

McAfee®
VirusScan® Plus 2008

AntiVirus, Firewall & AntiSpyware
Gebbruikershandleiding

Inhoud

Inleiding	3
McAfee SecurityCenter	5
SecurityCenter-functies	6
SecurityCenter gebruiken	7
SecurityCenter bijwerken	13
Beveiligingsproblemen oplossen of negeren	17
Werken met waarschuwingen	23
Gebeurtenissen weergeven	29
McAfee VirusScan	31
VirusScan-functies	33
Real-time virusbeveiliging starten	34
Aanvullende beveiliging starten	37
Virusbeveiliging instellen	41
De computer scannen	59
Werken met scanresultaten	63
McAfee Personal Firewall	67
Functies van Personal Firewall	68
Firewall starten	71
Werken met waarschuwingen	73
Informatieve waarschuwingen beheren	77
Het beveiligingsniveau van Firewall configureren	79
Programma's en toegangsregels beheren	93
Systemservices beheren	105
Computerverbindingen beheren	111
Logbestanden, controles en analyses	121
Informatie over internetbeveiliging	133
McAfee QuickClean	135
Functies van QuickClean	136
De computer opschonen	137
De computer defragmenteren	141
Taken plannen	142
McAfee Shredder	147
Functies van Shredder	148
Bestanden, mappen en schijven vernietigen	149
McAfee Network Manager	151
Functies van Network Manager	152
Informatie over pictogrammen van Network Manager	153
Een beheerd netwerk instellen	155
Het netwerk op afstand beheren	163
McAfee EasyNetwork	169
Functies van EasyNetwork	170
EasyNetwork instellen	171
Bestanden delen en versturen	177
Printers delen	183

Naslag	185
Verklarende woordenlijst	186
<hr/>	
McAfee	201
<hr/>	
Copyright	201
Licentie	202
Klant- en technische ondersteuning	203
McAfee Virtual Technician gebruiken	204
Ondersteuning en downloads	205
Index	214
<hr/>	

HOOFDSTUK 1

Inleiding

McAfee VirusScan Plus biedt proactieve computerbeveiliging om aanvallen te verhinderen, zodat u alles kunt beschermen wat voor u van waarde is en u onbezorgd op internet kunt surfen, zoeken en downloaden. De risicoclassificaties van McAfee SiteAdvisor helpen u onveilige websites te vermijden. Deze service voorkomt bovendien aanvallen langs meerdere routes, door antivirus-, antispyware- en firewalltechnologie met elkaar te combineren. Met de beveiligingsservice van McAfee bent u voortdurend verzekerd van de nieuwste software, zodat uw bescherming altijd actueel is. U kunt nu eenvoudig beveiligingsfuncties toevoegen en beheren voor meerdere computers bij u thuis. De prestaties zijn verbeterd, zodat u ongestoord wordt beschermd.

In dit hoofdstuk

McAfee SecurityCenter	5
McAfee VirusScan	31
McAfee Personal Firewall	67
McAfee QuickClean.....	135
McAfee Shredder	147
McAfee Network Manager.....	151
McAfee EasyNetwork	169
Naslag.....	185
McAfee	201
Klant- en technische ondersteuning	203

HOOFDSTUK 2

McAfee SecurityCenter

Met McAfee SecurityCenter kunt u de beveiligingsstatus van uw computer bijhouden, direct zien of de beveiligingsservices voor virussen, spyware, e-mail en de firewall op uw computer zijn bijgewerkt en kunt u beveiligingsproblemen oplossen. Het biedt alle navigatiehulpmiddelen voor het coördineren en beheren van alle gebieden van computerbeveiliging.

Voordat u begint met de configuratie en het beheer van de beveiliging van uw computer, moet u de interface van SecurityCenter bekijken en nagaan of u het verschil begrijpt tussen de beveiligingsstatus, de beveiligingscategorieën en de beveiligingsservices. Werk vervolgens SecurityCenter bij, zodat u over de meest recente beveiliging van McAfee kunt beschikken.

Na het voltooien van de eerste configuratietaken kunt u SecurityCenter gebruiken voor het bijhouden van de beveiligingsstatus van de computer. Als SecurityCenter een beveiligingsprobleem vaststelt, ontvangt u hierover een waarschuwing, zodat u het probleem kunt oplossen of negeren (op basis van de ernst ervan). U kunt ook de SecurityCenter-gebeurtenissen, zoals wijzigingen in de configuratie voor virusscans, in een gebeurtenislogboek bekijken.

Opmerking: SecurityCenter stelt u op de hoogte van kritieke en niet-kritieke beveiligingsproblemen zodra deze worden vastgesteld. Als u hulp nodig hebt bij het analyseren van beveiligingsproblemen, kunt u McAfee Virtual Technician uitvoeren.

In dit hoofdstuk

SecurityCenter-functies.....	6
SecurityCenter gebruiken.....	7
SecurityCenter bijwerken	13
Beveiligingsproblemen oplossen of negeren	17
Werken met waarschuwingen.....	23
Gebeurtenissen weergeven	29

SecurityCenter-functies

SecurityCenter biedt de volgende functies:

Vereenvoudigde beveiligingsstatus

Hiermee kunt u gemakkelijk de beveiligingsstatus van de computer inspecteren, op updates controleren en potentiële beveiligingsproblemen oplossen.

Geautomatiseerde updates en upgrades

U kunt automatisch updates downloaden en installeren voor uw geregistreerde programma's. Wanneer er een nieuwe versie van een geregistreerd McAfee-programma beschikbaar is, ontvangt u die gratis gedurende de looptijd van uw abonnement. Zo bent u er zeker van dat uw beveiliging altijd up-to-date is.

Real-time waarschuwingen

Via beveiligingswaarschuwingen wordt u op de hoogte gebracht van nieuwe virusuitbraken en veiligheidsrisico's, en beschikt u over opties om de bedreigingen te verwijderen, neutraliseren of er meer informatie over te lezen.

HOOFDSTUK 3

SecurityCenter gebruiken

Voordat u SecurityCenter gaat gebruiken, moet u de onderdelen en configuratiegebieden bestuderen voor het beheer van de beveiligingsstatus van de computer. Zie De beveiligingsstatus begrijpen (pagina 8) en De beveiligingscategorieën begrijpen (pagina 9) voor meer informatie over de terminologie die in deze afbeelding wordt gebruikt. Vervolgens kunt u uw McAfee-accountinformatie controleren en nagaan of uw abonnement nog geldig is.



In dit hoofdstuk

De beveiligingsstatus begrijpen	8
De beveiligingscategorieën begrijpen	9
De beveiligingservices begrijpen	10
Uw McAfee-account beheren	11

De beveiligingsstatus begrijpen

De beveiligingsstatus van de computer wordt weergegeven in het beveiligingsstatusgebied van het deelvenster Startpagina van SecurityCenter. Hier wordt aangeduid of de computer volledig is beschermd tegen de meest recente veiligheidsrisico's of kan worden beïnvloed door zaken als externe aanvallen op de beveiliging, andere beveiligingsprogramma's en programma's die toegang hebben tot internet.

De beveiligingsstatus van de computer kan rood, geel of groen zijn.

Beveiligingsstatus	Beschrijving
Rood	<p>Uw computer is niet beschermd. Het beveiligingsstatusgebied op het deelvenster Startpagina van SecurityCenter Home is rood en duidt aan dat u niet beveiligd bent. SecurityCenter meldt dat u ten minste één kritiek beveiligingsprobleem hebt.</p> <p>Als u over volledige beveiliging wilt beschikken, moet u alle kritieke beveiligingsproblemen in elke beveiligingscategorie oplossen (de status van de probleemcategorie wordt ingesteld op Actie vereist, tevens in rood). Zie Beveiligingsproblemen oplossen (pagina 18) voor informatie over het oplossen van beveiligingsproblemen.</p>
Geel	<p>Uw computer is gedeeltelijk beschermd. Het beveiligingsstatusgebied in het deelvenster Startpagina van SecurityCenter is geel en duidt aan dat u niet beveiligd bent. SecurityCenter meldt dat u ten minste één niet-kritiek beveiligingsprobleem hebt.</p> <p>Voor volledige beveiliging moet u de niet-kritieke beveiligingsproblemen in elke beveiligingscategorie oplossen of negeren. Zie Beveiligingsproblemen oplossen of negeren (pagina 17) voor informatie over het oplossen of negeren van beveiligingsproblemen.</p>
Groen	<p>Uw computer is volledig beschermd. Het beveiligingsstatusgebied in het deelvenster Startpagina van SecurityCenter is groen en duidt aan dat u beveiligd bent. SecurityCenter meldt geen kritieke of niet-kritieke beveiligingsproblemen.</p> <p>In elke beveiligingscategorie worden de services vermeld die uw computer beveiligen.</p>

De beveiligingscategorieën begrijpen

De beveiligingsservices van SecurityCenter zijn onderverdeeld in vier categorieën: Computer en bestanden, Internet en netwerk, E-mail en expresberichten en Ouderlijk toezicht. Met behulp van deze categorieën kunt u door de beveiligingsservices navigeren die uw computer beschermen, en deze configureren.

Als u een beveiligingsservice wilt configureren, klikt u op een categorienaam, waarna de bijbehorende beveiligingsservices worden weergegeven en eventuele beveiligingsproblemen die voor deze services zijn vastgesteld. Als de beveiligingsstatus van de computer rood of geel is, wordt voor een of meer categorieën het bericht *Actie vereist* of *Opgelet* weergegeven, waarmee wordt aangeduid dat SecurityCenter een probleem binnen deze categorie heeft vastgesteld. Zie *De beveiligingsstatus begrijpen* (pagina 8) voor meer informatie over de beveiligingsstatus.

Beveiligings-categorie	Beschrijving
Computer en bestanden	In de categorie Computer en bestanden kunt u de volgende beveiligingsservices configureren: <ul style="list-style-type: none"> ▪ Virusbeveiliging ▪ MOP-beveiliging ▪ Systeemcontroles ▪ Beveiliging van Windows
Internet en netwerk	In de categorie Internet en netwerk kunt u de volgende beveiligingsservices configureren: <ul style="list-style-type: none"> ▪ Firewallbeveiliging ▪ Bescherming van de identiteit
E-mail en expresberichten	In de categorie E-mail en expresberichten kunt u de volgende beveiligingsservices configureren: <ul style="list-style-type: none"> ▪ E-mailbeveiliging ▪ Spambeveiliging
Parental Controls	In de categorie Parental Controls kunt u de volgende beveiligingsservices configureren: <ul style="list-style-type: none"> ▪ Inhoud blokkeren

De beveiligingsservices begrijpen

Beveiligingsservices zijn de kernonderdelen van SecurityCenter die u configureert om de computer te beveiligen. Beveiligingsservices komen rechtstreeks overeen met McAfee-programma's. Als u bijvoorbeeld VirusScan installeert, zijn de volgende beveiligingsservices na installatie beschikbaar: Virusbeveiliging, MOP-beveiliging, Systeemcontroles en Beveiliging van Windows. Raadpleeg de Help van VirusScan voor gedetailleerde informatie over specifieke beveiligingsservices.

Alle beveiligingsservices die met een programma verband houden, zijn standaard ingeschakeld als u het programma installeert; u kunt echter op elk gewenst moment een beveiligingsservice uitschakelen. Als u bijvoorbeeld Privacy Service installeert, zijn Inhoud blokkeren en Bescherming van de identiteit beide ingeschakeld. Als u de beveiligingsservice Inhoud blokkeren niet wilt gebruiken, kunt u deze volledig uitschakelen. U kunt tijdens het uitvoeren van installaties of onderhoudstaken een beveiligingsservice tijdelijk uitschakelen.

Uw McAfee-account beheren

U kunt uw McAfee-account beheren vanuit SecurityCenter en de accountgegevens hierin gemakkelijk weergeven en controleren, evenals de status van uw abonnement.

Opmerking: als u de McAfee-programma's vanaf cd-rom hebt geïnstalleerd, moet u deze op de McAfee-website registreren om de McAfee-account in te stellen of bij te werken. Alleen dan hebt u recht op regelmatige, automatische programma-updates.


Uw McAfee-account beheren

U hebt gemakkelijk toegang tot de McAfee-accountgegevens (Mijn account) vanuit SecurityCenter.

- 1 Klik op **Mijn account** onder **Algemene taken**.
- 2 Meld u aan bij uw McAfee-account.

Uw abonnement controleren

U moet regelmatig de geldigheid van uw abonnement controleren.

- Klik met de rechtermuisknop op het pictogram  van het SecurityCenter in het systeemvak, uiterst rechts op de taakbalk en klik vervolgens op **Abonnement controleren**.

HOOFDSTUK 4

SecurityCenter bijwerken

SecurityCenter zorgt ervoor dat uw geregistreerde McAfee-programma's up-to-date blijven doordat het programma elke vier uur op online updates controleert en deze installeert. Afhankelijk van de programma's die u hebt geïnstalleerd en geregistreerd, kunnen online updates de meest recente virusdefinitiebestanden bevatten en upgrades voor de beveiliging tegen hackers, spam, spyware of bescherming van uw privacy. Als u binnen de standaardperiode van vier uur op updates wilt controleren, kunt u dat op elk gewenst moment doen. Terwijl er in SecurityCenter naar updates wordt gezocht, kunt u doorgaan met andere taken.

Hoewel dit niet wordt aanbevolen, kunt u de manier wijzigen waarop SecurityCenter op updates controleert en deze installeert. U kunt SecurityCenter bijvoorbeeld configureren voor het downloaden, maar niet installeren van updates, of u kunt een waarschuwing ontvangen voordat updates worden gedownload of geïnstalleerd. U kunt het automatisch bijwerken ook uitschakelen.

Opmerking: als u de McAfee-programma's vanaf een cd-rom hebt geïnstalleerd, kunt u alleen regelmatige, automatische updates voor deze programma's ontvangen als u ze op de McAfee-website registreert.

In dit hoofdstuk

Controleren op updates.....	14
Automatische updates configureren	14
Automatische updates uitschakelen.....	15

Controleren op updates

SecurityCenter controleert standaard elke vier uur op updates wanneer uw computer een internetverbinding heeft; u kunt, als u dat wilt, ook binnen de periode van vier uur op updates controleren. Als u automatische updates hebt uitgeschakeld, is het uw eigen verantwoordelijkheid om regelmatig op updates te controleren.

- Klik in het deelvenster Startpagina van SecurityCenter op **Bijwerken**.

Tip: u kunt controleren op updates zonder SecurityCenter te starten door met de rechtermuisknop op het

SecurityCenter-pictogram  in het systeemvak geheel rechts op de taakbalk te klikken, en vervolgens op **Updates** te klikken.

Automatische updates configureren

SecurityCenter controleert standaard automatisch elke vier uur op updates en installeert deze als uw computer verbinding heeft met internet. Als u dit standaardgedrag wilt wijzigen, kunt u SecurityCenter configureren om updates automatisch te downloaden en u te melden wanneer de updates gereed zijn om te worden geïnstalleerd, of om u een melding te geven voordat de updates worden gedownload.

Opmerking: SecurityCenter stelt u met behulp van een waarschuwing op de hoogte als updates kunnen worden gedownload of geïnstalleerd. Vanuit de waarschuwing kunt u de updates downloaden of installeren, of de updates uitstellen. Als u programma's bijwerkt vanuit een waarschuwing, wordt u mogelijk gevraagd om uw abonnement te controleren voordat u kunt downloaden en installeren. Zie Werken met waarschuwingen (pagina 23) voor meer informatie.

- 1 Open het configuratiedeelvenster van SecurityCenter.
Hoe?
 1. Klik op **Startpagina** onder **Algemene taken**.
 2. Klik in het rechterdeelvenster, onder **SecurityCenter-informatie**, op **Configureren**.
- 2 Klik in het configuratiedeelvenster van SecurityCenter, onder **Automatische updates zijn uitgeschakeld**, op **Aan**, en klik vervolgens op **Geavanceerd**.
- 3 Klik op een van de volgende knoppen:
 - **De updates automatisch installeren en een waarschuwing weergeven wanneer mijn services zijn bijgewerkt (aanbevolen)**

- **De updates automatisch downloaden en een waarschuwing weergeven wanneer ze gereed zijn voor installatie**
- **Een waarschuwing weergeven voordat updates worden gedownload**

4 Klik op **OK**.

Automatische updates uitschakelen

Als u automatische updates uitschakelt, is het uw eigen verantwoordelijkheid om regelmatig op updates te controleren. Anders beschikt uw computer niet over de meest recente beveiliging. Zie Controleren op updates (pagina 14) voor informatie over het handmatig controleren op updates.

