



AVG Email Server Edition 2012

Gebruikershandleiding

Documentrevisie 2012.04 (1/4/2012)

Copyright AVG Technologies CZ, s.r.o. Alle rechten voorbehouden.
Alle overige handelsmerken zijn het eigendom van de respectieve eigenaren.

Dit product maakt gebruik van RSA Data Security, Inc. MD5 Message-Digest-algoritme, Copyright (C) 1991-2, RSA Data Security, Inc. Opgericht in 1991.

Dit product gebruikt code van de C-SaCzech bibliotheek, Copyright © 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).

Dit product gebruikt compressiebibliotheek zlib, copyright (c) 1995-2002 Jean-loup Gailly en Mark Adler.



Inhoud

1. Inleiding	4
2. AVG-installatievereisten	5
2.1 Ondersteunde besturingssystemen	5
2.2 Ondersteunde e-mailserveren	5
2.3 Hardwarevereisten	5
2.4 Vorige versies verwijderen	5
2.5 MS Exchange Service Packs	6
3. AVG installatieprocedure	7
3.1 Start van installatie	7
3.2 Uw licentie activeren	8
3.3 Installatietype selecteren	9
3.4 Aangepaste installatie - aangepaste opties	10
3.5 Voltooien installatie	11
4. E-mailscanner voor MS Exchange Server 2007/2010	13
4.1 Overzicht	13
4.2 E-mailscanner voor MS Exchange (routing TA)	16
4.3 E-mailscanner voor MS Exchange (SMTP TA)	17
4.4 E-mailscanner voor MS Exchange (VSAPI)	18
4.5 Technische kennisgeving	20
4.6 Detectiebewerkingen	21
4.7 Mailfiltering	22
5. E-mailscanner voor MS Exchange Server 2003	24
5.1 Overzicht	24
5.2 E-mailscanner voor MS Exchange (VSAPI)	27
5.3 Detectiebewerkingen	30
5.4 Mailfiltering	31
6. AVG for Kerio MailServer	32
6.1 Configuratie	32
6.1.1 Antivirus	32
6.1.2 Bijlagefilter	32
7. Anti-Spamconfiguratie	37



7.1 Antispaminterface	37
7.2 Antispam principes	39
7.3 Anti-Spaminstellingen	39
7.3.1 De wizard Antispamtraining	39
7.3.2 Selecteer de map met berichten	39
7.3.3 Opties voor het filteren van berichten	39
7.4 Prestaties	44
7.5 RBL	45
7.6 Witte lijst	46
7.7 Zwarte lijst	47
7.8 Expertinstellingen	48
8. AVG Settings Manager	49
9. Veelgestelde vragen en technische ondersteuning	52



1. Inleiding

Deze gebruikershandleiding bevat uitgebreide informatie over **AVG Email Server Edition 2012**.

Gefeliciteerd met uw aankoop van AVG Email Server Edition 2012!

AVG Email Server Edition 2012 is één van een reeks onderscheiden AVG-producten die zijn ontwikkeld om uw gemoedsrust te bevorderen en uw server volledig te beschermen. Net als alle andere AVG-producten is **AVG Email Server Edition 2012** volledig opnieuw vormgegeven, vanaf het fundament, om de bekende en geroemde beveiliging van AVG aan te kunnen bieden op een nieuwe, meer gebruiksvriendelijke en efficiëntere manier.

AVG is ontwikkeld om de omgeving waarin uw computer en netwerk moeten functioneren, te beschermen. Geniet van de volledige bescherming van AVG.

Opmerking: in dit document staan beschrijvingen van specifieke functies van de *E-mail Server Edition*. Als u informatie nodig hebt over andere functies van AVG, raadpleegt u de gebruikershandleiding bij de *Internet Security Edition*; daar staan alle details in. U kunt die handleiding downloaden van <http://www.avg.com>.



2. AVG-installatievereisten

2.1. Ondersteunde besturingssystemen

AVG Email Server Edition 2012 is ontworpen om e-mailserver met de volgende besturingssystemen te beschermen:

- Windows 2008 Server Edition (x86 en x64)
- Windows 2003 Server (x86, x64) SP1

2.2. Ondersteunde e-mailserver

De volgende e-mailserver worden ondersteund

- MS Exchange 2003 Server-versie
- MS Exchange 2007 Server-versie
- MS Exchange 2010 Server-versie
- AVG for Kerio MailServer – versie 6.7.2 en hoger

2.3. Hardwarevereisten

De minimale hardwarevereisten voor **AVG Email Server Edition 2012** zijn:

- Intel Pentium-processor 1,5 GHz
- 500 MB vrije schijfruimte (voor de installatie)
- 512 MB RAM-geheugen

Aanbevolen hardwarevereisten voor **AVG Email Server Edition 2012** zijn:

- Intel Pentium-processor 1,8 GHz
- 600 MB vrije schijfruimte (voor de installatie)
- 512 MB RAM-geheugen

2.4. Vorige versies verwijderen

Als er een oudere versie van AVG Email Server is geïnstalleerd, zult u die installatie handmatig ongedaan moeten maken, voordat u **AVG Email Server Edition 2012** installeert. U dient die oudere versie handmatig te verwijderen met de standaardfunctionaliteit van Windows.

- Kies **Start/Instellingen/Configuratiescherm/Programma's toevoegen of verwijderen** en



selecteer het programma in de lijst met geïnstalleerde software. Controleer of u het juiste programma van AVG selecteert om te verwijderen. U moet de Email Server Edition verwijderen voordat u de AVG File Server Edition verwijdert.

- Als u de Email Server Edition hebt verwijderd, kunt u de AVG File Server Edition verwijderen. Dat kan via **Start/Alle programma's/AVG/Installatie van AVG ongedaan maken**
- Als de oudere versie AVG 8.x of ouder was, maak dan ook de installatie van serverinvoegtoepassingen ongedaan.

Opmerking: tijdens het ongedaan maken van de installatie zal de store-service opnieuw moeten worden opgestart.

Exchange-invoegtoepassing – voer setupes.exe uit met de parameter /uninstall vanuit de map waar de invoegtoepassing is geïnstalleerd.

Bijv. C:\AVG4ES2K\setupes.exe /uninstall

Lotus Domino/Notes-invoegtoepassing – voer setupln.exe uit met de parameter /uninstall vanuit de map waar de invoegtoepassing is geïnstalleerd.

Bijv. C:\AVG4LN\setupln.exe /uninstall

2.5. MS Exchange Service Packs

Voor Exchange 2003 Server is geen aanvullend service pack vereist. Het wordt echter wel aanbevolen om uw systeem zo up-to-date mogelijk te houden met behulp van de nieuwste service packs en hotfixes voor een maximale veiligheid.

Service Pack voor MS Exchange 2003 Server (optioneel):

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

Aan het begin van de installatie worden de versies van alle systeembibliotheken onderzocht. Als blijkt dat er nieuwe bibliotheken moeten worden geïnstalleerd, worden de oude bibliotheken door het installatieprogramma aangevuld met de extensie .delete. Deze bestanden worden verwijderd nadat het systeem opnieuw is opgestart.

Service Pack voor MS Exchange 2007 Server (optioneel):

<http://www.microsoft.com/downloads/details.aspx?FamilyID=44c66ad6-f185-4a1d-a9ab-473c1188954c&displaylang=en>



3. AVG installatieprocedure

Voor installatie van AVG op uw computer dient u te beschikken over het nieuwste installatiebestand. U kunt het installatiebestand gebruiken dat op de cd staat die onderdeel uitmaakt van de editie in de doos, maar dat bestand kan verouderd zijn. We raden u daarom aan het nieuwste installatiebestand online op te vragen. U kunt het bestand downloaden van de [website van AVG \(http://www.avg.com/download?prd=msw\)](http://www.avg.com/download?prd=msw)

Opmerking: er zijn twee installatiepakketten voor uw product – voor de 32-bits versie van het besturingssysteem (aangeduid met x86) en voor de 64-bits versie van het besturingssysteem (aangeduid met x64). Download de versie die compatibel is met uw besturingssysteem..

Tijdens het installatieproces wordt naar uw licentienummer gevraagd. Zorg ervoor dat u het bij de hand hebt voordat u met de installatie begint. Het nummer staat op de cd-hoes. Als u uw exemplaar van AVG online hebt aangeschaft, hebt u het licentienummer per e-mail ontvangen.

Als u het installatiebestand hebt gedownload en opgeslagen op uw vaste schijf, kunt u de installatieprocedure starten. De installatieprocedure bestaat uit een reeks dialoogvensters met steeds een korte beschrijving bij elke stap. Hieronder volgt een toelichting op de dialoogvensters:

3.1. Start van installatie



Bij de start van de installatieprocedure wordt het venster **Welkom** weergegeven. In dit venster selecteert u de taal voor installatie en geeft u aan dat u de gebruiksvoorwaarden accepteert. Klik op de knop **Printversie** om de licentieovereenkomst in een nieuw venster te openen. Klik op de knop **Accepteren** om uw instemming te betuigen en verder te gaan naar het volgende dialoogvenster.

Let op: in een later stadium van de installatieprocedure kunt u extra talen selecteren voor uitvoering van de toepassing na installatie.



3.2. Uw licentie activeren

In het dialoogvenster **Licentie activeren** vult u uw licentienummer in.

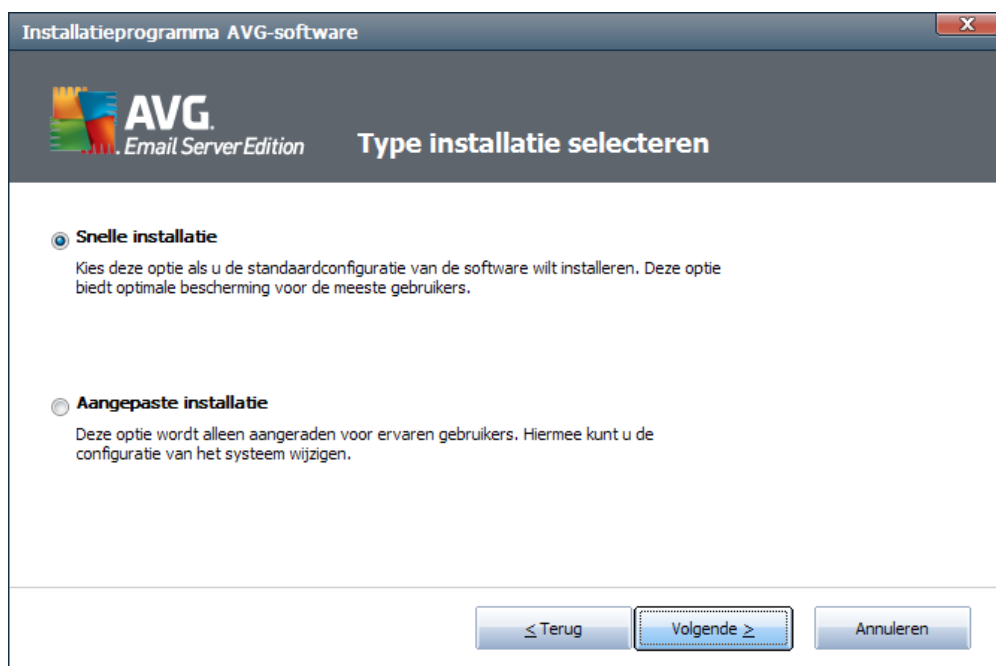
Voer het licentienummer in in het vak **Licentienummer**. Het licentienummer staat in de bevestiging die u via e-mail hebt ontvangen na aankoop van AVG online. U moet dat nummer precies zo typen als het wordt weergegeven. Als u beschikt over de digitale versie van het licentienummer (in de e-mail), is het raadzaam het nummer over te nemen met kopiëren-en-plakken.



Klik op de knop **Volgende** om verder te gaan met de installatieprocedure.



3.3. Installatietype selecteren



In het dialoogvenster **Installatietype selecteren** kunt u kiezen uit twee soorten installaties: **Snelle installatie** en **Aangepaste installatie**.

We raden de meeste gebruikers aan de **Snelle installatie** te gebruiken, waarbij AVG in een automatische modus wordt geïnstalleerd met vooraf door de leverancier ingestelde instellingen. Die configuratie combineert maximale bescherming met een efficiënt gebruik van o.a. werkgeheugen. Als het in de toekomst nodig mocht blijken om de configuratie aan te passen, kunt u dat altijd vanuit de AVG toepassing doen.

Een aangepaste installatie is alleen aanbevolen voor ervaren gebruikers die een goede reden hebben om AVG te installeren met afwijkende instellingen, bijvoorbeeld om te voldoen aan specifieke systeemvereisten.

3.4. Aangepaste installatie - aangepaste opties



In het dialoogvenster **Doelmap** kunt u opgeven in welke map AVG moet worden geïnstalleerd. Standaard wordt AVG geïnstalleerd in de map Program Files op station C:. Als u de voorkeur geeft aan een andere locatie, klikt u op de knop **Bladeren** om de mapstructuur weer te geven, en selecteert u de map van uw keuze.

In het dialoogvenster **Onderdelen selecteren** staat een overzicht van alle AVG onderdelen die kunnen worden geïnstalleerd. Als de standaardinstellingen niet voldoen, kunt u onderdelen toevoegen of verwijderen.

U kunt echter alleen kiezen uit onderdelen die deel uitmaken van de door u gekochte AVG Edition. Alleen die onderdelen worden voor installatie weergegeven in het dialoogvenster Onderdelen selecteren!

- **AVG Remote Admin Client** – selecteer deze optie als u van plan bent om AVG te koppelen aan een AVG-DataCenter (AVG Netwerkedities).

Opmerking: *alleen servercomponenten die in de lijst staan kunnen extern worden beheerd!*

- **Settings Manager**– een hulpprogramma waarmee netwerkbeheerders AVG-configuraties kunnen kopiëren, bewerken en distribueren. De configuratie kan worden opgeslagen op een verwisselbaar medium (USB-stick, e.d.) en vervolgens handmatig of op een willekeurige andere manier worden toegepast op geselecteerde stations.
- **Extra geïnstalleerde talen** – u kunt ook opgeven in welke taal (talen) AVG moet worden geïnstalleerd. Schakel het selectievakje **Extra geïnstalleerde talen** in en selecteer daarna de gewenste talen in het menu.

Basisoverzicht van de afzonderlijke servercomponenten (**Serverinvoegtoepassingen**):



- **Anti-Spamserver voor MS Exchange**

controleert alle binnenkomende e-mailberichten en markeert ongewenste e-mails als SPAM. Het onderdeel maakt gebruik van verschillende analysemethoden om elk e-mailbericht te verwerken. Dit biedt de best mogelijke bescherming tegen ongewenste e-mailberichten.

- **E-mail Scanner for MS Exchange (routing Transport Agent)**

controleert alle binnenkomende, uitgaande en interne e-mailberichten die de MS Exchange HUB passeren.

Beschikbaar voor MS Exchange 2007/2010; kan alleen voor de HUB-functie worden geïnstalleerd.

- **E-mail Scanner for MS Exchange (SMTP Transport Agent)**

controleert alle e-mailberichten die de SMTP-interface van MS Exchange passeren

Alleen beschikbaar voor MS Exchange 2007/2010; kan voor zowel de EDGE- als de HUB-functie worden geïnstalleerd.

- **E-mailscanner voor MS Exchange (VSAPI)**

controleert alle e-mailberichten die in de postbussen van gebruikers zijn opgeslagen. Als er virussen worden gedetecteerd, worden ze naar de Quarantaine verplaatst of volledig verwijderd.

Opmerking: er zijn verschillende opties voor verschillende versies van MS Exchange.

Klik op de knop **Volgende** om verder te gaan.

3.5. Voltooien installatie

Als u de module **Remote Administration Component** hebt geselecteerd bij het selecteren van modules, kunt u in het laatste dialoogvenster de verbindingstring definiëren voor de verbinding met het AVG DataCenter.



AVG is nu op uw computer geïnstalleerd en volledig functioneel. Het programma wordt volledig automatisch op de achtergrond uitgevoerd.

