McAfee®

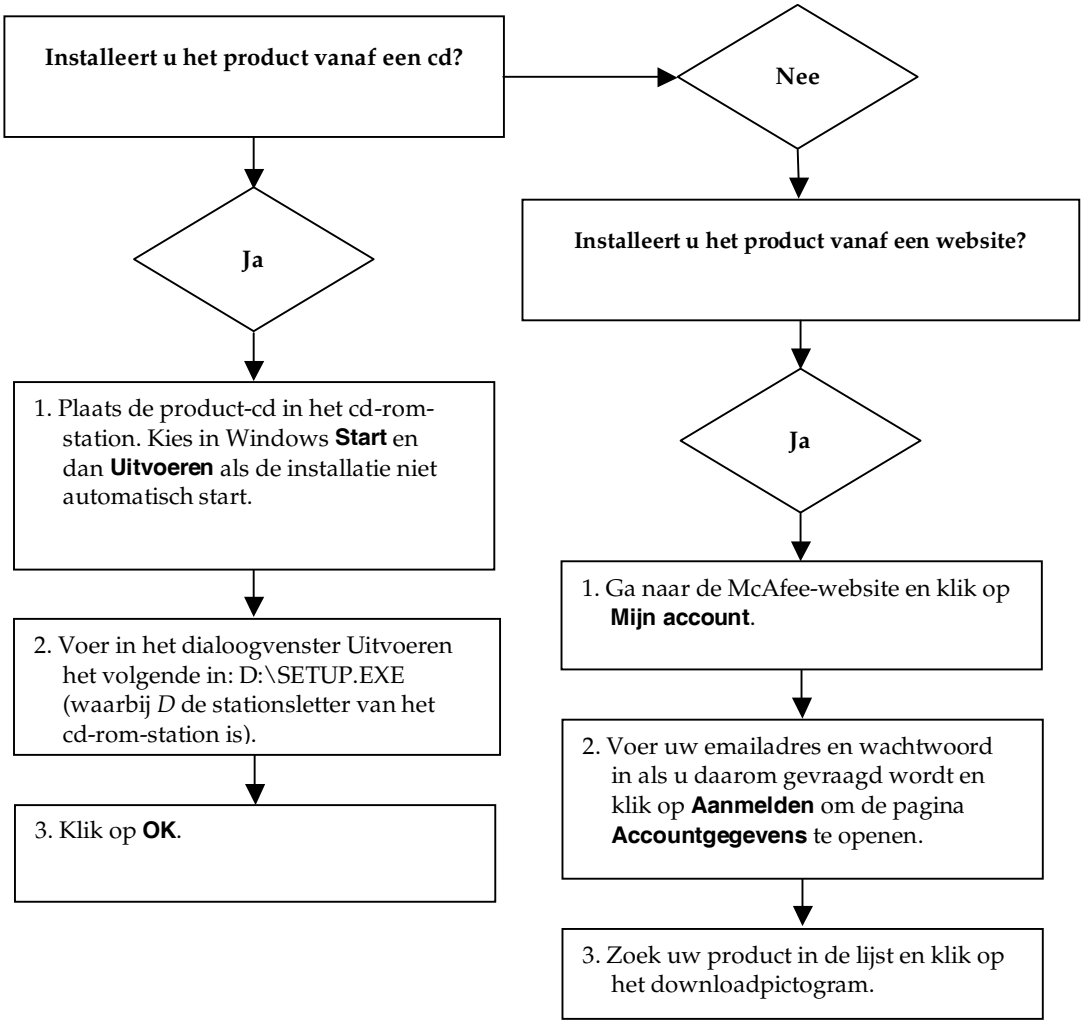
virusscan®

Gebruikershandleiding

McAfee®

Aan de slag

Als u het product installeert vanaf een cd of een website, kunt u deze handige pagina afdrukken ter referentie.



Meer informatie

Als u de Gebruikershandleidingen op de product-cd wilt bekijken, moet Acrobat Reader zijn geïnstalleerd. Als dit niet het geval is, kunt u Adobe Acrobat Reader nu installeren vanaf de product-cd van McAfee.

1. Plaats de product-cd in het cd-rom-station.
2. Open de Verkenner: Klik op **Start** op het Windows-bureaublad en klik vervolgens op **Zoeken**.
3. Zoek naar de map Manuals en dubbelklik op het PDF-bestand van de gebruikershandleiding die u wilt openen.

Voordelen van registratie

McAfee raadt u aan om de eenvoudige registratiestappen in het product uit te voeren om uw registratiegegevens rechtstreeks naar ons te verzenden. Als u zich registreert, kunt u rechtstreeks contact opnemen met een medewerker van de technische ondersteuning. Daarnaast hebt u recht op:

- Gratis elektronische ondersteuning
- Updates voor virusdefinitiebestanden (.DAT) tot een jaar na installatie als u de VirusScan-software aanschaft

  Ga naar nl.mcafee.com om te zien wat u betaalt voor een extra jaar updates voor virusdefinitiebestanden.
- 60 dagen garantie: uw software-cd wordt vervangen bij een defect of beschadiging
- Als u SpamKiller aanschaft, ontvangt u een jaar lang filterupdates na installatie van SpamKiller

  Ga naar nl.mcafee.com om te zien wat u betaalt voor een extra jaar filterupdates.
- Updates voor McAfee Internet Security Suite tot een jaar na aanschaf van de MIS-software

  Ga naar nl.mcafee.com om te zien wat u betaalt voor een extra jaar updates voor inhoud.

Technische ondersteuning

Ga voor technische ondersteuning naar http://www.mcafeehulp.com/.

Via onze ondersteuningssite hebt u 24 uur per dag toegang tot de gebruiksvriendelijke antwoordwizard voor antwoorden op veelgestelde vragen.

Ervaren gebruikers kunnen ook gebruikmaken van onze geavanceerde opties, zoals een trefwoordenindex en Help-structuur. Als u geen oplossing vindt voor uw probleem, hebt u eveneens toegang tot de gratis chat- en e-mailvoorzieningen. Met behulp van deze voorzieningen kunt u via internet snel en gratis contact opnemen met onze ondersteuningsmedewerkers. U kunt echter ook telefonische ondersteuning krijgen. Voor de contactgegevens gaat u naar http://www.mcafeehulp.com/.

Inhoud

Aan de slag 1

Welkom bij McAfee VirusScan.

McAfee VirusScan is een antivirusservice voor abonnees, die uitgebreide, betrouwbare en up-to-date beveiliging tegen virussen biedt. VirusScan is gebaseerd op de veelgeprezen scantechnologie van McAfee en biedt bescherming tegen virussen, wormen, Trojaanse paarden, schadelijke scripts en hybride aanvallen.

Als u zich op VirusScan abonneert, beschikt u over de volgende voorzieningen:

ActiveShield: bestanden scannen zodra deze door u of de computer worden gebruikt.

Scan: naar virussen of mogelijk ongewenste programma's zoeken op vaste schijven en diskettes en in afzonderlijke mappen en bestanden.

Quarantaine: geïnfecteerde en verdachte bestanden coderen en tijdelijk isoleren in de quarantainemap totdat de meest geschikte actie kan worden uitgevoerd.

Opsporing van schadelijke activiteiten: uw computer controleren op virusachtige activiteiten veroorzaakt door wormachtige activiteiten en schadelijke scripts.

Nieuwe functies

Deze versie van VirusScan bevat de volgende nieuwe functies:

- **Detectie en opschoning van spyware en adware**
  VirusScan detecteert en verwijdert spyware, adware en andere programma's die uw privacy in gevaar brengen en de prestaties van uw computer nadelig beïnvloeden.
- **Dagelijkse automatische updates**
  Dagelijkse automatische updates van de VirusScan beschermen u tegen de allernieuwste bekende en onbekende virussen.
- **Snel scannen op de achtergrond**
  Snelle, onopvallende scans detecteren en vernietigen virussen, Trojaanse paarden, wormen, spyware, adware, dialers en andere schadelijke programma's zonder uw werk te onderbreken.
- **Real-time beveiligingswaarschuwingen**
  Door middel van beveiligingswaarschuwingen wordt u op de hoogte gebracht van nieuwe virusuitbraken en veiligheidsrisico's en krijgt u de mogelijkheid aangeboden de bedreigingen te verwijderen, neutraliseren of er meer informatie over te lezen.

- **Detecteren en opschonen op meerdere ingangspunten**
  VirusScan bewaakt en schoont uw computer op de belangrijkste ingangspunten op: e-mail, inkomende bijlagen bij expresberichten en downloads van internet.
- **E-mailbewaking op wormachtige activiteiten**
  WormStopper™ controleert op verdachte bulkmailactiviteit en voorkomt dat virussen en wormen zich via e-mail kunnen verspreiden naar andere computers.
- **Scriptbewaking op wormachtige activiteiten**
  ScriptStopper™ controleert op verdachte scriptuitvoeringen en voorkomt dat virussen en wormen zich via e-mail kunnen verspreiden naar andere computers.
- **Gratis technische ondersteuning via expresberichten en e-mail**
  Altijd technische ondersteuning voor een snelle en eenvoudig hulp door middel van expresberichten en e-mail.

Systeemvereisten

- Microsoft® Windows 98, Windows Me, Windows 2000 of Windows XP
- Personal computer met Pentium-compatibele processor
  Windows 98, 2000: 133 MHz of hoger
  Windows Me: 150 MHz of hoger
  Windows XP (Home en Professional): 300 MHz of hoger
- RAM
  Windows 98, Me en 2000: 64 MB
  Windows XP (Home en Professional): 128 MB
- 40 MB aan ruimte op de vaste schijf
- Microsoft® Internet Explorer 5.5 of hoger

Opmerking
Als u een upgrade wilt uitvoeren naar de nieuwste versie van Internet Explorer, gaat u naar de Microsoft-website op http://www.microsoft.nl/.

