

AVG 8.5 Email Server Edition

Benutzerhandbuch

Dokumentversion 85.4 (30.4.2009)

Copyright AVG Technologies CZ, s.r.o. Alle Rechte vorbehalten.
Alle anderen Markenzeichen sind das Eigentum der jeweiligen Inhaber.

Dieses Produkt verwendet RSA Data Security, Inc. MD5 Message-Digest Algorithm, Copyright (C) 1991-2, RSA Data Security, Inc. Erstellt 1991.

Dieses Produkt verwendet Code aus der Bibliothek C-SaCzech, Copyright © 1996–2001 Jaromir Dolecek
<dolecek@ics.muni.cz>

Dieses Produkt verwendet die Kompressionsbibliothek zlib, Copyright © 1995-2002 Jean-Loup Gailly und Mark Adler.

Inhalt

1. Einleitung	4
2. Installationsvoraussetzungen für AVG	5
2.1 Unterstützte Betriebssysteme	5
2.2 Unterstützte eMail-Server	5
2.3 Minimale Hardware-Anforderungen	5
2.4 Deinstallieren vorheriger Versionen	6
2.5 Service Packs für MS Exchange	6
3. Installationsvorgang bei AVG	8
3.1 Beginn der Installation	8
3.2 Lizenzvereinbarung	9
3.3 Systemstatus wird geprüft	9
3.4 Bitte wählen Sie den Installationstyp	9
3.5 AVG aktivieren	10
3.6 Benutzerdefinierte Installation – Zielverzeichnis	11
3.7 Benutzerdefinierte Installation – Komponentenauswahl	12
3.8 Benutzerdefinierte Installation – DataCenter	13
3.9 Setup – Zusammenfassung	14
3.10 Installieren	14
3.11 Installation beendet	14
4. Optionen für die Installation von AVG eMail-Server	15
4.1 Beginn der Installation	15
4.2 Lizenzvereinbarung	15
4.3 Speicherort	15
4.4 Dateien Kopieren	16
4.5 Neustart des Speicherdienstes	16
4.6 Installation beendet	17
5. AVG für MS Exchange Server 2007	18
5.1 Konfiguration	18
5.1.1 Status	18
5.1.2 VSAPI 2.0	18
5.1.3 Allgemeine Eigenschaften	18
5.1.4 Diagnoseprotokolle	18

5.2 Server-Überwachung	22
5.2.1 Online-Überwachung	22
6. AVG für MS Exchange Server 2000/2003	24
6.1 Konfiguration	24
6.1.1 Status	24
6.1.2 VSAPI 2.0	24
6.1.3 Allgemeine Eigenschaften	24
6.1.4 Diagnoseprotokolle	24
6.2 Server-Überwachung	28
6.2.1 Online-Überwachung	28
6.2.2 Ereignisprotokoll	28
7. AVG for Kerio MailServer	33
7.1 Konfiguration	33
7.1.1 Anti-Virus	33
7.1.2 Filter für Anhänge	33
8. Anti-Spam-Konfiguration	39
8.1 Benutzeroberfläche des Anti-Spam	39
8.2 Grundlagen zu Anti-Spam	40
8.3 Anti-Spam-Einstellungen	40
8.3.1 Anti-Spam-Trainingsassistent	40
8.3.2 Ordner mit Nachrichten auswählen	40
8.3.3 Optionen für Nachrichtenfilterung	40
8.4 Leistung	46
8.5 RBL	47
8.6 Whitelist	48
8.7 Blacklist	49
8.8 Erweiterte Einstellungen	51
9. eMail-Scanner	52
9.1 Zertifizierung	53
9.2 eMail-Filterung	54
10. FAQ und technischer Support	55

1. Einleitung

Dieses Benutzerhandbuch bietet eine umfassende Dokumentation zu **AVG 8.5 Email Server Edition**.

Herzlichen Glückwunsch zum Kauf von AVG 8.5 Email Server Edition!

AVG 8.5 Email Server Edition zählt zu einer Reihe von preisgekrönten AVG-Produkten, die vollständige Sicherheit für Ihren PC bieten, damit Sie in Ruhe arbeiten können. Wie alle AVG-Produkte wurde **AVG 8.5 Email Server Edition** von Grund auf vollkommen neu gestaltet, um den anerkannten Schutz von AVG noch benutzerfreundlicher und effizienter bereitzustellen.

AVG wurde entwickelt, um Ihre Computer- und Netzwerkaktivitäten zu schützen. Genießen Sie den vollständigen Rundumschutz von AVG.

2. Installationsvoraussetzungen für AVG

2.1. Unterstützte Betriebssysteme

AVG 8.5 Email Server Edition wurde zum Schutz von eMail-Servern konzipiert, die unter folgenden Betriebssystemen ausgeführt werden:

- Windows 2008 Server Edition (x86 und x64)
- Windows Server 2003 (x86, x64 und Itanium) SP1
- Windows 2000 Server SP4 + Updaterollup 1

(sowie ggf. höhere Service Packs für bestimmte eMail-Server)

2.2. Unterstützte eMail-Server

Folgende eMail-Server werden unterstützt:

- **MS Exchange 2000 Server (mit Service Pack 1 oder höher)**

Hinweis: Für Exchange 2000 Server muss zuerst das Service Pack 1 (oder höher) installiert werden, bevor die AVG-Engine verwendet werden kann; **AVG for MS Exchange 2000/2003 Server** verwendet die Oberfläche von VSAPI 2.0 (oder 2.5 mit Exchange 2003 Server), die in diesem Service Pack enthalten ist.

- **MS Exchange 2003 Server-Version**
- **MS Exchange 2007 Server-Version**
- **AVG for Kerio MailServer** – Version 5.x/6.x und höher

2.3. Minimale Hardware-Anforderungen

Hardware-Mindestanforderungen für **AVG 8.5 Email Server Edition**:

- Intel Pentium CPU 1,2 GHz
- 250 MB freier Festplattenspeicher (für die Installation)

- 256 MB RAM-Speicher

2.4. Deinstallieren vorheriger Versionen

Wenn Sie eine ältere AVG eMail Server Version installiert haben, müssen Sie diese vor der Installation von **AVG 8.5 Email Server Edition** zunächst manuell deinstallieren. Sie müssen die frühere Version mit Hilfe der Windows-Standardfunktion manuell deinstallieren.

- Wählen Sie im Startmenü **Start/Einstellungen/Systemsteuerung/Software** aus der Liste der installierten Software das entsprechende Programm aus. Achten Sie darauf, das richtige AVG-Programm zur Deinstallation auszuwählen. Sie müssen die eMail Server Edition vor der AVG File Server Edition deinstallieren.
- Sobald Sie die eMail Server Edition deinstalliert haben, können Sie die ältere Version einer AVG File Server Edition deinstallieren. Dies können Sie einfach über das Startmenü über **„Start/Programme/AVG/Deinstallation von AVG“ vornehmen.**

2.5. Service Packs für MS Exchange

Da **AVG for MS Exchange 2000/2003 Server** die Virus Scanning Application Programming Interface VSAPI 2.0/2.5 verwendet, muss das Service Pack 1 (oder höher) für MS Exchange 2000 Server in Ihrem System installiert sein. Unter nachfolgendem Link finden Sie das neueste Service Pack für MS Exchange 2000 Server:

Service Pack für MS Exchange 2000 Server:

<http://www.microsoft.com/technet/prodtechnol/exchange/downloads/2000/sp3/default.aspx>

Für MS Exchange 2003 Server ist kein zusätzliches Service Pack erforderlich. Es wird dennoch empfohlen, das System über die neuesten Service Packs und Hotfixes auf dem aktuellen Stand zu halten, damit die maximale Sicherheit gewährleistet ist.

Service Pack für MS Exchange 2003 Server (optional):

<http://www.microsoft.com/exchange/evaluation/sp2/overview.aspx>

Zu Beginn des Setups werden alle Versionen der Systembibliotheken geprüft. Wenn die Installation neuer Bibliotheken erforderlich ist, fügt das Installationsprogramm den alten Bibliotheken die Erweiterung .delete hinzu. Diese werden bei einem

Neustart des Systems gelöscht.

3. Installationsvorgang bei AVG

Für die Installation von AVG auf Ihrem Computer benötigen Sie die aktuellste Installationsdatei. Sie können die Installationsdatei auf der CD verwenden, die Bestandteil Ihrer Edition ist. Diese Datei ist jedoch möglicherweise nicht mehr aktuell. Es wird daher empfohlen, die aktuellste Installationsdatei online herunterzuladen. Sie können die Datei von der [AVG-Website](http://www.avg.com/download?prd=msw) (unter <http://www.avg.com/download?prd=msw>) herunterladen.

Während des Installationsvorgangs werden Sie nach Ihrer Lizenz-/Vertriebsnummer gefragt. Halten Sie diese bereit, bevor Sie mit der Installation beginnen. Die Vertriebsnummer befindet sich auf der Verpackung der CD. Wenn Sie AVG online erworben haben, wurde Ihnen die Lizenznummer per eMail zugeschickt.

Nachdem Sie die Installationsdatei heruntergeladen und auf Ihrer Festplatte gespeichert haben, können Sie den Installationsvorgang starten. Der Installationsvorgang besteht aus einer Abfolge von Dialogen, die jeweils eine kurze Beschreibung der erforderlichen Schritte enthalten. Im Folgenden werden die einzelnen Dialoge erläutert:

3.1. Beginn der Installation



Der Installationsvorgang beginnt mit dem Fenster **Willkommen**. Hier können Sie die Sprache für den Installationsvorgang auswählen. Im unteren Teil des Dialogs befindet sich die Option **Sprache für die Installation auswählen**, wo Sie die gewünschte Sprache im Dropdown-Menü auswählen können. Klicken Sie anschließend auf **Weiter**,

um mit dem nächsten Dialog fortzufahren.

Achtung: Hier wählen Sie nur die Sprache für den Installationsvorgang aus. Sie wählen nicht die Sprache für die AVG-Anwendung aus – diese können Sie später während des Installationsvorgangs festlegen!

3.2. Lizenzvereinbarung

Der Dialog **Lizenzvereinbarung** enthält den vollständigen Text der Lizenzvereinbarung mit AVG. Bitte lesen Sie die Vereinbarung sorgfältig durch, und bestätigen Sie mit der Schaltfläche **Akzeptieren**, dass Sie die Vereinbarung gelesen, verstanden und akzeptiert haben. Falls Sie der Lizenzvereinbarung nicht zustimmen, klicken Sie auf **Nicht akzeptieren**, um den Installationsvorgang abzubrechen.

3.3. Systemstatus wird geprüft

Nachdem Sie die Lizenzvereinbarung akzeptiert haben, wird erneut der Dialog **Systemstatus wird geprüft...** angezeigt. In diesem Dialog ist keine Aktion erforderlich. Das System wird geprüft, bevor die Installation von AVG gestartet werden kann. Bitte warten Sie, bis der Prozess abgeschlossen ist und der folgende Dialog angezeigt wird.

3.4. Bitte wählen Sie den Installationstyp



Im Dialog **Installationstyp wählen** können Sie zwischen zwei Installationsoptionen

wählen: **Standardinstallation** und **benutzerdefinierte Installation**.

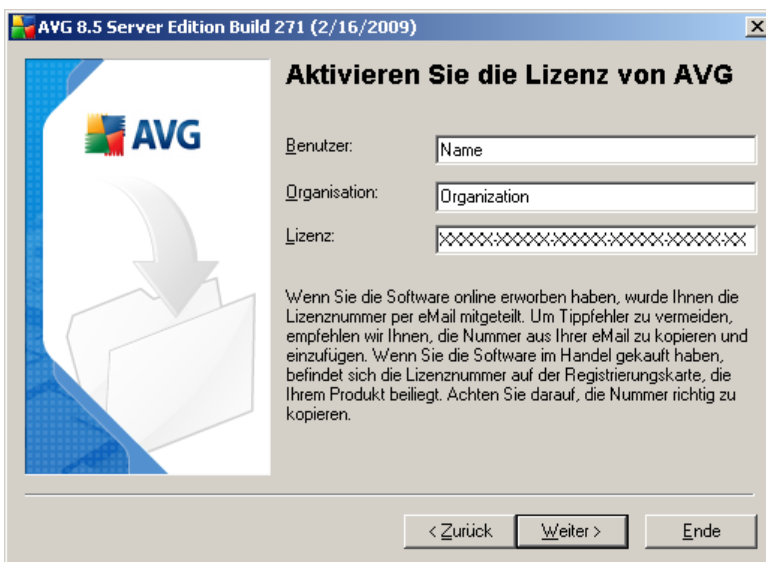
Den meisten Benutzern wird empfohlen, die **Standardinstallation** beizubehalten, mit der AVG vollständig automatisch mit den vom Programmhersteller vordefinierten Einstellungen installiert wird. Diese Konfiguration bietet die höchste Sicherheit, verbunden mit einer optimalen Ressourcennutzung. Wenn die Konfiguration zukünftig geändert werden muss, können Sie diese Änderungen immer direkt in der Anwendung AVG vornehmen.

Die benutzerdefinierte Installation sollte nur von erfahrenen Benutzern verwendet werden, die einen wichtigen Grund haben, AVG nicht mit den Standardeinstellungen zu installieren. Dies könnte beispielsweise der Fall sein, wenn bestimmte Systemanforderungen eingehalten werden müssen.

3.5. AVG aktivieren

Im Dialog **AVG-Lizenz aktivieren** müssen Sie Ihre Registrierungsdaten eingeben. Geben Sie Ihren Namen (Feld **Benutzer**) und den Namen Ihrer Organisation (Feld **Organisation**) ein.

Geben Sie anschließend Ihre Lizenz-/Vertriebsnummer in das Textfeld **Lizenznummer** ein. Die Lizenznummer ist in der Bestätigungs-eMail enthalten, die Sie nach dem Online-Kauf von AVG erhalten haben. Sie müssen die Nummer exakt wie dargestellt eingeben. Wenn die Lizenznummer in digitaler Form verfügbar ist (in der eMail), wird empfohlen, sie zu kopieren und einzufügen.

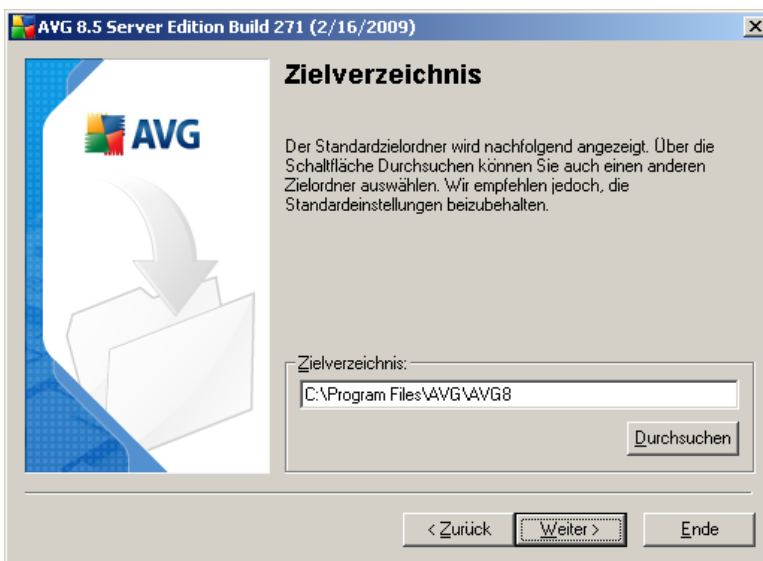


The screenshot shows a dialog box titled "AVG 8.5 Server Edition Build 271 (2/16/2009)". The main heading is "Aktivieren Sie die Lizenz von AVG". On the left, there is a graphic with the AVG logo and a white envelope icon with a grey arrow pointing to it. The right side of the dialog contains three input fields: "Benutzer:" with a text box containing "Name", "Organisation:" with a text box containing "Organization", and "Lizenz:" with a text box containing a series of 'x' characters. Below these fields is a paragraph of text: "Wenn Sie die Software online erworben haben, wurde Ihnen die Lizenznummer per eMail mitgeteilt. Um Tippfehler zu vermeiden, empfehlen wir Ihnen, die Nummer aus Ihrer eMail zu kopieren und einzufügen. Wenn Sie die Software im Handel gekauft haben, befindet sich die Lizenznummer auf der Registrierungskarte, die Ihrem Produkt beiliegt. Achten Sie darauf, die Nummer richtig zu kopieren." At the bottom of the dialog are three buttons: "< Zurück", "Weiter >", and "Ende".

Klicken Sie auf **Weiter**, um mit der Installation fortzufahren.

