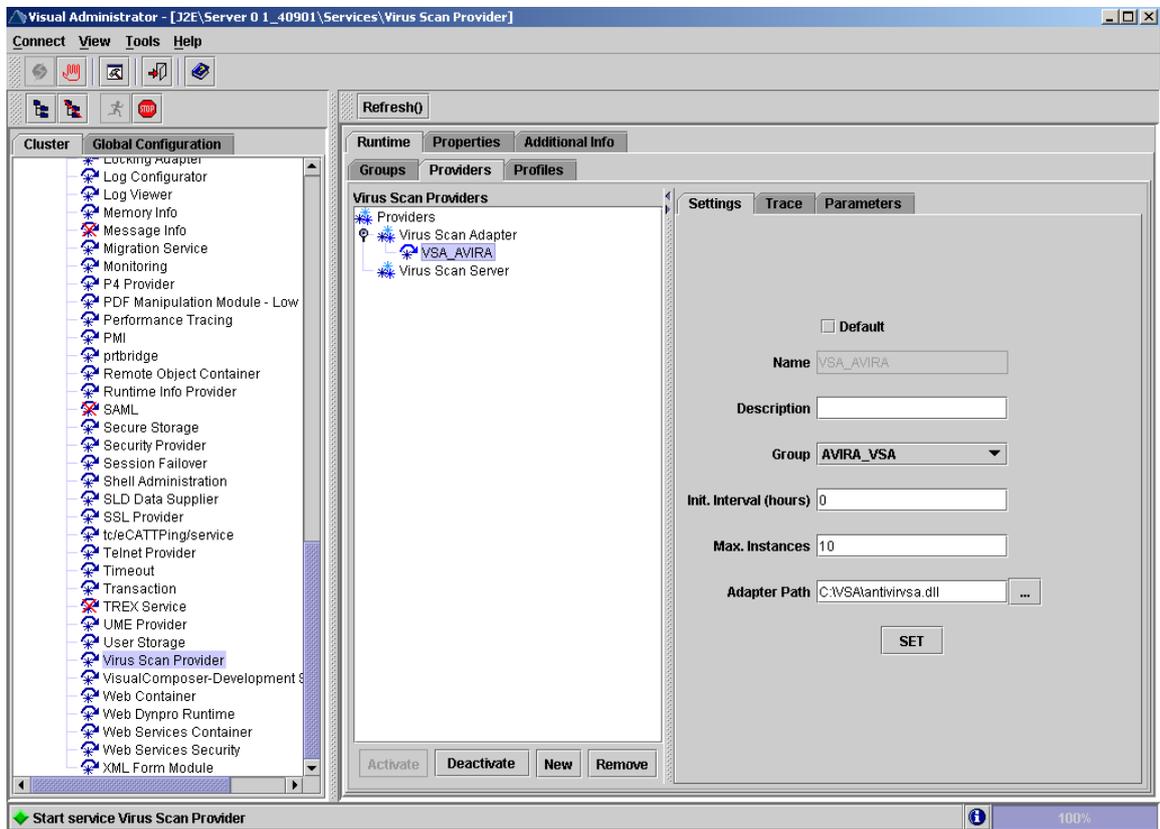
Settings for the
Virus Scan
Adapter

Field	Entry
Default	When activated, the provider will be automatically selected, if no other VSA is specified.
Name	Name of the virus scan adapter. The name entered is automatically saved with the prefix "VSA_".
Description	Description of the current adapter.
Group	The drop down list shows the available groups to which you can assign the current adapter.
Init Interval	The time interval (in hours) for the NetWeaver to end VSA and restart it. Values: 0 restart only when the Virus Scan Service ends/starts, or when the Virus Scan Provider is deactivated/activated. 1 for test environments. Advantage: the configuration is read hourly, without having to end the servlet engine.
Max Instances	The maximum scan instances allowed to the VSA by NetWeaver. Default: 10.
Adapter Path	Complete path to the storage location of the adapter, as specified in Installing a Virus Scan Server as a Self-Starter – Page 41. If you leave this field empty, the environment variable VSA_LIB is set.

- ▶ To save your entries, press **Set**.

You do not have to make any configuration on the **Parameters** and **Trace** tab at this point.

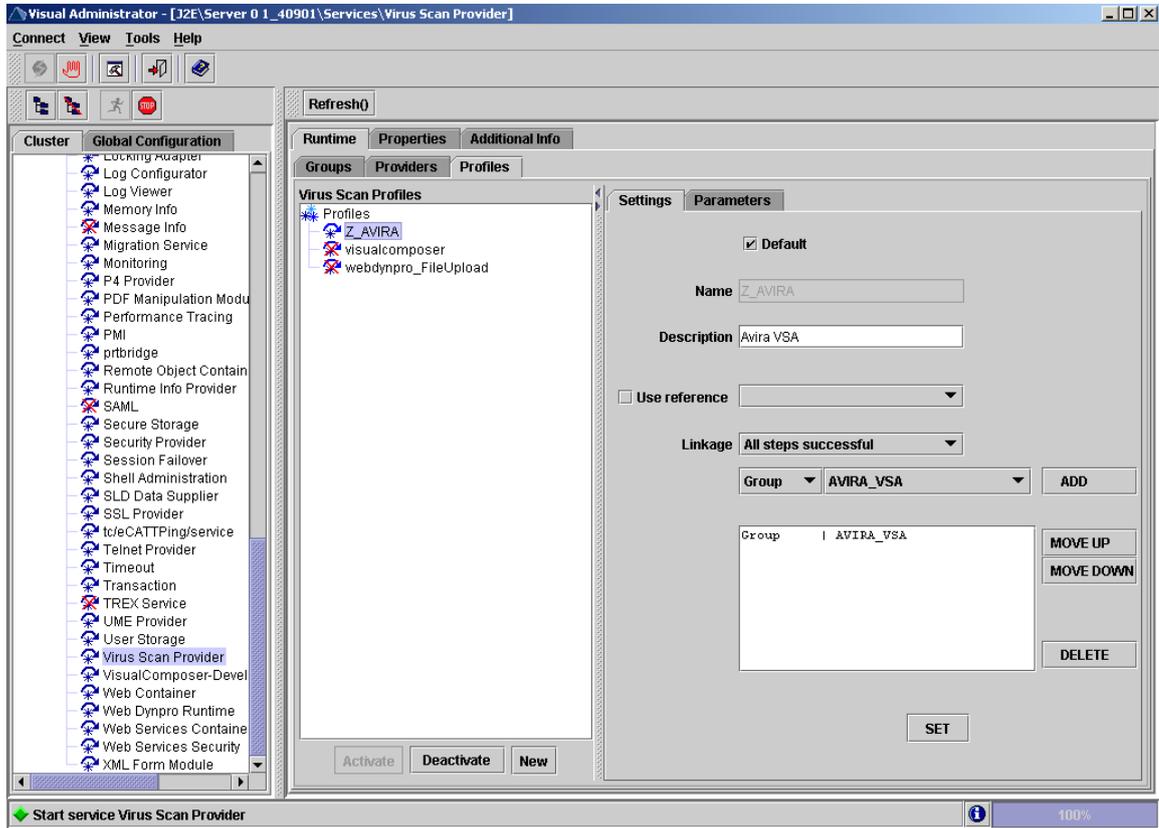
- ▶ To activate the virus scan provider, select it and choose **Activate**. It will be marked as active.



You have defined a virus scan provider and can define virus scan profiles in the next step.

8.1.3 Define a Virus Scan Profile

- ▶ In the Visual Administrator, choose the cluster **Virus Scan Provider**.
- ▶ On the **Profiles** tab, create a new virus scan profile by choosing the **New** button.
- ▶ Type the name for the new profile (AVIRA). The name entered is automatically saved with the prefix “Z_”.
- ▶ Select the new profile.



- ▶ On the **Settings** tab, activate the **Default** option, to set the profile as default and eventually adjust the values described in the table below.

Data for a Self-Configured Profile

Field	Comment
Default	When activated, the profile will be automatically selected.
Name	Name of the new profile
Description	Description of the new profile
Use reference	<p>Leave this inactive. When activated, the other input fields would be hidden.</p> <p>Since a virus scan profile can use another virus scan profile as a reference profile, it is possible to operate multiple applications using the same virus scan profile. To create a link to an existing reference profile, proceed as follows:</p> <ul style="list-style-type: none"> ▶ Activate the option Use reference. ▶ Select a reference profile from the drop down list.

Field	Comment
Linkage	<p>Linkage of the steps of this profile:</p> <p>All steps successful: AND linkage, with which every step must be successful for the overall result to be successful. (Default)</p> <p>At least one Step successful: OR linkage, with which only one step needs to be successful for the overall result to be successful.</p>
Group	Use the drop down list to select a group

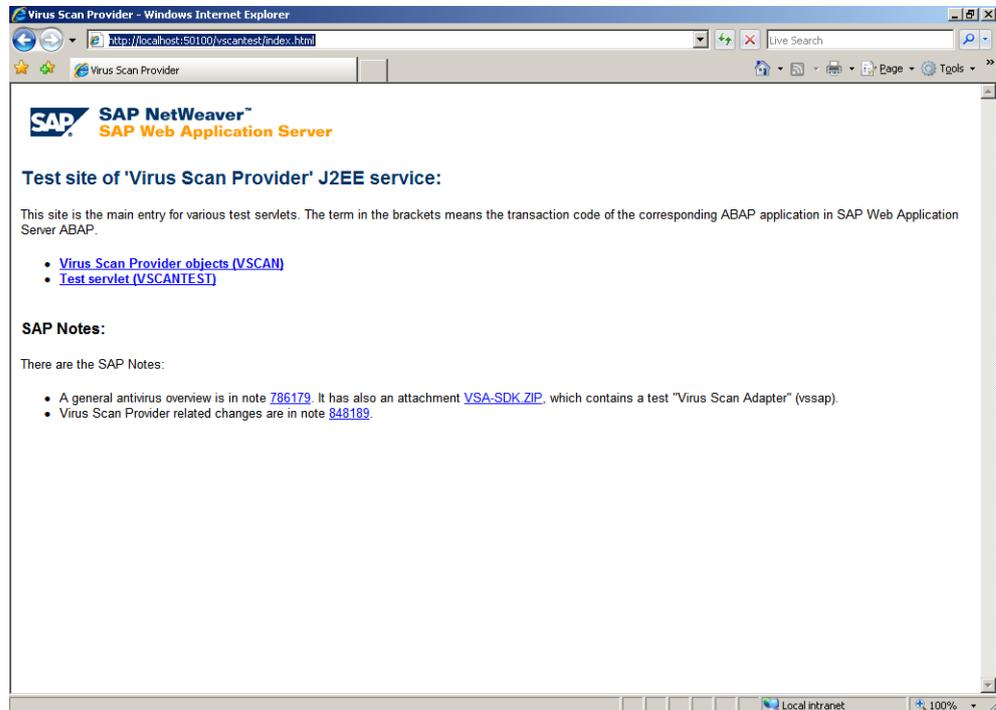
- ▶ To transfer the selection for the **Group** fields, choose **Add**.
- ▶ Configure the list with the buttons **MOVE UP**, **MOVE DOWN** and **DELETE**. When checking for viruses, the list is processed from top to bottom with the linkage from the **Linkage** field.
- ▶ To save the profile, press **Set**.
- ▶ To activate the profile, select it and choose **Activate**.

You have defined a virus scan profile and therefore performed the last configuration step for the virus scan provider. Finally you can check the configuration (see [Check the Configuration](#) – Page 64).

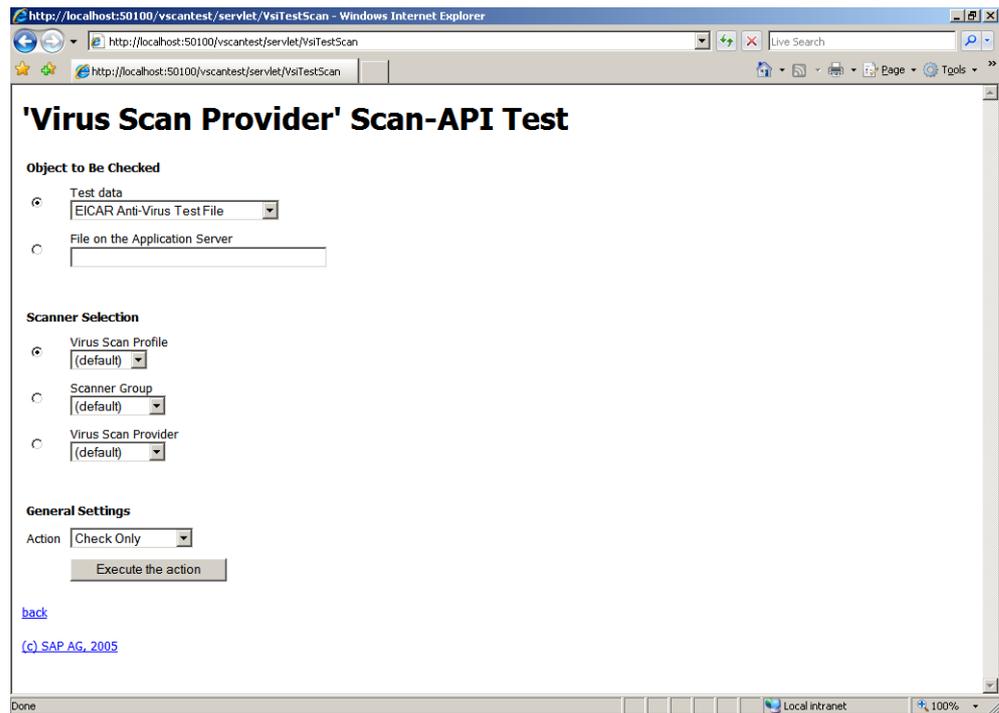
8.1.4 Check the Configuration

You can use the test applet provided by SAP NetWeaver, to check the functionality of the Virus Scan Service.

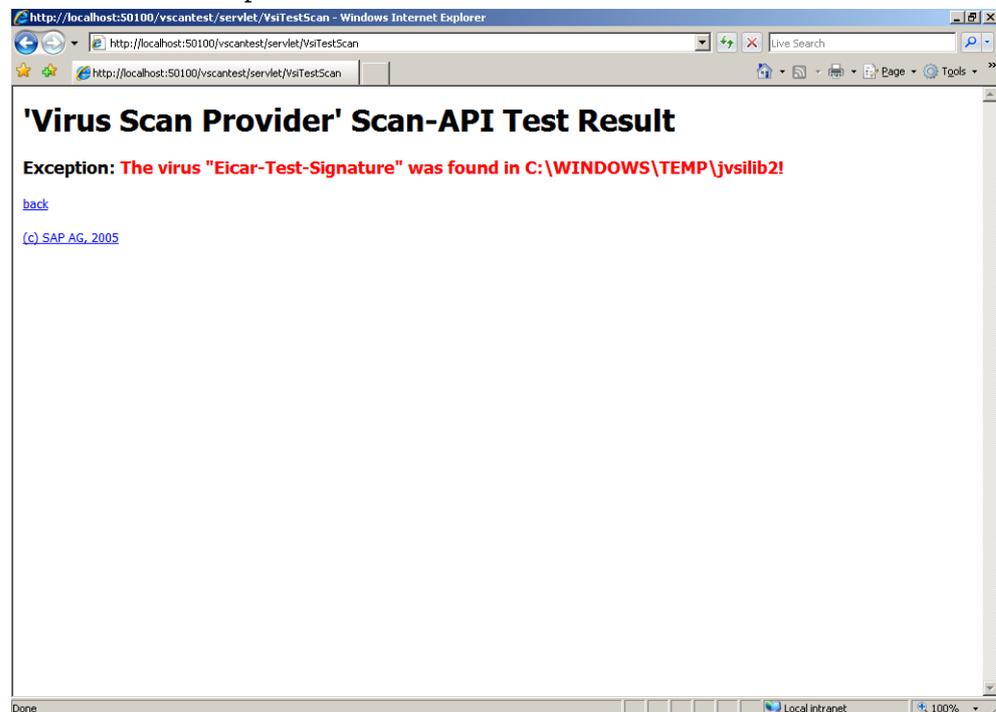
- ▶ Open an Internet browser and type the following address:
[http://\[server IP address\]:\[port\]/vscantest](http://[server IP address]:[port]/vscantest)



- ▶ Click the link to **Test servlet**.

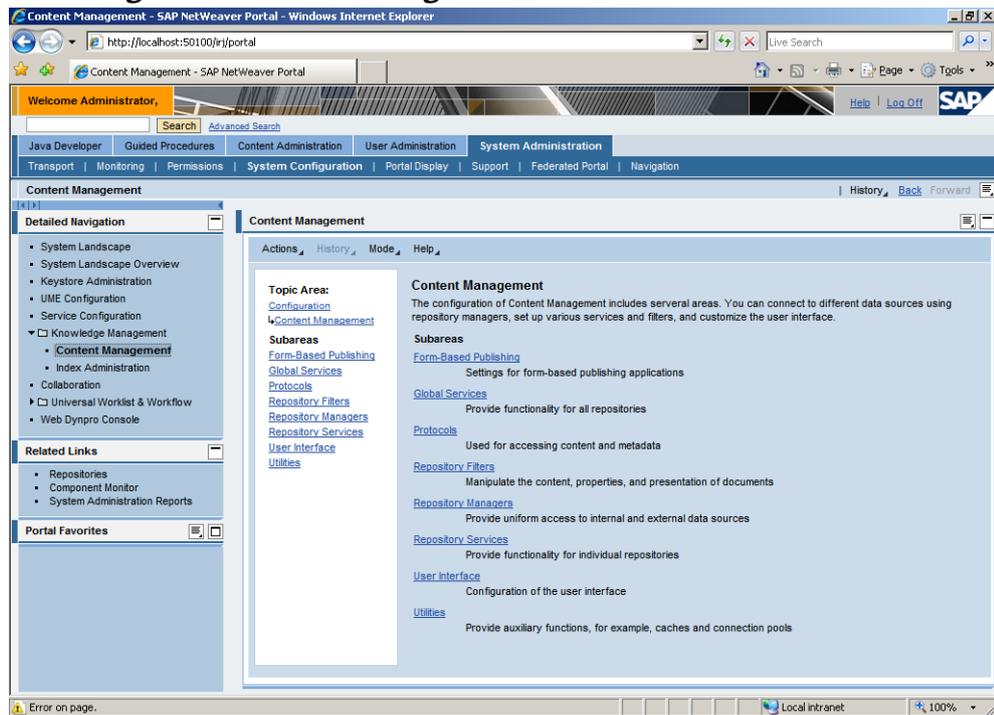


- ▶ Select the EICAR Anti-Virus Test File under **Object to Be Checked**.
- ▶ Select the (default) profile under **Scanner Selection**.
- ▶ Leave selected the option Check Only under **General Settings**.
- ▶ Press the button **Execute the action**.
- ↳ The test should report the detection of the EICAR test file.

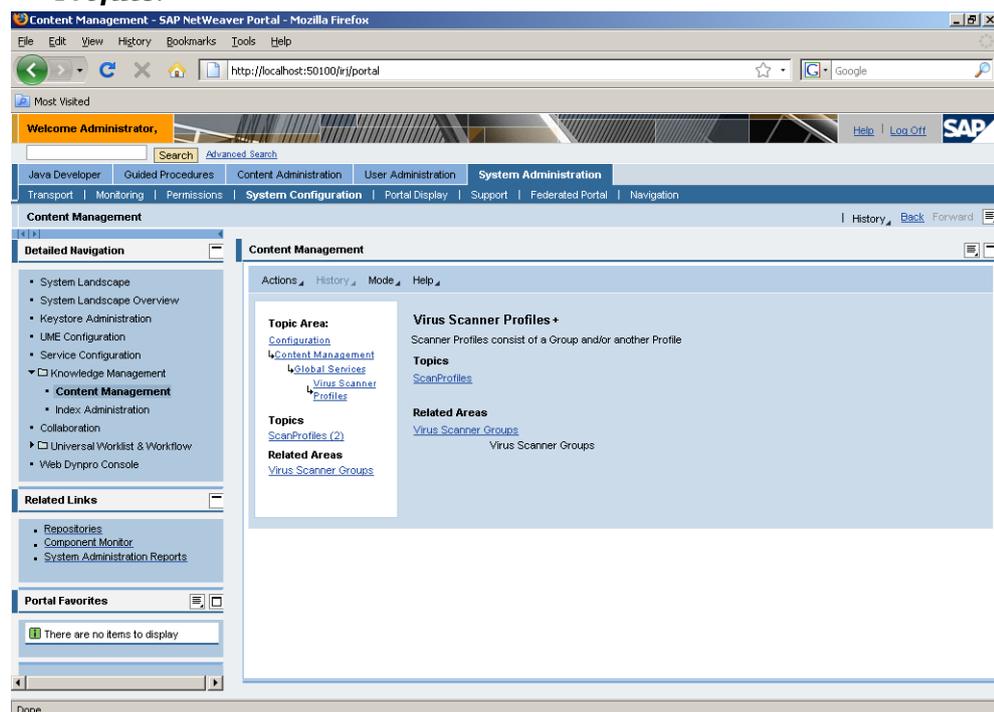


8.2 Integration with the Enterprise Portal and the Knowledge Management Center

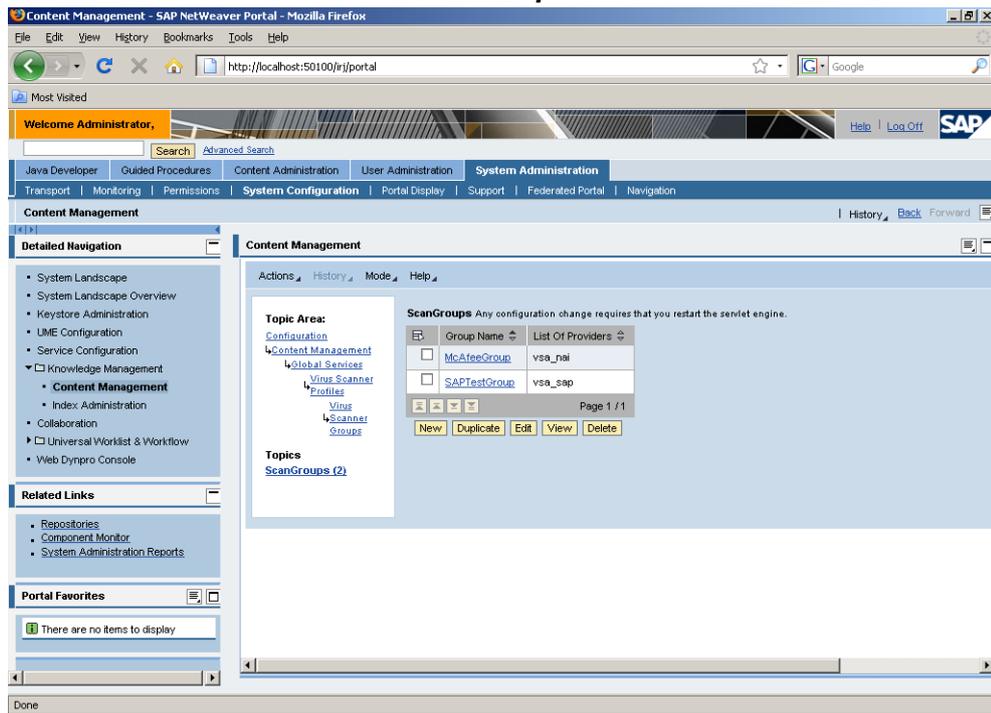
- ▶ Open an Internet browser and connect to the SAP NetWeaver Portal as administrator.
- ▶ Go to the menu **System Administrator/ System Configuration**.
- ▶ On the left panel, select under **Detailed Navigation** the item **Knowledge Management/ Content Management**.



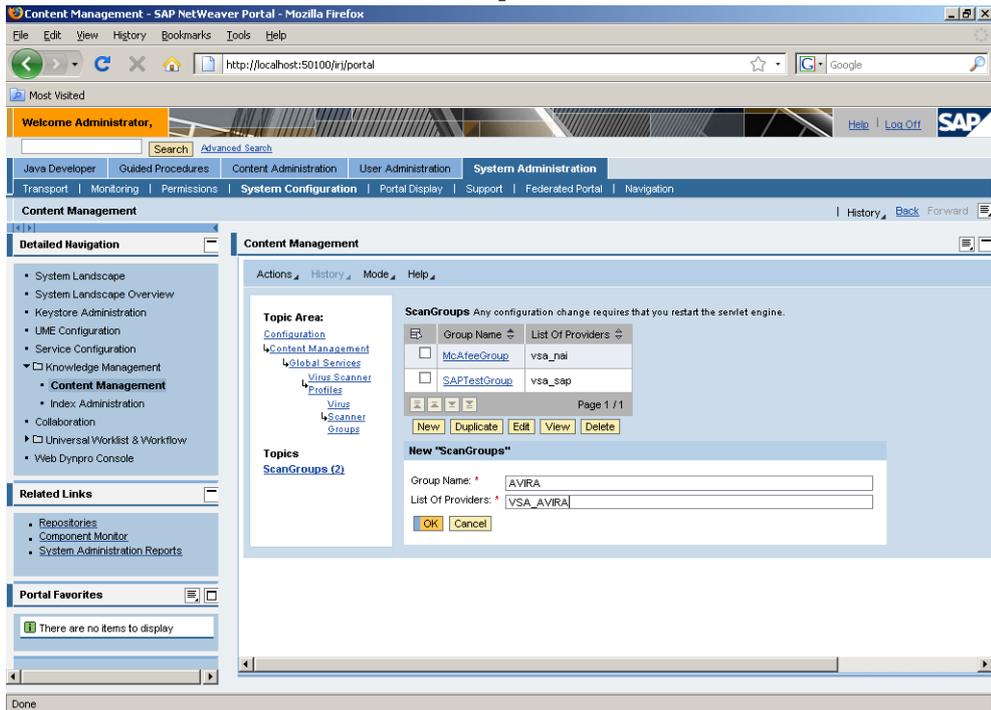
- ▶ On the right panel, go to the **Mode** menu and select **Advanced**.
- ▶ Under **Topic Area**, select **Global Services**, then scroll down and select **Virus Scanner Profiles**.



► Click on the link to **Virus Scanner Groups**.



► Press **New** to create a new Scan Group.

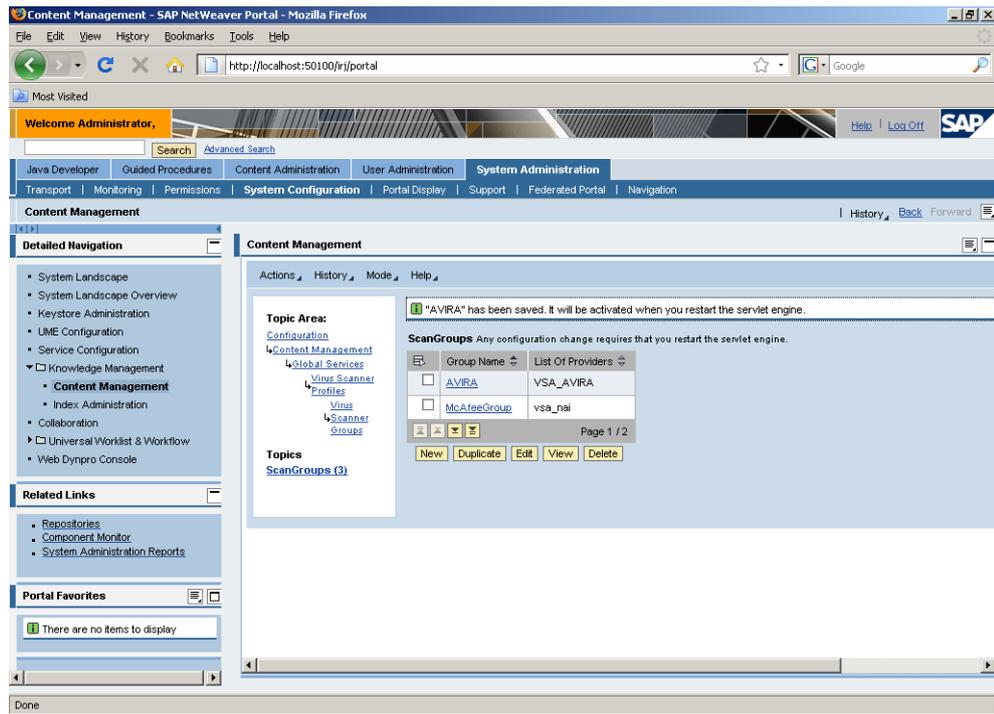


► In the field **Group Name** write AVIRA and in the **List of Providers** write VSA_AVIRA.

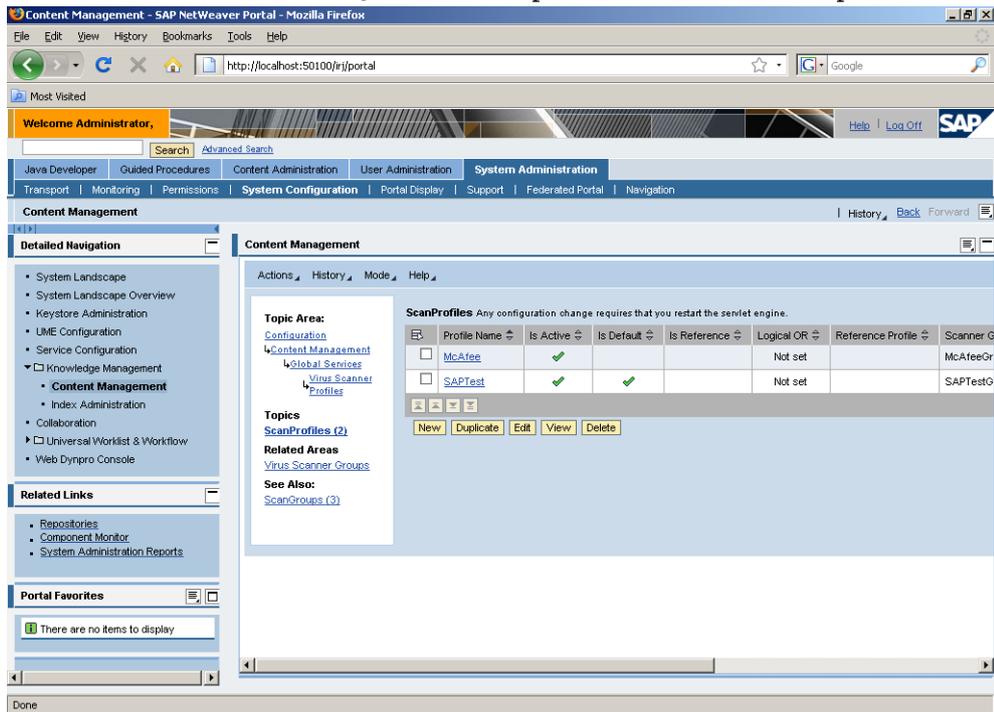


The values are case sensitive. You have to use the same names as in the Visual Administrator.

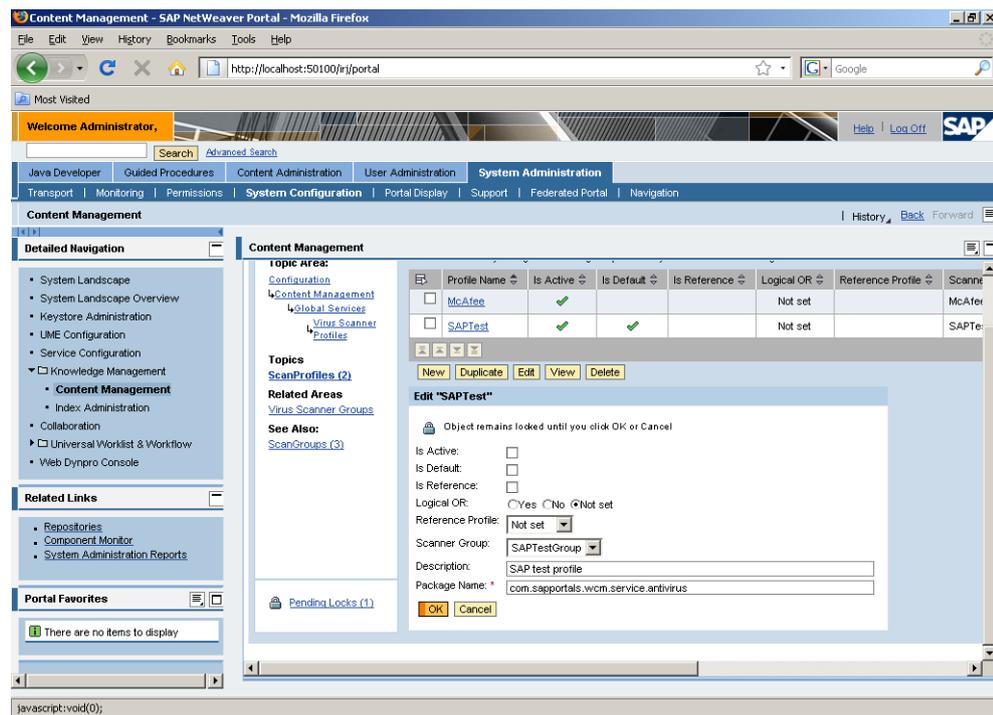
► Press **OK**.



► Select **Virus Scanner Profiles** in the Topic Area, to return to the profiles list.

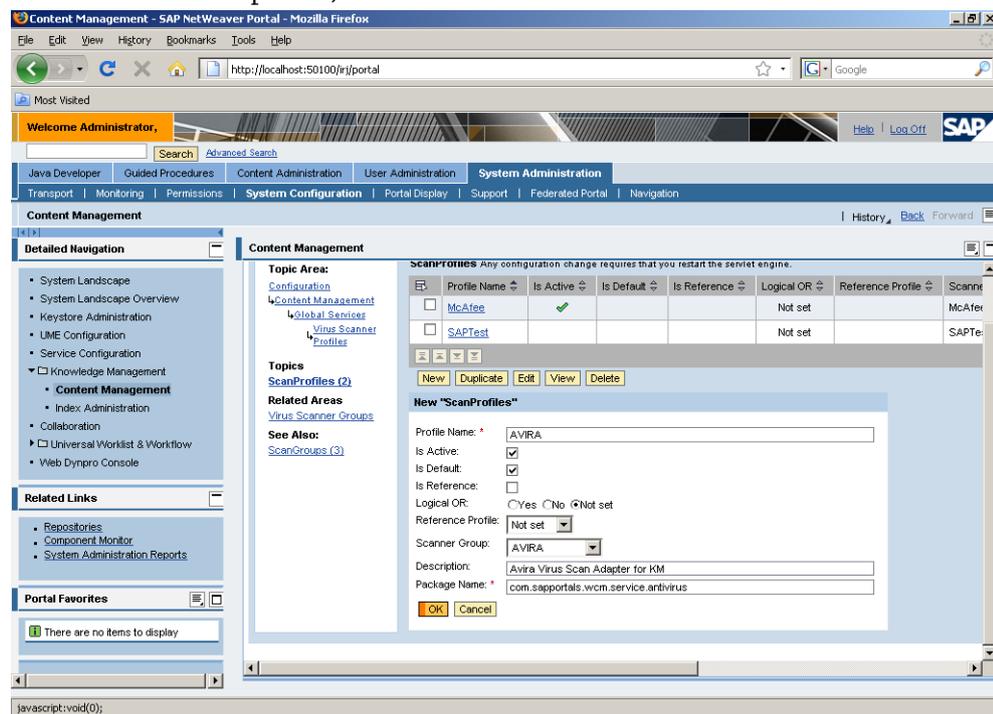


- ▶ Activate the checkbox in front of SAPTest and click Edit.



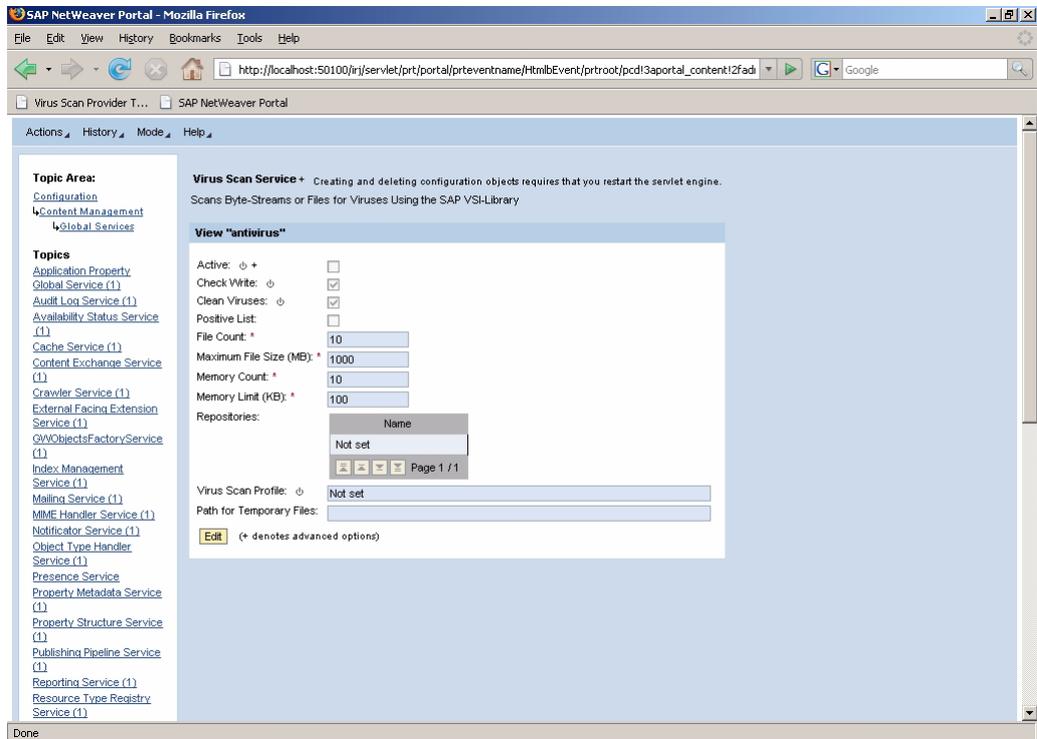
- ▶ Deselect the checkbox for the option **Is Default** and press **OK**.

- ▶ To create a new profile, click **New**.

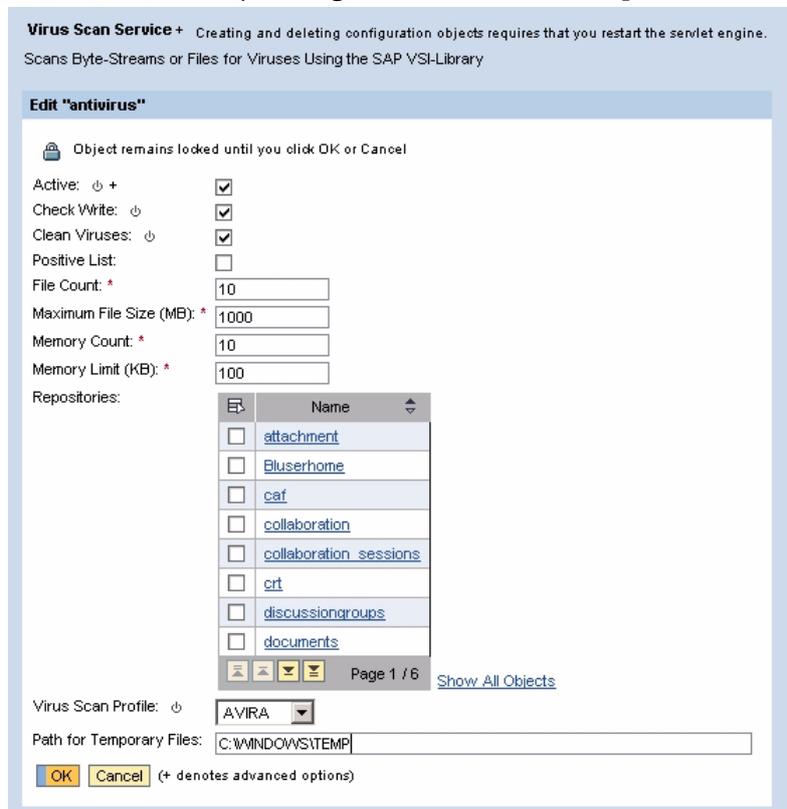


- ▶ In the field **Profile Name** write AVIRA.
- ▶ Select the checkboxes for the options **Is Active** and **Is Default**.
- ▶ The option **Is Reference** must remain inactive.
- ▶ For the option **Logical OR** activate the value **Not set**.
- ▶ **Reference Profile** must remain **Not set**.
- ▶ From the **Scanner Group** drop down list select AVIRA.
- ▶ The field **Description** is optional.

- ▶ Type in the **Package Name**: `com.sapportals.wcm.service.antivirus`
- ▶ Press **OK** to save the profile.
- ▶ To activate the Virus Scan Service, return to the Topic Area, select **Global Services** and click **Edit**.



- ▶ Make the necessary settings (see table below) and press **OK**.



- ▶ Restart the servlet engine, to activate the settings.

Option	Description
Active	Select the checkbox to activate the Virus Scan Service in KMC.
Check Write	Specifies if the virus scan should occur only at download, or at upload, too.
Clean Viruses	When active, the antivirus tries to clean infected files.
Positive List	When active, the virus scanner checks ONLY the selected repositories. Otherwise, the scanner checks all repositories, EXCEPT the selected ones.
File Count	Maximum number of files to be scanned simultaneously. (default: 10)
Maximum File Size (MB)	Maximum size of the files to be scanned. Bigger files cannot be loaded in the Knowledge Management, for safety reasons. It depends on the File Count and Path for Temporary Files . For example, if you set the maximum size to 1000 MB and the File Count is 10, the temp directory should be 10 GB.
Memory Count	Sets the number of memory blocks available to the scanner. Default: 10.
Memory Limit (KB)	Sets the maximum size of the memory space allowed for the files being scanned. Default: 1000.
Repositories	When Positive List is active, the virus scanner checks ONLY the selected repositories. Otherwise, the scanner checks all repositories, EXCEPT the selected ones.
Virus Scan Profile	Select the profile to be used (AVIRA).
Path for Temporary Files	Specifies the temporary folder for the files to be scanned (C:\Windows\Temp). If this option is left empty, the default value of the Java engine is used (<i>java.io.tmpdir</i>).

9 Operation

9.1 Reaction to Viruses/ Unwanted Programs Detected

If correctly configured, AntiVir has automatically completed all important tasks on your computer.

In the case of detection of viruses or unwanted programs, you should do the following:

- ▶ Try to detect the way the virus/ unwanted program infiltrated your system.
- ▶ Perform targeted scanning on the data storage supports you used.
- ▶ Inform your team, superiors or partners.

Submit Infected Files to Avira GmbH

- ▶ Please send us the viruses, unwanted programs and suspicious files that our product does not yet recognize or detect and also any suspicious files. Send us the virus or unwanted program packed in a password-protected archive (PGP, gzip, WinZIP, PKZip, Arj), attached to an email message, to virus@avira.com.



When packing, use the password `virus`. In this way the file will not be deleted by virus scanners on an email gateway.

10 Service

10.1 Support

Support Service Our website <http://www.avira.com> contains all the necessary information on our extensive support service.

The expertise and experience of our developers is available to you. The experts of Avira answer your questions and help you with difficult technical problems.

During the first 30 days after you have purchased a license, you can use our AntiVir Installation Support by phone, email or by online form.

In addition we recommend that you also purchase our AntiVir Classic Support, with which you can contact and obtain advice from our experts during business hours when you encounter technical problems. The annual fee for this service, which includes eliminating viruses and hoax support, is 20 % of the list price of your purchased AntiVir program.

Another optional service is the AntiVir Premium Support which, in addition to the scope of the AntiVir Classic Supports, allows you to contact expert partners at any time - even outside business hours in the event of an emergency. When virus alerts occur, you will receive an SMS on your cell phone.

Email Support Support via email can be obtained at <http://www.avira.com>.



We cannot provide support for configuration problems which do not directly concern AntiVir VSA.

To answer your questions or to solve your problems, we can direct you to an SAP consultant with technical security know-how.

10.2 Contact

Address Avira GmbH
Lindauer Strasse 21
D-88069 Tettngang
Germany

Internet You can find further information on us and our products by visiting <http://www.avira.com>.

11 Appendix

11.1 Glossary

Item	Meaning
ABAP	Advanced Business Application Language: the SAP programming language, for application logic.
Backdoor (BDC)	A backdoor is a program that infiltrates the system in order to steal data from the computer without the user's knowledge. This program is manipulated by third parties using remote backdoor control software via the Internet or network.
CCMS	Computing Center Management System
cron (daemon)	A daemon which starts other programs at specified times.
Daemon	A background process for administration on UNIX systems. On average, there are about a dozen daemons running on a computer. These processes usually start up and shut down with the computer.
Dialer	Paid dialing program. When installed on your computer, this program sets up a premium rate number Internet connection, charging you at high rates. This can lead to huge phone bills. AntiVir detects Dialers.
Engine	The scanning module of AntiVir software.
Heuristics	The systematic process of solving a problem using general and specific rules drawn from previous experience. However, solution is not guaranteed. AntiVir uses a heuristic process to detect unknown macro viruses. When typical virus-like functions are found, the respective macro is classified as "suspicious".
Kernel	The basic component of a UNIX operating system, which performs elementary functions (e.g. memory and process administration).
Logfile	also: Report file. A file containing reports generated by the program during run-time when a certain event occurs.
Malware	Generic term for "foreign bodies" of any type. These can be interferences such as viruses or other software which the user generally considers as unwanted (see also Unwanted Programs).
PMS (Possibly Malicious Software)	Software that does not usually harm the computer. It is programmed to harm other users. For example, mail bombs: with such a program, the victim can be attacked by thousands of emails. AntiVir detects PMS.
root	The user with unlimited access rights (such as system administrator on Windows).

Item	Meaning
SAVAPI	Secure AntiVirus Application Programming Interface: AntiVir SAVAPI ensures quick and simple integration of the latest Avira technology for detection and protection against malware in third-party programs and applications.
Signature	A bytes-combination used to recognize a virus or unwanted program.
Script	A text file containing commands to be executed by the system (similar to batch files in DOS).
SMP (Symmetric Multi Processing)	Computer architecture with multiple similar CPUs working in parallel.
SMTP	Simple Mail Transfer Protocol: protocol for email communication on the Internet.
syslog daemon	A daemon used by programs for logging various information. These reports are written in different logfiles. The syslog daemon configuration is in <i>/etc/syslog.conf</i> .
Unwanted programs	The name for programs that do not directly harm the computer, but are not wanted by the user or administrator. These can be backdoors, dialers, jokes and games. AntiVir detects various types of unwanted programs.
VDF (Virus Definition File)	A file with known signatures for viruses and unwanted programs. In many cases it is sufficient for an update to load the most recent version of this file.
VFS	Virtual File System

11.2 Further Information

You can find further information on viruses, worms, macro viruses and other unwanted programs at <http://www.avira.com> .

11.3 Golden Rules for Protection Against Viruses

- ▶ Always keep boot disks for your network server and for your workstations.
- ▶ Always remove floppy disks from the drive after finishing work. Even if they have no executable programs, disks can contain program code in the boot sector and these can serve to carry boot sector viruses.
- ▶ Regularly back up your files.
- ▶ Limit program exchange: particularly with other networks, mailboxes, the Internet and acquaintances.
- ▶ Scan new programs before installation and the disk after this. If the program is archived, you can detect a virus only after unpacking and during installation.

If there are other users connected to your computer, you should define the following rules for protection against viruses:

- ▶ Use a test computer to check downloads of new software, demo versions or virus-suspicious media (floppies, CD-R, CD-RW, removable drives).
- ▶ Disconnect the test computer from the network!
- ▶ Appoint a person responsible for virus infection operations and establish all steps for virus elimination.
- ▶ Draw up an emergency plan as a precaution for preventing damage due to destruction, theft, failure or loss/change due to incompatibility. You can replace programs and storage devices, but not your vital business data.
- ▶ Draw up a plan for data protection and recovery.
- ▶ Your network must be correctly configured and the access rights must be wisely assigned. This represents good protection against viruses.



Avira GmbH

Lindauer Str. 21
88069 Tettnang
Germany
Telephone: +49 (0) 7542-500 0
Fax: +49 (0) 7542-525 10
Internet: <http://www.avira.com>

© Avira GmbH. All rights reserved.

This manual was created with great care. However, errors in design and contents cannot be excluded. The reproduction of this publication or parts thereof in any form is prohibited without previous written consent from Avira GmbH.

Errors and technical subject to change.

Issued Q4-2008

AntiVir[®] is a registered trademark of the Avira GmbH.

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. However, this does not mean that they may be used freely.