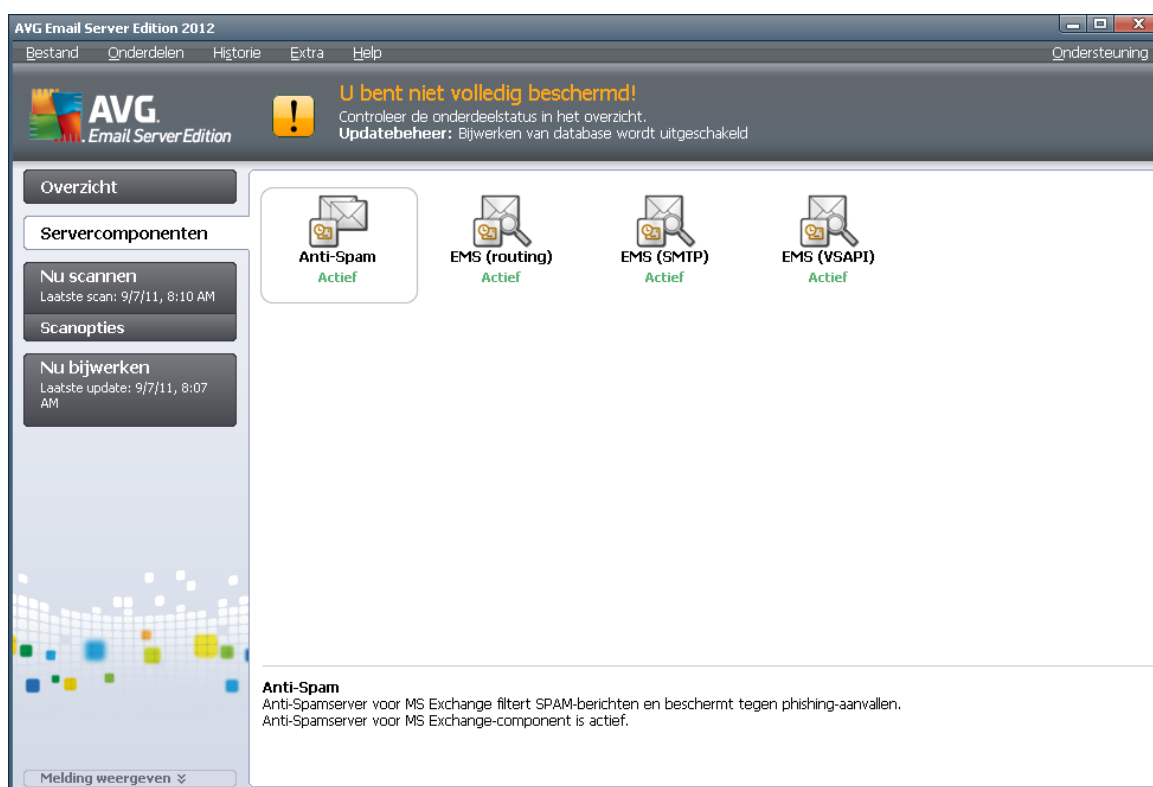
Ga naar het hoofdstuk dat van toepassing is voor instellen van bescherming voor de e-mailserver:

- [E-mailscanner voor MS Exchange Server 2007/2010](#)
- [E-mailscanner voor MS Exchange Server 2003](#)
- [AVG voor Kerio MailServer](#)

4. E-mailscanner voor MS Exchange Server 2007/2010

4.1. Overzicht

De configuratieopties voor AVG voor MS Exchange Server 2007/2010 zijn volledig geïntegreerd in AVG Email Server Edition 2012 in de vorm van servercomponenten.



Basisoverzicht van de afzonderlijke servercomponenten:

- [**Anti-spam – Anti-Spamserver voor MS Exchange**](#)
controleert alle binnenkomende e-mailberichten en markeert ongewenste e-mails als SPAM. Het onderdeel maakt gebruik van verschillende analysemethoden om elk e-mailbericht te verwerken. Dit biedt de best mogelijke bescherming tegen ongewenste e-mailberichten.
- [**EMS \(routing\) - E-mailscanner voor MS Exchange \(routing Transport Agent\)**](#)
controleert alle binnenkomende, uitgaande en interne e-mailberichten die de MS Exchange HUB passeren.

Beschikbaar voor MS Exchange 2007/2010; kan alleen voor de HUB-functie worden geïnstalleerd
- [**EMS \(SMTP\) – E-mailscanner voor MS Exchange \(SMTP Transport Agent\)**](#)



controleert al e-mailberichten die de SMTP-interface van MS Exchange passeren

Alleen beschikbaar voor MS Exchange 2007/2010; kan voor zowel de EDGE- als de HUB-functie worden geïnstalleerd.

- **[EMS \(VSAPI\) – E-mailscanner voor MS Exchange \(VSAPI\)](#)**

controleert alle e-mailberichten die in de postbussen van gebruikers zijn opgeslagen. Als er virussen worden gedetecteerd, worden ze naar de Quarantaine verplaatst of volledig verwijderd.

Belangrijke opmerking: Als u VSAPI hebt geïnstalleerd en gebruikt in combinatie met Routing Transport Agent in een Hub Exchange-functie, wordt de e-mail twee maal gescand. Lees om dat te voorkomen het hieronder volgende hoofdstuk [Technische kennisgeving](#) voor meer informatie.

Dubbelklik op een component om de interface te openen. Met uitzondering van Anti-spam hebben alle componenten de volgende knoppen en koppelingen:

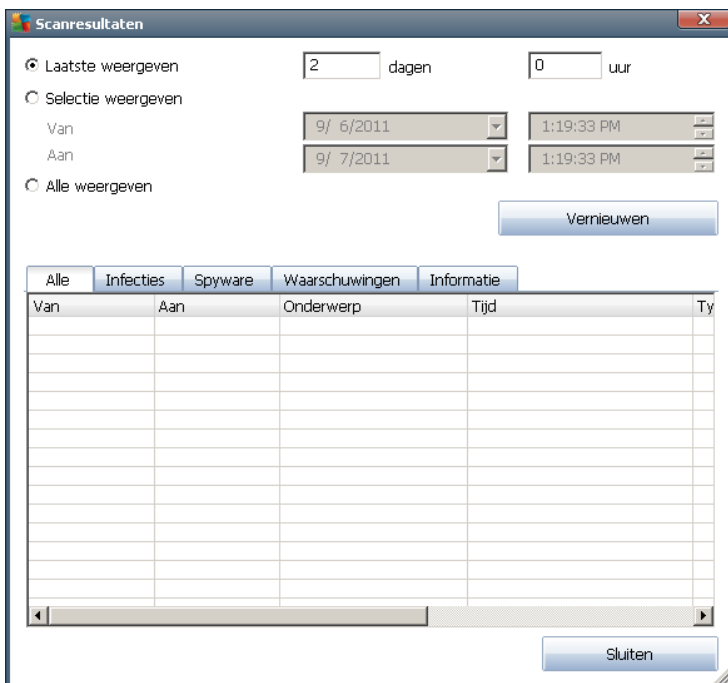
The screenshot shows the AVG Email Server Edition 2012 interface. At the top, there is a warning message: "U bent niet volledig beschermd! Controleer de onderdeelstatus in het overzicht. Updatebeheer: Bijwerken van database wordt uitgeschakeld." Below this, the main content area displays the status of the "Component E-mailscanner voor MS Exchange (VSAPI)". It is marked as "Actief" (Active) with a green checkmark. The interface shows the following statistics:

Sinds: 9/7/2011, 8:05 AM		
Gecontroleerde e-maildelen:	802	
Gedetecteerde bedreigingen:	0	
Gedetecteerde infecties:	0	Gedetecteerde PUP's: 0
Gedetecteerde waarschuwingen:	0	Gedetecteerde informatie: 0
Verplaatst naar de quarantaine:	0	
Verwijderd:	0	
Genegeerd:	0	

At the bottom of the component view, there are buttons for "Instellingen" (Settings) and "Terug" (Back). Links for "Scanresultaten", "Statistische waarden vernieuwen", and "Statische gegevens resetten" are also present.

- ***Scanresultaten***

Opent een nieuw dialoogvenster met scanresultaten:



Op tabbladen zijn berichten naar ernst gesorteerd. Zie de configuratie van afzonderlijke componenten voor het aanpassen van de ernst en rapportage.

Standaard worden alleen de resultaten van de laatste twee dagen weergegeven. U kunt met de volgende opties instellingen opgeven voor een andere periode:

- **Weergeven laatste** – weergave aan de hand van een opgegeven aantal dagen en uren.
- **Selectie weergeven** – weergave aan de hand van een opgegeven interval voor dagen en tijd.
- **Alles weergeven** – weergave van de resultaten van de hele periode.

Klik op de knop **Vernieuwen** om de resultaten opnieuw te laden.

- **Statistische waarden vernieuwen** – het bovengenoemde materiaal bijwerken.
- **Statistische waarden resetten** – alle cijfermateriaal terugzetten op nul.

Het dialoogvenster heeft de volgende knoppen:

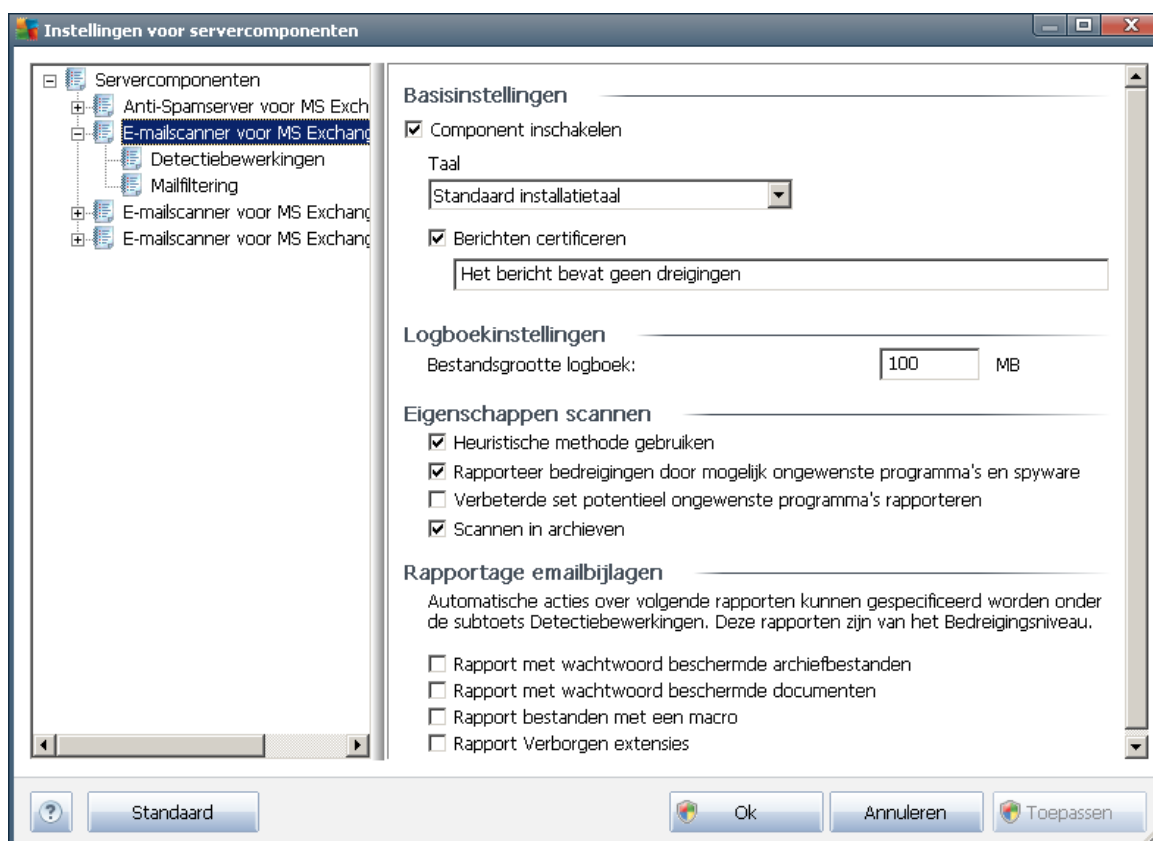
- **Instellingen** – de instellingen voor de component weergeven.
- **Terug** – klik op deze knop om terug te keren naar het Overzicht van Servercomponenten.

In de volgende hoofdstukken staat meer informatie over instellingen voor de afzonderlijke componenten.

4.2. E-mailscanner voor MS Exchange (routing TA)

Als u de instellingen van *E-mailscanner for MS Exchange (routing transport agent)* wilt openen, klikt u op de knop Instellingen in het venster van het onderdeel.

Selecteer in de lijst *Servercomponenten E-mailscanner for MS Exchange (routing TA)*:



In het **basisgedeelte** staan de volgende opties:

- **Onderdeel inschakelen** – schakel het selectievakje uit als u het onderdeel in zijn geheel wilt uitschakelen.
- **Taal** – selecteer de gewenste taal voor het onderdeel.
- **Berichten certificeren** – schakel het selectievakje in als u aan alle gescande berichten een certificeringsbericht wilt toevoegen. U kunt in het volgende veld een tekst opstellen voor het bericht.

Het gedeelte **Loginstellingen**:

- **Bestandsgrootte logboek** – geef op hoe groot het bestand voor het logboek mag zijn. Standaardwaarde: 100 MB.

Het gedeelte **Scaneigenschappen**:



- **Heuristische methode gebruiken** – schakel dit selectievakje in als u tijdens het scannen gebruik wilt maken van heuristische analyse.
- **Rapporteur bedreigingen door mogelijk ongewenste programma's en spyware** – al dan niet rapporteren van potentieel ongewenste programma's en spyware.
- **Uitgebreide set van mogelijk ongewenste programma's rapporteren** – schakel dit selectievakje in om uitgebreide pakketten van spyware te detecteren: programma's waar op zich niets aan mankeert als u ze direct van de fabrikant krijgt, maar die wel in een later stadium voor kwaadaardige praktijken kunnen worden misbruikt, of die nooit kwaadaardig zijn, maar wel hinderlijk (verschillende werkbalken, e.d.) Dit is een aanvullende maatregel ter bevordering van de veiligheid en het plezier van uw computer, al kunnen er ook legale programma's door worden geblokkeerd; om die reden is de functie standaard uitgeschakeld. Opmerking: deze detectiefunctie is een aanvulling op de vorige optie, dus als u beschermd wilt blijven tegen basistypen spyware, houdt u het vorige selectievakje ingeschakeld.
- **Scannen in archieven** – het scannen van archiefbestanden (zip, rar, enz.) in- en uitschakelen

In het gedeelte **Rapportage E-mailbijlagen** kunt u kiezen wat precies moet worden gerapporteerd tijdens het scannen. Als u het selectievakje inschakelt, wordt bij elk e-mailbericht met een dergelijke bijlage de tekst [INFORMATIE] toegevoegd aan de onderwerpsregel. Dat is de standaardconfiguratie die u kunt wijzigen in het gedeelte **Detectiebewerkingen**, bij **Informatie** (zie hieronder).

De volgende opties zijn beschikbaar:

- **Rapport met wachtwoord beschermde archieven**
- **Rapport met wachtwoord beschermde documenten**
- **Rapport bestanden met een macro**
- **Rapport verborgen extensies**

De volgende structuur heeft bovendien de volgende subitems:

- [Detectiebewerkingen](#)
- [Mailfiltering](#)

4.3. E-mailscanner voor MS Exchange (SMTP TA)

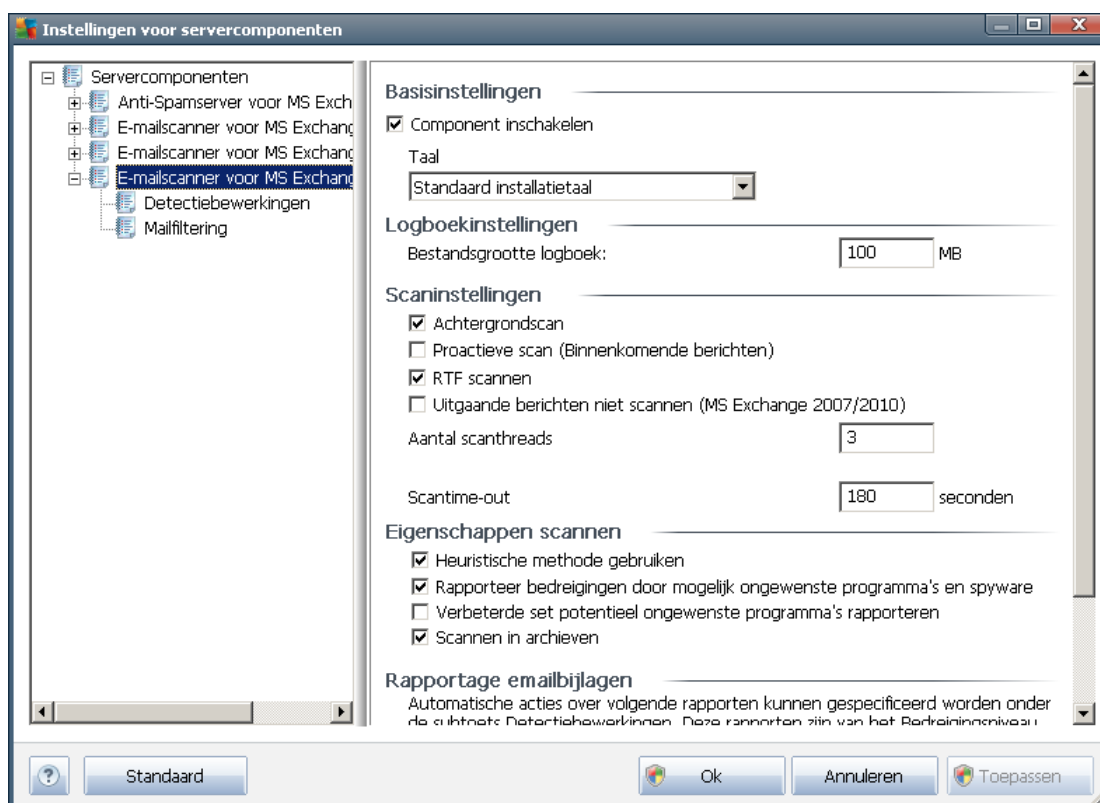
De configuratie voor **E-mail Scanner for MS Exchange (SMTP Transport Agent)** is identiek aan die van de routing transport agent. Zie voor meer informatie het hoofdstuk [E-mail Scanner for MS Exchange \(routing TA\)](#) hiervoor.

De volgende structuur heeft bovendien de volgende subitems:

- [Detectiebewerkingen](#)
- [Mailfiltering](#)

4.4. E-mailscanner voor MS Exchange (VSAPI)

Dit item betreft de instellingen voor *E-mail Scanner for MS Exchange (VSAPI)*



In het **basisgedeelte** staan de volgende opties:

- **Onderdeel inschakelen** – schakel het selectievakje uit als u het onderdeel in zijn geheel wilt uitschakelen.
- **Taal** – selecteer de gewenste taal voor het onderdeel.

Het gedeelte **Loginstellingen**:

- **Bestandsgrootte logboek** – geef op hoe groot het bestand voor het logboek mag zijn. Standaardwaarde: 100 MB.