Wenn Sie im vorherigen Schritt die Standardinstallation ausgewählt haben, wird der Dialog **Setup – Zusammenfassung** angezeigt. Wenn Sie die benutzerdefinierte Installation ausgewählt haben, wird der Dialog **Zielverzeichnis** angezeigt.

3.6. Benutzerdefinierte Installation – Zielverzeichnis



Im Dialog **Zielverzeichnis** können Sie den Speicherort für die Installation von AVG angeben. Standardmäßig wird AVG im Ordner C:/Programme installiert. Wenn Sie einen anderen Speicherort angeben möchten, klicken Sie auf **Durchsuchen**, um die Verzeichnisstruktur anzuzeigen, und wählen Sie den gewünschten Ordner aus. Klicken Sie zum Bestätigen auf **Weiter**.

3.7. Benutzerdefinierte Installation – Komponentenauswahl



Im Dialog **Komponentenauswahl** wird eine Übersicht aller Komponenten von AVG angezeigt, die installiert werden können. Wenn die Standardeinstellungen nicht Ihren Anforderungen entsprechen, können Sie einzelne Komponenten entfernen oder hinzufügen.

Sie können jedoch nur Komponenten auswählen, die in Ihrer AVG Edition enthalten sind. Nur diese Komponenten werden im Dialogfeld „Komponentenauswahl“ zur Installation angeboten!

- **Kommunikationsbibliothek für die Remote-Verwaltung** – Wählen Sie diese Option, wenn Sie AVG mit einem AVG DataCenter (AVG Netzwerk Editionen) verbinden möchten.

Hinweis: Es können nicht alle eMail-Server per Remote-Zugriff verwaltet werden.

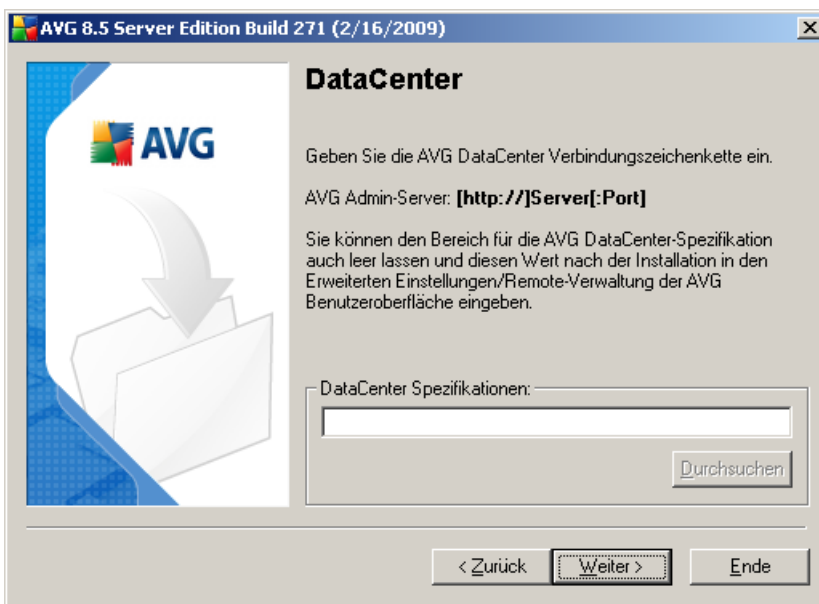
- **Weitere installierte Sprachen** – Sie können die Sprache(n) auswählen, in der AVG installiert werden soll. Aktivieren Sie die Option **Weitere installierte Sprachen**, und wählen Sie anschließend die gewünschte Sprachen aus dem Menü.
- **Anti-Spam-Server (für eMail-Server)** – Wählen Sie diese Option, wenn Sie den Anti-Spam-Schutz für Ihren eMail-Server installieren möchten.

- **eMail-Scanner (für eMail-Server)** – Wählen Sie die Option, wenn Sie den Viren-/Malwareschutz für Ihren eMail-Server installieren möchten.

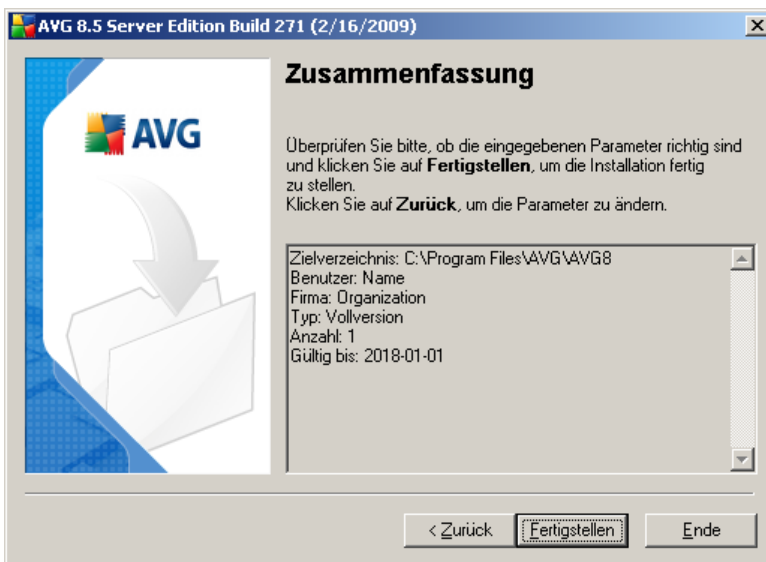
Klicken Sie zum Fortfahren auf die Schaltfläche **Weiter** .

3.8. Benutzerdefinierte Installation – DataCenter

Wenn Sie bei der Modulauswahl das Modul **Kommunikationsbibliothek für die Remote-Verwaltung** ausgewählt haben, können Sie in dieser Ansicht die Verbindungszeichenkette für die Verbindung zum AVG DataCenter festlegen.



3.9. Setup – Zusammenfassung



Der Dialog **Setup – Zusammenfassung** bietet eine Übersicht über alle Parameter des Installationsvorgangs. Bitte überprüfen Sie, ob alle Informationen korrekt sind. Wenn ja, klicken Sie zum Fortfahren auf **Fertigstellen**. Andernfalls können Sie mit der Schaltfläche **Zurück** zum entsprechenden Dialog zurückkehren und die Informationen korrigieren.

3.10. Installieren

Im Dialog **Installation läuft...** wird der Fortschritt des Installationsvorgangs angezeigt. Hier ist keine Aktion erforderlich. Bitte warten Sie, bis die Installation abgeschlossen ist und der Dialog **Installation ist fertig!** angezeigt wird.

3.11. Installation beendet

Der Dialog **Installation beendet** wird als letzter Schritt der AVG-Installation angezeigt. AVG ist nun auf Ihrem Computer installiert und voll funktionsfähig. Das Programm wird im Hintergrund vollständig automatisch ausgeführt.

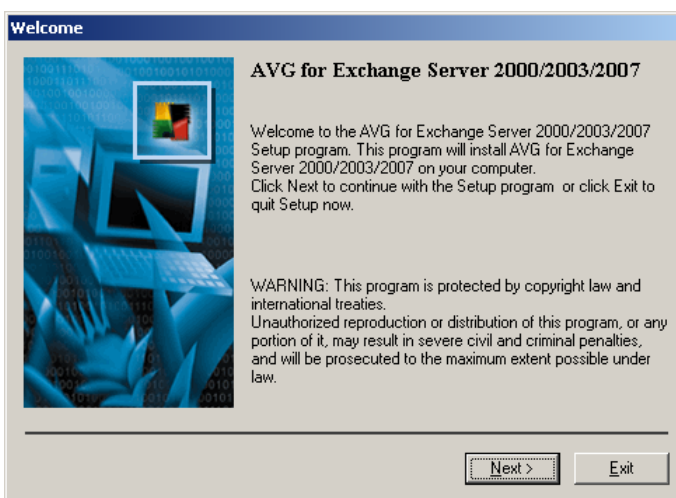
Abhängig vom installierten eMail-Server stehen verschiedene Installationsdialoge zur Verfügung (siehe unten).

4. Optionen für die Installation von AVG eMail-Server

Nachdem AVG erfolgreich installiert wurde, beginnt die Installation einzelner eMail-Sever.

Hinweis: In Kerio MailServer ist der Virenschutz direkt integriert. Weitere Informationen dazu finden Sie im Kapitel [AVG for Kerio MailServer](#).

4.1. Beginn der Installation



Der Installationsvorgang beginnt mit dem Fenster **Willkommen**. Klicken Sie auf **Weiter**, um mit dem nächsten Dialog fortzufahren.

4.2. Lizenzvereinbarung

Dieser Dialog enthält den vollständigen Text der Lizenzvereinbarung von AVG. Bitte lesen Sie die Vereinbarung sorgfältig durch, und bestätigen Sie mit der Schaltfläche **Ja**, dass Sie die Vereinbarung gelesen, verstanden und akzeptiert haben. Falls Sie der Lizenzvereinbarung nicht zustimmen, klicken Sie auf **Nein**, um den Installationsvorgang abubrechen.

4.3. Speicherort

Im nächsten Fenster werden Sie aufgefordert, den Installationsordner auszuwählen. Klicken Sie auf Durchsuchen, um einen anderen Speicherort als den Standardspeicherort auszuwählen. Wenn kein triftiger Grund vorliegt, die Standardeinstellungen zu ändern, wird empfohlen, den aktuellen Speicherort

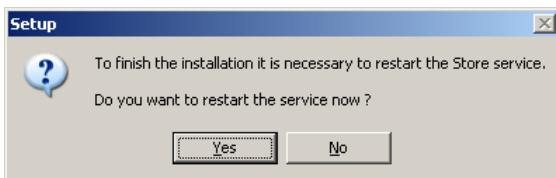
beizubehalten. Klicken Sie zum Fortfahren auf **Weiter**.

4.4. Dateien Kopieren

Das Setup fordert Sie auf, die Installationsdateien zu kopieren, bevor die Installation beendet wird. Stimmen Sie durch Klicken auf **Weiter** zu.

4.5. Neustart des Speicherdienstes

Während des Installationsprozesses bzw. nachdem Sie den Setup-Dialog geschlossen haben, werden Sie aufgefordert, den Speicherdienst für den Exchange Server neu zu starten:

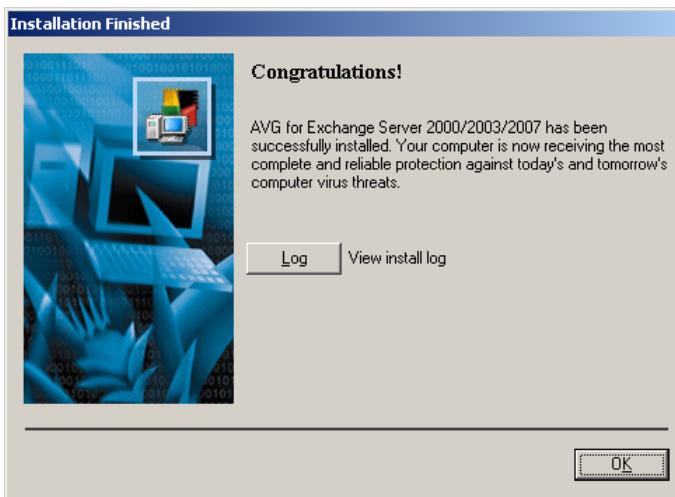


Klicken Sie auf **Ja**, um den Speicherdienst inklusive aller enthaltenen Komponenten von **AVG für MS Exchange** neu zu starten.

Hinweis: *Durch den Neustart des Dienstes ist der Server für einige Zeit nicht erreichbar! Warnen Sie die Benutzer vor einem Neustart, da für alle Benutzer, die während des Neustarts online sind, die Verbindung automatisch getrennt wird.*

4.6. Installation beendet

Nachdem der Installationsassistent alle erforderlichen Dateien auf die Festplatte kopiert hat, ist die Installation beendet.



Sie können die Logdatei der Installation anzeigen, indem Sie auf **Log** klicken.

Sie können das Setup-Protokoll auch später in der Datei „setup.log“ in Ihrem temporären Systemordner finden.

Klicken Sie im Fenster **Installation beendet** auf **OK**, um den Setup-Dialog zu schließen.

Nach der Installation wird automatisch der Erste Schritte-Assistent für AVG gestartet, der Sie in wenigen Schritten durch die grundlegende **AVG 8.5 Email Server Edition** Konfiguration führt. Auch wenn die Konfiguration von AVG jederzeit während der Ausführung von AVG aufgerufen werden kann, wird dringend empfohlen, diese Option zu verwenden und die Basiskonfiguration mit Hilfe des Assistenten durchzuführen.

Um individuellen Schutz für Ihren eMail-Server einzurichten, folgen Sie den Anweisungen im entsprechenden Kapitel:

- [**AVG für MS Exchange Server 2007**](#)
- [**AVG für MS Exchange Server 2000/2003**](#)
- [**AVG für Kerio MailServer**](#)

5. AVG für MS Exchange Server 2007

5.1. Konfiguration

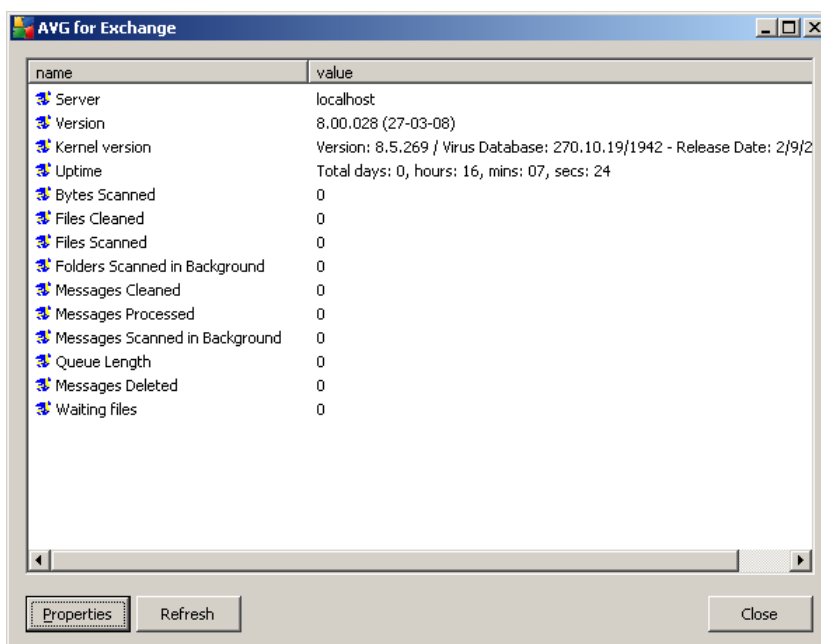
Wenn der Speicherdienst für Exchange 2007 Server nach der Installation von AVG for MS Exchange 2007 Server neu gestartet wird, sind für dessen Start keine weiteren Aktionen erforderlich.

5.1.1. Status

Um den Status oder die Konfiguration von **AVG** anzuzeigen, müssen Sie zunächst die Verwaltungsanwendung „AVG für Exchange“ starten. Diese befindet sich standardmäßig im Installationsverzeichnis:

C:\AVG4ES2K

Navigieren Sie zu diesem Verzeichnis und starten Sie **avg4es2kadm.exe**. Daraufhin wird ein Informationsfenster geöffnet, das eine Übersicht über verschiedene Daten enthält.



Die in diesem Fenster angezeigten Informationen enthalten den Servernamen, die Version der Anwendung, die Datenbankversion, die Kernel-Version und die

Gesamtzeit, die das Programm seit dem letzten Neustart ausgeführt wurde. Zusätzlich werden hier Elemente mit Informationen zur Virenschutzleistung angezeigt (*Zähler zur Leistungsüberwachung*).

AVG für Exchange 2007 Server prüft alle Nachrichten in den Datenbanken der privaten und öffentlichen Ordner. Wenn ein Virus gefunden wird, vermerkt AVG für Exchange 2007 Server dies in der AVG-Logdatei und im Ereignisprotokoll.

5.1.2. VSAPI 2.0

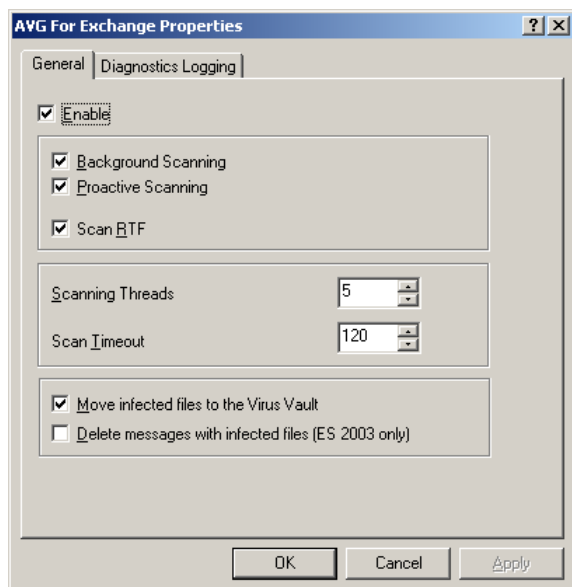
In der Virenschnittstelle **API 2.5** (*VSAPI 2.5 wie in MS Exchange 2003 Server*) können außerdem infizierte Nachrichten gelöscht werden. Diese Funktion kann im Dialog **Eigenschaften** eingerichtet werden (siehe unten).