Ondersteunde e-mailprogramma's

- POP3 (Outlook Express, Outlook, Eudora, Netscape)

Ondersteunde programma's voor expresberichten

- AOL Instant Messenger 2.1 of hoger
- Yahoo Messenger 4.1 of hoger
- Microsoft Windows Messenger 3.6 of hoger
- MSN Messenger 6.0 of hoger

VirusScan testen

U kunt het beste de installatie testen voordat u VirusScan voor het eerst gaat gebruiken. Voer de onderstaande stappen uit om de functies ActiveShield en Scannen afzonderlijk te testen.

ActiveShield testen

Opmerking
Klik op **VirusScan testen** op het tabblad VirusScan in SecurityCenter om ActiveShield te testen en een on line overzicht van veelgestelde vragen te zien waarin de stappen daarvoor worden uitgelegd.

Ga als volgt te werk om ActiveShield te testen:

1. Ga met uw webbrowser naar http://www.eicar.com/.
2. Klik op de koppeling **The AntiVirus testfile eicar.com**.
3. Ga naar het onderste gedeelte van de pagina. U ziet vier koppelingen onder **Download area**.
4. Klik op **eicar.com**.

Als ActiveShield naar behoren werkt, wordt het bestand eicar.com direct opgespoord nadat u op de koppeling hebt geklikt. U kunt proberen geïnfecteerde bestanden te verwijderen of in quarantaine te plaatsen om na te gaan hoe ActiveShield omgaat met virussen. Zie *Beveiligingswaarschuwingen begrijpen* op pagina 24 voor meer informatie.

Scannen testen

Als u Scannen wilt testen, moet u ActiveShield uitschakelen om te voorkomen dat deze de geïnfecteerde bestanden vóór Scannen detecteert. Vervolgens moet u de testbestanden downloaden.

Ga als volgt te werk om de testbestanden te downloaden:

1. Schakel ActiveShield uit: Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **Uitschakelen**.
2. Download de EICAR-testbestanden van de EICAR-website:
   a. Ga naar http://www.eicar.com/.
   b. Klik op de koppeling **The AntiVirus testfile eicar.com**.

c Ga naar het onderste gedeelte van de pagina. U ziet de volgende koppelingen onder **Download area**:

eicar.com bevat een regel tekst die door VirusScan zal worden gezien als een virus.

eicar.com.txt (optioneel) is hetzelfde bestand maar met een andere bestandsnaam. Deze koppeling is voor gebruikers die problemen ondervinden bij het downloaden van het eerste bestand. Wijzig de naam van het bestand in eicar.com nadat u het hebt gedownload.

eicar_com.zip is een kopie van het testvirus in een ZIP-bestand (een WinZip™-bestandsarchief).

eicarcom2.zip is een kopie van het testvirus in een ZIP-bestand dat zich weer in een ander ZIP-bestand bevindt.

d Klik op een koppeling om het bijbehorende bestand te downloaden. Voor elk bestand wordt het dialoogvenster **Bestand downloaden** weergegeven.

e Klik op **Opslaan**, klik op de knop **Nieuwe map maken** en noem de map vervolgens **VSO Scan**.

f Dubbelklik op de map **VSO Scan** en klik vervolgens op **Opslaan** in elk van de dialoogvensters **Opslaan als**.

3 Sluit Internet Explorer wanneer u klaar bent met het downloaden van de bestanden.

4 Schakel ActiveShield in: Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **Inschakelen**.

Ga als volgt te werk om Scannen te testen:

1 Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **Scannen op virussen**.

2 Ga in de directorystructuur in het linkerdeelvenster van het dialoogvenster naar de map **VSO Scan** waarin u de bestanden hebt opgeslagen:

a Klik op de **+** naast het pictogram voor station C.

b Klik op de map **VSO Scan** om deze te markeren (klik niet op de **+** ernaast).

Scannen controleert dan alleen de desbetreffende map op virussen. U kunt de bestanden desgewenst ook naar willekeurige locaties op de vaste schijf verplaatsen om na te gaan of Scannen de bestanden ook in dat geval weet op te sporen.

3 Controleer of alle opties zijn geselecteerd in het gedeelte **Scanopties** van het dialoogvenster **Scannen op virussen**.

4 Klik op **Scannen** rechtsonder in het dialoogvenster.

VirusScan scant de map **VSO Scan**. De EICAR-testbestanden die u in de map hebt opgeslagen, verschijnen in de **Lijst met gedetecteerde bestanden**. Als dat het geval is, werkt Scannen correct.

U kunt proberen geïnfecteerde bestanden te verwijderen of in quarantaine te plaatsen om na te gaan hoe Scannen omgaat met virussen. Zie *Opsporen van bedreigingen begrijpen* op pagina 32 voor meer informatie.

McAfee SecurityCenter gebruiken

McAfee SecurityCenter is de centrale plaats voor uw beveiliging, die u eenvoudig opent via het pictogram op de taakbalk of het bureaublad van Windows. Met SecurityCenter kunt u de volgende nuttige taken uitvoeren:

- Gratis beveiligingsanalyse voor uw computer.
- Al uw McAfee-abonnementen starten, beheren en configureren met één pictogram.
- Voortdurend bijgewerkte viruswaarschuwingen en de meest recente productinformatie bekijken.
- Snelkoppelingen naar veelgestelde vragen en accountgegevens op de McAfee-website.

Opmerking
Klik op **Help** in het dialoogvenster **SecurityCenter** voor meer informatie over de functies van deze toepassing.

Wanneer SecurityCenter actief is en alle op de computer geïnstalleerde McAfee-voorzieningen zijn ingeschakeld, wordt een rood M-pictogram weergegeven in het systeemvak van Windows. Het systeemvak is het gebied in de taakbalk waar u ook de tijd ziet.

Als één of meer op uw computer geïnstalleerde McAfee-toepassingen is uitgeschakeld, wordt het pictogram van McAfee zwart.

Ga als volgt te werk om McAfee SecurityCenter te openen:

1 Klik met de rechter muisknop op het McAfee-pictogram.

2 Klik op **SecurityCenter openen**.

U kunt als volgt toegang krijgen tot een functie van VirusScan:

1 Klik met de rechter muisknop op het McAfee-pictogram.

2 Kies **VirusScan** en klik op de gewenste functie.

McAfee VirusScan gebruiken 2

ActiveShield gebruiken

Wanneer ActiveShield wordt gestart (in het computergeheugen wordt geladen) en ingeschakeld, biedt dit programma voortdurende bescherming van uw computer. ActiveShield scant bestanden zodra deze door de computer of door uzelf worden gebruikt. Wanneer er een geïnfecteerd bestand wordt aangetroffen, probeert ActiveShield dit bestand automatisch op te schonen. Als dit niet mogelijk is, geeft ActiveShield u de keuze tussen het bestand in quarantaine plaatsen of het verwijderen.

ActiveShield in- en uitschakelen

ActiveShield wordt standaard gestart (geladen in het geheugen van de computer) en ingeschakeld (wat wordt aangeduid met het rode pictogram in het systeemvak van Windows) zodra u de computer na het installatieproces opnieuw hebt opgestart.

Als ActiveShield is gestopt (niet wordt geladen) of is uitgeschakeld (het pictogram is zwart), kunt u deze functie handmatig starten of deze configureren om automatisch te starten wanneer Windows wordt gestart.

ActiveShield inschakelen

Ga als volgt te werk om ActiveShield alleen voor deze Windows-sessie in te schakelen:

Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **Inschakelen**. Het McAfee-pictogram wordt rood .

Als ActiveShield nog steeds is geconfigureerd om te starten wanneer Windows wordt gestart, krijgt u een bericht dat u nu beschermd bent tegen virussen. Als dit niet het geval is, verschijnt er een dialoogvenster waarin u ActiveShield kunt configureren om te starten wanneer Windows wordt gestart (Afbeelding 2-1 op pagina 14).

ActiveShield uitschakelen

Ga als volgt te werk om ActiveShield alleen voor de huidige Windows-sessie uit te schakelen:

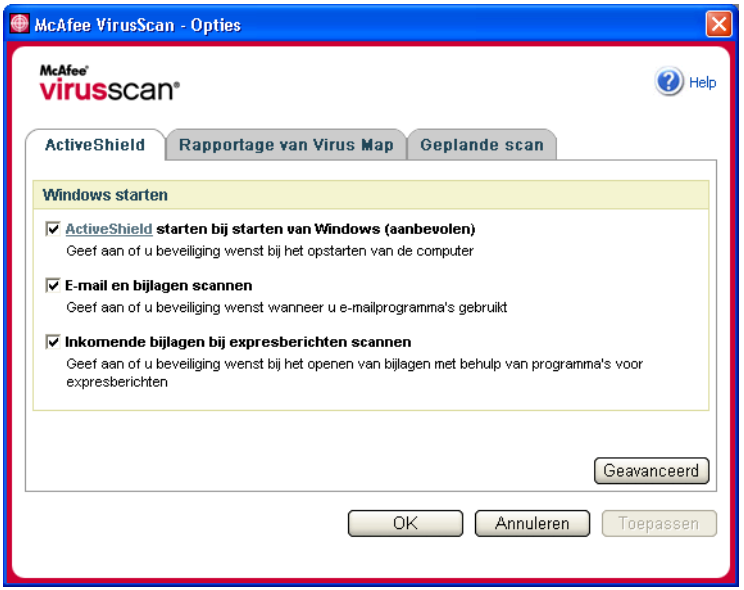
1. Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **Uitschakelen**.
2. Klik op **Ja** om te bevestigen.

   Het McAfee-pictogram wordt zwart .

Als ActiveShield nog steeds is geconfigureerd om te starten wanneer Windows wordt gestart, is uw computer weer beveiligd tegen virussen zodra u de computer opnieuw opstart.

ActiveShield-opties configureren

U kunt de ActiveShield-opties voor starten en scannen wijzigen op het tabblad **ActiveShield** van het dialoogvenster **Opties** van VirusScan (Afbeelding 2-1). U opent dit venster door op het McAfee-pictogram in het systeemvak van Windows te klikken.



Afbeelding 2-1. ActiveShield-opties

ActiveShield starten

ActiveShield wordt standaard gestart (geladen in het geheugen van de computer) en ingeschakeld (het pictogram is rood) zodra u de computer na het installatieproces opnieuw hebt opgestart.