1 Open het configuratiedeelvenster van SecurityCenter.

Hoe?

1. Klik op **Startpagina** onder **Algemene taken**.
2. Klik in het rechterdeelvenster, onder **SecurityCenter-informatie**, op **Configureren**.

2 Klik in het configuratiedeelvenster van SecurityCenter, onder **Automatische updates zijn ingeschakeld**, op **Uit**.

Tip: u schakelt automatische updates in door op de knop **Aan** te klikken of door de optie **Automatisch bijwerken uitschakelen en handmatige controle op updates toestaan** uit te schakelen in het deelvenster Update-opties.

HOOFDSTUK 5

Beveiligingsproblemen oplossen of negeren

SecurityCenter stelt u op de hoogte van kritieke en niet-kritieke beveiligingsproblemen zodra deze worden vastgesteld. Voor kritieke beveiligingsproblemen is onmiddellijk actie vereist omdat deze uw beveiligingsstatus in gevaar brengen (de kleur wordt gewijzigd in rood). Voor niet-kritieke problemen is geen onmiddellijke actie vereist; deze kunnen de beveiligingsstatus in gevaar brengen, maar dat hoeft niet het geval te zijn (dit is afhankelijk van het type probleem). Als u een groene beveiligingsstatus wilt bereiken, moet u alle kritieke problemen oplossen en alle niet-kritieke problemen oplossen of negeren. Als u hulp nodig hebt bij het analyseren van beveiligingsproblemen, kunt u McAfee Virtual Technician uitvoeren. Raadpleeg de Help van McAfee Virtual Technician voor meer informatie over McAfee Virtual Technician.

In dit hoofdstuk

Beveiligingsproblemen oplossen	18
Beveiligingsproblemen negeren	20

Beveiligingsproblemen oplossen

De meeste beveiligingsproblemen worden automatisch opgelost; voor andere problemen moet u echter actie ondernemen. Als Firewallbeveiliging bijvoorbeeld is uitgeschakeld, kunt u dit automatisch door SecurityCenter laten inschakelen. Als Firewallbeveiliging echter niet is geïnstalleerd, moet u het eerst installeren. In de volgende tabel worden enkele acties beschreven die u kunt ondernemen voor het handmatig oplossen van problemen:

Probleem	Actie
In de afgelopen 30 dagen is uw computer niet volledig gescand.	Voer handmatig een scan uit voor de computer. Raadpleeg de Help van VirusScan voor meer informatie.
Uw signatuurbestanden voor detectie (DAT's) zijn verouderd.	Werk de beveiliging handmatig bij. Raadpleeg de Help van VirusScan voor meer informatie.
Een programma is niet geïnstalleerd.	Installeer het programma vanaf de website of de cd-rom van McAfee.
Bepaalde onderdelen ontbreken voor een programma.	Installeer het programma opnieuw vanaf de website of de cd-rom van McAfee.
Een programma is niet geregistreerd en kan daarom niet volledig worden beveiligd.	Registreer het programma op de McAfee-website.
Een programma is verlopen.	Controleer uw accountstatus op de McAfee-website.

Opmerking: één beveiligingsprobleem is meestal van invloed op meerdere beveiligingscategorieën. In dat geval, wordt het probleem voor alle categorieën opgelost als u het in één beveiligingscategorie herstelt.

Beveiligingsproblemen automatisch herstellen

SecurityCenter kan de meeste beveiligingsproblemen automatisch oplossen. De wijzigingen in de configuratie die door SecurityCenter worden aangebracht bij het automatisch oplossen van problemen, worden niet in het gebeurtenislogboek vastgelegd. Zie Gebeurtenissen weergeven (pagina 29) voor meer informatie over gebeurtenissen.

- 1 Klik op **Startpagina** onder **Algemene taken**.
- 2 Klik in het deelvenster Startpagina van SecurityCenter, in het beveiligingsgebied, op **Herstellen**.

Beveiligingsproblemen handmatig herstellen

Als een of meer beveiligingsproblemen blijven bestaan nadat u deze automatisch hebt opgelost, kunt u de problemen handmatig herstellen.

- 1 Klik op **Startpagina** onder **Algemene taken**.
- 2 Klik in het deelvenster Startpagina van SecurityCenter op de beveiligingscategorie waarin SecurityCenter het probleem heeft gemeld.
- 3 Klik op de koppeling na de beschrijving van het probleem.

Beveiligingsproblemen negeren

Als door SecurityCenter een niet-kritiek probleem wordt vastgesteld, kunt u het oplossen of negeren. Andere niet-kritieke problemen (die bijvoorbeeld ontstaan als Anti-Spam of Privacy Service niet zijn geïnstalleerd) worden automatisch genegeerd. Genegeerde problemen worden alleen weergegeven in het gebied met beveiligingscategorie-informatie van het deelvenster Startpagina van SecurityCenter als de beveiligingsstatus van de computer groen is. Als u een probleem negeert en later besluit dat u het wilt weergeven in het gebied met beveiligingscategorie-informatie, zelfs als de beveiligingsstatus van de computer niet groen is, kunt u het genegeerde probleem alsnog weergeven.

Een beveiligingsprobleem negeren

Als door SecurityCenter een niet-kritiek probleem wordt vastgesteld dat u niet wilt oplossen, kunt u het negeren. Als u het probleem negeert, wordt het verwijderd uit het gebied met beveiligingscategorie-informatie in SecurityCenter.

- 1 Klik op **Startpagina** onder **Algemene taken**.
- 2 Klik in het deelvenster Startpagina van SecurityCenter op de beveiligingscategorie waarin het probleem is vastgesteld.
- 3 Klik op de koppeling **Negeren** naast het beveiligingsprobleem.

Genegeerde problemen weergeven of verbergen

U kunt een genegeerd beveiligingsprobleem, afhankelijk van de ernst hiervan, weergeven of verbergen.

- 1 Open het deelvenster Waarschuwingsopties.
Hoe?
 1. Klik op **Startpagina** onder **Algemene taken**.
 2. Klik in het rechterdeelvenster, onder **SecurityCenter-informatie**, op **Configureren**.
 3. Klik op **Geavanceerd** onder **Waarschuwingen**.
- 2 Klik in het configuratiedeelvenster van SecurityCenter op **Genegeerde problemen**.
- 3 Ga in het deelvenster Genegeerde problemen op een van de volgende manieren te werk:
 - Als u een probleem wilt negeren, schakelt u het bijbehorende selectievakje in.
 - Als u een probleem wilt rapporteren in het gebied met beveiligingscategorie-informatie, schakelt u het bijbehorende selectievakje uit.

4 Klik op **OK**.

Tip: u kunt een probleem ook negeren door op de koppeling **Negeren** naast het gemelde probleem te klikken in het gebied met beveiligingscategorie-informatie.

HOOFDSTUK 6

Werken met waarschuwingen

Waarschuwingen zijn kleine pop-upvensters die worden weergegeven in de rechterbenedenhoek van het scherm als bepaalde SecurityCenter-gebeurtenissen plaatsvinden. In een waarschuwing ziet u gedetailleerde informatie over een gebeurtenis en aanbevelingen en opties voor het oplossen van problemen die mogelijk aan de gebeurtenis zijn gekoppeld. Bepaalde waarschuwingen kunnen ook koppelingen bevatten naar aanvullende informatie over de gebeurtenis. Met deze koppelingen kunt u de wereldwijde website van McAfee openen of informatie verzenden naar McAfee voor probleemoplossing.

Er zijn drie typen waarschuwingen: rood, geel en groen.

Type waarschuwing	Beschrijving
Rood	Een rode waarschuwing is een kritieke melding waarbij een reactie van u vereist is. Rode waarschuwingen vinden plaats als SecurityCenter niet kan vaststellen hoe een beveiligingsprobleem automatisch kan worden opgelost.
Geel	Een gele waarschuwing is een niet-kritieke melding waarbij meestal een reactie van u vereist is.
Groen	Een groene waarschuwing is een niet-kritieke melding waarbij geen reactie van u vereist is. In groene waarschuwingen ziet u eenvoudige informatie over een gebeurtenis.

Omdat waarschuwingen een cruciale rol spelen bij het bewaken en beheren van de beveiligingsstatus, kunt u deze niet uitschakelen. U kunt echter wel bepalen of bepaalde typen informatieve waarschuwingen worden weergegeven en u kunt bepaalde andere waarschuwingsopties instellen (zoals of SecurityCenter een geluid afspeelt bij een waarschuwing of het startscherm van McAfee wordt weergegeven bij het opstarten).

In dit hoofdstuk

Informatiewaarschuwingen weergeven en verbergen	24
Waarschuwingsopties configureren	26

Informatiewaarschuwingen weergeven en verbergen

Informatiewaarschuwingen worden weergegeven wanneer er gebeurtenissen optreden die de beveiliging van uw computer niet in gevaar brengen. Als u bijvoorbeeld Firewallbeveiliging instelt, wordt er standaard een informatiewaarschuwing weergegeven als aan een programma op uw computer toegang tot internet wordt verleend. Als u wilt dat bepaalde typen informatiewaarschuwingen niet worden weergegeven, kunt u deze verbergen. Als u wilt dat geen enkele informatiewaarschuwing wordt weergegeven, kunt u deze geheel verbergen. U kunt ook alle informatiewaarschuwingen verbergen als u een spel in de modus Volledig scherm op de computer speelt. Als u klaar bent met het spel en de modus Volledig scherm uitschakelt, worden de informatiewaarschuwingen opnieuw door SecurityCenter weergegeven.

Als u een informatiewaarschuwing ongewild hebt verborgen, kunt u deze op elk moment opnieuw weergeven. Door SecurityCenter worden standaard alle informatiewaarschuwingen weergegeven.

Informatiewaarschuwingen weergeven of verbergen

U kunt SecurityCenter configureren op weergave van bepaalde informatiewaarschuwingen, terwijl andere worden verborgen, of u kunt alle informatiewaarschuwingen verbergen.

- 1 Open het deelvenster Waarschuwingsopties.
Hoe?
 1. Klik op **Startpagina** onder **Algemene taken**.
 2. Klik in het rechterdeelvenster, onder **SecurityCenter-informatie**, op **Configureren**.
 3. Klik op **Geavanceerd** onder **Waarschuwingen**.
- 2 Klik in het configuratiedeelvenster van SecurityCenter op **Informatiewaarschuwingen**.
- 3 Ga in het deelvenster Informatiewaarschuwingen op een van de volgende manieren te werk:
 - Als u een informatiewaarschuwing wilt weergeven, schakelt u het bijbehorende selectievakje uit.
 - Als u een informatiewaarschuwing wilt verbergen, schakelt u het bijbehorende selectievakje in.
 - Schakel het selectievakje **Informatieve waarschuwingen niet weergeven** in als u alle informatiewaarschuwingen wilt verbergen.

4 Klik op **OK**.

Tip: u kunt een informatiewaarschuwing ook verbergen door het selectievakje **Deze waarschuwing niet meer tonen** in de waarschuwing zelf in te schakelen. Als u dit doet, kunt u de informatiewaarschuwing opnieuw weergeven door het bijbehorende selectievakje uit te schakelen in het deelvenster Informatiewaarschuwingen.

Informatiewaarschuwingen weergeven of verbergen bij het spelen van spelletjes

U kunt informatiewaarschuwingen verbergen als u een spel in de modus Volledig scherm op de computer speelt. Als u klaar bent met het spel en de modus Volledig scherm uitschakelt, worden de informatiewaarschuwingen opnieuw door SecurityCenter weergegeven.

1 Open het deelvenster Waarschuwingsopties.

Hoe?

1. Klik op **Startpagina** onder **Algemene taken**.
2. Klik in het rechterdeelvenster, onder **SecurityCenter-informatie**, op **Configureren**.
3. Klik op **Geavanceerd** onder **Waarschuwingen**.

2 Schakel in het deelvenster Waarschuwingsopties de optie **Informatiewaarschuwingen weergeven wanneer de spelletjesmodus wordt gedetecteerd** in of uit.

3 Klik op **OK**.

Waarschuwingsopties configureren

Het uiterlijk en de frequentie van waarschuwingen wordt door SecurityCenter ingesteld; u kunt echter enkele basisopties voor waarschuwingen aanpassen. U kunt bijvoorbeeld een geluid laten afspelen bij waarschuwingen of voorkomen dat het opstartscherm wordt weergegeven als Windows wordt opgestart. U kunt ook waarschuwingen verbergen over nieuwe virussen en andere beveiligingsrisico's binnen de online gemeenschap.

Een geluid afspelen bij waarschuwingen

Als u wilt horen dat een waarschuwing wordt weergegeven, kunt u SecurityCenter configureren op het afspelen van een geluid bij elke waarschuwing.

- 1 Open het deelvenster Waarschuwingsopties.
Hoe?
 1. Klik op **Startpagina** onder **Algemene taken**.
 2. Klik in het rechterdeelvenster, onder **SecurityCenter-informatie**, op **Configureren**.
 3. Klik op **Geavanceerd** onder **Waarschuwingen**.
- 2 Schakel in het deelvenster Waarschuwingsopties, onder **Geluid**, het selectievakje **Geluid afspelen wanneer er een waarschuwing optreedt** in.

Het opstartscherm verbergen bij het opstarten

Het opstartscherm van McAfee wordt standaard kort weergegeven bij het opstarten van Windows, waarmee wordt aangeduid dat SecurityCenter uw computer beschermt. U kunt de weergave van het opstartscherm echter voorkomen als u dat wilt.

- 1 Open het deelvenster Waarschuwingsopties.
Hoe?
 1. Klik op **Startpagina** onder **Algemene taken**.
 2. Klik in het rechterdeelvenster, onder **SecurityCenter-informatie**, op **Configureren**.
 3. Klik op **Geavanceerd** onder **Waarschuwingen**.
- 2 Schakel in het deelvenster Waarschuwingsopties, onder **Opstartscherm**, het selectievakje **Opstartscherm van McAfee weergeven bij opstarten van Windows** uit.

Tip: u kunt het opstartscherm op elk willekeurig tijdstip opnieuw weergeven door het selectievakje **Opstartscherm van McAfee weergeven bij opstarten van Windows** in te schakelen.

Waarschuwingen voor virusuitbraken verbergen

U kunt waarschuwingen verbergen over virusuitbraken en andere beveiligingsrisico's binnen de online gemeenschap.

1 Open het deelvenster Waarschuwingsopties.

Hoe?

1. Klik op **Startpagina** onder **Algemene taken**.
2. Klik in het rechterdeelvenster, onder **SecurityCenter-informatie**, op **Configureren**.
3. Klik op **Geavanceerd** onder **Waarschuwingen**.

2 Schakel het selectievakje **Waarschuw mij wanneer een virus of een veiligheidsrisico optreedt** in het deelvenster Waarschuwingsopties uit.

Tip: u kunt waarschuwingen over virusuitbraken op elk gewenst moment weergeven door het selectievakje **Waarschuw mij wanneer een virus of een veiligheidsrisico optreedt** in te schakelen.

HOOFDSTUK 7

Gebeurtenissen weergeven

Een gebeurtenis is een actie of configuratiewijziging die plaatsvindt binnen een beveiligingscategorie en bijbehorende beveiligingsservices. Door verschillende beveiligingsservices worden verschillende typen gebeurtenissen vastgelegd.

SecurityCenter legt bijvoorbeeld een gebeurtenis vast als een beveiligingsservice wordt in- of uitgeschakeld; Virusbeveiliging legt een gebeurtenis vast als een virus wordt vastgesteld en verwijderd, en Firewallbeveiliging legt een gebeurtenis vast als een poging tot een internetverbinding wordt geblokkeerd. Zie Beveiligingscategorieën begrijpen (pagina 9) voor meer informatie over beveiligingscategorieën.