5.1.3. Allgemeine Eigenschaften

Das Konfigurationsfenster für AVG für MS Exchange 2007 Server kann durch Klicken auf die Schaltfläche **Eigenschaften** geöffnet werden.

Das Konfigurationsfenster **Eigenschaften von AVG für Exchange** enthält zwei Reiter. Hier können Sie die Einstellungen für den eMail-Virenschutz und das Protokollverhalten ändern.

Reiter „General“



Auf dem Reiter **General** befinden sich mehrere voreingestellte Optionen, die sich auf

die Leistung des eMail-Virenschutzes von AVG für MS Exchange 2007 Server beziehen:

- **Enable** – Hier können Sie das Scannen der eMails aktivieren und deaktivieren.
- **Background Scanning** – Hier können Sie den Prozess der Hintergrundprüfung aktivieren und deaktivieren. Die Hintergrundprüfung ist eine der Eigenschaften der VSAPI 2.0/2.5-Anwendungsschnittstelle. Es handelt sich um das Scannen der Exchange Messaging Datenbanken in eigenen Threads. Wird ein Objekt in den Ordnern der Benutzerpostfächer gefunden, das noch nicht gescannt wurde, wird es zum Scannen an AVG für Exchange 2007/ Server weitergeleitet. Die Suche nach nicht geprüften Objekten und der Virentest werden parallel ausgeführt.

Für jede Datenbank wird ein bestimmter Thread niedriger Priorität verwendet, um sicherzustellen, dass andere Aufgaben (z. B. das Speichern von eMail-Nachrichten in der Microsoft Exchange-Datenbank) vorrangig ausgeführt werden.

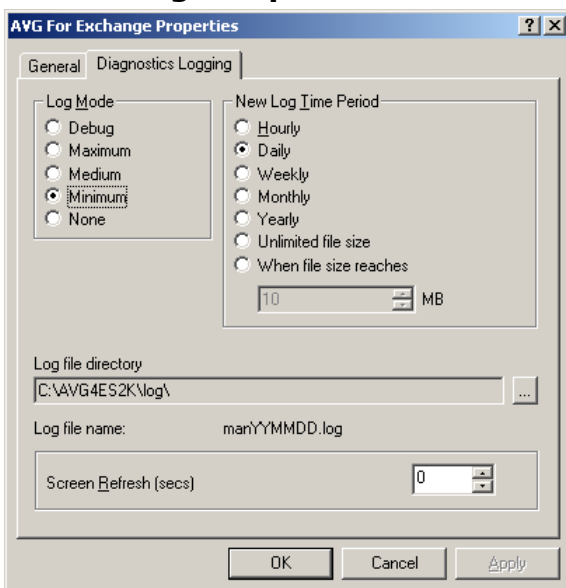
- **Proactive Scanning** – Hier können Sie die Funktion zum vorausschauenden Scannen von VSAPI 2.0/2.5 aktivieren und deaktivieren. Beim vorausschauenden Scannen wird ein dynamisches Prioritätsmanagement der Objekte in der Prüfungswarteschlange genutzt. Objekte mit niedrigerer Priorität werden erst gescannt, wenn der Scan für alle Objekte höherer Priorität abgeschlossen ist (meist werden diese auf Anforderung in die Warteschlange gestellt). Objekte erhalten jedoch durch einen Clientzugriff eine höhere Priorität, d.h. die Priorität des Objekts wird entsprechend der Benutzeraktivität geändert.
- **Scan RTF** – Sie können hier festlegen, ob RTF-Dateien geprüft werden sollen.
- **Scanning Threads** – Der Prozess der Virenprüfung ist in der Standardeinstellung in verschiedene Threads aufgeteilt, um die Scan-Leistung auf einem hohen Niveau zu halten. Sie können hier die Anzahl der Threads ändern. Die Standardanzahl wird nach der Formel „2 × 'Anzahl der Prozessoren' + 1“ berechnet.
- **Feld „Scan Timeout“** – Die maximale Wartezeit (in Sekunden) eines Threads für den Zugriff auf eine zu scannende Nachricht.
- **Infizierte Dateien in die Virenquarantäne verschieben** – Wenn dieses Kontrollkästchen aktiviert ist, wird jede infizierte eMail in die AVG **Virenquarantäne** verschoben.
- **Nachrichten mit infizierten Dateien löschen (nur ES 2003/2007)** – Wenn dieser Eintrag aktiviert ist, werden infizierte eMails gelöscht. Wenn dieses Kontrollkästchen deaktiviert ist, wird die infizierte Nachricht an den Empfänger übertragen, und der infizierte Anhang wird durch einen Text über den gefundenen Virus ersetzt. Diese Option ist nur bei VSAPI 2.5 in Exchange 2007 Server verfügbar.

Alle Funktionen auf dieser Registerkarte sind benutzerspezifische Erweiterungen der Dienste der Microsoft VSAPI 2.0/2.5-Benutzerschnittstelle. Ausführliche Informationen über die VSAPI 2.0/2.5 finden Sie unter folgenden Adressen und über die dortigen Links:

- <http://support.microsoft.com:80/support/kb/articles/Q285/6/67.ASP> für allgemeine Informationen über VSAPI 2.0 in Exchange 2000 Server Service Pack 1
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k> – Für Informationen über die Interaktion zwischen Exchange- und Antiviren-Software
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;823166> für Informationen über zusätzliche Features von VSAPI 2.5 in der Anwendung Exchange 2003 Server.

Hinweis: Das Scan-Verhalten wird von der Anwendung AVG gesteuert. Wählen Sie im Hauptmenü der Anwendung „Tools/Erweiterte Einstellungen“ aus. (Weitere Informationen finden Sie im Kapitel [eMail-Scanner](#)).

5.1.4. Diagnoseprotokolle

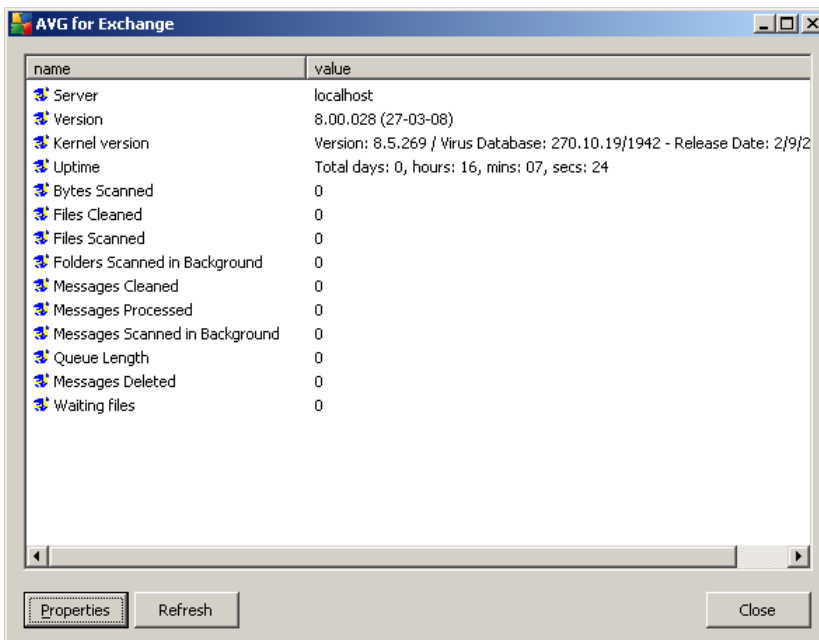


Auf diesem Reiter können Sie die Häufigkeit der Protokollierung für die Virenprüfung und das allgemeine Verhalten definieren. Auf dem Reiter Diagnostics Logging sind einige Felder voreingestellt:

- **Log Mode** – Hier können Sie die Menge der protokollierten Informationen festlegen.
- **New Log Time Period** – Hier können Sie definieren, wann eine neue Logdatei angelegt werden soll und wie groß diese werden darf.
- **Log file directory** – Hier können Sie den Standardspeicherort der Logdatei ändern.
- **Log file name** – Hier wird der Standardname der Logdatei angezeigt.
- **Screen Refresh (secs)** – Hier können Sie festlegen, wie oft der Bildschirm im Monitor (zu sehen im Informationsfenster „AVG für Exchange Server“) aktualisiert werden soll.

5.2. Server-Überwachung

5.2.1. Online-Überwachung



name	value
Server	localhost
Version	8.00.028 (27-03-08)
Kernel version	Version: 8.5.269 / Virus Database: 270.10.19/1942 - Release Date: 2/9/2
Uptime	Total days: 0, hours: 16, mins: 07, secs: 24
Bytes Scanned	0
Files Cleaned	0
Files Scanned	0
Folders Scanned in Background	0
Messages Cleaned	0
Messages Processed	0
Messages Scanned in Background	0
Queue Length	0
Messages Deleted	0
Waiting files	0

Buttons: Properties, Refresh, Close

Im Informationsfenster AVG für MS Exchange Server (Siehe hierzu den Abschnitt [Konfiguration/Status](#)) werden verschiedene Felder angezeigt:

Die ersten vier Einträge bieten allgemeine Informationen über den Status des Servers und von AVG für MS Exchange 2007 Server:

- **Server** – Servername
- **Version** – Version von AVG für MS Exchange 2007 Server
- **Kernel version** – Version des Virenschutz-Kernels und dessen interner Virendatenbank
- **Uptime** – Gesamtzeit seit dem letzten Neustart des Exchange-Servers

Die anderen Einträge stellen bestimmte Zähler der Leistungsüberwachung der VSAPI 2.0/2.5 mit Bezug auf die Virenprüfung von Exchange 2007 Server dar. Die Zähler haben folgende Bedeutung:

- **Bytes Scanned** – Gesamtanzahl der Bytes in allen vom Virenscanner gescannten Dateien
- **Files Cleaned** – Gesamtanzahl der einzelnen vom Virenscanner bereinigten Dateien
- **Gescannte Dateien** – Gesamtanzahl der vom Virenscanner gescannten Dateien
- **Folders Scanned in Background** – Gesamtanzahl der Ordner, die durch die Hintergrundprüfung bearbeitet werden
- **Messages Cleaned** – Gesamtanzahl der vom Virenscanner desinfizierten Nachrichten oberster Priorität.
- **Messages Processed** – Kumulierte Anzahl der Nachrichten oberster Priorität, die vom Virenscanner verarbeitet wurden
- **Messages Scanned in Background** – Gesamtanzahl der Nachrichten, die durch die Hintergrundprüfung verarbeitet werden
- **Queue Length** – Aktuelle Anzahl ausstehender Anforderungen zur Virenprüfung in der Warteschlange
- **Messages Deleted** – Gesamtanzahl aller verdächtigen Nachrichten, die vom Virenscanner gelöscht wurden (nur in VSAPI 2.5 verfügbar)
- **Waiting Files** – Anzahl der Dateien, die auf eine Virenprüfung warten

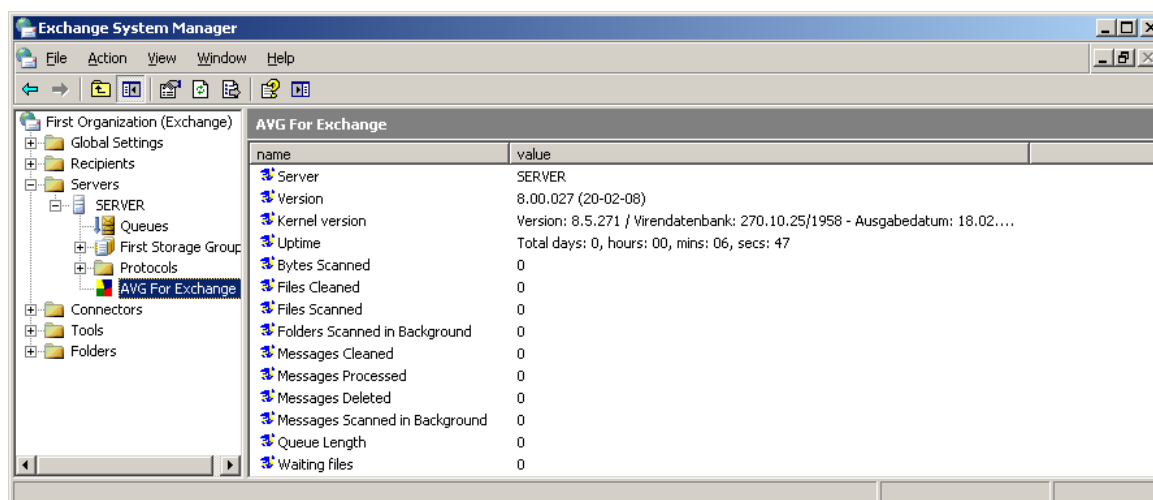
6. AVG für MS Exchange Server 2000/2003

6.1. Konfiguration

Wird der Speicherdienst für Exchange 2000/2003 Server nach der Installation von **AVG for MS Exchange 2000/2003 Server** neu gestartet, sind für dessen Start keine weiteren Aktionen erforderlich.

6.1.1. Status

Um den Status von **AVG** anzuzeigen, starten Sie den MS Exchange System-Manager. Wählen Sie in der Baumstruktur im Zweig Server (*auf der linken Seite des Hauptfensters*) einen bestimmten Server aus. Im Unterzweig des Servers befindet sich der Zweig AVG for Exchange. Wenn Sie diesen Zweig auswählen, wird das Informationsfenster geöffnet, das einen Überblick über verschiedene Daten enthält.



Die in diesem Fenster angezeigten Informationen enthalten den Servernamen, die Version der Anwendung, die Datenbankversion, die Kernel-Version und die Gesamtzeit, die das Programm seit dem letzten Neustart ausgeführt wurde. Zusätzlich werden hier Elemente mit Informationen zur Virenschutzleistung angezeigt (*Zähler zur Leistungsüberwachung*).

AVG für Exchange 2000/2003 Server prüft alle Nachrichten in den Datenbanken der privaten und öffentlichen Ordner. Wenn ein Virus gefunden wird, vermerkt AVG für Exchange 2000/2003 Server dies in der AVG Logdatei und im Ereignisprotokoll.

6.1.2. VSAPI 2.0

In der Virus Scanning Application Programming Interface **API 2.0** (VSAPI 2.0 wie in Exchange 2000 Server) können infizierte eMail-Dateien nicht gelöscht werden. Da der virenfizierte Anhang der eMail-Nachricht nicht gelöscht werden kann, wird der Dateiname geändert: AVG für Exchange 2000/2003 Server hängt dem ursprünglichen Dateinamen die Erweiterung .virusinfo.txt an. Der Dateiinhalt wird mit einer Nachricht zum bekannten Virus überschrieben. Wenn sich direkt in der Nachricht ein Virus befindet, wird der gesamte eMail-Text mit dem Hinweis überschrieben, dass in der Nachricht ein Virus gefunden wurde.

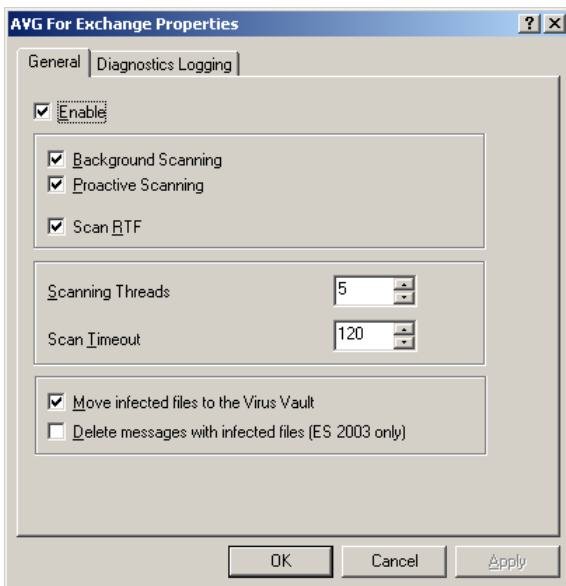
In der Virus Scanning Application Programming Interface **API 2.5** (VSAPI 2.5 wie in MS Exchange 2003 Server) können außerdem infizierte Nachrichten gelöscht werden. Diese Funktion kann im Konfigurationsdialog AVG für MS Exchange 2000/2003 Server eingerichtet werden.