Het gedeelte **Scaninstellingen**:

- **Achtergrondscan** – de scanfunctie op de achtergrond in- en uitschakelen. Scannen als achtergrondbewerking is een van de voorzieningen van de VSAPI 2.0/2.5-toepassingsinterface. Het biedt een via threading uitgevoerde scanvoorziening van de Exchange Messaging-databases. Telkens wanneer er een item wordt aangetroffen in de postvakmappen van de gebruiker dat nog niet is gescand met de nieuwste AVG-virusdatabase-update, wordt dit item voorgelegd aan AVG voor Exchange Server om te worden gescand. De scanbewerking en de zoekactie naar de nog niet onderzochte objecten worden parallel uitgevoerd.



Voor elke database wordt een speciale thread met een lage prioriteit gebruikt, wat ervoor zorgt dat andere taken (bijv. het opslaan van e-mailberichten in de database van Microsoft Exchange) altijd met voorrang worden uitgevoerd.

- **Proactieve scan (binnenkomende berichten)**

met dit selectievakje kunt u aangeven of de proactieve scanfunctie van VSAPI 2.0/2.5 moet worden in- of uitgeschakeld. Deze scan wordt uitgevoerd wanneer een item wordt afgeleverd bij een map zonder dat er een verzoek is gedaan door een client.

Zodra berichten worden aangeboden aan de opslag van Exchange, worden ze in de wachtrij voor de globale scan geplaatst met een lage prioriteit (maximaal 30 items). Ze worden gescand op basis van het FIFO-principe (First In, First Out). Als een item wordt geadresseerd terwijl het zich nog steeds in de wachtrij bevindt, krijgt het een hoge prioriteit.

Opmerking: *Overflow-berichten gaan ongescand naar de opslag.*

Opmerking: *zelfs als u zowel de **Achtergrondscan** als de **Proactieve scan** uitschakelt, zal de Scanner bij toegang nog steeds actief zijn als een gebruiker probeert een bericht te downloaden met de MS Outlook-client.*

- **RTF scannen** – met dit selectievakje kunt u aangeven of bestanden met de indeling RTF wel of niet moeten worden gescand.

- **Aantal scanthreads** – standaard is ingesteld dat het scanproces via meerdere threads verloopt om de algehele scanprestaties te verhogen met een bepaald niveau van parallelle verwerking. U kunt het aantal threads in dit veld aanpassen.

Het standaard aantal threads wordt als volgt berekend: 2 maal het 'aantal_processoren' + 1.

Het minimum aantal threads wordt als volgt berekend: ('aantal_processoren' + 1) gedeeld door 2.

Het maximum aantal threads wordt als volgt berekend: 'aantal_processoren' vermenigvuldigd met 5 + 1.

Als de waarde buiten de maximale of minimale waarden valt, wordt de standaardwaarde gebruikt.

- **Scantime-out** – dit veld geeft de maximale aaneengesloten periode (in seconden) weer gedurende welke een thread het bericht mag adresseren dat wordt gescand (de standaardwaarde is 180 seconden).

Het gedeelte **Scaneigenschappen**:

- **Heuristische methode gebruiken** – schakel dit selectievakje in als u tijdens het scannen gebruik wilt maken van heuristische analyse.
- **Rapporteer bedreigingen door mogelijk ongewenste programma's en spyware** – al dan niet rapporteren van potentieel ongewenste programma's en spyware.
- **Uitgebreide set van mogelijk ongewenste programma's rapporteren** – schakel dit selectievakje in om uitgebreide pakketten van spyware te detecteren: programma's waar op zich niets aan mankeert als u ze direct van de fabrikant krijgt, maar die wel in een later stadium voor kwaadaardige praktijken kunnen worden misbruikt, of die nooit kwaadaardig zijn, maar wel hinderlijk (verschillende werkbalken, e.d.) Dit is een aanvullende maatregel



ter bevordering van de veiligheid en het plezier van uw computer, al kunnen er ook legale programma's door worden geblokkeerd; om die reden is de functie standaard uitgeschakeld. Opmerking: deze detectiefunctie is een aanvulling op de vorige optie, dus als u beschermd wilt blijven tegen basistypen spyware, houdt u het vorige selectievakje ingeschakeld.

- **Scannen in archieven** – het scannen van archiefbestanden (zip, rar, enz.) in- en uitschakelen

In het gedeelte **Rapportage E-mailbijlagen** kunt u kiezen wat precies moet worden gerapporteerd tijdens het scannen. Dat is de standaardconfiguratie die u kunt wijzigen in het gedeelte **Detectiebewerkingen**, bij **Informatie** (zie hieronder).

De volgende opties zijn beschikbaar:

- **Rapport met wachtwoord beschermde archieven**
- **Rapport met wachtwoord beschermde documenten**
- **Rapport bestanden met een macro**
- **Rapport verborgen extensies**

De voorzieningen op dit tabblad zijn overwegend gebruikersextensies van de services van de Microsoft VSAPI 2.0/2.5-toepassingsinterface. Raadpleeg voor gedetailleerde informatie over de VSAPI 2.0/2.5 de volgende koppelingen (en ook de koppelingen die u vanuit deze koppelingen weer kunt volgen):

- <http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k> – informatie over de interactie tussen Exchange en antivirussoftware
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;823166> informatie over aanvullende functies van VSAPI 2.5 in de toepassing Exchange 2003 Server.

De volgende structuur heeft bovendien de volgende subitems:

- [Detectiebewerkingen](#)
- [Mailfiltering](#)

4.5. Technische kennisgeving

Deze informatie heeft betrekking op de situatie waarin u zowel VSAPI als Routing Transport Agent gebruikt in een Hub Exchange-functie. In dat geval worden e-mailberichten twee maal gescand (eerst door de VSAPI On-access scanner en dan door de Routing Transport Agent).

Door de manier waarop VSAPI werkt, kunnen de scanresultaten inconsistenties vertonen en is er bovendien een overbodige werkbelasting. We bevelen dan ook een kleine fix aan (zie hieronder) waarmee het probleem direct wordt opgelost.

Opmerking: wijzigen van het register wordt alleen aanbevolen aan ervaren gebruikers. Wij raden u aan om, voordat u het register bewerkt, een back-up te maken van het register en ervoor te zorgen dat u weet hoe u het register met behulp van de back-up kunt herstellen.



Open het register van Windows (menu **Start/Uitvoeren**, typ **regedit** en druk op Enter). Ga naar het volgende item:

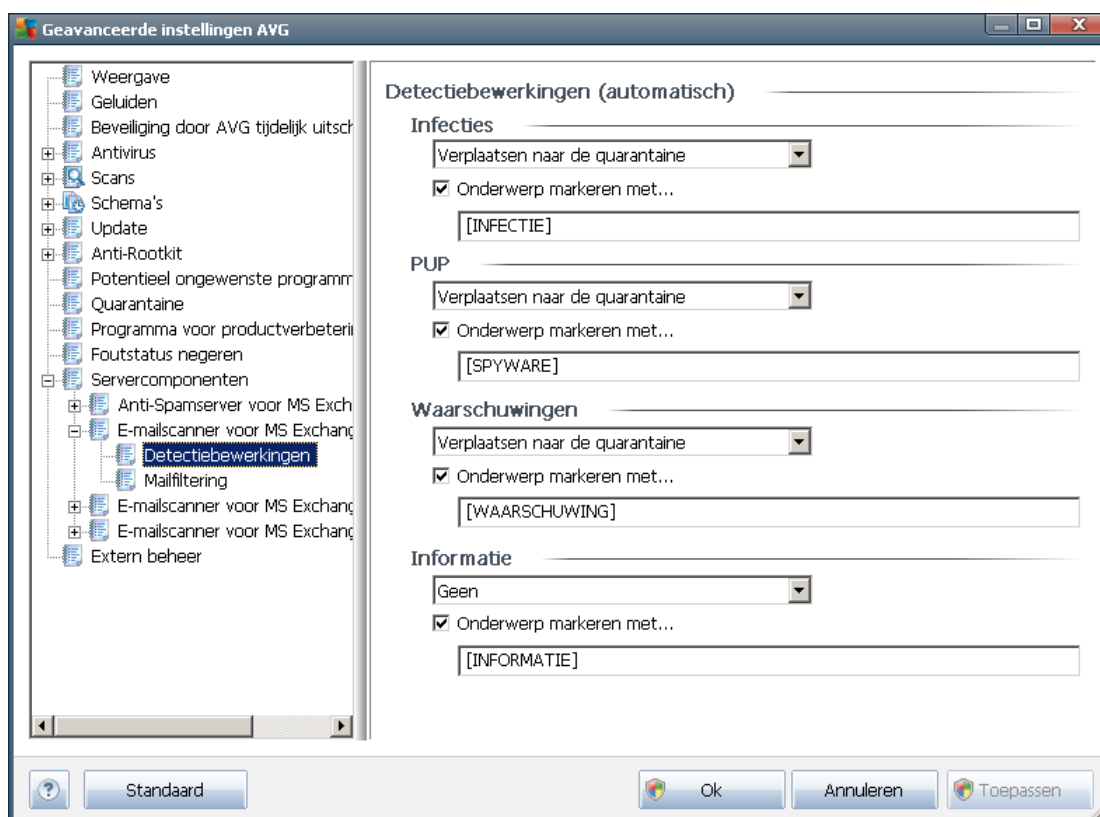
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchange\Scan

Klik met de rechtermuisknop in het rechterdeelvenster en selecteer in het snelmenu **Nieuw/DWORD (32-bits waarde)**. Noem de nieuwe waarde **TransportExclusion**. Dubbelklik op de nieuwe waarde en wijzig de waarde in **1**.

Stel de waarde **ReloadNow** in op 1 om de wijziging toe te passen op MS Exchange server. Dat kan door op de waarde te dubbelklikken en die te wijzigen in 1.

Hiermee schakelt u het scannen van uitgaande berichten door de VSAPI On-access scanner uit. De wijziging dient binnen een paar minuten actief te zijn.

4.6. Detectiebewerkingen



Bij het subitem **Detectiebewerkingen** kunt u automatische acties instellen die worden uitgevoerd tijdens het scanproces.

Er zijn bewerkingen voor de volgende situaties:

- **Infecties**

- **PUP (Potentieel Ongewenste Programma's)**
- **Waarschuwingen**
- **Informatie**

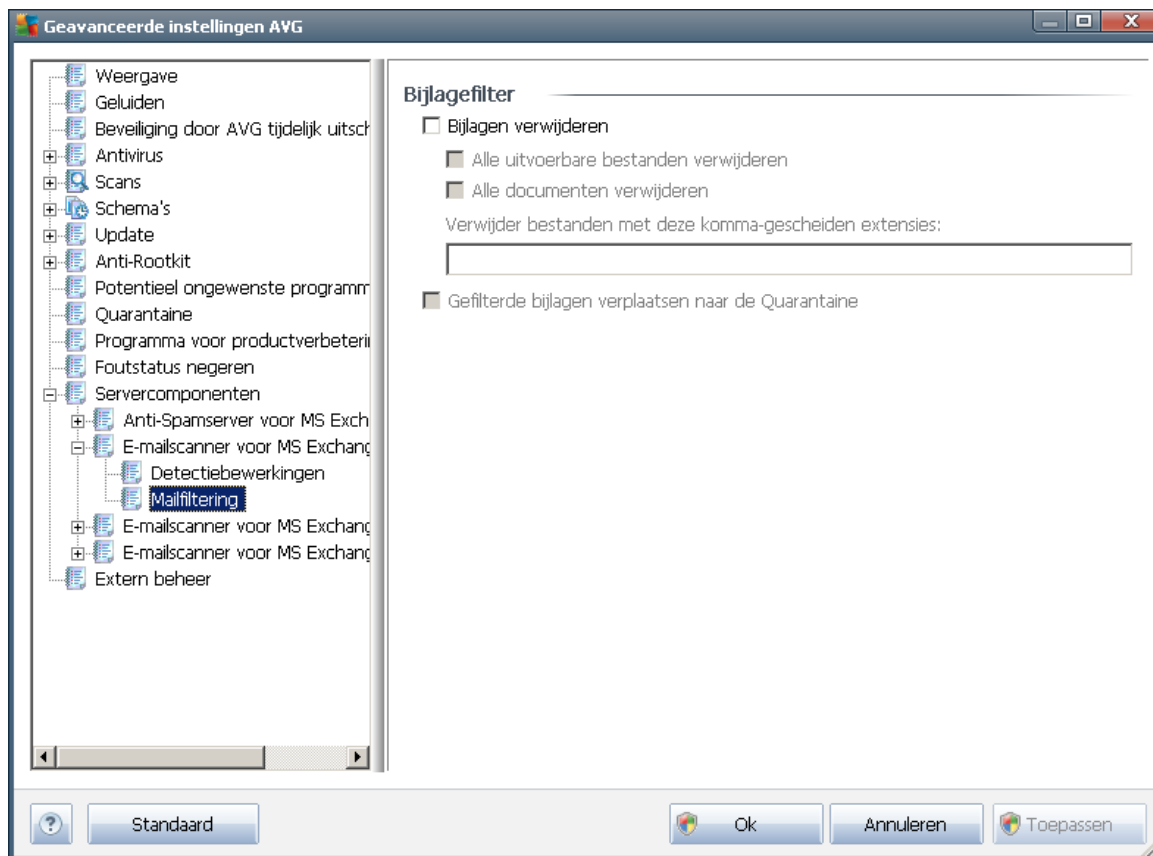
Maak in de vervolgkeuzelijst een keuze voor elk van de situaties:

- **Geen** – er wordt geen actie ondernomen.
- **Naar quarantaine verplaatsen** – de bedreiging zal worden verplaatst naar de Quarantaine.
- **Verwijderen** – de bedreiging wordt verwijderd.

Schakel het selectievakje **Onderwerp markeren met...** in en maak een keuze uit de voorgedefinieerde waarden als u een aangepaste tekst wilt selecteren voor berichten met de desbetreffende bedreiging.

Opmerking: de genoemde functie is niet beschikbaar voor E-mailscanner voor MS Exchange VSAPI.

4.7. Mailfiltering



Bij het subitem **Mailfiltering** kunt u aangeven welke bijlagen u eventueel meteen wilt verwijderen.



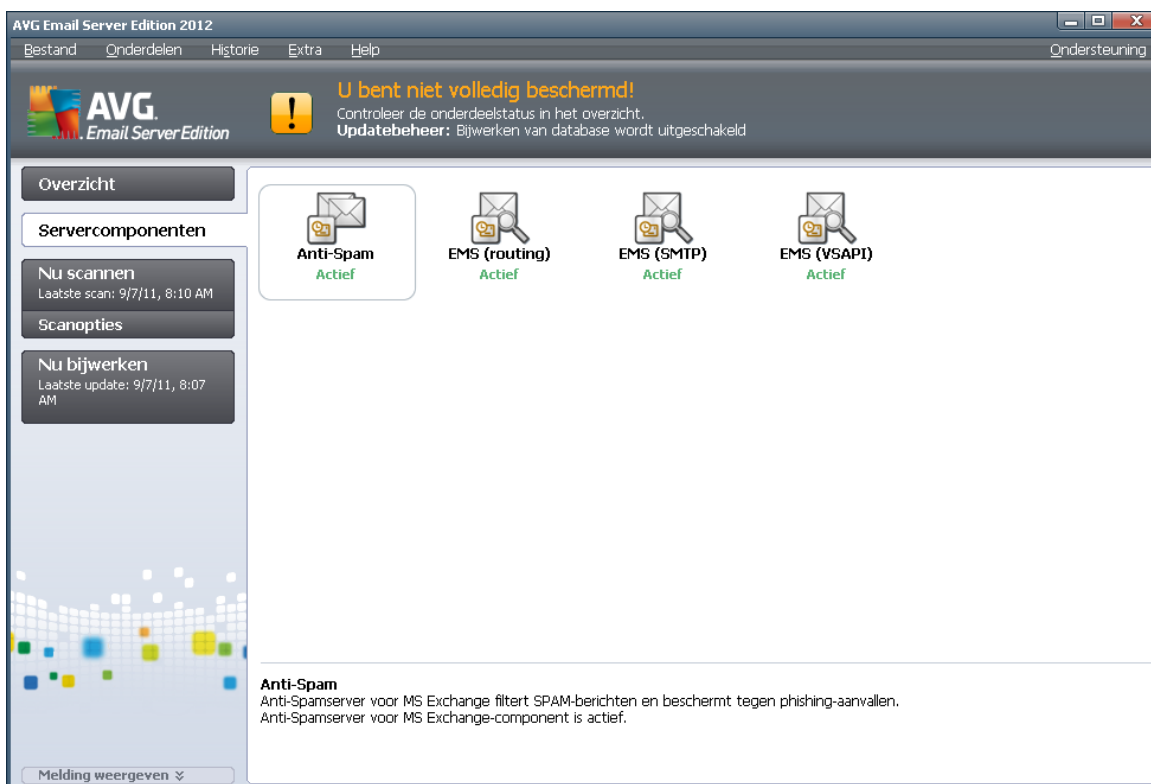
De volgende opties zijn beschikbaar:

- ***Bijlagen verwijderen*** – schakel dit selectievakje in om de functie in te schakelen.
- ***Alle uitvoerbare bestanden verwijderen*** – alle uitvoerbare bestanden worden verwijderd.
- ***Alle documenten verwijderen*** – alle documentbestanden verwijderen.
- ***Bestanden verwijderen met de volgende kommagescheiden extensies*** – geef in het tekstvak de extensie op van bestanden die u automatisch wilt verwijderen. Scheid die extensies van elkaar met komma's.
- ***Gefilterde bijlagen verplaatsen naar de Quarantaine*** – controle mogelijk maken van bestanden om te bepalen of ze werkelijk moeten worden verwijderd. Als u dit selectievakje inschakelt, worden alle in dit dialoogvenster genoemde bijlagen verplaatst naar de Quarantaine. Dat is een veilige ruimte voor opslag van mogelijk gevaarlijke bestanden – u kunt er de bestanden inzien en onderzoeken zonder uw systeem in gevaar te brengen. De Quarantaine is bereikbaar via de menubalk van het **AVG Email Server Edition 2012** hoofdscherm. Klik op het menu **Historie** en kies **Quarantaine** in de vervolkeuzelijst.

