McAfee®

virus scan professional™

Gebruikershandleiding

Versie 9.0

McAfee®

COPYRIGHT

HANDELSMERKEN

LICENTIES

Licentieovereenkomst

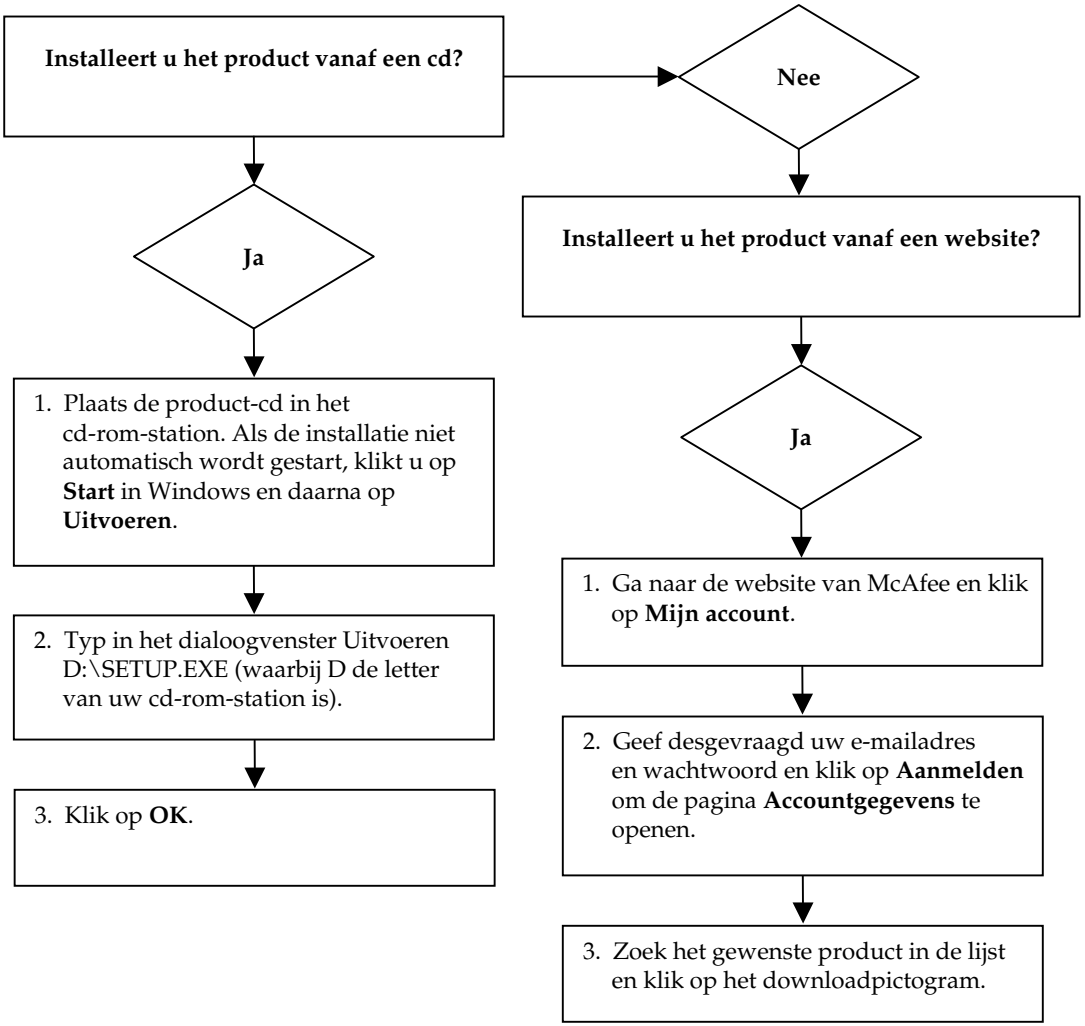
Bijdragen

Dit product bevat (mogelijk):

♦ Software ontwikkeld door OpenSSL Project voor gebruik in OpenSSL Toolkit (http://www.openssl.org/). ♦ Cryptografiesoftware van Eric A. Young en software van Tim J. Hudson. ♦ Bepaalde software waarvoor aan de gebruiker een licentie (of sublicentie) is verleend onder de GNU-voorwaarden van GPL (General Public License) of andere, soortgelijke licenties voor vrije software. Hierbij is het de gebruiker onder andere toegestaan om bepaalde programma's of gedeelten daarvan te kopiëren, wijzigen of te herdistribueren. De GPL schrijft voor dat voor alle software die onder de GPL valt en wordt gedistribueerd als uitvoerbaar binair bestand, de broncode eveneens beschikbaar wordt gesteld aan deze gebruikers. Voor alle software die onder de GPL valt, wordt de broncode beschikbaar gesteld op deze cd-rom. Als er licenties zijn die vereisen dat McAfee, Inc. rechten verleent om software te gebruiken, kopiëren of te wijzigen die verder strekken dan de rechten die in deze overeenkomst zijn vastgelegd, hebben de rechten in kwestie voorrang op de rechten en beperkingen in dit document. ♦ Software oorspronkelijk geschreven door Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. ♦ Software oorspronkelijk geschreven door Robert Nordier, Copyright © 1996-7 Robert Nordier. ♦ Software geschreven door Douglas W. Sauder. ♦ Software ontwikkeld door Apache Software Foundation (http://www.apache.org/). Een exemplaar van de licentieovereenkomst voor deze software vindt u op www.apache.org/licenses/LICENSE-2.0.txt. ♦ International Components for Unicode (ICU) Copyright © 1995-2002 International Business Machines Corporation en anderen. ♦ Software ontwikkeld door CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc. ♦ FEAD® Optimizer® technology, Copyright Netopsystems AG, Berlijn, Germany. ♦ Outside In® Viewer Technology © 1992-2001 Stellent Chicago, Inc. en /of Outside In® HTML Export, © 2001 Stellent Chicago, Inc. ♦ Software met copyright van Thai Open Source Software Center Ltd. en Clark Cooper, © 1998, 1999, 2000. ♦ Software met copyright van Expat maintainers. ♦ Software met copyright van The Regents of the University of California, © 1989. ♦ Software met copyright van Gunnar Ritter. ♦ Software met copyright van Sun Microsystems®, Inc.© 2003. ♦ Software met copyright van Gisle Aas. © 1995-2003. ♦ Software met copyright van Michael A. Chase, © 1999-2000. ♦ Software met copyright van Neil Winton, © 1995-1996. ♦ Software met copyright van RSA Data Security, Inc., © 1990-1992. ♦ Software met copyright van Sean M. Burke, © 1999, 2000. ♦ Software met copyright van Martijn Koster, © 1995. ♦ Software met copyright van Brad Appleton, © 1996-1999. ♦ Software met copyright van Michael G. Schwern, © 2001. ♦ Software met copyright van Graham Barr, © 1998. ♦ Software met copyright van Larry Wall and Clark Cooper, © 1998-2000. ♦ Software met copyright van Frodo Looijaard, © 1997. ♦ Software met copyright van Python Software Foundation, Copyright © 2001, 2002, 2003. Een exemplaar van de licentieovereenkomst voor deze software kunt u vinden op www.python.org. ♦ Software met copyright van Beman Dawes, © 1994-1999, 2002. ♦ Software geschreven door Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. ♦ Software met copyright van Simone Bordet & Marco Cravero, © 2002. ♦ Software met copyright van Stephen Purcell, © 2001. ♦ Software ontwikkeld door Indiana University Extreme! Lab (http://www.extreme.indiana.edu/). ♦ Software met copyright van International Business Machines Corporation en anderen, © 1995-2003. ♦ Software ontwikkeld door de University of California, Berkeley en haar medewerkers. ♦ Software ontwikkeld door Ralf S. Engelschall <rse@engelschall.com> voor gebruik in het mod_ssl project (http://www.modssl.org/). ♦ Software met copyright van Kevlin Henney, © 2000-2002. ♦ Software met copyright van Peter Dimov en Multi Media Ltd. © 2001, 2002. ♦ Software met copyright van David Abrahams, © 2001, 2002. Zie http://www.boost.org/libs/bind/bind.html voor de documentatie. ♦ Software met copyright van Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000. ♦ Software met copyright van Boost.org, © 1999-2002. ♦ Software met copyright van Nicolai M. Josuttis, © 1999. ♦ Software met copyright van Jeremy Siek, © 1999-2001. ♦ Software met copyright van Daryle Walker, © 2001. ♦ Software met copyright van Chuck Allison en Jeremy Siek, © 2001, 2002. ♦ Software met copyright van Samuel Krempp, © 2001. Zie http://www.boost.org voor updates, documentatie en wijzigingsgeschiedenis. ♦ Software met copyright van Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. ♦ Software met copyright van Cadenza New Zealand Ltd., © 2000. ♦ Software met copyright van Jens Maurer, © 2000, 2001. ♦ Software met copyright van Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000. ♦ Software met copyright van Ronald Garcia, © 2002. ♦ Software met copyright van David Abrahams, Jeremy Siek en Daryle Walker, © 1999-2001. ♦ Software met copyright van Stephen Cleary (shammah@voyager.net), © 2000. ♦ Software met copyright van Housemarque Oy <http://www.housemarque.com>, © 2001. ♦ Software met copyright van Paul Moore, © 1999. ♦ Software met copyright van Dr. John Maddock, © 1998-2002. ♦ Software met copyright van Greg Colvin en Beman Dawes, © 1998, 1999. ♦ Software met copyright van Peter Dimov, © 2001, 2002. ♦ Software met copyright van Jeremy Siek and John R. Bandela, © 2001. ♦ Software met copyright van Joerg Walter en Mathias Koch, © 2000-2002.