6.1.3. Allgemeine Eigenschaften

Das Konfigurationsfenster AVG für Exchange 2000/2003 Server kann geöffnet werden, indem Sie mit der rechten Maustaste auf den Zweig **AVG for Exchange** klicken und **Eigenschaften** auswählen. Alternativ können Sie das Fenster öffnen, indem Sie im oberen Menü auf **Aktion** klicken.

Das Konfigurationsfenster **Eigenschaften von AVG for Exchange** enthält zwei Reiter. Hier können Sie die Einstellungen für den eMail-Virenschutz und das Protokollverhalten ändern.

Reiter „General“



Auf dem Reiter **General** befinden sich mehrere voreingestellte Optionen, die sich auf die Leistung des eMail-Virenschutzes von AVG für Exchange 2000/2003 Server beziehen:

- **Enable** – Hier können Sie das Scannen der eMails aktivieren und deaktivieren.
- **Background Scanning** – Hier können Sie den Prozess der Hintergrundprüfung aktivieren und deaktivieren. Die Hintergrundprüfung ist eine der Eigenschaften der VSAPI 2.0/2.5-Anwendungsschnittstelle. Es handelt sich um das Scannen der Exchange Messaging Datenbanken in eigenen Threads. Wenn ein Objekt vor dem Speichern in den Ordnern der Benutzerpostfächer nicht gescannt wurde, wird es zum Scannen an AVG für Exchange 2000/2003 Server weitergeleitet. Die Suche nach nicht geprüften Objekten und der Virentest werden parallel ausgeführt.

Für jede Datenbank wird ein bestimmter Thread niedriger Priorität verwendet, um sicherzustellen, dass andere Aufgaben (z. B. das Speichern von eMail-Nachrichten in der Microsoft Exchange-Datenbank) vorrangig ausgeführt werden.

- **Proactive Scanning** – Hier können Sie die Funktion zum vorausschauenden Scannen von VSAPI 2.0/2.5 aktivieren und deaktivieren. Beim vorausschauenden Scannen wird ein dynamisches Prioritätsmanagement der Objekte in der Prüfungswarteschlange genutzt. Objekte mit niedrigerer Priorität werden erst gescannt, wenn der Scan für alle Objekte höherer Priorität abgeschlossen ist (meist werden diese auf Anforderung in die Warteschlange gestellt). Objekte erhalten jedoch durch einen Clientzugriff eine höhere Priorität,

d.h. die Priorität des Objekts wird entsprechend der Benutzeraktivität geändert.

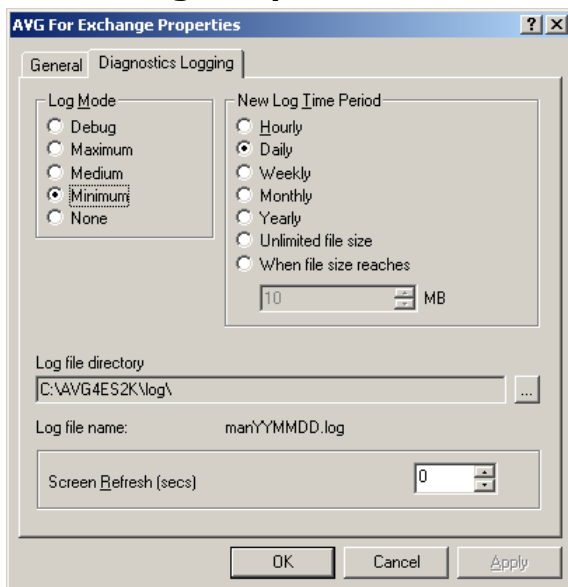
- **Scan RTF** – Sie können hier festlegen, ob RTF-Dateien geprüft werden sollen.
- **Scanning Threads** – Der Prozess der Virenprüfung ist in der Standardeinstellung in verschiedene Threads aufgeteilt, um die Scan-Leistung auf einem hohen Niveau zu halten. Sie können hier die Anzahl der Threads ändern. Die Standardanzahl wird nach der Formel „2 × 'Anzahl der Prozessoren' + 1“ berechnet.
- **Feld „Scan Timeout“** – Die maximale Wartezeit (in Sekunden) eines Threads für den Zugriff auf eine zu scannende Nachricht.
- **Move infected files to the Virus Vault** – Wenn dieses Kontrollkästchen aktiviert ist, wird jede infizierte eMail in die **AVG Virenquarantäne** verschoben.
- **Delete messages with infected files (ES 2003 only)** – Wenn dieses Kontrollkästchen aktiviert ist, werden infizierte eMails gelöscht. Wenn dieses Kontrollkästchen deaktiviert ist, wird die infizierte Nachricht an den Empfänger übertragen, und der infizierte Anhang wird durch einen Text über den gefundenen Virus ersetzt. Diese Option ist nur bei VSAPI 2.5 in Exchange 2003 Server verfügbar.

Alle Funktionen auf dieser Registerkarte sind benutzerspezifische Erweiterungen der Dienste der Microsoft VSAPI 2.0/2.5-Benutzerschnittstelle. Ausführliche Informationen über die VSAPI 2.0/2.5 finden Sie unter folgenden Adressen und über die dortigen Links:

- <http://support.microsoft.com:80/support/kb/articles/Q285/6/67.ASP> für allgemeine Informationen über VSAPI 2.0 in Exchange 2000 Server Service Pack 1
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k> – Für Informationen über die Interaktion zwischen Exchange- und Antiviren-Software
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;823166> für Informationen über zusätzliche Features von VSAPI 2.5 in der Anwendung Exchange 2003 Server.

Hinweis: Das Scan-Verhalten wird von der Anwendung AVG eMail Server gesteuert. Wählen Sie im Hauptmenü der Anwendung „Tools/Erweiterte Einstellungen“ aus. (Weitere Informationen finden Sie im Kapitel [eMail-Scanner](#)).

6.1.4. Diagnoseprotokolle

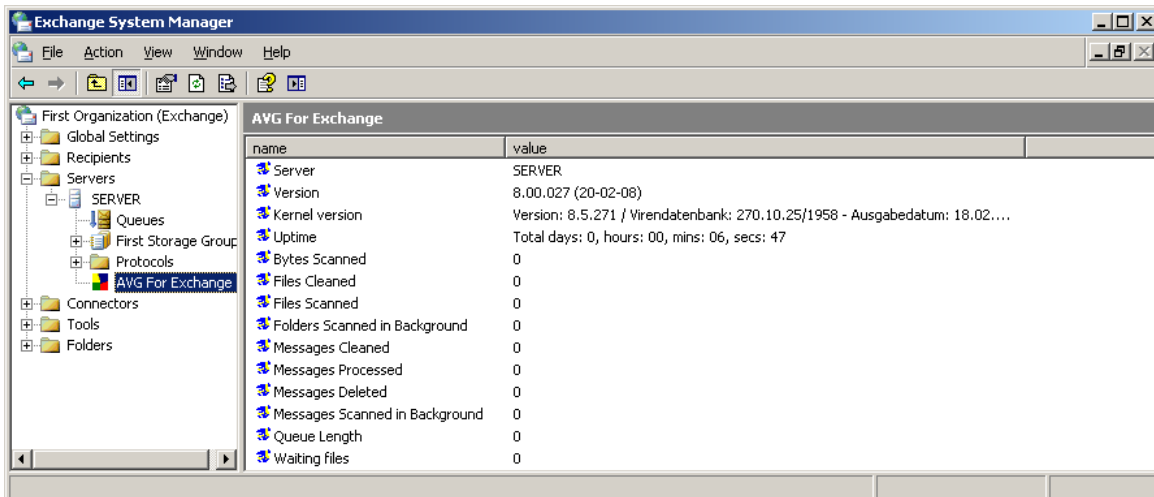


Auf diesem Reiter können Sie die Häufigkeit der Protokollierung für die Virenprüfung und das allgemeine Verhalten definieren. Auf dem Reiter Diagnostics Logging sind einige Felder voreingestellt:

- **Log Mode** – Hier können Sie die Menge der protokollierten Informationen festlegen.
- **New Log Time Period** – Hier können Sie definieren, wann eine neue Logdatei angelegt werden soll und wie groß diese werden darf.
- **Log file directory** – Hier können Sie den Standardspeicherort der Logdatei ändern.
- **Log file name** – Hier wird der Standardname der Logdatei angezeigt.
- **Screen Refresh (secs)** – Hier können Sie festlegen, wie oft der Bildschirm im Monitor (zu sehen im Informationsfenster „AVG für Exchange 2000/2003 Server“) aktualisiert werden soll.

6.2. Server-Überwachung

6.2.1. Online-Überwachung



name	value
Server	SERVER
Version	8.00.027 (20-02-08)
Kernel version	Version: 8.5.271 / Virendatenbank: 270.10.25/1958 - Ausgabedatum: 18.02....
Uptime	Total days: 0, hours: 00, mins: 06, secs: 47
Bytes Scanned	0
Files Cleaned	0
Files Scanned	0
Folders Scanned in Background	0
Messages Cleaned	0
Messages Processed	0
Messages Deleted	0
Messages Scanned in Background	0
Queue Length	0
Waiting files	0

Im Informationsfenster AVG für MS Exchange 2000/2003 Server (Siehe hierzu den Abschnitt [Konfiguration/Status](#)) werden verschiedene Felder angezeigt:

Die ersten vier Einträge bieten allgemeine Informationen über den Status des Servers und von AVG für Exchange 2000/2003 Server:

- **Server** – Servername
- **Version** – Version von AVG für Exchange 2000/2003 Server
- **Kernel version** – Version des Virenschutz-Kernels und dessen interner Virendatenbank
- **Uptime** – Gesamtzeit seit dem letzten Neustart des Exchange-Servers
- **Waiting Files** – Anzahl der Dateien, die auf eine Virenprüfung warten

Die anderen Einträge stellen bestimmte Zähler der Leistungsüberwachung der VSAPI 2.0/2.5 mit Bezug auf die Virenprüfung von Exchange 2000/2003 Server dar und sind möglicherweise nicht immer sichtbar. Die Zähler haben folgende Bedeutung:

- **Bytes Scanned** – Gesamtanzahl der Bytes in allen vom Virenscanner gescannten Dateien
- **Files Cleaned** – Gesamtanzahl der einzelnen vom Virenscanner bereinigten Dateien

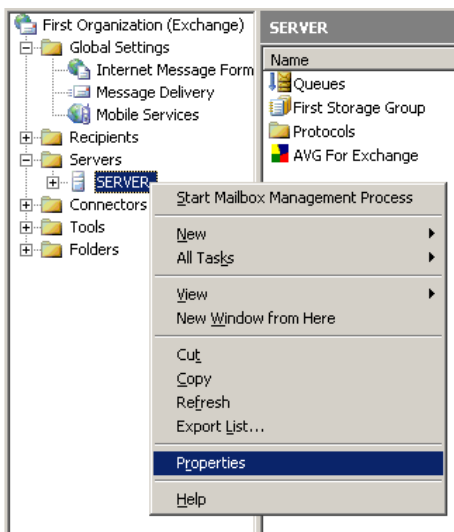
- **Files Cleaned/sec** – Rate, mit der einzelne Dateien durch den Virenschanner desinfiziert werden
- **Files Quarantined** – Gesamtanzahl der einzelnen vom Virenschanner in die Quarantäne verschobenen Dateien
- **Files Quarantined/sec** – Rate, mit der einzelne Dateien durch den Virenschanner in die Quarantäne verschoben werden
- **Folders Scanned in Background** – Gesamtanzahl der Ordner, die durch die Hintergrundprüfung bearbeitet werden
- **Messages Cleaned** – Gesamtanzahl der vom Virenschanner desinfizierten Nachrichten oberster Priorität.
- **Messages Cleaned/sec** – Rate, mit der Nachrichten oberster Priorität durch den Virenschanner desinfiziert werden
- **Messages Quarantined** – Gesamtanzahl der vom Virenschanner in die Quarantäne verschobenen Nachrichten oberster Priorität
- **Messages Quarantined/sec** – Rate, mit der Nachrichten oberster Priorität durch den Virenschanner in die Quarantäne verschoben werden
- **Messages Processed** – Kumulierte Anzahl der Nachrichten oberster Priorität, die vom Virenschanner verarbeitet wurden
- **Messages Processed/sec** – Rate, mit der Nachrichten oberster Priorität durch den Virenschanner verarbeitet werden
- **Messages Scanned in Background** – Gesamtanzahl der Nachrichten, die durch die Hintergrundprüfung verarbeitet werden
- **Messages Deleted** – Gesamtanzahl aller verdächtigen Nachrichten, die vom Virenschanner gelöscht wurden (nur in VSAPI 2.5 verfügbar)
- **Messages Deleted/sec** – Rate, mit der verdächtige Nachrichten vom Virenschanner gelöscht werden (nur in VSAPI 2.5 verfügbar)
- **Queue Length** – Aktuelle Anzahl ausstehender Anforderungen zur Virenprüfung in der Warteschlange

6.2.2. Ereignisprotokoll

Neben der Online-Überwachung von AVG für Exchange 2000/2003 Server können Sie auch eine Protokollierung von Ereignissen des Virenschanners im **Ereignisprotokoll** konfigurieren. Mit den verfügbaren Ereignissen können viele Aspekte erfasst werden, z. B. Hinweise hinsichtlich des Ladens von Programmbibliotheken, Ereignisse zu gefundenen Viren, Warnungen zur Fehlerbehandlung usw.

Die Protokollebenen der Exchange VSAPI 2.0/2.5 konfigurieren Sie im Hauptfenster des *Exchange System Managers* (Siehe Protokollabschnitt [Konfiguration/Diagnoseprotokoll](#)).

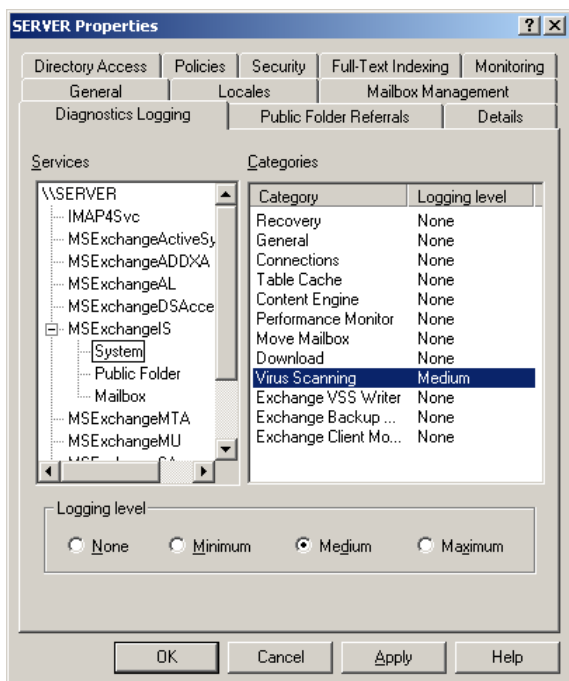
- Doppelklicken Sie in der Baumstruktur auf den Zweig **Server**.
- Wählen Sie den entsprechenden Server aus (Im untenstehenden Bild ist der Servername hervorgehoben)
- Klicken Sie mit der rechten Maustaste auf den Servernamen und wählen Sie im Kontextmenü die Option **Eigenschaften** aus.