5. E-mailscanner voor MS Exchange Server 2003

5.1. Overzicht

De configuratieopties voor MS Exchange Server 2003 zijn volledig geïntegreerd in AVG Email Server Edition 2012 in de vorm van servercomponenten.



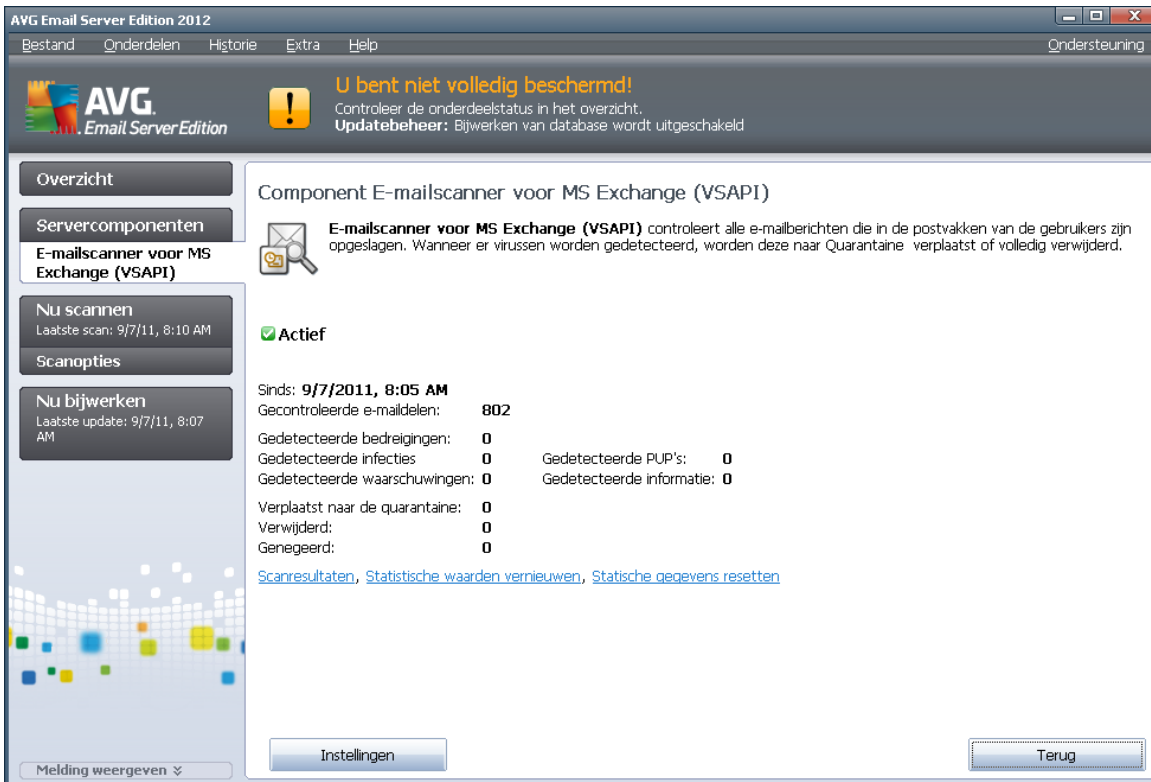
Het gaat om de volgende servercomponenten:

Basisoverzicht van de afzonderlijke servercomponenten:

- **[Anti-spam – Anti-Spamserver voor MS Exchange](#)**
controleert alle binnenkomende e-mailberichten en markeert ongewenste e-mails als SPAM. Het onderdeel maakt gebruik van verschillende analysemethoden om elk e-mailbericht te verwerken. Dit biedt de best mogelijke bescherming tegen ongewenste e-mailberichten.
- **[EMS \(VSAPI\) – E-mailscanner voor MS Exchange \(VSAPI\)](#)**
controleert alle e-mailberichten die in de postbussen van gebruikers zijn opgeslagen. Als er virussen worden gedetecteerd, worden ze naar de Quarantaine verplaatst of volledig verwijderd.

Dubbelklik op een component om de interface te openen. Het aparte, unieke scherm van het **Anti-Spam-onderdeel** wordt in een [afzonderlijk hoofdstuk](#) beschreven. In de interface voor de **E-**

mailscanner for MS Exchange vindt u de volgende knoppen en koppelingen:



The screenshot shows the AVG Email Server Edition 2012 interface. The main window title is "AVG Email Server Edition 2012". The menu bar includes "Bestand", "Onderdelen", "Historie", "Extra", and "Help". The status bar at the bottom right says "Ondersteuning".

The interface features a sidebar on the left with the following sections:

- Overzicht**
- Servercomponenten**
 - E-mailscanner voor MS Exchange (VSAPI)**
 - Nu scannen**
Laatste scan: 9/7/11, 8:10 AM
 - Scanopties**
 - Nu bijwerken**
Laatste update: 9/7/11, 8:07 AM

The main content area displays the status for the "Component E-mailscanner voor MS Exchange (VSAPI)". It includes a warning icon and the text: "U bent niet volledig beschermd! Controleer de onderdeelstatus in het overzicht. Updatebeheer: Bijwerken van database wordt uitgeschakeld." Below this, there is a description of the mail scanner and a status indicator "Actief".

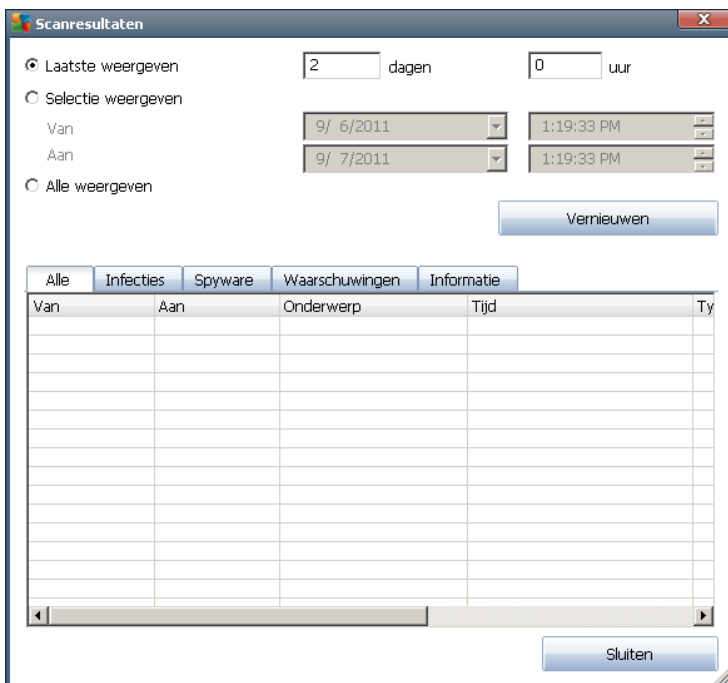
The status information is as follows:

- Sinds: 9/7/2011, 8:05 AM
- Gecontroleerde e-maildelen: 802
- Gedetecteerde bedreigingen: 0
- Gedetecteerde infecties: 0
- Gedetecteerde waarschuwingen: 0
- Verplaatst naar de quarantaine: 0
- Verwijderd: 0
- Genegeerd: 0
- Gedetecteerde PUP's: 0
- Gedetecteerde informatie: 0

At the bottom of the main content area, there are three links: [Scanresultaten](#), [Statistische waarden vernieuwen](#), and [Statische gegevens resetten](#). At the bottom of the window, there are buttons for "Melding weergeven", "Instellingen", and "Terug".

- **Scanresultaten**

Opent een nieuw dialoogvenster met scanresultaten:



Op tabbladen zijn berichten naar ernst gesorteerd. Zie de configuratie van afzonderlijke componenten voor het aanpassen van de ernst en rapportage.

Standaard worden alleen de resultaten van de laatste twee dagen weergegeven. U kunt met de volgende opties instellingen opgeven voor een andere periode:

- **Weergeven laatste** – weergave aan de hand van een opgegeven aantal dagen en uren.
- **Selectie weergeven** – weergave aan de hand van een opgegeven interval voor dagen en tijd.
- **Alles weergeven** – weergave van de resultaten van de hele periode.

Klik op de knop **Vernieuwen** om de resultaten opnieuw te laden.

- **Statistische waarden vernieuwen** – het bovengenoemde materiaal bijwerken.
- **Statistische waarden resetten** – alle cijfermateriaal terugzetten op nul.

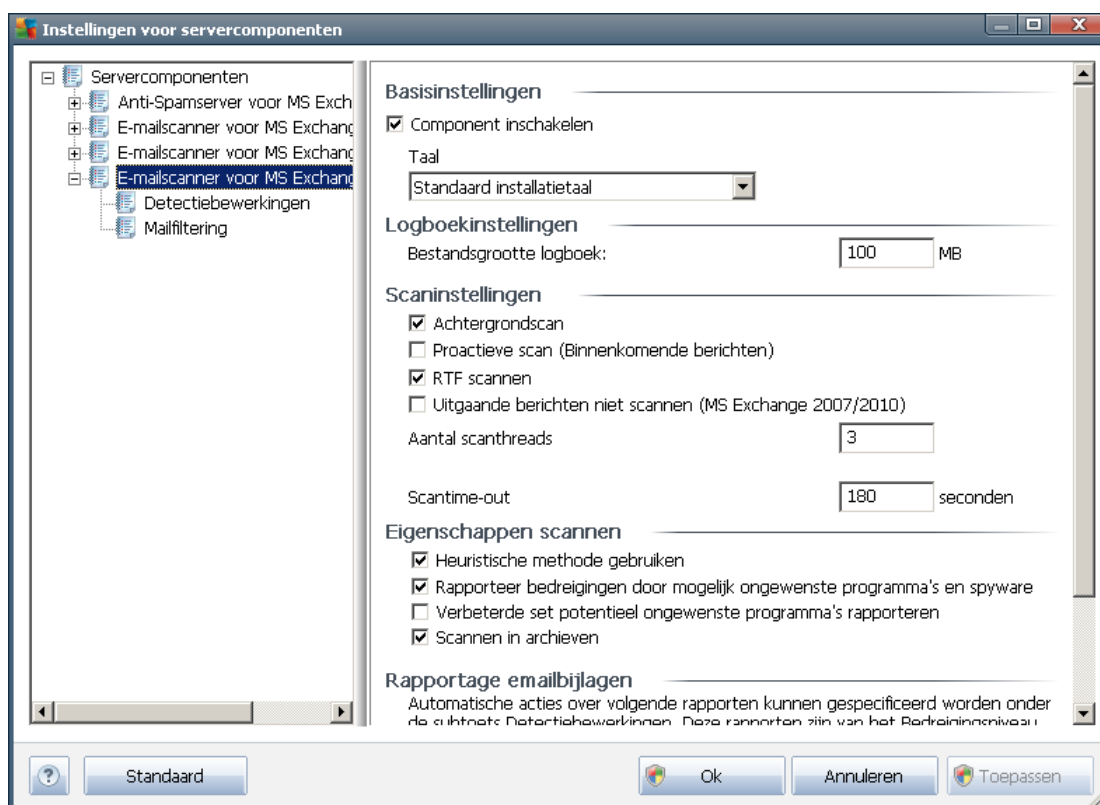
Het dialoogvenster heeft de volgende knoppen:

- **Instellingen** – de instellingen voor de component weergeven.
- **Terug** – klik op deze knop om terug te keren naar het Overzicht van Servercomponenten.

In de volgende hoofdstukken staat meer informatie over instellingen voor de afzonderlijke componenten.

5.2. E-mailscanner voor MS Exchange (VSAPI)

Dit item betreft de instellingen voor *E-mail Scanner for MS Exchange (VSAPI)*



In het **basisgedeelte** staan de volgende opties:

- **Onderdeel inschakelen** – schakel het selectievakje uit als u het onderdeel in zijn geheel wilt uitschakelen.
- **Taal** – selecteer de gewenste taal voor het onderdeel.

Het gedeelte **Loginstellingen**:

- **Bestandsgrootte logboek** – geef op hoe groot het bestand voor het logboek mag zijn. Standaardwaarde: 100 MB.

Het gedeelte **Scaninstellingen**:

- **Achtergrondscan** – de scanfunctie op de achtergrond in- en uitschakelen. Scannen als achtergrondbewerking is een van de voorzieningen van de VSAPI 2.0/2.5-toepassingsinterface. Het biedt een via threading uitgevoerde scanvoorziening van de Exchange Messaging-databases. Telkens wanneer er een item wordt aangetroffen in de postvakmappen van de gebruiker dat nog niet is gescand met de nieuwste AVG-virusdatabase-update, wordt dit item voorgelegd aan AVG voor Exchange Server om te worden gescand. De scanbewerking en de zoekactie naar de nog niet onderzochte objecten worden parallel uitgevoerd.



Voor elke database wordt een speciale thread met een lage prioriteit gebruikt, wat ervoor zorgt dat andere taken (bijv. het opslaan van e-mailberichten in de database van Microsoft Exchange) altijd met voorrang worden uitgevoerd.

- **Proactieve scan (binnenkomende berichten)**

met dit selectievakje kunt u aangeven of de proactieve scanfunctie van VSAPI 2.0/2.5 moet worden in- of uitgeschakeld. Deze scan wordt uitgevoerd wanneer een item wordt afgeleverd bij een map zonder dat er een verzoek is gedaan door een client.

Zodra berichten worden aangeboden aan de opslag van Exchange, worden ze in de wachtrij voor de globale scan geplaatst met een lage prioriteit (maximaal 30 items). Ze worden gescand op basis van het FIFO-principe (First In, First Out). Als een item wordt geadresseerd terwijl het zich nog steeds in de wachtrij bevindt, krijgt het een hoge prioriteit.

Opmerking: *Overflow-berichten gaan ongescand naar de opslag.*

Opmerking: *zelfs als u zowel de **Achtergrondscan** als de **Proactieve scan** uitschakelt, zal de Scanner bij toegang nog steeds actief zijn als een gebruiker probeert een bericht te downloaden met de MS Outlook-client.*

- **RTF scannen** – met dit selectievakje kunt u aangeven of bestanden met de indeling RTF wel of niet moeten worden gescand.

- **Aantal scanthreads** – standaard is ingesteld dat het scanproces via meerdere threads verloopt om de algehele scanprestaties te verhogen met een bepaald niveau van parallele verwerking. U kunt het aantal threads in dit veld aanpassen.

Het standaard aantal threads wordt als volgt berekend: 2 maal het 'aantal_processoren' + 1.

Het minimum aantal threads wordt als volgt berekend: ('aantal_processoren' + 1) gedeeld door 2.

Het maximum aantal threads wordt als volgt berekend: 'aantal_processoren' vermenigvuldigd met 5 + 1.

Als de waarde buiten de maximale of minimale waarden valt, wordt de standaardwaarde gebruikt.

- **Scantime-out** – dit veld geeft de maximale aaneengesloten periode (in seconden) weer gedurende welke een thread het bericht mag adresseren dat wordt gescand (de standaardwaarde is 180 seconden).

Het gedeelte **Scaneigenschappen**:

- **Heuristische methode gebruiken** – schakel dit selectievakje in als u tijdens het scannen gebruik wilt maken van heuristische analyse.
- **Rapporteer bedreigingen door mogelijk ongewenste programma's en spyware** – al dan niet rapporteren van potentieel ongewenste programma's en spyware.
- **Uitgebreide set van mogelijk ongewenste programma's rapporteren** – schakel dit selectievakje in om uitgebreide pakketten van spyware te detecteren: programma's waar op zich niets aan mankeert als u ze direct van de fabrikant krijgt, maar die wel in een later stadium voor kwaadaardige praktijken kunnen worden misbruikt, of die nooit kwaadaardig zijn, maar wel hinderlijk (verschillende werkbalken, e.d.) Dit is een aanvullende maatregel



ter bevordering van de veiligheid en het plezier van uw computer, al kunnen er ook legale programma's door worden geblokkeerd; om die reden is de functie standaard uitgeschakeld. Opmerking: deze detectiefunctie is een aanvulling op de vorige optie, dus als u beschermd wilt blijven tegen basistypen spyware, houdt u het vorige selectievakje ingeschakeld.

- **Scannen in archieven** – het scannen van archiefbestanden (zip, rar, enz.) in- en uitschakelen

In het gedeelte **Rapportage E-mailbijlagen** kunt u kiezen wat precies moet worden gerapporteerd tijdens het scannen. Dat is de standaardconfiguratie die u kunt wijzigen in het gedeelte **Detectiebewerkingen**, bij **Informatie** (zie hieronder).