Snelstartkaart

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



Meer informatie

Als u de Gebruikershandleiding op de cd-rom 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

U kunt het beste de stappen in het product uitvoeren 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 aanschaf van de VirusScan-software

  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/.

Telefoonnummers voor noodgevallen

Land	Telefoonnummer
België	02 27 50 703
Brazilië	11 4196-7077
Denemarken	03 5258 321
Duitsland	06 966 404 330
Finland	09 229 06 000
Frankrijk	01 70 20 0 008
Ierland	01 601 55 80
Italië	02 45 28 15 10
Luxemburg	040 666 15670
Nederland	020 504 0586
Noorwegen	02 3050420
Oostenrijk	017 908 75 810
Portugal	00 31 20 586 6430 (Engels gesproken)
Spanje	901-120 175 (* laag tarief)
Verenigd Koninkrijk	020 794 901 07
Zuid-Afrika	011 700-8216
Zweden	08 57 92 9004
Zwitserland	022 310 1033

Inhoud

Aan de slag 1

Welkom bij McAfee VirusScan. McAfee VirusScan Professional Edition bevat McAfee VirusScan, McAfee SpamKiller en McAfee Shredder. Zie *Professional Edition gebruiken* op pagina 39 voor meer informatie over deze extra programma's.

> **Opmerking**
> Dit is een kort overzicht. Raadpleeg voor uitgebreide informatie de online Help voor VirusScan, SpamKiller of Shredder.

McAfee VirusScan is een antivirusservice die uitgebreide, betrouwbare en up-to-date beveiliging tegen virussen biedt. U kunt zich op deze service abonneren. 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: scant bestanden zodra deze door u of de computer worden gebruikt.

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

Quarantaine: codeert geïnfecteerde en verdachte bestanden en isoleert deze tijdelijk in de quarantainemap totdat de meest geschikte actie kan worden uitgevoerd.

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

Nieuwe functies

Deze versie van VirusScan bevat de volgende nieuwe functies:

- **Scannen op mogelijk ongewenste programma's**
  VirusScan kan scannen op mogelijk ongewenste programma's (bijvoorbeeld spyware, adware en dialers) tijdens het handmatig scannen, het scannen van uitgaande e-mailberichten, het verzenden van expresberichten (Instant Messaging, IM), via het snelmenu van Windows Verkenner en via het werkbalkpictogram van Microsoft Outlook.

- **Grote uitgaande bijlagen scannen**
  Omdat er steeds meer mensen een breedbandverbinding gebruiken en providers grotere opslagmogelijkheden en overdrachtsformaten voor e-mailberichten bieden, is VirusScan nu geoptimaliseerd voor het scannen van grote e-mailbijlagen zonder conflicten met de time-outwaarden van het e-mailprogramma.

- **Scannen van e-mail**
  Inkomende (POP3) en uitgaande (SMTP) e-mail en berichtbijlagen worden automatisch door VirusScan gescand voor de meestgebruikte e-mailclients, zoals Microsoft Outlook, Netscape Mail, Eudora en Pegasus.

- **Scannen van expresberichten**
  Inkomende bestanden worden automatisch door VirusScan gescand voor de meestgebruikte clients voor expresberichten, zoals Yahoo Messenger, AOL Instant Messenger en MSN Messenger.

- **Opsporing van schadelijke activiteiten**
  VirusScan is voorzien van ScriptStopper™ en WormStopper™, hulpprogramma's die virusachtige activiteiten, veroorzaakt door schadelijke scripts en wormachtige activiteiten, opsporen en blokkeren en hierover waarschuwingen verzenden.

- **Automatisch opschonen van geïnfecteerde bestanden**
  Zodra er geïnfecteerde of verdachte bestanden worden gedetecteerd, worden deze meteen automatisch opgeschoond door VirusScan.

- **Gepland scannen**
  U kunt zelf het interval bepalen voor het automatisch scannen van uw computer op virussen.

- **Bestandsquarantaine**
  Gebruik de quarantainefunctie om geïnfecteerde en verdachte bestanden te coderen en ze tijdelijk in de quarantainemap te isoleren totdat de meest geschikte actie kan worden uitgevoerd. Zodra een in quarantaine geplaatst bestand is opgeschoond, kan het terug worden gezet op de oorspronkelijke locatie.

- **Bestanden naar AVERT versturen**
  VirusScan is nu voorzien van de mogelijkheid om verdachte bestanden direct vanuit de quarantainefunctie naar het McAfee AntiVirus Emergency Response Team (AVERT™) te sturen voor onderzoek.

- **Rapportage van Virus Map**
  U kunt nu anoniem traceergegevens van virussen toevoegen aan onze World Virus Map. U kunt zich automatisch voor deze uiterst veilige, gratis voorziening registreren en de nieuwste wereldwijde virusstatistieken bekijken via McAfee SecurityCenter.

Systeemvereisten

- Microsoft® Windows 98, ME, 2000 of XP
- Pc met processor
  Windows 98 of ME: Pentium 150 MHz of hoger
  Windows 2000 of XP: Pentium 233 MHz-processor of hoger
- RAM
  Windows 98: 32 MB (64 MB aanbevolen)
  Windows ME, 2000 of XP: 64 MB (128 MB aanbevolen)
- 40 MB vrije ruimte op de vaste schijf
- Microsoft® Internet Explorer 5.5 of later

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

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 Scan afzonderlijk te testen.

ActiveShield testen

Ga als volgt te werk om ActiveShield te testen:

1. Ga in 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 *Als ActiveShield een virus vindt* op pagina 25 voor meer informatie.

Scan testen

Als u Scan wilt testen, moet u ActiveShield uitschakelen om te voorkomen dat deze de geïnfecteerde bestanden voor Scan detecteert, en vervolgens de testbestanden downloaden.

Ga als volgt te werk om de testbestanden te downloaden:

1. Schakel ActiveShield uit: Klik met de rechtermuisknop op het McAfee-pictogram, wijs **VirusScan** aan 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 rechtermuisknop op het McAfee-pictogram, wijs **VirusScan** aan en klik op **Inschakelen**.

Ga als volgt te werk om Scan te testen:

1. Klik met de rechtermuisknop op het McAfee-pictogram, wijs **VirusScan** aan 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).

      Scan 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 Scan 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.

   De map **VSO Scan** wordt nu gescand door VirusScan. De bestanden die u in die map hebt opgeslagen, worden weergegeven in de **Lijst met gedetecteerde bestanden**. Als dit inderdaad het geval is, werkt Scan goed.

U kunt proberen geïnfecteerde bestanden te verwijderen of in quarantaine te plaatsen om na te gaan hoe Scan omgaat met virussen. Zie *Als Scan een virus of een mogelijk ongewenst programma aantreft* op pagina 34 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 profiteert u van het volgende:

- Gratis beveiligingsanalyse voor uw computer.
- Al uw McAfee-abonnementen starten, beheren en configureren met één pictogram.
- Voortdurend bijgewerkte viruswaarschuwingen en de meest recente productinformatie.
- 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 McAfee-voorzieningen die op de computer zijn geïnstalleerd, zijn ingeschakeld, wordt een rood M-pictogram  weergegeven in het systeemvak van Windows. Het systeemvak is het gebied rechtsonder op het bureaublad. In dit vak ziet u tevens de systeemklok.

Als een of meer van de geïnstalleerde McAfee-toepassingen op de computer zijn uitgeschakeld, is het McAfee-pictogram zwart  .

Ga als volgt te werk om McAfee SecurityCenter te openen:

1. Klik met de rechtermuisknop op het McAfee-pictogram  .
2. Klik op **SecurityCenter openen**.

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

1. Klik met de rechtermuisknop op het McAfee-pictogram  .
2. Wijs **VirusScan** aan 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 het bestand in quarantaine te plaatsen of te 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 uitvoeren of 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 rechtermuisknop op het McAfee-pictogram, wijs **VirusScan** aan en klik op **Inschakelen**. Het McAfee-pictogram wordt rood  .

Als ActiveShield automatisch wordt gestart 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 16).

ActiveShield uitschakelen

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

1. Klik met de rechtermuisknop op het McAfee-pictogram, wijs **VirusScan** aan 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 rechtermuisknop op het McAfee-pictogram, wijs **VirusScan** aan en klik op **Opties**.

   Het dialoogvenster **Opties** van VirusScan wordt geopend (Afbeelding 2-1 op pagina 16).

2. Schakel het selectievakje **ActiveShield starten wanneer Windows wordt gestart (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, mag de computer niet verbonden zijn met internet.

Ga als volgt te werk om te voorkomen dat ActiveShield wordt gestart wanneer Windows wordt gestart:

1. Klik met de rechtermuisknop op het McAfee-pictogram, wijs **VirusScan** aan en klik op **Opties**.

   Het dialoogvenster **Opties** van VirusScan wordt geopend (Afbeelding 2-1 op pagina 16).

2. Schakel het selectievakje **ActiveShield starten wanneer Windows wordt gestart (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

De opties voor het scannen van e-mailberichten en automatisch opschonen zijn standaard ingeschakeld via de optie **E-mail en bijlagen scannen** (Afbeelding 2-1 op pagina 16) en de optie **Automatisch geïnfecteerde bijlagen opschonen (aanbevolen)** (Afbeelding 2-2 op pagina 20).

Wanneer deze twee opties zijn 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 (Afbeelding 2-2 op pagina 20) en WormStopper (Afbeelding 2-5 op pagina 25) 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 waarschuwingsbestand 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
- Er wordt een waarschuwingsbestand met het nieuwe e-mailbericht meegezonden dat informatie bevat over de bewerkingen die zijn uitgevoerd om de infectie te verwijderen

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

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 rechtermuisknop op het McAfee-pictogram, wijs **VirusScan** aan en klik op **Opties**.
2. Klik op **Geavanceerd** en klik vervolgens op de tab **E-mail Scan** (Afbeelding 2-2 op pagina 20).
3. Schakel **Inkomende e-mailberichten** of **Uitgaande e-mailberichten** uit en klik vervolgens op **OK**.

Als de e-mailserver zodanig is ingesteld dat er alleen e-mailberichten kunnen worden verzonden en ontvangen wanneer u de computer gebruikt, kunt u het automatisch opschonen uitschakelen. U wordt dan telkens gevraagd of u geïnfecteerde e-mailberichten wilt opschonen. Voer de onderstaande stappen uit om de optie voor automatisch opschonen uit te schakelen en zie vervolgens *Geïnfecteerde e-mailberichten beheren* op pagina 26 voor informatie over het reageren op waarschuwingen.

Afbeelding 2-2. Scanopties voor e-mailberichten

Ga als volgt te werk om het automatisch opschonen van geïnfecteerde e-mailberichten uit te schakelen:

1. Klik met de rechtermuisknop op het McAfee-pictogram, wijs **VirusScan** aan en klik op **Opties**.
2. Klik op **Geavanceerd** en klik vervolgens op de tab **E-mail Scan** (Afbeelding 2-2).
3. Klik op **Vragen wanneer een bijlage moet worden opgeschoond** en klik vervolgens op **OK**.

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 16).

Wanneer deze optie is ingeschakeld, worden inkomende bijlagen in expresberichten automatisch door VirusScan gescand en indien nodig opgeschoond voor de meestgebruikte clients 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 voor het gebruik van 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 optimaal gebruik van de scanfunctie.

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

1. Klik met de rechtermuisknop op het McAfee-pictogram, wijs **VirusScan** aan en klik op **Opties**.
2. Klik op **Geavanceerd** en klik vervolgens op de tab **ActiveShield** (Afbeelding 2-3 op pagina 22).
3. Klik op **Alle bestanden (aanbevolen)** en vervolgens op **OK**.

Afbeelding 2-3. Geavanceerde ActiveShield-opties

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 rechtermuisknop op het McAfee-pictogram, wijs **VirusScan** aan en klik op **Opties**.
2. Klik op **Geavanceerd** en klik vervolgens op de tab **ActiveShield** (Afbeelding 2-3).
3. Klik op **Alleen programmabestanden en documenten** en vervolgens op **OK**.

Scannen op onbekende virussen

Als u ActiveShield configureert voor het gebruik van 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 rechtermuisknop op het McAfee-pictogram, wijs **VirusScan** aan en klik op **Opties**.
2. Klik op **Geavanceerd** en klik vervolgens op de tab **ActiveShield** (Afbeelding 2-3 op pagina 22).
3. Klik op **Scannen op onbekende virussen (aanbevolen)** en vervolgens op **OK**.

Scannen op scripts en 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, voorkomen ScriptStopper™ en WormStopper™ dat virussen, wormen en Trojaanse paarden zich verder kunnen verspreiden.

Met de beveiligingsmechanismen van ScriptStopper en 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 actief script waarmee bestanden worden gemaakt, gekopieerd of verwijderd of waarmee het Windows-register wordt geopend
- 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 voor het gebruik van de standaardopties **ScriptStopper inschakelen (aanbevolen)** en **WormStopper inschakelen (aanbevolen)** in het dialoogvenster **Geavanceerde opties**, worden scripts en e-mailactiviteiten door ScriptStopper en 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 op schadelijke scripts en wormachtige activiteiten:

1. Klik met de rechtermuisknop op het McAfee-pictogram, wijs **VirusScan** aan en klik op **Opties**.
2. Klik op **Geavanceerd** en klik vervolgens op de tab **ScriptStopper**.
3. Klik op **ScriptStopper inschakelen (aanbevolen)** (Afbeelding 2-4 op pagina 24).

Afbeelding 2-4. ScriptStopper-opties

4 Klik op de tab **WormStopper**, klik op **WormStopper inschakelen (aanbevolen)** en klik vervolgens op **OK** (Afbeelding 2-5 op pagina 25).

De volgende gedetailleerde opties zijn standaard ingeschakeld:

- Jokertekens 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 mogelijk wormvirus is gevonden (zie *Mogelijke wormen beheren* op pagina 27 voor meer informatie):

- Verdachte uitgaande e-mailberichten automatisch blokkeren

Afbeelding 2-5. WormStopper-opties

Als ActiveShield een virus vindt

Als ActiveShield een virus vindt, wordt er een viruswaarschuwing weergegeven dat lijkt op Afbeelding 2-6. Bij de meeste virussen, Trojaanse paarden en wormen wordt het bestand automatisch door ActiveShield opgeschoond. U kunt vervolgens zelf bepalen hoe geïnfecteerde bestanden, geïnfecteerde e-mailberichten, verdachte scripts en mogelijke wormen moeten worden beheerd en of geïnfecteerde bestanden voor onderzoek naar het McAfee AVERT-team moeten worden verzonden.

Afbeelding 2-6. Viruswaarschuwing

Geïnfecteerde bestanden beheren

1 Als het bestand door ActiveShield kan worden opgeschoond, kunt u als volgt 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 **Doorgaan met waar ik mee bezig was** om de waarschuwing te negeren en te sluiten.

2 Als het bestand niet door ActiveShield kan worden opgeschoond, klikt u op **Het geïnfecteerde bestand 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 geïnfecteerde bestand verwijderen** om het bestand te verwijderen.

Geïnfecteerde e-mailberichten beheren

1 Als u de optie voor het automatisch opschonen van e-mailberichten hebt uitgeschakeld, kunt u als volgt meer informatie opvragen en e-mailberichten opschonen:

a Klik op **Meer informatie** als u de bestandsnaam, virusnaam, infectiestatus, afzender en het onderwerp van het geïnfecteerde e-mailbericht wilt weten.

b Klik op **De geïnfecteerde bijlage opschonen**.

2 Als het e-mailbericht niet door ActiveShield kan worden opgeschoond, klikt u op **De geïnfecteerde bijlage 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 e-mailbericht niet door ActiveShield in quarantaine kan worden geplaatst, klikt u op **De geïnfecteerde bijlage verwijderen** om het bestand te verwijderen.

Verdachte scripts beheren

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

   a. Klik op **Meer informatie** als u de naam, locatie en beschrijving van de activiteit van het verdachte script wilt weten.

   b. Klik op **Dit script stoppen** om te voorkomen dat het verdachte script wordt uitgevoerd.

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

   a. Klik op **Dit keer volledig script toestaan** om alle scripts in een bestand een keer uit te voeren.

   b. Klik op **Doorgaan met waar ik mee bezig was** om de waarschuwing te negeren en het script uit te voeren.

Mogelijke wormen beheren

1. Als er door ActiveShield een mogelijke worm wordt gevonden, kunt u als volgt meer informatie opvragen en de e-mailactiviteit stoppen als u de worm niet wilt initialiseren:

   a. Klik op **Meer informatie** als u de lijst met geadresseerden en de onderwerpregel, berichttekst en beschrijving van het verdachte e-mailbericht wilt bekijken.

   b. Klik op **Dit e-mailbericht tegenhouden** om te voorkomen dat het verdachte bericht wordt verzonden en om het uit de berichtenwachtrij te verwijderen.

2. 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.

Uw computer handmatig scannen

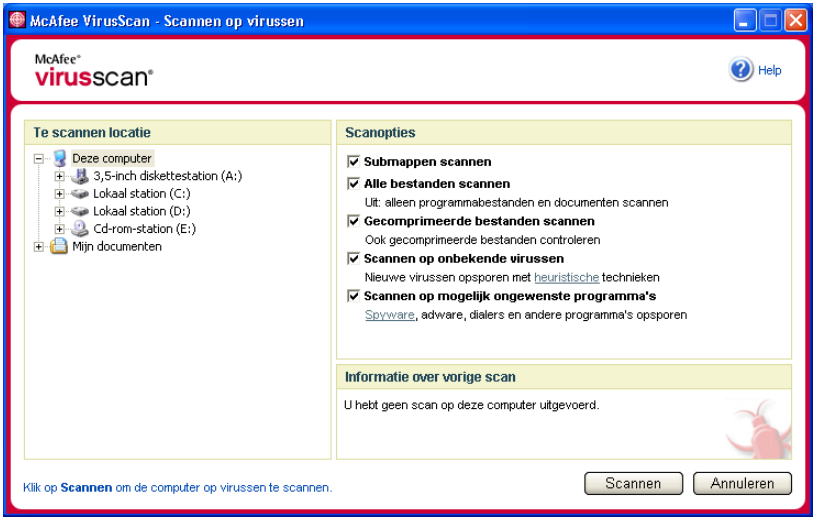
Met Scan kunt u selectief naar virussen en mogelijk ongewenste programma's zoeken op vaste schijven en diskettes en in afzonderlijke bestanden en mappen. Wanneer Scan een geïnfecteerd bestand aantreft, wordt automatisch geprobeerd het bestand op te schonen, tenzij het een mogelijk ongewenst programma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

Handmatig scannen op virussen en mogelijk ongewenste programma's

Ga als volgt te werk om de computer te scannen:

1 Klik met de rechtermuisknop op het McAfee-pictogram, wijs **VirusScan** aan en klik op **Scannen op virussen**.

Het dialoogvenster **Scannen op virussen** wordt geopend (Afbeelding 2-7).



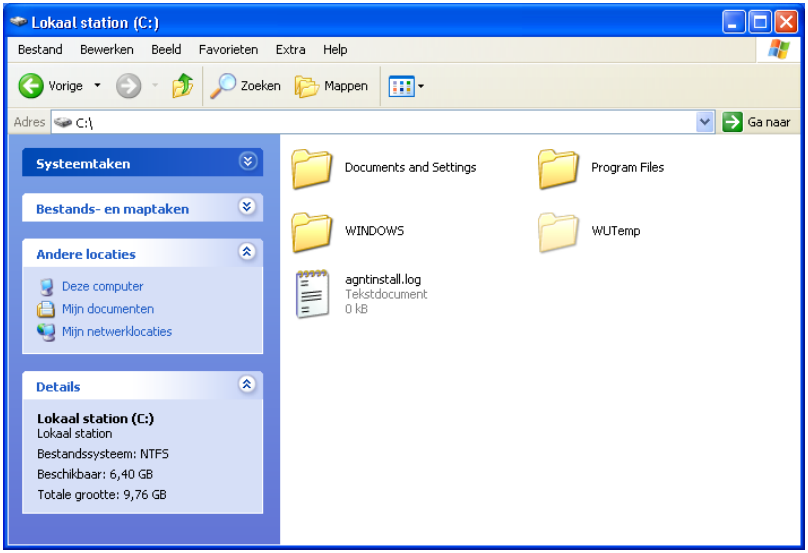
Afbeelding 2-7. Scannen op virussen

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

3 Selecteer de gewenste scanopties. Standaard zijn alle scanopties geselecteerd zodat de bestanden zo grondig mogelijk worden gescand (Afbeelding 2-7 op pagina 28):

- **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 2-8 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 2-8. 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. Scan kan deze virussen opsporen zolang u deze optie ingeschakeld laat.

- **Scannen op onbekende virussen**: gebruik deze optie om de nieuwste virussen te zoeken waarvoor mogelijk nog geen oplossing is. Deze optie gebruikt 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 Scan 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.

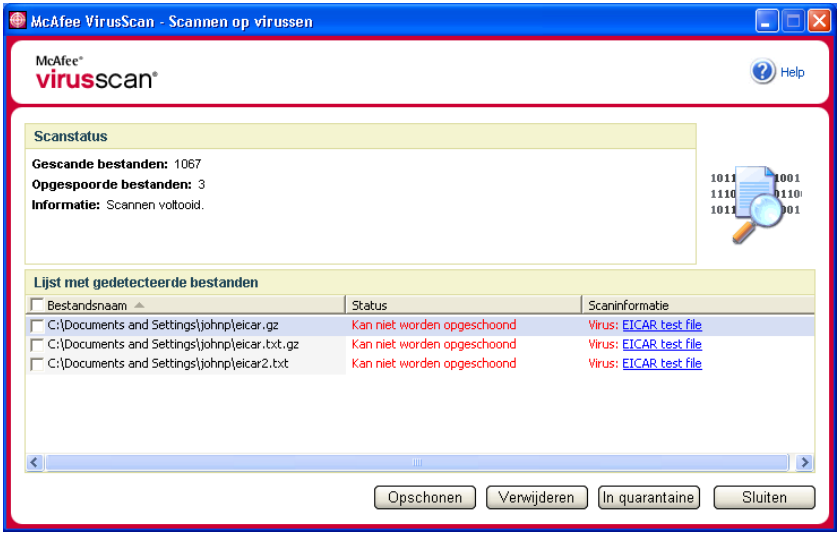
- **Scannen op mogelijk ongewenste programma's**: gebruik deze optie om spyware, adware, dialers en andere programma's op te sporen die u niet op de computer had willen installeren.

  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 2-9 op pagina 31).



Afbeelding 2-9. Scanresultaten

Opmerking
Met Scan wordt een gecomprimeerd bestand (met de extensie ZIP, CAB, enzovoort) 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 anders het gedeelte *Als Scan een virus of een mogelijk ongewenst programma aantreft* op pagina 34.

Scannen via Windows Verkenner

In VirusScan kunt u via een snelmenu de geselecteerde bestanden, mappen of stations vanuit 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 rechtermuisknop 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 zodat de bestanden zo grondig mogelijk worden gescand (Afbeelding 2-7 op pagina 28).

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-mailberichten  .

   Het scannen van e-mailbestanden wordt gestart. Standaard zijn alle scanopties geselecteerd zodat de bestanden zo grondig mogelijk worden gescand (Afbeelding 2-7 op pagina 28).

Automatisch scannen op virussen en mogelijk ongewenste programma's

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 rechtermuisknop op het McAfee-pictogram, wijs **VirusScan** aan en klik op **Opties**.

   Het dialoogvenster **Opties** van VirusScan wordt geopend.
2. Klik op de tab **Geplande scan** (Afbeelding 2-10 op pagina 33).

Afbeelding 2-10. 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**.

  b. 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 tot u een andere geldige optie selecteert.

c. Selecteer het tijdstip waarop de computer moet worden gescand in het vak **Starttijd**.

d. 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 **Op standaard instellen**. Klik anders op **OK**.

Als Scan een virus of een mogelijk ongewenst programma aantreft

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 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* 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. Raadpleeg Een noodhersteldiskette maken in de online Help voor meer informatie.

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

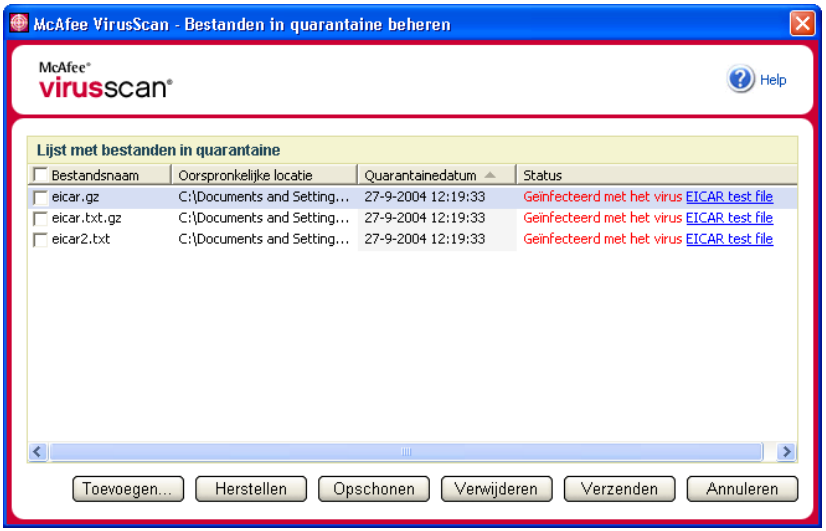
Bestanden in quarantaine beheren

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 worden teruggezet op de oorspronkelijke locatie.

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

1 Klik met de rechtermuisknop op het McAfee-pictogram, wijs **VirusScan** aan en klik op **Bestanden in quarantaine beheren**.

Er wordt een lijst met in quarantaine geplaatste bestanden weergegeven (Afbeelding 2-11 op pagina 36).



Afbeelding 2-11. 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 lijst.

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.

Professional Edition gebruiken 3

McAfee VirusScan Professional Edition bevat McAfee VirusScan en extra software, McAfee SpamKiller en McAfee Shredder.

Opmerking
Dit is een kort overzicht. Raadpleeg de Help van VirusScan, SpamKiller of Shredder voor meer informatie.

McAfee SpamKiller gebruiken

Met McAfee SpamKiller kunt u voorkomen dat spam in uw Postvak IN terechtkomt.

Opmerking
McAfee SpamKiller filtert MSN/Hotmail, maar filtert momenteel niet AOL, Yahoo of andere e-mailaccounts op internet.