- Das Fenster **Eigenschaften** wird angezeigt.
- Wechseln Sie zum Reiter **Diagnoseprotokoll**.
- Wählen Sie im Baum **Dienste** den Ordner „MExchangeIS/System“ aus.
- Markieren Sie in der Liste **Kategorien** den Eintrag **Viren werden geprüft**

Wählen Sie den Protokolliergrad für das Ereignisprotokoll des Betriebssystems aus. Folgende Ebenen stehen zur Verfügung:

- **Keine**
- **Minimal**
- **Mittel**
- **Maximal**



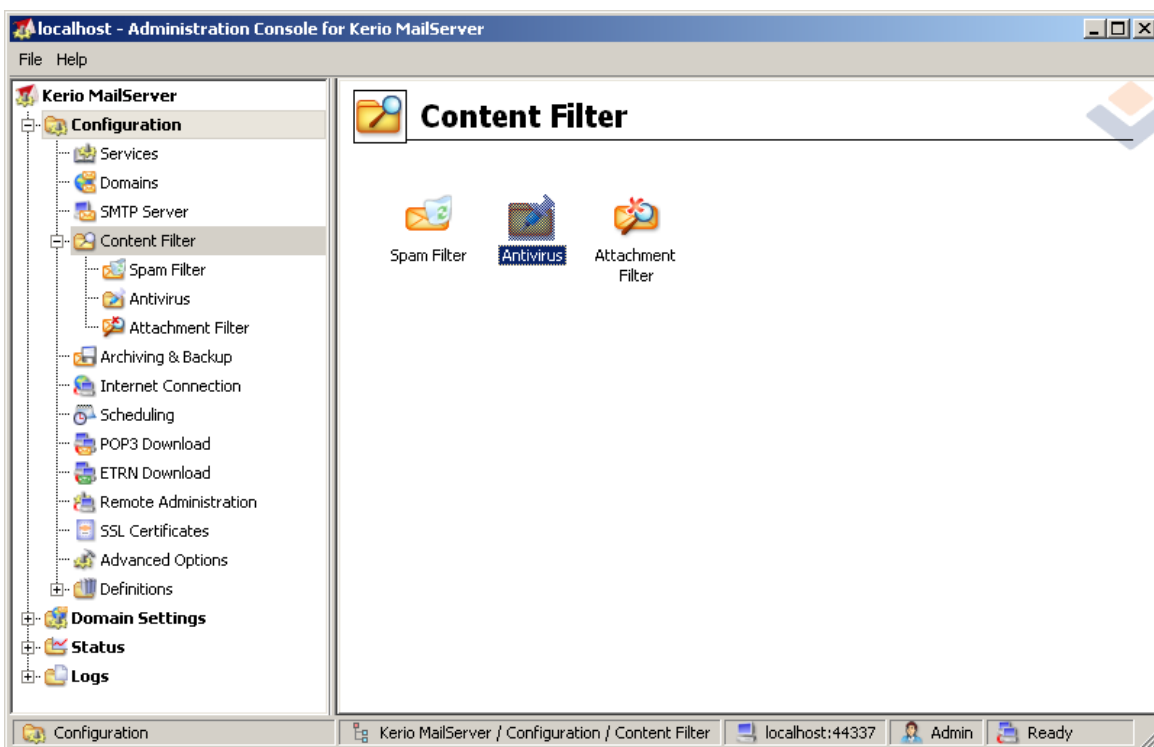
Hinweis: Eine vollständige Beschreibung der Ereignisse der VSAPI 2.0/2.5 finden Sie unter folgendem Link:

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;294336>.

7. AVG for Kerio MailServer

7.1. Konfiguration

In Kerio MailServer ist der Virenschutz direkt integriert. Starten Sie die Kerio-Administrationskonsole, um den eMail-Schutz von Kerio MailServer über die Scan-Engine von AVG zu aktivieren. Wählen Sie in der Baumstruktur auf der linken Seite des Anwendungsfensters im Zweig Konfiguration den Unterzweig Inhaltsfilter aus:

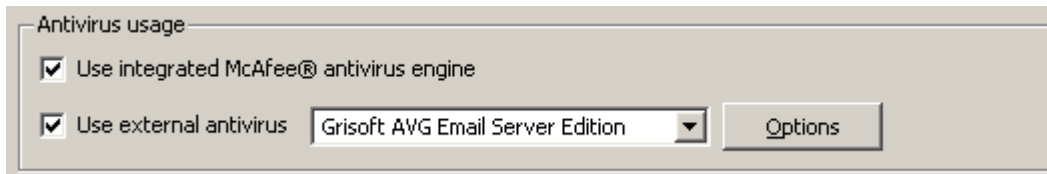


Wenn Sie auf den Eintrag „Inhaltsfilter“ klicken, wird ein Dialog mit drei Einträgen angezeigt:

- **Spamfilter**
- **Antivirus** (siehe Abschnitt **Antivirus**)
- **Mailanhänge** (siehe Abschnitt **Mailanhänge**)

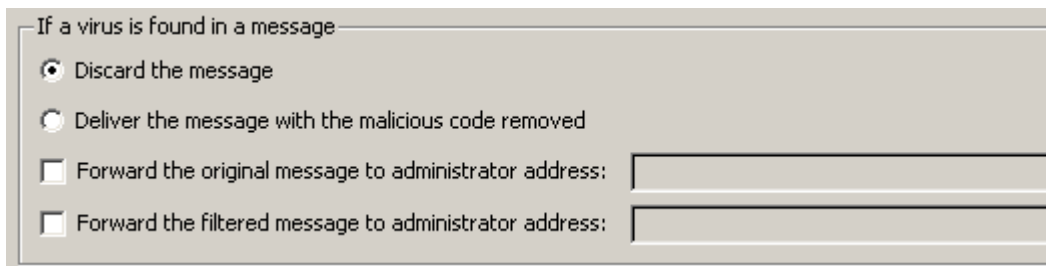
7.1.1. Anti-Virus

Zum Aktivieren von AVG für Kerio MailServer aktivieren Sie das Kontrollkästchen „Externes Antivirusprogramm verwenden“ und wählen Sie im Menü für die externe Antivirus-Software im Konfigurationsfenster im Bereich Antivirusbenutzung die Option „AVG eMail Server Edition“ aus:



Im folgenden Abschnitt können Sie festlegen, was mit einer infizierten oder gefilterten Datei geschehen soll:

- **In einer eMail wird ein Virus entdeckt**

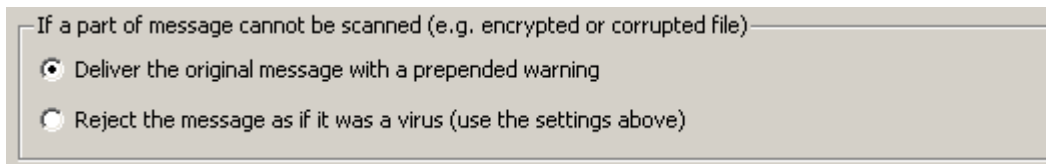


Hier wird festgelegt, welche Aktion durchgeführt werden soll, wenn ein Virus in einer Nachricht entdeckt wird oder wenn eine Nachricht mit einem Filter für Anhänge überprüft wird:

- **Nachricht verwerfen** – Wenn dieses Optionsfeld aktiviert ist, wird die infizierte oder gefilterte Nachricht gelöscht.
- **Nachricht mit entferntem schädlichem Code senden** – Wenn dieses Optionsfeld aktiviert ist, wird die Nachricht an den Empfänger gesendet, jedoch ohne den möglicherweise schädlichen Anhang.
- **Ursprüngliche Nachricht an Administratoradresse weiterleiten** – Wenn dieses Optionsfeld aktiviert ist, wird die vireninferierte Nachricht an die im entsprechenden Textfeld angegebene Adresse gesendet.
- **Gefilterte Nachricht an Administratoradresse weiterleiten** – Wenn dieses Optionsfeld aktiviert ist, wird die gefilterte Nachricht an die im

entsprechenden Textfeld angegebene Adresse weitergeleitet.

- **Ein Teil einer Nachricht kann nicht gescannt werden (z. B. bei einer verschlüsselten oder beschädigten Datei)**



If a part of message cannot be scanned (e.g. encrypted or corrupted file)

- Deliver the original message with a prepended warning
- Reject the message as if it was a virus (use the settings above)

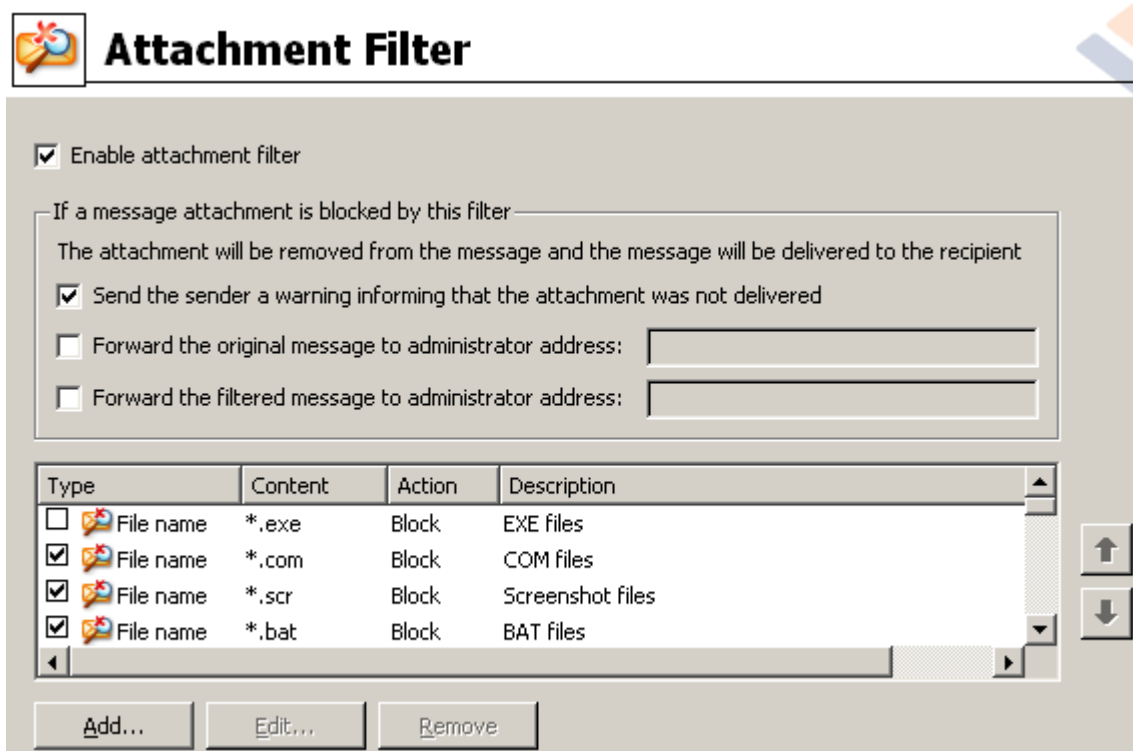
Hier wird festgelegt, welche Aktion durchgeführt werden soll, wenn ein Teil der Nachricht oder des Anhangs nicht gescannt werden kann:

- **Senden der ursprünglichen Nachricht mit einer vorbereiteten Warnung** – Die Nachricht (oder der Anhang) wird ungeprüft übermittelt. Der Benutzer wird gewarnt, dass die Nachricht möglicherweise immer noch Viren enthält.
- **Nachricht als infiziert behandeln und zurückweisen** – Das System reagiert so, als wäre ein Virus erkannt worden (z. B. wird die Nachricht ohne Anhang ausgeliefert oder der Anhang wird entfernt). Diese Option ist zwar sicher, jedoch ist das Senden von kennwortgeschützten Archiven nicht mehr möglich.

Hinweis: Das Scan-Verhalten wird von der Anwendung AVG eMail Server gesteuert. Wählen Sie im Hauptmenü der Anwendung „Tools/Erweiterte Einstellungen“ aus. (Weitere Informationen finden Sie im Kapitel [eMail-Scanner](#)).

7.1.2. Filter für Anhänge

Im Menü Filter für Anhänge befindet sich eine Liste verschiedener Anhangsdefinitionen:



Über das Kontrollkästchen Filter für Anhang aktivieren können Sie den Filter für eMail-Anhänge aktivieren/deaktivieren. Optional können Sie die folgenden Einstellungen ändern:

- **Warnung an den Absender schicken, dass der Anhang nicht übertragen wurde**

Der Absender erhält eine Warnung von Kerio MailServer, dass eine Nachricht mit einem Virus oder einem blockierten Anhang versendet wurde.

- **Ursprüngliche Nachricht an Administratoradresse weiterleiten**

Die Nachricht wird (so wie sie ist – mit dem infizierten oder blockierten Anhang) an eine festgelegte eMail-Adresse gesendet – unabhängig davon, ob es sich bei der Adresse um eine lokale oder externe Adresse handelt.

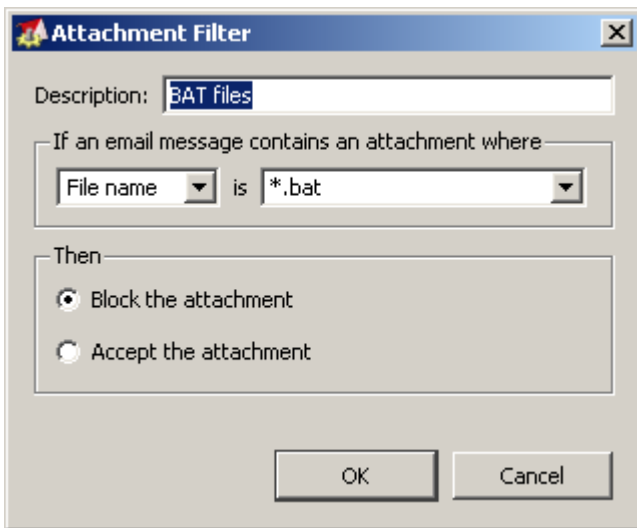
- **Gefilterte Nachricht an Administratoradresse weiterleiten**

Die Nachricht wird ohne den infizierten oder blockierten Anhang (ausgenommen der unten ausgewählten Aktionen) an die angegebene eMail-Adresse weitergeleitet. Mit dieser Option kann überprüft werden, ob AVG Anti-Virus und/oder der Filter für Anhänge fehlerfrei funktionieren.

Jedes Element der Erweiterungsliste verfügt über vier Felder:

- **Typ** – Angabe zu der Art des Anhangs, der über die Erweiterung im Feld „Inhalt“ festgelegt wurde. Mögliche Werte sind Dateiname oder MIME-Typ. Sie können das entsprechende Kontrollkästchen in diesem Feld aktivieren, um das Filtern des Anhangs für dieses Element zu aktivieren.
- **Inhalt** – Hier kann eine zu filternde Erweiterung eingegeben werden. Hierfür können Sie Platzhalter des Betriebssystems nutzen (zum Beispiel steht die Zeichenfolge '*.doc.*' für alle Dateien mit der Erweiterung „.doc“ usw.).
- **Aktion** – Definiert die Aktion, die mit dem entsprechenden Anhang durchgeführt werden soll. Mögliche Aktionen sind „Akzeptieren“ (akzeptiert den Anhang) und „Blockieren“ (blockiert den Anhang, wie auf dem Reiter „Aktion“ festgelegt).
- **Beschreibung** – In diesem Feld wird die Beschreibung des Anhangs festgelegt.

Durch Klicken auf Entfernen können Sie einen Eintrag aus der Liste entfernen. Der Liste können weitere Einträge hinzugefügt werden, indem Sie auf **Hinzufügen** klicken. Sie können auch einen bestehenden Eintrag ändern, indem Sie auf **Bearbeiten** klicken. Dann wird folgendes Fenster angezeigt:

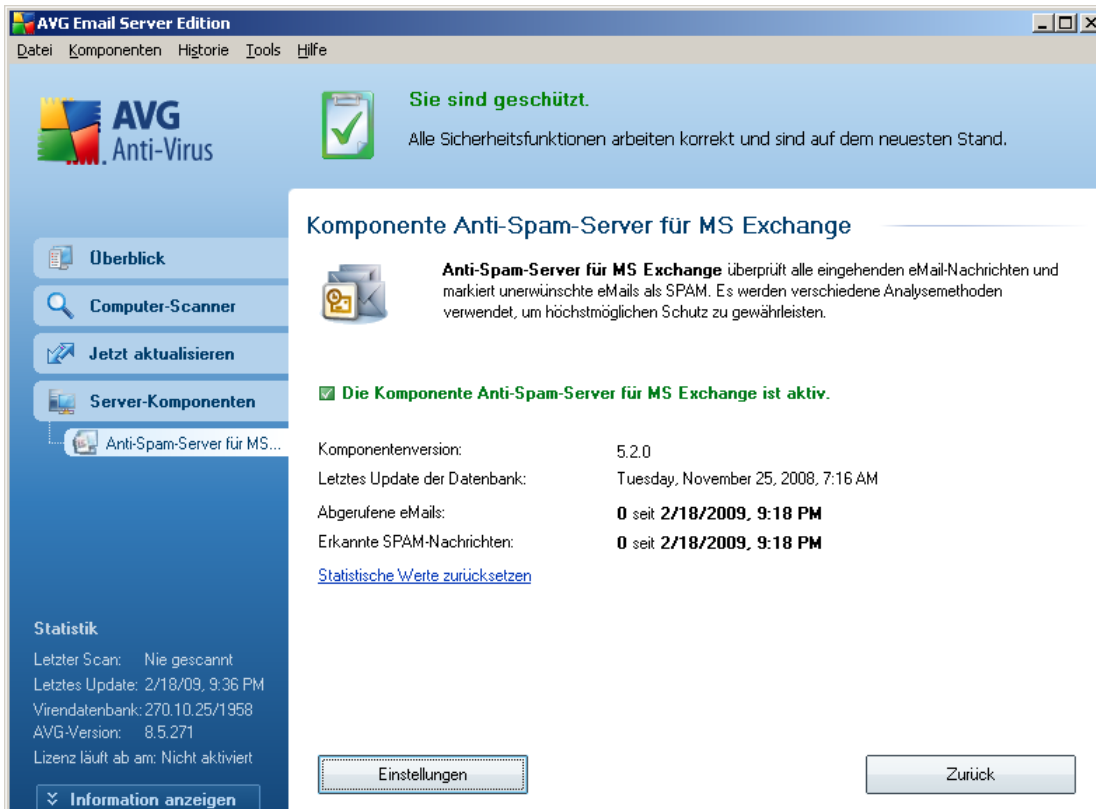


- Im Feld Beschreibung können Sie eine kurze Beschreibung des zu filternden Anhangs eingeben.
- Im Feld Wenn eine eMail den folgenden Anhang enthält können Sie die Art des Anhangs auswählen (Dateiname oder MIME-Typ). Sie können auch eine bestimmte Erweiterung aus der angebotenen Liste der Erweiterungen auswählen oder den Platzhalter für die Erweiterung direkt eingeben.