De volgende opties zijn beschikbaar:

- **Rapport met wachtwoord beschermde archieven**
- **Rapport met wachtwoord beschermde documenten**
- **Rapport bestanden met een macro**
- **Rapport verborgen extensies**

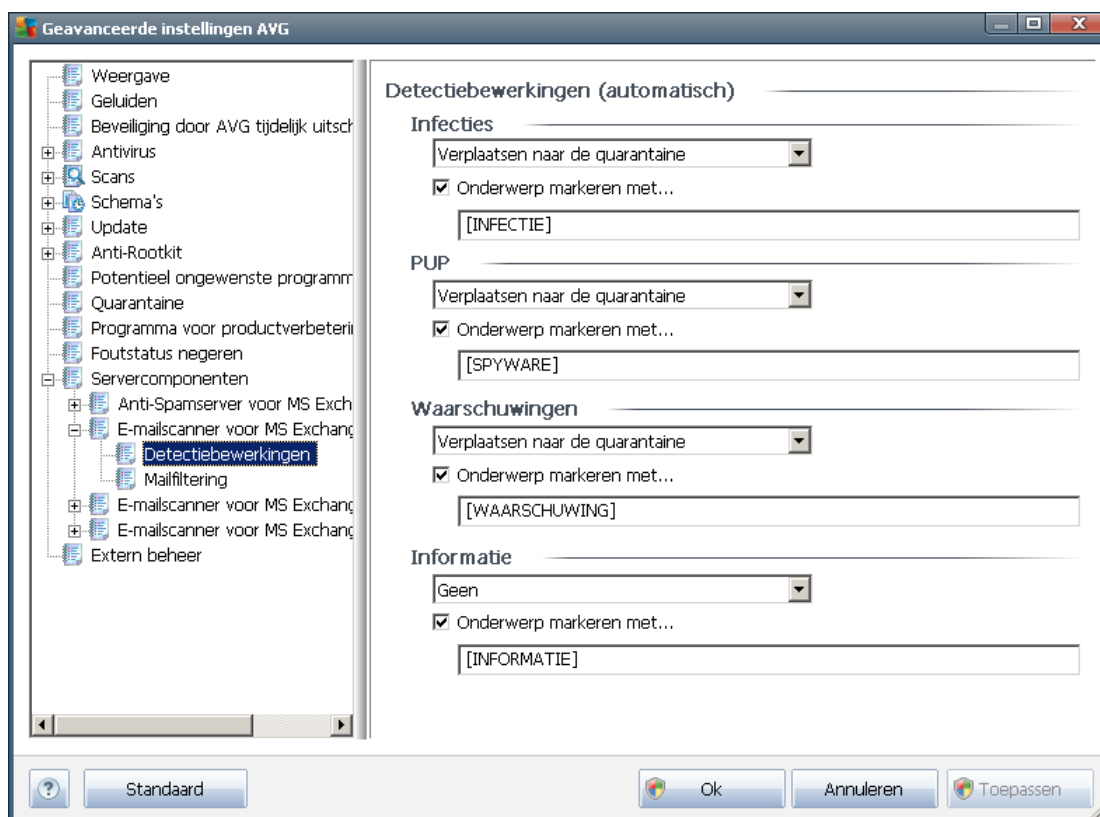
De voorzieningen op dit tabblad zijn overwegend gebruikersextensies van de services van de Microsoft VSAPI 2.0/2.5-toepassingsinterface. Raadpleeg voor gedetailleerde informatie over de VSAPI 2.0/2.5 de volgende koppelingen (en ook de koppelingen die u vanuit deze koppelingen weer kunt volgen):

- <http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k> – informatie over de interactie tussen Exchange en antivirussoftware
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;823166> informatie over aanvullende functies van VSAPI 2.5 in de toepassing Exchange 2003 Server.

De volgende structuur heeft bovendien de volgende subitems:

- [Detectiebewerkingen](#)
- [Mailfiltering](#)

5.3. Detectiebewerkingen



Bij het subitem **Detectiebewerkingen** kunt u automatische acties instellen die worden uitgevoerd tijdens het scanproces.

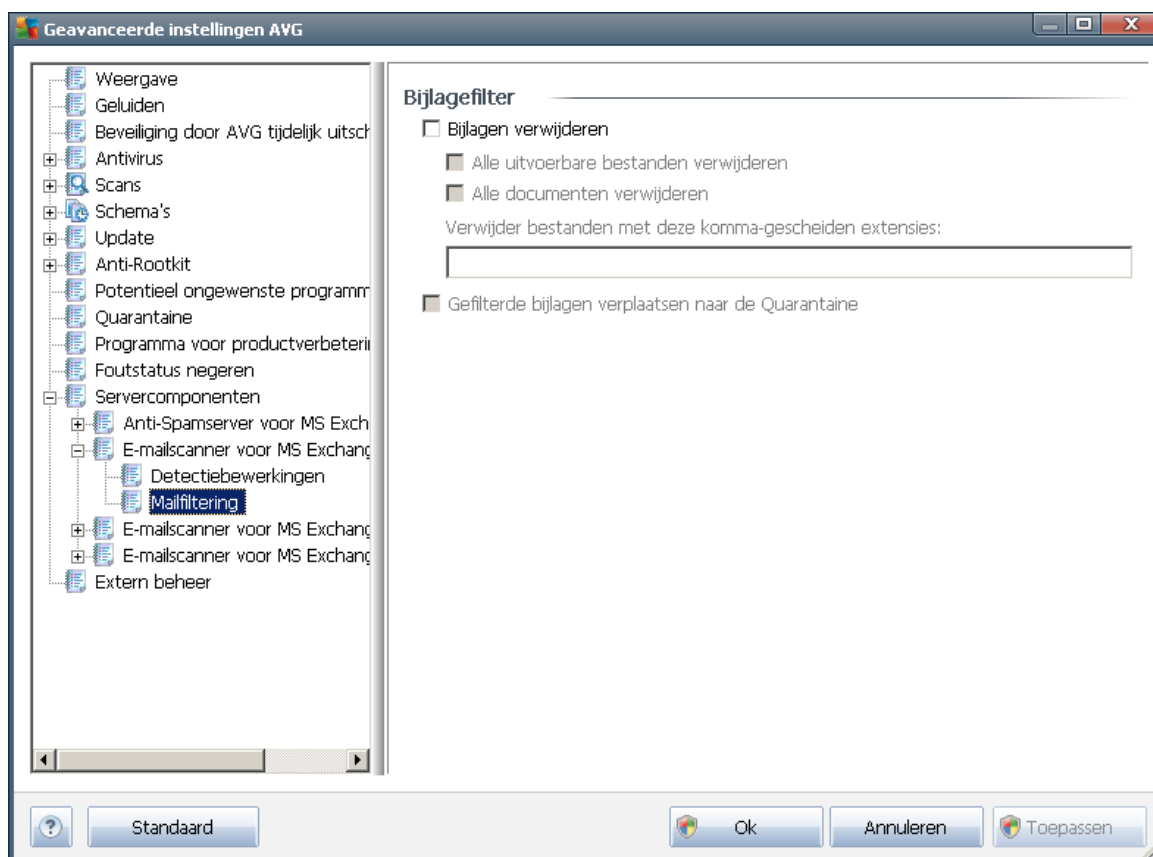
Er zijn bewerkingen voor de volgende situaties:

- **Infecties**
- **PUP (Potentieel Ongewenste Programma's)**
- **Waarschuwingen**
- **Informatie**

Maak in de vervolgkeuzelijst een keuze voor elk van de situaties:

- **Geen** – er wordt geen actie ondernomen.
- **Naar quarantaine verplaatsen** – de bedreiging zal worden verplaatst naar de Quarantaine.
- **Verwijderen** – de bedreiging wordt verwijderd.

5.4. Mailfiltering



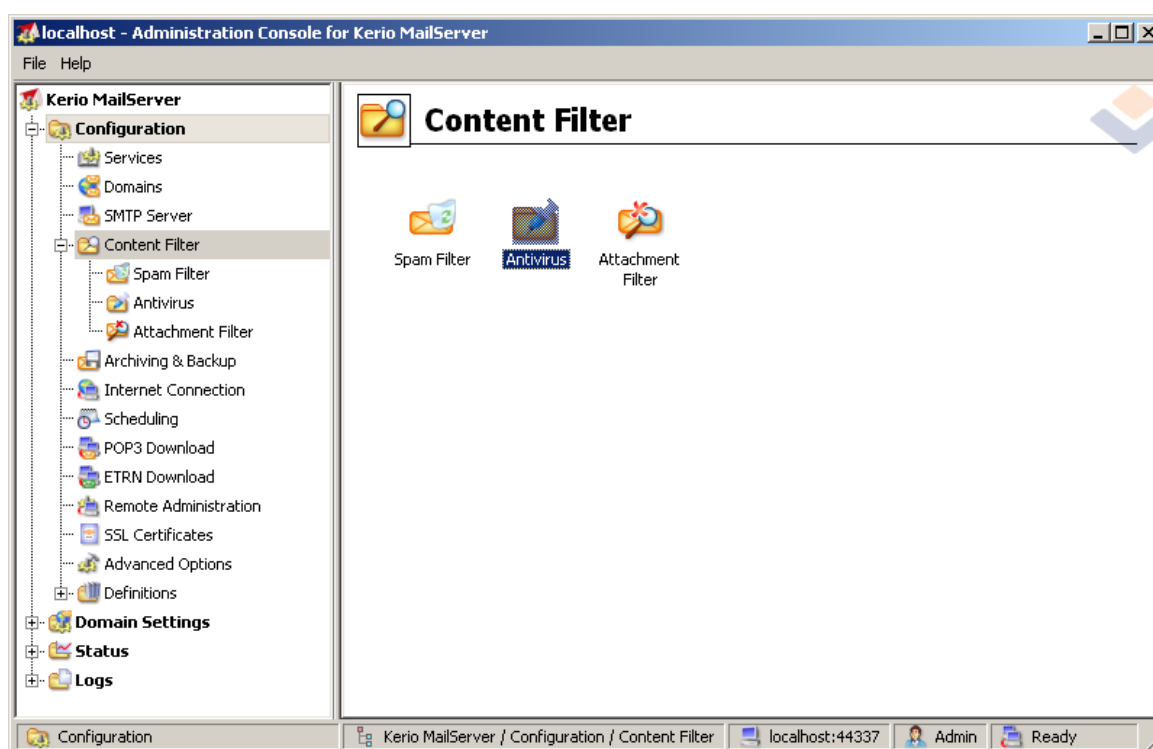
Bij het subitem **Mailfiltering** kunt u aangeven welke bijlagen u eventueel meteen wilt verwijderen. De volgende opties zijn beschikbaar:

- **Bijlagen verwijderen** – schakel dit selectievakje in om de functie in te schakelen.
- **Alle uitvoerbare bestanden verwijderen** – alle uitvoerbare bestanden worden verwijderd.
- **Alle documenten verwijderen** – alle documentbestanden verwijderen.
- **Bestanden verwijderen met de volgende kommagescheiden extensies** – geef in het tekstvak de extensie op van bestanden die u automatisch wilt verwijderen. Scheid die extensies van elkaar met komma's.
- **Gefilterde bijlagen verplaatsen naar de Quarantaine** – controle mogelijk maken van bestanden om te bepalen of ze werkelijk moeten worden verwijderd. Als u dit selectievakje inschakelt, worden alle in dit dialoogvenster genoemde bijlagen verplaatst naar de Quarantaine. Dat is een veilige ruimte voor opslag van mogelijk gevaarlijke bestanden – u kunt er de bestanden inzien en onderzoeken zonder uw systeem in gevaar te brengen. De Quarantaine is bereikbaar via de menubalk van het **AVG Email Server Edition 2012** hoofdscherm. Klik op het menu **Historie** en kies **Quarantaine** in de vervolgkeuzelijst.

6. AVG for Kerio MailServer

6.1. Configuratie

Het antivirusbeschermingsmechanisme is rechtstreeks geïntegreerd in de toepassing Kerio MailServer. Start de toepassing Kerio Administration Console om de e-mailbeveiliging van Kerio MailServer door de scanengine van AVG te activeren. Kies uit de controlestructuur aan de linkerzijde van het toepassingsvenster het subitem Content Filter (Inhoudsfilter) bij het item Configuration (Configuratie):



Als u op het item Content Filter (Inhoudsfilter) klikt, wordt een dialoogvenster met drie opties geopend:

- **Spam Filter (Spamfilter)**
- [Antivirus](#) (zie het gedeelte **Antivirus**)
- [Bijlagefilter](#) (zie het gedeelte **Bijlagefilter**)

6.1.1. Antivirus

Om AVG voor Kerio MailServer te selecteren, schakelt u het selectievakje Use external antivirus (Externe antivirussoftware gebruiken) in en kiest u de optie AVG Email Server Edition in het menu met externe software in het kader Antivirus usage (Antivirusgebruik) van het configuratievenster:



Antivirus usage

Use integrated McAfee® antivirus engine

Use external antivirus AVG Email Server Edition Options

In de volgende sectie kunt u aangeven wat er dient te gebeuren met een geïnfecteerd of gefilterd bericht:

- ***If a virus is found in a message (Als er een virus is aangetroffen in een bericht)***

If a virus is found in a message

Discard the message

Deliver the message with the malicious code removed

Forward the original message to administrator address:

Forward the filtered message to administrator address:

Dit kader laat zien welke actie wordt uitgevoerd als er een virus wordt gedetecteerd in een bericht, of wanneer een bericht wordt uitgefilterd door een bijlagefilter:

- ***Discard the message (Bericht verwijderen)*** – als u deze optie inschakelt, wordt het geïnfecteerde of gefilterde bericht verwijderd.
 - ***Deliver the message with the malicious code removed (E-mail afleveren bij ontvanger, zonder kwaadaardige code)*** – het bericht wordt bij de ontvanger afgeleverd, nadat eerst de potentieel schadelijke bijlage is verwijderd.
 - ***Forward the original message to administrator address (Oorspronkelijk bericht doorsturen naar adres beheerder)*** – als u dit selectievakje hebt ingeschakeld, wordt het met een virus besmette bericht doorgestuurd naar het adres dat is opgegeven in het tekstveld voor het bestemmingsadres
 - ***Forward the filtered message to administrator address (Gefilterd bericht doorsturen naar adres beheerder)*** – als u dit selectievakje hebt ingeschakeld, wordt het door een filter onderschepte bericht doorgestuurd naar het adres dat is opgegeven in het tekstveld voor het bestemmingsadres
- ***If a part of message cannot be scanned (e.g. encrypted or corrupted file) (Als een deel van een bericht niet kan worden gescand, bijvoorbeeld omdat het gecodeerd of beschadigd is)***

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)

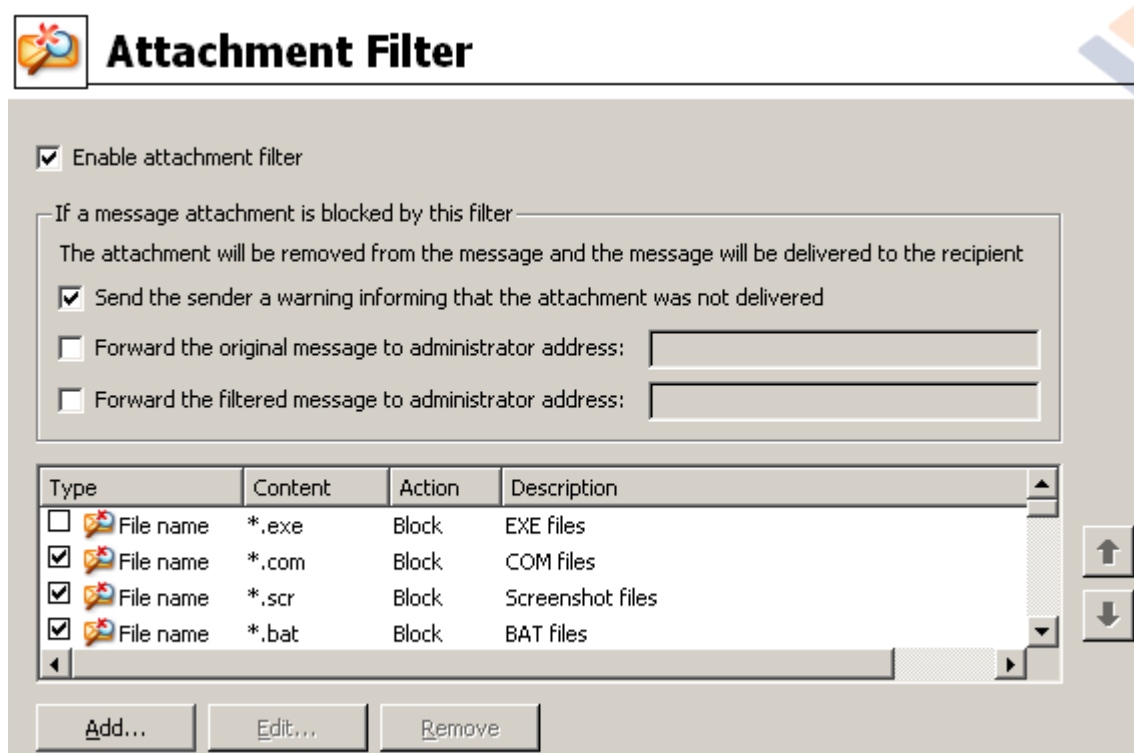
In dit kader staat vermeld welke actie moet worden ondernomen wanneer een deel van het

bericht of de bijlage niet kan worden gescand:

- **Deliver the original message with a prepared warning (Oorspronkelijk bericht afleveren, voorzien van voorgedefinieerde waarschuwing)** – het bericht (of de bijlage) wordt afgeleverd zonder dat het wordt gecontroleerd. De gebruiker wordt gewaarschuwd dat het bericht nog steeds virussen kan bevatten.
- **Reject the message as if it was virus (Bericht weigeren als ware het een virus) – het systeem reageert op dezelfde manier als bij de detectie van een virus (dat wil zeggen dat het bericht wordt afgeleverd zonder bijlage(n) of wordt geweigerd).** Deze optie is veilig, maar maakt het sturen van archieven die met een wachtwoord zijn beveiligd nagenoeg onmogelijk.

6.1.2. Bijlagefilter

In het menu Bijlagefilter treft u een lijst aan met diverse definities voor bijlagen:



U kunt het filteren van bijlagen bij e-mailberichten in- of uitschakelen met het selectievakje Enable attachment filter (Bijlagefilter inschakelen). De volgende instellingen kunt u desgewenst aanpassen:

- **Send a warning to sender that the attachment was not delivered (Waarschuwing naar afzender sturen dat de bijlage niet is afgeleverd)**

De afzender ontvangt een waarschuwing van Kerio MailServer dat hij/zij een bericht heeft gestuurd dat een virus of geblokkeerde bijlage bevatte.