Overzicht

Tijdens de installatie hebt u een of meer e-mailaccounts geconfigureerd voor het van ongewenste berichten. U hebt ook het adresboek van uw e-mailprogramma naar uw vriendenlijst geïmporteerd om te voorkomen dat berichten van bekenden worden geblokkeerd.

Ga als volgt te werk om spam te beheren:

1. Open uw e-mailprogramma op de gebruikelijke wijze om berichten te bekijken, verzenden en ontvangen.
2. SpamKiller openen:

   Klik met de rechtermuisknop op het McAfee-pictogram  , wijs **SpamKiller** aan en klik vervolgens op **Geblokkeerde e-mail bekijken**, **Overzicht weergeven**, **Vrienden weergeven** of **Instellingen**. De bijbehorende pagina verschijnt.

   Opmerking
   Als het **aanmeldvenster** verschijnt, voert u het SpamKiller-wachtwoord in en klikt u op **OK**.

Overzichtspagina

Klik op de tab **overzicht** om de overzichtspagina te openen. Hier vindt u de volgende informatie:

- Bij **Status** wordt aangegeven of de filtering is ingeschakeld, wanneer een vriendenlijst het laatst is bijgewerkt en hoeveel spamberichten u vandaag hebt ontvangen. Hier kunt u de filtering van SpamKiller in- of uitschakelen, vriendenlijsten bijwerken en de pagina Geblokkeerde e-mail openen.
- Bij **recente spam** staan de laatste spamberichten die SpamKiller heeft geblokkeerd (uit uw Postvak IN heeft verwijderd). Als u een bericht wilt terugzetten in uw Postvak IN, klikt u op het **reddingspictogram** naast het bericht.
- Bij **overzicht e-mail** staat het totale aantal e-mailberichten, het aantal spamberichten (geblokkeerde berichten) en het percentage spam dat u in totaal hebt ontvangen.
- Bij **recente spam** wordt het soort spam dat u de afgelopen 30 dagen hebt ontvangen, uitgesplitst.

Integratie met Microsoft Outlook en Outlook Express

U kunt de kernfuncties van SpamKiller direct openen vanuit Outlook Express 6.0, Outlook 98, Outlook 2000 en Outlook XP. U kunt spam blokkeren, mensen aan uw vriendenlijst toevoegen en in quarantaine geplaatste e-mail bekijken met een klik op een van de knoppen die zijn geïntegreerd in de werkbalk van Outlook en Outlook Express:

- Klik op het pictogram **Bericht blokkeren** als u het geselecteerde bericht uit uw Postvak IN van Microsoft Outlook wilt verwijderen en het wilt opslaan in de map Geblokkeerde e-mail van SpamKiller.
- Klik op het pictogram **Geblokkeerde berichten bekijken** als u berichten wilt bekijken die zijn geblokkeerd voor uw Microsoft Outlook-account en vervolgens zijn verplaatst naar de map Geblokkeerde e-mail van SpamKiller.
- Klik op het pictogram **Vriend toevoegen** als u het e-mailadres van de afzender wilt toevoegen aan uw Persoonlijke vriendenlijst.

De werkbalk van SpamKiller wordt rechts van de standaardwerkbalken weergegeven in Outlook en Outlook Express. Als de balk niet zichtbaar is, moet u het venster van het e-mailprogramma vergroten of op de pijlen klikken om meer werkbalken weer te geven.

Wanneer de SpamKiller-werkbalk voor het eerst in uw e-mailprogramma verschijnt, kunnen de opdrachten in de werkbalk alleen worden toegepast op nieuwe berichten. Bestaande spam moet handmatig worden verwijderd.

Werken met geblokkeerde en geaccepteerde berichten

Klik op de tab **berichten** om toegang te krijgen tot uw geblokkeerde en geaccepteerde berichten. De pagina's Geblokkeerde e-mail en Geaccepteerde e-mail hebben vrijwel dezelfde functies.

Geblokkeerde e-mail (pagina)

Klik op de tab **Geblokkeerde e-mail** op de berichtenpagina om geblokkeerde berichten te bekijken.

> **Opmerking**
> U kunt de pagina met geblokkeerde berichten ook openen vanuit uw Microsoft Outlook-account door het Postvak IN te openen en op te klikken op de werkbalk van Microsoft Outlook of Microsoft Outlook Express.

Geblokkeerde berichten zijn berichten die door SpamKiller zijn geïdentificeerd als spam, waarna ze zijn verwijderd uit uw Postvak IN en zijn opgeslagen in de map Geblokkeerde e-mail.

Op de pagina Geblokkeerde e-mail staan alle spamberichten die uit uw e-mailaccounts zijn verwijderd. Als u de geblokkeerde e-mail voor een bepaalde account wilt bekijken, klikt u op de vervolgkeuzepijl op de tab **Geblokkeerde e-mail** en selecteert u vervolgens de gewenste account.

In het bovenste berichtenvenster staan de spamberichten gesorteerd op datum. Het meest recente bericht staat bovenaan. In het onderste deelvenster staat de tekst van het geselecteerde bericht.

> **Opmerking**
> Als uw computer Windows 2000 of Windows XP gebruikt, er meerdere gebruikers aan SpamKiller zijn toegevoegd en u zich als gebruiker met beperkte rechten hebt aangemeld, wordt de inhoud van het bericht niet in het onderste deelvenster weergegeven.

In het detailvenster in het midden staan details over het bericht. Klik op de vervolgkeuzepijlen als u het deelvenster met de berichtdetails wilt vergroten en u de berichttekst en de koptekst zonder opmaak, met HTML-labels, wilt bekijken. In het detailvenster staat het volgende:

- **Actie**: hier wordt beschreven hoe SpamKiller het spambericht heeft verwerkt. Het veld Actie is gekoppeld aan de actie van het filter dat het bericht heeft geblokkeerd.
- **Reden**: hiermee wordt aangegeven waarom Spamkiller het bericht heeft geblokkeerd. U kunt op de reden klikken om de filtereditor te openen en het filter te bekijken. In de filtereditor staat waar het filter in een bericht naar zoekt en welke actie SpamKiller moet nemen tegen berichten die door het filter worden gevonden.

- **Van**: hier staat de afzender van het bericht.
- **Datum**: hier staat de datum waarop het bericht aan u is verzonden.
- **Aan**: hier staat aan wie het bericht is verzonden.
- **Onderwerp**: hier staat het onderwerp dat op de onderwerpregel van het bericht wordt weergegeven.

In de linkerkolom staan pictogrammen naast de berichten als er handmatig klachten of foutberichten zijn verzonden:

 Er is een klacht over het bericht verzonden.

 Er is een foutbericht verzonden aan het antwoordadres van het spambericht.

 Er is een klacht en een foutbericht verzonden.

Geaccepteerde e-mail (pagina)

Klik op de tab **Geaccepteerde e-mail** op de berichtenpagina om geaccepteerde berichten te bekijken.

Op de pagina Geaccepteerde e-mail staan alle berichten die in het postvak voor binnenkomende e-mail van al uw e-mailaccounts terecht zijn gekomen. Voor MAPI-accounts staat op de pagina Geaccepteerde e-mail echter geen interne e-mail. Als u de geaccepteerde e-mail voor een bepaalde account wilt bekijken, klikt u op de vervolgkeuzepijl  op de tab **Geaccepteerde e-mail** en selecteert u vervolgens de gewenste account.

> **Opmerking**
> SpamKiller is ontworpen om legitieme e-mail te accepteren. Als er toch legitieme berichten in de lijst Geblokkeerde e-mail terechtkomen, kunt u deze weer in uw Postvak IN (en in de lijst Geaccepteerde e-mail) plaatsen door de berichten te selecteren en vervolgens op **Dit bericht redden** te klikken.

Net als op de pagina Geblokkeerde e-mail staan in het bovenste berichtvenster de berichten gesorteerd op datum. In het onderste deelvenster staat de tekst van het geselecteerde bericht.

Het middelste deelvenster geeft aan of een bericht is verzonden door iemand op een vriendenlijst of dat het bericht voldoet aan de criteria van een filter waarvan de filteractie is ingesteld op **Accepteren** of **Markeren als mogelijke spam**. Klik op de vervolgkeuzepijlen  als u het deelvenster met de berichtdetails wilt vergroten en u de berichttekst en de koptekst zonder opmaak, met HTML-labels, wilt bekijken.

In het detailvenster staat het volgende:

- **Actie**: hier wordt beschreven hoe SpamKiller het bericht heeft verwerkt.
- **Reden**: hier staat waarom Spamkiller het bericht heeft gemarkeerd.
- **Van**: hier staat de afzender van het bericht.
- **Datum**: hier staat de datum waarop het bericht aan u is verzonden.
- **Aan**: hier staat aan wie het bericht is verzonden.
- **Onderwerp**: hier staat het onderwerp dat op de onderwerpregel van het bericht wordt weergegeven.

Naast het geaccepteerde bericht wordt een van de volgende pictogrammen weergegeven:


SpamKiller heeft gedetecteerd dat de afzender van het bericht in een vriendenlijst staat.


Het bericht voldoet aan een filter waarvan de actie is ingesteld op **Markeren als mogelijke spam**.


Er is een klacht over het bericht verzonden.


Er is een foutbericht verzonden aan het antwoordadres van het spambericht.


Er is een klacht en een foutbericht verzonden.

Taken voor geblokkeerde en geaccepteerde e-mail

In het rechterdeelvenster van de pagina's Geblokkeerde e-mail en Geaccepteerde e-mail staan taken die u kunt uitvoeren:

- **Dit bericht blokkeren**: hier wordt een bericht uit uw Postvak IN verwijderd en in de Spamkiller-map Geblokkeerde e-mail opgeslagen. (Deze optie staat alleen op de pagina Geaccepteerde e-mail.)
- **Dit bericht redden**: hier wordt een bericht teruggeplaatst in uw Postvak IN en wordt het dialoogvenster Reddingsopties geopend. (Deze optie staat alleen op de pagina Geblokkeerde e-mail.) U kunt de afzender automatisch aan uw vriendenlijst toevoegen en alle berichten van deze afzender redden.
- **Dit bericht verwijderen**: hier wordt een geselecteerd bericht verwijderd.
- **Vriend toevoegen**: hier wordt de naam van de afzender, het e-mailadres, een domein of een mailinglijst aan een vriendenlijst toegevoegd.
- **Filter toevoegen**: hier wordt een filter gemaakt.

- **Rapporteren aan McAfee**: hier kunt u McAfee informeren over specifieke spamberichten die u hebt ontvangen.
- **Klacht verzenden**: hier kunt u een klacht over spam verzenden aan de beheerder van het domein van de afzender of naar een ander e-mailadres dat u opgeeft.
- **Foutbericht verzenden**: hier kunt u een foutbericht verzenden aan het antwoordadres van het spambericht.

Berichten redden

Als er op de pagina Geblokkeerde e-mail legitieme berichten terechtkomen, kunt u deze berichten terugzetten in uw Postvak IN.

Ga als volgt te werk om een bericht te redden:

1. Bekijk uw geblokkeerde e-mailberichten:
   - Klik in SpamKiller op de tab **berichten** en klik vervolgens op de tab **Geblokkeerde e-mail**.
   - Klik in uw Postvak IN van Microsoft Outlook of Outlook Express op om de pagina Geblokkeerde e-mail voor die account te openen.

   De pagina Geblokkeerde e-mail verschijnt.
2. Selecteer een bericht en klik vervolgens op **Dit bericht redden**.

   Het dialoogvenster Reddingsopties wordt geopend met de volgende geselecteerde standaardopties:
   - **Vriend toevoegen**
   - **Alle berichten van deze afzender redden**
3. Klik op **OK**. De afzender is aan uw vriendenlijst toegevoegd en alle berichten van deze afzender zijn in uw Postvak IN en de map Geaccepteerde e-mail teruggezet.

Berichten blokkeren

U kunt spamberichten blokkeren die al in uw Postvak IN staan. Wanneer u een bericht blokkeert, maakt SpamKiller automatisch een filter om dat bericht uit uw Postvak IN te verwijderen. U kunt berichten in uw Postvak IN blokkeren vanaf de pagina Geaccepteerde e-mail of vanuit Microsoft Outlook of Outlook Express.

Ga als volgt te werk om een bericht vanaf de pagina Geaccepteerde e-mail te blokkeren:

1. Klik op de tab **berichten** en vervolgens op de tab **Geaccepteerde e-mail**. De pagina Geaccepteerde e-mail wordt weergegeven met daarop de berichten momenteel in uw Postvak IN staan.
2. Selecteer een bericht en klik vervolgens op **Dit bericht blokkeren**. Het bericht wordt uit uw Postvak IN en van de pagina Geaccepteerde e-mail verwijderd en een kopie ervan verschijnt op de pagina Geblokkeerde e-mail.

Ga als volgt te werk om een bericht vanuit Microsoft Outlook te blokkeren:

1. Open in Microsoft Outlook of Outlook Express uw Postvak IN. U kunt alleen externe berichten (afkomstig van een internetserver) blokkeren.
2. Selecteer een bericht en klik op  . Een kopie van het bericht wordt in de map Geblokkeerde e-mail geplaatst.

Berichten verwijderen

Spam die door SpamKiller wordt gevonden, wordt standaard uit het Postvak IN verwijderd en in de SpamKiller-map Geblokkeerde e-mail opgeslagen. SpamKiller verwijdert de geblokkeerde berichten automatisch uit de map Geblokkeerde e-mail na 15 dagen. U kunt instellen hoe vaak SpamKiller de geblokkeerde berichten automatisch verwijdert. U kunt ook de berichten handmatig verwijderen.

Berichten in de map Geaccepteerde e-mail worden niet automatisch verwijderd, omdat de inhoud van deze map overeenkomt met de huidige inhoud van uw Postvak IN.

Spamberichten hoeven niet naar de map Geblokkeerde e-mail te worden verplaatst. SpamKiller kan ook aan de onderwerpregel van de e-mail het label [spam] of een label naar uw keuze toevoegen en het bericht in uw Postvak IN laten staan. Het labelen van berichten kan handig zijn als u de gelabelde berichten naar een andere map in uw e-mailclient wilt verplaatsen, bijvoorbeeld een map met de naam 'troep'. U kunt de gelabelde berichten verplaatsen door in uw e-mailclient een regel te maken die naar berichten met het label [spam] zoekt en deze vervolgens in een door u te bepalen map opslaat.

Ga als volgt te werk om de instelling voor het automatisch verwijderen van geblokkeerde e-mail te wijzigen:

1 Klik op de tab **Instellingen** en klik vervolgens op het pictogram **Filteropties**.

2 Selecteer hoe SpamKiller spamberichten moet verwerken:

- **Spam in het postvak Geblokkeerde e-mail plaatsen**: spamberichten worden uit het Postvak IN verwijderd en in de map Geblokkeerde e-mail van SpamKiller geplaatst.
- **Geblokkeerde e-mail bewaren gedurende ____ dagen**: geblokkeerde berichten blijven gedurende het opgegeven aantal dagen in de map Geblokkeerde e-mail staan.
- **Spam labelen en bewaren in het Postvak IN**: spamberichten blijven in uw Postvak IN staan, maar aan de onderwerpregel wordt [spam] of een door u opgegeven label toegevoegd.

3 Klik op **OK**.

Ga als volgt te werk om een bericht handmatig te verwijderen:

1 Uw geblokkeerde e-mailberichten bekijken:

- Klik in SpamKiller op de tab **berichten** en klik vervolgens op de tab **Geblokkeerde e-mail**.
- Klik in uw Postvak IN van Microsoft Outlook of Outlook Express op om de pagina Geblokkeerde e-mail voor die account te openen.

De pagina Geblokkeerde e-mail verschijnt.

2 Selecteer het bericht dat u wilt verwijderen en klik op **Dit bericht verwijderen**. Er verschijnt een dialoogvenster waarin om bevestiging wordt gevraagd.

3 Klik op **Ja** om het bericht te verwijderen.

Spam rapporteren aan McAfee

U kunt spam rapporteren aan McAfee. De spam wordt vervolgens geanalyseerd om filterupdates te maken.

Ga als volg te werk om spam aan McAfee te rapporteren:

1 Klik op de tab **berichten** en klik vervolgens op de tab **Geblokkeerde e-mail** of **Geaccepteerde e-mail**. De pagina Geblokkeerde e-mail of Geaccepteerde e-mail verschijnt.

2 Selecteer een bericht en klik vervolgens op **Rapporteren aan McAfee**. Er verschijnt een dialoogvenster waarin om bevestiging wordt gevraagd.

3 Klik op **Ja** om het bericht automatisch naar McAfee te verzenden.

Handmatig klachten verzenden

U kunt een klacht verzenden om te voorkomen dat een afzender u nog meer spam stuurt. Zie 'Klachten en foutberichten verzenden' in de Help voor meer informatie.

Ga als volgt te werk om handmatig een klacht te verzenden:

1. Klik op de tab **berichten** en klik vervolgens op de tab **Geblokkeerde e-mail** of **Geaccepteerde e-mail**. Er verschijnt een berichtenlijst.
2. Selecteer een bericht waarover u wilt klagen en klik vervolgens op **Klacht verzenden**. Het dialoogvenster Klacht verzenden verschijnt.
3. Selecteer een ontvanger voor de klacht:

   Waarschuwing
   In de meeste gevallen kunt u beter niet **De afzender** selecteren. Door een klacht aan de afzender te sturen, maakt u kenbaar dat uw e-mailadres bestaat, waardoor u in de toekomst nog meer spam van die afzender kunt ontvangen.

4. Klik op **Volgende** en volg de instructies in de dialoogvensters die verschijnen.

Foutberichten verzenden

U kunt een foutbericht verzenden om te voorkomen dat een afzender u nog meer spam stuurt. Zie 'Klachten en foutberichten verzenden' in de Help voor meer informatie.

Ga als volgt te werk om handmatig een foutbericht te verzenden:

1. Klik op de tab **berichten** en klik vervolgens op de tab **Geblokkeerde e-mail** of **Geaccepteerde e-mail**. Er verschijnt een berichtenlijst.
2. Selecteer een bericht en klik vervolgens op **Foutbericht verzenden**. Er wordt een foutbericht verzonden aan het antwoordadres van het spambericht.

McAfee Shredder gebruiken

Met McAfee Shredder  wordt uw privacy beschermd doordat ongewenste bestanden snel en veilig kunnen worden gewist.

U kunt verwijderde bestanden altijd terugzetten, zelfs nadat u de Prullenbak hebt leeggemaakt. Als u een bestand verwijdert, wordt deze ruimte op de schijf in Windows aangegeven als niet langer in gebruik, maar het bestand is er nog wel.

Waarom bestanden in Windows niet definitief worden verwijderd

Als u een bestand definitief wilt verwijderen, moet u het herhaaldelijk overschrijven met nieuwe gegevens. Als in Microsoft Windows bestanden definitief worden verwijderd, zouden bestandsbewerkingen erg langzaam worden uitgevoerd. Als u een document vernietigt, wordt niet altijd voorkomen dat dit bestand wordt teruggezet. In bepaalde programma's worden namelijk verborgen kopieën gemaakt van geopende documenten. Als u alleen documenten vernietigt die in de Verkenner worden weergegeven, hebt u mogelijk nog steeds tijdelijke kopieën van deze documenten. U kunt het beste regelmatig de beschikbare ruimte op uw schijf opschonen zodat de tijdelijke bestanden definitief worden verwijderd.

Opmerking
Met de hulpprogramma's voor computercriminalistiek kunt u belastingoverzichten, curricula vitae of andere documenten die u hebt verwijderd, terughalen.

Wat wordt er gewist met McAfee Shredder

Met McAfee Shredder kunt u de volgende onderdelen veilig en definitief wissen:

- Een of meer bestanden of mappen
- Een hele schijf
- De sporen die u achterlaat tijdens het surfen op het web

Bestanden definitief wissen in Windows Verkenner

Ga als volgt te werk om bestanden te vernietigen via Windows Verkenner:

1. Open Windows Verkenner en selecteer de bestanden die u wilt vernietigen.
2. Klik met de rechtermuisknop op de geselecteerde bestanden, wijs **Kopiëren naar** aan en klik op **McAfee Shredder**.

De Windows Prullenbak leegmaken

McAfee Shredder biedt een veiliger methode voor het leegmaken van de Prullenbak.

Ga als volgt te werk om de inhoud van de Prullenbak te vernietigen:

1. Klik met de rechtermuisknop op de Prullenbak op het bureaublad in Windows.
2. Selecteer **Prullenbak-inhoud vernietigen** en volg de instructies op het scherm.

Shredder-instellingen aanpassen

U kunt uw Shredder-instellingen aanpassen:

- Het gewenste aantal vernietigingscycli opgeven.
- Een waarschuwingsbericht weergeven als u bestanden vernietigt.
- De vaste schijf controleren op fouten voordat u bestanden gaat vernietigen.
- McAfee Shredder toevoegen aan het menu Kopiëren naar.
- Een Shredder-pictogram op het bureaublad plaatsen.

Als u de Shredder-instellingen wilt aanpassen, opent u McAfee Shredder, klikt u op **Eigenschappen** en volgt u de instructies op het scherm.

Index

P

Q

S

T

U

V

W

Voor meer informatie over producten, diensten wereldwijd en ondersteuning kunt u contact opnemen met een officiële McAfee-vertegenwoordiger of schrijft u naar:

McAfee
International BV
PO Box 58326, 1040 HH Amsterdam
Nederland

nl.mcafee.com

http://www.mcafeehulp.com

NA-675-0010-NL-1