Im Feld Auszuführende Aktion können Sie festlegen, ob der definierte Anhang blockiert oder akzeptiert werden soll.

8. Anti-Spam-Konfiguration

8.1. Benutzeroberfläche des Anti-Spam



Der Dialog der Server-Komponente **Anti-Spam** befindet sich im Abschnitt **Server-Komponenten** (Menü links). Dieser Dialog enthält Informationen zur Funktionsweise der Server-Komponente, zum aktuellen Status (*Anti-Spam-Server für MS Exchange ist aktiv*) sowie statistische Daten.

Sie können die Statistik zurücksetzen, indem Sie auf den Verweis **Statistische Werte zurücksetzen** klicken.

Folgende Schaltflächen stehen zur Verfügung:

- **Einstellungen** – Klicken Sie auf diese Schaltfläche, um die [Anti-Spam-Einstellungen](#) zu öffnen.

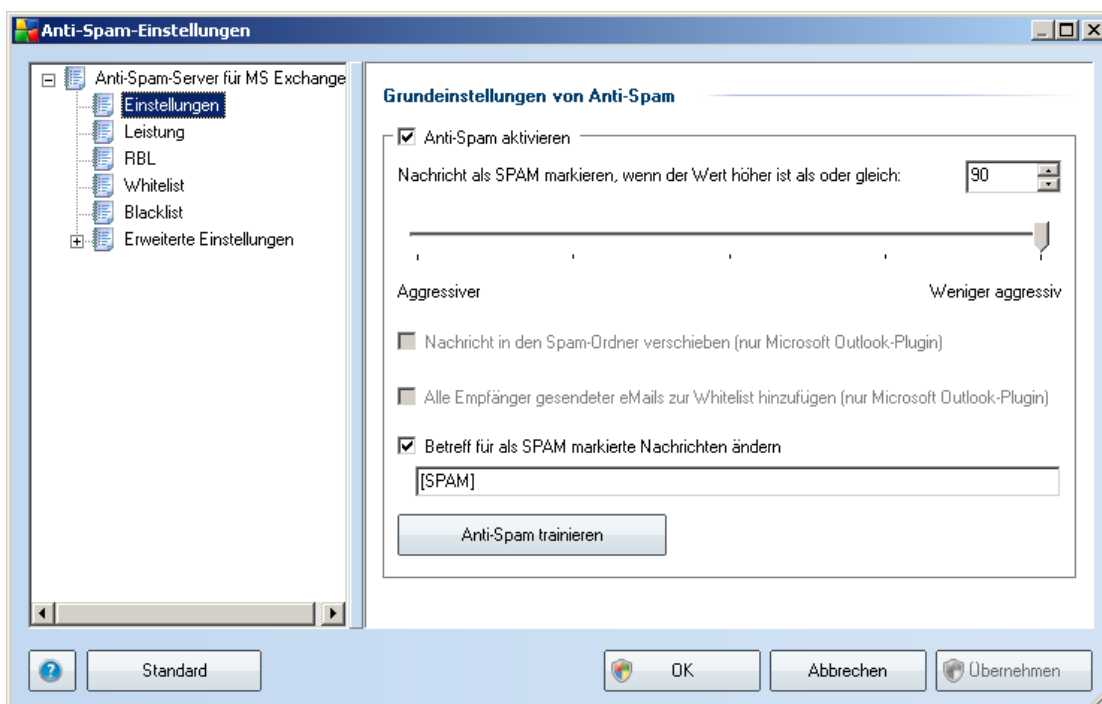
- **Zurück** – Klicken Sie auf diese Schaltfläche, um zur Übersicht über die Server-Komponenten zurückzukehren.

8.2. Grundlagen zu Anti-Spam

Unter Spam versteht man unerwünschte eMails, die meist für ein Produkt oder eine Dienstleistung werben. Sie werden mittels Massenversand an eine riesige Anzahl von eMail-Adressen verschickt und füllen so die Mailboxen der Empfänger. Spam bezieht sich nicht auf legitime Werbemails, für die der Verbraucher sein Einverständnis gegeben hat. Spam ist nicht nur störend, sondern auch oft eine Quelle für Betrugsversuche, Viren und beleidigende Inhalte.

Anti-Spam überprüft alle eingehenden eMails und markiert unerwünschte eMails als SPAM. Die Komponente verwendet verschiedene Analysemethoden, um die einzelnen eMails zu verarbeiten, und bietet damit den größtmöglichen Schutz gegen unerwünschte eMail-Nachrichten.

8.3. Anti-Spam-Einstellungen



Im Dialog **Grundeinstellungen für Anti-Spam** können Sie über die Option **Anti-Spam aktivieren** festlegen, ob Sie die Überprüfung Ihrer eMail-Kommunikation auf

Spam zulassen oder verweigern möchten.

In diesem Dialog können Sie zudem mehr oder weniger aggressive Bewertungen auswählen. Der **Anti-Spam**-Filter weist jeder Nachricht eine Bewertung zu (z. B. *wie sehr der Nachrichteninhalt SPAM ähnelt*), die auf verschiedenen dynamischen Prüftechniken basiert. Sie können die Einstellung **Nachricht als Spam markieren, wenn der Wert höher ist als oder gleich**: anpassen, indem Sie entweder den Wert (0 bis 100) eingeben oder den Schieberegler nach links oder rechts verschieben (*mit dem Schieberegler können nur Werte zwischen 50 und 90 eingestellt werden*).

Wir empfehlen, den Schwellenwert zwischen 50 und 90 oder, wenn Sie wirklich unsicher sind, auf 90 einzustellen. Im Folgenden finden Sie eine kurze Erläuterung der Schwellenwerte:

- **Wert 90–99** – Die meisten eingehenden eMails werden normal in den Posteingang geleitet (ohne als [Spam](#) gekennzeichnet zu werden). Die am leichtesten als [Spam](#) identifizierbaren eMails werden ausgefiltert, aber es kann immer noch ein großer Anteil an [Spam](#) auf Ihren Computer gelangen.
- **Wert 80–89** – eMail-Nachrichten, die [Spam](#) sein könnten, werden ausgefiltert. Auch einige nicht als Spam zu klassifizierende Nachrichten werden eventuell fälschlicherweise ausgefiltert.
- **Wert 60–79** – Als relativ aggressive Konfiguration einzuordnen. Alle eMails, die möglicherweise als [Spam](#) einzustufen sind, werden ausgefiltert. Es ist wahrscheinlich, dass auch nicht als Spam zu klassifizierende Nachrichten ausgefiltert werden.
- **Wert 1–59** – Sehr aggressive Konfiguration. Es ist sehr wahrscheinlich, dass auch Nachrichten abgefangen werden, die nicht wirklich [Spam](#) sind. Dieser Wertebereich wird für den normalen Gebrauch nicht empfohlen.
- **Wert 0** – In diesem Modus erhalten Sie nur eMails von Absendern, die in Ihre [Whitelist](#) eingetragen sind. Alle anderen eMails werden als [Spam](#) betrachtet. **Dieser Wertebereich wird für den normalen Gebrauch nicht empfohlen.**

Sie können außerdem festlegen, wie die erkannten [Spam](#)-Nachrichten behandelt werden sollen:

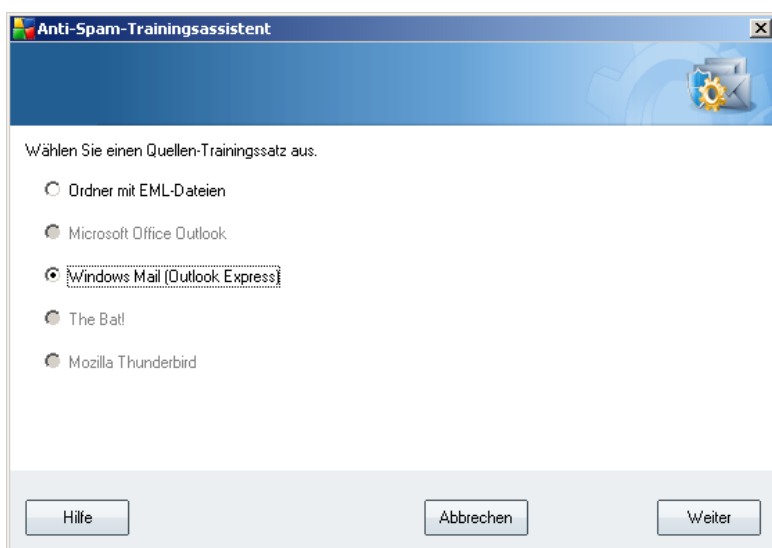
- **Betreff für als SPAM markierte Nachrichten ändern** – Aktivieren Sie dieses Kontrollkästchen, wenn alle als [Spam](#) erkannten Nachrichten mit einem bestimmten Wort oder Zeichen im Betrefffeld markiert werden sollen (geben Sie den gewünschten Text in das aktivierte Textfeld ein)

Die Schaltfläche [Anti-Spam trainieren](#) dient zum Öffnen des [Anti-Spam-](#)

Trainingsassistenten, der im [nächsten Kapitel](#) genauer beschrieben wird.

8.3.1. Anti-Spam-Trainingsassistent

Im ersten Dialog des **Anti-Spam-Trainingsassistenten** werden Sie dazu aufgefordert, die Quelle der eMail-Nachrichten auszuwählen, die Sie für das Training verwenden möchten. In der Regel wählen Sie eMails aus, die nicht als Spam erkannt oder fälschlicherweise als Spam eingestuft worden sind.



Dabei stehen Ihnen die folgenden Optionen zur Verfügung:

- **Ein bestimmter eMail-Client** – Wenn Sie einen der aufgelisteten eMail-Clients verwenden (*MS Outlook, Outlook Express, The Bat! oder Mozilla Thunderbird*), wählen Sie einfach die entsprechende Option aus
- **Ordner mit EML-Dateien** – Wenn Sie ein anderes eMail-Programm verwenden, sollten Sie die Nachrichten zunächst in einem bestimmten Ordner speichern (im *.eml-Format*) oder sich den Speicherort der Nachrichtenordner Ihres eMail-Clients merken. Wählen Sie anschließend **Ordner mit EML-Dateien**, damit Sie den gewünschten Ordner im nächsten Schritt auffinden können

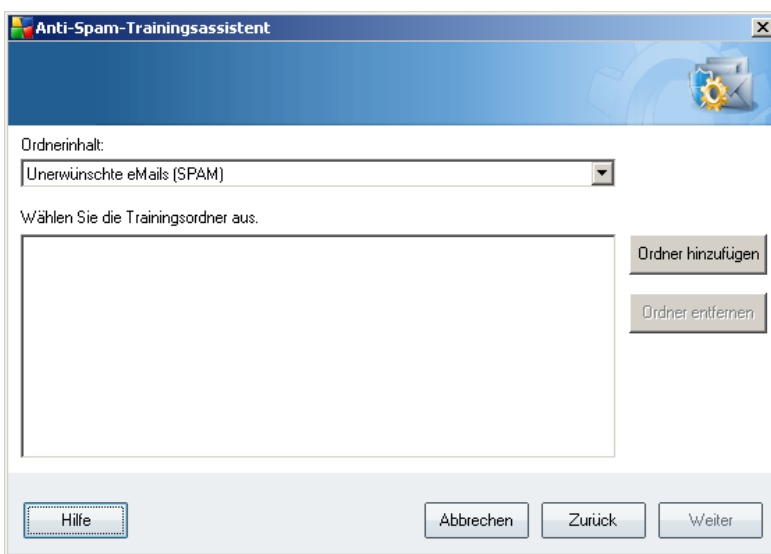
Um das Trainingsverfahren zu beschleunigen, ist es empfehlenswert, die eMails in den Ordnern zunächst zu sortieren, damit der Ordner, den Sie für Trainingszwecke verwenden, ausschließlich Übungsnachrichten enthält (entweder gewünschte oder unerwünschte). Dieser Schritt ist jedoch nicht zwingend erforderlich, da Sie die eMails auch später filtern können.

Wählen Sie die entsprechende Option, und klicken Sie auf **Weiter**, um mit dem Assistenten fortzufahren.

8.3.2. Ordner mit Nachrichten auswählen

Der in diesem Schritt angezeigte Dialog hängt von Ihrer vorherigen Auswahl ab.

Ordner mit EML-Dateien



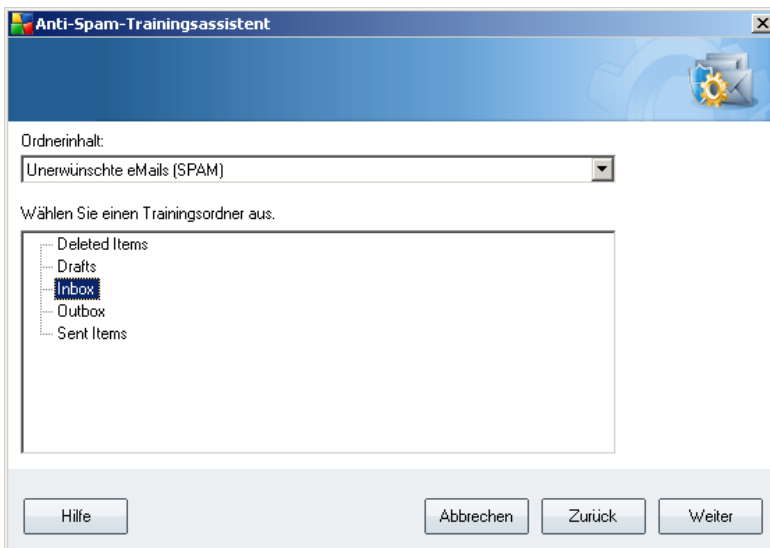
Wählen Sie in diesem Dialog bitte den Ordner mit den Nachrichten aus, den Sie für Trainingszwecke verwenden möchten. Klicken Sie auf die Schaltfläche **Ordner hinzufügen**, um den Ordner mit den EML-Dateien zu suchen (*gespeicherte eMail-Nachrichten*). Der ausgewählte Ordner wird anschließend im Dialog angezeigt.

Wählen Sie im Dropdown-Menü **Ordnerinhalt** eine der zwei Optionen – ob der ausgewählte Ordner gewünschte (*HAM-*) oder unerwünschte (*SPAM-*) Nachrichten enthält. Bitte beachten Sie, dass Sie die Nachrichten im nächsten Schritt filtern können; der Ordner muss also nicht nur Trainings-eMails umfassen. Sie können nicht gewollte ausgewählte Ordner auch aus der Liste entfernen, indem Sie auf die Schaltfläche **Ordner entfernen** klicken.

Klicken Sie im Anschluss daran auf **Weiter**, um zum Dialog zu den [Filteroptionen für Nachrichten](#) zu gelangen.

Ein bestimmter eMail-Client

Sobald Sie eine der Optionen bestätigen, wird ein neuer Dialog angezeigt.