Als ActiveShield is gestopt (het pictogram is zwart), kunt u deze functie configureren om automatisch te starten wanneer Windows wordt gestart (aanbevolen).

> **Opmerking**
> Tijdens updates van VirusScan wordt ActiveShield mogelijk tijdelijk afgesloten door de **Wizard Update**, zodat er nieuwe bestanden kunnen worden geïnstalleerd. ActiveShield wordt weer gestart nadat u in de **Wizard Update** op **Voltooien** hebt geklikt.

Ga als volgt te werk om ActiveShield automatisch te laten starten wanneer Windows wordt gestart:

1. Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **Opties**.

   Het dialoogvenster **Opties** van VirusScan wordt geopend (Afbeelding 2-1 op pagina 14).

2. Schakel het selectievakje **ActiveShield starten bij starten van Windows (aanbevolen)** in en klik op **Toepassen** om de wijzigingen op te slaan.

3. Klik op **OK** om te bevestigen en klik vervolgens nogmaals op **OK**.

ActiveShield stoppen

> **Waarschuwing**
> Als u ActiveShield stopt, is uw computer niet beschermd tegen virussen. Als u ActiveShield om een andere reden dan voor het bijwerken van VirusScan moet stoppen, zorg er dan voor dat de computer niet is verbonden met internet.

Ga als volgt te werk om ActiveShield niet te laten starten wanneer Windows wordt gestart:

1. Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **Opties**.

   Het dialoogvenster **Opties** van VirusScan wordt geopend (Afbeelding 2-1 op pagina 14).

2. Schakel het selectievakje **ActiveShield starten bij starten van Windows (aanbevolen)** uit en klik op **Toepassen** om de wijzigingen op te slaan.

3. Klik op **OK** om te bevestigen en klik vervolgens nogmaals op **OK**.

E-mailberichten en bijlagen scannen

Het scannen van e-mail en het automatisch opschonen worden standaard ingeschakeld via de optie **E-mail en bijlagen scannen** (Afbeelding 2-1 op pagina 14).

Wanneer deze optie is ingeschakeld, worden inkomende (POP3) en uitgaande (SMTP) e-mailberichten en bijlagen automatisch door ActiveShield gescand en indien nodig opgeschoond voor de meestgebruikte e-mailclients, zoals:

- Microsoft Outlook Express 4.0 of hoger
- Microsoft Outlook 97 of hoger
- Netscape Messenger 4.0 of hoger
- Netscape Mail 6.0 of hoger
- Eudora Light 3.0 of hoger
- Eudora Pro 4.0 of hoger
- Eudora 5.0 of hoger
- Pegasus 4.0 of hoger

Opmerking

Het scannen van e-mailberichten wordt niet ondersteund voor de volgende e-mailclients: webmail, IMAP, AOL, POP3 SSL en Lotus Notes. E-mailbijlagen worden echter door ActiveShield gescand wanneer ze worden geopend.

Als u de optie **E-mail en bijlagen scannen** uitschakelt, worden de opties voor E-mail Scan en WormStopper (Afbeelding 2-2 op pagina 17) automatisch uitgeschakeld. Als u het scannen van uitgaande e-mailberichten uitschakelt, worden de opties van WormStopper automatisch uitgeschakeld.

Als u de opties voor het scannen van e-mailberichten wijzigt, moet u het e-mailprogramma opnieuw starten om de wijzigingen te voltooien.

Inkomende e-mailberichten

Als een inkomend e-mailbericht of een bijlage is geïnfecteerd, voert ActiveShield de volgende stappen uit:

- Er wordt geprobeerd het geïnfecteerde bericht op te schonen
- Er wordt geprobeerd een e-mailbericht dat niet kan worden opgeschoond in quarantaine te plaatsen of te verwijderen
- Er wordt een waarschuwing in het inkomende e-mailbericht opgenomen, dat informatie bevat over de bewerkingen die zijn uitgevoerd om de infectie te verwijderen

Uitgaande e-mailberichten

Als een uitgaand e-mailbericht of een bijlage is geïnfecteerd, voert ActiveShield de volgende stappen uit:

- Er wordt geprobeerd het geïnfecteerde bericht op te schonen
- Er wordt geprobeerd een e-mailbericht dat niet kan worden opgeschoond in quarantaine te plaatsen of te verwijderen

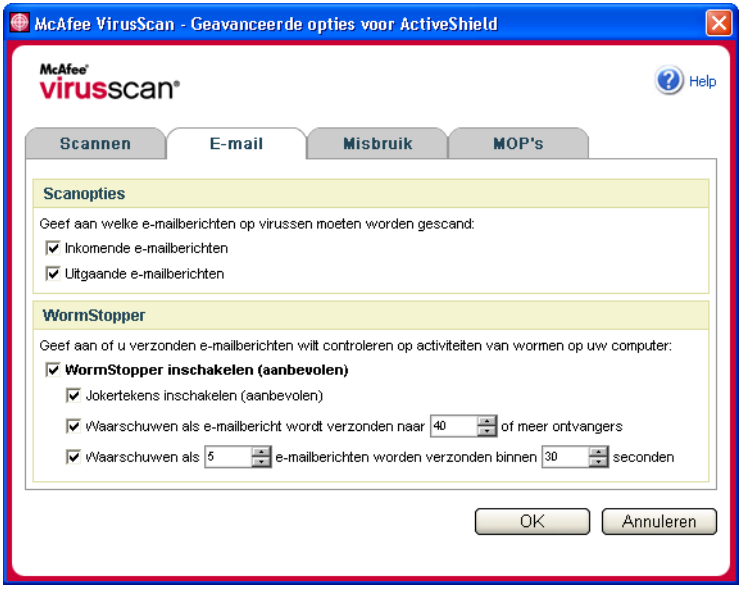
> **Opmerking**
> Raadpleeg de on line Help voor meer informatie over scanfouten voor uitgaande e-mailberichten.

Het scannen van e-mail uitschakelen

ActiveShield scant standaard zowel inkomende als uitgaande e-mailberichten. Als u echter meer controle wilt, kunt u ActiveShield zodanig instellen dat alleen uw inkomende of uitgaande e-mailberichten worden gescand.

Ga als volgt te werk om het scannen van inkomende of uitgaande e-mailberichten uit te schakelen:

1. Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **Opties**.
2. Klik op **Geavanceerd** en klik vervolgens op het tabblad **E-mail** (Afbeelding 2-2).
3. Schakel **Inkomende e-mailberichten** of **Uitgaande e-mailberichten** uit en klik vervolgens op **OK**.



Afbeelding 2-2. Geavanceerde opties voor ActiveShield - tabblad E-mail

Scannen op wormen

VirusScan controleert de computer op verdachte activiteiten die erop kunnen wijzen dat er een virusdreiging op de computer aanwezig is. Terwijl VirusScan virussen opschoont, voorkomt WormStopper™ dat virussen en wormen zich verder kunnen verspreiden.

Een "worm" op de computer is een zichzelf vermenigvuldigend virus dat zich in het actieve geheugen nestelt en mogelijk via e-mail kopieën van zichzelf verspreidt. Zonder WormStopper zou u wormen alleen opmerken als hun ongecontroleerde vermenigvuldiging uw systeembronnen gebruikt, waardoor de computer langzamer wordt of taken gestopt worden.

Met het beveiligingsmechanisme van WormStopper worden schadelijke activiteiten opgespoord. Bovendien wordt er melding gemaakt van deze activiteiten en worden de activiteiten geblokkeerd. Verdachte activiteiten zijn bijvoorbeeld de volgende bewerkingen:

- Een poging e-mailberichten door te sturen naar een groot gedeelte van uw adresboek
- Pogingen om meerdere e-mailberichten vlak na elkaar door te sturen

Als u ActiveShield configureert met de standaardoptie **WormStopper inschakelen (aanbevolen)** in het dialoogvenster **Geavanceerde opties**, wordt e-mailactiviteit door WormStopper gecontroleerd op verdachte patronen en ontvangt u een waarschuwing wanneer een specifiek aantal e-mailberichten of geadresseerden binnen een opgegeven tijdsperiode is overschreden.

Ga als volgt te werk om ActiveShield in te stellen voor het scannen van verzonden e-mailberichten op wormachtige activiteiten:

1. Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **Opties**.
2. Klik op **Geavanceerd** en klik vervolgens op het tabblad **E-mail**.
3. Klik op **WormStopper inschakelen (aanbevolen)** (Afbeelding 2-3).

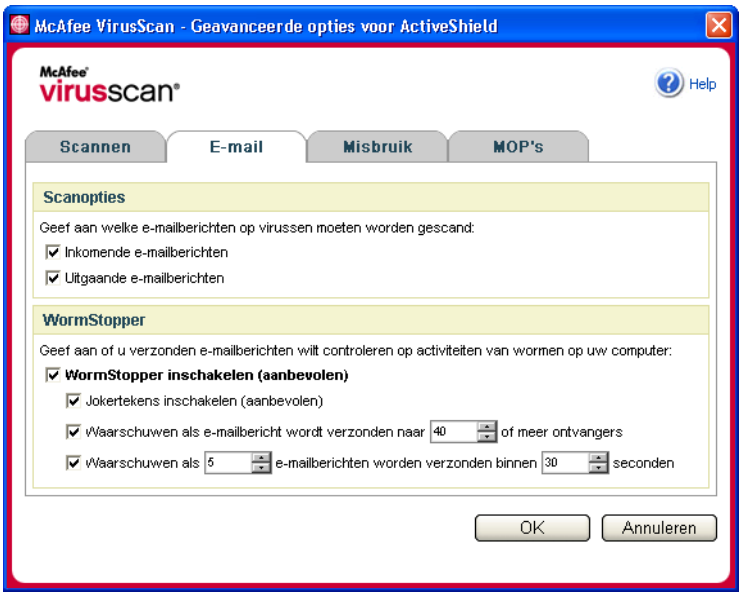
   De volgende gedetailleerde opties zijn standaard ingeschakeld:

   - Patroonherkenning voor het opsporen van verdachte activiteiten
   - Waarschuwen wanneer een e-mailbericht wordt verzonden naar 40 of meer ontvangers
   - Waarschuwen wanneer 5 of meer e-mailberichten worden verzonden binnen 30 seconden

     Opmerking
     Als u het aantal ontvangers of seconden wijzigt voor het controleren van verzonden e-mailberichten, kan dit leiden tot onjuiste detectie. McAfee raadt u daarom aan op **Nee** te klikken om de standaardinstellingen te behouden. Klik op **Ja** als u de standaardinstelling wilt wijzigen.