U kunt gebeurtenissen weergeven bij het oplossen van configuratieproblemen en het controleren van bewerkingen die door andere gebruikers zijn uitgevoerd. Veel ouders gebruiken het gebeurtenislogboek om het gedrag van hun kinderen op internet bij te houden. U kunt recente gebeurtenissen weergeven als u alleen de laatste 30 gebeurtenissen wilt bekijken. U kunt alle gebeurtenissen weergeven als u een uitgebreide lijst met alle gebeurtenissen die hebben plaatsgevonden wilt bekijken. Als u alle gebeurtenissen weergeeft, wordt het gebeurtenislogboek door SecurityCenter geopend, waarin de gebeurtenissen worden gesorteerd op basis van de beveiligingscategorie waarin deze hebben plaatsgevonden.

In dit hoofdstuk

Recente gebeurtenissen weergeven.....	29
Alle gebeurtenissen weergeven.....	30

Recente gebeurtenissen weergeven

U kunt recente gebeurtenissen weergeven als u alleen de laatste 30 gebeurtenissen wilt bekijken.

- Klik onder **Algemene taken** op **Recente gebeurtenissen weergeven**.

Alle gebeurtenissen weergeven

U kunt alle gebeurtenissen weergeven als u een uitgebreide lijst met alle gebeurtenissen die hebben plaatsgevonden wilt bekijken.

- 1 Klik onder **Algemene taken** op **Recente gebeurtenissen weergeven**.
- 2 Klik in het deelvenster Recente gebeurtenissen op **Logboek weergeven**.
- 3 Klik in het linkerdeelvenster van het gebeurtenislogboek op het type gebeurtenis dat u wilt weergeven.

 HOOFDSTUK 8

McAfee VirusScan

De geavanceerde detectie- en beveiligingservices van VirusScan beschermen u en uw computer tegen de meest recente beveiligingsrisico's, zoals Trojaanse paarden, trackingcookies, spyware, adware en andere mogelijk ongewenste programma's. De beveiliging gaat verder dan de bestanden en mappen op uw pc, want er worden tevens bedreigingen voorkomen die via andere toegangspunten verlopen, waaronder e-mails, expresberichten en internet.

Met VirusScan wordt uw computer onmiddellijk en voortdurend beveiligd (geen lastig beheer vereist). Tijdens het werken, spelen, surfen op het web of het lezen van e-mail, wordt de beveiliging op de achtergrond uitgevoerd, waarbij de bewaking, het scannen en het vaststellen van mogelijk gevaar in real-time wordt uitgevoerd. Uitgebreide scans worden volgens een schema uitgevoerd, waarbij uw computer regelmatig wordt gecontroleerd met behulp van een meer geavanceerde verzameling opties. VirusScan biedt u flexibiliteit om dit gedrag aan te passen aan uw wensen; als u dit niet wilt doen, is uw computer desondanks beveiligd.

Bij normaal computergebruik kunnen virussen, wormen en andere mogelijke gevaren uw computer binnendringen. Als dit het geval is, wordt u door VirusScan op de hoogte gesteld van de bedreiging, waarbij deze meestal door het programma wordt afgehandeld, dat geïnfecteerde items opschoont of in quarantaine plaatst voordat kwaad kan geschieden. Hoewel dit zelden het geval is, kan aanvullende actie vereist zijn. In dergelijke gevallen laat VirusScan u bepalen wat er moet gebeuren (een nieuwe scan uitvoeren als u de computer opnieuw opstart, het vastgestelde item behouden of het vastgestelde item verwijderen).

Opmerking: SecurityCenter stelt u op de hoogte van kritieke en niet-kritieke beveiligingsproblemen zodra deze worden vastgesteld. Als u hulp nodig hebt bij het analyseren van beveiligingsproblemen, kunt u McAfee Virtual Technician uitvoeren.

In dit hoofdstuk

VirusScan-functies	33
Real-time virusbeveiliging starten	34
Aanvullende beveiliging starten.....	37
Virusbeveiliging instellen	41
De computer scannen.....	59
Werken met scanresultaten.....	63

VirusScan-functies

VirusScan biedt de volgende functies.

Uitgebreide virusbescherming

De geavanceerde detectie- en beveiligingsservices van VirusScan beschermen u en uw computer tegen de meest recente beveiligingsrisico's, zoals Trojaanse paarden, trackingcookies, spyware, adware en andere mogelijk ongewenste programma's. De beveiliging gaat verder dan de bestanden en mappen op uw pc, want er worden tevens bedreigingen voorkomen die via andere toegangspunten verlopen, waaronder e-mails, expresberichten en internet. Er is geen omslachtig beheer vereist.

Scanopties op basis van beschikbare bronnen

Als de scansnelheden laag liggen, kunt u de optie voor het gebruik van minimale computerbronnen uitschakelen, maar daarbij wordt aan virusbeveiliging hogere prioriteit verleend dan aan andere taken. VirusScan biedt u flexibiliteit om opties voor real-time en handmatige scans aan te passen aan uw wensen; als u dit niet wilt doen, is uw computer desondanks beveiligd.

Automatisch herstel

Als VirusScan een beveiligingsrisico vaststelt tijdens een real-time of handmatige scan, probeert het programma deze dreiging automatisch af te handelen op basis van het type risico. Op deze manier kunnen de meeste risico's worden vastgesteld en uitgeschakeld zonder uw tussenkomst. Hoewel dit zelden voorkomt, kan VirusScan mogelijk een risico niet op eigen kracht uitschakelen. In dergelijke gevallen laat VirusScan u bepalen wat er moet gebeuren (een nieuwe scan uitvoeren als u de computer opnieuw opstart, het vastgestelde item behouden of het vastgestelde item verwijderen).

Taken pauzeren in de modus Volledig scherm

Als u films bekijkt, spellen speelt op uw computer of een andere activiteit uitvoert die het volledige computerscherm in beslag neemt, wordt een aantal taken door VirusScan gepauzeerd, waaronder automatische updates en handmatige scans.

Real-time virusbeveiliging starten

VirusScan biedt twee typen virusbeveiliging: real-time en handmatig. Bij real-time virusbeveiliging wordt uw computer voortdurend gecontroleerd op virusactiviteit en worden bestanden telkens gescand als deze op uw computer worden geopend. Bij handmatige virusbeveiliging kunt u bestanden op verzoek scannen. Als u ervoor wilt zorgen dat uw computer beveiligd is tegen de meest recente beveiligingsrisico's, is het aan te raden om de real-time virusbeveiliging ingeschakeld te laten en een schema in te stellen voor regelmatige, meer uitgebreide handmatig scans. Door VirusScan wordt standaard eenmaal per week een geplande scan uitgevoerd. Zie voor meer informatie over real-time en handmatig scannen De computer scannen (pagina 59).

Hoewel dit zelden het geval is, kan het voorkomen dat u real-time scannen tijdelijk wilt uitschakelen (bijvoorbeeld om bepaalde scanopties te wijzigen of om een probleem in verband met de prestaties op te lossen). Als u de real-time virusbeveiliging uitschakelt, is de computer niet beveiligd en is de beveiligingsstatus van SecurityCenter rood. Zie 'De beveiligingsstatus begrijpen' in de Help van SecurityCenter voor meer informatie over de beveiligingsstatus.

Real-time virusbeveiliging starten

Real-time virusbeveiliging is standaard ingeschakeld en beveiligt uw computer zo tegen virussen, Trojaanse paarden en andere beveiligingsrisico's. Als u de real-time virusbeveiliging uitschakelt, moet u het opnieuw inschakelen om uw computer te beschermen.

- 1 Open het configuratiedeelvenster van Computer en bestanden.
Hoe?
 1. Klik in het linkerdeelvenster op **menu Geavanceerd**.
 2. Klik op **Configureren**.
 3. Klik in het configuratiedeelvenster op **Computer en bestanden**.
- 2 Klik onder **Virusbeveiliging** op **Aan**.

Real-time virusbeveiliging stoppen

U kunt real-time virusbeveiliging tijdelijk stoppen en opgeven wanneer u de service wilt hervatten. U kunt de beveiliging automatisch laten hervatten na 15, 30, 45 of 60 minuten, als de computer opnieuw wordt gestart, of nooit.

- 1 Open het configuratievenster van Computer en bestanden.
Hoe?
 1. Klik in het linkerdeelvenster op **menu Geavanceerd**.
 2. Klik op **Configureren**.
 3. Klik in het configuratievenster op **Computer en bestanden**.
- 2 Klik onder **Virusbeveiliging** op **Uit**.
- 3 Selecteer de optie voor het hervatten van real-time scannen in het dialoogvenster.
- 4 Klik op **OK**.

HOOFDSTUK 9

Aanvullende beveiliging starten

Naast real-time virusbeveiliging biedt VirusScan geavanceerde beveiliging tegen scripts, spyware en mogelijk schadelijke bijlagen bij e-mail en expresberichten. Het scannen van scripts, spyware, e-mails en expresberichten is standaard ingeschakeld ter beveiliging van uw computer.

Beveiliging via Scripts scannen

Scripts scannen stelt mogelijk schadelijke scripts vast en voorkomt dat deze op de computer worden uitgevoerd. Hiermee wordt uw computer gecontroleerd op verdachte scriptactiviteiten, zoals een script dat bestanden maakt, kopieert of verwijdert of dat het Windows-register opent. U ontvangt een waarschuwing als schade wordt toegebracht.

Spywarebeveiliging

Spywarebeveiliging stelt spyware, adware en andere mogelijk ongewenste programma's vast. Spyware is software die in het geheim op uw computer kan worden geïnstalleerd om uw gedrag bij te houden, om persoonlijke gegevens te verzamelen en zelfs uw beheer van de computer te beïnvloeden, via de installatie van aanvullende software of het omleiden van browseractiviteiten.

E-mailbeveiliging

E-mailbeveiliging stelt verdachte activiteit in e-mails en bijlagen vast die u verzendt en ontvangt.

Beveiliging van expresberichten

Via beveiliging van expresberichten worden mogelijk beveiligingsrisico's vastgesteld in bijlagen bij de expresberichten die u ontvangt. Er wordt tevens voorkomen dat persoonlijke gegevens worden uitgewisseld via programma's voor expresberichten.

In dit hoofdstuk

Beveiliging via Scripts scannen starten	38
Spywarebeveiliging starten	38
E-mailbeveiliging starten.....	39
Beveiliging van expresberichten starten	39

Beveiliging via Scripts scannen starten

Schakel beveiliging via Scripts scannen in om mogelijk schadelijke scripts vast te stellen en te voorkomen dat deze op de computer worden uitgevoerd. Met beveiliging via Scripts scannen ontvangt u een waarschuwing als een script probeert om bestanden op uw computer te maken, te kopiëren of hiervan te verwijderen, of om wijzigingen aan te brengen in het Windows-register.

- 1 Open het configuratiedeelvenster van Computer en bestanden.

Hoe?

1. Klik in het linkerdeelvenster op **menu Geavanceerd**.
2. Klik op **Configureren**.
3. Klik in het configuratiedeelvenster op **Computer en bestanden**.

- 2 Klik onder **Beveiliging via Scripts scannen** op **Aan**.

Opmerking: hoewel u beveiliging via Scripts scannen op elk moment kunt uitschakelen, is uw computer hierdoor kwetsbaar voor schadelijke scripts.

Spywarebeveiliging starten

Als u spywarebeveiliging inschakelt worden spyware, adware en andere mogelijk ongewenste programma's die gegevens verzamelen en verzenden zonder uw toestemming, vastgesteld en verwijderd.

- 1 Open het configuratiedeelvenster van Computer en bestanden.

Hoe?

1. Klik in het linkerdeelvenster op **menu Geavanceerd**.
2. Klik op **Configureren**.
3. Klik in het configuratiedeelvenster op **Computer en bestanden**.

- 2 Klik onder **Beveiliging via Scripts scannen** op **Aan**.

Opmerking: hoewel u spywarebeveiliging op elk moment kunt uitschakelen, is uw computer hierdoor kwetsbaar voor mogelijk ongewenste programma's.

E-mailbeveiliging starten

Als u e-mailbeveiliging inschakelt, kunt u wormen en mogelijke bedreigingen in uitgaande (SMTP) en binnenkomende (POP3) e-mailberichten en bijlagen vaststellen.

- 1 Open het deelvenster voor configuratie van e-mail en expresberichten.

Hoe?

1. Klik in het linkerdeelvenster op **menu Geavanceerd**.
2. Klik op **Configureren**.
3. Klik in het configuratiedeelvenster op **E-mail en expresberichten**.

- 2 Klik onder **E-mailbeveiliging** op **Aan**.

Opmerking: hoewel u e-mailbeveiliging op elk moment kunt uitschakelen, is uw computer hierdoor kwetsbaar voor bedreigingen via e-mail.

Beveiliging van expresberichten starten

Als u beveiliging van expresberichten inschakelt, kunt u beveiligingsrisico's vaststellen in bijlagen bij binnenkomende expresberichten.

- 1 Open het deelvenster voor configuratie van e-mail en expresberichten.

Hoe?

1. Klik in het linkerdeelvenster op **menu Geavanceerd**.
2. Klik op **Configureren**.
3. Klik in het configuratiedeelvenster op **E-mail en expresberichten**.

- 2 Klik onder **Beveiliging van expresberichten** op **Aan**.

Opmerking: hoewel u beveiliging van expresberichten op elk moment kunt uitschakelen, is uw computer hierdoor kwetsbaar voor schadelijke bijlagen bij expresberichten.

HOOFDSTUK 10

Virusbeveiliging instellen

VirusScan biedt twee typen virusbeveiliging: real-time en handmatig. Door real-time virusbeveiliging worden bestanden gescand telkens als ze door u of de computer worden geopend. Bij handmatige virusbeveiliging kunt u bestanden op verzoek scannen. U kunt verschillende opties instellen voor elk type beveiliging. Omdat de computer bij real-time beveiliging voortdurend wordt bewaakt, kunt u bijvoorbeeld een bepaalde reeks eenvoudige scanopties instellen, waarbij u een uitgebreidere reeks scanopties reserveert voor handmatige beveiliging op verzoek.

In dit hoofdstuk

Opties voor real-time scannen instellen	42
Opties voor handmatige scans instellen.....	44
SystemGuard-opties gebruiken	48
Lijsten met vertrouwde items gebruiken.....	55

Opties voor real-time scannen instellen

Als u real-time virusbeveiliging inschakelt, wordt door VirusScan een standaardverzameling opties gebruikt voor het scannen van bestanden; u kunt de standaardopties echter volledig aan uw wensen aanpassen.

Als u de opties voor real-time scans wilt wijzigen, moet u beslissingen nemen over de items die door VirusScan worden gecontroleerd tijdens een scan, en moet u de locatie en het type van bestanden opgeven die moeten worden gescand. U kunt bijvoorbeeld bepalen of VirusScan moet scannen op onbekende virussen of op cookies die websites kunnen gebruiken om uw gedrag bij te houden; u kunt tevens instellen of het programma aan uw computer toegewezen netwerkstations moet scannen of alleen lokale stations. U kunt ook instellen welk type bestanden wordt gescand (alle bestanden of alleen programmabestanden en documenten, omdat daarin de meeste virussen worden aangetroffen).

Als u de opties voor real-time scans wijzigt, moet u ook bepalen of uw computer over bescherming voor overschrijding van de bufferlimiet moet beschikken. Een buffer is een gedeelte van het geheugen dat wordt gebruikt voor het tijdelijk opslaan van computergegevens. Overschrijdingen van de bufferlimiet kunnen plaatsvinden wanneer de hoeveelheid informatie die verdachte programma's of processen in een buffer opslaan de capaciteit van de buffer overschrijdt. Als dit gebeurt, is uw computer kwetsbaarder voor aanvallen.

Opties voor real-time scannen instellen

Via het instellen van de opties voor real-time scannen, kunt u aanpassen welke items VirusScan zoekt tijdens een real-time scan, en kunt u de locaties en bestandstypen opgeven die worden gescand. De opties zijn onder andere het scannen op onbekende virussen en trackingcookies en het instellen van bescherming voor overschrijding van bufferlimieten. U kunt real-time scannen ook instellen op het controleren van netwerkstations die aan uw computer zijn toegewezen.