- **Forward the original message to administrator address (Oorspronkelijk bericht**

doorsturen naar adres beheerder)

Het bericht wordt doorgestuurd (ongewijzigd – dus inclusief de geïnfecteerde of verboden bijlage) naar een vooraf gedefinieerd e-mailadres, ongeacht of dat een lokaal of extern adres is.

- **Forward the filtered message to administrator address (Gefilterd bericht doorsturen naar adres beheerder)**

Het bericht wordt, ontdaan van de geïnfecteerde of verboden bijlage (behalve bij toepassing van de hieronder geselecteerde acties), doorgestuurd naar het opgegeven e-mailadres. Deze functie kan worden gebruikt om te verifiëren of het antivirus- en/of bijlagefilter goed werkt.

In de lijst met extensies heeft elk item vier velden:

- **Type** – specificatie van het soort bijlage, op basis van de extensie die is opgegeven in het veld Content (Inhoud). Mogelijke typen zijn Bestandsnaam of MIME-type. U kunt het bijbehorende selectievakje van dit veld in- of uitschakelen om aan te geven of dit item moet worden opgenomen in de filterbewerking van bijlagen.
- **Content (Inhoud)** – hier kunt u een extensie opgeven voor de filteractie. Hierbij zijn jokertekens voor het besturingssysteem toegestaan (de tekenreeks `*.doc.*` staat bijvoorbeeld voor elk bestand met de extensie `.doc`, waarna elke mogelijke extensie kan volgen).
- **Action (Actie)** – definieer hier welke actie moet worden uitgevoerd op de desbetreffende bijlage. Mogelijke acties zijn Accept (Accepteren, de bijlage accepteren), en Block (Blokkeren, er wordt dan een actie uitgevoerd zoals aangegeven boven de lijst met uitgeschakelde bijlagen).
- **Description (Beschrijving)** – in dit veld is een beschrijving van de bijlage gedefinieerd.

U kunt een item uit de lijst verwijderen door op de knop Remove (Verwijderen) te klikken. Klik op de knop **Add (Toevoegen)** om een item toe te voegen aan de lijst. Of klik op de knop **Edit (Bewerken)** als u een bestaand item wilt bewerken. Het volgende venster wordt geopend:





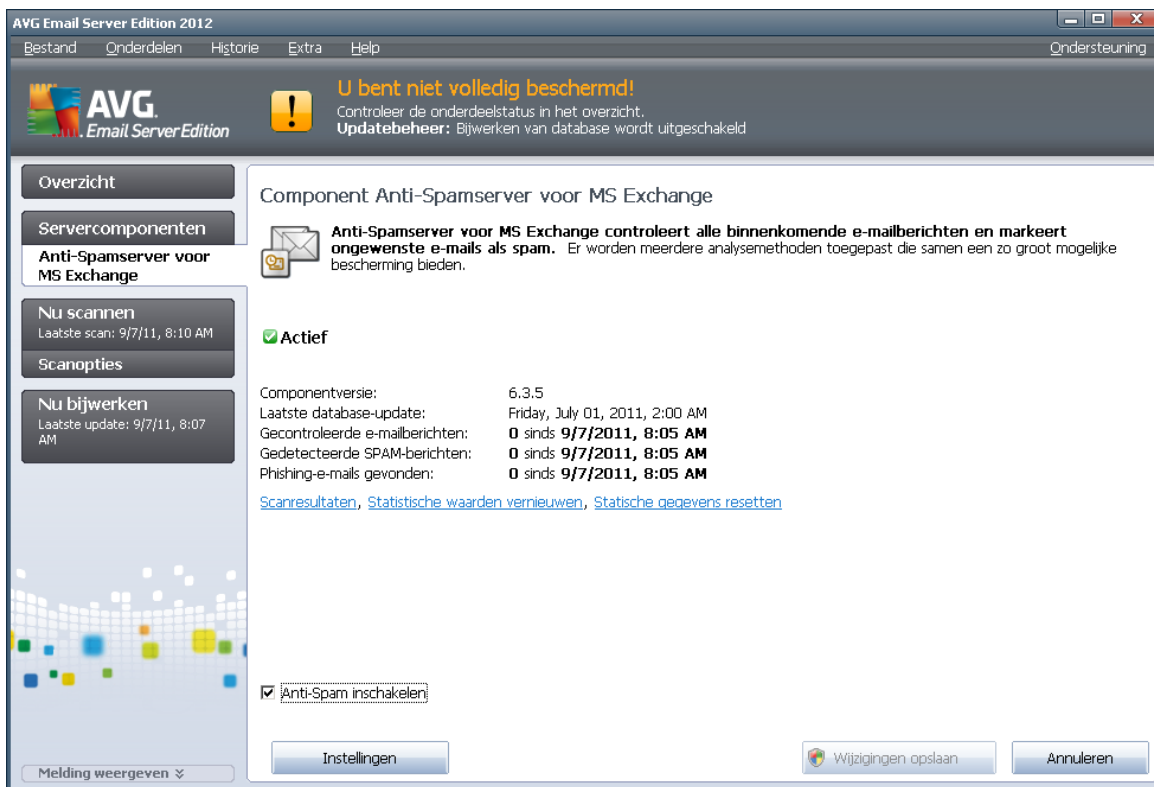
- In het veld Description (Beschrijving) kunt u een korte beschrijving invoeren van de bijlage die moet worden gefilterd.
- In het veld If a mail message contains an attachment where (Als het e-mailbericht een bijlage bevat met daarin) kunt u een type bijlage selecteren (Bestandsnaam of MIME-type). U kunt ook een bepaalde extensie kiezen in de lijst met extensies, of u kunt direct het jokerteken voor de extensie invoeren.

In het veld Then (ga dan als volgt te werk) kunt u opgeven of de gedefinieerde bijlage vervolgens moet worden geblokkeerd of geaccepteerd.



7. Anti-Spamconfiguratie

7.1. Antispaminterface

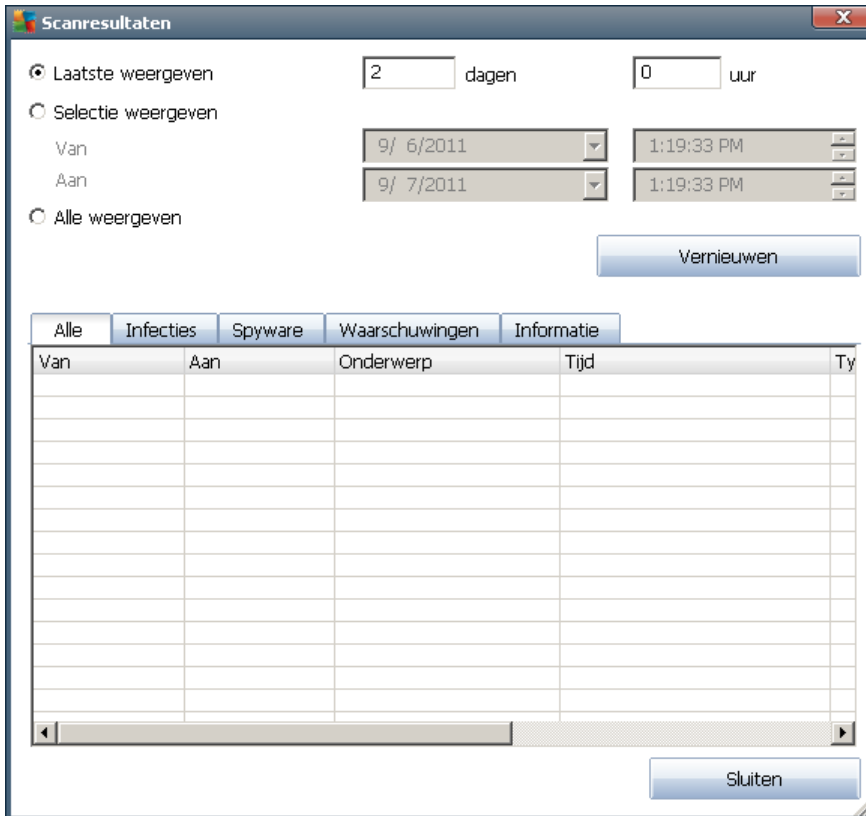


Het dialoogvenster van de **Anti-Spamserver** onderdeel bij het onderdeel **Servercomponenten** (linkerdeelvenster). Er wordt beknopte informatie gegeven over de functionaliteit van de servercomponent, informatie over de huidige status (*Onderdeel Anti-Spamserver voor MS Exchange is actief.*) en een paar statistieken:

Koppelingen:

- **Scanresultaten**

er wordt een nieuw dialoogvenster geopend waarin de resultaten worden weergegeven van antispamscans:



In het venster kunt u berichten controleren die als SPAM (ongewenste berichten) of pogingen tot Phishing (een poging persoonlijke gegevens te stelen, bijv. bankgegevens, identiteit, enz.) zijn gedetecteerd. Standaard worden alleen de resultaten van de laatste twee dagen weergegeven. U kunt met de volgende opties instellingen opgeven voor een andere periode:

- **Weergeven laatste** – weergave aan de hand van een opgegeven aantal dagen en uren.
- **Selectie weergeven** – weergave aan de hand van een opgegeven interval voor dagen en tijd.
- **Alles weergeven** – weergave van de resultaten van de hele periode.

Klik op de knop **Vernieuwen** om de resultaten opnieuw te laden.

- **Statistische waarden vernieuwen** – het bovengenoemde materiaal bijwerken.
- **Statistische waarden resetten** – alle cijfermateriaal terugzetten op nul.

In het gedeelte **Antispaminstellingen** van het dialoogvenster staat één selectievakje: **Anti-spam inschakelen**. Schakel het selectievakje uit om de bescherming tegen spam uit te schakelen. U kunt de bescherming tegen spam weer inschakelen met behulp van hetzelfde selectievakje, of met een zelfde selectievakje bij de [Antispaminstellingen](#).

Het dialoogvenster heeft de volgende knoppen:

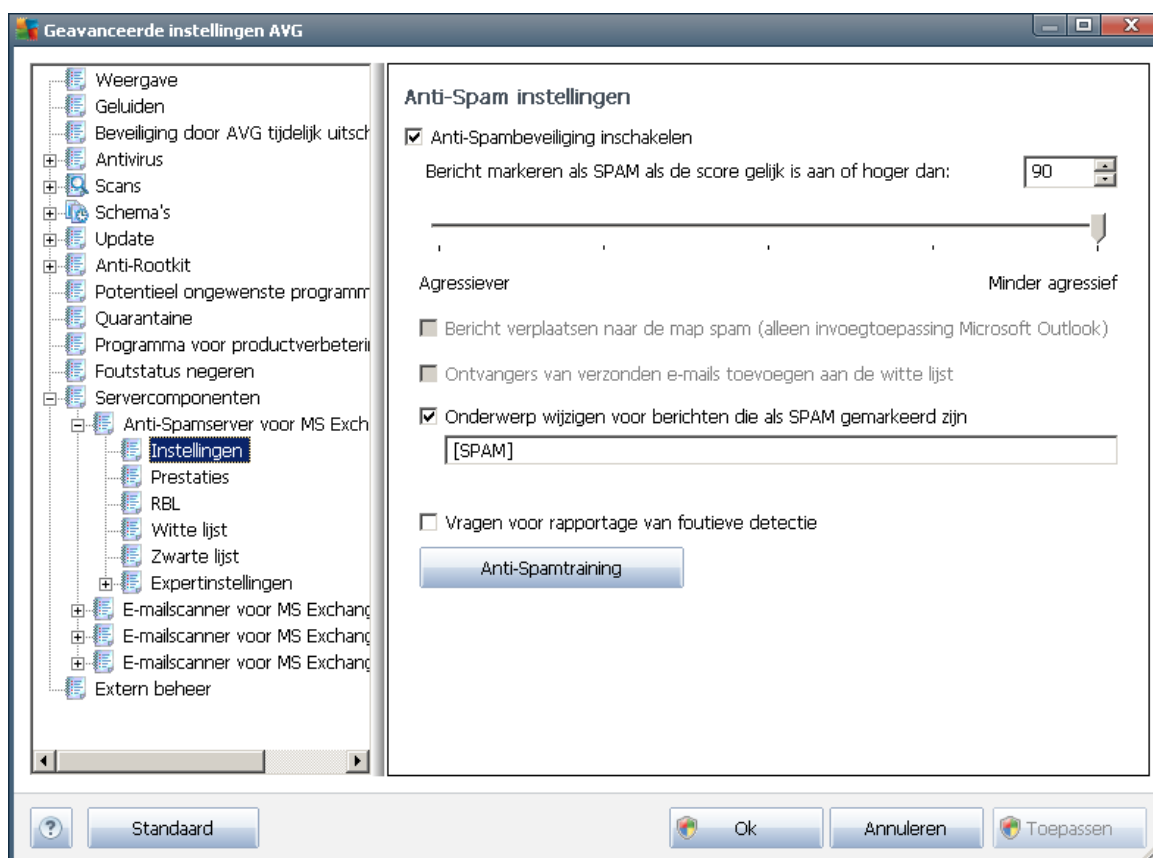
- **Instellingen** – open met deze knop het dialoogvenster [Anti-Spaminstellingen](#).
- **Terug** – klik op deze knop om terug te keren naar het Overzicht van Servercomponenten.

7.2. Antispam principes

Spam verwijst naar ongewenste e-mailberichten, die meestal reclame maken voor een product of service en naar grote aantallen e-mailadressen die tegelijk verstuurd worden, waardoor de postbussen van ontvangers vol raken. Spam verwijst niet naar wettige commerciële e-mail waarvoor klanten hun toestemming hebben gegeven. Spam is niet alleen vervelend, maar kan ook een bron zijn van zwendel, virussen of aanstootgevende inhoud.

Anti-Spam controleert alle binnenkomende e-mailberichten en markeert ongewenste e-mails als SPAM. Het onderdeel maakt gebruik van verschillende analysemethoden om elk e-mailbericht te verwerken. Dit biedt de best mogelijke bescherming tegen ongewenste e-mailberichten.

7.3. Anti-Spaminstellingen



In het dialoogvenster **Anti-Spam basisinstellingen** kunt u het selectievakje **Anti-Spambeveiliging inschakelen** in- en uitschakelen om het scannen van e-mail op spam in of uit



te schakelen.

In dit dialoogvenster kunt u meer of minder agressieve scoremaatregelen selecteren. Het **Anti-Spam** filter wijst een score aan elk bericht toe (*bijvoorbeeld in hoeverre de inhoud van het bericht spam benadert*) op basis van verschillende dynamische scantechnieken. U kunt de optie **Bericht als spam markeren als score gelijk is aan of hoger dan:** aanpassen door een waarde (*tussen 50 en 90*) in te voeren of door de schuifregelaar naar links of rechts te slepen.

Hieronder volgt een algemeen overzicht van de scoredrempel.

- **Waarde 90** – De meeste binnenkomende e-mailberichten worden normaal afgeleverd (zonder als [spam](#) gemarkeerd te worden). De gemakkelijkst herkenbare [spam](#) wordt gefilterd, maar een aanzienlijke hoeveelheid [spam](#) wordt nog doorgelaten.
- **Waarde 80-89** - E-mailberichten waarvan de kans groot is dat ze [spam](#) bevatten, worden gefilterd. Het kan zijn dat sommige niet-spamberichten ook gefilterd worden.
- **Waarde 60-79** – Een vrij agressieve configuratie. E-mailberichten die mogelijk [spam](#) zijn, worden gefilterd. Er worden waarschijnlijk ook niet-spamberichten als spam aangeduid.
- **Waarde 50-59** – Een zeer agressieve configuratie. Zowel niet-spamberichten als echte [spam](#)berichten worden gefilterd. Deze instelling is niet raadzaam voor normaal gebruik.

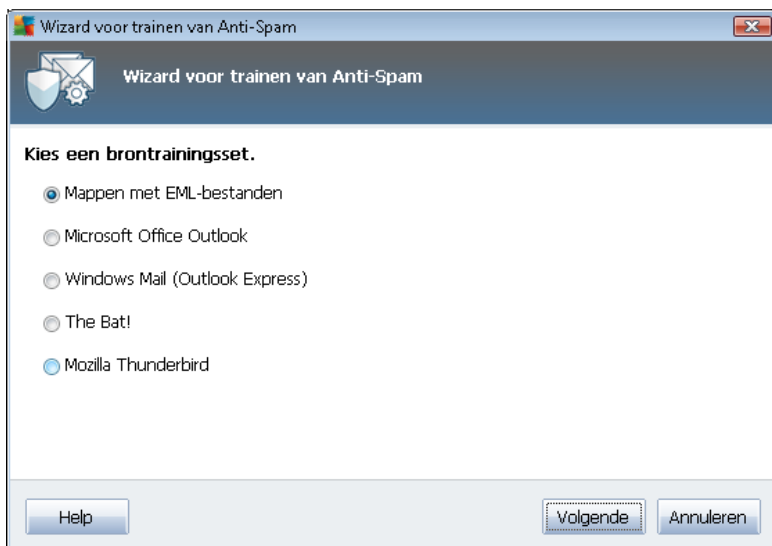
U kunt nader opgeven hoe gedetecteerde [spamberichten](#) moeten worden verwerkt:

- **Onderwerp wijzigen voor berichten die als spam gemarkeerd zijn** – schakel dit selectievakje in als u alle berichten die als [spam](#) worden gedetecteerd, wilt markeren met een bepaald woord of teken op de onderwerpsregel van het bericht; U kunt het desbetreffende woord of teken in het geactiveerde tekstveld typen.
- **Vragen voor rapportage van foutieve detectie** – vooropgesteld dat u de tijdens de installatieprocedure hebt aangegeven dat u wilt meewerken aan het Programma voor productverbetering – met dat programma zamelen we up-to-date informatie in over de nieuwste bedreigingen van iedereen die wereldwijd meewerkt, zodat wij de bescherming voor iedereen kunnen verbeteren – kunt u hier het toestaan nuanceren van rapportage van gedetecteerde bedreigingen naar AVG. De rapportage vindt automatisch plaats. Als u echter dit selectievakje inschakelt, kunt u het rapporteren van een detectie aan AVG al dan niet bevestigen, zodat u in de gelegenheid bent vast te stellen of het bericht echt als spam moet worden geclassificeerd.

Anti-Spam training – de [wizard Anti-Spamtraining](#) starten, die gedetailleerd wordt beschreven in het [volgende hoofdstuk](#).

7.3.1. De wizard Antispamtraining

In het eerste dialoogvenster van de **wizard Anti-Spamtraining** wordt u gevraagd de bron van e-mailberichten te selecteren die u voor training wilt gebruiken. Over het algemeen gebruikt u daarvoor de e-mails die onterecht zijn aangemerkt als SPAM en spamberichten die niet als zodanig zijn herkend.



U kunt kiezen uit de volgende opties:

- **Een specifieke e-mailclient** - als u met één van de genoemde e-mailclients (*MS Outlook*, *Outlook Express*, *The Bat!*, *Mozilla Thunderbird*) werkt, kiest u de corresponderende optie
- **Map met EML-bestanden** - als u een ander e-mailprogramma gebruikt, dient u eerst de berichten in een bepaalde map op te slaan (in *.eml format*), of ervoor te zorgen dat u de locatie van uw map met e-mailclientberichten kent. Selecteer vervolgens **Map met EML-bestanden** om het pad naar die map op te geven

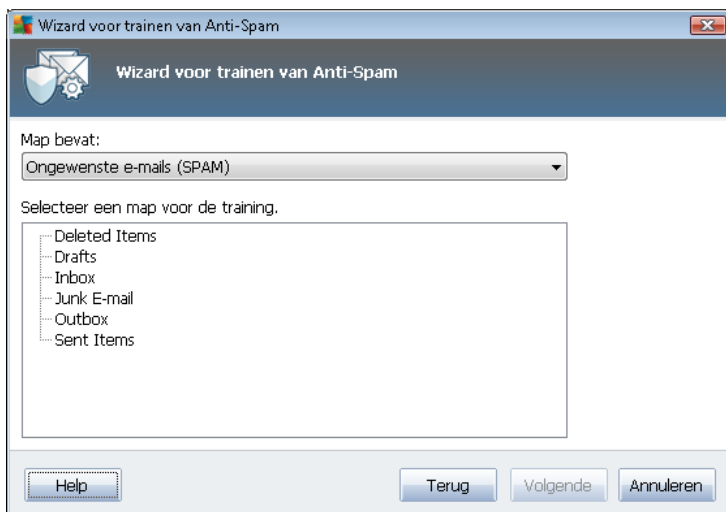
Het trainingsproces verloopt sneller en gemakkelijker als u de e-mails in de mappen van tevoren sorteert, zodat de map die u wilt gebruiken voor de training alleen de trainingsberichten bevat (ofwel gewenst ofwel ongewenst). Maar dat is niet noodzakelijk, omdat u de e-mails ook later in deze wizard kunt filteren.

Selecteer een optie en klik op **Volgende** om verder te gaan met de wizard.

7.3.2. Selecteer de map met berichten

De weergave van het dialoogvenster bij deze stap is afhankelijk van uw keuze hiervoor.

Mappen met EML-bestanden



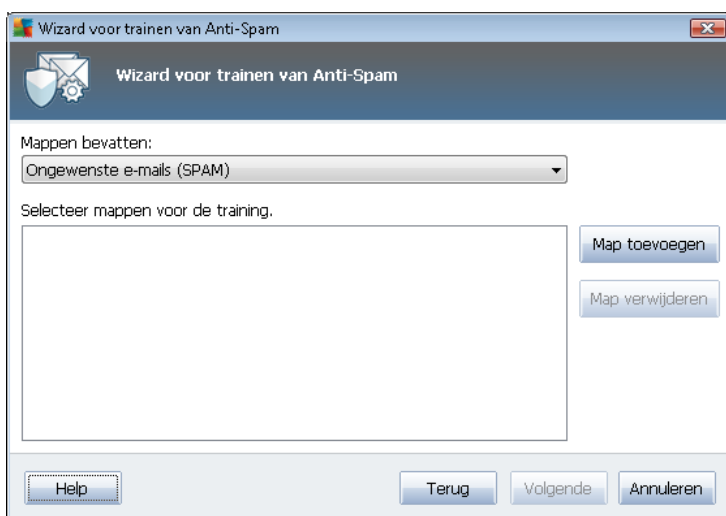
Zoek in dit dialoogvenster de map met de berichten die u wilt gebruiken voor de training. Klik op de knop **Map toevoegen** om de map te zoeken met de .eml-bestanden (*opgeslagen e-mailberichten*). De geselecteerde map zal vervolgens in het dialoogvenster worden weergegeven.

Maak met de vervolgkeuzelijst **Mappen bevatten** een keuze of de geselecteerde map gewenste berichten bevat (*HAM*) of ongewenste berichten (*SPAM*). NB: U kunt de berichten in de volgende stap filteren, dus de map hoeft niet uitsluitend trainingse-mails te bevatten. U kunt ook een ongewenste selectie van mappen in de lijst ongedaan maken door te klikken op de knop **Map verwijderen**.

Klik, als u klaar bent, op **Volgende** en ga verder met [Opties voor het filteren van berichten](#).

Specifieke e-mailclient

Als u een van de opties hebt bevestigd, wordt een nieuw dialoogvenster geopend.

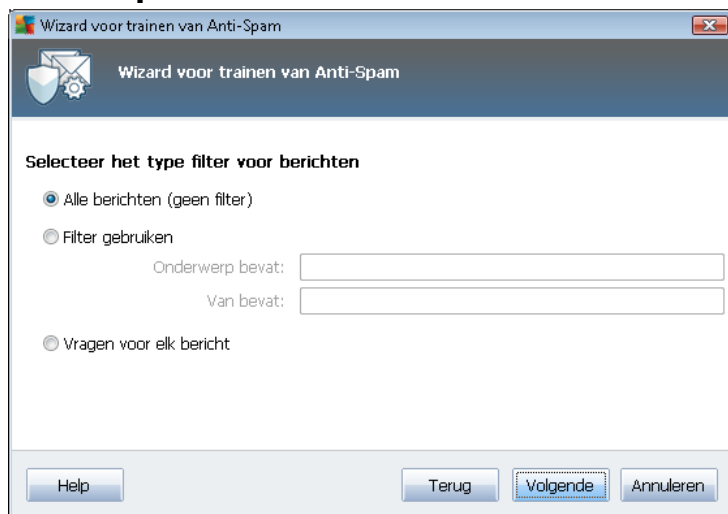


Opmerking: als het MS Outlook betreft, wordt u eerst gevraagd het MS Outlook-profiel te kiezen.

Maak met de vervolgkeuzelijst **Mappen bevatten** een keuze of de geselecteerde map gewenste berichten bevat (**HAM**) of ongewenste berichten (**SPAM**). NB: U kunt de berichten in de volgende stap filteren, dus de map hoeft niet uitsluitend trainingse-mails te bevatten. Op het scherm staat de navigatiestructuur van de geselecteerde e-mailclient in het hoofdgedeelte van het dialoogvenster. Zoek de gewenste map in de structuur en selecteer deze met uw muis.

Klik, als u klaar bent, op **Volgende** en ga verder met [Opties voor het filteren van berichten](#).

7.3.3. Opties voor het filteren van berichten

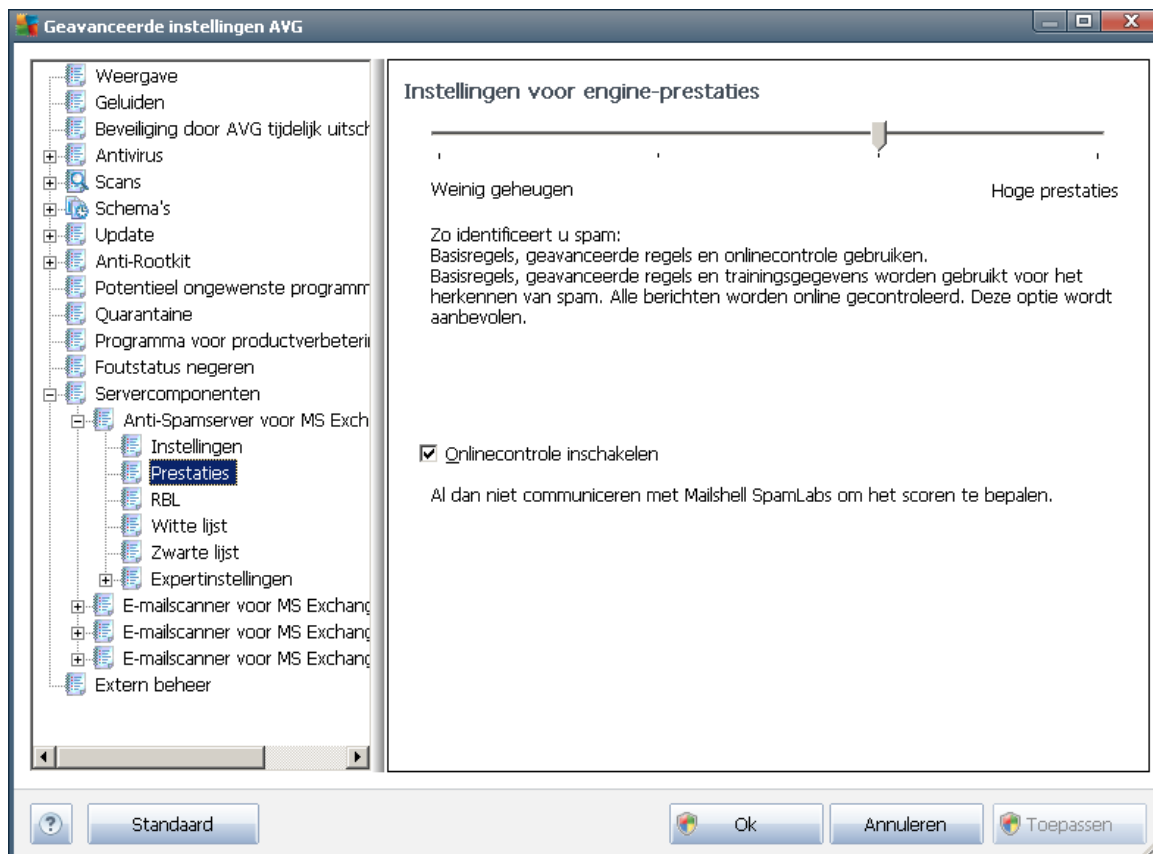


In dit dialoogvenster kunt u de filtering instellen voor e-mailberichten.

- **Alle berichten (geen filter)** – als u zeker weet of de geselecteerde map uitsluitend berichten bevat die u voor training kunt gebruiken, selecteert u de optie **Alle berichten (geen filter)**.
- **Filter gebruiken** - Als u geavanceerdere filtermogelijkheden wilt gebruiken, selecteert u de optie **Filter gebruiken**. U kunt een woord invullen (*naam*), deel van een woord of een zin waarnaar gezocht moet worden in het onderwerpveld en/of het veld van de afzender van de e-mail. Alle berichten die exact voldoen aan de ingevoerde criteria zullen worden gebruikt voor de training zonder verdere herinnering. Wanneer u beide tekstvelden invult, worden adressen die overeenkomen met een van de twee voorwaarden eveneens gebruikt.
- **Vragen bij elk bericht** - Als u niet zeker bent met betrekking tot de berichten in de map en als u wilt dat de wizard u bij elk bericht vraagt of dit kan worden gebruikt (*zodat u kunt bepalen of dit wel of niet voor trainingsdoeleinden kan worden gebruikt*), selecteert u de optie **Vragen bij elk bericht**.

Als u een keuze hebt gemaakt, klikt u op **Volgende**. Het dialoogvenster dat dan wordt geopend, heeft uitsluitend een informatieve functie en deelt mee dat de wizard klaar is om te beginnen met het verwerken van de berichten. Klik opnieuw op de knop **Volgende** om de training te starten. De training wordt vervolgens uitgevoerd aan de hand van de geselecteerde opties.

7.4. Prestaties



In het dialoogvenster **Instellingen voor engine-prestaties** (dat u opent met de optie **Prestaties** in de navigatiestructuur links) staan de instellingen voor de prestaties van het onderdeel **Anti-Spam**. Verplaats de schuifbalk naar links of naar rechts om de scanprestaties aan te passen tussen **Weinig geheugen** / **Hoge prestaties**.

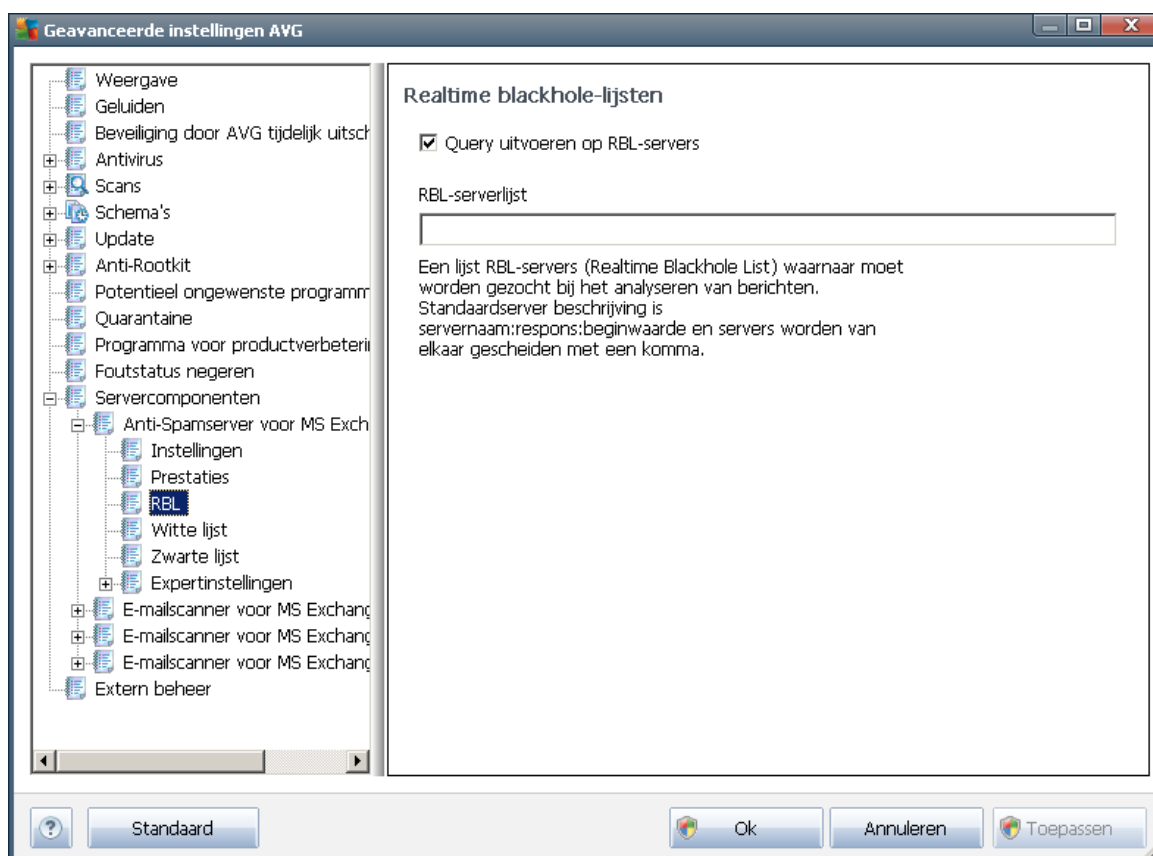
- **Weinig geheugen** – tijdens het scanproces ter detectie van [spam](#) worden geen regels gebruikt, maar alleen trainingsgegevens. Het is niet raadzaam deze modus voor normaal gebruik te selecteren, tenzij de computerhardware van lage kwaliteit is.
- **Hoge prestaties** – bij deze stand wordt een groot beroep gedaan op het geheugen van de computer. Bij het scanproces ter detectie van [spam](#) worden de volgende functies gebruikt: regels en [spam](#)database, basisregels, geavanceerde regels, IP-adressen van spammers en spammerdatabases.

De optie **Online controle inschakelen** is standaard ingeschakeld. Dit resulteert in een meer precieze [spam](#)detectie dankzij communicatie met de [Mailshell](#) servers, dat wil zeggen dat de gescande gegevens online worden vergeleken met [Mailshell](#) databases.

Over het algemeen is het raadzaam de standaardinstellingen aan te houden en die alleen te wijzigen als u daar een goede reden voor hebt. Wijzigen van deze configuratie is voorbehouden aan experts!

7.5. RBL

Met de optie **RBL** opent u het dialoogvenster **Realtime Blackhole Lists**:



In dit dialoogvenster kunt u de functie **Query uitvoeren op RBL-servers** in- en uitschakelen.

De RBL-server (*Realtime Blackhole List*) is een DNS-server met een uitgebreide database van bekende spammers. Wanneer deze functie ingeschakeld is, worden alle e-mailberichten gecontroleerd in de RBL-serverdatabase en als [spam](#) gemarkeerd wanneer ze identiek zijn aan een onderdeel van de database.

De RBL-serverdatabases bevatten de recentste spamvingerafdrukken, waardoor de beste en meest accurate [spam](#)detectie geboden kan worden. Deze functie is vooral nuttig voor gebruikers die grote hoeveelheden spam ontvangen die normaal niet door de antispamengine gedetecteerd wordt.

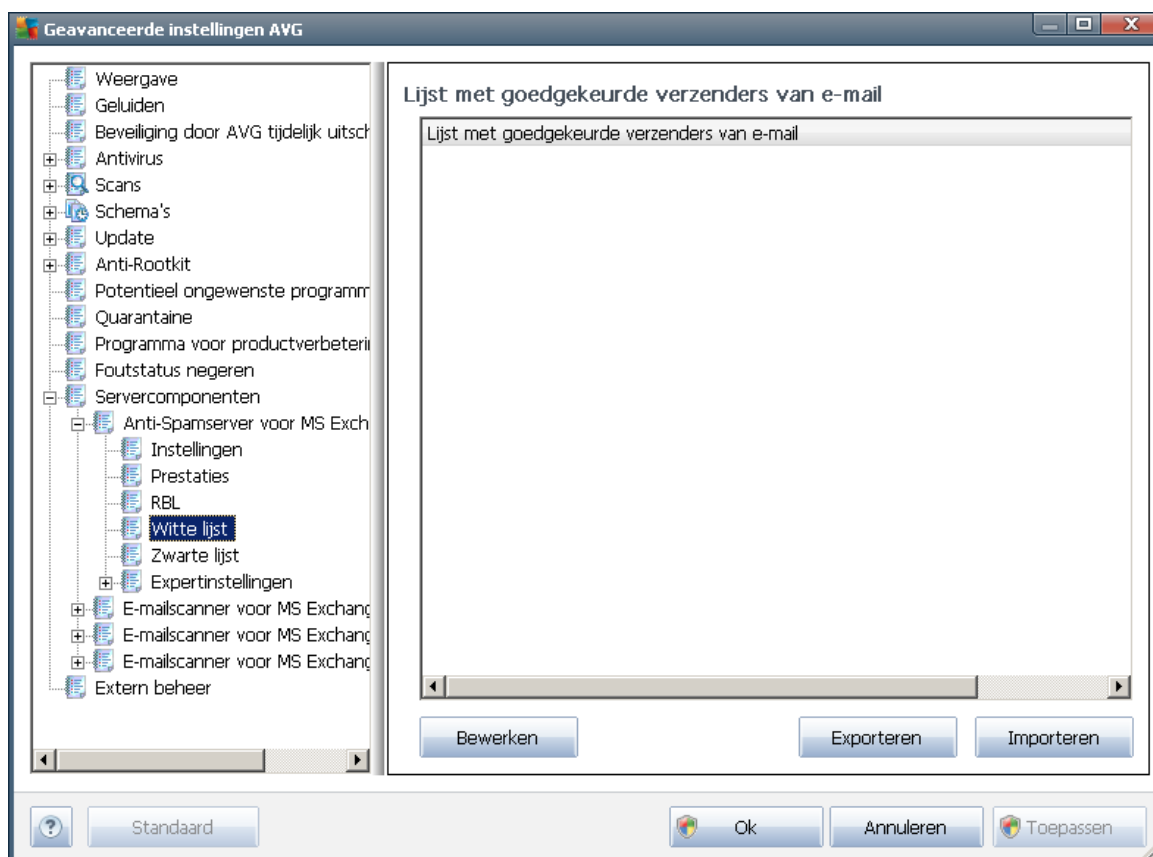
Op de **RBL-serverlijst** kunt u specifieke RBL-serverlocaties definiëren. Er worden standaard twee RBL-serveradressen opgegeven. Het is raadzaam de standaardinstellingen te behouden, tenzij u een ervaren gebruiker bent en een gegronde reden hebt om deze instellingen te wijzigen!

Opmerking: Wanneer u deze functie inschakelt, worden e-mailberichten op sommige systemen en configuraties trager ontvangen, aangezien elk bericht gecontroleerd moet worden in de RBL-serverdatabase.

Er worden geen persoonlijke gegevens naar de server verzonden!

7.6. Witte lijst

Met de optie **Witte lijst** opent u een dialoogvenster met een globale lijst met de e-mailadressen en domeinnamen van goedgekeurde afzenders. De berichten van deze afzenders zullen nooit als [spam](#) gemarkeerd worden.



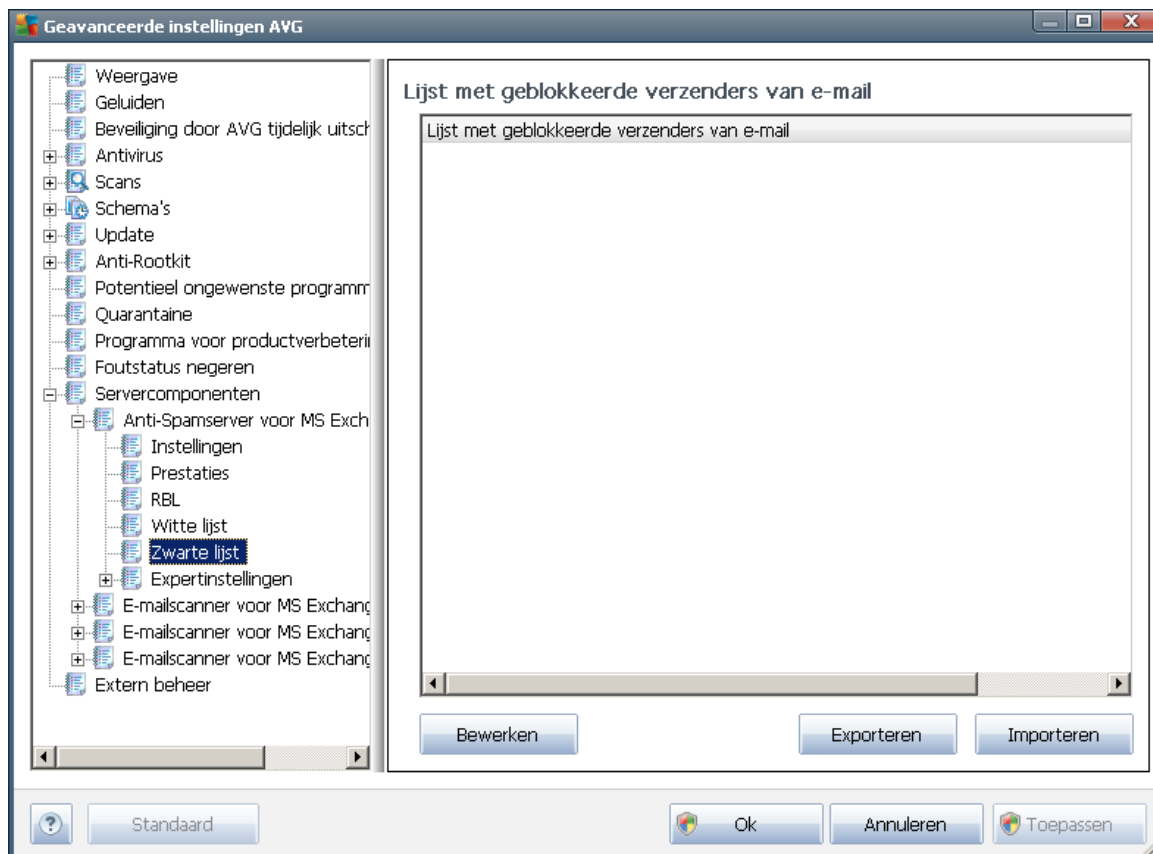
U kunt in het tekstverwerkingsgedeelte een lijst samenstellen met afzenders waarvan u zeker weet dat ze u geen ongewenste e-mail ([spam](#)) zullen sturen. U kunt ook een lijst samenstellen met domeinnamen (bijvoorbeeld *avg.com*), waarvan u weet dat ze geen spam genereren.

Als u eenmaal zo'n lijst met afzenders/domeinnamen hebt samengesteld, kunt u die op twee manieren invoeren: rechtstreeks elk e-mailadres afzonderlijk of in één keer door het importeren van de lijst. De volgende knoppen zijn beschikbaar:

- **Bewerken** – klik op deze knop om een dialoogvenster te openen waarin u handmatig een lijst met adressen kunt invoeren (u kunt ook *kopiëren en plakken*). Voeg één item (afzender, domeinnaam) per regel in.
- **Importeren** - klik op deze knop om uw bestaande e-mailadressen te importeren. Het invoerbestand mag een tekstbestand zijn (niet-opgemaakt, en op elke regel mag niet meer dan één item (adres, domeinnaam) staan) of een WAB-bestand; u kunt ook importeren vanuit het Adresboek van Windows en uit Microsoft Office Outlook.
- **Exporteren** - Als u de gegevens wilt exporteren, klikt u op deze knop. Alle gegevens worden dan naar een tekstbestand opgeslagen.

7.7. Zwarte lijst

Met de optie **Zwarte lijst** opent u een dialoogvenster met een globale lijst met geblokkeerde e-mailadressen en domeinnamen. De berichten van deze afzenders worden altijd als [spam](#) gemarkeerd.



U kunt in het tekstverwerkingsgedeelte een lijst samenstellen met afzenders waarvan u ongewenste e-mail verwacht ([spam](#)). U kunt ook een lijst met volledige domeinnamen samenstellen (zoals *spammingbedrijf.nl*), waarvan u spamberichten verwacht of ontvangt. Alle e-mailberichten die worden ontvangen van de weergegeven adressen/domeinen, worden gemarkeerd als spam.

Als u eenmaal zo'n lijst met afzenders/domeinnamen hebt samengesteld, kunt u die op twee manieren invoeren: rechtstreeks elk e-mailadres afzonderlijk of in één keer door het importeren van de lijst. De volgende knoppen zijn beschikbaar:

- **Bewerken** – klik op deze knop om een dialoogvenster te openen waarin u handmatig een lijst met adressen kunt invoeren (u kunt ook *kopiëren en plakken*). Voeg één item (afzender, domeinnaam) per regel in.
- **Importeren** - klik op deze knop om uw bestaande e-mailadressen te importeren. Het invoerbestand mag een tekstbestand zijn (niet-opgemaakt, en op elke regel mag niet meer dan één item (adres, domeinnaam) staan) of een WAB-bestand; u kunt ook importeren vanuit het Adresboek van Windows en uit Microsoft Office Outlook.



- **Exporteren** - Als u de gegevens wilt exporteren, klikt u op deze knop. Alle gegevens worden dan naar een tekstbestand opgeslagen.

7.8. Expertinstellingen

Over het algemeen is het raadzaam de standaardinstellingen aan te houden en die alleen te wijzigen als u daar een goede reden voor hebt. Wijzigen van de configuratie is voorbehouden aan experts!

Als u niettemin van mening bent dat u de configuratie van Anti-Spam op expertniveau moet wijzigen, volgt u de instructies die in de gebruikersinterface worden weergegeven. Over het algemeen is elk dialoogvenster gewijd aan één specifieke functie die u dan kunt wijzigen – de beschrijving van de functie staat steeds in datzelfde dialoogvenster:

- **Cache** – Vingerafdruk, Domeinreputatie, LegitRepute
- **Training** – max in te voeren woorden, drempel autotraining, gewicht
- **Filteren** – Taallijst, Landenlijst, Goedgekeurde IP's, Geblokkeerde IP's, Geblokkeerde landen, Geblokkeerde tekensets, Spoof-verzenders
- **RBL** – RBL-servers, Multihit, Drempel, Time-out, Max IP's
- **Internetverbinding** – Time-out, Proxyserver, Proxyserververificatie

8. AVG Settings Manager

AVG Settings Manager is een hulpprogramma dat vooral geschikt is voor kleinere netwerken, voor het kopiëren, bewerken en distribueren van een AVG-configuratie. De configuratie kan worden opgeslagen op een verwisselbaar medium (USB-stick, e.d.) en zo handmatig worden toegepast op andere stations.

Het programma maakt deel uit van de installatie van AVG en kan worden gestart via het menu Start van Windows:

Alle programma's/AVG 2012/AVG Settings Manager



- **AVG-instellingen**

- **AVG-instellingen bewerken** – het dialoogvenster openen met de instellingen van de lokale installatie van AVG. Alle wijzigingen die u in dat dialoogvenster doorvoert, gelden voor de lokale installatie van AVG.
- **AVG-instellingen laden en bewerken** – als u al een AVG-configuratiebestand (pck) hebt, kunt u het openen voor bewerking. Als u vervolgens de instellingen bevestigt door op de knop **OK** of de knop **Toepassen** te klikken worden de nieuwe instellingen in het configuratiebestand opgeslagen.

- **AVG Firewallinstellingen**

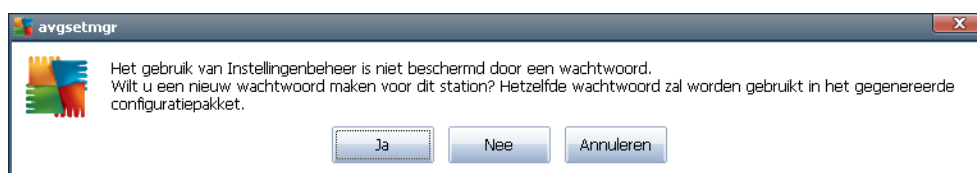
In dit gedeelte kunt u instellingen wijzigen van de lokale installatie van Firewall, of van een eerder gemaakt AVG-configuratiebestand (pck). Maar omdat het onderdeel Firewall in uw versie van AVG Email Server Edition 2012 ontbreekt, worden beide opties grijs weergegeven en zijn ze niet actief.

- **Opties voor laden**

- **Een opgeslagen set instellingen laden naar AVG** – een AVG-configuratiebestand (pck) openen en toepassen op de lokale installatie van AVG.

- **Opties opslaan**

- **Lokale AVG-instellingen opslaan in een bestand** – de instellingen van de lokale AVG-installatie opslaan in een AVG-configuratiebestand (pck). Als u geen wachtwoord hebt ingesteld voor Toegestane acties, wordt mogelijk het volgende dialoogvenster geopend:



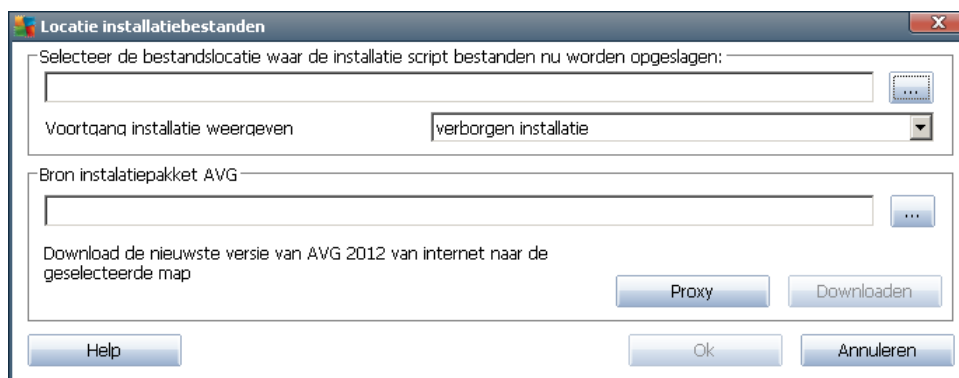
Klik op **Ja** als u nu een wachtwoord wilt instellen voor toegang tot Toegestane items en voer dan de vereiste gegevens in; bevestig de invoer. Klik op **Nee** om het maken van een wachtwoord over te slaan en door te gaan met het opslaan van de lokale AVG-configuratie in een bestand.

- **Opties klonen**

- **Identieke instellingen toepassen in het hele netwerk** – een kopie maken van de lokale AVG-installatie in een installatiepakket met eigen instellingen. In de kloon worden de meeste AVG-instellingen opgeslagen, met uitzondering van:

- ✓ *Taalinstellingen*
- ✓ *Instellingen voor geluiden*
- ✓ *Lijst Toegestaan en uitzonderingen op Potentieel ongewenste programma's van het onderdeel Identity Protection.*

Selecteer eerst een map waarin het installatiescript moet worden opgeslagen.



Maak dan een keuze in de vervolgkeuzelijst:

- ✓ *Verborgen installatie* – tijdens de installatie worden geen meldingen weergegeven.



- ✓ *Alleen de voortgang van de installatie weergeven* – De gebruiker hoeft zich niet met de installatie te bemoeien, maar de voortgang wordt wel weergegeven
- ✓ *Installatiewizard weergeven* – de installatie wordt weergegeven en de gebruiker moet handmatig alle stappen bevestigen

Klik op de knop **Downloaden** om het meest recente installatiepakket van AVG te downloaden van de website van AVG naar de geselecteerde map, of plaats het installatiepakket handmatig in die map.

Klik op de knop **Proxyserver** om instellingen voor een proxyserver op te geven als dat in uw netwerk vereist is voor een verbinding.

Klik op **OK** om het kloonproces, dat weinig tijd in beslag neemt, te starten. Mogelijk wordt nog een dialoogvenster geopend voor het instellen van een wachtwoord voor Toegestane items (zie hiervoor). Als de procedure is voltooid, dient er samen met andere bestanden een bestand **AvgSetup.bat** in de geselecteerde map te staan. Als u het bestand **AvgSetup.bat** uitvoert, zal AVG worden geïnstalleerd met de parameters die u hebt ingesteld.



9. Veelgestelde vragen en technische ondersteuning

Mocht u problemen ondervinden met AVG, op zakelijk of technisch gebied, raadpleeg dan de sectie met **veelgestelde vragen (FAQ)** op de website van AVG: <http://www.avg.com>.

Vindt u op die manier geen oplossing, neem dan via e-mail contact op met de technische ondersteuningsdienst. Gebruik daarvoor het contactformulier dat u kunt oproepen via het menu **Help / Online Help**.