U kunt deze optie automatisch inschakelen na de eerste keer dat er een mogelijke worm is gevonden (zie *Mogelijke wormen beheren* op pagina 25 voor meer informatie):

- Verdachte uitgaande e-mailberichten automatisch blokkeren



Afbeelding 2-3. Geavanceerde opties voor ActiveShield - tabblad E-mail

Inkomende bijlagen bij expresberichten scannen

Het scannen van bijlagen in expresberichten is standaard ingeschakeld via de optie **Inkomende bijlagen bij expresberichten scannen** (Afbeelding 2-1 op pagina 14).

Wanneer deze optie is ingeschakeld, worden inkomende bijlagen in expresberichten automatisch door VirusScan gescand en indien nodig opgeschoond voor de meestgebruikte programma's voor expresberichten, zoals:

- MSN Messenger 6.0 of hoger
- Yahoo Messenger 4.1 of hoger
- AOL Instant Messenger 2.1 of hoger

Opmerking
Voor uw eigen bescherming kunt u de optie voor het automatisch opschonen van inkomende bijlagen in expresberichten niet uitschakelen.

Als er een geïnfecteerde bijlage wordt aangetroffen in een expresbericht, voert VirusScan de volgende stappen uit:

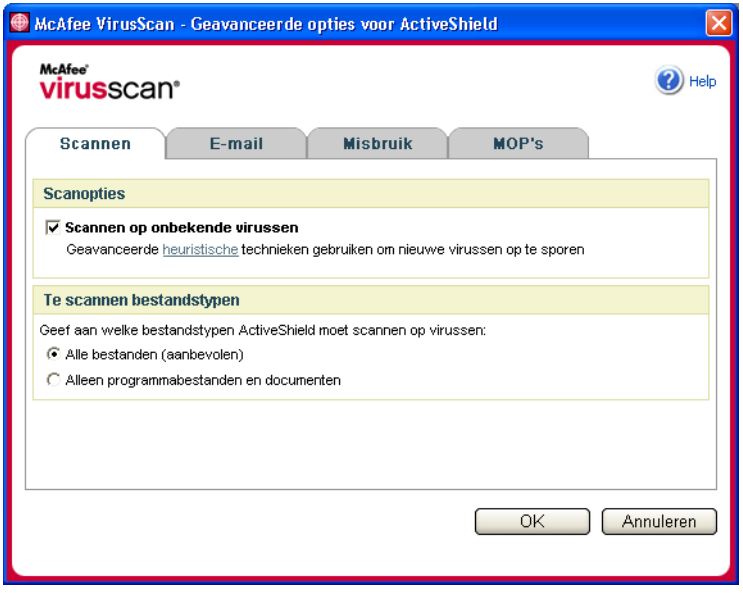
- Er wordt geprobeerd het geïnfecteerde bericht op te schonen
- U wordt gevraagd of u een bericht dat niet kan worden opgeschoond in quarantaine wilt plaatsen of wilt verwijderen

Alle bestanden scannen

Als u ActiveShield configureert met de standaardoptie **Alle bestanden (aanbevolen)**, worden alle bestandstypen die door de computer worden gebruikt, gescand wanneer ze door de computer worden geopend. Wanneer deze optie is ingeschakeld, maakt u zo grondig mogelijk gebruik van de scanfunctie.

Ga als volgt te werk om ActiveShield in te stellen voor het scannen van alle bestandstypen:

1. Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **Opties**.
2. Klik op **Geavanceerd** en klik vervolgens op het tabblad **Scannen** (Afbeelding 2-4 op pagina 20).
3. Klik op **Alle bestanden (aanbevolen)** en klik vervolgens op **OK**.



Afbeelding 2-4. Geavanceerde opties voor ActiveShield - tabblad Scannen

Alleen programmabestanden en documenten scannen

Als u ActiveShield configureert voor het gebruik van de optie **Alleen programmabestanden en documenten**, worden alleen programmabestanden en documenten gescand en geen andere bestanden die door de computer worden gebruikt. Het meest recente virushandtekeningbestand (DAT-bestand) bepaalt welke bestandstypen door ActiveShield worden gescand. Ga als volgt te werk om alleen programmabestanden en documenten te scannen in ActiveShield:

1. Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **Opties**.
2. Klik op **Geavanceerd** en klik vervolgens op het tabblad **Scannen** (Afbeelding 2-4).
3. Klik op **Alleen programmabestanden en documenten** en vervolgens op **OK**.

Scannen op onbekende virussen

Als u ActiveShield configureert met de standaardoptie **Scannen op onbekende virussen (aanbevolen)** , gebruikt deze optie geavanceerde heuristische technieken waarmee wordt geprobeerd de bestanden te vergelijken met bestaande virussen, terwijl er ook wordt gelet op signalen van onbekende virussen in de bestanden.

Ga als volgt te werk om ActiveShield in te stellen voor het scannen op onbekende virussen:

1. Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **Opties**.
2. Klik op **Geavanceerd** en klik vervolgens op het tabblad **Scannen** (Afbeelding 2-4).
3. Klik op **Scannen op onbekende virussen (aanbevolen)** en vervolgens op **OK**.

Scannen op scripts

VirusScan controleert de computer op verdachte activiteiten die erop kunnen wijzen dat er een virusdreiging op de computer aanwezig is. Terwijl VirusScan virussen opschoont, voorkomt ScriptStopper™ dat Trojaanse paarden scripts kunnen uitvoeren waardoor virussen zich verder kunnen verspreiden.

Een "Trojaans paard" is een schadelijk programma dat zich voordoet als een bonafide toepassing. Trojaanse paarden zijn geen virussen omdat ze zichzelf niet vermenigvuldigen, maar ze kunnen even schadelijk zijn.

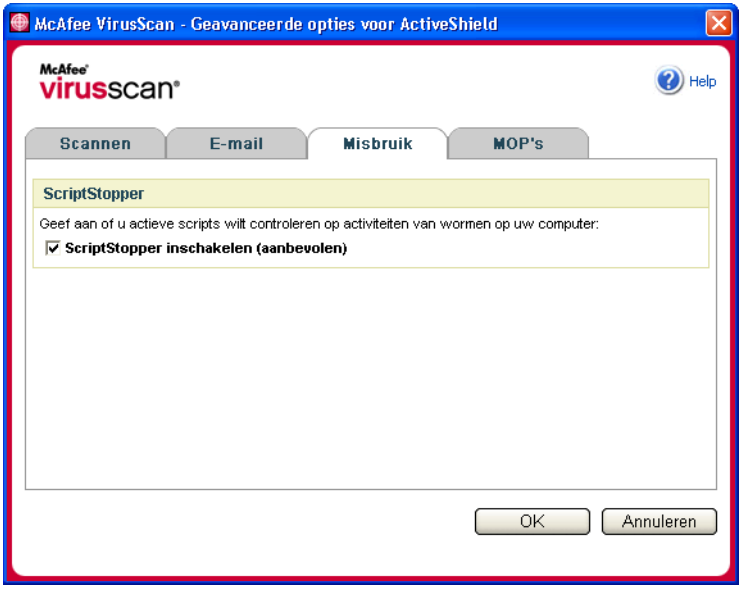
Met het beveiligingsmechanisme van ScriptStopper worden schadelijke activiteiten opgespoord. Bovendien wordt er melding gemaakt van deze activiteiten en worden de activiteiten geblokkeerd. Verdachte activiteiten zijn bijvoorbeeld de volgende bewerkingen op uw computer:

- Een actief script waarmee bestanden worden gemaakt, gekopieerd of verwijderd of waarmee het Windows-register wordt geopend

Als u ActiveShield configureert met de standaardoptie **ScriptStopper inschakelen (aanbevolen)** in het dialoogvenster **Geavanceerde opties**, wordt scriptactiviteit door ScriptStopper gecontroleerd op verdachte patronen en ontvangt u een waarschuwing wanneer een specifiek aantal e-mailberichten of geadresseerden binnen een opgegeven tijdsperiode is overschreden.

Ga als volgt te werk om ActiveShield in te stellen voor het scannen van uitgevoerde scripts op wormachtige activiteiten:

1. Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **Opties**.
2. Klik op **Geavanceerd** en klik vervolgens op het tabblad **Misbruik** (Afbeelding 2-5).
3. Klik op **ScriptStopper inschakelen (aanbevolen)** en klik vervolgens op **OK**.



Afbeelding 2-5. Geavanceerde opties voor ActiveShield - tabblad Misbruik

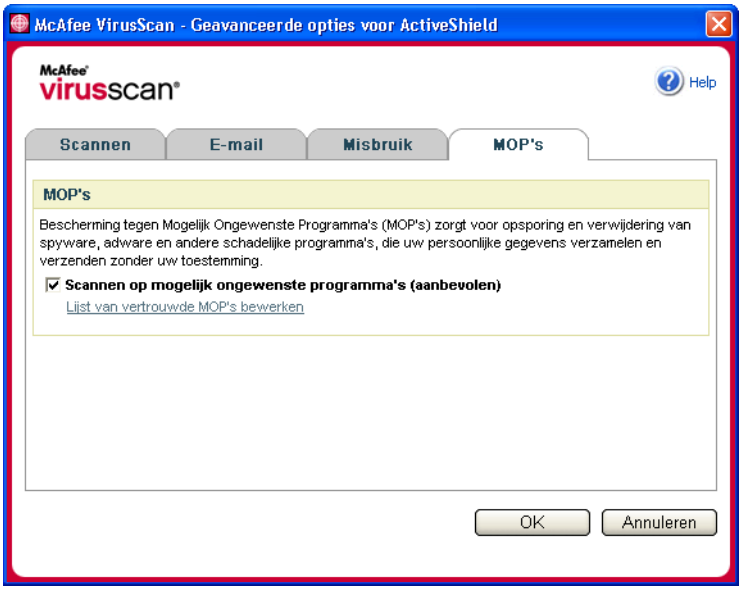
Scannen op mogelijk ongewenste programma's (MOP's)

Opmerking
Als McAfee AntiSpyware is geïnstalleerd op uw computer, dan controleert deze alle activiteiten van mogelijk ongewenste programma's. Open McAfee AntiSpyware om de opties te configureren.

Als u ActiveShield configureert met de standaardoptie **Scannen op mogelijk ongewenste programma's (aanbevolen)** in het dialoogvenster **Geavanceerde opties**, worden spyware, adware en andere schadelijke programma's die uw persoonlijke gegevens zonder uw toestemming verzamelen en verzenden, snel opgespoord, geblokkeerd en verwijderd.

Ga als volgt te werk om ActiveShield in te stellen voor het scannen op MOP's:

1. Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **Opties**.
2. Klik op **Geavanceerd** en klik vervolgens op het tabblad **MOP's** (Afbeelding 2-6).
3. Klik op **Scannen op mogelijk ongewenste programma's (aanbevolen)** en vervolgens op **OK**.



Afbeelding 2-6. Geavanceerde ActiveShield-opties - tabblad MOP's

Beveiligingswaarschuwingen begrijpen

Als ActiveShield een virus vindt, wordt er een viruswaarschuwing weergegeven dat lijkt op Afbeelding 2-7. Bij de meeste virussen, Trojaanse paarden en wormen wordt het bestand automatisch door ActiveShield opgeschoond en wordt u gewaarschuwd. ActiveShield spoort mogelijk ongewenste programma's (MOP's) op, blokkeert ze automatisch en waarschuwt u.

Afbeelding 2-7. Viruswaarschuwing

U kunt vervolgens zelf bepalen hoe geïnfecteerde bestanden, geïnfecteerde e-mailberichten, verdachte scripts, mogelijke wormen of MOP's moeten worden beheerd en of geïnfecteerde bestanden voor onderzoek naar het McAfee AVERT-team moeten worden verzonden.

Als extra bescherming vraagt ActiveShield u om de hele computer te scannen als een verdacht bestand wordt opgespoord. Als u de vraag niet verbergt, wordt u er regelmatig aan herinnerd totdat u de scan uitvoert.

Geïnfecteerde bestanden beheren

1. Als het bestand door ActiveShield kan worden opgeschoond, kunt u meer informatie opvragen of de waarschuwing negeren:
   - Klik op **Meer informatie** als u de naam, locatie en virusnaam van het geïnfecteerde bestand wilt weten.
   - Klik op **Verdergaan** om de waarschuwing te negeren en te sluiten.
2. Als het bestand niet door ActiveShield kan worden opgeschoond, klikt u op **Het in quarantaine plaatsen** om geïnfecteerde en verdachte bestanden te coderen en tijdelijk te isoleren in de quarantainemap totdat er een geschikte actie kan worden ondernomen.

   Er wordt een bevestigingsbericht weergegeven waarin u wordt gevraagd de computer op virussen te controleren. Klik op **Scannen** om het quarantaineproces te voltooien.
3. Als het bestand niet door ActiveShield in quarantaine kan worden geplaatst, klikt u op **Het bestand verwijderen** om het bestand te verwijderen.

Geïnfecteerde e-mailberichten beheren

Standaard wordt bij het scannen van e-mail automatisch geprobeerd om een geïnfecteerd e-mailbericht op te schonen. In het binnenkomende bericht wordt een waarschuwing opgenomen, waarmee u kunt zien of het bericht is opgeschoond, in quarantaine geplaatst of verwijderd.

Verdachte scripts beheren

Als er door ActiveShield een verdacht script wordt gevonden, kunt u meer informatie opvragen en het script stoppen als u het niet wilt initialiseren:

- Klik op **Meer informatie** als u de naam, locatie en beschrijving van de activiteit van het verdachte script wilt weten.
- Klik op **Dit script stoppen** om te voorkomen dat het verdachte script wordt uitgevoerd.

Als u zeker weet dat u het script kunt vertrouwen, kunt u toestaan dat het script wordt uitgevoerd:

- Klik op **Dit script deze keer toestaan** om alle scripts in een bestand één keer uit te voeren.
- Klik op **Doorgaan met waar ik mee bezig was** om de waarschuwing te negeren en het script uit te voeren.

Mogelijke wormen beheren

Als ActiveShield een mogelijke worm vindt, kunt u meer informatie opvragen en de e-mailactiviteit stoppen als u dat niet wilde uitvoeren:

- Klik op **Meer informatie** als u de lijst met geadresseerden en de onderwerpregel, berichttekst en beschrijving van het verdachte e-mailbericht wilt bekijken.
- Klik op **Dit e-mailbericht tegenhouden** om te voorkomen dat het verdachte bericht wordt verzonden en om het uit de berichtenwachtrij te verwijderen.

Als u zeker weet dat u de e-mailactiviteit kunt vertrouwen, klikt u op **Doorgaan met waar ik mee bezig was** om de waarschuwing te negeren en het e-mailbericht te verzenden.

MOP's beheren

Als ActiveShield een mogelijk ongewenst programma (MOP) vindt en tegenhoudt, kunt u meer informatie opvragen en het programma verwijderen als u het niet wilde installeren:

- Klik op **Meer informatie** als u de naam, locatie en aanbevolen actie voor het MOP wilt weten.
- Klik op **Dit MOP verwijderen** om het programma te verwijderen als u het niet wilde installeren.

  Er verschijnt een bevestigingsbericht.

  - Als u (a) het MOP niet herkent of (b) het MOP niet hebt geïnstalleerd als onderdeel van een pakket of geen licentieovereenkomst voor zo'n programma hebt geaccepteerd, klik dan op **OK** om het programma te verwijderen volgens de McAfee-methode.

  - Klik anders op **Annuleren** om het automatische verwijderingsproces af te sluiten. Als u later van gedachten verandert, kunt u het programma handmatig verwijderen met het bijbehorende deïnstallatieprogramma.
- Klik op **Doorgaan met waar ik mee bezig was** om de waarschuwing te negeren en het programma deze keer te blokkeren.

Als u (a) het MOP herkent of (b) het MOP hebt geïnstalleerd als onderdeel van een pakket of een licentieovereenkomst voor zo'n programma hebt geaccepteerd, kunt u het uitvoeren ervan toestaan:

- Klik op **Dit MOP vertrouwen** om het programma te vertrouwen en uitvoeren ervan altijd toe te staan.

  Zie "*Vertrouwde MOP's beheren*" voor meer informatie.

Vertrouwde MOP's beheren

De programma's die u toevoegt aan de lijst Vertrouwde MOP's, worden niet door McAfee VirusScan opgespoord.

Als een MOP wordt opgespoord en dan wordt toegevoegd aan de lijst Vertrouwde MOP's, kunt u het desgewenst later van de lijst verwijderen.

Als de lijst Vertrouwde MOP's vol is, dan moet u enkele items verwijderen voordat een ander MOP vertrouwd kan worden.

Ga als volgt te werk om een programma uit de lijst Vertrouwde MOP's te verwijderen:

1. Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **Opties**.
2. Klik op **Geavanceerd** en klik vervolgens op het tabblad **MOP's**.
3. Klik op **Lijst van vertrouwde MOP's bewerken**, schakel het selectievakje voor de bestandsnaam in en klik op **Verwijderen**. Klik op **OK** als u klaar bent met het verwijderen van items.

Uw computer handmatig scannen

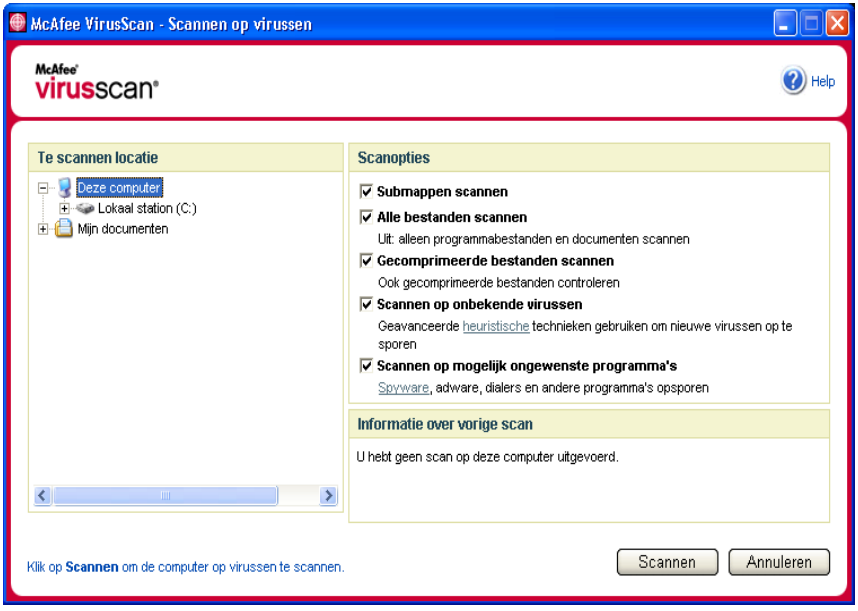
Met Scannen kunt u selectief naar virussen en mogelijk ongewenste programma's zoeken op vaste schijven en diskettes en in afzonderlijke bestanden en mappen. Wanneer Scannen een geïnfecteerd bestand aantreft, wordt automatisch geprobeerd het bestand op te schonen, tenzij het een mogelijk ongewenst programma is. Als Scannen het bestand niet kan opschonen, kunt u het bestand in quarantaine plaatsen of verwijderen.

Handmatig scannen op virussen en andere bedreigingen

Ga als volgt te werk om de computer te scannen:

1 Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **Scannen op virussen**.

Het dialoogvenster **Scannen op virussen** wordt geopend (Afbeelding 2-8).



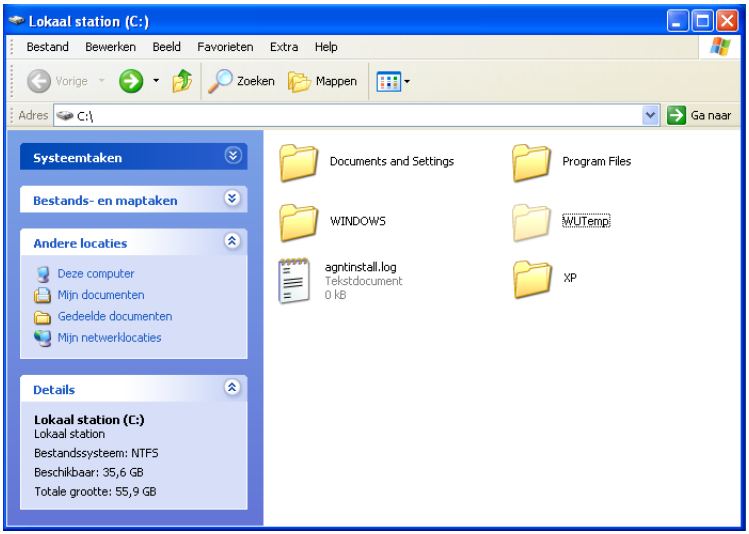
Afbeelding 2-8. Dialoogvenster Scannen op virussen

2 Klik op het station, de map of het bestand dat u wilt scannen.

3 Selecteer de gewenste **Scanopties**. Standaard zijn alle **Scanopties** geselecteerd, voor de grondigste scan (Afbeelding 2-8):

- **Submappen scannen**: gebruik deze optie om bestanden in uw submappen te scannen. Schakel dit selectievakje uit als u wilt toestaan dat alleen de bestanden worden gescand die u ziet wanneer u een map of station opent.

Voorbeeld: Alleen de bestanden in Afbeelding 2-9 worden gescand als u het selectievakje **Submappen scannen** uitschakelt. De mappen en de inhoud worden niet gescand. Als u wilt dat ook deze mappen en de inhoud worden gescand, moet u het selectievakje ingeschakeld laten.



Afbeelding 2-9. Inhoud van lokale schijf

- **Alle bestanden scannen**: gebruik deze optie om alle bestandstypen grondig te scannen. Schakel dit selectievakje uit als u de duur van de scanbewerking wilt verkorten en wilt toestaan dat alleen programmabestanden en documenten worden gescand.
- **Gecomprimeerde bestanden scannen**: gebruik deze optie om verborgen geïnfecteerde bestanden op te sporen in ZIP-bestanden en andere gecomprimeerde bestanden. Schakel dit selectievakje uit als u wilt voorkomen dat bestanden of gecomprimeerde bestanden in het gecomprimeerde bestand worden gescand.

  Soms plaatsen virusmakers een virus in een ZIP-bestand en wordt dat ZIP-bestand vervolgens opgenomen in een ander ZIP-bestand in een poging virusscanners te omzeilen. Scannen kan deze virussen opsporen zolang u deze optie ingeschakeld laat.
- **Scannen op onbekende virussen**: gebruik deze optie om de nieuwste virussen op te sporen, waarvoor nog geen "remedies" bestaan. Deze optie maakt gebruik van geavanceerde heuristische technieken waarmee wordt geprobeerd de bestanden te vergelijken met bestaande virussen, terwijl er ook wordt gelet op signalen van onbekende virussen in de bestanden.

Met deze scanmethode wordt ook gezocht naar bestandseigenschappen waarmee kan worden uitgesloten dat een bestand een virus bevat. Zodoende wordt de kans beperkt dat Scannen onjuiste aanwijzingen geeft. Toch moet u een virus dat met een heuristische scanbewerking is gevonden, net zo voorzichtig behandelen als een bestand waarvan u weet dat het een virus bevat.

Met deze optie voert u de grondigste scanbewerking uit, maar dit duurt wel langer dan een normale scanbewerking.

- **Scannen op mogelijk ongewenste programma's**: gebruik deze optie om spyware, adware, dialers en andere programma's op te sporen die u niet op de computer had willen installeren.

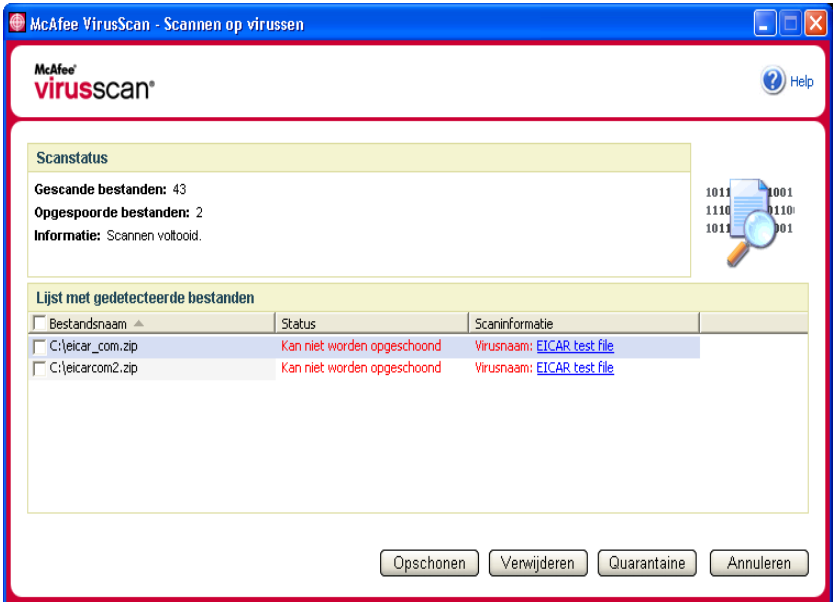
Opmerking

Laat alle opties ingeschakeld als u een zo grondig mogelijke scan wilt uitvoeren. Hierbij wordt elk bestand op het geselecteerde station of in de geselecteerde map gescand. Trek dus voldoende tijd uit om de scanbewerking te voltooien. Hoe groter de vaste schijf is en hoe meer bestanden u hebt, hoe langer het scannen duurt.

4 Klik op **Scannen** om te beginnen met het scannen van bestanden.

Wanneer het scannen is voltooid, wordt er een scanoverzicht weergegeven met het aantal gescande bestanden, het aantal gedetecteerde bestanden, het aantal mogelijk ongewenste programma's en het aantal automatisch opgeschoonde bestanden.

5 Klik op **OK** om het overzicht te sluiten en de lijst met gedetecteerde bestanden te bekijken in het dialoogvenster **Scannen op virussen** (Afbeelding 2-10).



Afbeelding 2-10. Scanresultaten

Opmerking
Met Scannen wordt een gecomprimeerd bestand (met de extensie ZIP, CAB, enz.) beschouwd als één bestand onder **Gescande bestanden**. Het aantal gescande bestanden kan ook variëren als u tijdelijke internetbestanden hebt verwijderd sinds de laatste scanbewerking.

6 Als Scan geen virussen of mogelijk ongewenste programma's vindt, klikt u op **Terug** zodat u een ander station of een andere map kunt selecteren om te scannen of klikt u op **Sluiten** om het dialoogvenster te sluiten. Zie ook *Opsporen van bedreigingen begrijpen* op pagina 32.

Scannen via Windows Verkenner

In VirusScan kunt u via een snelmenu de geselecteerde bestanden, mappen of stations in Windows Verkenner scannen op virussen en mogelijk ongewenste programma's.

Ga als volgt te werk om bestanden te scannen in Windows Verkenner:

1 Open Windows Verkenner.

2 Klik met de rechter muisknop op het station, de map of het bestand dat u wilt scannen en klik vervolgens op **Scannen op virussen**.

Het dialoogvenster **Scannen op virussen** wordt geopend en de scanbewerking wordt gestart. Standaard zijn alle **Scanopties** geselecteerd, voor de grondigste scan (Afbeelding 2-8 op pagina 27).

Scannen via Microsoft Outlook

In VirusScan kunt u met een werkbalkpictogram een scanbewerking uitvoeren op geselecteerde berichtenarchieven en de bijbehorende submappen, postvakmappen of e-mailberichten die bijlagen bevatten in Microsoft Outlook 97 of hoger.

Ga als volgt te werk om e-mailberichten te scannen in Microsoft Outlook:

1 Open Microsoft Outlook.

2 Klik op het berichtenarchief, de map of het e-mailbericht dat een bijlage bevat die u wilt scannen en klik vervolgens op het werkbalkpictogram voor het scannen van e-mail  .

Het scannen van e-mailbestanden wordt gestart. Standaard zijn alle **Scanopties** geselecteerd, voor de grondigste scan (Afbeelding 2-8 op pagina 27).

Automatisch scannen op virussen en andere bedreigingen

Hoewel VirusScan bestanden scant zodra ze door de computer of door uzelf worden gebruikt, kunt u met Windows Taakplanner een automatische scanbewerking instellen, zodat uw computer op gezette tijden grondig op virussen of mogelijk ongewenste programma's wordt gecontroleerd.

Ga als volgt te werk om een scanbewerking te plannen:

1 Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **Opties**.

Het dialoogvenster **Opties** van VirusScan wordt geopend.

2 Klik op het tabblad **Geplande scan** (Afbeelding 2-11 op pagina 31).

Afbeelding 2-11. Opties voor geplande scanbewerkingen

3 Schakel het selectievakje **Mijn computer scannen op een gepland tijdstip** in om automatisch scannen in te schakelen.

4 Ga als volgt te werk om een schema voor automatisch scannen op te geven:

- Als u het standaardschema (elke vrijdag om 20:00 uur) wilt gebruiken, klikt u op **OK**.
- Ga als volgt te werk om het schema te bewerken:

  a. Klik op **Bewerken**.

  Geef aan hoe vaak de computer moet worden gescand in de lijst **Taak plannen** en selecteer daaronder vervolgens extra opties:

  Dagelijks: geef aan om de hoeveel dagen er een scanbewerking moet plaatsvinden.

Wekelijks (standaard): geef aan om de hoeveel weken er een scanbewerking moet plaatsvinden en geef de namen van de dagen van de week op.

Maandelijks: geef aan op welke dag van de maand er een scanbewerking moet plaatsvinden. Klik op **Maanden selecteren** om aan te geven in welke maanden er een scanbewerking moet plaatsvinden en klik vervolgens op **OK**.

Een keer: geef aan op welke datum er een scanbewerking moet plaatsvinden.

Opmerking
De volgende opties in Windows Taakplanner worden niet ondersteund:
Bij opstarten, **Indien niet-actief** en **Meerdere schema's weergeven**. Het laatste ondersteunde schema blijft ingeschakeld totdat u een geldige optie selecteert.

b. Selecteer het tijdstip waarop de computer moet worden gescand in het vak **Begintijd**.

c. Klik op **Geavanceerd** als u geavanceerde opties wilt selecteren.

Het dialoogvenster **Geavanceerde planningsopties** wordt geopend.

i. Geef een begindatum, einddatum, duur en eindtijd op en geef aan of de taak op de opgegeven tijd moet worden gestopt als de scanbewerking op dat moment nog wordt uitgevoerd.

ii. Klik op **OK** om de wijzigingen op te slaan en het dialoogvenster te sluiten. Klik anders op **Annuleren**.

5 Klik op **OK** om de wijzigingen op te slaan en het dialoogvenster te sluiten. Klik anders op **Annuleren**.

6 Als u terug wilt gaan naar het standaardschema, klikt u op **Standaard**. Klik anders op **OK**.

Opsporen van bedreigingen begrijpen

Bij de meeste virussen, Trojaanse paarden en wormen probeert Scan automatisch het bestand op te schonen. U kunt vervolgens kiezen hoe u gedetecteerde bestanden wilt beheren. Desgewenst kunt u de bestanden naar McAfee AVERT sturen voor nader onderzoek. Als een mogelijk ongewenst programma wordt aangetroffen, kunt u het handmatig opschonen, in quarantaine plaatsen of verwijderen (de optie voor verzending naar AVERT is niet beschikbaar).

Ga als volgt te werk om een virus of mogelijk ongewenst programma te beheren:

1 Als er een bestand in de **Lijst met gedetecteerde bestanden** voorkomt, klikt u op het selectievakje om het te selecteren.

Opmerking
Als de lijst meerdere bestanden bevat, kunt u het selectievakje voor de lijst **Bestandsnaam** inschakelen om dezelfde bewerking uit te voeren voor alle bestanden. U kunt ook in de lijst **Scaninformatie** op de bestandsnaam klikken voor meer informatie uit de Virus Information Library.

2 Als het bestand een mogelijk ongewenst programma is, kunt u op **Opschonen** klikken om het bestand op te schonen.

3 Als het bestand niet door Scannen kan worden opgeschoond, klikt u op **In quarantaine** om geïnfecteerde en verdachte bestanden te coderen en tijdelijk te isoleren in de quarantainemap totdat er een geschikte actie kan worden ondernomen. (Zie *Bestanden in quarantaine beheren* op pagina 33 voor meer informatie.)

4 Als het bestand niet kan worden opgeschoond of in quarantaine kan worden geplaatst, hebt u de volgende mogelijkheden:

- Klik op **Verwijderen** om het bestand te verwijderen.
- Klik op **Annuleren** om het dialoogvenster te sluiten zonder verdere actie te ondernemen.

Als het gedetecteerde bestand niet kan worden opgeschoond of verwijderd, raadpleegt u de Virus Information Library op http://nl.mcafee.com/virusInfo/default.asp voor instructies over het handmatig verwijderen van het bestand.

Als het gedetecteerde bestand de internetverbinding of de gehele computer heeft geblokkeerd, kunt u een noodhersteldiskette gebruiken om de computer opnieuw op te starten. In veel gevallen kunt u een computer die door een virus is geblokkeerd, weer opnieuw opstarten met de noodhersteldiskette. Zie *Een noodhersteldiskette maken* op pagina 35 voor meer informatie.

Raadpleeg voor meer informatie de klantenservice van McAfee op http://www.mcafeehulp.com/.

Bestanden in quarantaine beheren

Met de quarantainefunctie kunt u geïnfecteerde en verdachte bestanden coderen en tijdelijk isoleren in de quarantainemap tot er een gepaste actie kan worden ondernomen. Zodra een in quarantaine geplaatst bestand is opgeschoond, kan het terug worden gezet op de oorspronkelijke locatie.

Ga als volgt te werk om een bestand in quarantaine te beheren:

1 Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **Bestanden in quarantaine beheren**.

Er wordt een lijst met in quarantaine geplaatste bestanden weergegeven (Afbeelding 2-12).

Afbeelding 2-12. Dialoogvenster Bestanden in quarantaine beheren

2 Schakel het selectievakje in naast de bestanden die u wilt opschonen.

> **Opmerking**
> Als de lijst meerdere bestanden bevat, kunt u het selectievakje voor de lijst **Bestandsnaam** inschakelen om dezelfde bewerking uit te voeren voor alle bestanden. U kunt ook klikken op de naam van het virus in de lijst **Status** om meer informatie uit de Virus Information Library te bekijken.
>
> Of klik op **Toevoegen**, selecteer het verdachte bestand dat u aan de lijst met bestanden in quarantaine wilt toevoegen, klik op **Openen** en selecteer het bestand vervolgens in de quarantainelijst.

3 Klik op **Opschonen**.

4 Als het bestand is opgeschoond, klikt u op **Herstellen** om het bestand te verplaatsen naar de oorspronkelijke locatie.

5 Als het geïnfecteerde bestand niet door VirusScan kan worden opgeschoond, klikt u op **Verwijderen** om het bestand te verwijderen.

6 Als het bestand niet door VirusScan kan worden opgeschoond of verwijderd en het geen mogelijk ongewenst programma betreft, kunt u het bestand naar AVERT™ (McAfee AntiVirus Emergency Response Team) sturen voor nader onderzoek:

   a Werk uw virushandtekeningbestanden bij als deze ouder zijn dan twee weken.

   b Controleer uw abonnement.

   c Selecteer het bestand en klik op **Verzenden** om het bestand naar AVERT te sturen.

      VirusScan verstuurt het in quarantaine geplaatste bestand als een bijlage mee met een e-mailbericht dat de volgende gegevens bevat: uw e-mailadres, land, softwareversie, besturingssysteem en de oorspronkelijke naam en locatie van het bestand. Per dag kan maximaal één uniek bestand van 1,5 MB worden verstuurd.

7 Klik op **Annuleren** om het dialoogvenster te sluiten zonder verdere actie te ondernemen.

Een noodhersteldiskette maken

U kunt met het hulpprogramma Rescue Disk opstartdiskettes maken. Met een opstartdiskette kunt u de computer opstarten en op virussen scannen als een virus voorkomt dat de computer op de normale wijze kan worden gestart.

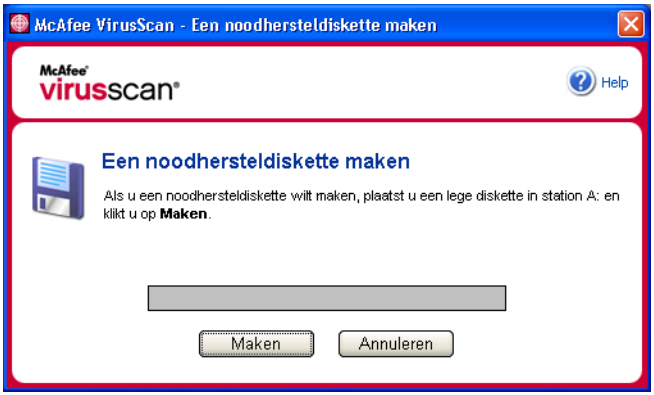
> **Opmerking**
> U moet verbinding hebben met internet om het imagebestand voor de noodhersteldiskette te kunnen downloaden. Rescue Disk is alleen beschikbaar voor computers met vaste-schijfpartities van het type FAT (FAT 16 en FAT 32). Dit hulpprogramma is overbodig voor NTFS-partities.

Ga als volgt te werk om een noodhersteldiskette te maken:

1 Plaats op een niet-geïnfecteerde computer een niet-geïnfecteerde diskette in station A. Mogelijk wilt u de computer en de diskette eerst met Scannen op virussen scannen. (Zie *Handmatig scannen op virussen en andere bedreigingen* op pagina 27 voor meer informatie.)

2 Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **Noodhersteldiskette maken**.

Het dialoogvenster **Een noodhersteldiskette maken** wordt geopend (Afbeelding 2-13).



Afbeelding 2-13. Dialoogvenster Een noodhersteldiskette maken

3 Klik op **Maken** om de noodhersteldiskette te maken.

Als u voor het eerst een noodhersteldiskette maakt, krijgt u een bericht dat er een imagebestand voor de noodhersteldiskette moet worden gedownload. Klik op **OK** om het onderdeel nu te downloaden of klik op **Annuleren** om het later te downloaden.

U krijgt een waarschuwing dat de inhoud van de diskette verloren gaat.

4 Klik op **Ja** om door te gaan met het maken van de noodhersteldiskette.

De status wordt weergegeven in het dialoogvenster **Noodhersteldiskette maken**.

5 Wanneer u het bericht ziet dat het maken van de noodhersteldiskette is voltooid, klikt u op **OK** en sluit u het dialoogvenster **Noodhersteldiskette maken**.

6 Verwijder de noodhersteldiskette uit het station, beveilig de diskette tegen schrijven en bewaar de diskette op een veilige plaats.

Een noodhersteldiskette beveiligen tegen schrijven

Ga als volgt te werk om een noodhersteldiskette te beveiligen tegen schrijven:

1 Leg de diskette met het label naar beneden (zodat de metalen cirkel zichtbaar is).

2 Kijk waar het schuifje van de schrijfbeveiliging zit. Verplaats het schuifje, zodat de opening zichtbaar wordt.

Een noodhersteldiskette gebruiken

Ga als volgt te werk om een noodhersteldiskette te gebruiken:

1. Schakel de geïnfecteerde computer uit.
2. Plaats de noodhersteldiskette in het station.
3. Schakel de computer in.

   Er wordt een grijs venster met verschillende opties weergegeven.
4. Kies de gewenste optie met de juiste functietoetsen (bijvoorbeeld F2, F3).

   Opmerking
   De noodhersteldiskette wordt automatisch binnen 60 seconden gestart als u niet op een functietoets drukt.

Een noodhersteldiskette bijwerken

Het is raadzaam de noodhersteldiskette regelmatig bij te werken. Volg hiervoor dezelfde instructies als voor het maken van een nieuwe noodhersteldiskette.

Automatisch virussen rapporteren

U kunt anoniem virusinformatie verzenden om deze te laten opnemen in de World Virus Map. U kunt zich automatisch aanmelden voor deze uitermate veilige, gratis voorziening tijdens de installatie van VirusScan (in het dialoogvenster **Rapportage van Virus Map**) of op een willekeurig ander tijdstip op het tabblad **Rapportage van Virus Map** van het dialoogvenster **Opties** van VirusScan.

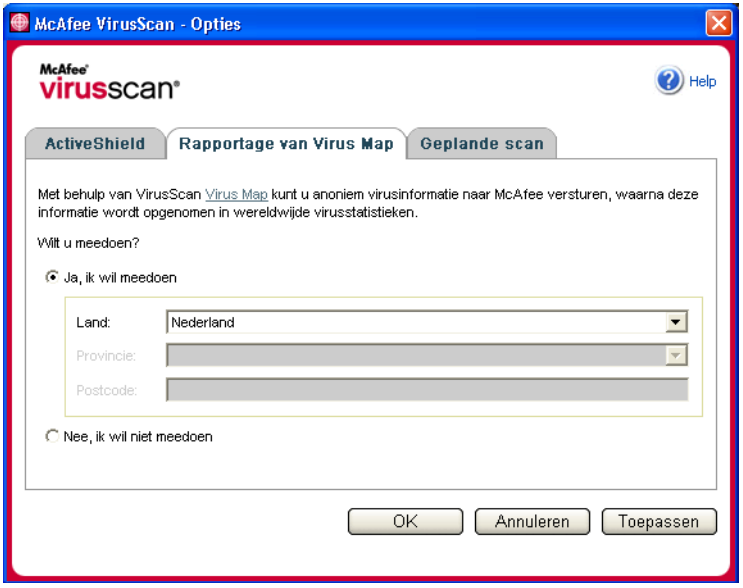
Rapporteren bij de World Virus Map

Ga als volgt te werk om automatisch virusinformatie te rapporteren bij de World Virus Map:

1. Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **Opties**.

   Het dialoogvenster **Opties** van VirusScan wordt geopend.

2 Klik op het tabblad **Rapportage van Virus Map** (Afbeelding 2-14).



Afbeelding 2-14. Rapportageopties voor Virus Map

3 Accepteer de standaardwaarde **Ja, ik wil meedoen** om de virusinformatie anoniem naar McAfee te verzenden om te worden opgenomen in de World Virus Map met wereldwijde virusstatistieken. Als u niet wilt dat deze informatie wordt verzonden, kiest u **Nee, ik wil niet meedoen**.

4 Als u zich in de Verenigde Staten bevindt, selecteert u de staat en geeft u de postcode op waar uw computer zich bevindt. Als u ergens anders woont, probeert VirusScan automatisch te achterhalen in welk land uw computer zich bevindt.

5 Klik op **OK**.

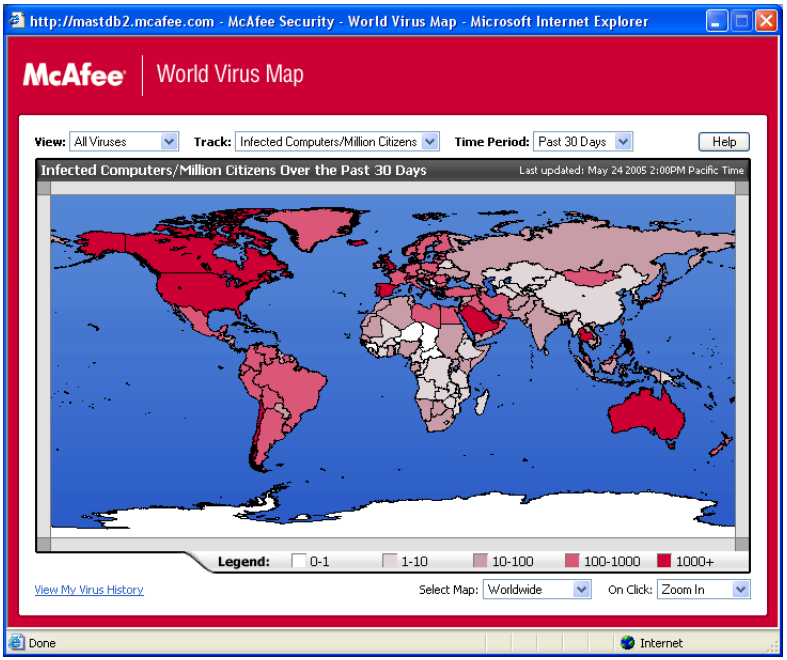
De World Virus Map bekijken

Ongeacht of u meedoet aan de World Virus Map, kunt u de nieuwste wereldwijde virusstatistieken bekijken via het McAfee-pictogram in het systeemvak van Windows.

Ga als volgt te werk om de World Virus Map te bekijken:

- Klik met de rechter muisknop op het McAfee-pictogram, kies **VirusScan** en klik op **World Virus Map**.

De webpagina **World Virus Map** wordt geopend (Afbeelding 2-15).



Afbeelding 2-15. World Virus Map

Standaard laat de World Virus Map het aantal computers zien dat wereldwijd gedurende de afgelopen 30 dagen geïnfecteerd is geraakt. Ook wordt aangegeven wanneer de gegevens voor het laatst zijn bijgewerkt. U kunt de kaartweergave wijzigen zodat het aantal geïnfecteerde bestanden wordt weergegeven, of de rapportageperiode wijzigen zodat alleen de resultaten van de afgelopen 7 dagen of de afgelopen 24 uur worden weergegeven.

In het gedeelte **Virus Tracking (virusoverzicht)** ziet u totalen voor het aantal gescande bestanden, geïnfecteerde bestanden en geïnfecteerde computers dat sinds de weergegeven datum is gerapporteerd.

VirusScan bijwerken

Wanneer u verbinding hebt met internet, controleert VirusScan automatisch elke vier uur op updates. Zonder dat u uw werk hoeft te onderbreken worden automatisch wekelijkse updates van de virusdefinities gedownload en geïnstalleerd.

Virusdefinitiebestanden zijn ongeveer 100 kB groot en hebben daardoor tijdens het downloaden weinig invloed op de systeemprestaties.

In het geval van een productupdate of een virusuitbraak wordt er een waarschuwing weergegeven. U kunt vervolgens VirusScan bijwerken om de virusdreiging onschadelijk te maken.

Automatisch controleren op updates

McAfee SecurityCenter controleert, indien u bent verbonden met internet, om de vier uur automatisch op updates voor al uw McAfee-services en meldt u dit met waarschuwingen en geluiden. Standaard worden beschikbare updates door SecurityCenter automatisch gedownload en geïnstalleerd.

Opmerking
In sommige gevallen wordt u gevraagd de computer opnieuw op te starten om de update te voltooien. Sla al uw werk op en sluit alle toepassingen voordat u de computer opnieuw opstart.

Handmatig controleren op updates

Naast de automatische controles op updates die elke vier uur plaatsvinden wanneer u verbinding hebt met internet, kunt u op elk gewenst moment ook handmatig op updates controleren.

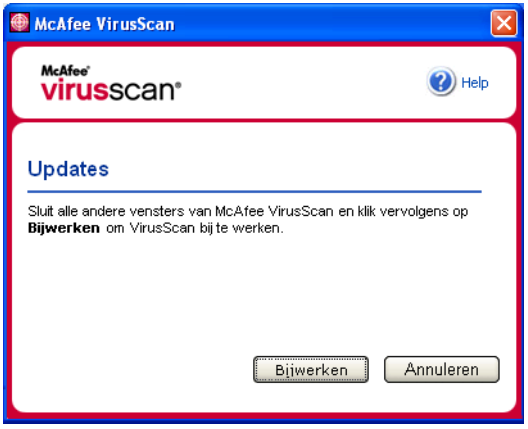
Ga als volgt te werk om handmatig te controleren op updates voor VirusScan:

1. Zorg ervoor dat uw computer verbinding heeft met internet.
2. Klik met de rechter muisknop op het McAfee-pictogram en klik vervolgens op **Updates**.

   Het dialoogvenster **Updates voor SecurityCenter** wordt geopend.
3. Klik op **Nu controleren**.

   Als er een update beschikbaar is, wordt het dialoogvenster **VirusScan Updates (updates van VirusScan)** geopend (Afbeelding 2-16 op pagina 40). Klik op **Bijwerken** om door te gaan.

   Als er geen updates beschikbaar zijn, krijgt u het bericht dat VirusScan up-to-date is. Klik op **OK** om het dialoogvenster te sluiten.



Afbeelding 2-16. Dialoogvenster Updates

4 Meld u aan bij de website als u hierom wordt gevraagd. De update wordt automatisch geïnstalleerd door de **Wizard Update**.

5 Klik op **Voltooien** wanneer de update is geïnstalleerd.

Opmerking
In sommige gevallen wordt u gevraagd de computer opnieuw op te starten om de update te voltooien. Sla al uw werk op en sluit alle toepassingen voordat u de computer opnieuw opstart.

Index

N

O

P

Q

S

T

U

V

W