1 Open het deelvenster Real-time scannen.

Hoe?

1. Klik op **Startpagina** onder **Algemene taken**.
 2. Klik in het deelvenster Startpagina van SecurityCenter op **Computer en bestanden**.
 3. Klik in het gedeelte voor gegevens van Computer en bestanden op **Configureren**.
 4. Controleer in het configuratiedeelvenster van Computer en bestanden of de virusbeveiliging is ingeschakeld en klik op **Geavanceerd**.
- 2 Geef de opties voor real-time scannen op en klik op **OK**.

Om...	Doet u het volgende...
Onbekende virussen en nieuwe varianten van bekende virussen vast te stellen	Schakel het selectievakje Scannen op onbekende virussen met behulp van heuristische technieken in.
Cookies op te sporen	Schakel het selectievakje Trackingcookies scannen en verwijderen in.
Virussen vast te stellen en andere mogelijke bedreigingen op stations die met het netwerk verbonden zijn	Schakel het selectievakje Netwerkstations scannen in.
De computer te beschermen tegen overschrijdingen van bufferlimieten	Schakel het selectievakje Bescherming overschrijding bufferlimiet inschakelen in.
Aan te geven welke bestandstypen moeten worden gescand	Klik op Alle bestanden (aanbevolen) of op Alleen programmabestanden en documenten .

Opties voor handmatige scans instellen

Bij handmatige virusbeveiliging kunt u bestanden op verzoek scannen. Als u een handmatige scan start, wordt de computer door VirusScan gecontroleerd op virussen en andere mogelijk schadelijke items met een meer uitgebreide verzameling scanopties. Als u de opties voor handmatige scans wilt wijzigen, moet u beslissingen nemen over de items die VirusScan zoekt tijdens een scan. U kunt bijvoorbeeld bepalen of VirusScan onbekende virussen zoekt, mogelijk ongewenste programma's zoals spyware of adware, stealth-programma's zoals rootkits die ongemachtigde toegang tot uw computer kunnen verlenen, en cookies die websites kunnen gebruiken om uw gedrag bij te houden. U moet ook beslissingen nemen over het soort bestanden dat wordt gecontroleerd. U kunt bijvoorbeeld instellen of VirusScan alle bestanden controleert of alleen programmabestanden en documenten (omdat daarin de meeste virussen worden aangetroffen). U kunt ook instellen of archiefbestanden (bijvoorbeeld .zip-bestanden) in de scan worden opgenomen.

VirusScan controleert standaard alle stations en mappen op uw computer als een handmatige scan wordt uitgevoerd; u kunt echter de standaardlocaties geheel aan uw eisen en wensen aanpassen. U kunt bijvoorbeeld alleen kritieke systeembestanden scannen, items op het bureaublad of items in de map met programmabestanden. U kunt een regelmatig schema instellen voor de scans of besluiten dat u de handmatige scans telkens zelf wilt starten. Bij de geplande scans wordt de volledige computer altijd gecontroleerd met de standaardopties voor scannen. Door VirusScan wordt standaard eenmaal per week een geplande scan uitgevoerd.

Als de scansnelheden volgens u laag liggen, kunt u besluiten om de optie voor het gebruik van minimale computerbronnen uit te schakelen, maar daarbij wordt aan virusbeveiliging hogere prioriteit verleend dan aan andere taken.

Opmerking: als u films bekijkt, spellen speelt op uw computer of een andere activiteit uitvoert die het volledige computerscherm in beslag neemt, wordt een aantal taken door VirusScan gepauzeerd, waaronder automatische updates en handmatige scans.

Opties voor handmatige scans instellen

Via het instellen van de opties voor handmatig scannen, kunt u aanpassen welke items VirusScan zoekt tijdens een handmatige scan, en kunt u de locaties en bestandstypen opgeven die worden gescand. Opties zijn onder andere het scannen op onbekende virussen, bestandsarchieven, spyware en mogelijk ongewenste programma's, trackingcookies, rootkits en stealth-programma's.

1 Open het deelvenster Handmatig scannen.

Hoe?

1. Klik op **Startpagina** onder **Algemene taken**.
2. Klik in het deelvenster Startpagina van SecurityCenter op **Computer en bestanden**.
3. Klik in het gedeelte voor gegevens van Computer en bestanden op **Configureren**.
4. Controleer in het configuratiedeelvenster van Computer en bestanden of de virusbeveiliging is ingeschakeld en klik vervolgens op **Geavanceerd**.
5. Klik in het deelvenster Virusbeveiliging op **Handmatig scannen**.

2 Geef de opties voor handmatig scannen op en klik op **OK**.

Om...	Doet u het volgende...
Onbekende virussen en nieuwe varianten van bekende virussen vast te stellen	Schakel het selectievakje Scannen op onbekende virussen met behulp van heuristische technieken in.
Virussen in zip-bestanden en andere archiefbestanden vast te stellen en te verwijderen	Schakel het selectievakje ZIP- en andere archiefbestanden scannen in.
Spyware, adware en andere mogelijk ongewenste programma's vast te stellen	Schakel het selectievakje Scannen op spyware en mogelijk ongewenste programma's in.
Cookies op te sporen	Schakel het selectievakje Trackingcookies scannen en verwijderen in.
Rootkits en stealth-programma's vast te stellen die bestaande systeembestanden van Windows kunnen wijzigen en uitbuiten	Schakel het selectievakje Scannen op rootkits en andere stealth-programma's in.

Minder processorkracht te gebruiken voor scans en een hogere prioriteit te verlenen aan andere taken (zoals surfen op het web en het openen van documenten)	Schakel het selectievakje Scannen met minimale computerbronnen in.
Aan te geven welke bestandstypen moeten worden gescand	Klik op Alle bestanden (aanbevolen) of op Alleen programmabestanden en documenten .

Locaties voor handmatige scans instellen

Via het instellen van de locaties voor handmatig scannen, bepaalt u waar VirusScan zoekt naar virussen en andere schadelijke items tijdens een handmatige scan. U kunt alle bestanden, mappen en stations op de computer scannen of het scannen beperken tot bepaalde mappen en stations.

1 Open het deelvenster Handmatig scannen.

Hoe?

1. Klik op **Startpagina** onder **Algemene taken**.
2. Klik in het deelvenster Startpagina van SecurityCenter op **Computer en bestanden**.
3. Klik in het gedeelte voor gegevens van Computer en bestanden op **Configureren**.
4. Controleer in het configuratiedeelvenster van Computer en bestanden of de virusbeveiliging is ingeschakeld en klik vervolgens op **Geavanceerd**.
5. Klik in het deelvenster Virusbeveiliging op **Handmatig scannen**.

2 Klik op **Standaardlocatie voor scannen**.

3 Geef de locatie voor handmatig scannen op en klik op **OK**.

Om...	Doet u het volgende...
Alle bestanden en mappen op de computer te scannen	Schakel het selectievakje (Deze) Computer in.
Specifieke bestanden, mappen en stations op de computer te scannen	Schakel het selectievakje (Deze) Computer uit en selecteer een of meer mappen en stations.
Kritieke systeembestanden te scannen	Schakel het selectievakje (Deze) Computer uit en schakel het selectievakje Kritieke systeembestanden in.

Een scan plannen

U kunt scans plannen om de computer grondig te controleren op virussen en andere bedreigingen op elke willekeurige dag van de week en elk tijdstip. Bij de geplande scans wordt de volledige computer altijd gecontroleerd met de standaardopties voor scannen. Door VirusScan wordt standaard eenmaal per week een geplande scan uitgevoerd. Als de scansnelheden volgens u laag liggen, kunt u besluiten om de optie voor het gebruik van minimale computerbronnen uit te schakelen, maar daarbij wordt aan virusbeveiliging hogere prioriteit verleend dan aan andere taken.

1 Open het deelvenster Geplande scan.

Hoe?

1. Klik op **Startpagina** onder **Algemene taken**.
2. Klik in het deelvenster Startpagina van SecurityCenter op **Computer en bestanden**.
3. Klik in het gedeelte voor gegevens van Computer en bestanden op **Configureren**.
4. Controleer in het configuratiedeelvenster van Computer en bestanden of de virusbeveiliging is ingeschakeld en klik vervolgens op **Geavanceerd**.
5. Klik in het deelvenster Virusbeveiliging op **Geplande scan**.

2 Schakel **Gepland scannen inschakelen** in.

- 3 Schakel **Scannen met minimale computerbronnen** in om de hoeveelheid processorkracht te beperken die normaal gesproken voor het scannen wordt gebruikt.
- 4 Selecteer een of meer dagen.
- 5 Geef een begintijd op.
- 6 Klik op **OK**.

Tip: als u het standaardschema wilt herstellen, klikt u op **Opnieuw instellen**.

SystemGuard-opties gebruiken

SystemGuards zorgen voor het bewaken en beheren van mogelijk niet-gemachtigde wijzigingen die in het Windows-register of in kritieke systeembestanden op de computer worden aangebracht en leggen gegevens hierover vast in logboeken en rapporten. Onbevoegde wijzigingen in het register en in bestanden kunnen uw computer schade toebrengen, de beveiliging van uw computer in gevaar brengen en waardevolle systeembestanden beschadigen.

Wijzigingen in het register en bestanden komen normaal gesproken veel voor op een computer. Omdat de meeste wijzigingen geen schade toebrengen, zijn de standaardinstellingen van SystemGuards geconfigureerd met het oog op het bieden van betrouwbare, slimme en realistische beveiliging tegen onbevoegde wijzigingen die potentieel grote schade kunnen toebrengen. Als SystemGuards bijvoorbeeld wijzigingen vaststellen die ongebruikelijk zijn en mogelijk een grote bedreiging vormen, wordt deze activiteit onmiddellijk gerapporteerd en in een logboek vastgelegd. Wijzigingen die vrij algemeen zijn, maar die toch tot schade zouden kunnen leiden, worden alleen in een logboek vastgelegd. Het controleren op standaardwijzigingen of wijzigingen die geen gevaar opleveren, is echter standaard uitgeschakeld. De SystemGuards-technologie kan worden geconfigureerd om een groter beveiligingsgebied te omvatten.

Er zijn drie typen SystemGuards: SystemGuards voor programma's, SystemGuards voor Windows en SystemGuards voor browsers.

SystemGuards voor programma's

SystemGuards voor programma's stellen mogelijk onbevoegde wijzigingen vast in het register van de computer en andere kritieke bestanden die van essentieel belang zijn voor Windows. Deze belangrijke registeritems en -bestanden zijn onder andere ActiveX-installaties, opstartitems, Windows-shell-uitvoeringshooks en Vertraagd laden Shell-serviceobjecten. De SystemGuards-technologie voor programma's controleert deze items en stopt verdachte ActiveX-programma's (die van internet zijn gedownload) en spyware, en mogelijk ongewenste programma's die automatisch kunnen worden gestart als Windows wordt gestart.

SystemGuards voor Windows

SystemGuards voor Windows stellen tevens mogelijk onbevoegde wijzigingen vast in het register van de computer en andere kritieke bestanden die van essentieel belang zijn voor Windows. Deze belangrijke registeritems en -bestanden zijn onder andere handlers voor contextmenu's, appInit DLL's en het hosts-bestand van Windows. De SystemGuards-technologie houdt deze items bij en voorkomt dat uw computer onbevoegde of persoonlijke gegevens via internet verzendt of ontvangt. Deze stopt tevens verdachte programma's die ongewenste wijzigingen kunnen aanbrengen in het uiterlijk en gedrag van de programma's die van groot belang zijn voor u en uw gezin.

SystemGuards voor browsers

Net als SystemGuards voor programma's en Windows stellen SystemGuards voor browsers mogelijk onbevoegde wijzigingen vast in het register van de computer en andere kritieke bestanden die van essentieel belang zijn voor Windows. SystemGuards voor browsers houden wijzigingen bij in belangrijke registeritems en -bestanden zoals invoegtoepassingen voor Internet Explorer, URL's voor Internet Explorer en beveiligingszones voor Internet Explorer. De SystemGuards-technologie voor browsers houdt deze items bij en helpt onbevoegde browseractiviteit te voorkomen, zoals het doorleiden naar verdachte websites, wijzigingen in browserinstellingen en -opties die u niet hebt goedgekeurd en het instellen van verdachte websites als vertrouwde websites.

Beveiliging via SystemGuards inschakelen

U kunt beveiliging via SystemGuards inschakelen, zodat mogelijk onbevoegde wijzigingen in het Windows-register en in bestanden op de computer kunnen worden vastgesteld en u hiervan op de hoogte wordt gebracht. Onbevoegde wijzigingen in het register en in bestanden kunnen uw computer schade toebrengen, de beveiliging van uw computer in gevaar brengen en waardevolle systeembestanden beschadigen.

- 1 Open het configuratievenster van Computer en bestanden.

Hoe?

1. Klik in het linkerdeelvenster op **menu Geavanceerd**.
2. Klik op **Configureren**.
3. Klik in het configuratiedeelvenster op **Computer en bestanden**.

2 Klik onder **SystemGuard-beveiliging** op **Aan**.

Opmerking: u kunt SystemGuard-beveiliging uitschakelen door op **Uit** te klikken.

Opties voor SystemGuards configureren

Gebruik het deelvenster SystemGuards om de opties voor beveiliging, logboekregistratie en waarschuwingen tegen onbevoegde wijzigingen in het register en in bestanden in verband met Windows-bestanden, -programma's en Internet Explorer in te stellen. Onbevoegde wijzigingen in het register en in bestanden kunnen uw computer schade toebrengen, de beveiliging van uw computer in gevaar brengen en waardevolle systeembestanden beschadigen.

1 Open het deelvenster SystemGuards.

Hoe?

1. Klik op **Startpagina** onder **Algemene taken**.
2. Klik in het deelvenster Startpagina van SecurityCenter op **Computer en bestanden**.
3. Klik in het gedeelte voor gegevens van Computer en bestanden op **Configureren**.
4. Controleer in het configuratiedeelvenster van Computer en bestanden of de SystemGuard-beveiliging is ingeschakeld en klik vervolgens op **Geavanceerd**.

2 Selecteer een type SystemGuard in de lijst.

- **SystemGuards voor programma's**
- **SystemGuards voor Windows**
- **SystemGuards voor browsers**

3 Ga op een van de volgende manieren te werk onder **Ik wil:**

- Klik op **Waarschuwingen weergeven** om onbevoegde wijzigingen in het register en in bestanden die zijn gekoppeld aan de SystemGuards voor bestanden, voor Windows en voor browsers vast te stellen en hierover informatie op te slaan in logboekbestanden en rapporten.
- Klik op **Wijzigingen alleen vastleggen in logboek** om onbevoegde wijzigingen in het register en in bestanden die zijn gekoppeld aan de SystemGuards voor bestanden, voor Windows en voor browsers vast te stellen en hierover informatie op te slaan in logboekbestanden.

- Klik op **SystemGuards uitschakelen** om het vaststellen van onbevoegde wijzigingen in het register en in bestanden die zijn gekoppeld aan de SystemGuards voor bestanden, voor Windows en voor browsers uit te schakelen.

Opmerking: zie Informatie over typen SystemGuards (pagina 51) voor meer informatie over typen SystemGuards.

Informatie over typen SystemGuards

SystemGuards stellen mogelijk onbevoegde wijzigingen vast in het register van de computer en andere kritieke bestanden die van essentieel belang zijn voor Windows. Er zijn drie typen SystemGuards: SystemGuards voor programma's, SystemGuards voor Windows en SystemGuards voor browsers

SystemGuards voor programma's

De SystemGuards-technologie voor programma's stopt verdachte ActiveX-programma's (die van internet zijn gedownload) en spyware, en mogelijk ongewenste programma's die automatisch kunnen worden gestart als Windows wordt gestart.

SystemGuard	Spoort de volgende items op...
ActiveX-installaties	Onbevoegde registerwijzigingen in ActiveX-installaties die uw computer schade kunnen toebrengen, de beveiliging van uw computer in gevaar kunnen brengen en waardevolle systeembestanden kunnen beschadigen.
Opstartitems	Spyware, adware en andere mogelijk ongewenste programma's die bestandswijzigingen in opstartitems kunnen installeren, zodat verdachte programma's kunnen worden uitgevoerd wanneer u uw computer opstart.
Windows-shell-uitvoeringshoks	Spyware, adware en andere mogelijk ongewenste programma's die Windows-shell-uitvoeringshooks kunnen installeren om te voorkomen dat beveiligingsprogramma's correct worden uitgevoerd.
Vertraagd laden Shell-serviceobject	Spyware, adware en andere mogelijk ongewenste programma's die registerwijzigingen kunnen aanbrengen in het Vertraagd laden Shell-serviceobject, zodat schadelijke bestanden kunnen worden uitgevoerd wanneer u uw computer opstart.

SystemGuards voor Windows

De SystemGuards-technologie voorkomt dat uw computer onbevoegde of persoonlijke gegevens via internet verzendt of ontvangt. Deze stopt tevens verdachte programma's die ongewenste wijzingen kunnen aanbrengen in het uiterlijk en gedrag van de programma's die van groot belang zijn voor u en uw gezin.

SystemGuard	Spoort de volgende items op...
Handlers voor contextmenu	Onbevoegde registerwijzigingen in handlers voor Windows-contextmenu's die de weergave en het gedrag van Windows-menu's kunnen beïnvloeden. Met behulp van contextmenu's kunt u bewerkingen op uw computer uitvoeren, zoals door met de rechtermuisknop op bestanden te klikken.
AppInit DLL's	Onbevoegde registerwijzigingen in Windows appInit DLL's die tot gevolg kunnen hebben dat mogelijk schadelijke bestanden worden uitgevoerd wanneer u uw computer opstart.
Hosts-bestand van Windows	Spyware, adware en mogelijk ongewenste programma's die onbevoegde wijzigingen in uw Windows-hostsbestand kunnen aanbrengen, waardoor uw browser wordt doorgestuurd naar verdachte websites en software-updates worden geblokkeerd.
Winlogon-shell	Spyware, adware en andere mogelijk ongewenste programma's die registerwijzigingen kunnen aanbrengen in de Winlogon-shell, zodat andere programma's Windows Verkenner kunnen vervangen.
Winlogon UserInit	Spyware, adware en andere mogelijk ongewenste programma's die registerwijzigingen kunnen aanbrengen in Winlogon UserInit, zodat verdachte programma's kunnen worden uitgevoerd als u zich bij Windows aanmeldt.
Windows-protocollen	Spyware, adware en andere mogelijk ongewenste programma's die registerwijzigingen kunnen aanbrengen in Windows-protocollen, wat invloed heeft op de manier waarop uw computer informatie naar internet verzendt en van internet ontvangt.
Gelaagde serviceproviders van Winsock	Spyware, adware en andere mogelijk ongewenste programma's die registerwijzigingen kunnen installeren in gelaagde serviceproviders van Winsock, waardoor informatie die u verzendt naar en ontvangt van internet kan worden onderschept en gewijzigd.

Open-opdracht en voor Windows-shell	Onbevoegde wijzigingen in open-opdrachten voor Windows-shell die wormen en andere schadelijke programma's de mogelijkheid kunnen bieden om op uw computer te worden uitgevoerd.
Gedeelde taakplanner	Spyware, adware en andere mogelijk ongewenste programma's die register- en bestandswijzigingen kunnen aanbrengen in de gedeelde taakplanner, zodat mogelijk schadelijke bestanden kunnen worden uitgevoerd wanneer u uw computer opstart.
Windows Messenger Service	Spyware, adware en andere mogelijk ongewenste programma's die registerwijzigingen kunnen aanbrengen in de Windows Messenger Service, waardoor ongevraagde advertenties en van afstand bestuurd programma's op uw computer kunnen worden uitgevoerd.
Win.ini-bestand van Windows	Spyware, adware en andere mogelijk ongewenste programma's die wijzigingen kunnen aanbrengen in het Win.ini-bestand, zodat verdachte programma's kunnen worden uitgevoerd wanneer u uw computer opstart.

SystemGuards voor browsers

De SystemGuards-technologie voor browsers helpt onbevoegde browseractiviteit te voorkomen, zoals het doorleiden naar verdachte websites, wijzigingen in browserinstellingen en -opties die u niet hebt goedgekeurd en het instellen van verdachte websites als vertrouwde websites.

SystemGuard	Spoort de volgende items op...
Browser Helper-objecten	Spyware, adware en andere mogelijk ongewenste programma's die Browser Helper-objecten kunnen gebruiken om te registreren welke websites u bezoekt en ongevraagde advertenties te vertonen.
Internet Explorer-balken	Onbevoegde registerwijzigingen in de lijst met balken in Internet Explorer, zoals Zoeken en Favorieten, die de weergave en het gedrag van Internet Explorer kunnen beïnvloeden.
Internet Explorer-software toevoegingen	Spyware, adware en andere mogelijk ongewenste programma's die Internet Explorer-softwaretoevoegingen kunnen installeren om te registreren welke websites u bezoekt en ongevraagde advertenties te vertonen.
Internet Explorer ShellBrowser	Onbevoegde registerwijzigingen in de Internet Explorer ShellBrowser die de weergave en het gedrag van uw webbrowsen kunnen beïnvloeden.

Internet Explorer-webbrowser	Onbevoegde registerwijzigingen in de Internet Explorer-webbrowser die de weergave en het gedrag van uw webbrowser kunnen beïnvloeden.
Internet Explorer-hooks voor zoeken van URL's	Spyware, adware en andere mogelijk ongewenste programma's die registerwijzigingen kunnen aanbrengen in Internet Explorer-hooks voor het zoeken van URL's, waardoor uw browser wordt doorgestuurd naar verdachte websites wanneer u op internet zoekt.
Internet Explorer-URL's	Spyware, adware en andere mogelijk ongewenste programma's die registerwijzigingen kunnen aanbrengen in URL's van Internet Explorer, die de instellingen van uw browser beïnvloeden.
Internet Explorer-restricties	Spyware, adware en andere mogelijk ongewenste programma's die registerwijzigingen kunnen aanbrengen in Internet Explorer-restricties, die de instellingen en opties van uw browser beïnvloeden.
Beveiligde zones in Internet Explorer	Spyware, adware en andere mogelijk ongewenste programma's die registerwijzigingen kunnen aanbrengen in beveiligde zones in Internet Explorer, zodat mogelijk schadelijke bestanden kunnen worden uitgevoerd wanneer u uw computer opstart.
Vertrouwde sites van Internet Explorer	Spyware, adware en andere mogelijk ongewenste programma's die registerwijzigingen kunnen aanbrengen in vertrouwde websites van Internet Explorer, waardoor uw webbrowser verdachte websites gaat vertrouwen.
Internet Explorer-policy	Spyware, adware en andere mogelijk ongewenste programma's die registerwijzigingen kunnen aanbrengen in policy's van Internet Explorer, die de weergave en het gedrag van uw browser beïnvloeden.

Lijsten met vertrouwde items gebruiken

Als VirusScan een wijziging in een bestand of het register (SystemGuard), in een programma, of een overschrijding van de bufferlimiet vaststelt, wordt u gevraagd om het item als vertrouwd aan te merken of te verwijderen. Als u het item vertrouwt en aangeeft dat u geen verdere meldingen wilt ontvangen over de activiteit ervan, wordt het item toegevoegd aan een lijst met vertrouwde items en wordt het door VirusScan niet langer vastgesteld en ontvangt u geen verdere meldingen over de activiteit ervan. Als u een item hebt toegevoegd aan een lijst met vertrouwde items, maar u de activiteit ervan wilt blokkeren, kunt u dit doen. Als u het item blokkeert, kan het niet worden uitgevoerd of kan het geen wijzigingen aanbrengen op de computer zonder dat u eerst een melding ontvangt als een poging hiertoe wordt gedaan. U kunt een item ook verwijderen uit een lijst met vertrouwde items. Als u een item verwijdert, kan VirusScan de activiteit ervan opnieuw vaststellen.

Lijsten met vertrouwde items beheren

Gebruik het deelvenster Lijsten met vertrouwde items om items als vertrouwd aan te merken of items te blokkeren die eerder zijn vastgesteld en als vertrouwd zijn aangemerkt. U kunt een item ook verwijderen uit een lijst met vertrouwde items, zodat het opnieuw door VirusScan kan worden vastgesteld.

1 Open het deelvenster Lijsten met vertrouwde items.

Hoe?

1. Klik op **Startpagina** onder **Algemene taken**.
2. Klik in het deelvenster Startpagina van SecurityCenter op **Computer en bestanden**.
3. Klik in het gedeelte voor gegevens van Computer en bestanden op **Configureren**.
4. Controleer in het configuratiedeelvenster van Computer en bestanden of de virusbeveiliging is ingeschakeld en klik vervolgens op **Geavanceerd**.
5. Klik in het deelvenster Virusbeveiliging op **Lijsten met vertrouwde items**.

2 Selecteer een van de typen lijsten met vertrouwde items:

- **SystemGuards voor programma's**
- **SystemGuards voor Windows**
- **SystemGuards voor browsers**
- **Vertrouwde programma's**
- **Overschrijding van limieten van vertrouwde buffers**

3 Ga op een van de volgende manieren te werk onder **Ik wil**:

- Klik op **Vertrouwen** als u wilt toestaan dat een vastgesteld item wijzigingen aanbrengt in het Windows-register of kritieke systeembestanden op de computer zonder dat u hiervan op de hoogte wordt gesteld.
- Klik op **Blokkeren** als u wilt voorkomen dat een vastgesteld item wijzigingen aanbrengt in het Windows-register of kritieke systeembestanden op de computer zonder dat u hiervan op de hoogte wordt gesteld.
- Klik op **Verwijderen** om het vastgestelde item te verwijderen uit de lijsten met vertrouwde items.

4 Klik op **OK**.

Opmerking: zie Informatie over typen lijsten met vertrouwde items (pagina 56) voor meer informatie over typen lijsten met vertrouwde items.

Informatie over typen lijsten met vertrouwde items

SystemGuards in het deelvenster Lijsten met vertrouwde items vertegenwoordigen eerder door VirusScan vastgestelde en onbevoegde wijzigingen in het register en bestanden, die u echter hebt toegestaan vanuit een waarschuwing of vanuit het deelvenster Scanresultaten. Er zijn vijf typen lijsten met vertrouwde items die u kunt beheren vanuit het deelvenster Lijsten met vertrouwde items: SystemGuards voor programma's, SystemGuards voor Windows, SystemGuards voor browsers, Vertrouwde programma's en Overschrijdingen van limieten van vertrouwde buffers.

Optie	Beschrijving
SystemGuards voor programma's	<p>SystemGuards voor programma's in het deelvenster Lijsten met vertrouwde items vertegenwoordigen eerder door VirusScan vastgestelde en onbevoegde wijzigingen in het register en bestanden, die u echter hebt toegestaan vanuit een waarschuwing of vanuit het deelvenster Scanresultaten.</p> <p>SystemGuards voor programma's stellen onbevoegde wijzigingen in het register en in bestanden vast in verband met ActiveX-installaties, opstartitems, Windows-shell-uitvoeringshooks en activiteit van het Vertraagd laden Shell-serviceobject. Deze typen onbevoegde wijzigingen in het register en in bestanden kunnen uw computer schade toebrengen, de beveiliging van uw computer in gevaar brengen en waardevolle systeembestanden beschadigen.</p>

SystemGuards voor Windows	<p>SystemGuards voor Windows in het deelvenster Lijsten met vertrouwde items vertegenwoordigen eerder door VirusScan vastgestelde en onbevoegde wijzigingen in het register en bestanden, die u echter hebt toegestaan vanuit een waarschuwing of vanuit het deelvenster Scanresultaten.</p> <p>SystemGuards voor Windows stellen onbevoegde wijzigingen vast in het register en in bestanden in verband met handlers voor contextmenu's, appInit DLL's, het hosts-bestand van Windows, de Winlogon-shell, gelaagde serviceproviders van Winsocks enzovoort. Deze typen onbevoegde wijzigingen in het register en in bestanden kunnen van invloed zijn op de manier waarop uw computer gegevens verzendt en ontvangt via internet, kunnen het uiterlijk en gedrag van programma's wijzigen en kunnen ervoor zorgen dat verdachte programma's op uw computer worden uitgevoerd.</p>
SystemGuards voor browsers	<p>SystemGuards voor browsers in het deelvenster Lijsten met vertrouwde items vertegenwoordigen eerder door VirusScan vastgestelde en onbevoegde wijzigingen in het register en bestanden, die u echter hebt toegestaan vanuit een waarschuwing of vanuit het deelvenster Scanresultaten.</p> <p>SystemGuards voor browsers stellen onbevoegde wijzigingen in het register en ander ongewenst gedrag vast in verband met Browser Helper-objecten, softwaretoevoegingen voor Internet Explorer, URL's van Internet Explorer, beveiligingszones van Internet Explorer enzovoort. Dit type onbevoegde wijzigingen in het register kan resulteren in ongewenst browsergedrag zoals het doorleiden naar verdachte websites, wijzigingen in browserinstellingen en -opties en het instellen van verdachte websites als vertrouwde websites.</p>
Vertrouwde programma's	<p>Vertrouwde programma's zijn mogelijk ongewenste programma's die eerder door VirusScan zijn vastgesteld, maar die u hebt aangeduid als vertrouwd vanuit een waarschuwing of vanuit het deelvenster Scanresultaten.</p>

Overschrijding van limieten van vertrouwde buffers	<p>Overschrijding van limieten van vertrouwde buffers zijn ongewenste activiteiten die eerder door VirusScan zijn vastgesteld, maar die u hebt aangeduid als vertrouwd vanuit een waarschuwing of vanuit het deelvenster Scanresultaten.</p> <p>Overschrijdingen van bufferlimieten kunnen uw computer schade toebrengen en bestanden beschadigen. Overschrijdingen van bufferlimieten vinden plaats wanneer de hoeveelheid informatie die verdachte programma's of processen in een buffer opslaan de capaciteit van de buffer overschrijdt.</p>
--	---

HOOFDSTUK 11

De computer scannen

Als u SecurityCenter voor het eerst start, beschermt de real-time virusbeveiliging van VirusScan's uw computer onmiddellijk tegen mogelijk schadelijke virussen, Trojaanse paarden en andere beveiligingsrisico's. Als u real-time virusbeveiliging hebt ingeschakeld, wordt uw computer voortdurend door VirusScan gecontroleerd op virusactiviteit en worden bestanden telkens gescand als deze op uw computer worden geopend, met behulp van de door u ingestelde opties voor real-time scannen. Als u ervoor wilt zorgen dat uw computer beveiligd is tegen de meest recente beveiligingsrisico's, is het aan te raden om de real-time virusbeveiliging ingeschakeld te laten en een schema in te stellen voor regelmatige, meer uitgebreide handmatig scans. Zie voor meer informatie over real-time en handmatig scannen Virusbeveiliging instellen (pagina 41).

VirusScan biedt een uitgebreidere verzameling scanopties voor handmatige virusbeveiliging, waarmee u regelmatig meer diepgaande scans kunt uitvoeren. U kunt handmatige scans uitvoeren vanuit SecurityCenter, en de scans richten op specifieke locaties op basis van een door u ingesteld schema. U kunt handmatige scans echter ook rechtstreeks uitvoeren in Windows Verkenner tijdens uw werkzaamheden. Het scannen in SecurityCenter biedt het voordeel dat u mogelijkheden hebt om de scanopties op elk gewenst moment direct te wijzigen. Het scannen vanuit Windows Verkenner biedt echter een gemakkelijke manier om computerbeveiliging toe te passen.

Of u nu een handmatige scan uitvoert vanuit SecurityCenter of Windows Explorer, u kunt de scanresultaten naderhand altijd weergeven. U kunt de scanresultaten bestuderen om na te gaan of VirusScan virussen, Trojaanse paarden, spyware, adware, cookies of mogelijk ongewenste programma's heeft vastgesteld, hersteld of in quarantaine heeft geplaatst. U kunt de resultaten van een scan op verschillende manieren weergeven. U kunt bijvoorbeeld een eenvoudig overzicht van scanresultaten weergeven of gedetailleerde informatie, zoals de infectiestatus en het infectietype. U kunt ook algemene scan- en detectiestatistieken weergeven.

In dit hoofdstuk

De computer scannen.....	60
Scanresultaten weergeven.....	61

De computer scannen

U kunt een handmatige scan uitvoeren vanuit het menu Geavanceerd of Basis in SecurityCenter. Als u een scan uitvoert vanuit het menu Geavanceerd, kunt u de opties voor handmatig scannen instellen voordat u de scan uitvoert. Als u een scan uitvoert vanuit het menu Basis, wordt de scan onmiddellijk gestart door VirusScan met de bestaande scanopties. U kunt ook een scan uitvoeren in Windows Explorer met de bestaande scanopties.

- Voer een van de volgende handelingen uit:

Scannen in SecurityCenter

Om...	Doet u het volgende...
Te scannen met bestaande instellingen	Klik op Scannen in het menu Basis.
Te scannen met gewijzigde instellingen	Klik op Scannen in het menu Geavanceerd, selecteer de locaties die u wilt scannen, stel de scanopties in en klik op Nu scannen .

Scannen in Windows Verkenner

- Open Windows Verkenner.
- Klik met de rechtermuisknop op een bestand, een map of station en klik vervolgens op **Scannen**.

Opmerking: de scanresultaten worden weergegeven in de waarschuwing Scan voltooid. De resultaten omvatten het aantal gescande, vastgestelde, herstelde, in quarantaine geplaatste en verwijderde items. Klik op **Scandetails weergeven** voor meer informatie over de scanresultaten of het werken met geïnfecteerde items.

Scanresultaten weergeven

Als een handmatige scan is voltooid, geeft u de resultaten weer om te bepalen wat tijdens de scan is gevonden en om de huidige beveiligingsstatus van de computer te analyseren. De scanresultaten tonen of VirusScan virussen, Trojaanse paarden, spyware, adware, cookies of mogelijk ongewenste programma's heeft vastgesteld, hersteld of in quarantaine heeft geplaatst.

- Klik in het menu Basis of Geavanceerd op **Scannen** en voer een van de volgende handelingen uit:

Om...	Doet u het volgende...
Scanresultaten weer te geven in de waarschuwing	Raadpleeg de scanresultaten in de waarschuwing Scan voltooid.
Meer informatie te bekijken over scanresultaten	Klik op Scandetails weergeven in de waarschuwing Scan voltooid.
Een snel overzicht weer te geven van de scanresultaten	Wijs het pictogram Scan voltooid aan in het systeemvak op de taakbalk.
De scan- en detectiestatistieken weer te geven	Dubbelklik op het pictogram Scan voltooid in het systeemvak op de taakbalk.
Gedetailleerde informatie weer te geven over vastgestelde items, infectiestatus en -type	Dubbelklik op het pictogram Scan voltooid in het systeemvak op de taakbalk en klik vervolgens op Resultaten weergeven in het deulvenster Voortgang van scannen: handmatig scannen.

HOOFDSTUK 12

Werken met scanresultaten

Als VirusScan een beveiligingsrisico vaststelt tijdens een real-time of handmatige scan, probeert het programma deze dreiging automatisch af te handelen op basis van het type risico. Als VirusScan bijvoorbeeld een virus, een Trojaans paard of een trackingcookie op de computer vaststelt, probeert het programma om het geïnfecteerde bestand op te schonen. Als het bestand niet kan worden opgeschoond, probeert VirusScan het in quarantaine te plaatsen.

Bij bepaalde beveiligingsrisico's is VirusScan mogelijk niet in staat om een bestand op te schonen of in quarantaine te plaatsen. In dat geval wordt u gevraagd om de bedreiging verder af te handelen. U kunt verschillende stappen ondernemen op basis van het type bedreiging. Als bijvoorbeeld een virus is vastgesteld, maar VirusScan het bestand niet kan opschoonen of in quarantaine plaatsen, wordt verdere toegang tot het bestand ontzegd. Als er trackingcookies worden vastgesteld, maar VirusScan de cookies niet kan opschoonen of in quarantaine plaatsen, kunt u besluiten of u deze wilt verwijderen of als vertrouwd wilt markeren. Als mogelijk ongewenste programma's worden vastgesteld, onderneemt VirusScan geen automatische actie; in plaats hiervan kunt u besluiten om het programma in quarantaine te plaatsen of als vertrouwd aan te duiden.

Als VirusScan items in quarantaine plaatst, worden deze gecodeerd en vervolgens afgezonderd in een map, zodat wordt voorkomen dat de bestanden, programma's of cookies de computer kunnen schaden. U kunt de items in quarantaine terugzetten of verwijderen. In de meeste gevallen kunt u een in quarantaine geplaatste cookie verwijderen zonder dat dit van invloed is op het systeem. Als VirusScan echter een programma in quarantaine heeft geplaatst dat u kent en gebruikt, moet u overwegen om het te herstellen.

In dit hoofdstuk

Werken met virussen en Trojaanse paarden.....	64
Werken met mogelijk ongewenste programma's	64
Werken met in quarantaine geplaatste bestanden ...	65
Werken met bestanden en cookies in quarantaine ..	65

Werken met virussen en Trojaanse paarden

Als VirusScan een virus of een Trojaans paard vaststelt in een bestand op uw computer tijdens een real-time of een handmatige scan, probeert het programma het bestand op te schonen. Als het bestand niet kan worden opgeschoond, probeert VirusScan het in quarantaine te plaatsen. Als dit tevens mislukt, wordt toegang tot het bestand geweigerd (alleen bij real-time scans).

1 Open het deelvenster Scanresultaten.

Hoe?

1. Dubbelklik op het pictogram **Scan voltooid** in het systeemvak uiterst rechts op de taakbalk.
2. Klik in het deelvenster Voortgang van scannen: handmatige scan op **Resultaten weergeven**.

2 Klik in de lijst met scanresultaten op **Virussen en Trojaanse paarden**.

Opmerking: zie Werken met in quarantaine geplaatste bestanden (pagina 65) voor informatie over het werken met bestanden die in quarantaine zijn geplaatst.

Werken met mogelijk ongewenste programma's

Als VirusScan een mogelijk ongewenst programma op de computer vaststelt tijdens een real-time of een handmatige scan, kunt u het programma verwijderen of als vertrouwd aanmerken. Als u het mogelijk ongewenste programma verwijdert, wordt dit echter niet van het systeem verwijderd. Verwijderen betekent in dit geval dat het programma in quarantaine wordt geplaatst, waarmee wordt voorkomen dat het aan de computer of bestanden schade kan aanrichten.

1 Open het deelvenster Scanresultaten.

Hoe?

1. Dubbelklik op het pictogram **Scan voltooid** in het systeemvak uiterst rechts op de taakbalk.
2. Klik in het deelvenster Voortgang van scannen: handmatige scan op **Resultaten weergeven**.

2 Klik in de lijst met scanresultaten op **Mogelijk ongewenste programma's**.

3 Selecteer een mogelijk ongewenst programma.

4 Klik onder **Ik wil** op **Verwijderen** of **Vertrouwen**.

5 Bevestig de geselecteerde optie.

Werken met in quarantaine geplaatste bestanden

Als VirusScan geïnfecteerde bestanden in quarantaine plaatst, worden deze gecodeerd en vervolgens naar een map verplaatst, zodat wordt voorkomen dat de bestanden de computer kunnen schaden. U kunt de bestanden in quarantaine terugzetten of verwijderen.

1 Open het deelvenster Bestanden in quarantaine.

Hoe?

1. Klik in het linkerdeelvenster op **menu Geavanceerd**.
2. Klik op **Herstellen**.
3. Klik op **Bestanden**.

2 Selecteer een bestand dat in quarantaine is geplaatst.

3 Voer een van de volgende handelingen uit:

- Klik op **Herstellen** als u het geïnfecteerde bestand wilt herstellen en terugzetten op de oorspronkelijke locatie op uw computer.
- Klik op **Verwijderen** om het geïnfecteerde bestand van de computer te verwijderen.

4 Klik op **Ja** om de geselecteerde optie te bevestigen.

Tip: u kunt meerdere bestanden tegelijkertijd herstellen of verwijderen.

Werken met bestanden en cookies in quarantaine

Als VirusScan mogelijk ongewenste programma's of trackingcookies in quarantaine plaatst, worden deze gecodeerd en verplaatst naar een beveiligde map, zodat wordt voorkomen dat de programma's of cookies schade kunnen toebrengen aan de computer. U kunt de items in quarantaine herstellen of verwijderen. In de meeste gevallen kunt u een cookie in quarantaine verwijderen zonder dat dit invloed heeft op het systeem.

1 Open het deelvenster In quarantaine geplaatste programma's en trackingcookies.

Hoe?

1. Klik in het linkerdeelvenster op **menu Geavanceerd**.
2. Klik op **Herstellen**.
3. Klik op **Programma's en cookies**.
- 2 Selecteer een programma of cookie in quarantaine.
- 3 Voer een van de volgende handelingen uit:
 - Klik op **Herstellen** als u het geïnfecteerde bestand wilt herstellen en terugzetten op de oorspronkelijke locatie op uw computer.
 - Klik op **Verwijderen** om het geïnfecteerde bestand van de computer te verwijderen.
- 4 Klik op **Ja** om de bewerking te bevestigen.

Tip: u kunt meerdere programma's en cookies tegelijkertijd herstellen of verwijderen.

HOOFDSTUK 13

McAfee Personal Firewall

Personal Firewall biedt geavanceerde beveiliging voor uw computer en uw persoonlijke gegevens. Personal Firewall vormt een barrière tussen uw computer en internet, waarbij het internetverkeer wordt gecontroleerd op verdachte activiteiten, zonder dat hiervan melding wordt gemaakt.

Opmerking: SecurityCenter stelt u op de hoogte van kritieke en niet-kritieke beveiligingsproblemen zodra deze worden vastgesteld. Als u hulp nodig hebt bij het analyseren van beveiligingsproblemen, kunt u McAfee Virtual Technician uitvoeren.

In dit hoofdstuk

Functies van Personal Firewall.....	68
Firewall starten.....	71
Werken met waarschuwingen.....	73
Informatieve waarschuwingen beheren.....	77
Het beveiligingsniveau van Firewall configureren ...	79
Programma's en toegangsregels beheren	93
Systemservices beheren.....	105
Computerverbindingen beheren	111
Logbestanden, controles en analyses	121
Informatie over internetbeveiliging.....	133

Functies van Personal Firewall

Personal Firewall biedt de volgende functies:

Standaard- en aangepaste beveiligingsniveaus

U kunt zich beschermen tegen inbraken en verdachte activiteiten met behulp van de standaardbeveiligingsinstellingen van Firewall. U kunt deze instellingen ook aanpassen.

Real-time aanbevelingen

Dynamische aanbevelingen bieden u hulp om te bepalen of programma's verbinding met internet mogen maken of dat netwerkverkeer kan worden vertrouwd.

Intelligent toegangsbeheer voor programma's

Via waarschuwingen en gebeurtenislogboeken kunt u de internettoegang voor programma's beheren. Ook kunt u de toegangsrechten voor specifieke programma's configureren.

Beveiliging voor games

Hiermee verbergt u waarschuwingen over inbraakpogingen en verdachte activiteiten tijdens het spelen van schermvullende games.

Opstartbeveiliging

Zodra Windows® wordt gestart, beschermt Firewall uw computer tegen inbraakpogingen, ongewenste programma's en ongewenst netwerkverkeer.

Controle van systeemservicepoorten

Hiermee beheert u open en gesloten systeemservicepoorten die nodig zijn voor sommige programma's.

Computerverbindingen beheren

Hiermee kunt u verbindingen tussen uw computer en andere, externe computers toestaan en blokkeren.

Geïntegreerde HackerWatch-informatie

Deze functie brengt wereldwijde patronen van hack- en inbraakpogingen in kaart en verschaft de meest actuele informatie over programma's op uw computer en over wereldwijde beveiligingsgebeurtenissen en biedt statistische gegevens van internetpoorten.

Firewall vergrendelen

Hiermee blokkeert u onmiddellijk al het inkomend en uitgaand verkeer tussen uw computer en internet.

De standaardinstellingen van Firewall herstellen

U kunt de oorspronkelijke beveiligingsinstellingen van Firewall onmiddellijk weer herstellen.

Geavanceerde opsporing van Trojaanse paarden

Hiermee spoort u mogelijk kwaadaardige toepassingen, zoals Trojaanse paarden, op en verhindert u dat deze uw persoonlijke gegevens naar internet overbrengen.

Gebeurtenisregistratie

Hiermee volgt u recente inkomende en uitgaande gebeurtenissen en inbraakgebeurtenissen.

Internetverkeer controleren

Met wereldkaarten wordt de bron van vijandige aanvallen en vijandig verkeer aangegeven. Verder vindt u gedetailleerde contact- en eigenaargegevens en geografische gegevens van de bron-IP-adressen. Ook kunt inkomend en uitgaand verkeer analyseren en de bandbreedte en activiteiten van programma's controleren.

Inbraakpreventie

Hiermee beschermt u uw privacy tegen mogelijke bedreigingen vanaf internet. Met behulp van heuristische functionaliteit biedt McAfee een derde beschermingslaag door items te blokkeren die de kenmerken van een aanval of een hackpoging vertonen.

Geavanceerde verkeersanalyse

U kunt inkomend en uitgaand internetverkeer en inkomende en uitgaande programmaverbindingen analyseren, waaronder programma's die actief luisteren naar geopende verbindingen. Hiermee kunt u zien welke programma's kwetsbaar zijn voor inbraak en kunt u zo nodig actie ondernemen.

HOOFDSTUK 14

Firewall starten

Zodra u Firewall hebt geïnstalleerd, is uw computer beschermd tegen inbraak en ongewenst netwerkverkeer. Bovendien kunt u dan reageren op waarschuwingen en kunt u inkomende en uitgaande internettoegang voor bekende en onbekende programma's beheren. Slimme aanbevelingen en het beveiligingsniveau Vertrouwend worden automatisch ingeschakeld. Hierbij wordt de optie ingeschakeld om programma's alleen uitgaande internettoegang te bieden.

Het is mogelijk om Firewall uit te schakelen via het deelvenster Internet- en netwerkconfiguratie. Uw computer is dan echter niet langer beschermd tegen inbraak en ongewenst netwerkverkeer. Bovendien is het dan niet meer mogelijk om inkomende en uitgaande netwerkverbindingen op effectieve wijze te beheren. Als u de firewall moet uitschakelen, doe dat dan tijdelijk en uitsluitend wanneer het nodig is. U kunt Firewall ook weer inschakelen via het deelvenster Internet- en netwerkconfiguratie.

Wanneer Windows® Firewall is geïnstalleerd, wordt deze automatisch door Firewall uitgeschakeld en wordt Firewall ingesteld als de standaardfirewall.

Opmerking: Als u Firewall wilt configureren, opent u het deelvenster Netwerk en internetconfiguratie.

In dit hoofdstuk

Firewallbescherming starten.....	71
Firewallbescherming stoppen.....	72

Firewallbescherming starten

U kunt Firewall inschakelen om uw computer te beschermen tegen inbraak en ongewenst netwerkverkeer. Ook kunt u er in- en uitgaande internetverbindingen mee beheren.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configureren**.
- 2 Klik in het deelvenster Internet- en netwerkconfiguratie onder **Firewallbescherming is uitgeschakeld** op **Aan**.

Firewallbescherming stoppen

U kunt Firewall uitschakelen als u uw computer niet meer wilt beschermen tegen inbraak en ongewenst netwerkverkeer. Als Firewall is uitgeschakeld, kunt u inkomende en uitgaande netwerkverbindingen niet beheren.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configureren**.
- 2 Klik in het deelvenster Internet- en netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Uit**.

HOOFDSTUK 15

Werken met waarschuwingen

Firewall kent een breed scala aan waarschuwingen dat u ondersteunt bij het beheren van uw beveiliging. Deze waarschuwingen kunnen worden ingedeeld in drie basistypen:

- Rode waarschuwingen
- Gele waarschuwingen
- Groene waarschuwingen

Waarschuwingen kunnen ook informatie bevatten op basis waarvan u kunt bepalen hoe de desbetreffende waarschuwing moet worden afgehandeld. Daarnaast kunnen waarschuwingen informatie bevatten waarmee u informatie kunt ophalen over programma's die op uw computer worden uitgevoerd.

In dit hoofdstuk

Informatie over waarschuwingen 74

Informatie over waarschuwingen

Firewall kent drie basistypen waarschuwingen. Sommige van deze waarschuwingen bevatten informatie die u laat weten hoe u meer te weten kunt komen over programma's die op uw computer worden uitgevoerd.

Rode waarschuwingen

Een rode waarschuwing wordt weergegeven als Firewall een Trojaans paard op uw computer detecteert en blokkeert. Vervolgens wordt u aangeraden om uw computer op andere bedreigingen te scannen. Trojaanse paarden lijken legitieme programma's, maar deze programma's kunnen de werking van uw computer onderbreken, gegevens beschadigen en toegang tot uw gegevens verlenen aan onbevoegde personen. Deze waarschuwing wordt op alle beveiligingsniveaus weergegeven, behalve Open.

Gele waarschuwingen

Gele waarschuwingen zijn het meest gangbaar en informeren u over een activiteit van een programma of een netwerkgebeurtenis die door Firewall is gedetecteerd. In dat geval wordt de programma-activiteit of netwerkgebeurtenis in de waarschuwing beschreven. Ook worden een aantal opties aangeboden waarop u moet reageren. De waarschuwing **Nieuw netwerk aangetroffen** verschijnt bijvoorbeeld als een computer waarop Firewall is geïnstalleerd, wordt aangesloten op een nieuw netwerk. U kunt kiezen of u het netwerk wel of niet wilt vertrouwen. Als u het netwerk vertrouwt, wordt verkeer van en naar andere computers in het netwerk toegestaan en wordt het netwerk toegevoegd aan de lijst met vertrouwde IP-adressen. Als Slimme aanbevelingen is ingeschakeld, worden programma's toegevoegd aan het deelvenster Programmamachtigingen.

Groene waarschuwingen

Groene waarschuwingen bevatten meestal basisinformatie over een gebeurtenis en vergen geen handelingen van de gebruiker. Groene waarschuwingen zijn standaard uitgeschakeld en worden gewoonlijk weergegeven in gevallen waarin de beveiligingsniveaus Standaard, Vertrouwend, Strikt en Stealth zijn ingesteld.

Hulp voor gebruikers

Veel Firewall-waarschuwingen bevatten aanvullende informatie die u bij het beheren van de beveiliging van uw computer van dienst kan zijn, waaronder:

- **Meer informatie over dit programma:** Hiermee start u de McAfee-website over mondiale beveiliging, zodat er informatie kan worden opgehaald over een programma dat Firewall op uw computer heeft gedetecteerd.
- **McAfee op de hoogte stellen van dit programma:** Hiermee kunt u informatie over een onbekend bestand dat door Firewall op uw computer is gedetecteerd, naar McAfee verzenden.
- **McAfee raadt aan:** Hiermee geeft u advies weer over hoe waarschuwingen moeten worden afgehandeld. Het kan bijvoorbeeld zijn dat u via een bericht wordt aangeraden om een programma toegang te verlenen.

HOOFDSTUK 16

Informatieve waarschuwingen beheren

Met Firewall kunt u informatieve berichten weergeven of verbergen die worden gegenereerd als inbraakpogingen of verdachte activiteiten worden gedetecteerd tijdens bepaalde gebeurtenissen, bijvoorbeeld als u een game schermvullend speelt.

In dit hoofdstuk

Waarschuwingen weergeven tijdens het spelen van games	77
Informatieve waarschuwingen verbergen.....	78

Waarschuwingen weergeven tijdens het spelen van games

U kunt opgeven dat informatieve berichten van Firewall worden weergegeven als inbraakpogingen of verdachte activiteiten worden gedetecteerd terwijl u schermvullend games speelt.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Menu Geavanceerd**.
- 2 Klik op **Configureren**.
- 3 Klik in het deelvenster voor configuratie van SecurityCenter op **Geavanceerd** onder **Waarschuwingen**.
- 4 Selecteer in het deelvenster Waarschuwingsopties de optie **Informatiewaarschuwingen weergeven wanneer de spelletjesmodus wordt gedetecteerd**.
- 5 Klik op **OK**.

Informatieve waarschuwingen verbergen

U kunt opgeven dat informatieve berichten van Firewall over inbraakpogingen en verdachte activiteiten die worden gedetecteerd, niet worden weergegeven .

- 1 Klik in het deelvenster McAfee SecurityCenter op **Menu Geavanceerd**.
- 2 Klik op **Configureren**.
- 3 Klik in het deelvenster voor configuratie van SecurityCenter op **Geavanceerd** onder **Waarschuwingen**.
- 4 Klik in het deelvenster voor configuratie van SecurityCenter op **Informatiewaarschuwingen**.
- 5 Ga in het deelvenster Informatiewaarschuwingen op een van de volgende manieren te werk:
 - Selecteer **Informatieve waarschuwingen niet weergeven** als u alle informatieve waarschuwingen wilt verbergen.
 - Als u een afzonderlijke waarschuwing wilt verbergen, schakelt u deze waarschuwing uit.
- 6 Klik op **OK**.

HOOFDSTUK 17

Het beveiligingsniveau van Firewall configureren

Firewall biedt een aantal methoden voor het beheren van de beveiliging, waarbij u de wijze waarop er op beveiligingsgebeurtenissen en waarschuwingen moet worden gereageerd, kunt aanpassen.

Als u Firewall voor het eerst installeert, wordt het beveiligingsniveau voor de bescherming van uw computer ingesteld op Vertrouwend en wordt aan de programma's op de computer alleen uitgaande toegang tot internet toegestaan. Firewall biedt echter ook andere beveiligingsniveaus die uiteenlopen van zeer restrictief tot zeer tolerant.

Daarnaast biedt Firewall u de mogelijkheid om aanbevelingen bij waarschuwingen en bij internettoegang voor programma's weer te geven.

In dit hoofdstuk

Beveiligingsniveaus van Firewall beheren	80
Slimme aanbevelingen configureren voor waarschuwingen	85
Firewall-beveiliging optimaliseren	87
Firewall vergrendelen en problemen oplossen.....	90

Beveiligingsniveaus van Firewall beheren

Met de beveiligingsniveaus van Firewall kunt u bepalen in welke mate u waarschuwingen wilt beheren en erop wilt reageren. Deze waarschuwingen verschijnen als ongewenst netwerkverkeer of ongewenste ingaande en uitgaande internetverbindingen worden gedetecteerd. Het beveiligingsniveau van Firewall is standaard ingesteld op Vertrouwend waarbij alleen uitgaande toegang is toegestaan.

Als het beveiligingsniveau is ingesteld op Vertrouwend en als Slimme aanbevelingen is ingeschakeld, bieden gele waarschuwingen de optie om toegang toe te staan of te blokkeren voor onbekende programma's die inkomende toegang vereisen. Als bekende programma's worden gedetecteerd, verschijnen er groene informatieve waarschuwingen en wordt automatisch toegang verleend. Als toegang wordt verleend, mag een programma uitgaande verbindingen maken en luisteren naar ongevraagde inkomende verbindingen.

Over het algemeen geldt dat hoe restrictiever het beveiligingsniveau is (Stealth en Strikt), hoe meer opties en waarschuwingen er worden weergegeven, die u vervolgens moet afhandelen.

In de volgende tabel worden de zes beveiligingsniveaus van Firewall beschreven, van het meest tot het minst strikte:

Niveau	Beschrijving
Vergrendelen	Hiermee blokkeert u alle inkomende en uitgaande netwerkverbindingen, waaronder toegang tot websites, e-mail en beveiligingsupdates. Dit beveiligingsniveau heeft hetzelfde resultaat als het loskoppelen van de internetverbinding. U kunt deze instelling gebruiken om poorten te blokkeren die u in het deelvenster System services hebt ingesteld op Open.
Stealth	Hiermee blokkeert u alle inkomende internetverbindingen, met uitzondering van open poorten, en verbergt u de aanwezigheid van uw computer op het internet. De firewall waarschuwt u wanneer nieuwe programma's proberen een uitgaande internetverbinding te maken of aanvragen voor inkomende verbindingen ontvangen. Geblokkeerde en toegevoegde programma's worden weergegeven in het deelvenster Programmamachtigingen.

Strikt	Hiermee wordt u gewaarschuwd wanneer nieuwe programma's proberen een uitgaande internetverbinding te maken of aanvragen voor inkomende verbindingen ontvangen. Geblokkeerde en toegevoegde programma's worden weergegeven in het deelvenster Programmamachtigingen. Als het beveiligingsniveau is ingesteld op Strikt, vraagt een programma alleen het type toegang aan dat op dat moment is vereist, bijvoorbeeld alleen uitgaande toegang. U kunt deze toegang verlenen of blokkeren. Als het programma later zowel een inkomende als een uitgaande verbinding nodig heeft, kunt u via het deelvenster Programmamachtigingen volledige toegang voor het programma verlenen.
Standaard	Hiermee controleert u inkomende en uitgaande verbindingen en wordt u gewaarschuwd wanneer nieuwe programma's proberen internettoegang te krijgen. Geblokkeerde en toegevoegde programma's worden weergegeven in het deelvenster Programmamachtigingen.
Vertrouwend	Hiermee staat u inkomende en uitgaande (volledige toegang) of alleen uitgaande internetverbindingen voor programma's toe. Het standaard beveiligingsniveau is Vertrouwend, waarbij voor programma's alleen uitgaande toegang is toegestaan. Als u een programma volledige toegang verleent, wordt het automatisch door Firewall vertrouwd en aan de lijst met toegestane programma's in het deelvenster Programmamachtigingen toegevoegd. Als u een programma alleen uitgaande toegang verleent, wordt het door Firewall alleen automatisch vertrouwd als het een uitgaande internetverbinding start. Inkomende verbindingen worden niet automatisch vertrouwd.
Open	Hiermee worden alle inkomende en uitgaande internetverbindingen toegestaan.

Met Firewall is het ook mogelijk om het beveiligingsniveau Vertrouwend direct in te stellen (en alleen uitgaande toegang toe te staan) in het deelvenster Standaardwaarden van firewallbescherming herstellen.

Beveiligingsniveau instellen op Vergrendelen

U kunt het beveiligingsniveau van Firewall instellen op Vergrendelen om alle inkomende en uitgaande netwerkverbindingen te blokkeren.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configureren**.
- 2 Klik in het deelvenster Internet- en netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Verplaats de schuifregelaar in het deelvenster Beveiligingsniveau zodat **Vergrendelen** wordt weergegeven als het huidige niveau.
- 4 Klik op **OK**.

Beveiligingsniveau instellen op Stealth

U kunt het beveiligingsniveau van Firewall instellen op Stealth. Hiermee blokkeert u alle inkomende internetverbindingen, met uitzondering van open poorten, en verbergt u de aanwezigheid van uw computer op het internet.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configureren**.
- 2 Klik in het deelvenster Internet- en netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Verplaats de schuifregelaar in het deelvenster Beveiligingsniveau zodat **Stealth** wordt weergegeven als het huidige niveau.
- 4 Klik op **OK**.

Opmerking: In de modus Stealth ontvangt u een waarschuwing van Firewall als nieuwe programma's uitgaande internetverbindingen aanvragen of aanvragen voor inkomende verbindingen ontvangen.

Beveiligingsniveau instellen op Strikt

Als u het beveiligingsniveau instelt op Strikt, wordt u geïnformeerd als nieuwe programma's proberen uitgaande internetverbindingen tot stand te brengen of aanvragen voor inkomende verbindingen ontvangen.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configureren**.
- 2 Klik in het deelvenster Internet- en netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Verplaats de schuifregelaar in het deelvenster Beveiligingsniveau zodat **Strikt** wordt weergegeven als het huidige niveau.
- 4 Klik op **OK**.

Opmerking: Als het beveiligingsniveau is ingesteld op Strikt, vraagt een programma alleen het type toegang aan dat op dat moment is vereist, bijvoorbeeld alleen uitgaande toegang. U kunt deze toegang verlenen of blokkeren. Als het programma later zowel een inkomende als een uitgaande verbinding nodig heeft, kunt u via het deelvenster Programmamachtigingen volledige toegang voor het programma verlenen.

Beveiligingsniveau instellen op Standaard

Als u het beveiligingsniveau instelt op Standaard, worden inkomende en uitgaande internetverbindingen gecontroleerd en wordt u gewaarschuwd wanneer nieuwe programma's internettoegang proberen te krijgen.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configureren**.
- 2 Klik in het deelvenster Internet- en netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Verplaats de schuifregelaar in het deelvenster Beveiligingsniveau zodat **Standaard** wordt weergegeven als het huidige niveau.
- 4 Klik op **OK**.

Beveiligingsniveau instellen op Vertrouwend

U kunt het beveiligingsniveau van Firewall instellen op Vertrouwend om volledige of alleen uitgaande internettoegang te verlenen.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configureren**.
- 2 Klik in het deelvenster Internet- en netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Verplaats de schuifregelaar in het deelvenster Beveiligingsniveau zodat **Vertrouwend** wordt weergegeven als het huidige niveau.
- 4 Voer een van de volgende handelingen uit:
 - Selecteer **Volledige toegang toestaan** om uitgaande en inkomende netwerktoegang (volledige toegang) te verlenen.
 - Selecteer **Alleen uitgaande toegang toestaan** om alleen uitgaande netwerktoegang te verlenen.
- 5 Klik op **OK**.

Opmerking: Alleen uitgaande toegang toestaan is de standaardinstelling.

Beveiligingsniveau instellen op Open

U kunt het beveiligingsniveau van Firewall instellen op Open om alle inkomende en uitgaande netwerkverbindingen toe te staan.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configureren**.
- 2 Klik in het deelvenster Internet- en netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Verplaats de schuifregelaar in het deelvenster Beveiligingsniveau zodat **Open** wordt weergegeven als het huidige niveau.
- 4 Klik op **OK**.

Slimme aanbevelingen configureren voor waarschuwingen

Waarschuwingen die worden gegenereerd als programma's proberen toegang tot internet te krijgen, kunnen vergezeld gaan van aanbevelingen. U kunt instellen of deze aanbevelingen moeten worden toegevoegd, uitgesloten of weergegeven. Slimme aanbevelingen bieden u hulp om te besluiten hoe u moet reageren op waarschuwingen.

Als Slimme aanbevelingen is ingeschakeld (en als het beveiligingsniveau is ingesteld op Vertrouwend waarbij alleen uitgaande toegang is toegestaan), wordt voor bekende programma's automatisch toegang verleend of geblokkeerd en bevatten waarschuwingen die u ontvangt als onbekende of potentieel schadelijke programma's worden gedetecteerd, aanbevelingen wat u het beste kunt doen.

Als Slimme aanbevelingen is uitgeschakeld, wordt internettoegang niet automatisch toegestaan of geblokkeerd en worden er ook geen aanbevelingen gedaan over wat u het beste kunt doen.

Als Slimme aanbevelingen is ingesteld op Alleen weergeven, wordt u via een waarschuwing gevraagd om toegang te verlenen of te blokkeren en krijgt u aanbevelingen wat u het beste kunt doen.

Slimme aanbevelingen inschakelen

U kunt Slimme aanbevelingen inschakelen zodat Firewall programma's automatisch toestaat of blokkeert en u waarschuwt voor onbekende en mogelijk schadelijke programma's.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configureren**.
- 2 Klik in het deelvenster Internet- en netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Selecteer in het deelvenster Beveiligingsniveau, onder **Slimme aanbevelingen**, de optie **Slimme aanbevelingen inschakelen**.
- 4 Klik op **OK**.

Slimme aanbevelingen uitschakelen

U kunt Slimme aanbevelingen uitschakelen. Programma's worden in dat geval automatisch door Firewall toegestaan of geblokkeerd en u ontvangt waarschuwingen voor onbekende en mogelijk schadelijke programma's. De waarschuwingen bevatten echter geen aanbevelingen hoe u de toegang voor programma's het beste kunt afhandelen. Als een nieuw programma wordt gedetecteerd dat verdacht is of dat bekend staat als potentieel schadelijk, wordt voor dat programma automatisch de toegang tot internet geblokkeerd.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configureren**.
- 2 Klik in het deelvenster Internet- en netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Selecteer in het deelvenster Beveiligingsniveau, onder **Slimme aanbevelingen**, de optie **Slimme aanbevelingen uitschakelen**.
- 4 Klik op **OK**.

Slimme aanbevelingen alleen weergeven

U kunt instellen dat Slimme aanbevelingen voor waarschuwingen alleen worden weergegeven. U ontvangt dan aanbevelingen wat u het beste kunt doen, maar besluit zelf of u onbekende en potentieel schadelijke programma's toestaat of blokkeert.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configureren**.
- 2 Klik in het deelvenster Internet- en netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Selecteer in het deelvenster Beveiligingsniveau, onder **Slimme aanbevelingen**, de optie **Alleen weergeven**.
- 4 Klik op **OK**.

Firewall-beveiliging optimaliseren

Er zijn vele manieren waarop de veiligheid van uw computer in gevaar kan komen. Er zijn bijvoorbeeld programma's die proberen om toegang tot internet te krijgen voordat Windows® is gestart. Verder zijn er handige computergebruikers die uw computer kunnen traceren (of een ping kunnen uitvoeren) om vast te stellen of deze op een netwerk is aangesloten. Met Firewall kunt u uw computer verdedigen tegen beide typen inbraken, doordat u opstartbeveiliging kunt inschakelen en pingaanvragen kunt blokkeren. Met de eerste instelling kunnen programma's tijdens het starten van Windows geen toegang krijgen tot internet. Met de tweede instelling worden pingaanvragen geblokkeerd waarmee andere gebruikers uw computer op een netwerk kunnen detecteren.

Bij de standaardinstallatie-instellingen worden de meest voorkomende inbraakpogingen, zoals Denial of Service-aanvallen en -misbruik, voorkomen. Met de standaardinstallatie-instellingen bent u beschermd tegen dergelijke aanvallen en scans. Via het deelvenster 'Inbraakdetectie' kunt u echter de automatische detectie voor een of meer aanvallen of scans uitschakelen.

Computer beveiligen tijdens het opstarten

U kunt uw computer beveiligen terwijl Windows opstart door nieuwe programma's te blokkeren die geen internettoegang hadden tijdens het opstarten, maar die dat nu wel nodig hebben. Firewall toont relevante waarschuwingen voor programma's die tijdens het opstarten toegang tot internet hebben aangevraagd. U kunt de toegang toestaan of blokkeren. Deze optie is niet beschikbaar als het beveiligingsniveau is ingesteld op 'Open' of 'Vergrendelen'.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Selecteer in het deelvenster Beveiligingsniveau onder **Beveiligingsinstellingen Opstartbeveiliging inschakelen**.
- 4 Klik op **OK**.

Opmerking: als opstartbeveiliging is ingeschakeld, worden geblokkeerde verbindingen en inbraken niet geregistreerd.

Instellingen voor pingaanvragen configureren

U kunt toestaan of voorkomen dat uw computer op het netwerk kan worden gedetecteerd door andere computergebruikers.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 In het deelvenster 'Beveiligingsniveau', onder **Beveiligingsinstellingen**, gaat u op een van de volgende manieren te werk:
 - Selecteer **ICMP-pingaanvragen toestaan** als u wilt toestaan dat uw computer op het netwerk kan worden gedetecteerd door middel van pingaanvragen.
 - Maak de selectie van **ICMP-pingaanvragen toestaan** ongedaan als u wilt voorkomen dat uw computer op het netwerk kan worden gedetecteerd door middel van pingaanvragen.
- 4 Klik op **OK**.

Inbraakdetectie configureren

U kunt inbraakpogingen detecteren om uw computer te beschermen tegen aanvallen en niet-geautoriseerde scans. Bij de standaard Firewallinstelling worden de meest voorkomende inbraakpogingen, zoals Denial of Service-aanvallen en -misbruik, voorkomen. Maar u kunt het automatisch detecteren van één of meer aanvallen of scans ook uitschakelen.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Klik op **Inbraakdetectie** in het deelvenster Firewall.
- 4 Ga onder **Pogingen tot indringing detecteren** op een van de volgende manieren te werk:
 - Selecteer een naam als u de aanval of scan automatisch wilt laten detecteren.
 - Wis een naam als u het automatisch detecteren van de aanval of scan wilt uitschakelen.
- 5 Klik op **OK**.

De instellingen van de beveiligingsstatus van Firewall configureren

U kunt Firewall zo configureren dat specifieke problemen op uw computer niet gerapporteerd worden aan het SecurityCenter.

- 1 Klik in het deelvenster McAfee SecurityCenter onder **SecurityCenter-informatie** op **Configureren**.
- 2 Klik in het deelvenster Configuratie van SecurityCenter onder **Beveiligingsstatus** op **Geavanceerd**.
- 3 Selecteer in het deelvenster Genegeerde problemen een of meer van de volgende opties:
 - **Firewallbescherming is uitgeschakeld.**
 - **Firewall is ingesteld op het beveiligingsniveau Open.**
 - **Firewallservice wordt niet uitgevoerd.**
 - **Firewallbescherming is niet geïnstalleerd op uw computer.**
 - **Uw Windows Firewall is uitgeschakeld.**
 - **Geen uitgaande firewall geïnstalleerd op uw computer.**
- 4 Klik op **OK**.

Firewall vergrendelen en problemen oplossen

Met Vergrendelen wordt direct al het inkomend en uitgaand netwerkverkeer geblokkeerd om u te helpen een probleem op uw computer te isoleren en op te lossen.

Firewall onmiddellijk vergrendelen

U kunt Firewall vergrendelen om direct al het netwerkverkeer tussen uw computer en internet te blokkeren.

- 1 Klik in het deelvenster McAfee SecurityCenter onder **Algemene taken** op **Firewall vergrendelen**.
- 2 Klik in het deelvenster Firewall vergrendelen op **Vergrendelen**.
- 3 Klik op **Ja** om te bevestigen.

Tip: U kunt de Firewall ook vergrendelen door met de rechtermuisknop te klikken op het pictogram van het SecurityCenter  in het systeemvak helemaal rechts op de taakbalk, klik vervolgens op **Snelkoppelingen** en op **Firewall vergrendelen**.

Firewall onmiddellijk ontgrendelen

U kunt Firewall ontgrendelen om direct al het netwerkverkeer tussen uw computer en internet toe te staan.

- 1 Klik in het deelvenster McAfee SecurityCenter onder **Algemene taken** op **Firewall vergrendelen**.
- 2 Klik in het deelvenster Vergrendelen ingeschakeld op **Ontgrendelen**.
- 3 Klik op **Ja** om te bevestigen.

Firewall opnieuw op de standaardwaarden instellen

U kunt Firewall opnieuw op de oorspronkelijke beveiligingsinstellingen instellen. Dit stelt de beveiligingsinstelling in op Vertrouwd en verleent alleen uitgaande toegang, schakelt Slimme aanbevelingen in, herstelt de lijst met standaardprogramma's en de toestemming hiervoor in het deelvak Programmamachtigingen, verwijdert vertrouwde en verboden IP-adressen en herstelt systeemservices, instellingen voor het gebeurtenislogboek en inbraakdetectie.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Standaardwaarden van Firewall herstellen**.
- 2 Klik in het deelvenster Standaardwaarden van firewall herstellen op **Standaardwaarden herstellen**.
- 3 Klik op **Ja** om te bevestigen.

Tip: U kunt de standaardwaarden van de Firewall ook herstellen door met de rechtermuisknop op het pictogram SecurityCenter te klikken  in het systeemvak helemaal rechts op de taakbalk, klik vervolgens op **Snelkoppelingen** en op **Standaardwaarden van firewall herstellen**.

HOOFDSTUK 18

Programma's en toegangsregels beheren

Met Firewall kunt u toegangsregels instellen en beheren voor bestaande en nieuwe programma's die inkomende en uitgaande internettoegang nodig hebben. Met Firewall kunt u volledige toegang of alleen uitgaande toegang verlenen voor programma's. U kunt de toegang voor programma's ook blokkeren.

In dit hoofdstuk

Internettoegang voor programma's toestaan	94
Alleen uitgaande toegang voor programma's toestaan	97
Internettoegang voor programma's blokkeren.....	99
Toegangsrechten voor programma's verwijderen....	101
Informatie over programma's.....	102

Internettoegang voor programma's toestaan

Sommige programma's, zoals internetbrowsers, hebben toegang tot internet nodig om naar behoren te kunnen functioneren.

In Firewall kunt u via de pagina 'Programmamachtigingen' het volgende doen:

- Toegang voor programma's toestaan
- Alleen uitgaande toegang voor programma's toestaan
- Toegang voor programma's blokkeren

Het is ook mogelijk om een programma volledige toegang en alleen uitgaande toegang te verlenen vanuit de logboeken 'Uitgaande gebeurtenissen' en 'Recente gebeurtenissen'.

Volledige toegang voor een programma toestaan

U kunt inkomende en uitgaande internettoegang volledig toestaan voor een bestaand geblokkeerd programma op uw computer.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Klik in het deelvenster 'Firewall' op **Programmamachtigingen**.
- 4 Selecteer onder **Programmamachtigingen** een programma met **Geblokkeerd** of **Alleen uitgaande toegang**.
- 5 Klik onder **Actie** op **Toegang toestaan**.
- 6 Klik op **OK**.

Volledige toegang voor een nieuw programma toestaan

U kunt inkomende en uitgaande internettoegang volledig toestaan voor een nieuw programma op uw computer.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Klik in het deelvenster 'Firewall' op **Programmamachtigingen**.
- 4 Klik onder **Programmamachtigingen** op **Toegestaan programma toevoegen**.
- 5 Zoek via het dialoogvenster **Programma toevoegen** naar het programma dat u wilt toevoegen en klik vervolgens op **Open**.

Opmerking: het wijzigen van machtigingen van nieuw toegevoegde programma's gaat op dezelfde manier als bij bestaande programma's: selecteer het programma en klik vervolgens onder **Actie** op **Alleen uitgaande toegang toestaan** of op **Toegang blokkeren**.

Volledige toegang toestaan vanuit het logboek voor recente gebeurtenissen

U kunt inkomende en uitgaande internettoegang volledig toestaan voor een bestaand geblokkeerd programma dat wordt weergegeven in het logboek voor recente gebeurtenissen.

- 1 Klik in het deelvenster McAfee SecurityCenter op het menu **Geavanceerd**.
- 2 Klik op **Rapporten en logboeken**.
- 3 Selecteer de beschrijving van de gebeurtenis onder **Recente gebeurtenissen** en klik vervolgens op **Toegang toestaan**.
- 4 Klik in het dialoogvenster Programmamachtigingen op **Ja** om te bevestigen.

Verwante onderwerpen

- Uitgaande gebeurtenissen weergeven (pagina 124)

Volledige toegang toestaan vanuit het logboek voor uitgaande gebeurtenissen

U kunt inkomende en uitgaande internettoegang volledig toestaan voor een bestaand geblokkeerd programma dat wordt weergegeven in het logboek voor uitgaande gebeurtenissen.

- 1 Klik in het deelvenster McAfee SecurityCenter op het menu **Geavanceerd**.
- 2 Klik op **Rapporten en logboeken**.
- 3 Klik onder **Recente gebeurtenissen** op **Logboek weergeven**.
- 4 Klik op **Internet en netwerk** en vervolgens op **Uitgaande gebeurtenissen**.
- 5 Selecteer een programma en klik onder **Ik wil** op **Toegang toestaan**.
- 6 Klik in het dialoogvenster Programmamachtigingen op **Ja** om te bevestigen.

Alleen uitgaande toegang voor programma's toestaan

Sommige programma's op uw computer hebben uitgaande toegang tot internet nodig. U kunt in Firewall programmamachtigingen configureren om alleen uitgaande toegang tot internet toe te staan.

Alleen uitgaande toegang voor een programma toestaan

U kunt een programma alleen uitgaande toegang tot internet toestaan.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Klik in het deelvenster 'Firewall' op **Programmamachtigingen**.
- 4 Selecteer onder **Programmamachtigingen** een programma met **Geblokkeerd** of **Volledige toegang**.
- 5 Klik onder **Actie** op **Alleen uitgaande toegang toestaan**.
- 6 Klik op **OK**.

Alleen uitgaande toegang toestaan vanuit het logboek voor recente gebeurtenissen

U kunt alleen uitgaande internettoegang toestaan voor een bestaand geblokkeerd programma dat wordt weergegeven in het logboek voor recente gebeurtenissen.

- 1 Klik in het deelvenster McAfee SecurityCenter op het menu **Geavanceerd**.
- 2 Klik op **Rapporten en logboeken**.
- 3 Selecteer de beschrijving van de gebeurtenis onder **Recente gebeurtenissen** en klik vervolgens op **Alleen uitgaande toegang toestaan**.
- 4 Klik in het dialoogvenster Programmamachtigingen op **Ja** om te bevestigen.

Alleen uitgaande toegang toestaan vanuit het logboek voor uitgaande gebeurtenissen

U kunt alleen uitgaande internettoegang toestaan voor een bestaand geblokkeerd programma dat wordt weergegeven in het logboek voor uitgaande gebeurtenissen.

- 1 Klik in het deelvenster McAfee SecurityCenter op het menu **Geavanceerd**.
- 2 Klik op **Rapporten en logboeken**.
- 3 Klik onder **Recente gebeurtenissen** op **Logboek weergeven**.
- 4 Klik op **Internet en netwerk** en vervolgens op **Uitgaande gebeurtenissen**.
- 5 Selecteer een programma en klik onder **Ik wil** op **Alleen uitgaande toegang toestaan**.
- 6 Klik in het dialoogvenster Programmamachtigingen op **Ja** om te bevestigen.

Internettoegang voor programma's blokkeren

Met Firewall kunt u de internettoegang voor bepaalde programma's blokkeren. Controleer dat het blokkeren van een programma niet tot gevolg heeft dat uw netwerkverbinding wordt onderbroken, of dat een programma dat verbinding met internet nodig heeft, niet meer naar behoren kan functioneren.

Toegang voor een programma blokkeren

U kunt inkomende en uitgaand internettoegang blokkeren voor een programma.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Klik in het deelvenster 'Firewall' op **Programmamachtigingen**.
- 4 Selecteer onder **Programmamachtigingen** een programma met **Volledige toegang** of **Alleen uitgaande toegang**.
- 5 Klik onder **Actie** op **Toegang blokkeren**.
- 6 Klik op **OK**.

Toegang voor een nieuw programma blokkeren

U kunt inkomende en uitgaand internettoegang blokkeren voor een nieuw programma.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Klik in het deelvenster 'Firewall' op **Programmamachtigingen**.
- 4 Klik onder **Programmamachtigingen** op **Geblokkeerd programma toevoegen**.
- 5 Zoek in het dialoogvenster Programma toevoegen naar het programma dat u wilt toevoegen en klik vervolgens op **Open**.

Opmerking: voor het wijzigen van machtigingen van nieuw toegevoegde programma's; selecteer het programma en klik vervolgens onder **Actie** op **Alleen uitgaande toegang toestaan** of op **Toegang toestaan**.

De toegang tot internet blokkeren vanuit het logboek voor recente gebeurtenissen

U kunt inkomende en uitgaande internettoegang blokkeren voor een programma dat wordt weergegeven in het logboek voor recente gebeurtenissen.

- 1 Klik in het deelvenster McAfee SecurityCenter op het menu **Geavanceerd**.
- 2 Klik op **Rapporten en logboeken**.
- 3 Selecteer de beschrijving van de gebeurtenis onder **Recente gebeurtenissen** en klik vervolgens op **Toegang blokkeren**.
- 4 Klik in het dialoogvenster Programmamachtigingen op **Ja** om te bevestigen.

Toegangsrechten voor programma's verwijderen

Controleer voordat u de toegangsrechten voor een programma verwijdert, of deze actie geen nadelige gevolgen heeft voor de functionaliteit van de computer of de netwerkverbinding.

Programmamachtigingen verwijderen

U kunt inkomende of uitgaand internettoegang verwijderen voor een programma.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Klik in het deelvenster 'