



Handbuch für Anwender

Avira AntiVir Virus Scan Adapter für SAP NetWeaver[®]

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

Inhaltsverzeichnis

Kapitel 1. Über dieses Handbuch	5
1.1 Einleitung	5
1.2 Aufbau des Handbuchs	5
1.3 Zeichen und Symbole	6
Kapitel 2. Produktinformationen	9
2.1 Lizenzierungskonzept	11
2.2 Funktionsweise von AntiVir VSA (Windows)	11
2.3 Systemvoraussetzungen	12
Kapitel 3. Installation	13
3.1 Installation von AntiVir VSA (UNIX)	13
3.1.1 Installationsdateien bereitstellen	13
3.1.2 Lizenzierung	14
3.1.3 AntiVir VSA installieren	14
3.1.4 AntiVir VSA erneut installieren	17
3.1.5 Hintergrund	17
3.2 Installation von AntiVir VSA (Windows)	18
3.2.1 Installationsdateien bereitstellen	18
3.2.2 Lizenzierung	18
3.2.3 AntiVir VSA installieren	18
3.2.4 Hintergrund	21
Kapitel 4. Konfiguration (UNIX)	23
4.1 Übersicht.....	23
4.2 Die Konfigurationsdateien	24
4.3 Konfigurationsskript configantivir	27
4.4 Konfigurieren regelmäßiger Updates.....	29
Kapitel 5. Konfiguration (Windows)	35
5.1 Mögliche Einträge in der Steuerdatei SAVAPI.INI	35
5.2 Möglicher Eintrag in der Steuerdatei SAVAPIDL.INI.....	38
5.3 Sofort-Updates	39
Kapitel 6. ABAP-spezifische Konfiguration	41
6.1 Viren-Scan-Schnittstelle einrichten	41
6.1.1 Scanner-Gruppen definieren	41
6.1.2 Virus Scan Server definieren	44
6.1.3 Viren-Scan-Profile definieren	53
6.1.4 BAdI für Viren-Scanner implementieren	59
6.2 Problemanalyse des Virus Scan Server	60
6.3 Installation des Virus Scan Server testen.....	62
6.4 Kommentiertes Beispielprogramm	63
Kapitel 7. Java-spezifische Konfiguration	65
Kapitel 8. Java-spezifische Konfiguration unter SAP NetWeaver 2004(s) und KMC	67
8.1 Konfiguration über den Visual Administrator.....	67
8.1.1 Scanner-Gruppen definieren	67
8.1.2 Virus Scan Provider definieren	70

8.1.3 Viren-Scan-Profile definieren	73
8.1.4 Konfiguration überprüfen	74
8.2 Einbindung mit Enterprise Portal und Knowledge Management Center	76
Kapitel 9. Bedienung	83
9.1 Vorgehen bei Fund eines Virus/unerwünschten Programms	83
Kapitel 10. Service	85
10.1 Support	85
10.2 Kontakt	85
Kapitel 11. Anhang	87
11.1 Glossar	87
11.2 Weitere Infoquellen	88
11.3 Goldene Regeln zur Virenvorsorge.....	89

1 Über dieses Handbuch

In diesem Kapitel erhalten Sie einen Überblick über Aufbau und Inhalt des Handbuchs. Nach einer kurzen Einleitung erhalten Sie Informationen zu folgenden Themen:

- [Aufbau des Handbuchs](#) – Seite 5
- [Zeichen und Symbole](#) – Seite 6

1.1 Einleitung

In diesem Handbuch haben wir für Sie alle nötigen Informationen zu AntiVir Virus Scan Adapter (for SAP Solutions) zusammengestellt und führen Sie Schritt für Schritt durch Installation, Konfiguration und Bedienung der Software.



Der vollständige Name des Programms lautet AntiVir Virus Scan Adapter (for SAP Solutions). Zur besseren Lesbarkeit wird dieser Name im gesamten Handbuch auf AntiVir VSA abgekürzt.



Wenn in diesem Handbuch von "Viren" gesprochen wird, so ist dies im Sinne von "Malware" als Überbegriff für Würmer, Trojaner, Hoaxes etc. zu verstehen.

Weitere Informationen und Hilfestellung bieten Ihnen darüber hinaus unsere Webseite, die Hotline unseres Technischen Supports und unser regelmäßiger Newsletter (siehe [Service](#) – Seite 85).

Ihr Team von Avira

1.2 Aufbau des Handbuchs

Das Handbuch zu Ihrer AntiVir VSA-Software besteht aus mehreren Kapiteln, in denen Sie folgende Informationen finden:

Kapitel	Inhalt
1 Über dieses Handbuch	Aufbau des Handbuchs, Zeichen und Symbole
2 Produktinformationen	Allgemeine Hinweise zur Software AntiVir VSA, zu Aufbau, Funktionsweise, Systemvoraussetzungen und Lizenzierung
3 Installation	Anleitung zur Installation von AntiVir VSA auf Ihrem System – unter UNIX sowohl Skript-basiert als auch über eine grafische Installationsroutine
4 Konfiguration (UNIX)	Anleitung zur optimalen Anpassung von AntiVir VSA auf Ihr UNIX-System
5 Konfiguration (Windows)	Anleitung zur optimalen Anpassung von AntiVir VSA auf Ihr Windows-System

Kapitel	Inhalt
6 ABAP-spezifische Konfiguration	Informationen zur ABAP-spezifischen Konfiguration von AntiVir VSA
7 Java-spezifische Konfiguration	Informationen zur Java-spezifischen Konfiguration von AntiVir VSA
8 Java-spezifische Konfiguration unter SAP NetWeaver 2004(s) und KMC	Konfiguration des Viren-Scanners auf Java Systemen über Visual Administrator; Einbindung mit dem Enterprise Portal und Knowledge Management Center
9 Bedienung	Verhalten beim Auffinden von Viren und unerwünschten Programmen
10 Service	Support und Service von Avira GmbH
11 Anhang	Glossar mit Erläuterungen zu Fachbegriffen und Abkürzungen, Goldene Regeln zur Virenvorsorge

1.3 Zeichen und Symbole

In diesem Handbuch werden folgende Zeichen und Symbole verwendet:

Symbol	Erläuterung
✓	... steht vor einer Voraussetzung, die vor dem Ausführen einer Handlung erfüllt sein muss
▶	... steht vor einem Handlungsschritt, den Sie ausführen
↳	... steht vor einem Ergebnis, das direkt aus der vorangehenden Handlung folgt
	... steht vor einer Warnung bei Gefahr von kritischem Datenverlust oder Schäden an der Hardware
	... steht vor einem Hinweis mit besonders wichtigen Informationen, z. B. zu den folgenden Handlungsschritten
	... steht vor einem Tipp, der das Verständnis und die Nutzung von AntiVir VSA erleichtert

Zur besseren Lesbarkeit und eindeutigen Kennzeichnung werden im Text außerdem folgende Hervorhebungen verwendet:

Hervorhebungen im Text	Erläuterung
Strg + Alt	Taste bzw. Tastenkombination
<code>/usr/lib/AntiVir/antivir</code>	Dateinamen und Pfadangaben
<code>ls usr/lib/AntiVir</code>	Eingaben des Anwenders
Komponente auswählen Alles Markieren	Elemente der Software-Oberfläche wie Menüpunkte, Fenstertitel, Schaltflächen in Dialogfenstern

Hervorhebungen im Text	Erläuterung
http://www.avira.com	URLs
Aufbau des Handbuchs – Seite 4	Querverweise innerhalb des Dokuments

2 Produktinformationen

AntiVir Virus Scan Adapter (for SAP Solutions) ist der weltweit erste und derzeit einzige von SAP zertifizierte Virens Scanner für SAP-Unternehmenslösungen. Er fügt sich in die Technologie-Plattform SAP NetWeaver ein, überwacht den Datenaustausch von SAP-Anwendungen über SAP Web Application Server und sichert sie vor Viren sowie unerwünschten Programmen.

So haben z. B. Unternehmen, über deren Webseite man sich online bewerben kann und die den Upload eines Lebenslaufs im MS-Word- oder PDF-Format ermöglichen, jetzt die Gewissheit, dass sich keine virulenten Objekte in der Datenbank befinden. Beliebige Dateien wie Tabellenkalkulations- oder Bilddateien, die von verschiedenen Mitarbeitern bearbeitet werden, können auf Malware überprüft werden, bevor sie "abgelegt" werden. Damit ist es möglich, Objekte sicher virenfrei abzulegen und diese wichtige Aufgabe nicht der Antiviren-Software auf dem Arbeitsrechner zu überlassen.

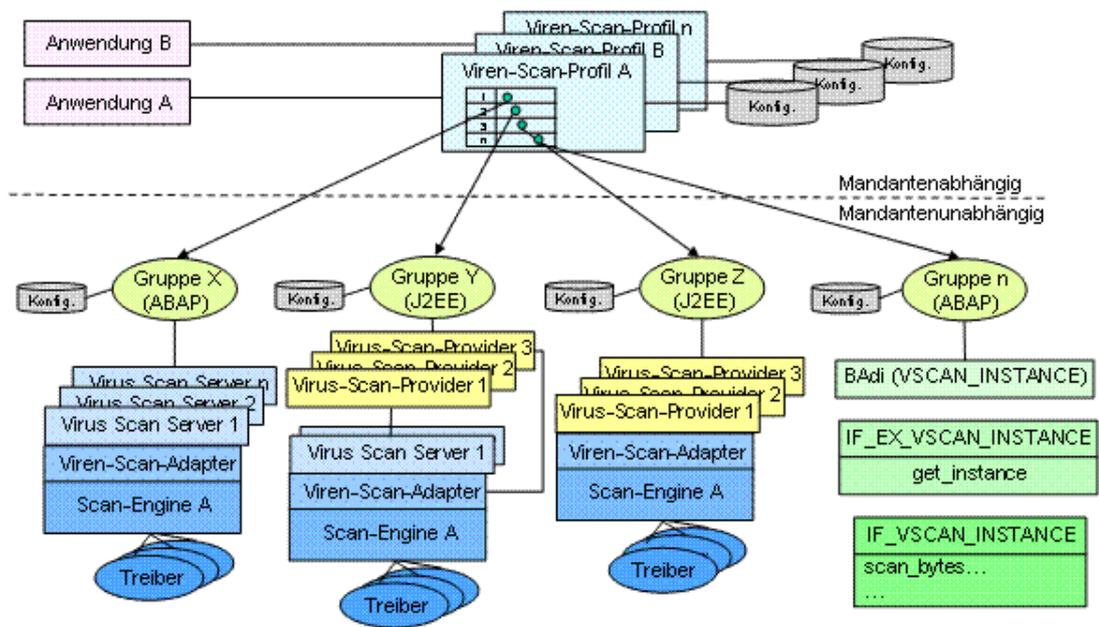
Automatische Internet Updates sorgen dafür, dass die Software immer auf dem aktuellsten Stand ist.

Mit der Viren-Scan-Schnittstelle binden Sie AntiVir VSA in das SAP-System ein, um die Sicherheit Ihres Systems zu erhöhen. Damit können Sie Dateien oder Dokumente, die von Anwendungen verarbeitet werden, mit einer performanten Integrationslösung auf Viren und unerwünschte Programme hin untersuchen. Dies gilt sowohl für von SAP ausgelieferte Anwendungen als auch für Ihre Eigenentwicklungen, z. B. bei Datenübertragungen über Netzwerke oder beim Dokumentenaustausch über Schnittstellen.

Die Schnittstelle besteht aus zwei Teilen:

- einem externen für die zertifizierten Antivirenprodukte der verschiedenen Hersteller und
- einem internen, mit dem Sie die Virensuchfunktionalität über ein Business Add-In in die eigenen Anwendungen integrieren können.

Die folgende Grafik zeigt eine integrierte ABAP-Java-Installation. Sie können die Viren-Scan-Schnittstelle jedoch auch für reine ABAP- oder Java-Installationen verwenden.



In der Grafik greift Anwendung A über das Viren-Scan-Profil A im ersten Schritt auf Gruppe X, im zweiten Schritt auf Gruppe Y und im dritten Schritt auf Gruppe Z zu. Dabei umfasst eine Gruppe jeweils die Antivirensoftware eines bestimmten Herstellers. Bei Gruppe X wird dabei einer der in der Gruppe enthaltenen von SAP ausgelieferten Virus Scan Server per Lastausgleich ausgewählt und greift über den zertifizierten Viren-Scan-Adapter des externen Herstellers auf dessen Antivirensoftware zu. Diese Software untersucht dann die von Anwendung A übergebenen Daten auf Viren. Bei Gruppe Y gibt es Virus Scan Provider mit und ohne Virus Scan Server, die alle über den zertifizierten Viren-Scan-Adapter des externen Herstellers auf dessen Antivirensoftware zugreifen. Bei Gruppe Z umfassen die Virus Scan Provider nur den zertifizierten Viren-Scan-Adapter des externen Herstellers, über den auf die Antivirensoftware zugegriffen wird.

Alternativ können Sie Ihre bisherige Virensuchlösung über ein Business Add-In (BAI) implementieren. Dies ist in der Grafik in Gruppe n dargestellt, auf die ebenfalls über ein Viren-Scan-Profil zugegriffen wird.

2.1 Lizenzierungskonzept

Um AntiVir VSA zu nutzen, benötigen Sie eine Lizenz. Sie erkennen damit die Lizenzbedingungen an (siehe http://www.avira.com/documents/general/pdf/de/avira_eula_de.pdf)

Die Lizenz wird über die Lizenzdatei *hbedv.key* vergeben. Diese erhalten Sie von Avira GmbH per Email. Sie enthält genaue Angaben, welche Programme Sie für welchen Zeitraum lizenziert haben. Sie kann also auch die Lizenz für mehrere Produkte von Avira GmbH enthalten.

Zum Leistungsumfang einer Vollversion gehören:

- Bereitstellung der AntiVir VSA-Version zum Download aus dem Internet
- Lizenzdatei per Email
- Ausführliche Installationsanleitung (digital)
- Bereitstellung von PDF-Handbüchern zum Download aus dem Internet
- Vierwöchiger Installationssupport ab Kaufdatum
- Newsletter-Service (per Email)
- Update-Service der Programmdateien und der VDF per Internet

2.2 Funktionsweise von AntiVir VSA (Windows)

Das Schutzpaket AntiVir VSA besteht aus 2 Teilen:

- AntiVir Savapi:
 - Savapi-Service: Stellt die eigentliche Scan- und Reparatur-Funktionalität bereit.
 - Savapi-Update-Service: Stellt über Ihre Internetverbindung sicher, dass AntiVir VSA immer auf dem neuesten Stand ist. Er prüft, ob Updates verfügbar sind, und aktualisiert ggf. Ihre Software automatisch.
- AntiVir Virus Scan Adapter (VSA):
Schnittstelle zu SAP, entspricht der Datei *ANTIVIRVSA.DLL*.



Sie können die *ANTIVIRVSA.DLL* auch an eine andere Stelle kopieren. In der SAP-Benutzeroberfläche müssen Sie dann entweder den absoluten Pfad angeben, wo sich der Adapter befindet, oder die Umgebungsvariable *VSA_LIB* anpassen.

2.3 Systemvoraussetzungen

AntiVir VSA stellt für einen erfolgreichen Einsatz folgende Mindestanforderungen an die Computer, auf denen es installiert werden soll:

SAP

- SAP NetWeaver 6.40 mit Support Package 7 oder höher;
- für ABAP Engine mit dem SAP_BASIS 640 Support Package 11 oder höher;
- für die J2EE Engine mit dem Support Package 13 oder höher;
- SAP NetWeaver 2004s (7.0).

UNIX

- Hardware: UNIX Pentium III 500 MHz;
- 256 RAM;
- 512 MB Festplattenspeicher;
- Betriebssysteme: UNIX glibc-2.2.5 und höher.
- Die folgenden Distributionen sind offiziell unterstützt:
 - 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: Solaris UltraSparc Iii 650 MHz;
- 768 MB RAM;
- 512 MB Festplattenspeicher;
- Betriebssysteme: Sun Solaris 8, 9, 10.

Windows

- Hardware: Pentium III 500 MHz;
- 256 RAM;
- 20 MB Festplattenspeicher;
- Betriebssysteme:
 - Windows 2000 Professional, SP3 empfohlen;
 - Windows 2000 Server, SP3 empfohlen;
 - Windows 2000 Advanced Server, SP3 empfohlen;
 - Windows 2003 Server;
 - Windows Server 2008;
 - Windows XP Pro;
 - Windows Vista (32 Bit).
- Administratorrechte für die Installation.

3 Installation

In diesem Kapitel wird die Installation für UNIX- und für Windows-Systeme beschrieben:

- [Installation von AntiVir VSA \(UNIX\)](#) – Seite 13
- [Installation von AntiVir VSA \(Windows\)](#) – Seite 18

3.1 Installation von AntiVir VSA (UNIX)

Die aktuelle Version von AntiVir VSA (UNIX) ist im Internet verfügbar oder auf der AntiVir-CD-ROM.

AntiVir VSA wird als gepacktes Archiv zur Verfügung gestellt.

Sie werden Schritt für Schritt durch die Installation geführt. Dieses Kapitel ist untergliedert in folgende Abschnitte:

- [Installationsdateien bereitstellen](#) – Seite 13
- [Lizenzierung](#) – Seite 14
- [AntiVir VSA installieren](#) – Seite 14
- [AntiVir VSA erneut installieren](#) – Seite 17

3.1.1 Installationsdateien bereitstellen

Programmdatei aus dem Internet laden

- ▶ Laden Sie die aktuelle Datei von unserer Webseite <http://www.avira.com> auf Ihren lokalen Rechner. Zurzeit heißt diese Datei *antivir-vsa-prof-<version>.tar.gz*.
- ▶ Legen Sie die Datei in einem Verzeichnis Ihrer Wahl auf dem Computer ab, auf dem AntiVir VSA laufen soll, z. B. unter */tmp*.

Programmdatei von CD-ROM laden

- ▶ Wählen Sie auf Ihrer CD-ROM den Ordner */de/products/vsa/unix*.
- ▶ Kopieren Sie die Datei *antivir-vsa-prof-<version>.tar.gz* in ein Verzeichnis, z. B. nach */tmp*.

Programmdatei entpacken

- ▶ Wechseln Sie in das temporäre Verzeichnis:
`cd /tmp`
- ▶ Entpacken Sie die Archivdatei für das AntiVir-Paket:
`tar -xzvf antivir-vsa-prof-<version>.tar.gz`
 - ↳ Ein Verzeichnis *antivir-vsa-prof-<version>* wird im temporären Verzeichnis angelegt.

3.1.2 Lizenzierung

Sie müssen AntiVir VSA lizenzieren, um es in vollem Umfang nutzen zu können (siehe [Lizenzierungskonzept](#) – Seite 11). Hierfür benötigen Sie eine Lizenzdatei *hbedv.key*.

Diese Lizenzdatei enthält Informationen zu Umfang und Dauer der Lizenz. Ohne Lizenzdatei läuft AntiVir VSA nicht, auch nicht mit reduziertem Leistungsumfang.

Lizenz erwerben

- ▶ Kontaktieren Sie uns telefonisch oder per Email (sales@avira.com), um eine gültige Lizenzdatei für AntiVir VSA zu erhalten.
 - ↳ Sie erhalten eine Lizenzdatei per Email zugesandt.

Lizenzdatei einspielen

- ▶ Kopieren Sie die Lizenzdatei *hbedv.key* in Ihr Installationsverzeichnis */tmp/antivir-vsa-prof-<version>*.



Sie können die Installation auch ohne Lizenzdatei durchführen, müssen dann die Lizenzdatei aber nachträglich in das AntiVir-Programmverzeichnis */usr/lib/AntiVir* kopieren. Ohne Lizenzdatei wird die Funktion von AntiVir VSA nicht verfügbar sein.

3.1.3 AntiVir VSA installieren

Die Installation von AntiVir VSA läuft weitgehend automatisch über ein Installationsskript ab. Dieses Skript führt folgende Aufgaben durch:

- Prüfen der Installationsdateien auf Vollständigkeit.
- Prüfen, ob Sie ausreichende Rechte zur Installation besitzen.
- Prüfen, inwieweit schon eine Version von AntiVir VSA auf dem Computer vorhanden ist.
- Kopieren der Programmdateien. Bereits vorhandene veraltete Dateien werden überschrieben.
- Kopieren der AntiVir-Konfigurationsdatei. Eine bereits vorhandene AntiVir-Konfigurationsdatei wird beibehalten.
- Optional Installieren des Internet Updater.
- Optional Konfigurieren eines automatischen Starts des Internet Updater beim Systemstart.

Installation vorbereiten

- ▶ Loggen Sie sich ein als **root**. Ansonsten haben Sie keine ausreichende Berechtigung für die Installation und das Skript bricht mit einer Fehlermeldung ab.
- ▶ Wechseln Sie in das Verzeichnis, in das Sie AntiVir VSA entpackt haben, also etwa:
`cd /tmp/antivir-vsa-prof-<version>`

AntiVir VSA installieren

- ▶ Geben Sie ein:
`./install`

Achten Sie auf den führenden Punkt und Schrägstrich. Ein Aufruf von "install" ohne diese Pfadangabe führt typischerweise zum Aufruf eines anderen, hier nicht zu involvierenden Kommandos und in der Folge zu Fehlermeldungen oder ungewollten

Aktivitäten. Der für den Lizenztext verwendete Dateibetrachter kann typischerweise mit der Taste 'q' verlassen werden.

- ↳ Das Installationsskript läuft an. Nach dem Akzeptieren der Lizenzbedingungen werden die Programmdateien kopiert. Optional übernimmt der Installer einen zuvor bereitgelegten Lizenzkey:

```
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
```

- ↳ Anschließend wird gefragt, ob der Internet Update Daemon installiert werden soll:

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

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



Der Internet Update Daemon ist nicht notwendig, um Updates zu erhalten. Sie können jederzeit mit AntiVir ein manuelles Update über das Internet starten. Für die Erstinstallation wird aber die Installation des Internet Update Daemons empfohlen. Sie können ihn später bei der Konfiguration wieder deaktivieren

Installation mit Updater

Wenn Sie den Internet Update Daemon installieren wollen (empfohlen):

- ▶ Geben Sie **Y** ein und drücken Sie **Enter**.

- ↳ Der Internet Update Daemon wird installiert. Anschließend werden Sie gefragt, ob der Daemon beim Systemstart automatisch gestartet werden soll:

```
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]
```

- ▶ Bestätigen Sie diese Frage mit **Y** oder **Enter**. Sie können diese Einstellung später wieder rückgängig machen.

- ↳ Der automatische Systemstart wird konfiguriert:

```
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
ohne Updater

Wenn Sie den Internet Update Daemon später oder gar nicht installieren wollen:

► Geben Sie **N** ein und drücken Sie **Enter**.

Installation
VSA library

↳ Anschließend wird die VSA library installiert:

```
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
```

Konfiguration
starten

↳ Danach haben Sie die Möglichkeit, AntiVir VSA zu konfigurieren:

```
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]
```



Wenn Sie hier mit **Y** bestätigen, wird das Konfigurationsskript für den AntiVir Updater gestartet. Die Konfiguration können Sie auch später jederzeit durchführen. Wir empfehlen, sich hierfür zunächst mit den Möglichkeiten der Konfiguration vertraut zu machen und die Konfiguration später durchzuführen.

► Brechen Sie mit **N** ab.

↳ Sie erhalten die Bestätigung, dass die Installation erfolgreich verlaufen ist:

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

↳ Eine abschließende Information über das weitere Vorgehen wird angezeigt:

```
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 AntiVir VSA erneut installieren

Sie können das Installationsskript jederzeit neu aufrufen. Hiermit sind folgende Vorgänge möglich:

- Installation einer neuen Version (Upgrade). Das Installationsskript prüft die bestehende Version und installiert notwendige neue Komponenten. Einstellungen, die Sie in der Konfigurationsdatei vorgenommen haben (siehe [Konfiguration \(UNIX\)](#) – Seite 23), werden dabei nicht überschrieben, sondern übernommen.
- Nachinstallation einzelner Komponenten, z. B. des Internet Update Daemon.
- Aktivierung oder Deaktivierung des automatischen Starts des Internet Update Daemon.

AntiVir VSA erneut installieren

Das Vorgehen ist für alle Fälle gleich:

- ▶ Wechseln Sie in das temporäre Verzeichnis, in das Sie AntiVir VSA entpackt haben, also etwa:

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

- ▶ Geben Sie ein:

```
./install
```

↳ Das Installationsskript läuft weitgehend ab wie in der Erstinstallation beschrieben (siehe [AntiVir VSA installieren](#) – Seite 14).

- ▶ Ändern Sie die entsprechenden Einstellungen während der Installation.

↳ AntiVir VSA ist mit den neuen Einstellungen installiert.

3.1.5 Hintergrund

Beachten Sie bei der Installation folgende Punkte:

- AntiVir VSA Library wird kopiert
- Die Umgebungsvariable `VSA_LIB` kann der Administrator selbst setzen (siehe System-Dok). Falls er das nicht tut, muss im SAP-Setup folgender Pfad eingetragen werden:
`/usr/lib/AntiVir/libantivirvsa.so.<version>`
- Das SAPCAR-Tool ist vom Administrator selbst in `/etc/avsapvsa.conf` einzutragen (siehe dort angegebenes Beispiel); ohne diesen Eintrag werden keine SAPCAR-Archive durchsucht:

```
SapCarProgram /usr/bin/SAPCAR
```

3.2 Installation von AntiVir VSA (Windows)

3.2.1 Installationsdateien bereitstellen

Programmdatei aus dem Internet laden

Auf unserer Webseite finden Sie die jeweils aktuelle Programmdatei für AntiVir VSA. Die liegt gepackt vor:

- im ZIP-Format (Entpackprogramm nötig, z. B. WinZip) oder
 - im EXE-Format als selbst entpackendes Archiv (kein zusätzliches Programm nötig)
- ▶ Laden Sie die aktuelle Programmdatei von unserer Webseite <http://www.avira.com> auf Ihren lokalen Rechner. Zurzeit heißt diese Datei *antivir_vsa_de.exe*.

Programmdatei von CD-ROM laden

- ▶ Wählen Sie auf Ihrer CD-ROM den Ordner
/de/products/vsa/windows
- ▶ Kopieren Sie die aktuelle Programmdatei auf ihren lokalen Rechner. Zurzeit heißt diese Datei *antivir_vsa_de.exe*.

3.2.2 Lizenzierung

Um AntiVir VSA nutzen zu können, benötigen Sie eine Lizenzdatei *hbedv.key* (siehe [Lizenzierungskonzept](#) – Seite 11). Diese Lizenzdatei enthält Informationen zu Umfang und Dauer der Lizenz.

Lizenz erwerben

- ▶ Kontaktieren Sie uns telefonisch oder per Email (sales@avira.com), um eine gültigen Lizenzdatei für AntiVir VSA zu erhalten.
- ↳ Sie erhalten eine Lizenzdatei per Email zugesandt.

3.2.3 AntiVir VSA installieren

- Voraussetzungen
- ▶ Beachten Sie folgende Voraussetzungen, um das einwandfreie Funktionieren der Software zu gewährleisten:
 - ✓ Stellen Sie sicher, dass die Systemvoraussetzungen erfüllt sind (siehe [Systemvoraussetzungen](#) – Seite 12).
 - ✓ Stellen Sie sicher, dass Sie als Administrator oder als Benutzer mit Administrator-Rechten angemeldet sind.
 - ✓ Stellen Sie sicher, dass eine Internetverbindung vorhanden ist und automatische Updates mit dem Internet Updater möglich sind.
 - ✓ Stellen Sie sicher, dass eine gültige Lizenzdatei *hbedv.key* vorhanden ist.
 - ▶ Wechseln Sie in das Verzeichnis, in das Sie die Programmdatei *antivir_vsa_de.exe* gespeichert haben.
 - ▶ Doppelklicken Sie auf die Datei *antivir_vsa_de.exe*.
 - ↳ Ein Dialogfenster erscheint, in dem das Setup gestartet werden kann.
 - ▶ Klicken Sie auf **Setup**.
 - ↳ Das Setup für AntiVir VSA startet.

↳ Das Dialogfenster **Willkommen** des InstallShield Wizard erscheint:



► Klicken Sie auf **Weiter**.

↳ Das Dialogfenster **Lizenzvereinbarung** erscheint:



Wenn Sie den Lizenzbestimmungen nicht zustimmen, kann das Setup nicht ausgeführt werden.

► Bestätigen Sie mit **Ja**.

↳ Das Dialogfenster **Zielpfad wählen** erscheint.

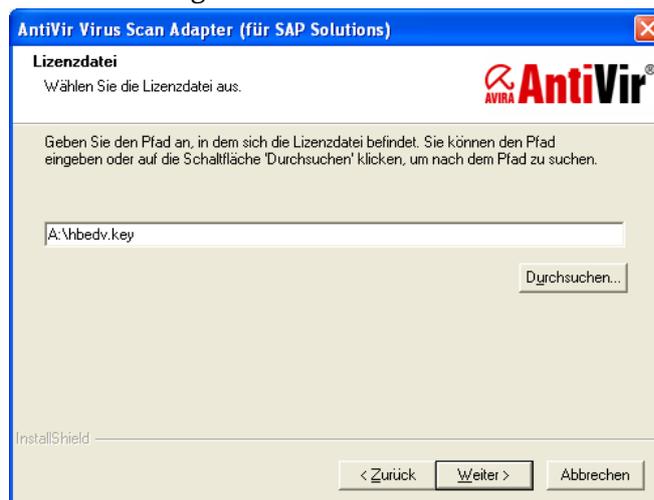


▶ Bestätigen Sie das angegebene Zielverzeichnis mit **Weiter**.

– ODER –

Wählen Sie mit **Durchsuchen** ein anderes Zielverzeichnis und bestätigen Sie mit **Weiter**.

↳ Das Dialogfenster **Lizenzdatei** erscheint:



▶ Wählen Sie das Verzeichnis, in dem die Lizenzdatei *hbedv.key* liegt, und bestätigen Sie mit **Weiter**.

↳ Das Dialogfenster **Install Shield Wizard abgeschlossen** erscheint.

▶ Klicken Sie auf **Fertigstellen**.

↳ Das Setup-Programm kopiert die Lizenzdatei, liest sie ein und installiert alle notwendigen Dateien im Zielverzeichnis.

↳ Die Installation von AntiVir VSA ist abgeschlossen. Ein Neustart Ihres Computers ist nicht notwendig.

3.2.4 Hintergrund

Während der Installation werden im Hintergrund folgende Operationen durchgeführt:

- Kopieren des eigentlichen Virus Scan Adapters (VSA) – Datei ANTIVIRVSA.DLL – in das Installationsverzeichnis.
- Setzen der Umgebungsvariablen VSA_LIB auf den absoluten Pfad des VSA, z. B. `VSA_LIB=C:\Program Files\Avira GmbH\AntiVir Savapi\ANTIVIRVSA.DLL`
- Suchen nach dem Tool, mit dem SAP-Archive (Format SAPCAR) entpackt werden können, d. h. die Umgebungsvariable PATH wird nach der Datei SAPCAR.EXE durchsucht.
- Setzen eines zusätzlichen Parameters in der SAVAPI.INI, der die SAPCAR-Archiv-Suche aktiviert, z. B.

`SapCarProgram= (leer -> kein SAPCAR.EXE gefunden)`

-oder-

`SapCarProgram=C:\SAPCAR\SAPCAR.EXE (Programm wurde gefunden)`

4 Konfiguration (UNIX)

Damit AntiVir VSA optimal auf Ihrem System läuft, müssen Sie es konfigurieren. Bereits im Anschluß an die Installation haben Sie die Möglichkeit, die wichtigsten Einstellungen vorzunehmen. Dabei werden Ihnen Einstellungen vorgeschlagen, die für viele Fälle sinnvoll sind.

Sie können jederzeit nachträglich diese Einstellungen ändern und so AntiVir VSA immer optimal anpassen.

Nach einer kurzen Übersicht werden Sie Schritt für Schritt in die Konfiguration eingeführt:

- Informationen über die Konfigurationsdateien erhalten Sie im Kapitel
 - [Parameter der Konfigurationsdatei avsapvsa.conf](#) – Seite 24 und
 - [Parameter der Konfigurationsdatei avupdater.conf](#) – Seite 26.Wenn Sie das Konfigurationsskript verwenden möchten, können Sie diesen Abschnitt überschlagen.
- Erklärungen zum allgemeinen Umgang mit dem Konfigurationsskript erhalten Sie im Kapitel [Konfigurationsskript configantivir](#) – Seite 27
- Spezifische Konfigurationen von AntiVir Updater werden erläutert in den Kapiteln
 - [Konfigurieren regelmäßiger Updates](#) – Seite 29

4.1 Übersicht

Konfigurationsdateien Die Konfigurationsdatei *avupdater.conf* definiert das automatische Update der Software; Datei *avsapvsa.conf* definiert Scan-Parameter und die Protokollierung beim Auftreten von Viren und unerwünschten Programmen.



Die Einstellungen werden direkt in der Konfigurationsdatei vorgenommen, was an sich nicht schwierig ist.

Die Updates können auch über ein im Programmpaket enthaltenes Konfigurationsskript vorgenommen werden, welches komfortabler ist, eventuelle Fehleingaben abfängt und falls notwendig betroffene Prozesse neu startet.

Konfigurationsskript Das Konfigurationsskript *configantivir* editiert die das Update betreffenden Einstellungen in *avupdater.conf*. Es befindet sich standardmäßig im Verzeichnis */usr/lib/AntiVir*.

4.2 Die Konfigurationsdateien

Dieser Abschnitt beschreibt den Aufbau der Konfigurationsdateien *avsapvsa.conf* und *avupdater.conf*. AntiVir VSA liest diese Dateien beim Programmstart ein. Leerzeilen und Zeilen, die mit # beginnen, werden ignoriert.

Bei Lieferung sind Werte eingestellt, die für viele Anwendungen sinnvoll sind. Einige Einträge sind durch ein vorgestelltes # deaktiviert (auskommentiert) und können durch Entfernen des # aktiviert werden.



Wenn Sie manuell Werte in *avupdater.conf* ändern, die den Internet Update Daemon betreffen, und nicht das Konfigurationsskript verwenden, müssen Sie anschließend den Internet Update Daemon manuell neu starten. Erst dann werden die Änderungen wirksam.

► Geben Sie dafür ein:

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

Parameter der Konfigurationsdatei *avsapvsa.conf*

Im Folgenden werden die Einträge in *avsapvsa.conf* kurz beschrieben. Diese Einträge beeinflussen das Verhalten des Scanners.

Viele der Einstellungen können auch über die SAP GUI konfiguriert werden und werden dann von SAP NetWeaver über den VSA an den eigentlichen Scanner übergeben. Die Einstellung eines solchen Parameters in der Datei *avsapvsa.conf* führt dazu, dass der Scanner zwar mit dem so eingestellten Wert startet, aber in der Folge sofort durch die Angaben aus der SAP GUI übersteuert wird. D.h. die bzgl AV-Scan in der SAP GUI vorgenommenen Einstellungen haben Vorrang gegenüber der *avsapvsa.conf* Konfigurationsdatei.

ArchiveScan	Archive prüfen: Bei der Einstellung 1 werden alle archivierten Dateien entpackt und geprüft. Bei der Einstellung 0 werden Archive nicht auf Viren und unerwünschte Programme geprüft (nicht empfohlen). ArchiveScan 1
ArchiveMax Size	Maximale Größe archivierter Dateien im entpackten Zustand: Bei der Einstellung 0 werden alle archivierten Dateien unabhängig von ihrer Größe entpackt. Bei einer Einstellung >0 werden alle Archive entpackt und geprüft, die die angegebene Größe (in Byte) nicht überschreiten. ArchiveMaxSize 1GB
ArchiveMax Recursion	Maximale Rekursionstiefe in Archiven: Bei der Einstellung 0 werden rekursive (verschachtelte) Archive unabhängig von ihrer Rekursionstiefe entpackt. Bei einer Einstellung >0 werden alle Archive entpackt, die die angegebene Rekursionstiefe nicht überschreiten. Dadurch wird die Verarbeitungszeit herabgesetzt. ArchiveMaxRecursion 20
ArchiveMax Ratio	„Mail-Bomben“ sperren: So genannte „Mail-Bomben“ mit einer sehr hohen Kompressionsrate können gesperrt werden. Sie können die maximale Differenz zwischen der gepackten und der entpackten Dateigröße festlegen. Die Einstellung 0 deaktiviert die Option (nicht empfehlenswert). Die Standardeinstellung lautet 150.

ArchiveMaxRatio 150

LogFile Logdatei:
Alle wichtigen Operationen von AntiVir werden über den *syslog*-Dämon protokolliert. Zusätzlich kann eine Logdatei geschrieben werden. Eine Voreinstellung gibt es nicht. Damit die Logdatei geschrieben werden kann, muss der volle Pfad zur Datei angegeben werden, z. B:
LogFile /var/log/avsapvsa.log

EmailTo Email-Nachrichten:
AntiVir kann Emails verschicken, wenn ein Virus oder unerwünschtes Programm entdeckt wird. Eine Voreinstellung gibt es nicht. Damit Emails verschickt werden können, muss also ein Adressat angegeben werden, z. B:
EmailTo root@localhost

Syslog... Syslog-Einstellung:
Für alle wichtigen Operationen gibt AntiVir Meldungen an den *syslog*-Dämon. Zusätzlich kann spezifiziert werden, welche Facility und Priorität diesen Meldungen mitgegeben wird. Voreingestellt sind:
SyslogFacility user
SyslogPriority notice
Diese Werte gelten auch, wenn die Einträge deaktiviert sind.

Detect... Erkennung weiterer unerwünschter Programme:
Neben Viren existieren noch andere Arten von Software, die Schaden anrichten können oder aus anderem Grund unerwünscht sind. Die Erkennung dieser Software kann mit folgenden Optionen aktiviert werden. Die Erkennung von Viren ist nicht optional und kann nicht deaktiviert werden.

Die Voreinstellungen sind:
DetectADSPY yes
DetectAPPL yes
DetectBDC yes
DetectDIAL yes
DetectGAME no
DetectHEUR-DBLEXT yes
DetectJOKE no
DetectPCK no
DetectPHISH yes
DetectSPR no

Heuristics Makrovirus-Heuristik:
Macro Diese Option aktiviert die Heuristik für Makroviren in Dokumenten.
HeuristicsMacro yes

Heuristics Win32-Heuristik:
Level Diese Option legt die Erkennungsstufe der Win32-Heuristik fest. Zulässige Werte sind 0 (Aus), 1 (Niedrig), 2 (Mittel) und 3 (Hoch).
HeuristicsLevel 0

SapCarProgram Unterstützung für CAR/SAR Archivformate:
Der AntiVir Virus Scan Adapter beinhaltet nativen Support für die gängigsten

Archivformate wie ZIP, CAB, TAR, etc. Zusätzlich können Archive mit dem SAP-spezifischen CAR/SAR-Format untersucht werden, wenn das externe "sapcar" Tool zur Verfügung steht. Mit dieser Option spezifizieren Sie den vollständigen Pfad zur Binärdatei dieses Tools. Eine Voreinstellung existiert nicht.

```
SapCarProgram /usr/local/bin/SAPCAR
```

Parameter der Konfigurationsdatei `avupdater.conf`

Im Folgenden werden die Einträge in `avupdater.conf` kurz beschrieben. Diese Einträge beeinflussen das Verhalten des Updaters. Diese Einträge können auch komfortabel über das [Konfigurationsskript configantivir](#) – Seite 27 vorgenommen werden, wobei dieses Script falls nötig betroffene Prozesse neu startet.

- AutoUpdate...** Update-Plan:
Die Software kann mit Hilfe des Internet Update Daemons regelmäßig online auf Updates geprüft und, wenn nötig, aktualisiert werden. In der Voreinstellung sind diese Optionen deaktiviert, es wird also kein automatisches Update durchgeführt. Um die AntiVir Software stets auf aktuellem Stand zu halten, aktivieren Sie bitte (nach gegebenenfalls notwendiger Konfiguration der HTTP-Proxy-Parameter) einen Update-Plan und starten Sie den Internet Update Daemon; oder richten Sie einen Update-Job im cron-Daemon ein.
Für Updates alle 2 Stunden muss folgende Option aktiviert werden:
`AutoUpdateEvery2Hours`
Für tägliche Updates muss folgende Option aktiviert werden:
`AutoUpdateDaily`
Wenn tägliche Updates eingestellt sind, kann in einem weiteren Eintrag die Uhrzeit für die Updates als HH:MM angegeben werden, z. B.:
`AutoUpdateTime 04:23`
- EmailTo** Email-Nachrichten:
AntiVir kann Emails verschicken, um über die Update-Aktivitäten zu benachrichtigen. Eine Voreinstellung gibt es nicht. Damit Emails verschickt werden können, muss also ein Adressat angegeben werden, z. B.:
`EmailTo root@localhost`
- LogTo** Logdatei:
Alle wichtigen Operationen von AntiVir werden über den `syslog`-Dämon protokolliert. Zusätzlich kann eine Logdatei geschrieben werden. Eine Voreinstellung gibt es nicht. Damit die Logdatei geschrieben werden kann, muss der volle Pfad zur Datei angegeben werden, z. B.:
`LogTo /var/log/avupdater.log`
- HTTPProxy...** Proxyserver:
Wenn der Rechner über einen HTTP-Proxyserver mit dem Internet verbunden ist, muss dies spezifiziert werden, damit der automatische Internet Updater korrekt arbeitet. Als Voreinstellung sind die Einträge deaktiviert; es wird also eine direkte Verbindung ins Internet angenommen. Eingestellt werden müssen:
- HTTP-Proxyserver
 - Port
 - Username und Passwort, wenn diese für den HTTP-Proxyserver erforderlich sind.

Beispiel:

HTTPProxyServer	proxy.domain.com
HTTPProxyPort	8080
HTTPProxyUsername	username
HTTPProxyPassword	password

Updater
Keeps
Backups

Der Internet-Updater ersetzt installierte Dateien durch neuere Versionen, sobald diese verfügbar sind. Auch wenn die Dateien erst nach umfangreichen Tests ersetzt werden, können Sie dennoch Backups der vorherigen Versionen anlegen.

Wird diese Option aktiviert, werden unterhalb des Verzeichnisses */usr/lib/AntiVir* weitere Verzeichnisse mit dem Namensschema *updater-backup-YYYYmdd-HHMMSS* angelegt und die ersetzten Dateien dort archiviert.



Falls Sie die Backup-Funktion des Internet Updaters aktivieren, sollten Sie regelmäßig diese Verzeichnisse prüfen und alte Versionen von Hand entfernen.

GnuPG... GnuPG-Einstellung:
Die Authentizität der AntiVir-Updates kann durch GnuPG verifiziert werden. Nähere Informationen hierzu siehe Abschnitt [Authentizität der Updates durch GnuPG verifizieren](#) – Seite 33. Wenn GnuPG verwendet wird, muss der Pfad zur GnuPG-Binärdatei angegeben werden, z. B.:

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

Zusätzliche GnuPG-Optionen können über `GnuPGOptions` spezifiziert werden, in Abhängigkeit von der speziellen GnuPG-Installation. Normalerweise ist dies aber nicht nötig. In der Voreinstellung sind beide Einträge aus Sicherheitsgründen deaktiviert.

Syslog... Syslog-Einstellung:
Für alle wichtigen Operationen gibt AntiVir Meldungen an den *syslog*-Dämon. Zusätzlich kann spezifiziert werden, welche Facility und Priorität diesen Meldungen mitgegeben wird. Voreingestellt sind:

```
SyslogFacility user  
SyslogPriority notice
```

Diese Werte gelten auch, wenn die Einträge deaktiviert sind.

4.3 Konfigurationsskript configantivir

Mit Hilfe des Konfigurationsskripts *configantivir* kann der AntiVir Internet Updater komfortabel angepaßt werden. Dieses Skript fängt eventuelle Fehleingaben ab und startet die notwendigen Prozesse neu.

Das Konfigurationsskript editiert die Einstellungen in *avupdater.conf*.

Der Umgang mit dem Skript ist sehr einfach:

► Geben Sie ein:

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

Das Skript liest die aktuell gesetzten Werte in *avupdater.conf* ein und fragt systematisch, ob neue Werte gesetzt werden sollen. Die möglichen neuen Werte werden angezeigt, die alten Werte werden dabei als Default vorgeschlagen.

Wenn Sie einen vorhandenen Wert übernehmen wollen:

- ▶ Drücken Sie **Enter**.

Wenn Sie einen Wert ändern wollen:

- ▶ Geben Sie den neuen Wert ein.
 - ↳ Nach der Abfrage der einzelnen Werte wird eine Zusammenfassung der Konfiguration angezeigt, z. B.:

```
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]
```

Wenn nicht alle Angaben der gewünschten Konfiguration entsprechen:

- ▶ Geben Sie N ein, um das Konfigurationsskript neu zu starten und die falschen Werte zu korrigieren.

Wenn alle Angaben der gewünschten Konfiguration entsprechen:

- ▶ Bestätigen Sie mit Y oder **Enter**, um die Konfigurationsdatei mit den neuen Werten abzuspeichern.
 - ↳ Das Skript meldet die Speicherung der Konfigurationsdatei. Es gibt Informationen zum Umgang mit dem Internet Update Daemon aus:

```
* 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]
```

- ▶ Geben Sie Y oder **Enter** ein, um den Internet Update Daemon zu starten.

-
- ↳ Der Internet Update Daemon wird gestartet. Wenn der Daemon bereits läuft, wird er automatisch neu gestartet, damit die neuen Einstellungen wirksam werden. Damit ist die Konfiguration abgeschlossen.

```
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 Konfigurieren regelmäßiger Updates

Die Leistungsfähigkeit und Wirksamkeit einer Antivirensoftware steht und fällt mit ihrer Aktualität. Deshalb bietet AntiVir VSA die Möglichkeit, jederzeit Updates über HTTP vom AntiVir-Webserver zu laden, und dies auf Wunsch auch automatisiert in regelmäßigen Abständen.

Bei diesen Updates werden die Bestandteile von AntiVir VSA, die den Schutz vor Viren und unerwünschten Programmen sicherstellen, auf den neuesten Stand gebracht.

Sie haben zwei unterschiedliche Möglichkeiten, automatische Updates von AntiVir VSA zu konfigurieren:

- Sie verwenden den mitgelieferten Internet Update Daemon, den Sie einfach konfigurieren können. Dies ist empfohlen, wenn Sie geringe UNIX-Kenntnisse haben und wenig eigene Anpassungen vornehmen möchten.
- Sie verwenden AntiVir VSA in Verbindung mit dem cron-Dämon. Dies ist empfohlen, wenn Sie vertiefte UNIX-Kenntnisse haben. Hier müssen Sie die Konfiguration selbst vornehmen, haben dadurch aber mehr Spielraum.

Internet-Zugang für Updates konfigurieren

- ✓ Stellen Sie sicher, dass Ihr Internetzugang funktioniert. In den meisten Fällen wird der Internetzugang bereits konfiguriert sein. Ansonsten entnehmen Sie die notwendigen Informationen Ihrer UNIX-Dokumentation.

Proxyserver Falls Sie über einen HTTP-Proxyserver mit dem Internet verbunden sind, müssen Sie AntiVir VSA entsprechend konfigurieren:

- ▶ Rufen Sie configantivir auf:

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

- ▶ Bestätigen Sie die Einstellungen mit **Enter**, bis die Abfrage zum Proxyserver kommt:

```
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]
```

- ▶ Geben Sie Y ein.
 - ↳ Anschließend wird nach dem Namen und dem Port des Proxyservers gefragt.
Geben Sie die Daten ein:

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

- ↳ Anschließend wird gefragt, ob für den Proxyserver ein Username und ein Passwort notwendig sind:

```
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]
```

Wenn ein Username und Passwort erforderlich sind:

- ▶ Geben Sie Y ein.
 - ↳ Anschließend werden Sie nach Username und Passwort gefragt.
- ▶ Geben Sie Username und Passwort ein.
 - ↳ Das Konfigurationsskript zeigt die Zusammenfassung der Einstellungen an und fragt nach der Bestätigung um die Konfigurationsdatei zu schreiben.

Der Internet-Zugang für Updates ist konfiguriert.

Automatische Updates über den Internet Update Daemon konfigurieren

Der Internet Update Daemon ist ein sehr einfacher Dienst, der in festgesetzten Abständen folgenden Befehl aufruft:

```
antivir --update
```



Damit die nachfolgenden Einstellungen wirksam werden können, muss der Internet Update Daemon installiert sein. Wenn Sie die Installation wie unter [AntiVir VSA installieren](#) – Seite 14 beschrieben vorgenommen haben, ist dies bereits der Fall. Ansonsten müssen Sie nochmals das Installationskript laufen lassen, siehe [AntiVir VSA erneut installieren](#) – Seite 17.

Folgende Einstellungen können definiert werden:

- Abstände der Aktualisierung. Möglich ist
 - Update alle zwei Stunden
 - Tägliches Update
- Zeitpunkt der Aktualisierung (bei täglichem Update). Möglich ist
 - Vom Benutzer eingestellter Zeitpunkt
 - Zufällig gewählter Zeitpunkt. Das Skript wählt in diesem Fall einmalig eine zufällige Zeit, die dann aber fest gesetzt wird. Dies ist dann sinnvoll, wenn der Rechner permanent online ist.
- ▶ Rufen Sie *configantivir* auf:


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

- ▶ Bestätigen Sie die Einstellungen mit **Enter** bis die Frage nach der Häufigkeit der Updates erscheint:

```
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]
```

- ▶ Wählen Sie
 - n, wenn Sie keine automatischen Updates durchführen wollen
 - 2 für Updates alle zwei Stunden
 - d für tägliche Updates
- ↳ Wenn Sie tägliche Updates gewählt haben, wird nach dem Zeitpunkt des Updates gefragt:

```
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]
```

- ▶ Geben Sie die Zeit im Format HH:MM ein
 - ODER -
 - Geben Sie R für einen zufälligen Zeitpunkt ein.
- ▶ Bestätigen Sie alle nachfolgenden Fragen des Konfigurationsskripts mit **Enter**.

-
- ↳ Die automatischen Updates über den Internet Update Daemon sind konfiguriert. Der Daemon wird automatisch gestartet (wenn er noch nicht lief) beziehungsweise neu gestartet (wenn er bereits lief).

Internet Update Daemon manuell starten und anhalten

Wenn Sie den Internet Update Daemon starten wollen:

- ▶ Geben Sie ein:

```
/usr/lib/AntiVir/avupdater start
```

Wenn Sie den Internet Update Daemon anhalten wollen:

- ▶ Geben Sie ein:

```
/usr/lib/AntiVir/avupdater stop
```

Wenn Sie den aktuellen Status des Internet Update Daemons feststellen wollen:

- ▶ Geben Sie ein:

```
/usr/lib/AntiVir/avupdater status
```

Updates über Cron steuern



Die Steuerung mit dem Cron-Dämon wird empfohlen!

Wenn Sie vertiefte UNIX-Kenntnisse haben, können Sie den Cron-Dämon zur Steuerung der automatischen AntiVir VSA-Updates nutzen.

Der Cron-Dämon steuert regelmäßig wiederkehrende Systemprozesse. Nähere Informationen hierüber entnehmen Sie Ihrer UNIX-Dokumentation.

Bei der Steuerung der Updates über den Cron-Dämon haben Sie mehr Konfigurationsmöglichkeiten als mit dem Internet Updater.

Beispiel ▶ Fügen Sie folgenden Cron-Job in `/etc/crontab` ein

```
45 */2 * * * root /usr/lib/AntiVir/antivir --update -q
```

- ↳ Dieser Eintrag bewirkt Updates alle zwei Stunden jeweils 15 Minuten vor der vollen Stunde, also um 0:45 Uhr, 2:45 Uhr, 4:45 Uhr und so weiter. Die Option `-q` bewirkt, dass keine Meldungen ausgegeben werden.

Internet Updater automatisch starten

Wenn Sie nicht mit dem Cron-Dämon arbeiten wollen, benutzen Sie den Internet Update Daemon. Wenn Sie die Installation so vorgenommen haben, wie in [AntiVir VSA installieren](#) – Seite 14 beschrieben, ist Ihr System schon entsprechend eingestellt.

Wenn der Internet Update Daemon noch nicht automatisch beim Systemstart gestartet wurde:

- ▶ Führen Sie eine erneute Installation mit den entsprechenden Einstellungen durch (siehe [AntiVir VSA erneut installieren](#) – Seite 17).

Authentizität der Updates durch GnuPG verifizieren

GnuPG ist eine kostenlose Alternative zum Verschlüsselungsprogramm PGP (Pretty Good Privacy). Mit GnuPG kann die Authentizität der Updates von AntiVir verifiziert werden.

Die Verwendung von GnuPG wird sehr empfohlen.



Allerdings setzt die Verwendung vertiefte Kenntnisse von UNIX und GnuPG voraus. Bei fehlerhafter Konfiguration besteht ansonsten die Gefahr, dass AntiVir VSA nicht mehr aktualisiert wird.

Diese Schritte müssen von dem Benutzer ausgeführt werden, der die Updates auf dem Rechner durchführt. Dies ist in den meisten Fällen der Benutzer mit Administratorrechten.

Weitere Informationen zu GnuPG enthalten Sie über <http://www.gnupg.org>

Führen Sie folgende Schritte durch, um die Unterstützung von GnuPG zu aktivieren:

- ▶ Laden Sie GnuPG von der GnuPG-Webseite <http://www.gnupg.org>. Hier erhalten Sie auch ein Handbuch mit weiterführenden Informationen zu PGP und dessen Anwendungsmöglichkeiten.
- ▶ Erzeugen Sie Ihren eigenen PGP-Schlüssel, wie in der GnuPG-Dokumentation beschrieben.
- ▶ Fügen Sie den öffentlichen AntiVir-PGP-Schlüssel zu Ihrem Schlüsselbund hinzu:
`gpg --import antivir.gpg`
– ODER –
Importieren Sie den öffentlichen AntiVir-PGP-Schlüssel direkt vom Keyserver:
`gpg --keyserver=wwwkeys.pgp.net --recv-keys 0F821C2E`
- ▶ Fordern Sie den Fingerabdruck des Schlüssels an, um sicherzustellen, dass es tatsächlich der öffentliche AntiVir-PGP-Schlüssel ist:
`gpg --fingerprint build@avira.com`
↳ Der 40-stellige Fingerabdruck wird ausgegeben.
- ▶ Stellen Sie sicher, dass der ausgegebene Fingerabdruck mit dem Fingerabdruck des öffentlichen AntiVir-PGP-Schlüssels übereinstimmt. Der Fingerabdruck des öffentlichen AntiVir-PGP-Schlüssels wird auf der Avira-Webseite (<http://www.avira.com>) angezeigt.
- ▶ Unterschreiben Sie den öffentlichen AntiVir-PGP-Schlüssel, um seine Gültigkeit zu beglaubigen:
`gpg --sign-key build@avira.com`
- ▶ Wechseln Sie in das Unterverzeichnis */bin* Ihres AntiVir-Installationsverzeichnis, also etwa:
`cd /tmp/antivir-vsa-prof-<version>/bin`
↳ In diesem Verzeichnis liegen die Dateien *antivir* und *antivir.asc*.
- ▶ Prüfen Sie die Unterschrift mit
`gpg --verify antivir.asc antivir`
↳ Wenn Sie keine Fehlermeldungen erhalten, ist GnuPG bereit für Updates von AntiVir.

-
- ▶ Aktivieren Sie GnuPG für AntiVir. Tragen Sie hierfür in */etc/avupdater.conf* im Eintrag `GnuPGBinary` den vollen Pfad zur GnuPG-Binärdatei ein, z. B.:
`GnuPGBinary /usr/local/bin/gpg`



Diese Option kann nur manuell in *avupdater.conf* editiert werden.
Eine Einstellung über das Konfigurationsscript ist nicht möglich, um die Gefahr einer fehlerhaften Konfiguration zu mindern.

- ▶ Starten Sie den Internet Update Daemon neu, um die geänderten Einstellungen in *avupdater.conf* wirksam werden zu lassen:
`/usr/lib/AntiVir/avupdater restart`
 - ↳ Die Authentizität der Updates wird ab jetzt durch GnuPG sichergestellt.

5 Konfiguration (Windows)

Die Savapi 2 besteht aus zwei Teilen: dem Savapi-Service und der SAVAPI.DLL. Beide können über eine Steuerdatei (INI-Datei) konfiguriert werden.



Beachten Sie, dass im Normalfall eine spezielle Konfiguration der SAVAPI 2 nicht notwendig ist. Die Standardeinstellungen sind meist ausreichend.

Beim ersten Start fährt der Dienst (Savapi-Service) mit sicheren Default-Werten hoch. Dabei wird die Datei *SAVAPI.INI* automatisch angelegt.

Die meisten Parameter können Sie ändern, während der Savapi-Service läuft. Ein Neustart des Dienstes ist nur für die folgenden Parameter nötig:

- Portnummer
- Verzeichnis für temporäre Dateien
- Verzeichnis für Updates
- Name der Lizenzdatei
- Name der Logdatei

Wenn Sie den Savapi-Service beenden wollen:

- ▶ Starten Sie das Dienste-Applet unter Services (Start\Einstellungen\Systemsteuerung\Computerverwaltung\Dienste).
- ▶ Wählen Sie den Savapi-Service.
- ▶ Stoppen Sie den Savapi-Service.
- ▶ Ändern Sie die Parameter.
- ▶ Starten Sie den Savapi-Service neu.
- ▶ Starten Sie ggf. das Programm neu, das die *SAVAPI.DLL* verwendet.

5.1 Mögliche Einträge in der Steuerdatei SAVAPI.INI

Folgende Parameter lassen sich in der Steuerdatei *SAVAPI.INI* ändern:

Portnummer

Dieser Wert gibt die Nummer des TCP/IP-Ports an, der für die Kommunikation zwischen Savapi-Service und der SAVAPI.DLL verwendet werden soll. Sollte dieser Port belegt sein, können Sie ihn beliebig ändern. Beachten Sie, dass Sie dann auch den entsprechenden Eintrag in der *SAVAPIDL.INI* ändern müssen (siehe Kapitel [Möglicher Eintrag in der Steuerdatei SAVAPIDL.INI](#) – Seite 38).

Beispiel `PortNumber=18370`

Verzeichnis für temporäre Dateien

Dieser Wert gibt das Verzeichnis an, in das der Savapi-Service seine temporären Dateien schreibt. Normalerweise ist dies das Unterverzeichnis `\temp` unterhalb des Installationsverzeichnisses. Sie können diese Variable aber auf ein beliebiges Verzeichnis setzen – genügend freien Plattenplatz vorausgesetzt.

Beispiel `TempDirectory=C:\Programme\Avira GmbH\AntiVir SAVAPI\temp\`

Verzeichnis für Updates

In dieses Verzeichnis speichert der Savapi-Service die vom Internet geladenen Updates zwischen. Es ist sozusagen das Arbeitsverzeichnis für den Updater (Savapi-Update-Service). Das Verzeichnis sollte normalerweise nicht geändert werden. Beachten Sie, dass der Savapi-Update-Service für dieses Verzeichnis Schreibrechte haben muss.

Beispiel `UpdateDirectory=C:\Programme\Avira GmbH\AntiVir SAVAPI\update\`

Name der Lizenzdatei

Dieser Parameter definiert den Namen der Lizenzdatei, die während der Installation in das Installationsverzeichnis der SAVAPI kopiert wird.

Beispiel `KeyFileName=C:\Programme\Avira GmbH\AntiVir SAVAPI\hbedv.key`

Name der Logdatei

Dieser Wert gibt den Namen der Logdatei des Savapi-Service an. Sie können die Logdatei an eine beliebige Stelle auf Ihren Festplatten verschieben. Beachten Sie, dass der Dienst dafür Schreibrechte besitzen muss.

Standardmäßig wird die Logdatei im Installationsverzeichnis angelegt und heißt `SAVAPI.LOG`.

Beispiel `LogFileName=C:\Programme\Avira GmbH\AntiVir SAVAPI\savapi.log`

Maximale Größe der Logdatei

Dieser Wert gibt die maximale Größe der Logdatei (in kB) an. Wird der Wert überschritten, werden die ältesten Einträge automatisch gelöscht.

Ist dieser Wert 0, wird die Größe der Logdatei nicht beschränkt.

Beispiel `LogFileSize=1000`

Servername für die Updates

Von der angegebenen URL holt sich der Savapi-Service die Updates (neue Virensignaturen). Falls Sie einen anderen Server verwenden wollen (z. B. über den Internet Update Manager), können Sie diese URL entsprechend ändern.

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

Falls Sie die Updates von einem freigegebenen Verzeichnis holen wollen, so ist zu beachten, dass unter `UpdateUrl` der Pfad des Verzeichnisses angegeben werden muss.

Ist eine Authentifizierung notwendig, so werden Benutzername und Passwort verwendet, den/das Sie unter `NetworkUserName` bzw. `NetworkPassword` angeben können. Beachten Sie, dass der Savapi-Update-Service unter einem Benutzerkonto (Standard ist der Local-System-Account) laufen muss, mit dem er Zugriff auf dieses Verzeichnis hat.

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

Intervall für die Suche nach neuen Updates

Dieser Wert gibt an, in welchen Intervallen der Internet Updater nach neuen Versionen auf dem unter `UpdateURL` festgelegten Server suchen soll. Der Wert wird in Minuten angegeben; Standardeinstellung: alle 120 Minuten. Der Savapi-Service führt direkt nach der ersten Aktion (Suche nach Viren und anderer Malware) automatisch ein Update der Engine und der Virensignaturen durch.

Ist dieser Wert 0, wird die automatische Suche nach neuen Updates deaktiviert.

Beispiel `UpdateInterval=120`

Proxy-Server für Updates verwenden

Falls dieser Wert aktiviert (1) ist, versucht der Savapi-Service, die Updates über den angegebenen Proxy-Server herunterzuladen. Standardmäßig wird kein Proxy-Server verwendet.

Beispiel `ProxyEnabled=0`

Adresse des Proxy-Servers

Tragen Sie hier den vollständigen Namen oder die IP-Adresse des Proxy-Servers ein, der für die Updates verwendet werden soll. Dieser Wert wird nur verwendet, wenn `ProxyEnabled` aktiviert ist.

Beispiel `ProxyUrl=proxy.mydomain.de`

Benutzername und Passwort für die Anmeldung am Proxy-Server (Proxy-Authentifizierung)

Tragen Sie hier Benutzername und Passwort ein, mit denen sich der Internet Updater am Proxy-Server anmelden soll. Diese Werte werden nur verwendet, wenn `ProxyEnabled` aktiviert ist.

Beispiel `ProxyUserName=fmeier`
 `ProxyPassword=password`

Email-Nachrichten versenden

Falls `SmtMailEnabled` aktiviert (1) ist, versendet der Savapi-Service Email-Nachrichten an den Empfänger, der unter `SmtRecipientAddress` angegeben ist. Email-Nachrichten können versendet werden, wenn ein Update erfolgreich bzw. nicht erfolgreich durchgeführt wurde.

Stellen Sie sicher, dass die Parameter `SmtMailMode`, `SmtHostName`, `SmtSenderAddress` und `SmtRecipientAddress` richtig gesetzt sind.

Standardmäßig ist `SmtMailEnabled` deaktiviert.

Der Parameter `SmtMailMode` legt fest, wann Emails versendet werden.

Beispiel `SmtMailEnabled=0`

`SmtMailMode=0`

0 = Emails werden nur versendet, wenn beim Update ein Fehler aufgetreten ist

1 = Emails werden in jedem Fall versendet (Update erfolgreich bzw. nicht erfolgreich)

Name des SMTP-Servers

Tragen Sie hier den vollständigen Namen oder die IP-Adresse Ihres SMTP-Servers an. Dieser Wert wird nur verwendet, wenn `SmtMailEnabled` aktiviert ist.

Beispiel `SmtHostName=smtp.domain.net`

Sender-Email-Adresse

Tragen Sie hier die Email-Adresse ein, die Sie zum Versenden der Emails nutzen möchten. Dieser Wert wird nur dann verwendet, wenn `SmtMailEnabled` aktiviert ist.

Beispiel `SmtSenderAddress=sender@domain.net`

Empfänger-Email-Adresse

Tragen Sie hier die Adresse ein, an die Emails gesendet werden sollen. Dieser Wert wird nur dann verwendet, wenn `SmtMailEnabled` aktiviert ist.

Beispiel `SmtRecipientAddress=recipient@domain.net`

5.2 Möglicher Eintrag in der Steuerdatei SAVAPIDL.INI

Die Steuerdatei für die *SAVAPI.DLL* ist die *SAVAPIDL.INI*. Sie dient der Kommunikation zwischen AntiVir VSA und der Engine. Standardmäßig ist diese Steuerdatei nicht vorhanden, es wird mit Standardeinstellungen gearbeitet.

Um den Default-Port für die Kommunikation mit dem Savapi-Service zu ändern, müssen Sie in dem Verzeichnis, in dem sich die *SAVAPI.DLL* befindet, eine Datei *SAVAPIDL.INI* erzeugen.

Diese enthält nur den folgenden Eintrag:

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

Portnummer

Dieser Wert gibt die Nummer des TCP-/IP-Ports an, der für die Kommunikation zwischen dem Savapi-Service und der *SAVAPI.DLL* verwendet werden soll. Sollte dieser Port belegt sein, können Sie ihn beliebig ändern.

Beachten Sie, dass Sie dann auch den entsprechenden Eintrag in der Steuerdatei des Savapi-Service (*SAVAPI.INI*) ändern müssen (siehe Kapitel [Mögliche Einträge in der Steuerdatei SAVAPI.INI](#) – Seite 35).

Beispiel `PortNumber=18370`

5.3 Sofort-Updates

Mit der Installation von AntiVir VSA wird standardmäßig ein automatisches Update aller zwei Stunden konfiguriert.

Das Update kann über das Internet, von einem beliebigen Computer in Ihrem Netzwerk über Intranet oder ein freigegebenes Verzeichnis erfolgen.

Mit der Anwendung *StartUpdate.exe* kann man dem Savapi-Service jedoch auch mitteilen, dass er sofort ein Update durchführen soll. Dieses wird dabei unabhängig von dem jeweils eingestellten Update-Intervall durchgeführt. Im Fehlerfall liefert die Anwendung (für Batch-Dateien sehr hilfreich) einen `Errorlevel` von 1 zurück. Ob das Update durchgeführt wurde, kann in der Logdatei *SAVAPI.LOG* nachgelesen werden. Die Anwendung selbst hat keine Ausgabe.

Hintergrund

Sofort-Updates sind z. B. sinnvoll, um Einstellungen in der SAVAPI-INI zu testen.

Es ist damit auch möglich, Updates komplett über die SAP-Umgebung zu steuern (falls das unterstützt wird). Sie müssten dann das Update-Intervall auf 0 setzen.

6 ABAP-spezifische Konfiguration

Dieses Kapitel beschreibt die Konfiguration der Viren-Scan-Schnittstelle für ABAP-Systeme. Die Texte wurden der SAP-Webseite entnommen.

6.1 Viren-Scan-Schnittstelle einrichten

Damit Sie den Virus Scan Server von SAP nutzen können, müssen Sie im Einführungsleitfaden (IMG) Daten pflegen. Führen Sie dazu folgende Schritte aus:

- [Scanner-Gruppen definieren](#) – Seite 41
- [Virus Scan Server definieren](#) – Seite 44
- [Viren-Scan-Profil definieren](#) – Seite 53
- [BAdI für Viren-Scanner implementieren](#) – Seite 59

6.1.1 Scanner-Gruppen definieren

Eine Scanner-Gruppe fasst mehrere gleichartige Viren-Scanner zusammen, um Lastverteilung zu erreichen. Da Sie den Virus Scan Server bei der Pflege der Viren-Scan-Profil über die Scanner-Gruppe auswählen, müssen Sie jeden Virus Scan Server einer Scanner-Gruppe zuordnen.

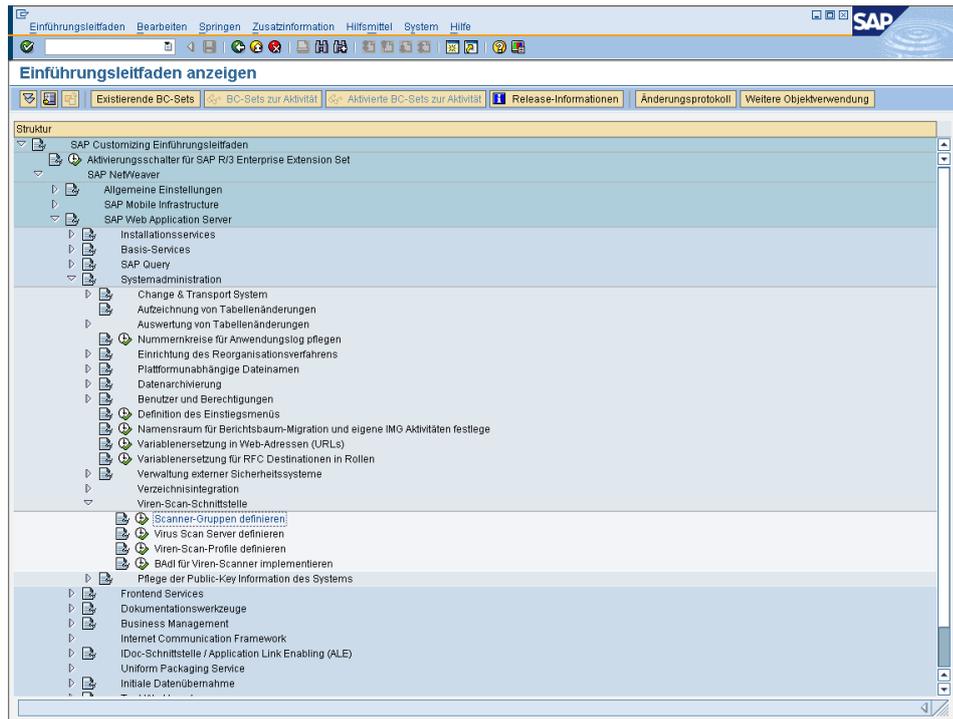
Pflegen Sie eine Scanner-Gruppe für jede Produktklasse von Viren-Scannern, die über den Virus Scan Server mit dem System verbunden wird. Wenn Sie eigene Viren-Scanner mit dem BAdI VSCAN_SERVER einbinden, legen Sie auch für jede Implementierung Ihres eigenen Scanners eine Scanner-Gruppe an und kennzeichnen Sie diese als BAdI-Implementierung.

Für jede Scanner-Gruppe können Sie Konfigurationsparameter hinterlegen. Diese teilen sich auf in Initialisierungsparameter und Scan-Parameter.

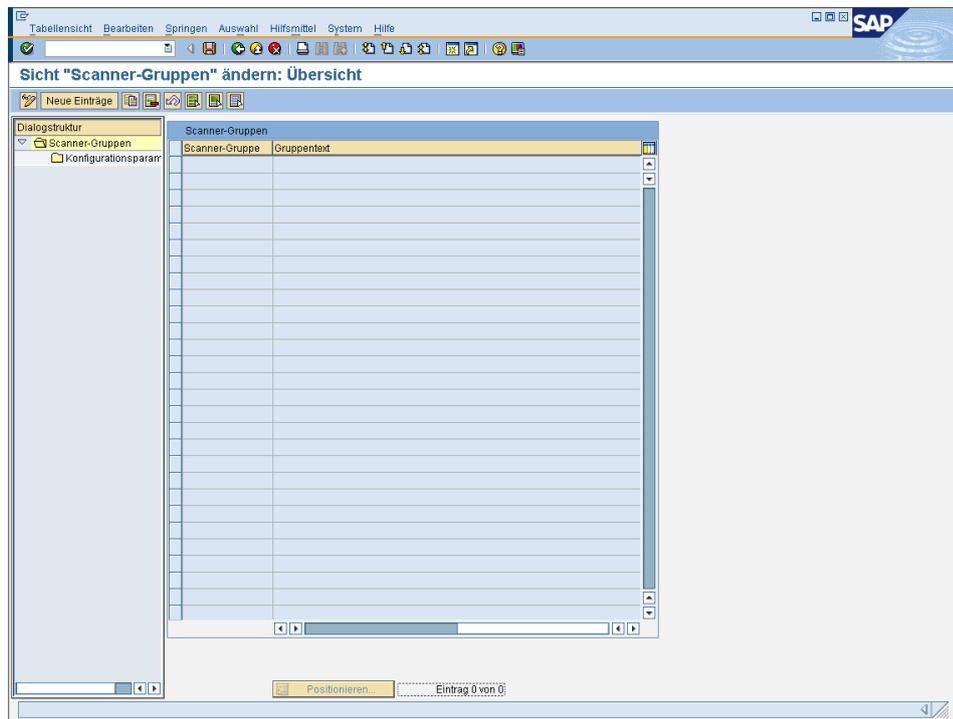
- Initialisierungsparameter werden beim Start eines Virus Scan Server diesem übergeben und sind erforderlich, um diesen überhaupt starten zu können. Wenn Sie das Business Add-In nutzen, werden diese Parameter der Methode zur Erzeugung der Scan-Instanz übergeben. Die Parameter enthalten z. B. den Pfad zu den Virensignaturen.
- Scan-Parameter werden pro Scan-Vorgang übergeben und steuern das Verhalten des einzelnen Auftrags, z. B. Scannen von Makros aktivieren ja/nein.

SAP liefert keine Scanner-Gruppen aus.

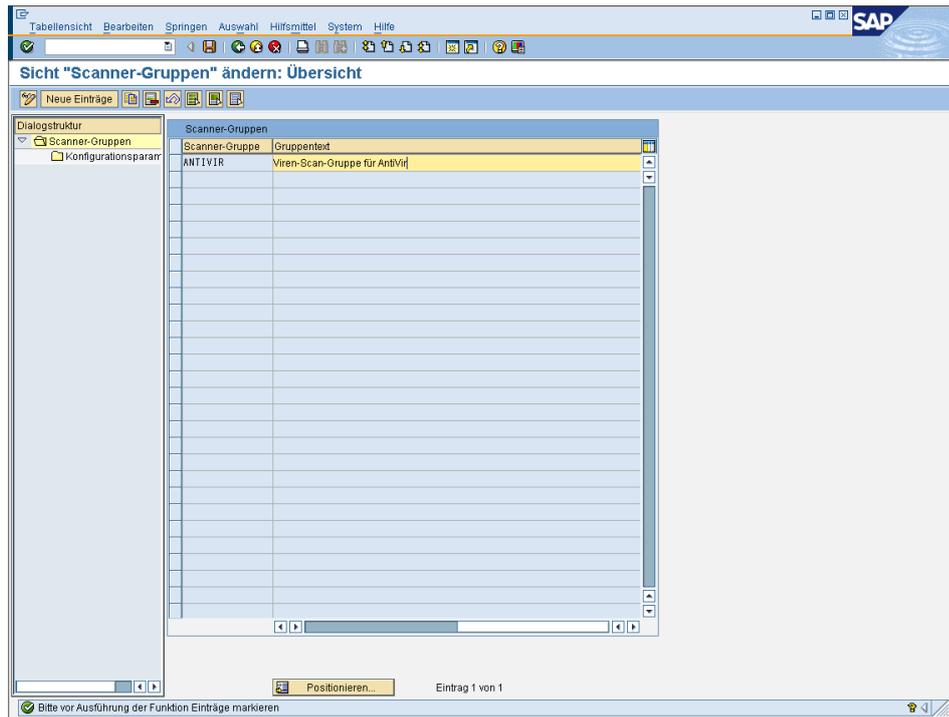
- ▶ Geben Sie die Transaktionsnummer **spro** ein (Eingabefeld links oben).
- ▶ Wählen Sie im Einführungsleitfaden (IMG) **SAP Web Application Server/ Systemadministration/Viren-Scan-Schnittstelle**:



- ▶ Wählen Sie neben **Scanner-Gruppen definieren** die Option **Ausführen**.
- ↳ Sie gelangen auf das Bild **Sicht: "Scanner-Gruppen" ändern: Übersicht**:



- ▶ Wählen Sie **Neue Einträge**.
- ↳ Sie gelangen auf das Bild **Neue Einträge: Übersicht Hinzugefügte**.



- Geben Sie die Daten für die Definition der Scanner-Gruppe an (siehe folgende Tabelle).

Feld	Kommentar
Scanner-Gruppe	Frei wählbarer Name der Scanner-Gruppe.
Business Add-In	Wenn dieses Kennzeichen gesetzt ist, übergibt das Programm die Anforderung einer Viren-Scan-Instanz für diese Scanner-Gruppe an das Business Add-In VSCAN_INSTANCE, das kundeneigene Viren-Scanner einbinden kann. Ist das Kennzeichen nicht gesetzt, sucht das Programm nach einem passenden Virus Scan Server in der Menge der im Customizing gepflegten Virus Scan Servers, die diese Scanner-Gruppe besitzen.
Gruppentext	Erläuterung zur Scanner-Gruppe.

- Sichern Sie Ihre Eingaben.

6.1.2 Virus Scan Server definieren

Der SAP Virus Scan Server ist ein ausführbares Programm, das Viren-Scanner zertifizierter Hersteller über eine Schnittstelle einbindet und den Anwendungsservern des Systems als registrierter RFC-Server Scan-Dienste anbietet.

Der Anwendungsserver steuert Aufgaben wie Start, Stop und Überwachung der Virus Scan Server. Die hierzu benötigten Daten konfigurieren Sie in diesem Schritt.



- ▶ Legen Sie mit dieser Vorgehensweise für jeden Virus Scan Server, den Sie einrichten wollen, einen Eintrag an. Aus Performance-Gründen empfehlen wir Ihnen, auf jedem Anwendungsserver mindestens einen Virus Scan Server einzurichten.
SAP liefert keine Konfigurationsdaten für Virus Scan Server aus.
-

- ✓ Sie haben mindestens eine Scanner-Gruppe angelegt.
- ✓ Sie haben entschieden, ob Sie den Virus Scan Server als Applikationsserverstarter oder als Selbststarter anlegen (siehe [Applikationsserver- oder Selbststarter](#) – Seite 48).

- ▶ Legen Sie in Transaktion SM59 eine RFC-Verbindung des Verbindungstyps **T** an.

Da die Konfiguration des Virus Scan Server folgende Namenskonvention erfordert, müssen Sie diese für die RFC-Destination eines Virus Scan Server verwenden:

- VSCAN_<Hostname>, wenn Sie auf dem Host nur einen Virus Scan Server starten wollen.
- VSCAN_<Hostname>-<Nummer>, wenn Sie auf dem Host mehrere Virus Scan Servers starten wollen. Die Nummer ist eine fortlaufende Zahl, die durch einen Bindestrich vom Hostnamen abgetrennt ist.

Mögliche Namen wären daher: VSCAN_HOST123, VSCAN_HOST345-1, VSCAN_HOST345-2 usw.

- ▶ Wählen Sie die Aktivierungsart **Registriertes Serverprogramm**.
- ▶ Verwenden Sie als Programm-ID den Namen der RFC-Destination.
- ▶ Tragen Sie als Gateway-Host und Gateway-Service die Adresse des Gateways des Systems ein. Wenn Sie den Virus Scan Server über das Computing Center Management System auf einem Anwendungsserver starten, wählen Sie das Gateway dieses Anwendungsservers.
- ▶ Wählen Sie im Einführungsleitfaden (IMG) SAP **Web Application Server/ Systemadministration/Viren-Scan-Schnittstelle**.
- ▶ Wählen Sie neben **Virus Scan Server definieren** die Option **Ausführen**.
 - ↳ Sie gelangen auf das Bild **Sicht "Virus-Scan-Server-Definition" ändern: Übersicht**.
- ▶ Wählen Sie **Neue Einträge**.
 - ↳ Sie gelangen auf das Bild **Neue Einträge: Detail Hinzugefügte**.
- ▶ Geben Sie im Feld **Scan Server** den Namen des Virus Scan Server ein. Der Name muss dem Namen der RFC-Destination entsprechen, welche die technische Verbindung zum Virus Scan Server enthält.

Sicht "Virus Scan Server Definition" ändern: Detail

Scan Server: VSCAN_ANTIVIR
 Status: Start Stop

Virus Scan Server Definition

Scanner-Gruppe: ANTIVIR

Status: Aktiv (Applikationsserver)

Server: id0133_UED_06

Tracelevel: Nur Fehler

Codepage: 1100

Init. Interv.: 24 Stunden Noch nicht initialisiert

Max. Instanzen: 20

Adapterpfad: /usr/lib/AntiVir/libantvirsa.so

Konfiguration:

Enginedaten

Version	6029.5
Versionstext	AntiVir (6.29.0.5)
Datum	Wed Dec 15 00:00:00 2004
Bekannte Viren	

Geladene Treiber

Version	Treibername	Datum	Bekannte Viren
6029.59	/usr/lib/AntiVir/libantvir.vdf	Wed Jan 12 16:20:37 2005	82455

Virus Scan Server

Version	1.50
Versionstext	Final Release of SAP Virus Scan Server, Copyright (c) SAP AG 1992-2005
Startzeitpunkt	Thu Jan 12 11:46:30 2005
Produktionsdaten	Release 640, Level 0, Patch 0 for Intel x86 with Linux on Jan 7 2005 (mt,dbg,ascii,SAP_CHAR/size_?void*=11414)

Adapterdaten

Hersteller	H+BEOV Datentechnik GmbH
Produktname	AntiVir Virus Scan Adapter
Version	1.0

Unterstützte Parameter

Parameter	Typ	Init	Parameterwert
SCANBESTEFFORT	BOOL	1	
SCANALLFILES	BOOL	1	
SCANALLEMBEDDED	BOOL	1	
SCANHEURISTICLEVEL	INT	0	
SCANEXTRACT	BOOL	1	
SCANEXTRACT_SIZE	SIZE_T		1073741824
SCANEXTRACT_DEPTH	INT	5	
SCANEXTRACT_RATIO	INT	150	

- Geben Sie unter **Virus Scan Server Definition** die Daten des Virus Scan Server ein (siehe folgende Tabelle).

Feld	Mögliche Werte	Kommentar
Scanner-Gruppe	Alle bereits angelegten Scanner-Gruppen, die mit der Werte-Hilfe angezeigt werden.	<p>Die Scanner-Gruppe fasst mehrere Virus Scan Server zusammen oder ermöglicht die Verwendung einer BAdI-Implementierung.</p> <p>Wenn Sie mehrere Virus Scan Server innerhalb einer Scanner-Gruppe anlegen, erreichen Sie Lastverteilung.</p> <p>Alle Virus Scan Server einer Scanner-Gruppe erhalten den gleichen Satz an Konfigurationsparametern und werden daher die gleiche Scan-Engine verwenden.</p>
Status	<ul style="list-style-type: none"> -ACTS (Aktiv als Selbststarter): Das CCMS überwacht zwar den Virus Scan Server (wenn er nicht verfügbar ist, wird ein Fehlerstatus ausgelöst), startet oder stoppt ihn jedoch nicht. Dieser Status eignet sich für Virus Scan Server, die z. B. als Service auf Betriebssystemebene gestartet werden. -ACTV: Aktiv (Anwendungsserver) Das CCMS überwacht den Virus Scan Server startet ihn bei Bedarf auf dem angegebenen Anwendungsserver -INAC (Inaktiv auf Anwendungsserver) Der Virus Scan Server wird durch das CCMS überwacht und bei Bedarf auf dem angegebenen Anwendungsserver gestoppt. -NONE: Keine Überwachung: Das CCMS überwacht den Virus Scan Server nicht. 	<p>Überwachungsstatus des Virus Scan Server im CCMS</p> <p>Bei den Status NONE und INAC kann die automatische Serverauswahl des Systems diesen Virus Scan Server nicht mehr finden.</p>
Server	Die Wertehilfe bietet die vorhandenen Server an. Geben Sie keinen anderen Servernamen an.	Anwendungsserver, auf dem der Virus Scan Server gestartet und/oder überwacht werden soll.
Trace-Level	<ul style="list-style-type: none"> -Nur Fehler -Fehler und Warnungen -Fehler, Warnungen und Informationen -Maximale Ausgabe 	<p>Gibt den Trace-Level für den Virus Scan Server an, der beim Start auf Betriebssystemebene durch das CCMS übergeben werden soll.</p> <p>Wir empfehlen, in Produktivsystemen nur einen der beiden ersten Trace-Levels Nur Fehler oder Fehler und Warnungen zu verwenden. Die beiden übrigen Trace-Levels stehen für die Fehlersuche während des Testbetriebs im Testsystem zur Verfügung.</p>

Feld	Mögliche Werte	Kommentar
Codepage	<p>Tragen Sie die für den Virus Scan Server gültige Codepage ein. Sie muss der Codepage des Anwendungsservers entsprechen, der mit dem Virus Scan Server kommuniziert:</p> <ul style="list-style-type: none"> -Wenn Sie nur eine Codepage innerhalb Ihrer Anwendungsserver benutzen, tragen Sie diese ein. -Wenn Sie Anwendungsserver in unterschiedlichen Codepages besitzen, richten Sie auf jedem Anwendungsserver einen Virus Scan Server ein und geben die jeweils gültige Codepage an. -Wenn Ihr System UNICODE nutzt, tragen Sie nichts ein. 	Codepage, die das CCMS beim Start des Virus Scan Server einstellt.
Init.Interval	<p>0 oder <leer>: keine automatische Reinitialisierung</p> <p>Wenn der Hersteller Ihres Viren-Scanners die von SAP angebotene Schnittstelle nutzt, über die eine Initialisierung von außen durchgeführt werden kann, können Sie das Feld frei lassen. Diese Schnittstelle steht zertifizierten Anbietern von Viren-Scannern zur Verfügung.</p> <p><n>: Intervall in Stunden</p>	<p>Gibt an, nach wieviel Stunden der Virus Scan Server regelmäßig neu initialisiert wird.</p> <p>Damit der Virus Scan Server neue Virendefinitionen vom Virus Scan Server lädt, müssen Sie ihn reinitialisieren.</p> <p>Die automatische Reinitialisierung erfolgt während der periodischen Überwachung der Virus Scan Servers durch das CCMS.</p>
Max. Instanzen		<p>Gibt die Höchstzahl der vom Virus Scan Server bereitgestellten Scan-Instanzen an.</p> <p>Ein Virus Scan Server kann möglicherweise mehrere Scan-Instanzen bereitstellen.</p> <p>Durch die hier angegebene Höchstzahl können Sie festlegen, wie viele dieser Instanzen angeboten werden. Wenn diese Zahl überschritten wird, steht der Virus Scan Server nicht mehr für Scan-Aufträge zur Verfügung. Die Anzahl der Instanzen soll der Anzahl der Workprozesse entsprechen.</p>

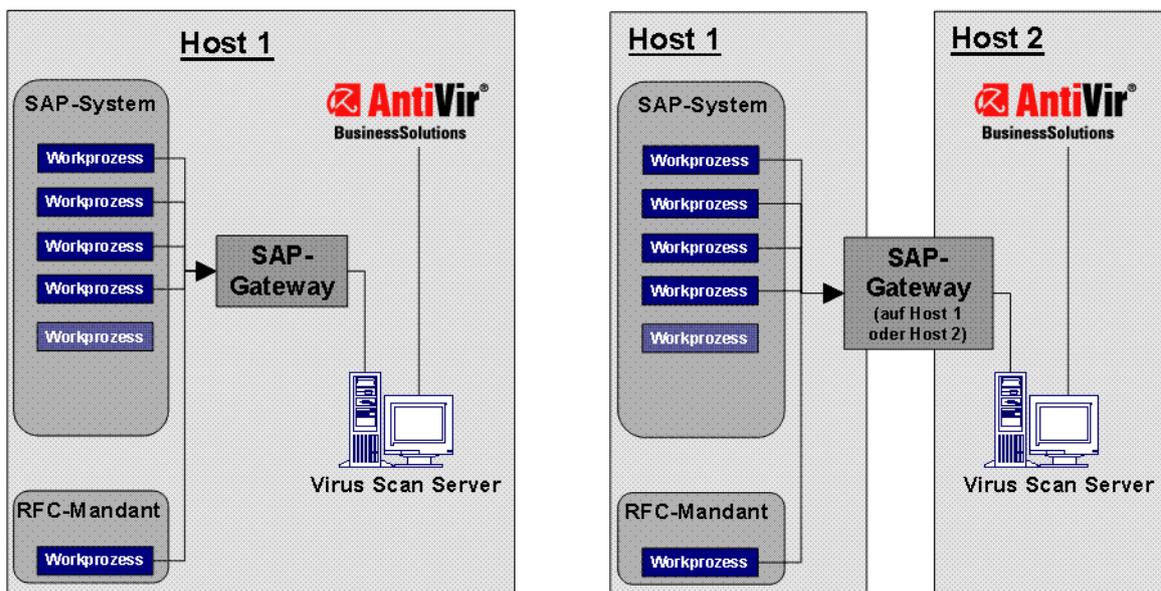
Feld	Mögliche Werte	Kommentar
Adapterpfad	Vollständiger Pfad der Bibliothek, die den Viren-Scan-Adapter enthält	Gibt den vollständigen Pfad zum Viren-Scan-Adapter an. Wenn Sie das Feld nicht ausfüllen, verwendet der Virus Scan Server den Inhalt der Umgebungsvariablen VSA_LIB.
Konfiguration	Vollständiger Pfad zur Konfigurationsdatei des Virus Scan Server	Gibt den vollständigen Pfad zur Konfigurationsdatei des Virus Scan Server an. Die Konfigurationsdatei des Virus Scan Server kann optionale Parameter enthalten, die der Virus Scan Server auswertet. Für fremdgestartete Virus Scan Servers ist die Konfigurationsdatei bereits auf der Kommandozeile des Virus Scan Server festgelegt und Sie können diese daher hier nicht ändern.

► Sichern Sie Ihre Eingaben.

Applikationsserver- oder Selbststarter

Bei der Konfiguration eines Virus Scan Server für ABAP-Systeme können Sie, statt des Applikationsserverstarters (vom Anwendungsserver gestartet) einen Selbststarter (z. B. extern als Dienst unter Microsoft Windows NT oder Dämon unter UNIX gestartet) installieren. Beim Applikationsserverstarter befinden sich alle Komponenten auf demselben Host. Im Gegensatz dazu können sich beim Selbststarter der Virus Scan Server und der SAP Web AS auf unterschiedlichen Hosts befinden. Damit können Sie einen nur für eine bestimmte Plattform verfügbaren Virus Scan Server verwenden, selbst wenn der SAP Web AS auf einer anderen Plattform installiert ist.

Virus Scan Server auf einem oder zwei Hosts:



Während des Betriebs wirkt sich diese Unterteilung in Applikations- und Selbststarter vor allem im Computing Center Management System (CCMS) aus. Sie können die Viren-Scanner mit dem CCMS (Transaktion RZ20) in der "Monitorsammlung SAP CCMS Monitors for Optional Components" (nähere Informationen siehe SAP-Webseite) im Monitor Virus Scan Server überwachen. Dabei gibt es folgende Unterschiede:

- Applikationsserverstarter:
In diesem Fall überprüft der Datensammler des CCMS automatisch, ob ein konfigurierter Virus Scan Server erreichbar ist. Ist dies nicht der Fall, löst das CCMS einen Alert aus und startet als Autoreaktion wieder den Virus Scan Server.
- Selbststarter:
In diesem Fall werden die Prozesse zwar vom CCMS überwacht, aber nicht automatisch gestoppt oder gestartet. Allerdings haben diese Selbststarter im CCMS eine eigene MTE-Klasse, der Sie selbst eine Autoreaktionsmethode zuweisen können, um auf Alerts zu reagieren. Sie können z. B. als Autoreaktionsmethode mit der MTE-Klasse CCMS_OnAlert_Email eine E-Mail oder SMS versenden (siehe "Automatische Alert-Benachrichtigung definieren" und "Alerts an das Alert Management (ALM) weiterleiten" auf der SAP-Webseite).



Achten Sie darauf, dass Sie Ihre RFC-Verbindungen mit Secure Network Communications (SNC) sichern wie im SNC-Handbuch beschrieben. Das SNC-Handbuch erhalten Sie auf dem SAP Service Marketplace unter <http://service.sap.com/security>
Security in Detail/Secure System Management.

Weitere Informationen zu Applikationsserverstarter und Selbststarter erhalten Sie in den folgenden beiden Abschnitten:

- Virus Scan Server als Applikationsserverstarter
- Virus Scan Server als Selbststarter installieren

Virus Scan Server als Applikationsserverstarter

Bei dieser Verwendung des Virus Scan Server liegen alle benötigten Komponenten auf einem Host im Arbeitsverzeichnis des SAP-Web-AS-Kernels. Der Virus Scan Server ist in der Standardauslieferung enthalten. Das bedeutet, dass Sie nur dafür sorgen müssen, dass die Voraussetzungen für den Betrieb des Applikationsserverstarters erfüllt sind:

- Sie haben das externe Antivirenprodukt und den zugehörigen Viren-Scan-Adapter gemäß Beschreibung in diesem Handbuch installiert.
- Das Kernel-Verzeichnis enthält folgende Komponenten:
 - vscan_rfc.exe (NT) oder vscan_rfc (UNIX)
 - die aktuelle RFC-Bibliothek bzw. LIBRFC (siehe Hinweis 413708)
 - sapcpp45.dll (NT) oder sapcpp45.<shared ext.> (UNIX)
 - xml63d.dll (NT) oder xml63d<shared ext> (UNIX)

Virus Scan Server als Selbststarter installieren

Der Selbststarter steht Ihnen als Alternative zur Verfügung, falls Sie den Applikationsserverstarter nicht einsetzen können, z. B. in folgenden Fällen:

- Der Kernel des SAP Web AS verwendet 64 Bit und das externe Antivirenprodukt bzw. der externe Viren-Scan-Adapter (VSA) verwendet 32 Bit.
- Der SAP Web AS und das externe Antivirenprodukt unterstützen unterschiedliche Architekturen, z. B. ist der SAP Web AS auf einer AIX-Plattform installiert, das Antivirenprodukt aber nur für Microsoft Windows erhältlich.

- ✓ Der Selbststarter startet die Viren-Scan-Engine über eine lokale XML-Konfigurationsdatei. Im Normalfall ist das die Datei `vscan_rfc.xml`, welche die benötigten Parameter des Viren-Scan-Adapters enthält. Der Start oder das erforderliche Neustarten des Servers muss durch Betriebssystemmittel erfolgen.
- ▶ Kopieren Sie die entsprechende Variante des Virus Scan Server von der CD oder über den SAP Service Marketplace in ein Startverzeichnis.
- ▶ Erzeugen Sie die Konfigurationsdatei über die in der nachfolgenden Tabelle aufgelisteten Befehle, mit denen Sie später auch die bestehende Konfiguration ändern können.

Folgender Aufruf erzeugt die Server sowie VSA-Konfiguration zu `savapi.dll` (Windows) oder `libantivirvsa.so.<version>` (UNIX):

Um neue Parameter zu setzen oder vorhandene zu überschreiben, übergeben Sie bei einem erneuten Aufruf weitere Befehle und Optionen, die dann in der XML-Konfiguration gesetzt werden.

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

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

In unserem Beispiel können Sie den Aufruf wie folgt ändern:

Windows: `vscan_rfc get_config -V <Laufwerk>:\vsa\savapi.dll -cfg <Laufwerk>:\vsa\vscan_rfc.xml -a VSCAN_LOCAL -g <Hostname des SAP-Gateways> -x <Servicename des SAP-Gateways> -c <SAP-Codepage>`

UNIX: `vscan_rfc get_config -V <Laufwerk>:/usr/local/AntiVir/libantivirvsa.so.<version> -cfg <Laufwerk>/usr/local/AntiVir/vscan_rfc.xml -a VSCAN_LOCAL -g <Hostname des SAP-Gateways> -x <Servicename des SAP-Gateways> -c <SAP-Codepage>`

Folgende Konfigurationsbefehle für den Selbststarter stehen zur Verfügung:

Befehl	Plattform	Kommentar
help	alle	Ruft die Online-Hilfe zu den Befehlen und Optionen auf.
regonly	alle	Registriert den Virus Scan Server nur am Gateway, ohne dabei die darunter liegende AntiVir Engine zu starten. Das CCMS verwendet diesen Befehl, um anschließend die RFC-Funktion <code>VSCAN_RFC_INIT</code> aufzurufen. Beachten Sie, wenn Sie diesen Befehl außerhalb des CCMS verwenden, dass der Server nicht betriebsbereit ist.
get_config	alle	Empfängt die VSA- sowie eigene Serverkonfiguration und speichert diese in eine lokale XML-Konfiguration. (Option <code>-cfg <Datei></code> ist hierfür zwingend notwendig). Die Optionen, die über die Befehlszeile empfangen wurden, werden dabei als Serverkonfiguration gespeichert. Wenn Sie keine Befehlszeilenoptionen angeben, werden die voreingestellten Werte gesetzt. Verwenden Sie diesen Befehl zu Beginn der Einrichtung eines Selbststarters. Bei Nichtvorhandensein der Datei, die über die Option <code>-cfg</code> angegeben wurde, wird eine neue erzeugt.

Befehl	Plattform	Kommentar
install	NT	<p>Installiert einen "neuen" VSCAN_XX Dienst im Service Control Manager (SCM) von Microsoft Windows NT.</p> <p>Dieser Befehl benötigt zwingend die Option -cfg mit Angabe einer lokalen Konfiguration. Bei erfolgreicher Initialisierung des VSA wird der Service installiert. Wenn Sie weitere Optionen angeben, werden diese auch in der verwendeten XML-Datei gespeichert. Die Option -srvc gibt die Nummer des Service an, d. h. Sie können bis zu 100 Dienste auf einem Host installieren. Standardwert für -srvc ist 00.</p>
remove	NT	<p>Löscht einen vorhandenen VSCAN_XX Dienst im Service Control Manager von Microsoft Windows NT.</p> <p>Über die Option -srvc können Sie den Service genauer spezifizieren. Beispiel: vscan_rfc remove -srvc 1 löscht den vorhandenen Dienst VSCAN_01.</p>
start	NT	<p>Startet einen installierten VSCAN_XX-Dienst. Dieser Befehl startet den Dienst mit den angegebenen Optionen.</p> <p>Der Microsoft-Windows-NT-Befehl "net start VSCAN_XX" startet den vorher installierten Dienst nur unter Verwendung der lokalen Konfiguration.</p>
stop	NT	<p>Stoppt einen laufenden VSCAN_XX-Dienst. Dieser Befehl entspricht dem Microsoft-Windows-NT-Befehl "net stop ...".</p>

Zusätzlich zu den Befehlen können Sie folgende Optionen für Selbststarter angeben:

Option	Plattform	Kommentar
-a	alle	Programm-ID der RFC-Destination, z. B. VSCAN_LOCAL
-g	alle	Hostname des SAP-Gateways
-x	alle	Servicename des SAP-Gateways, z. B. sapgw00
-cfg	alle	Vollständige Pfadangabe der lokalen XML-Konfigurationsdatei
-f	alle	Pfadangabe der zu verwendenden Trace-Datei
-l	alle	Trace-Level der Trace-Datei: 0 := Fehler 1 := Fehler und Warnungen (z. B. Vireninfectionen) 2 := Fehler, Warnungen, Aufrufe der Viren-Scan-Engine 3 := zusätzliche Informationen, alle RFC-Aufrufe, Speicheroperationen
-c	alle	SAP-Codepage bei NON-UNICODE-Virus-Scan-Servers
-v	alle	Pfadangabe des zu verwendenden Viren-Scan-Adapters. Falls Sie diese Option nicht setzen, wird die Umgebungsvariable VSA_LIB verwendet.
-p	alle	Profilname (Standard: VSA_CONFIG) für die aktuelle VSA-Konfiguration. Diese Option dient der Unterscheidung bei Verwendung mehrerer (unterschiedlicher) VSA-Konfigurationen in einer XML-Datei.
-T	alle	Maximale Anzahl von Threads, die der Server verwenden darf. Mögliche Werte: 1 bis 999.

Option	Plattform	Kommentar
-m	alle	Minimale Anzahl von Threads, die der Server verwenden soll. Hinweis: Es wird hier immer der Mittelwert von -m und -T als Threads offen gehalten.
-L	alle	Pfadangabe einer SNC-Bibliothek
-S	alle	Der SNC-Name dieser Instanz. Hinweis: Das Setzen von -L, -S oder -Q aktiviert SNC für den Server!
-Q	alle	SNC-Sicherheitsstufe. Mögliche Werte: 1:=Authentifizierung 2:=Schutz der Integrität 3:=Verschlüsselung 7:=Mindeststufe 8:=DEFAULT 9:=Höchststufe
-P	alle	Der SNC-Name der SAP-Instanz. Achtung: Wenn Sie diesen Namen setzen, werden nur Anfragen von SAP-Instanzen dieser SNC-Identität angenommen
-I	alle	Zeitüberschreitung in Sekunden für die internen Instanzoperationen RELOAD und SHUTDOWN.
-n	alle	Maximale Anzahl von Trace-Zeilen für das Speicher-Trace. Standardwert: 10000
-h	alle	Aufbewahrungszeit in Sekunden für Speicher-Trace: Standardwert: 86400 Sekunden
-srvc	NT	Dienstnummer der Microsoft-Windows-NT-Befehle install remove start stop
-daemon	UNIX	Startet den Virus Scan Server mit fork() als Dämonprozess.

Betrieb des Selbststarters

Sie können den Selbststarter auch als Dienst unter Microsoft Windows NT oder als Dämon unter UNIX betreiben.

Betrieb als Dienst Mit dem Microsoft Windows Service Control Manager (SCM) können Sie den Virus Scan Server als Dienst installieren. Sie können bis zu 100 solcher Dienste installieren (mit der Nummerierung 00 bis 99).

Durch den Betrieb als Dienst stehen Ihnen die Betriebssystemmittel für das Monitoring zur Verfügung, z. B. das Event Log. Außerdem können Sie mit dem SCM den Virus-Scan-Server-Dienst nach einem Abbruch neu starten. Über die Microsoft Management Console (MMC) können Sie den installierten Dienst auch remote überwachen und steuern.

► Installieren Sie einen Dienst mit

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

-
- Installieren Sie weitere Dienste (VSCAN_<xx>) mit

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



Sie müssen unbedingt die lokale Konfigurationsdatei (Option -cfg) angeben. Der Dienst wird nur nach erfolgreicher Initialisierung des Virus Scan Adapter sowie der Prüfung des SAP-Gateways installiert.

Betrieb als
Dämon (UNIX)

Sie können den Virus Scan Server als Dämon direkt beim Betriebssystemstart starten.

- Starten Sie einen Dämon mit

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

Sie können den Dämon mit Betriebssystemmitteln überwachen (CRONTAB, INITTAB).

Konfiguration des Selbststarters

Um den Selbststarter zu konfigurieren, haben Sie folgende Möglichkeiten:

- Sie rufen `get_config` erneut auf und gehen analog Abschnitt [Virus Scan Server als Selbststarter installieren](#) – Seite 49 vor.
- Sie bearbeiten die XML-Konfigurationsdatei direkt.
- Sie synchronisieren die Einstellungen über die IMG-Aktivität (siehe Kapitel [Virus Scan Server definieren](#) – Seite 44, Transaktion VSCAN).

Bei dieser Konfigurationsmöglichkeit werden die Parameter `Trace-Level` (Option -I), `Codepage` (Option -c), `Max. Threads` bzw. `Max. Instanzen` (Option -T) und `VSA_LIB` (Option -V) über die Taste Lokal in die angegebene Konfiguration gesichert. Falls Sie das Feld Konfiguration frei lassen, werden die Werte beim Selbststarter in der in Verwendung befindlichen XML-Konfiguration gesichert.



Nur falls bereits eine XML-Datei vorhanden ist, werden die Werte gesichert.

6.1.3 Viren-Scan-Profile definieren

Anwendungsprogramme benutzen Viren-Scan-Profile, um Daten auf Viren hin zu überprüfen. Ein Viren-Scan-Profil enthält eine Auflistung von Scanner-Gruppen, die ein Dokument prüfen. Außerdem können Sie mit einem Viren-Scan-Profil Konfigurationsparameter für den Viren-Scanner vergeben. Wenn Sie mit diesem Viren-Scan-Profil auf Viren prüfen, erhält der Viren-Scanner die Parameter.

Ein Viren-Scan-Profil benennt Schritte, die bei der Virenprüfung ablaufen sollen. Ein Schritt ist entweder ein Viren-Scanner, der über die Scanner-Gruppe gefunden wird, oder ein Schritt benennt wiederum ein Viren-Scan-Profil, das dann als Teil des umschließenden Viren-Scan-Profils ausgeführt wird.

Ein Viren-Scan wird unter dem Namen eines Viren-Scan-Profils durchgeführt. Mit dem Profil kann der Systemadministrator den Viren-Scan pro Komponente aktivieren oder deaktivieren.

Standardmäßig liefert jede SAP-Anwendung, die einen Viren-Scan integriert, ein Viren-Scan-Profil aus. Der Name dieser Viren-Scan-Profile ist wie folgt aufgebaut:

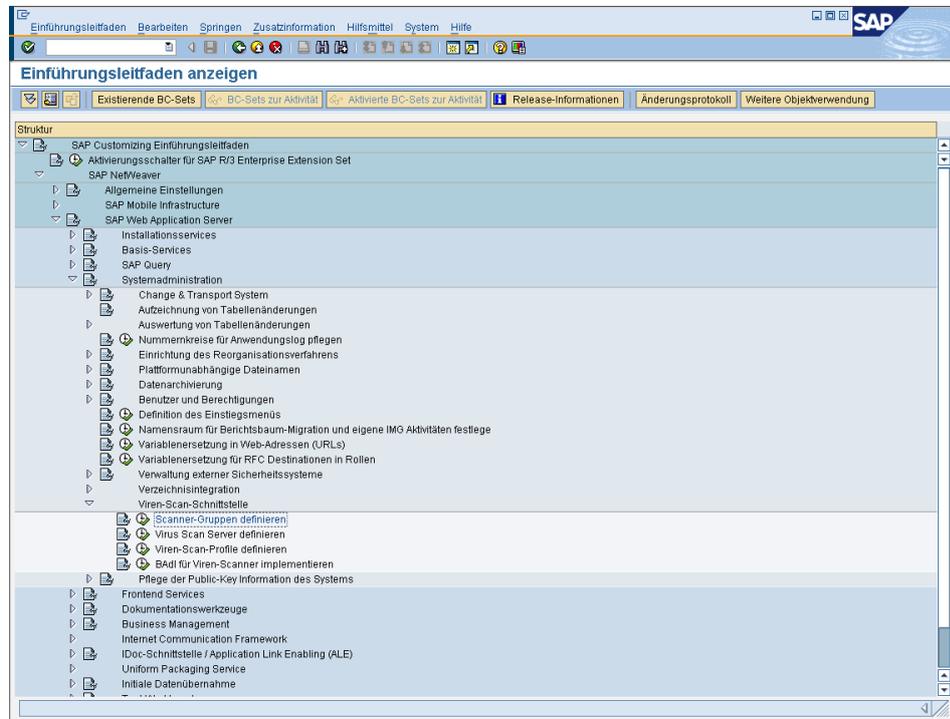
```
/<Name des Pakets der Anwendung>/<Name der Funktion>.
```

Überprüfen Sie die von SAP ausgelieferten Viren-Scan-Profile und legen Sie fest, für welche Komponenten Sie den Viren-Scan aktivieren oder deaktivieren.

Wenn Sie eigene Viren-Scan-Profile anlegen, stehen Ihnen hierfür die Namensräume Y* und Z* zur Verfügung.

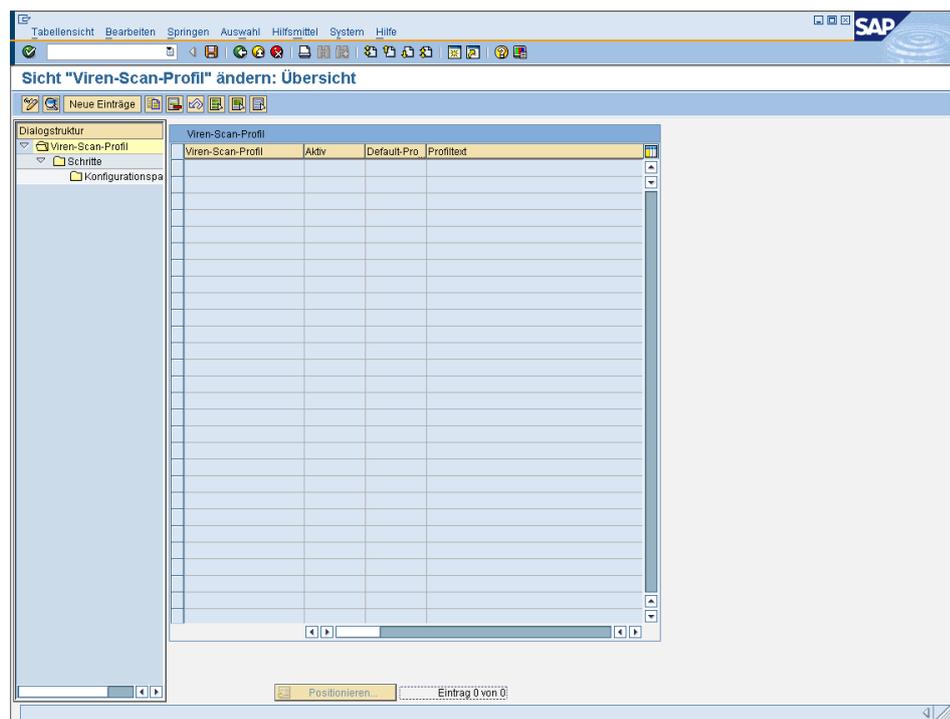
✓ Sie haben Scanner-Gruppen angelegt.

► Wählen Sie im Einführungsleitfaden (IMG) **SAP Web Application Server/ Systemadministration/Viren-Scan-Schnittstelle**.



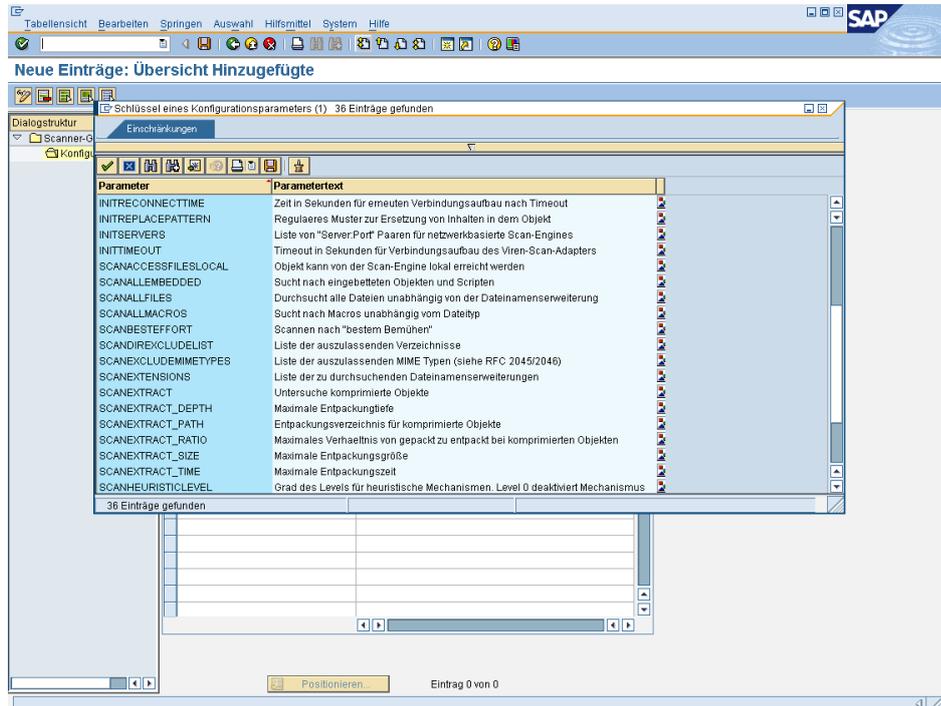
► Wählen Sie neben **Viren-Scan-Profil definieren** die Option **Ausführen**.

↳ Sie gelangen auf das Bild **Sicht: "Viren-Scan-Profil" ändern: Übersicht**.

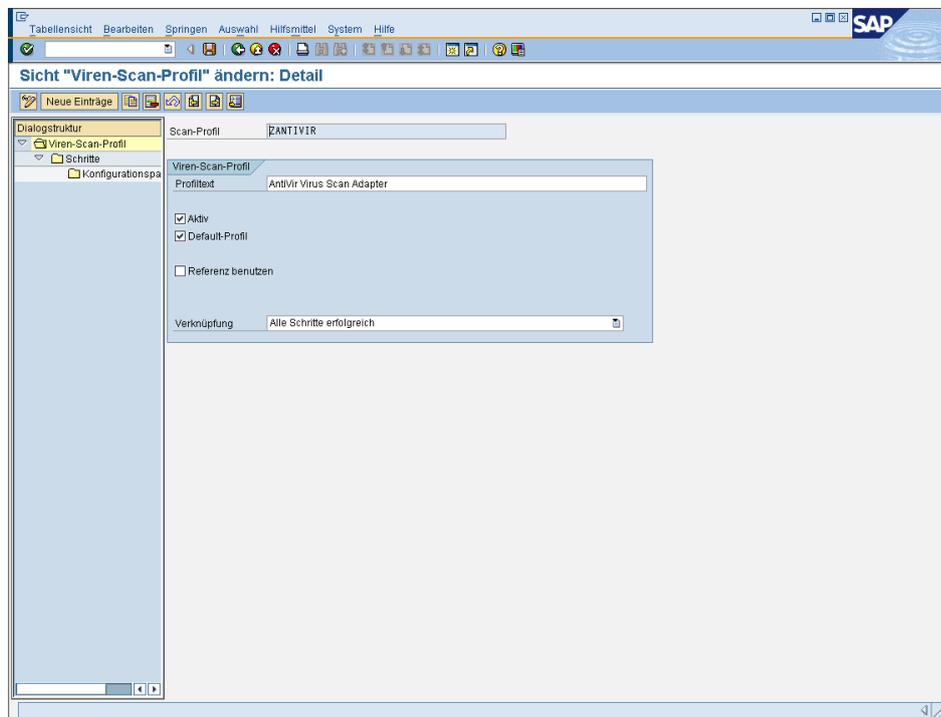


► Wählen Sie **Neue Einträge**.

↳ Sie gelangen auf das Bild **Neue Einträge: Übersicht Hinzugefügte**.



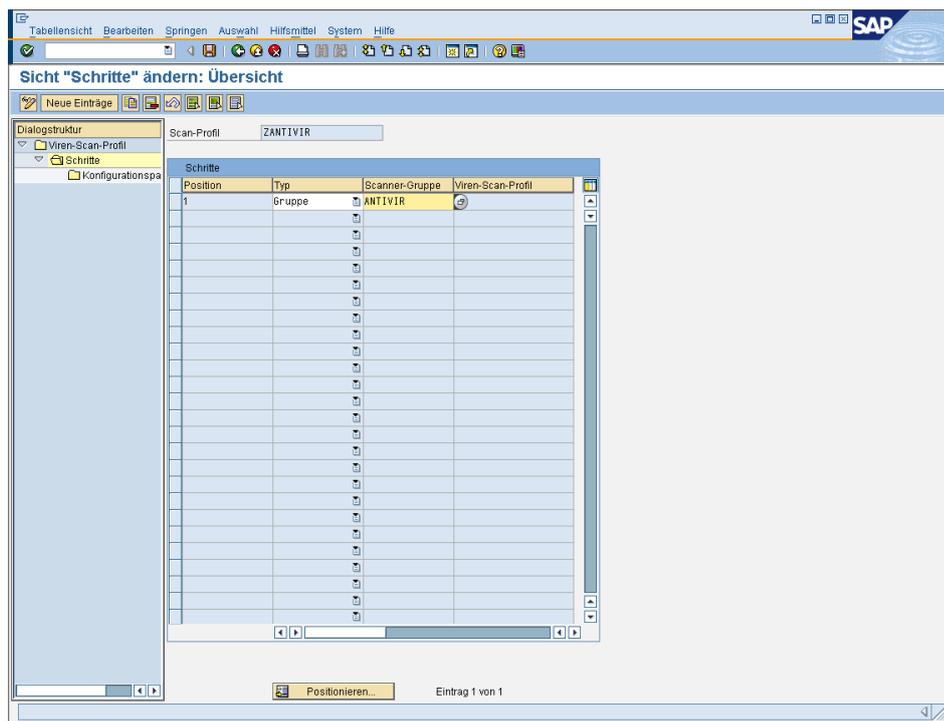
► Geben Sie die Daten für die Definition eines Viren-Scan-Profiles an (siehe folgende Tabelle):



Feld	Mögliche Werte	Kommentar
Scan-Profil		Gibt den Namen eines Viren-Scan-Profiles an.
Profiltext		Erklärender Text für ein Viren-Scan-Profil.
Aktiv		<p>Gibt an, dass dieses Viren-Scan-Profil aktiv ist.</p> <p>Nur wenn dieses Kennzeichen gesetzt ist, kann das Viren-Scan-Profil verwendet werden.</p> <p>SAP-Applikationen können fest vorgegebene Profilnamen verwenden, welche ausgeliefert werden. In der Voreinstellung sind diese Profile nicht aktiv, so dass das Anwendungsprogramm ohne Viren-Scan arbeitet.</p> <p>Durch Setzen dieses Kennzeichens können Sie den Viren-Scan pro Anwendung aktivieren.</p>
Default-Profil		<p>Kennzeichen, dass dieses Viren-Scan-Profil das Default-Profil ist.</p> <p>Sie dürfen dieses Kennzeichen für höchstens ein Viren-Scan-Profil setzen. Dieses Viren-Scan-Profil wird benutzt,</p> <ul style="list-style-type: none"> -wenn eine Anwendung ohne Angabe eines Viren-Scan-Profiles einen Viren-Scanner anfordert. -wenn ein Viren-Scan-Profil angefordert wird, welches das Kennzeichen Referenzprofil benutzen gesetzt hat und das Feld Referenzprofil leer ist.
Referenz benutzen		Um mehrere Anwendungen über das gleiche Viren-Scan-Profil zu bedienen, setzen Sie das Kennzeichen Referenz benutzen und geben das Referenzprofil an.

Feld	Mögliche Werte	Kommentar
Referenzprofil	Die Wertheilfe bietet alle bereits definierten Profile an. Wenn Sie das Feld frei lassen, verwendet das System das Default-Profil.	Gibt den Namen des Referenzprofils an. Da ein Viren-Scan-Profil ein anderes Viren-Scan-Profil als Referenzprofil nutzen kann, können Sie mehrere Anwendungen über dasselbe Viren-Scan-Profil bedienen. Wenn im Viren-Scan-Profil das Kennzeichen Referenzprofil verwenden gesetzt ist, gibt dieses Feld den Namen des zu verwendenden Referenzprofils an. Statt der Einstellungen des aktuellen Viren-Scan-Profiles werden dann die Einstellungen des Referenzprofils benutzt. Hierdurch können mehrere Viren-Scan-Profile die Einstellungen eines gemeinsamen Referenzprofils nutzen, z. B. die zu verwendenden Scanner-Gruppen.
Verknüpfung	Alle Schritte erfolgreich: Alle Schritte müssen die Virenprüfung ohne Fehler durchgeführt haben. Mindestens ein Schritt erfolgreich: Es ist ausreichend, dass ein Schritt die Virenprüfung fehlerfrei durchführen konnte.	Gibt die Art der logischen Verknüpfung für die Schritte im Viren-Scan-Profil an. Wenn für ein Viren-Scan-Profil mehrere Schritte definiert sind, die bei der Virenprüfung mit dem Profil abgearbeitet werden, können Sie mit diesem Feld steuern, wie das Gesamtergebnis der Virenprüfung zu bewerten ist. Durch die Verwendung mehrerer Schritte können Sie Dokumente mit Scan-Engines verschiedener Hersteller gleichzeitig scannen. Das Programm interpretiert eine Virenprüfung nur dann als fehlerfrei, wenn die Scan-Engine den Rückgabewert Überprüfung erfolgreich durchgeführt oder (beim Bereinigen) Bereinigung erfolgreich durchgeführt liefert. Alle anderen Rückgabewerte gelten als nicht erfolgreiche Virenprüfung. Dazu gehören auch Situationen wie z. B. -Das Programm hat das Dokument nicht überprüft, weil die Dateinamenserweiterung als unkritisch eingestuft wird. -Das Programm konnte das Dokument nicht überprüfen, weil das Dokument ein Archiv mit Kennwortschutz ist. -Die Scan-Engine ist veraltet.

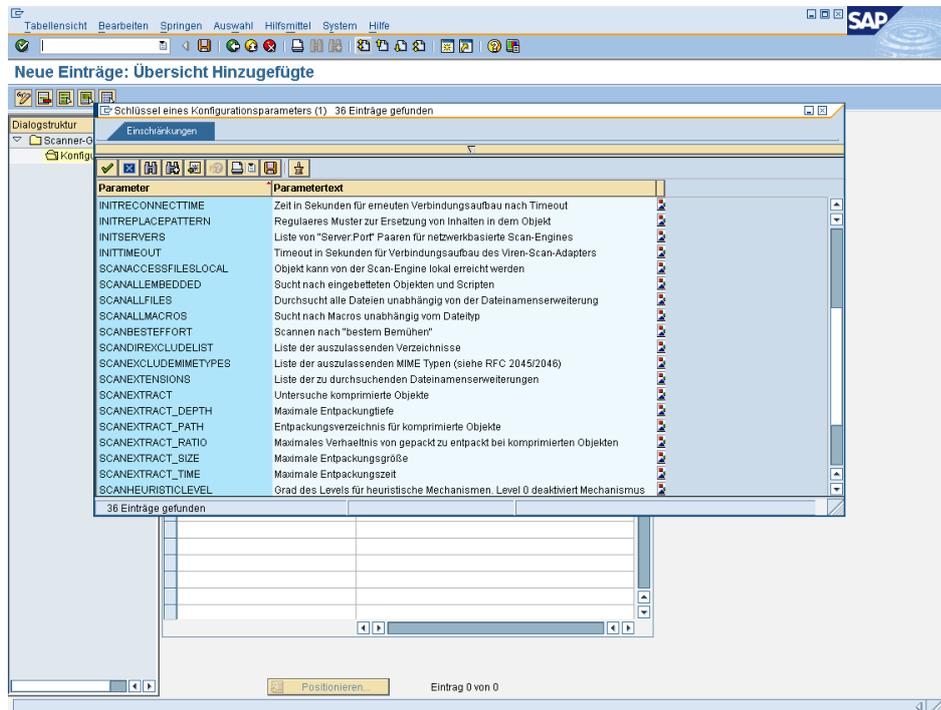
- ▶ Sichern Sie Ihre Eingaben.
- ▶ Um Schritte für das Profil zu definieren, markieren Sie in der Dialogstruktur den Knoten **Schritte** per Doppelklick.
- ▶ Wählen Sie **Neue Einträge**.



► Geben Sie für die Definition eines Schrittes des Viren-Scan-Profiles folgende Daten an:

Feld	Mögliche Werte	Kommentar
Position	<ganze Zahl>	Gibt die Position der Scanner-Gruppe im Viren-Scan-Profil an. Wenn ein Viren-Scan-Profil mehrere Scanner-Gruppen benutzt, bringen Sie diese durch Vergabe einer Positionsnummer in die gewünschte Reihenfolge.
Typ	Gruppe oder Profil	Gibt an, ob es sich bei einem Schritt im Viren-Scan-Profil um eine Scanner-Gruppe oder um ein anderes Viren-Scan-Profil handelt. Wenn Sie Gruppe wählen, verwendet das System bei der Virenprüfung einen Virus Scan Server dieser Gruppe (oder eine BAdI-Implementierung). Wenn Sie Profil wählen, arbeitet das Programm anstelle dieses Schrittes das angegebene Viren-Scan-Profil ab. Sie können beliebige Bedingungen definieren, indem Sie die Schritte des Viren-Scan-Profiles mit der Verknüpfungsart der Schritte (UND/ODER) kombinieren.
Scanner-Gruppe	Die Wertheilfe bietet alle vorhandenen Scanner-Gruppen an.	Fasst mehrere Virus Scan Servers zusammen oder ermöglicht die Verwendung einer BAdI-Implementierung. Alle Virus Scan Server einer Scanner-Gruppe erhalten den gleichen Satz an Konfigurationsparametern und werden daher die gleiche Scan-Engine verwenden.
Viren-Scan-Profil	Die Wertheilfe bietet alle vorhandenen Profile an.	Gibt den Namen eines Viren-Scan-Profiles an, das Sie als Schritt in das Profil einbinden, das Sie gerade bearbeiten.

- ▶ Sichern Sie Ihre Eingaben.
- ▶ Um Konfigurationsparameter für einen Schritt anzulegen, markieren Sie den Knoten **Konfigurationsparameter** per Doppelklick.



- ▶ Wählen Sie **Neue Einträge**.
- ▶ Geben Sie für die Definition der Konfigurationsparameter folgende Daten an:

Feld	Mögliche Werte	Kommentar
Parameter	Die Wertheilfe bietet alle vorhandenen Konstanten an.	Gibt den Schlüssel eines Konfigurationsparameters an. Ein Viren-Scanner benötigt Konfigurationsdaten. Die Menge der möglichen Konfigurationsparameter ist von SAP in Form einer vorgegebenen Menge an symbolischen Konstanten definiert.
Wert	<Wert>	Gibt den vom Hersteller angegebenen Wert eines Konfigurationsparameters an.

- ▶ Sichern Sie Ihre Eingaben.
 - ↳ Damit haben Sie ein Viren-Scan-Profil definiert und somit den letzten Konfigurationsschritt für den Viren Scan Server vorgenommen. Abschließend können Sie die Konfiguration überprüfen (siehe Kapitel [Problemanalyse des Virus Scan Server](#) – Seite 60).

6.1.4 BAdI für Viren-Scanner implementieren

Mit dem Business Add-In VSCAN_INSTANCE können Sie eigene Viren-Scanner in die Viren-Scan-Schnittstelle einbinden.

Um die BAdI-Implementierung zu integrieren, setzen Sie beim Anlegen der Scanner-Gruppe das Kennzeichen **BAdI-Implementierung**. Wenn Sie anschließend eine Virenprüfung mit dieser Scanner-Gruppe durchführen, ruft das Programm Ihre

Implementierung des BAdI für den Gruppennamen als Filterwert auf und Sie können eine Instanz Ihrer Scanner-Implementierung übergeben.

Legen Sie für jede Scanner-Gruppe, die die BAdI-Implementierung nutzen soll, eine Implementierung an. Sie können eine Implementierung für mehrere Filterwerte (Gruppennamen) benutzen.

SAP liefert keine Default-Implementierung aus. Stattdessen steht mit dem Virus Scan Server eine eigene Komponente bereit, die Scan-Engines zertifizierter Hersteller in die Viren-Scan-Schnittstelle integriert.

- ✓ Sie haben eine Scanner-Gruppe angelegt, welche Ihre Implementierung ansprechen soll.
- ▶ Wählen Sie im Einführungsleitfaden (IMG) **SAP Web Application Server/ Systemadministration/Viren-Scan-Schnittstelle**.
- ▶ Wählen Sie neben **BAdI für Viren-Scanner implementieren** die Option **Ausführen**.
 - ↳ Sie gelangen auf das Dialogfenster **BAdI-Builder: Alle Implementierungen zu Definition VSCAN_INSTANCE**.
- ▶ Wählen Sie **Anlegen**.
 - ↳ Sie gelangen auf das Dialogfenster **BAdI-Builder: Anlegen Implementierung**.
- ▶ Geben Sie im Feld **Implementierungsname** einen Namen an.
 - ↳ Sie gelangen auf das Bild **BAdI-Builder: Ändern Implementierung <Implementierungsname>**.
- ▶ Geben Sie im Feld **Kurztext zur Implementierung** eine kurze Beschreibung ein.
Um für Ihre Implementierung Filterausprägungen anzugeben:
- ▶ Wählen Sie bei **Filter-Ausprägungen** die Taste **Zeile einfügen** und geben mit der Wertehilfe Ihre Gruppe an.
- ▶ Sichern Sie Ihre Eingaben.
 - ↳ Sie haben für die Scanner-Gruppe eine Implementierung angelegt. Die weitere Vorgehensweise wird in der Dokumentation zum Interface IF_EX_VSCAN_INSTANCE beschrieben.

6.2 Problemanalyse des Virus Scan Server

Der Virus Scan Server gibt Fehler, Warnungen oder Zusatzinformationen entweder in eine Datei aus oder schreibt sie in den Speicher des Servers. Mit dem Analysewerkzeug VSCANTRACE können Sie diesen Speicherinhalt abfragen und ausgeben, um alle registrierten Virus Scan Servers während ihres produktiven Betriebs auf Fehler hin zu analysieren.

Beim Start des Servers ist das Trace für die Speicherausgabe deaktiviert. Aktivieren Sie es nur in Problemfällen, da es die Performance des Servers beeinträchtigt. Die Einstellungen zur Speicherausgabe sind nur eine bestimmte Zeit lang gültig (Vorschlagswert ist 24 Stunden). Danach werden sie deaktiviert.

- ✓ Damit Sie den Speicher-Trace verwenden können, muss mindestens ein Virus Scan Server aktiv sein.
- ▶ Starten Sie Transaktion VSCANTRACE.
- ▶ Wählen Sie den Server entweder über die Eingabehilfe, die alle definierten Virus Scan Servers aus Tabelle VSCAN_SERVER anzeigt, oder geben Sie ihn direkt an. Dazu muss er am SAP-Gateway über eine in Transaktion SM59 definierte RFC-Destination gestartet worden sein.
- ▶ Bestätigen Sie Ihre Eingabe mit **Enter**.

-
- ↳ Die Verbindung zum Virus Scan Server wird hergestellt. Kommt die Verbindung zum Server zustande, ist die Ampel grün.
 - ▶ Wählen Sie **Speicher**.
Andernfalls wird das Trace in eine Datei ausgegeben, die Sie unter den Entwickler-Traces (Transaktion ST11, Dateiname *dev_VSCAN_<Hostname>.trc*) anzeigen können.
 - ↳ Der aktuelle Trace-Level wird angezeigt.
 - ▶ Um für den Trace-Level einen neuen Wert zu setzen, markieren Sie die gewünschten Trace-Komponenten und wählen anschließend die Taste **Aktivieren**.



Sie können das Speicher-Trace mit der Taste **Deaktivieren** vollständig deaktivieren, die Fehlerausgabe in die Trace-Datei dagegen nicht. Sie können die Fehlerausgabe also nicht unterdrücken, indem Sie den Trace-Level für die Datei auf den Wert 0 setzen.

Wenn Sie die Auswahl von **Speicher** auf **Datei** oder umgekehrt ändern, können Sie den bereits für diese Option gewählten Trace-Level für die einzelnen Komponenten mit der Taste **Kopieren** anzeigen. Dabei wird die Auswahloption jeder aktiven Komponente aktiviert.

- ▶ Um das Speicher-Trace auszugeben, wählen Sie die Option **Ausführen**.
 - ↳ Sie gelangen auf die Übersicht, welche die Verfügbarkeit der verwendeten Anti-Virus-Engine, die Auslastung des Virus Scan Server, den der aktuellen Trace-Level für den Speicher sowie eine HTML-Ausgabe der aktuellen Trace-Informationen anzeigt.

In der Übersicht haben Sie folgende Optionen:

- **Aktualisieren**: Aktualisiert die Liste.
- **Löschen**: Löscht die Trace-Ausgabe.
- **Exportieren**: Exportiert die Liste in eine lokale Datei.
- **Status**: Gibt den aktuellen Status des verwendeten Virus Scan Server auch bei deaktiviertem Speicher-Trace aus. Diese Ausgabe enthält neben technischen Informationen zum Virus Scan Server auch dessen Konfiguration, sowie Informationen des geladenen Viren-Scan-Adapters samt Anti-Virus-Engine.
- **Stopp**: Stoppt den Virus Scan Server.
- **Konfiguration**: Verzweigt in den Anzeigemodus der IMG-Aktivität **Viren Scan Server** definieren.
- **Test**: Verzweigt in die Transaktion VSCANTEST.

6.3 Installation des Virus Scan Server testen

Mit dieser Vorgehensweise überprüfen Sie das Funktionieren des von Ihnen konfigurierten Virus Scan Server.

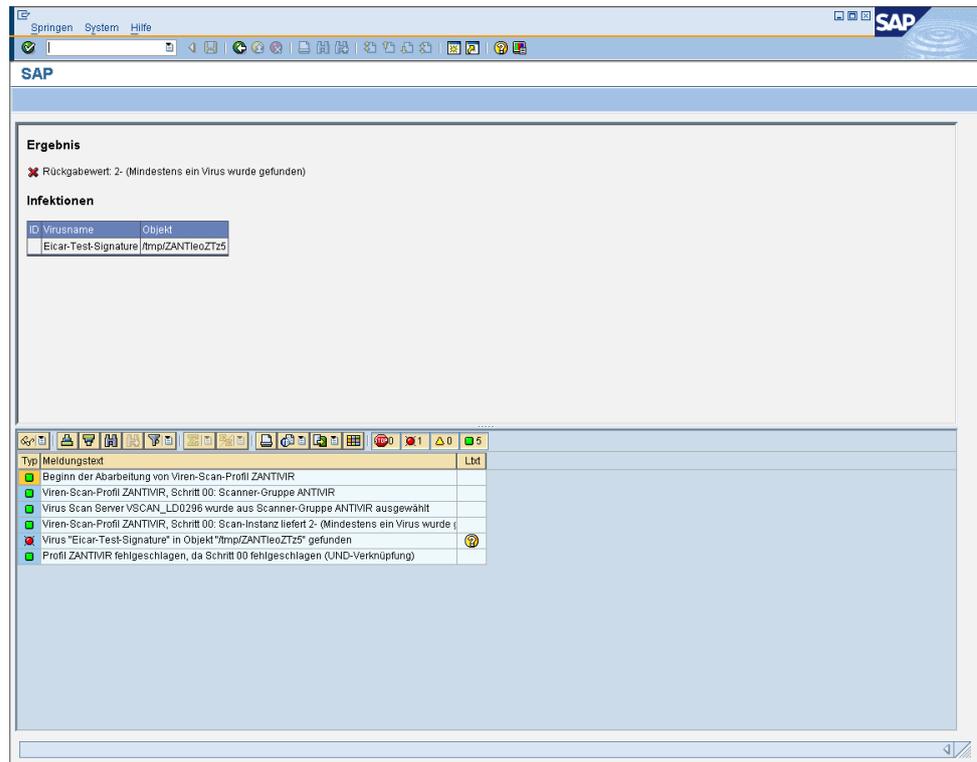
- ▶ Starten Sie Transaktion VSCANTEST.
- ▶ Geben Sie das zu prüfende Objekt an, entweder die ausgelieferten Testdaten oder Ihre eigene lokale Datei.

The screenshot shows the SAP 'Test für die Viren-Scan-Schnittstelle' (Test for the Virus Scan Interface) dialog box. The window title is 'Test für die Viren-Scan-Schnittstelle' and it features the SAP logo in the top right corner. The dialog is divided into three main sections:

- Zu prüfendes Objekt (Object to be tested):** This section has a radio button selected for 'Testdaten' (Test data). Below it, a dropdown menu shows 'EICAR Anti-Virus test file'. There are also two unselected radio buttons: 'Lokale Datei' (Local file) and 'Datei auf Applikationsserver' (File on application server), each followed by an empty text input field.
- Auswahl des Scanners (Scanner selection):** This section has a radio button selected for 'Viren-Scan-Profil' (Virus Scan Profile). Below it, a text input field contains '(Defaultprofil)'. There are also two unselected radio buttons: 'Scanner-Gruppe' (Scanner group) and 'Virus Scan Server', each followed by an empty text input field.
- Allgemeine Einstellungen (General settings):** This section has a label 'Aktion' (Action) followed by a dropdown menu currently set to 'Nur überprüfen' (Only check).

- ▶ Wählen Sie das zu testende Viren-Scan-Profil, die Scanner-Gruppe oder den Virus Scan Server aus.
- ▶ Wählen Sie eine Aktion aus.

- Bei **Nur überprüfen** untersucht das von Ihnen verwendete Antivirenprodukt die Daten auf Viren hin und gibt ein Ergebnis aus:



- Bei **Prüfen und bereinigen** versucht das Produkt, die Daten auch zu bereinigen, falls ein Virenbefall diagnostiziert wird.

6.4 Kommentiertes Beispielprogramm

Ein kommentiertes Beispielprogramm finden Sie auf der SAP-Webseite.

7 Java-spezifische Konfiguration

Dieses Kapitel beschreibt die Konfiguration der Viren-Scan-Schnittstelle für Java-Systeme. Die Texte wurden der SAP-Webseite entnommen.

Der Virus Scan Provider ist der Service der J2EE Engine der den SAP-Anwendungen der Engine die Schnittstelle `tc/sec/vsi/interface` zur Verfügung stellt.

Je nach Ihren Systemvoraussetzungen wählen Sie eine Installationsart für den Virus Scan Provider aus:

- **Viren-Scan-Adapter für reine Java-Installation:**
Diese Vorgehensweise beschreibt den Normalfall, bei dem Sie einen lokalen Viren-Scan-Adapter verwenden. Der Viren-Scan-Adapter ist eine native dynamische Bibliothek eines Drittanbieters, die direkt in die Prozessumgebung der J2EE Engine geladen werden kann. Damit können Sie Speicherinhalte direkt auf Viren hin überprüfen, wodurch eine hohe Performance gewährleistet ist.
- **Virus Scan Server für reine Java-Installation:**
Diese Vorgehensweise beschreibt den Sonderfall, bei dem die Plattform- oder Prozessarchitektur das Einbinden eines Viren-Scan-Adapters nicht direkt zulässt. Dies ist z. B. der Fall, wenn das erforderliche Betriebssystem von SAP NetWeaver nicht mit dem des externen Antivirenprodukts übereinstimmt. Dann verwenden Sie einen Virus Scan Server. Der Virus Scan Server kommuniziert über TCP/IP (SAP-RFC-Protokoll) mit der J2EE Engine und greift über einen Viren-Scan-Adapter auf das externe Antivirenprodukt zu.
- **Viren-Scan-Adapter oder Virus Scan Server für integrierte Installation (Java und ABAP)**

Beide reinen Java-Installationen bieten dieselbe Schnittstelle in `Instancejava` aus dem Paket `com.sap.security.core.server.vsi.api` an.

Die Konfiguration des Virus-Scan-Provider-Services ist im Configuration Manager der J2EE Engine abgelegt. Eine graphische Administration ist über den Visual Administrator möglich.

Voraussetzung: Sie sind Administrator der J2EE Engine.

Viren-Scan-Adapter für reine Java-Installation

Nachdem Sie das externe Antivirenprodukt samt zertifiziertem Adapter installiert haben, brauchen Sie im Feld `VSA_LIB` nur noch den Pfad zum Adapter einzutragen.

Virus Scan Server für reine Java-Installation

- ▶ Starten Sie das Standalone-Gateway.
- ▶ Starten Sie den Virus Scan Server mit den Optionen `-a`, `-x` und `-g` wie in [Virus Scan Server als Selbststarter installieren](#) – Seite 49 beschrieben. Geben Sie bei Option `-a` die Programm-ID unter Beachtung der Namenskonvention (Groß- und Kleinschreibung; Präfix `VSCAN_`) an.
- ▶ Richten Sie im Visual Administrator den Virus Scan Provider als Virus Scan Server ein wie in [Virus Scan Provider definieren](#) – Seite 70 beschrieben.
 - Geben Sie als Namen genau die Programm-ID an, die Sie oben unter Option `-a` definiert haben. Allerdings müssen Sie das Namenspräfix `VSCAN_` weglassen, da es automatisch hinzugefügt wird.
 - Geben Sie Servereinstellungen an, die mit denen des oben definierten Providers übereinstimmen. Geben Sie `-g` und `-x` wie unter Schritt 2 definiert an.

Viren-Scan-Adapter oder Virus Scan Server für integrierte Installation (Java und ABAP)

Führen Sie folgende Schritte durch:

- [Scanner-Gruppen definieren](#) – Seite 67
- [Virus Scan Provider definieren](#) – Seite 70
- [Viren-Scan-Profil definieren](#) – Seite 73

8 Java-spezifische Konfiguration unter SAP NetWeaver 2004(s) und KMC

Dieser Kapitel beschreibt die Einbindung des Avira AntiVir Virus Scan Adapters unter NetWeaver mit Java Engine über den Visual Administrator und die KMC Anbindung.

8.1 Konfiguration über den Visual Administrator

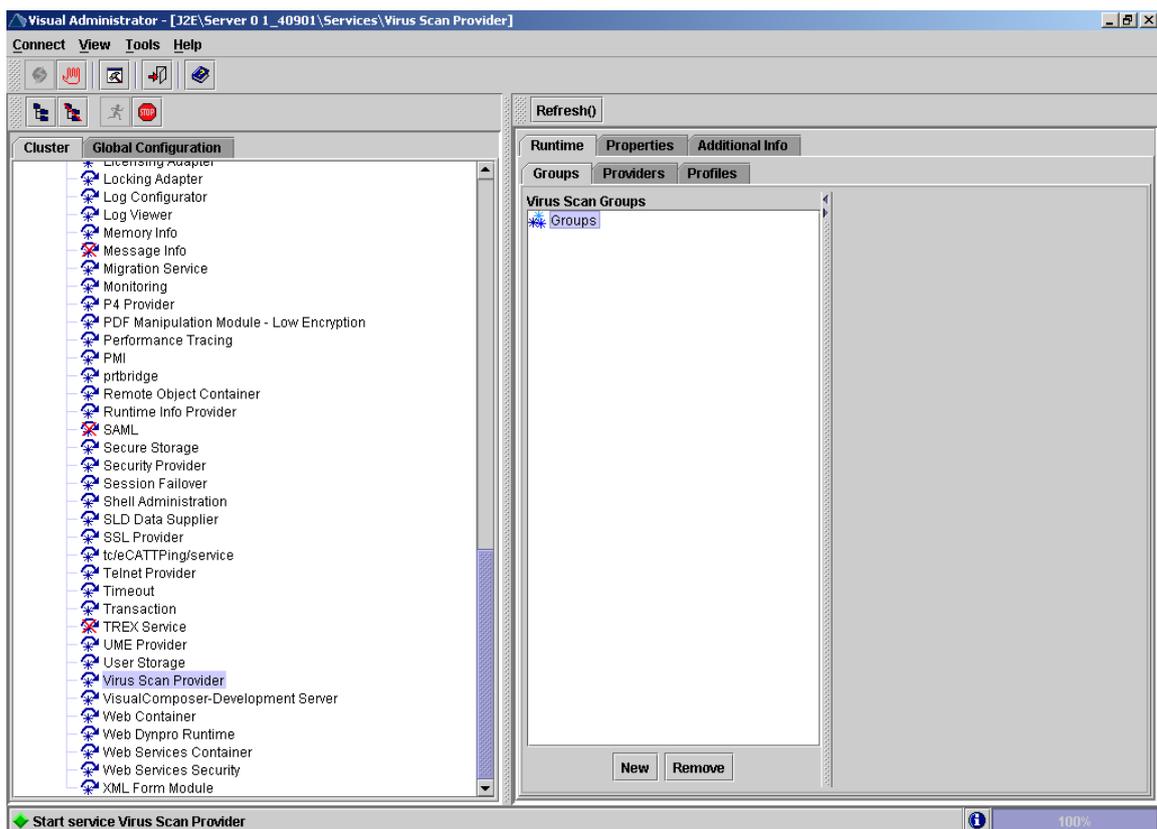
Führen Sie folgende Schritte durch:

- [Scanner-Gruppen definieren](#) – Page 67
- [Virus Scan Provider definieren](#) – Page 70
- [Viren-Scan-Profile definieren](#) – Page 73

8.1.1 Scanner-Gruppen definieren

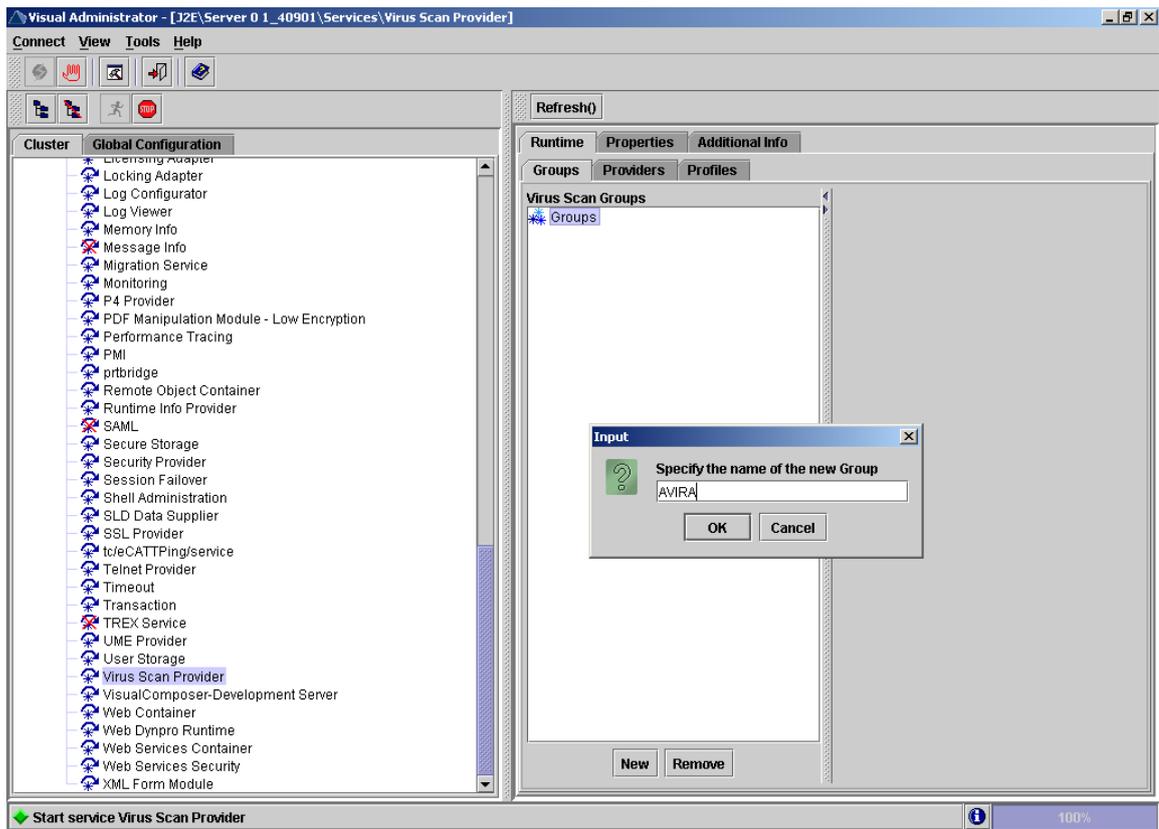
Eine Scanner-Gruppe fasst mehrere gleichartige Viren-Scanner zusammen. Sie benötigen die Gruppen, um später die Viren-Scan-Profile anzugeben. SAP liefert keine Scanner-Gruppen aus.

► Wählen Sie im Visual Administrator den Cluster **Virus Scan Provider**.



Sollte der Service noch nicht gestartet sein, starten Sie ihn bitte durch Anklicken des **Start**-Symbols in der Symbolleiste (oder durch einen rechten Mausklick auf **Virus Scan Providers** und die Auswahl **Start**).

- ▶ Legen Sie auf der Registerkarte **Groups** mit der Taste **New** eine Scanner-Gruppe an.

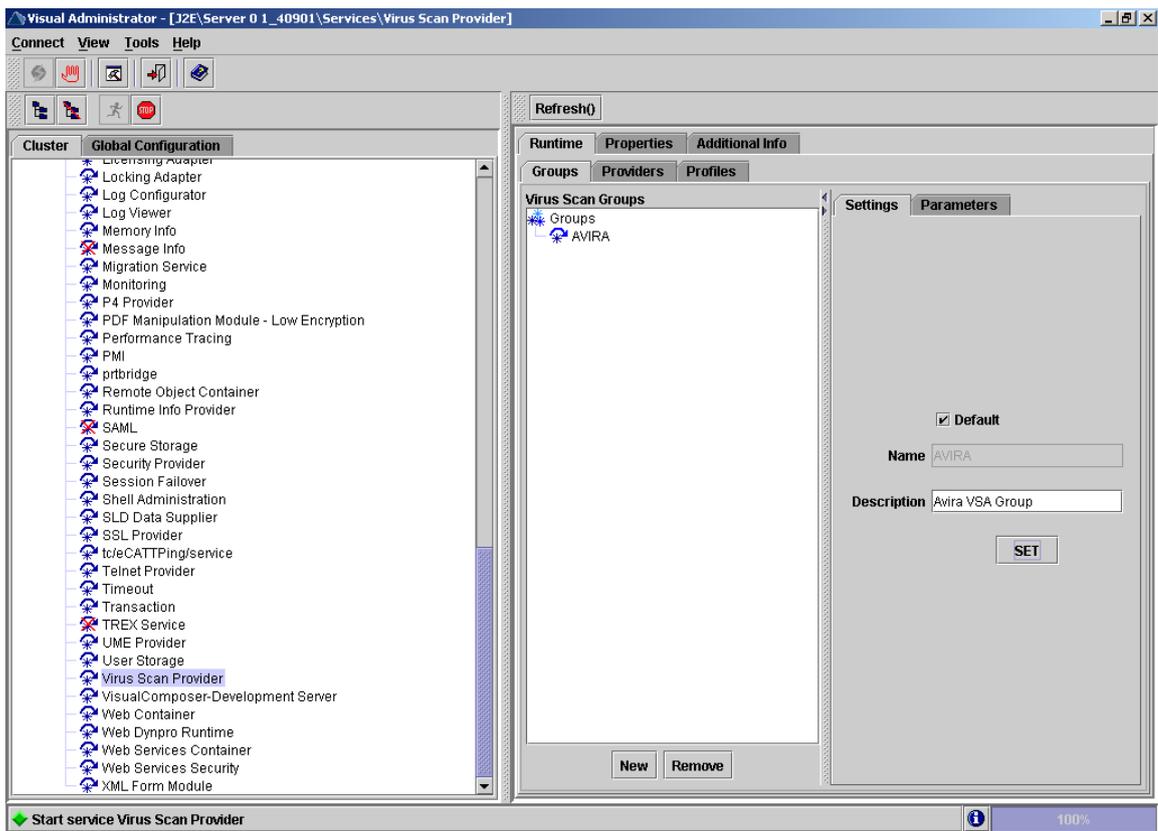


- ▶ Geben Sie im Dialogfenster den Namen der neuen Gruppe an (AVIRA), und bestätigen Sie Ihre Eingabe mit **OK**.



Bitte beachten Sie die Groß/Klein Schreibung der Eingaben. Diese Einstellungen müssen später im KMC benutzt werden.

- ▶ Markieren Sie den Knoten der neu angelegten Gruppe.



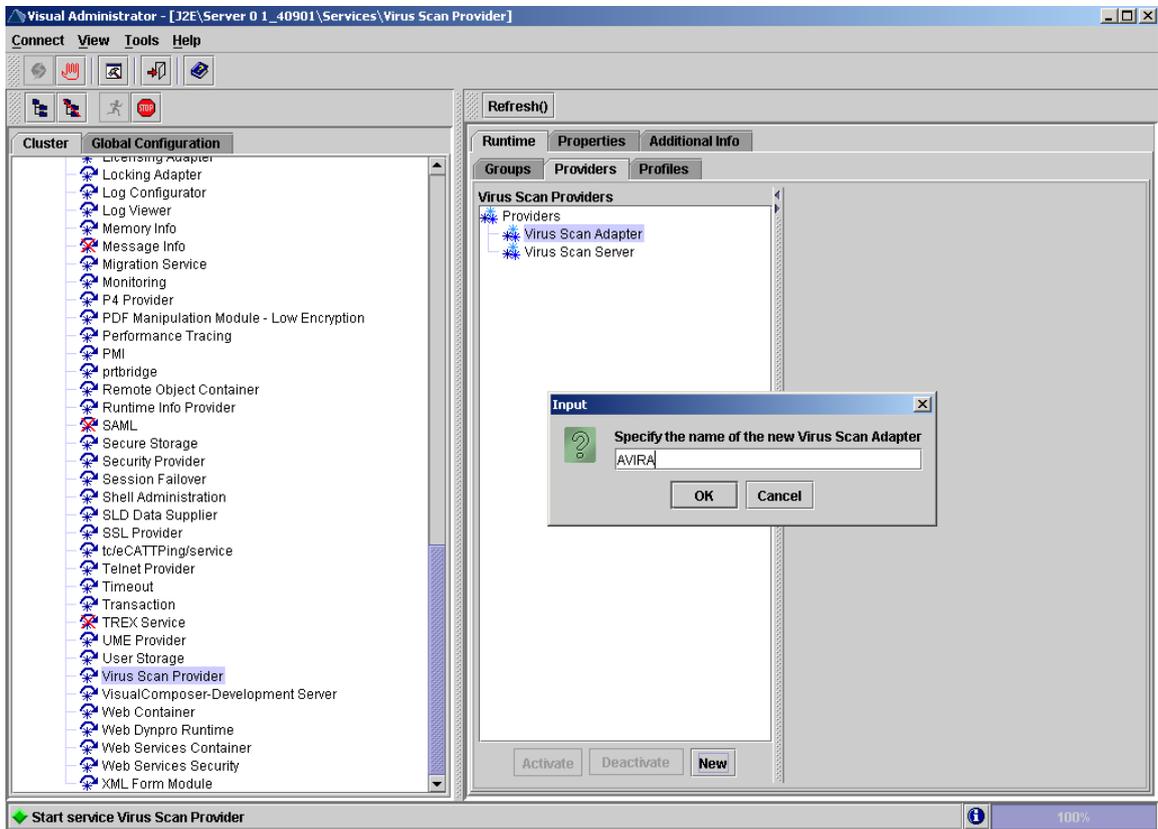
- ▶ Aktivieren Sie die **Default** Option auf der Registerkarte **Settings**, um die Gruppe als Voreinstellung zu benutzen.
- ▶ Geben Sie im Feld **Description** eine beliebige Beschreibung der Gruppe an.
- ▶ Um Ihre Eingabe zu sichern, wählen Sie **Set**.

Machen Sie zur Zeitpunkt keine Einstellungen auf der Registerkarte **Parameters**.

Als nächsten Schritt müssen Sie einen [Virus Scan Provider definieren](#) – Page 70.

8.1.2 Virus Scan Provider definieren

- ▶ Wählen Sie im Visual Administrator den Cluster **Virus Scan Provider**.
- ▶ Legen Sie auf der Registerkarte **Provider** unter dem Knoten **Virus Scan Adapter** mit der Taste **New** einen Virus Scan Adapter an.

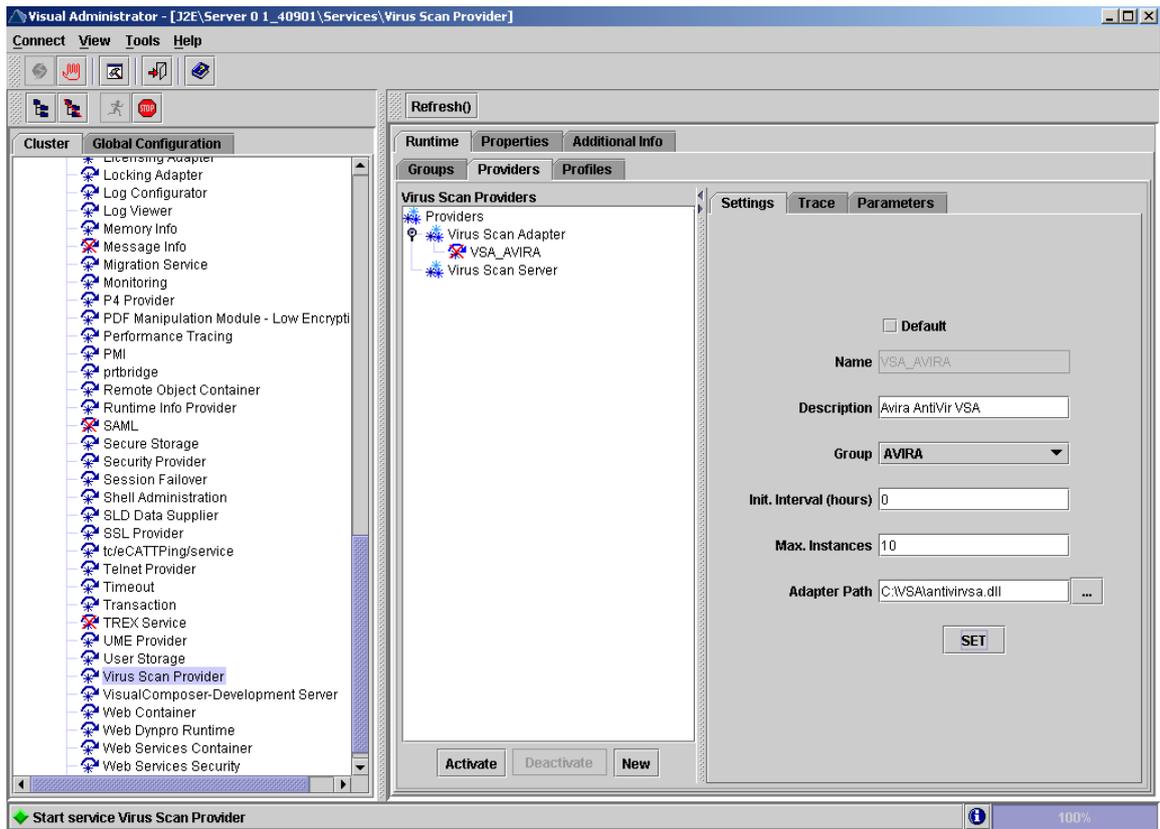


- ▶ Geben Sie im Dialogfenster den Namen des neuen Adapters an (AVIRA), und bestätigen Sie Ihre Eingabe mit **OK**. Der eingegebene Name wird automatisch mit dem Präfix „VSA_“ gesichert.



Bitte beachten Sie die Groß/Klein Schreibung der Eingaben. Diese Einstellungen müssen später im KMC benutzt werden.

- ▶ Markieren Sie den Knoten des neu angelegten Providers.



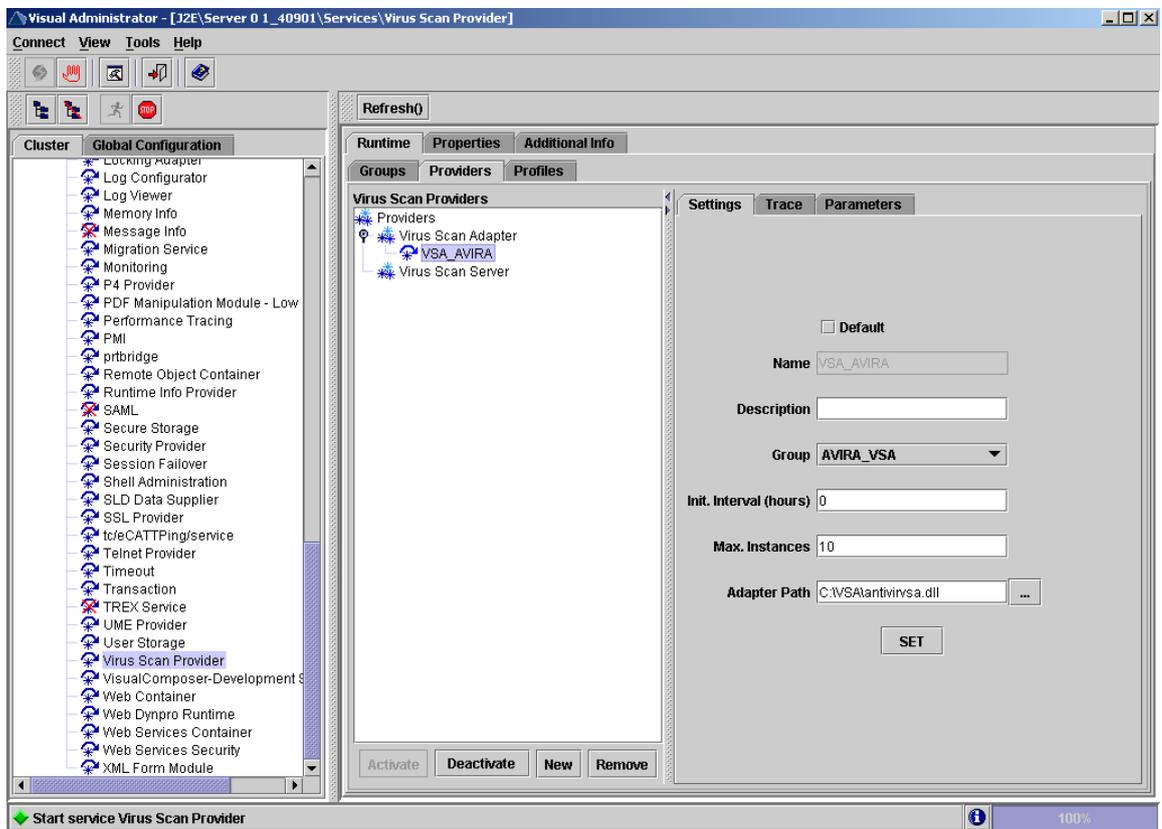
- ▶ Aktivieren Sie die **Default** Option auf der Registerkarte **Settings**, um den Provider als Voreinstellung zu benutzen, und geben Sie, die in der folgenden Tabelle angegebenen Daten an:

Einstellungen für den Virus Scan Adapter

Feld	Eingabe
Default	Dieser Adapter wird gewählt, wenn keine explizite VSA-Anforderung der Applikation vorliegt.
Name	Name des Viren-Scan-Adapters. Der eingegebene Name wird automatisch mit dem Präfix „VSA_“ gesichert.
Description	Beschreibung des aktuellen Adapters.
Group	Die Eingabehilfe bietet eine Liste der verfügbaren Gruppen, denen Sie den aktuellen Adapter zuordnen können.
Init. Interval	Angabe der Zeit (in Stunden), in der NetWeaver den Adapter stoppt und ihn neu startet. Eingaben: 0 neu starten, nur wenn der Virus Scan Service stoppt/ startet, oder wenn der Virus Scan Provider deaktiviert/ aktiviert wird. 1 für Testumgebungen. Vorteil: die Konfiguration wird stündlich neu gelesen, ohne die Servlet-Engine zu stoppen.

Feld	Eingabe
Max Instances	Größe des Vorrats an Instanzen, die an den VSA von NetWeaver ausgeliehen werden. Default: 10.
Adapter Path	Vollständiger Pfad zum Ablageort des Adapters wie im Abschnitt Virus Scan Server als Selbststarter installieren – Page 49 angegeben. Wenn leer, die Environment Variable VSA_LIB wird benutzt.

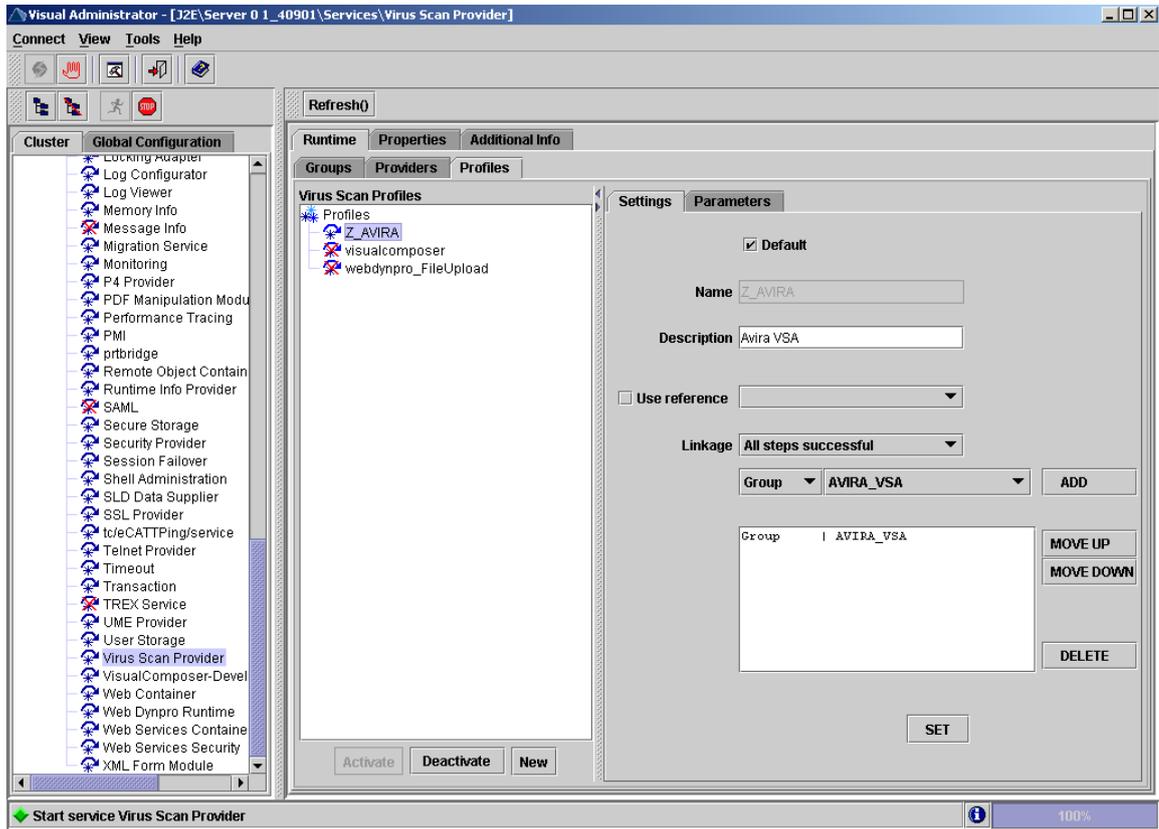
- ▶ Um Ihre Eingaben auf der Registerkarte **Settings** zu sichern, wählen Sie **Set**. Machen Sie zur Zeitpunkt keine Einstellungen auf den Registerkarten **Parameters** und **Trace**.
- ▶ Um den Virus Scan Provider zu aktivieren, markieren Sie ihn und wählen Sie **Activate**. Er wird als **aktiv** markiert.



Sie haben einen Virus Scan Provider definiert. Als nächsten Schritt müssen Sie [Viren-Scan-Profil definieren](#) – Page 73.

8.1.3 Viren-Scan-Profil definieren

- ▶ Wählen Sie im Visual Administrator den Cluster **Virus Scan Provider**.
- ▶ Legen Sie auf der Registerkarte **Profiles** mit der Taste **New** ein Viren-Scan-Profil an.
- ▶ Geben Sie im Dialogfenster den Namen des neuen Profils an (AVIRA), und bestätigen Sie Ihre Eingabe mit **OK**. Der eingegebene Name wird automatisch mit dem Präfix „Z_“ gesichert.
- ▶ Markieren Sie den Knoten des neu angelegten Profils.



- ▶ Aktivieren Sie die **Default** Option auf der Registerkarte **Settings**, um das Profil als Voreinstellung zu benutzen, und geben Sie, die in der folgenden Tabelle angegebenen Daten an.

Daten für ein selbst konfiguriertes Profil

Feld	Kommentar
Default	Dieses Profil wird automatisch gewählt.
Name	Name des neuen Profils
Description	Beschreibung des neuen Profils
Use reference	<p>Dieses Kennzeichen darf nicht gesetzt sein, da sonst die übrigen Eingabefelder ausgeblendet werden.</p> <p>Da ein Viren-Scan-Profil ein anderes Viren-Scan-Profil als Referenzprofil nutzen kann, ist es möglich, mehrere Anwendungen über das gleiche Viren-Scan-Profil zu bedienen. Damit stellen Sie eine Verknüpfung zu einem vorhandenen Referenzprofil her:</p> <ul style="list-style-type: none"> ▶ Setzen Sie das Kennzeichen Use reference. ▶ Wählen Sie mit der Eingabehilfe ein Referenzprofil aus.

Feld	Kommentar
Linkage	Verknüpfung der Schritte dieses Profils: All steps successful: UND-Verknüpfung, bei der jeder Schritt erfolgreich sein muss, damit das Gesamtergebnis erfolgreich ist. At least one Step successful: ODER-Verknüpfung, bei der nur ein Schritt erfolgreich sein muss, damit das Gesamtergebnis erfolgreich ist.
Group	Mit der Eingabehilfe wählen Sie eine Gruppe aus.

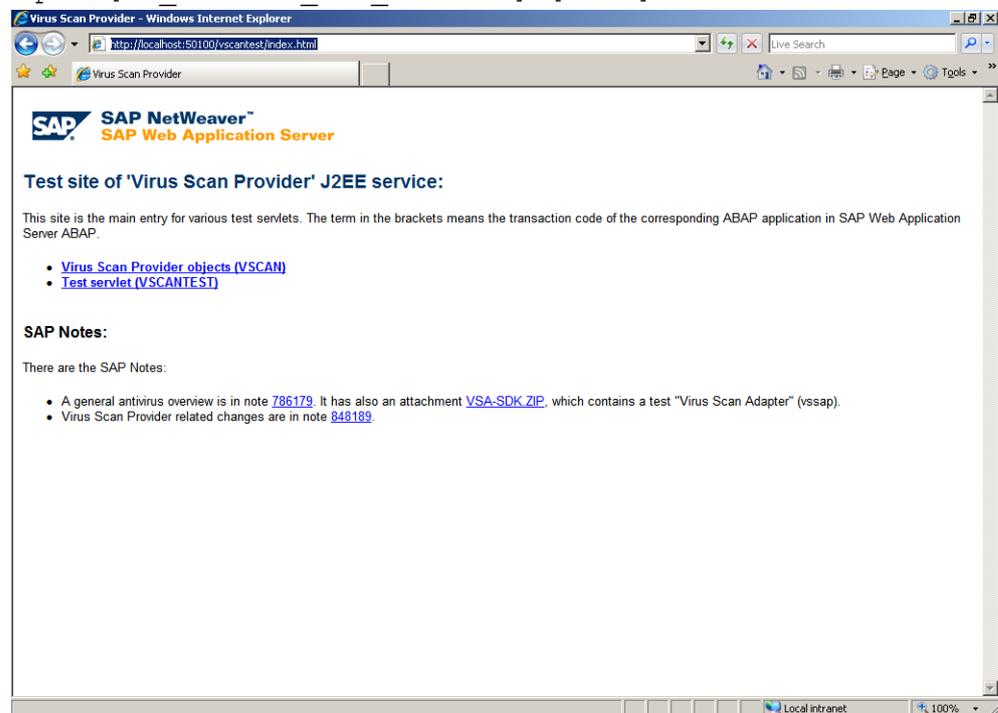
- ▶ Um die Auswahl der Felder **Group** und **Profile** zu übernehmen, wählen Sie **Add**.
- ▶ Konfigurieren Sie die Liste mit den Tasten **MOVE UP** (nach oben setzen), **MOVE DOWN** (nach unten setzen) und **DELETE** (Löschen). Die Liste wird bei der Virenprüfung mit der Verknüpfung des Feldes **Linkage** von oben nach unten abgearbeitet.
- ▶ Um das Profil zu sichern, wählen Sie **Set**.
- ▶ Um das Profil zu aktivieren, markieren Sie es und wählen **Activate**.

Damit haben Sie ein Viren-Scan-Profil definiert und somit den letzten Konfigurationsschritt für den Viren Scan Provider vorgenommen. Abschließend können Sie die Konfiguration überprüfen (see [Konfiguration überprüfen](#) – Page 74).

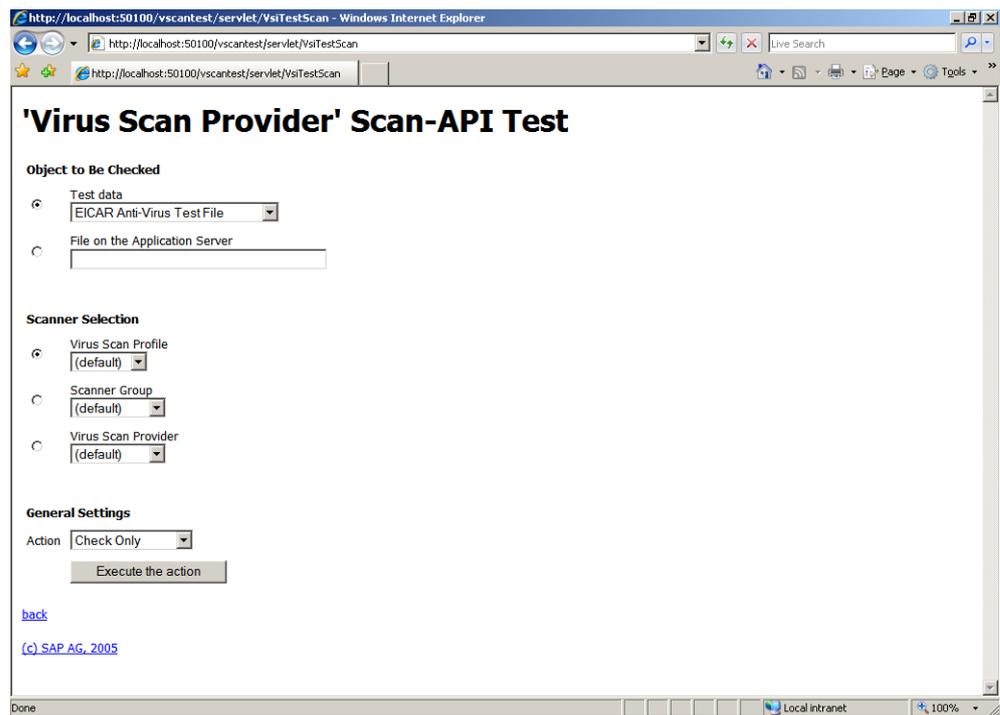
8.1.4 Konfiguration überprüfen

Sie können die Funktionalität von dem Virus Scan Service durch das Test-Applet von NetWeaver Server prüfen.

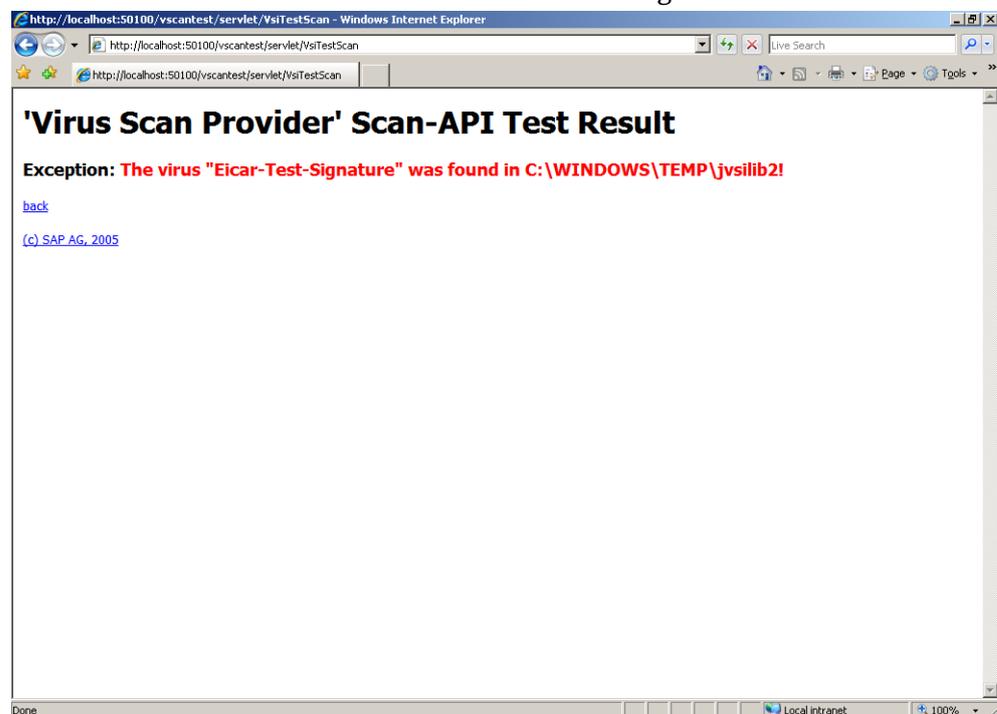
- ▶ Öffnen Sie einen Internet-Browser und geben Sie die folgende Adresse ein:
`http://[IP_Adresse_des_Servers]:[Port]/vscantest`



- ▶ Klicken Sie auf **Test servlet**.

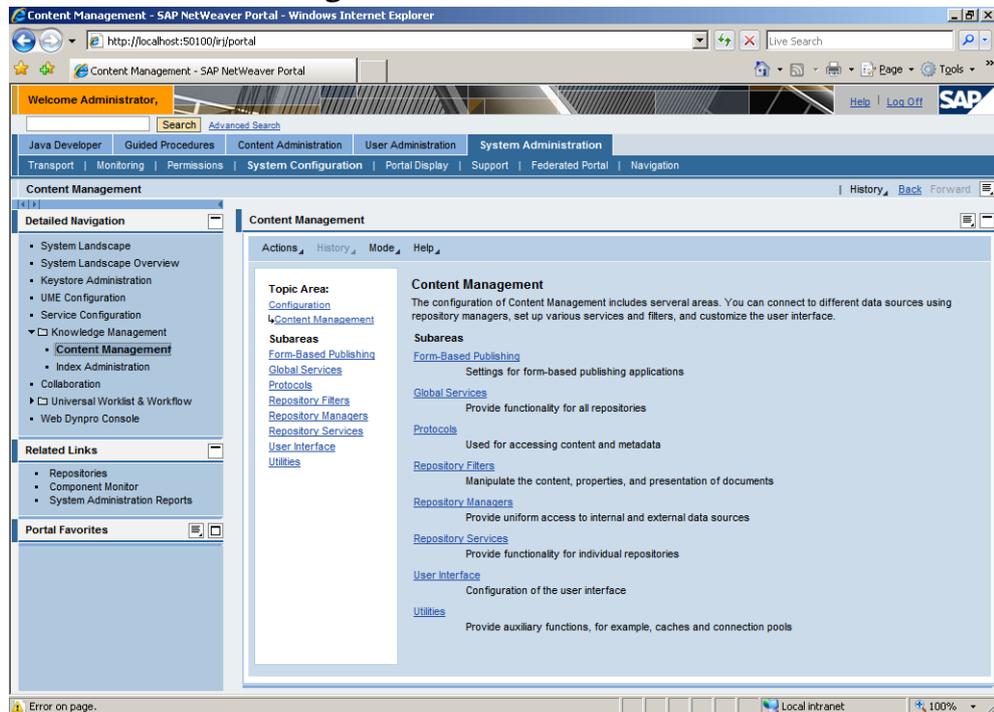


- ▶ Unter **Object to Be Checked**, wählen Sie EICAR Anti-Virus Test File.
- ▶ Unter **Scanner Selection**, wählen Sie (default) als Profil.
- ▶ Unter **General Settings**, behalten Sie die Option Check Only.
- ▶ Klicken Sie auf **Execute the action**.
- ↳ Der Test sollte den Fund der EICAR Test-Datei anzeigen.

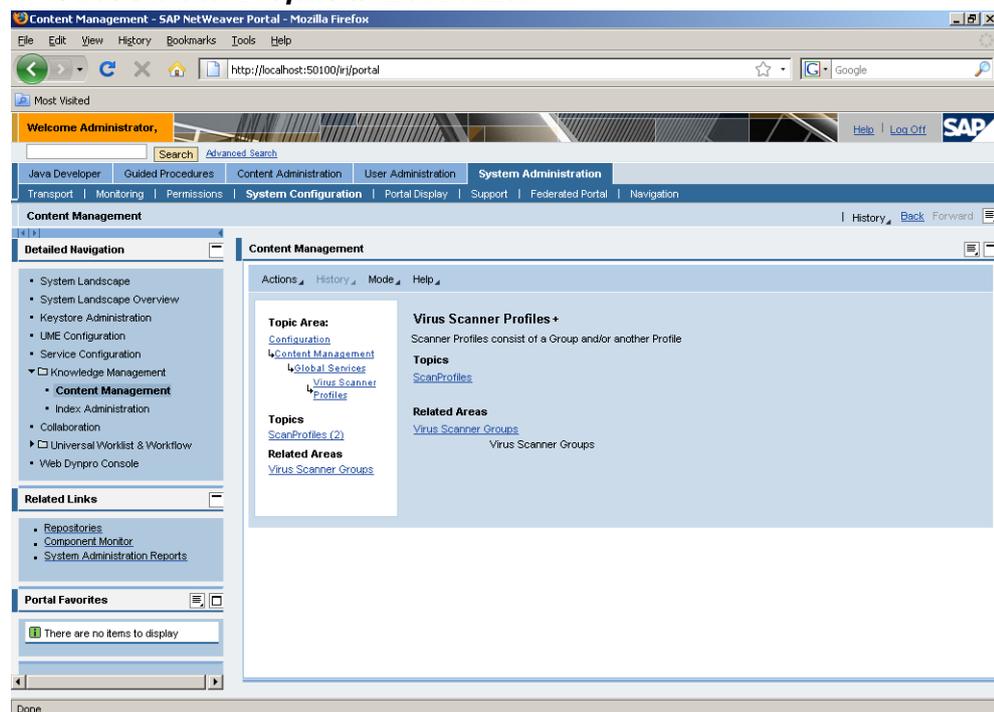


8.2 Einbindung mit Enterprise Portal und Knowledge Management Center

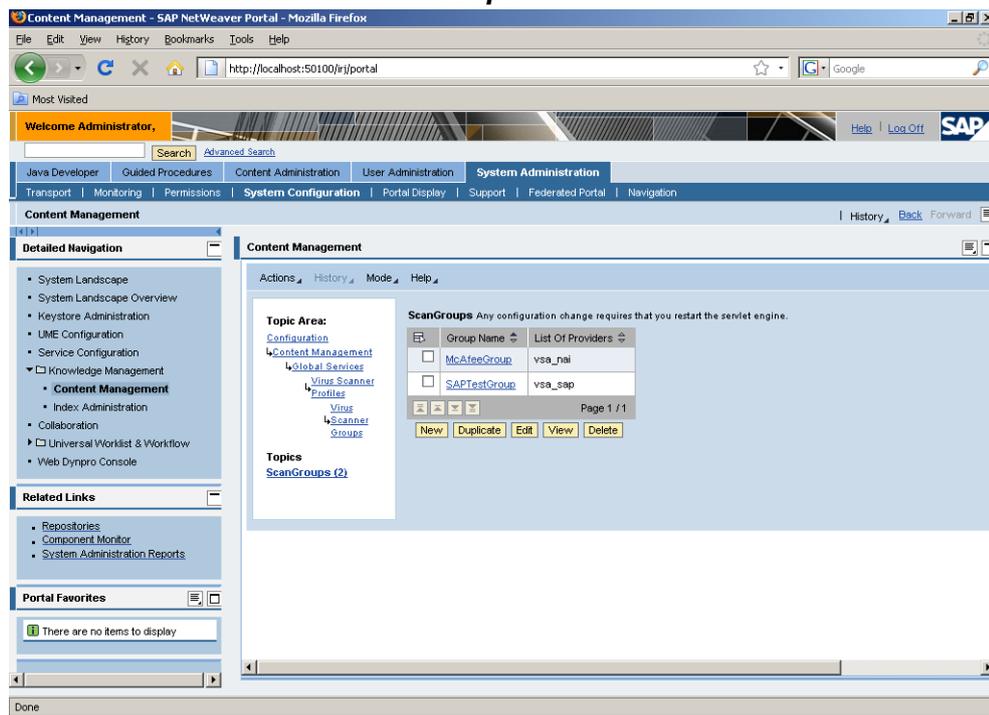
- ▶ Melden Sie sich als Administrator auf SAP NetWeaver Portal an.
- ▶ Wählen Sie das Menü **System Administrator/ System Configuration**.
- ▶ Wählen Sie den Punkt **Knowledge Management/ Content Management** aus dem Bereich **Detailed Navigation**.



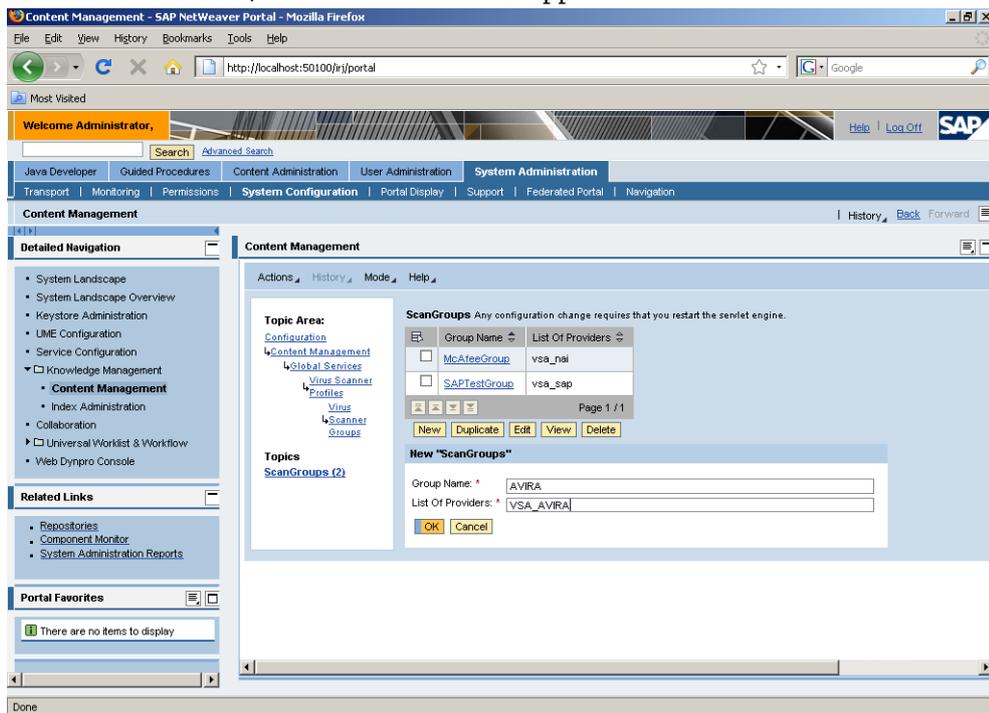
- ▶ Im rechten Bereich klicken Sie auf **Mode** und wählen Sie **Advanced**.
- ▶ Unter **Topic Area**, wählen Sie **Global Services**, dann nach unten scrollen, bis Sie **Virus Scanner Profiles** wählen können.



► Klicken Sie auf **Virus Scanner Groups**.



► Klicken Sie **New**, um eine neue Scan-Gruppe zu erstellen.



► Geben Sie AVIRA als **Group Name** und VSA_AVIRA als **List of Providers** ein.



Bitte beachten Sie die Groß/Klein Schreibung der Eingaben. Diese Einstellungen müssen auch im Visual Administrator benutzt werden.

► Bestätigen Sie mit **OK**.

Content Management - SAP NetWeaver Portal - Mozilla Firefox

http://localhost:50100/nrj/portal

Welcome Administrator, Help Log Off SAP

Search Advanced Search

Java Developer Guided Procedures Content Administration User Administration System Administration

Transport Monitoring Permissions System Configuration Portal Display Support Federated Portal Navigation

Content Management History Back Forward

Detailed Navigation

- System Landscape
- System Landscape Overview
- Keystore Administration
- UME Configuration
- Service Configuration
- Knowledge Management
 - Content Management
 - Index Administration
 - Collaboration
 - Universal Worklist & Workflow
 - Web Dynpro Console

Related Links

- Repositories
- Component Monitor
- System Administration Reports

Portal Favorites

There are no items to display

Content Management

Actions History Mode Help

Topic Area: Configuration Content Management Global Services Virus Scanner Profiles

ScanGroups Any configuration change requires that you restart the servlet engine.

Group Name	List Of Providers
<input type="checkbox"/> AVIRA	VSA_AVIRA
<input type="checkbox"/> McAfeeGroup	vsa_nai

Page 1 / 2

New Duplicate Edit View Delete

Topics ScanGroups (3)

► Unter Topic Area wählen Sie **Virus Scanner Profiles**.

Content Management - SAP NetWeaver Portal - Mozilla Firefox

http://localhost:50100/nrj/portal

Welcome Administrator, Help Log Off SAP

Search Advanced Search

Java Developer Guided Procedures Content Administration User Administration System Administration

Transport Monitoring Permissions System Configuration Portal Display Support Federated Portal Navigation

Content Management History Back Forward

Detailed Navigation

- System Landscape
- System Landscape Overview
- Keystore Administration
- UME Configuration
- Service Configuration
- Knowledge Management
 - Content Management
 - Index Administration
 - Collaboration
 - Universal Worklist & Workflow
 - Web Dynpro Console

Related Links

- Repositories
- Component Monitor
- System Administration Reports

Portal Favorites

There are no items to display

Content Management

Actions History Mode Help

Topic Area: Configuration Content Management Global Services Virus Scanner Profiles

ScanProfiles Any configuration change requires that you restart the servlet engine.

Profile Name	Is Active	Is Default	Is Reference	Logical OR	Reference Profile	Scanner G
<input type="checkbox"/> McAfee	✓			Not set		McAfeeGr
<input type="checkbox"/> SAPTest	✓	✓		Not set		SAPTestG

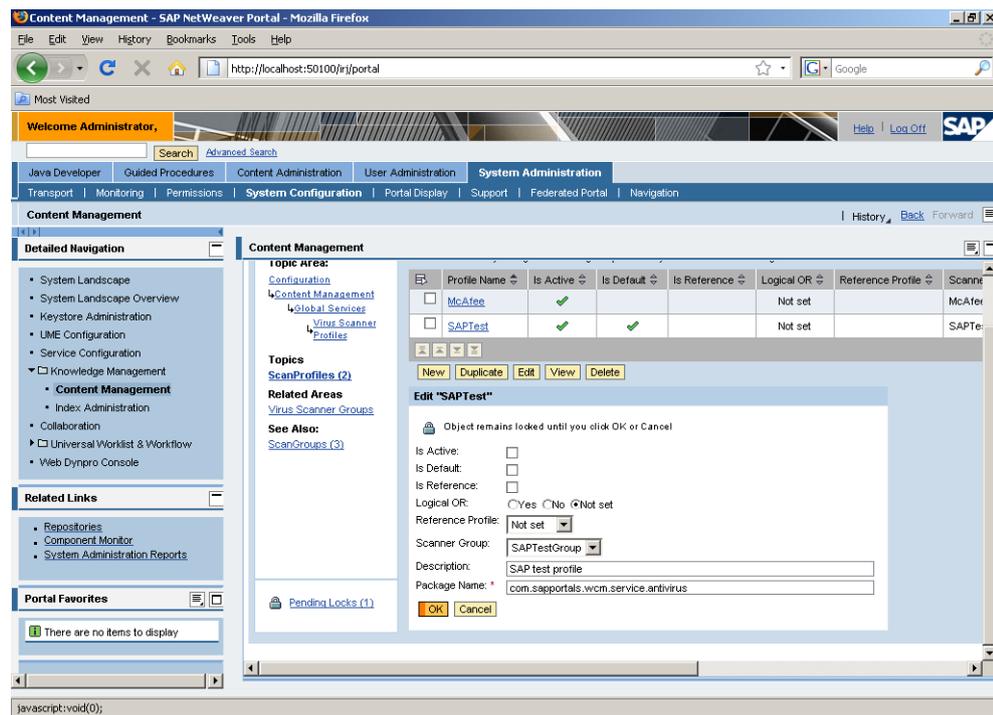
New Duplicate Edit View Delete

Topics ScanProfiles (2)

Related Areas Virus Scanner Groups

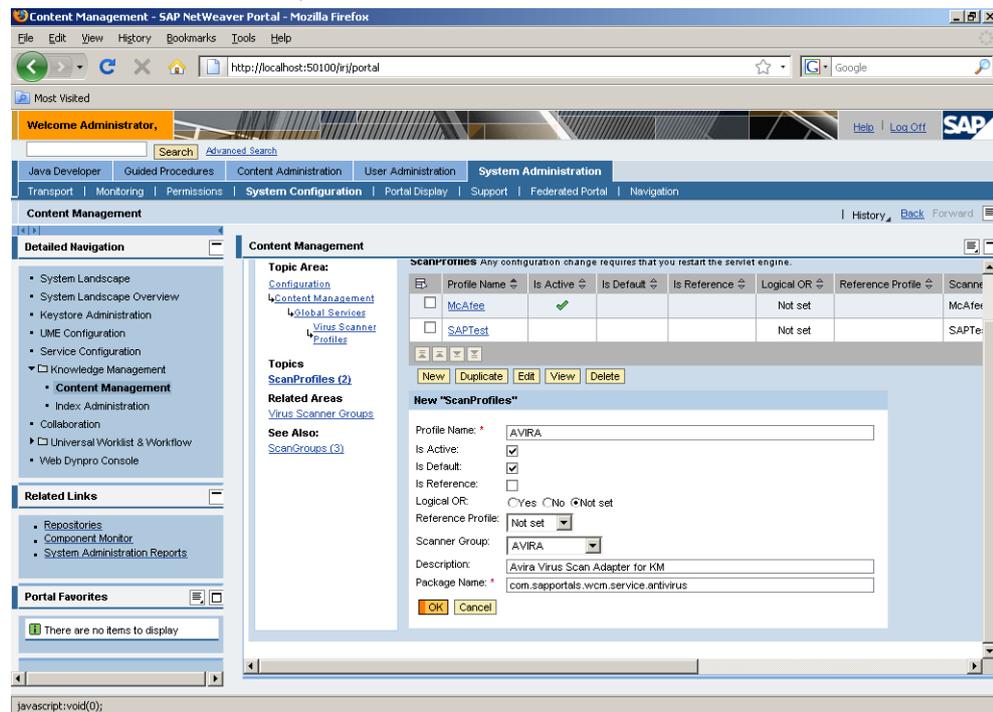
See Also: ScanGroups (3)

- ▶ Aktivieren Sie die Checkbox vor **SAPTest** und klicken Sie auf **Edit**.



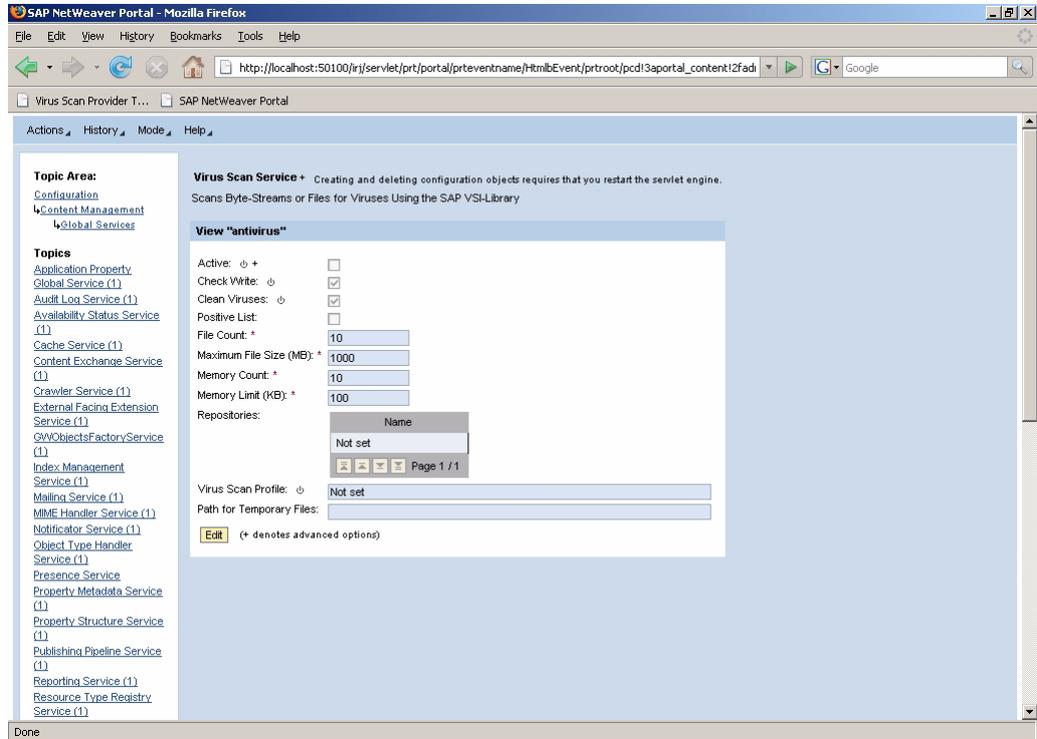
- ▶ Deaktivieren Sie die Checkbox für **Is Default** und klicken Sie auf **OK**.

- ▶ Klicken Sie auf **New**, um ein neues Profil zu erstellen.

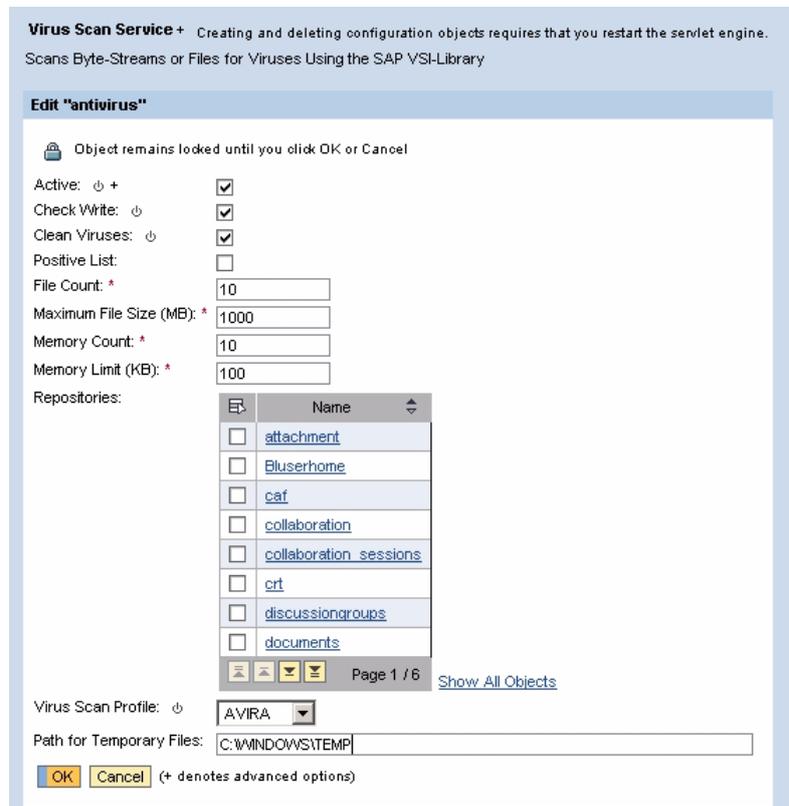


- ▶ Geben Sie als **Profile Name** AVIRA ein.
- ▶ Aktivieren Sie die Optionen **Is Active** und **Is Default**.
- ▶ Die Option **Is Reference** muss inaktiv bleiben.
- ▶ Für die Option **Logical OR** aktivieren Sie den Wert **Not set**.
- ▶ **Reference Profile** muss den Wert **Not set** haben.
- ▶ Wählen Sie AVIRA als **Scanner Group** aus.
- ▶ Das Feld **Description** ist optional.

- ▶ Im Feld **Package Name** geben Sie die folgende Adresse ein:
com.sapportals.wcm.service.antivirus
- ▶ Speichern Sie das Profil mit **OK**.
- ▶ Um den Virus Scan Service zu aktivieren, wählen Sie unter Topic Area **Global Services** und klicken Sie auf **Edit**.



- ▶ Konfigurieren Sie den Service (wie in der Tabelle unten beschrieben), dann klicken Sie auf **OK**.



- Starten Sie die Servlet-Engine neu, um die Konfiguration zu aktivieren.

Option	Beschreibung
Active	Aktivierung des Virus Scan Services im KMC.
Check Write	Viren Scan soll nur beim Download oder auch beim Upload erfolgen.
Clean Viruses	Soll die Antivirus-Softwareversuchen, die infizierte Dateien zu säubern?
Positive List	Positiv: Der Viren-Scanner prüft NUR die ausgewählte Repositories. Ansonsten: Der Scanner prüft alle Repositories, AUSSER den ausgewählten.
File Count	Maximale Anzahl der Dateien, die gleichzeitig gescannt werden können. (Default: 10)
Maximum File Size (MB)	Maximale Größe der Dateien, die gescannt werden können. Aus Sicherheitsgründen dürfen es keine größere Dateien auf Knowledge Management hochgeladen werden. Hängt von File Count und Path for Temporary Files ab. Z.B.: wenn Maximum File Size= 1000 MB und File Count=10, dann muss das temporäre Verzeichnis mindestens 10 GB sein.
Memory Count	Anzahl der Speicherblöcke, die dem Scanner zur Verfügung stehen. Default: 10.
Memory Limit (KB)	Maximale Speicher-Größe, die dem Scanner zur Verfügung steht. Default: 1000.
Repositories	Wenn Positive List aktiv ist, prüft der Scanner NUR die ausgewählten Repositories. Ansonsten prüft er alle Repositories, AUSSER den ausgewählten.
Virus Scan Profile	Das benutzte Profil (AVIRA).
Path for Temporary Files	Das temporäre Verzeichnis, in dem die zu scannenden Dateien abgelegt werden (C:\Windows\Temp). Wenn leer, dann wird den Default-Wert der Java-Engine verwendet (<i>java.io.tmpdir</i>).



9 Bedienung

9.1 Vorgehen bei Fund eines Virus/unerwünschten Programms

AntiVir VSA hat bei richtiger Konfiguration alle wichtigen Aufgaben auf Ihrem Rechner bereits automatisch erledigt.

Wurde ein Virus oder unerwünschtes Programm gefunden, sollten Sie auf jeden Fall folgende Schritte durchführen:

- ▶ Versuchen Sie zu ermitteln, auf welche Weise der Virus oder das unerwünschte Programm "eingeschleppt" wurde.
- ▶ Führen Sie gezielte Prüfungen an möglicherweise betroffenen Datenträgern durch.
- ▶ Informieren Sie Kollegen, Vorgesetzte oder Geschäftspartner.

Verdächtige Dateien an Avira GmbH schicken

- ▶ Senden Sie uns bitte Viren und unerwünschte Programme, die von unseren Produkten noch nicht erkannt oder entfernt werden können, zu. Das Gleiche gilt für sonstige verdächtige Dateien. Senden Sie uns den Virus oder das unerwünschte Programm gepackt und mit Passwortschutz im Anhang einer Email an virus@avira.com.



Verwenden Sie beim Packen das Passwort **virus**. Die Datei kann dann nicht von eventuellen Virensclannern in den Email-Gateways gelöscht werden.



10 Service

10.1 Support

Support-Service Auf unserer Webseite <http://www.avira.com> erhalten Sie alle Informationen zu unserem umfangreichen Support-Service.

Die Kompetenz und Erfahrung unserer Entwickler stehen Ihnen hier zur Verfügung. Die Experten der Avira GmbH beantworten Ihre Fragen und helfen bei kniffligen technischen Problemen weiter.

Während der ersten 30 Tage nach Erwerb einer Lizenz haben Sie die Möglichkeit, den AntiVir Installationssupport in Anspruch zu nehmen, telefonisch, per Email oder per Online-Formular.

Darüber hinaus empfehlen wir Ihnen optional den Erwerb unseres AntiVir Classic Supports, mit dem Sie bei auftretenden technischen Problemen unsere Fachleute während der Geschäftszeiten kontaktieren und zu Rate ziehen können.

Der ebenfalls optional verfügbare AntiVir Premium Support bietet Ihnen über den Leistungsumfang des AntiVir Classic Supports hinaus genügend Spielraum, auch bei Notfällen außerhalb der Geschäftszeiten jederzeit einen kompetenten Ansprechpartner zu erreichen. Bei Virenalarm wird auf Wunsch eine SMS-Benachrichtigung auf Ihr Mobiltelefon gesendet.

Email-Support Nähere Informationen zum Support per Email erhalten Sie unter <http://www.avira.com>.



Für Probleme mit der Konfiguration, die nicht direkt AntiVir VSA betreffen, können wir keinen Support übernehmen.

Bei Fragen und Problemen vermitteln wir Ihnen gern einen SAP-Consultant mit sicherheitstechnischem Know-how.

10.2 Kontakt

Postadresse Avira GmbH
Lindauer Strasse 21
D-88069 Tettngang
Deutschland

Internet Allgemeine Informationen zu uns und unseren Produkten erhalten Sie auf unserer Homepage <http://www.avira.com>.



11 Anhang

11.1 Glossar

Begriff	Erklärung
ABAP	Advanced Business Application Language: Die Programmiersprache der SAP zum Programmieren von Anwendungslogik.
Backdoor- Steuerprogramme (BDC)	Um Daten zu stehlen oder Rechner zu manipulieren, wird ein Backdoor-Steuerprogramm eingeschleust, ohne dass der Anwender es merkt. Über Internet oder Netzwerk kann dieses Programm über eine Backdoor-Steuersoftware (Client) von Dritten gesteuert werden.
CCMS	Computing Center Management System.
Cron-Dämon	Dämon, der andere Programme zu vorgegebenen Zeiten startet.
Dämon	Im Hintergrund laufender Prozess zur Systemverwaltung unter Linux. Im Schnitt laufen einige Dutzend Dämonen auf dem Rechner. Diese Prozesse werden beim Hochfahren des Rechners gestartet.
Dialer	Kostenverursachende Einwahlprogramme. Auf dem Rechner installiert, bauen diese Programme eine Internetverbindung über eine Premium-Rate-Nummer auf, deren Tarifgestaltung ein breites Spektrum umfassen kann (Vorwahl 0900 in Deutschland, 09x0 in Österreich und in der Schweiz). Manchmal werden Dialer bewusst unauffällig eingesetzt, bisweilen in betrügerischer Absicht. Dies kann zu horrenden Telefonrechnungen führen. AntiVir VSA erkennt Dialer.
Engine	Modul der AntiVir-Software, das die Virensuche steuert.
Heuristik	Systematisches Verfahren, das mit generellen und speziellen Regeln bestimmte Probleme zu lösen versucht. Das Auffinden einer Lösung kann damit allerdings nicht garantiert werden. AntiVir VSA verwendet ein heuristisches Verfahren zum Auffinden von noch unbekanntem Makroviren. Hierbei wird das Makro beim Auffinden von virustypischen Funktionen als "verdächtig" gemeldet.
Kernel	Innerster Teil des Betriebssystems mit elementaren Systemfunktionen (Speicherverwaltung, Prozessverwaltung).
Logdatei	Auch: Reportdatei, Protokolldatei. Datei, in die Meldungen von Programmen geschrieben werden.
Malware	Oberbegriff für Software-"Fremdkörper" jeglicher Art. Dies können Störungen wie Computerviren sein, aber auch andere Software, die vom Nutzer generell als unerwünscht betrachtet wird (siehe auch Unerwünschte Programme).

Begriff	Erklärung
PMS (Possibly Malicious Software)	"Möglicherweise schädliche Software": PMS richtet normalerweise keinen Schaden auf dem eigenen Rechner an. Sie wurde programmiert, um anderen Anwendern Schaden zuzufügen. Beispiel Mailbomber: Mit einem solchen Programm kann ein Opfer mit Tausenden von Emails attackiert werden. AntiVir VSA erkennt PMS.
root	Benutzer mit uneingeschränkten Rechten für die Systemverwaltung (entsprechend dem Administrator bei Windows).
SAVAPI	Secure AntiVirus Application Programming Interface Die AntiVir SAVAPI ermöglicht die schnelle und einfache Integration modernster Avira-Technologie zur Malware-Erkennung und -abwehr in Programme und Applikationen von Drittherstellern.
Signatur	Kombinationen von Bytefolgen, an denen ein Virus oder ein unerwünschtes Programm erkannt werden kann.
Skript	Textdatei mit Befehlen, ein unter UNIX sehr verbreiteter Mechanismus (entspricht etwa einer Batchdatei bei DOS).
SMP (Symmetric Multi Processing)	Rechnerarchitektur mit mehreren parallel arbeitenden gleichartigen CPUs.
SMTP	Simple Mail Transfer Protocol: Verfahren, auf dessen Basis Emails im Internet transportiert werden.
syslog-Dämon	Dämon, der die Meldungen diverser Programme protokolliert. Die Meldungen werden in unterschiedliche Logdateien geschrieben. Die Konfiguration des syslog-Dämons wird in <i>/etc/syslog.conf</i> festgelegt.
Unerwünschte Programme	Oberbegriff für Programme, die keinen direkten Schaden auf dem Rechner verursachen oder ohne Absicht des Anwenders oder Administrators installiert wurden. Hierzu zählen Backdoor-Steuerprogramme, Dialer, Witzprogramme und auch Spiele. AntiVir VSA erkennt verschiedene Arten unerwünschter Programme.
VDF (Virus Definition File)	Virendefinitionsdatei: Datei mit den Signaturen der bekannten Viren. In vielen Fällen ist es für ein Update ausreichend, diese Datei zu aktualisieren.
VFS	Virtual File System
Virendefinitionsdatei	siehe VDF

11.2 Weitere Infoquellen

Weitere Informationen zu verschiedenen Viren, Würmern, Makroviren und weiteren unerwünschten Programmen sind erhältlich unter <http://www.avira.de/de/threats/index.html>

11.3 Goldene Regeln zur Virenvorsorge

- ▶ Erstellen Sie Notfalldisketten/Startdisketten für Ihre Windows-Version sowie Ihren Netzwerkservers und die einzelnen Workstations. Notfalldisketten sind auch bei anderen Betriebssystemen hilfreich.
- ▶ Nehmen Sie Disketten nach Beenden Ihrer Arbeit immer aus dem Laufwerk heraus. Auch Disketten ohne ausführbare Programme enthalten Programmcode im Bootsektor und können Träger eines Bootsektorvirus sein.
- ▶ Fertigen Sie regelmäßig vollständige Backups Ihrer Daten an.
- ▶ Begrenzen Sie den Programmaustausch: Das gilt besonders für Netzwerk, Mailboxen, Internet und gute Bekannte.
- ▶ Prüfen Sie neue Programme vor und nach einer Installation. Liegt das Programm auf einem Datenträger komprimiert vor, lässt sich ein Virus in der Regel erst nach dem Auspacken bei der Installation finden.

Haben andere Personen einen Zugang zu Ihrem Rechner, sollten Sie folgende Spielregeln zum Schutz vor Viren beachten:

- ▶ Stellen Sie einen Computer als Testrechner zur Eingangskontrolle neuer Software, Demoversionen oder evtl. virenverdächtiger Datenträger (Disketten, CD-R, CD-RW, Wechsellaufwerk-Medien) und von Downloads bereit. Trennen Sie diesen Rechner aber vom Netzwerk!
- ▶ Benennen Sie einen Datenschutzbeauftragten, der bei einer Virusinfektion für die Behandlung verantwortlich ist, und bestimmen Sie im Voraus alle zu einer Beseitigung eines Virus notwendigen Schritte.
- ▶ Organisieren Sie vorsorglich einen durchführbaren Notfallplan: Dieser kann die Schäden durch mutwillige Zerstörung, Raub, Ausfall oder Zerstörungen/Veränderungen aufgrund von Inkompatibilitäten vermindern helfen. Programme und Massenspeicher lassen sich ersetzen; Daten, die für ein wirtschaftliches Überleben notwendig sind, nicht.
- ▶ Stellen Sie vorsorglich einen durchführbaren Schutz- und Wiederaufbauplan für Ihre Daten auf.
- ▶ Sorgen Sie für ein ordentlich installiertes Netzwerk, bei dem die Rechtevergabe vorbeugend eingesetzt wird. Es ist ein guter Schutz gegen Viren.



Avira GmbH

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

© Avira GmbH. Alle Rechte vorbehalten.

Dieses Handbuch wurde mit äußerster Sorgfalt erstellt. Dennoch sind Fehler in Form und Inhalt nicht ausgeschlossen. Die Vervielfältigung dieser Publikation oder von Teilen dieser Publikation in jeglicher Form ist ohne vorherige schriftliche Genehmigung durch die Avira GmbH nicht gestattet.

Irrtümer und technische Änderungen vorbehalten.

Ausgabe Q4-2008

AntiVir[®] ist ein registriertes Warenzeichen der Avira GmbH. Alle anderen Marken- und Produkt-namen sind Warenzeichen oder eingetragene Warenzeichen ihrer entsprechenden Besitzer. Geschützte Warenzeichen sind in diesem Handbuch nicht als solche gekennzeichnet. Dies bedeutet jedoch nicht, dass sie frei verwendet werden dürfen.