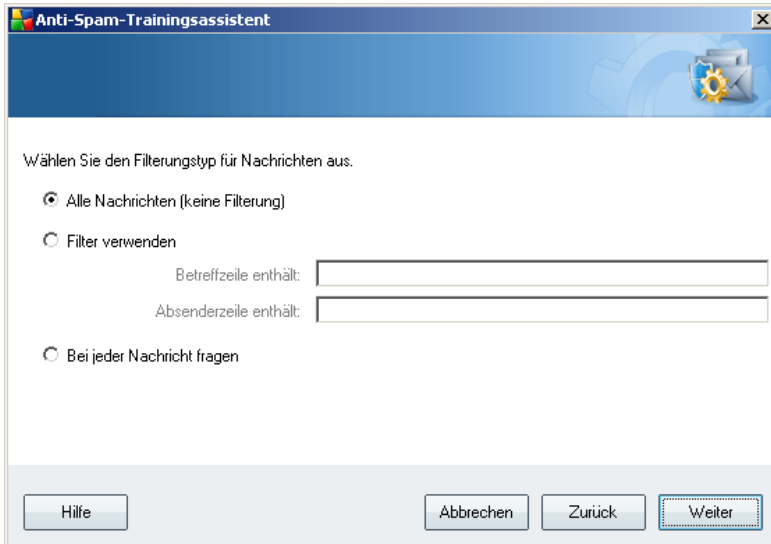


Hinweis: Wenn Sie Microsoft Office Outlook verwenden, werden Sie zunächst dazu aufgefordert, ein Profil in „MS Office Outlook“ auszuwählen.

Wählen Sie im Dropdown-Menü **Ordnerinhalte** eine der folgenden zwei Optionen – ob der ausgewählte Ordner erwünschte (*HAM*-) oder unerwünschte (*SPAM*-) Nachrichten enthält. Bitte beachten Sie, dass Sie die Nachrichten im nächsten Schritt filtern können; der Ordner muss also nicht nur Trainings-eMails umfassen. Im Hauptabschnitt des Dialogs wird eine Baumstruktur des ausgewählten eMail-Clients angezeigt. Bitte suchen Sie nach dem gewünschten Ordner, und wählen Sie ihn mit der Maus aus.

Klicken Sie im Anschluss daran auf **Weiter**, und fahren Sie fort mit den [Filteroptionen für Nachrichten](#).

8.3.3. Optionen für Nachrichtenfilterung



In diesem Dialog können Sie die Filtereinstellungen für Ihre eMail-Nachrichten vornehmen.

Wenn Sie sicher sind, dass der ausgewählte Ordner ausschließlich Nachrichten für Übungszwecke enthält, wählen Sie die Option **Alle Nachrichten (kein Filtern)**.

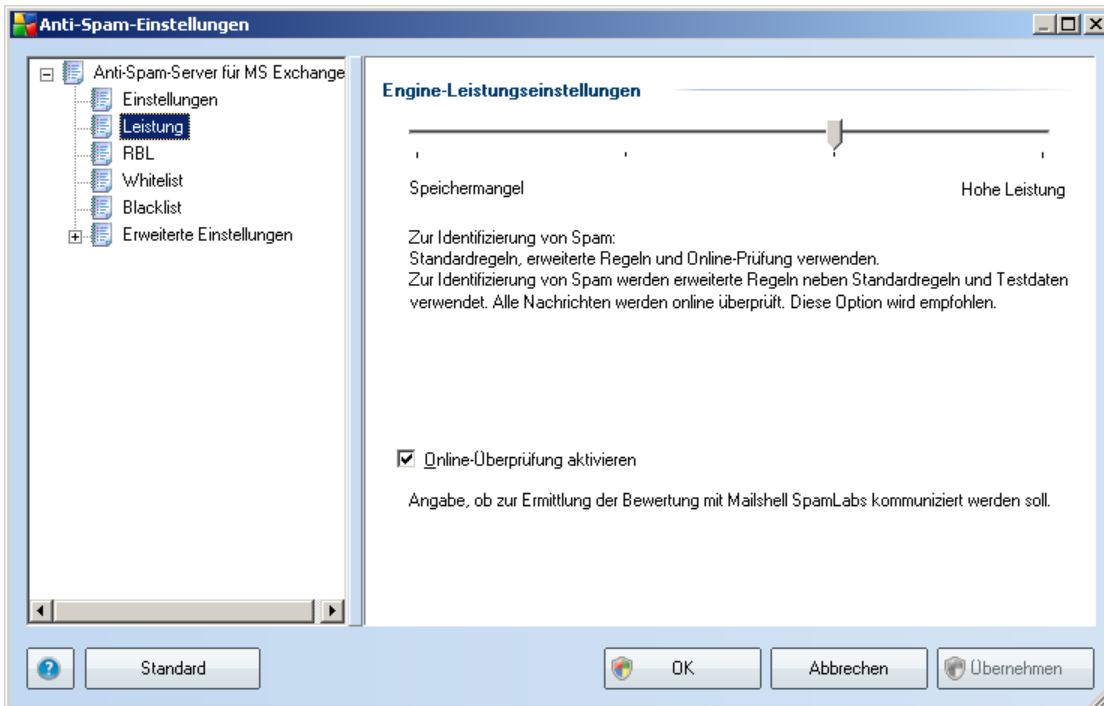
Wenn Sie sich angesichts der im Ordner enthaltenen Nachrichten nicht sicher sind, kann Sie der Assistent bei jeder einzelnen Nachricht fragen (so können Sie entscheiden, welche Nachrichten zu Übungszwecken verwendet werden sollen und welche nicht) – wählen Sie hierzu die Option **Bei jeder Nachricht fragen**.

Genauere Filtereinstellungen können Sie vornehmen, wenn Sie die Option **Filter verwenden** auswählen. Sie können ein Wort (*Name*), ein Teil eines Wortes oder eine Phrase eingeben, um im Betreff bzw. im Absenderfeld der eMail danach zu suchen. Alle Nachrichten, die den eingegebenen Kriterien genau entsprechen, werden ohne weitere Nachfrage für das Training verwendet.

Achtung! Wenn Sie beide Textfelder ausfüllen, werden auch Adressen verwendet, die lediglich eines der Kriterien erfüllen!

Nachdem Sie die gewünschte Option gewählt haben, klicken Sie auf **Weiter**. Im folgenden Dialog wird Ihnen lediglich mitgeteilt, dass der Assistent zur Bearbeitung der Nachrichten bereit ist. Um das Training zu starten, klicken Sie erneut auf die Schaltfläche **Weiter**. Das Training wird nun den zuvor ausgewählten Bedingungen entsprechend gestartet.

8.4. Leistung



Der Dialog **Engine-Leistungseinstellungen** (zu öffnen über das Element **Leistung** im linken Navigationsbereich) enthält Leistungseinstellungen für die Komponente **Anti-Spam**. Bewegen Sie den Schieberegler nach links oder rechts, um die Scan-Leistung zwischen den Modi **Speichermangel** / **Hohe Leistung** einzustellen.

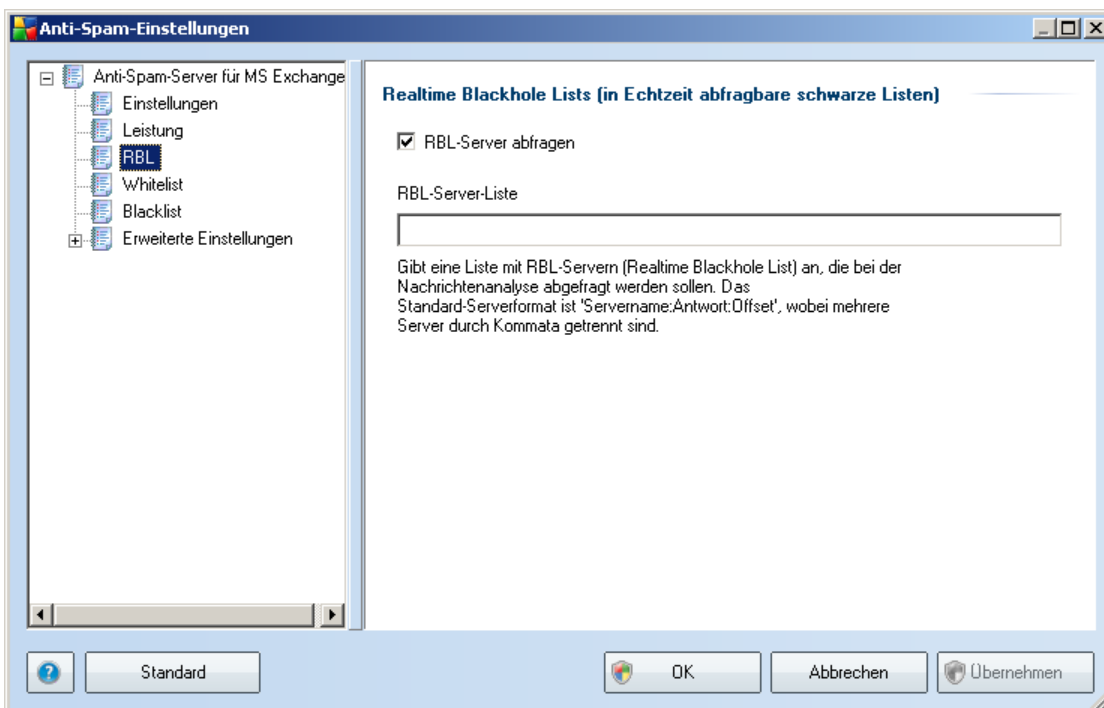
- **Speichermangel** – Beim Scanvorgang werden zur Identifizierung von [Spam](#) keine Regeln verwendet. Zur Identifizierung werden nur Testdaten verwendet. Dieser Modus ist nicht für den allgemeinen Gebrauch empfohlen, es sei denn, die Computer-Hardware ist wirklich sehr langsam.
- **Hohe Leistung** – Für diesen Modus ist sehr viel Speicher erforderlich. Während des Scanvorgangs werden zur Identifizierung von [Spam](#) folgende Funktionen verwendet: Regeln und [Spam](#)-Datenbank-Cache, einfache und erweiterte Regeln, IP-Adressen von Spammern und Spammer-Datenbanken.

Die Option **Online-Überprüfung aktivieren** ist standardmäßig aktiviert. Auf diese Weise wird eine genauere Erkennung von [Spam](#) durch Kommunikation mit den [Mailshell](#)-Servern ermöglicht (z. B. werden die gescannten Daten online mit den [Mailshell](#)-Datenbanken verglichen).

Grundsätzlich wird empfohlen, die Standardeinstellungen beizubehalten und nur dann zu ändern, wenn ein triftiger Grund vorliegt. Änderungen an dieser Konfiguration sollten nur von erfahrenen Benutzern durchgeführt werden!

8.5. RBL

Der Eintrag **RBL** öffnet den Bearbeitungsdialog **Realtime Blackhole List (in Echtzeit abfragbare schwarze Listen)**:



In diesem Dialog können Sie die Funktion **RBL-Server abfragen** aktivieren und deaktivieren.

Der RBL-Server (*Realtime Blackhole Lists (in Echtzeit abfragbare schwarze Listen)*) ist ein DNS-Server mit einer umfangreichen Datenbank bekannter Spam-Sender. Bei Aktivierung dieser Funktion werden alle eMails mit den Adressen der RBL-Serverdatenbank verglichen und als [Spam](#) markiert, wenn Sie einem Datenbankeintrag entsprechen.

Die RBL-Serverdatenbanken enthalten die allerneuesten Spam-Fingerabdrücke und ermöglichen so die beste und exakteste [Spam](#)-Erkennung. Diese Funktion ist besonders nützlich für Benutzer, die sehr viel Spam empfangen, der normalerweise

nicht vom Anti-Spam-Modul erkannt wird.

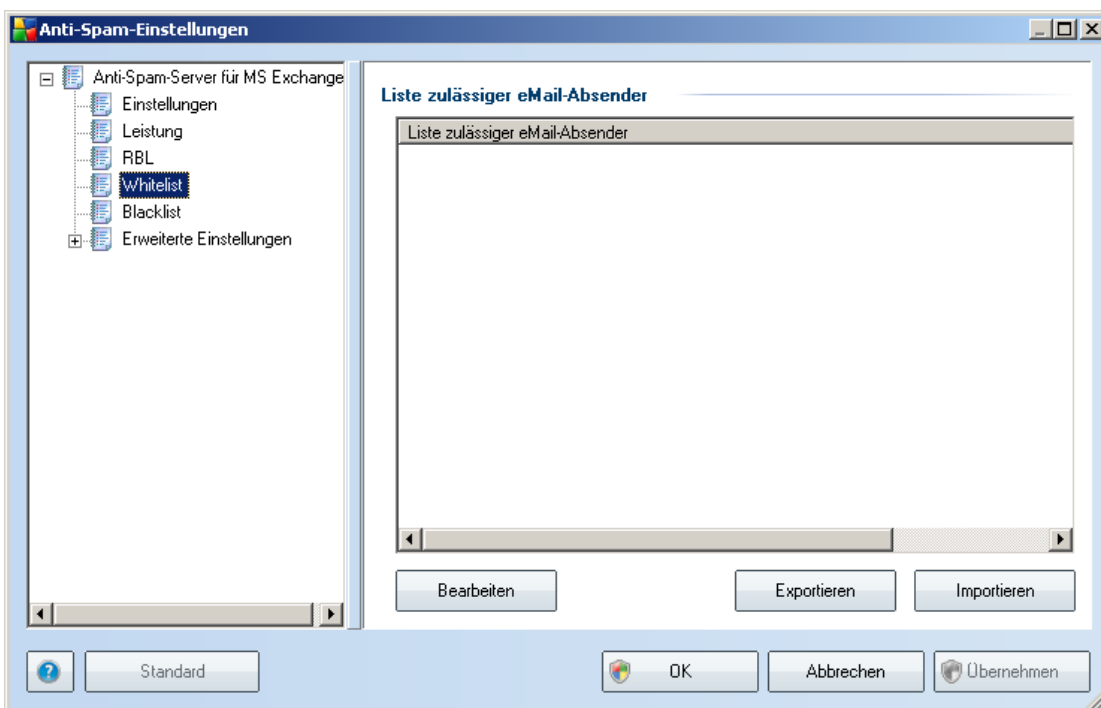
Über die **RBL-Server-Liste** können Sie spezielle RBL-Serverstandorte festlegen. Standardmäßig sind zwei RBL-Serveradressen festgelegt. Wir empfehlen, die Standardeinstellungen beizubehalten, sofern Sie kein erfahrener Benutzer sind und diese Einstellungen wirklich ändern müssen!

Hinweis: Wenn Sie diese Funktion aktivieren, kann das den Empfang von eMails auf einigen Systemen und unter einigen Konfigurationen verlangsamen, da jede einzelne Nachricht mit der RBL-Serverdatenbank abgeglichen werden muss.

Es werden keine persönlichen Daten an den Server gesendet!

8.6. Whitelist

Wenn Sie das Objekt **Whitelist** auswählen, wird ein Dialog mit einer allgemeinen Liste genehmigter eMail-Absenderadressen und Domainnamen angezeigt, deren Nachrichten nie als [Spam](#) markiert werden.



In der Bearbeitungsoberfläche können Sie eine Liste mit Absendern erstellen, bei denen Sie sicher sind, dass sie Ihnen nie unerwünschte Nachrichten ([Spam](#)) senden

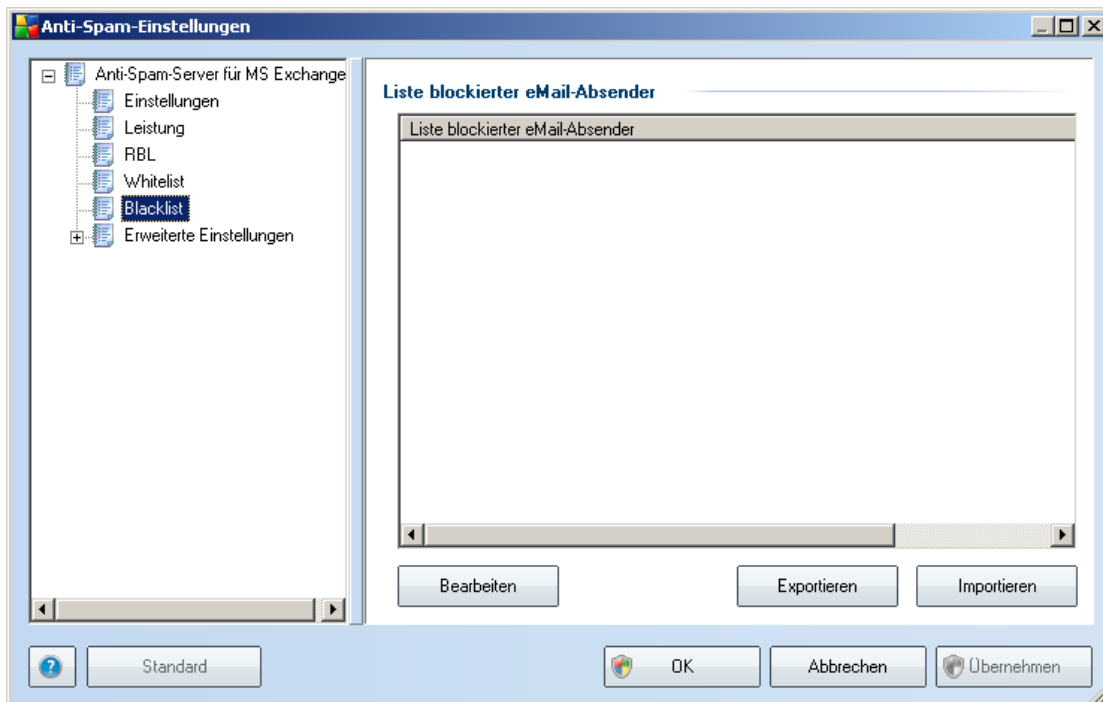
werden. Sie können außerdem eine Liste mit vollständigen Domainnamen (z. B. *avg.com*) erstellen, bei denen Sie wissen, dass sie keine Spam-Nachrichten erstellen.

Sobald Sie eine solche Liste von Absendern und/oder Domainnamen vorbereitet haben, können Sie die Adressen entweder direkt einzeln in die Liste eingeben oder die gesamte Liste in einem Schritt importieren. Folgende Schaltflächen sind verfügbar:

- **Bearbeiten** – Klicken Sie auf diese Schaltfläche, um einen Dialog zu öffnen, in dem Sie eine Liste von Adressen manuell eingeben können (Sie können die Adressen auch *kopieren und einfügen*). Geben Sie jeweils einen Eintrag (Absender, Domainname) pro Zeile ein.
- **Importieren** – Wenn Sie bereits eine Textdatei mit eMail-Adressen/ Domainnamen vorbereitet haben, können Sie sie einfach über diese Schaltfläche importieren. Die Eingabedatei muss in reinem Textformat vorliegen und der Inhalt darf jeweils nur ein Element (Adresse, Domainname) pro Zeile enthalten.
- **Exportieren** – Wenn Sie die Datensätze exportieren möchten, klicken Sie auf diese Schaltfläche. Alle Datensätze werden in einer reinen Textdatei gespeichert.

8.7. Blacklist

Wenn Sie den Eintrag **Blacklist** auswählen, wird ein Dialog mit einer allgemeinen Liste blockierter eMail-Absenderadressen und Domainnamen angezeigt, deren Nachrichten immer als [Spam](#) markiert werden.



In der Bearbeitungsoberfläche können Sie eine Liste mit Absendern erstellen, von denen Sie unerwünschte Nachrichten ([Spam](#)) erwarten. Sie können außerdem eine Liste mit vollständigen Domainnamen (z. B. *spammingunternehmen.com*) erstellen, von denen Sie Spam-Nachrichten erwarten oder erhalten. Sämtliche eMail-Nachrichten der aufgelisteten Adressen und Domains werden als Spam identifiziert.

Sobald Sie eine solche Liste von Absendern und/oder Domainnamen vorbereitet haben, können Sie die Adressen entweder direkt einzeln in die Liste eingeben oder die gesamte Liste in einem Schritt importieren. Folgende Schaltflächen sind verfügbar:

- **Bearbeiten** – Klicken Sie auf diese Schaltfläche, um einen Dialog zu öffnen, in dem Sie eine Liste von Adressen manuell eingeben können (Sie können die Adressen auch *kopieren und einfügen*). Geben Sie jeweils einen Eintrag (Absender, Domainname) pro Zeile ein.
- **Importieren** – Wenn Sie bereits eine Textdatei mit eMail-Adressen/ Domainnamen vorbereitet haben, können Sie sie einfach über diese Schaltfläche importieren. Die Eingabedatei muss in reinem Textformat vorliegen und der Inhalt darf jeweils nur ein Element (Adresse, Domainname) pro Zeile enthalten.
- **Exportieren** – Wenn Sie die Datensätze exportieren möchten, klicken Sie auf diese Schaltfläche. Alle Datensätze werden in einer reinen Textdatei

gespeichert.

8.8. Erweiterte Einstellungen

Grundsätzlich wird empfohlen, die Standardeinstellungen beizubehalten und nur dann zu ändern, wenn ein triftiger Grund vorliegt.

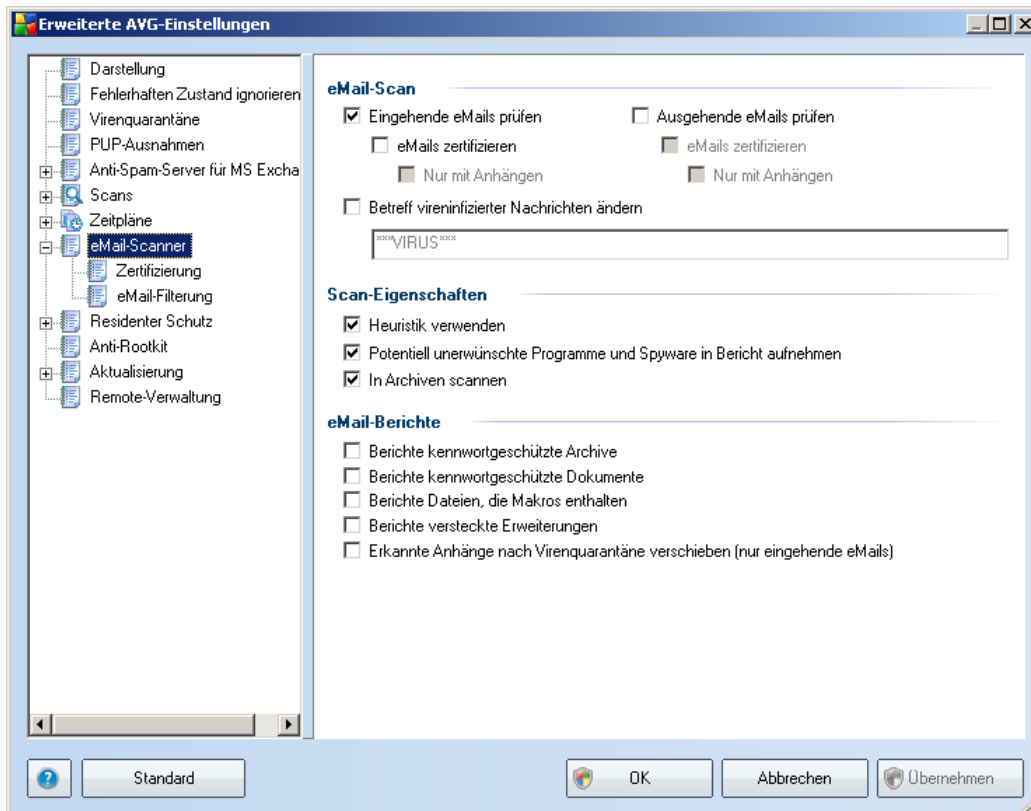
Konfigurationsänderungen sollten nur von erfahrenen Benutzern durchgeführt werden!

Wenn Sie dennoch der Meinung sind, dass Sie die Konfiguration von Anti-Spam im Detail ändern müssen, folgen Sie den Anweisungen direkt in der Benutzeroberfläche. Im Allgemeinen finden Sie in jedem Dialog eine bestimmte Funktion, die Sie bearbeiten können, sowie die zugehörige Beschreibung:

- **Cache** – Fingerabdruck, Domainprüfung, LegitRepute
- **Training** – Worttraining, Bewertungshistorie, Bewertungs-Offset, maximale Worteinträge, Schwellenwert für Autotraining, Gewicht, Schreibpuffer
- **Filtern** – Sprachenliste, Länderliste, genehmigte IPs, blockierte IPs, blockierte Länder, blockierte Zeichensätze, gefälschte Absender
- **RBL** – RBL-Server, Mehrfachtreffer, Schwellenwert, Timeout, maximale IPs
- **Internetverbindung** – Timeout, Proxyserver, Proxyserverauthentifizierung

9. eMail-Scanner

Die Einstellungen des **eMail-Scanners** werden innerhalb der AVG eMail Server Edition konfiguriert. Wählen Sie im Hauptmenü der Anwendung **Tools/Erweiterte Einstellungen** aus. Wählen Sie anschließend im linken Menü des Dialogs **Erweiterte Einstellungen** die Option **eMail-Scanner** aus.



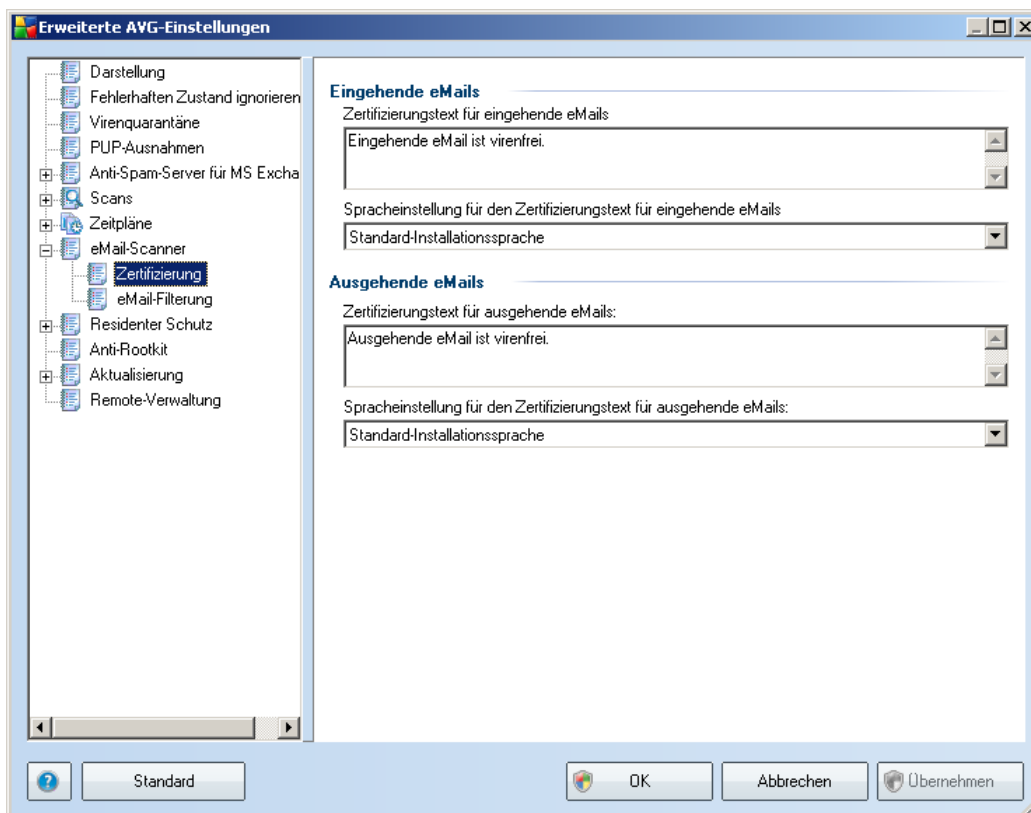
Der Dialog **eMail-Scanner** ist in drei Bereiche unterteilt:

- **eMail-Scan** – In diesem Bereich können Sie auswählen, ob eingehende/ ausgehende eMail-Nachrichten gescannt werden sollen und ob alle eMails oder nur eMails mit Anhang zertifiziert werden sollen (*die Zertifizierung von eMails als virenfrei wird im Format HTML/RTF nicht unterstützt*). Zusätzlich können Sie auswählen, ob AVG den Betreff für Nachrichten, die potentielle Viren enthalten, ändern soll. Markieren Sie das Kontrollkästchen **Betreff vireninfizierter Nachrichten ändern** und ändern Sie den Text nach Bedarf (*voreingestellt ist: ***VIRUS****).
- **Scan-Eigenschaften** – Geben Sie an, ob beim Scannen die heuristische

Analyse verwendet werden soll (**Heuristik verwenden**), ob nach potentiell unerwünschten Programmen (**Potentiell unerwünschte Programme und Spyware scannen**) gesucht werden soll und ob auch Archive gescannt werden sollen (**In Archiven scannen**).

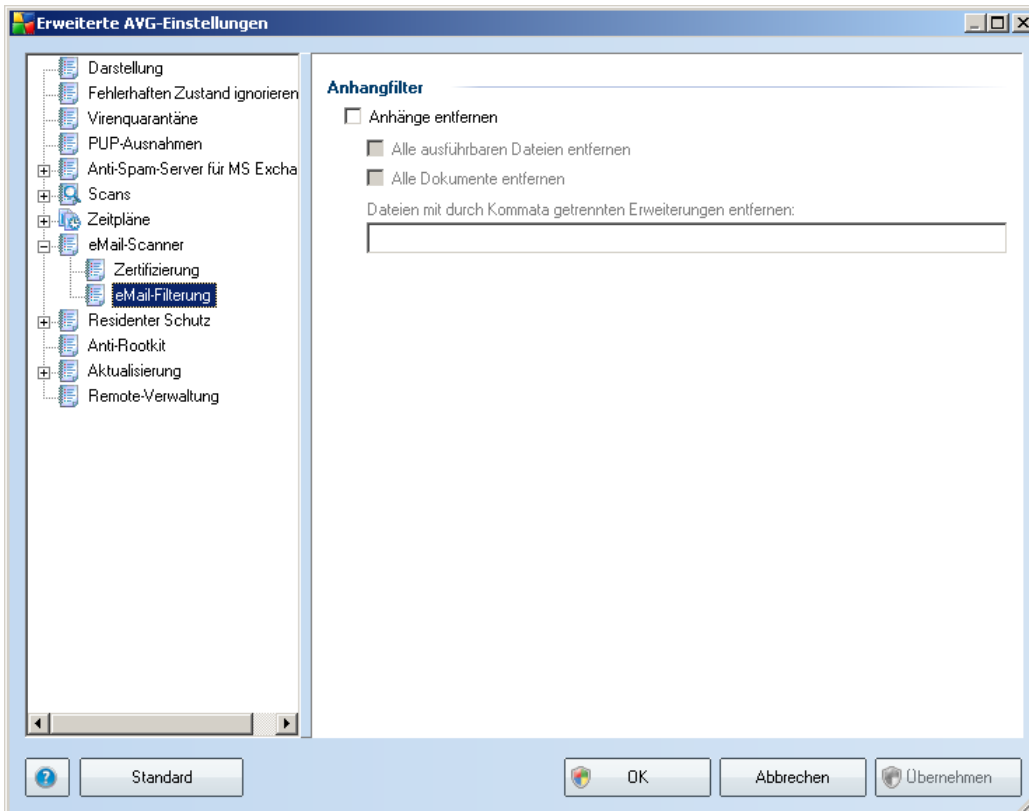
- **eMail-Berichte** – Geben Sie an, ob Sie per eMail über kennwortgeschützte Archive, kennwortgeschützte Dokumente, Dateien mit Makros und/oder Dateien mit versteckter Erweiterung benachrichtigt werden möchten, die als Anhang der gescannten eMail-Nachricht erkannt wurden. Wird eine solche Nachricht während des Scans identifiziert, geben Sie an, ob das erkannte infektiöse Objekt in die **Virenquarantäne** verschoben werden soll.

9.1. Zertifizierung



Im Dialog **Zertifizierung** können Sie genau angeben, welchen Text der Zertifizierungshinweis enthalten soll und in welcher Sprache er angezeigt werden soll. Definieren Sie einen separaten Text für **eingehende eMails** und **ausgehende eMails**.

9.2. eMail-Filterung



Im Dialog **Anhangfilter** können Sie Parameter für das Scannen von eMail-Anhängen festlegen. Standardmäßig ist die Option **Anhänge entfernen** deaktiviert. Wenn Sie die Option aktivieren, werden alle eMail-Anhänge, die als infektiös oder potentiell gefährlich erkannt werden, automatisch entfernt. Wenn Sie möchten, dass nur bestimmte Arten von Anhängen entfernt werden, wählen Sie die entsprechende Option aus:

- **Alle ausführbaren Dateien entfernen** – Alle Dateien des Typs *.exe werden gelöscht
- **Alle Dokumente entfernen** – Alle Dateien des Typs *.doc werden gelöscht
- **Dateien mit durch Kommata getrennten Erweiterungen entfernen** – Alle Dateien mit den definierten Erweiterungen werden entfernt

10. FAQ und technischer Support

Wenn bei der Installation oder Verwendung von AVG betriebliche oder technische Probleme auftreten, finden Sie im Bereich **FAQ** der AVG-Website unter www.avg.com hilfreiche Informationen.

Falls Sie auf diese Weise keine Lösung für Ihr Problem finden, wenden Sie sich bitte per eMail an den technischen Support. Verwenden Sie bitte das Kontaktformular, das im Systemmenü unter **Hilfe/Onlinehilfe** zur Verfügung steht.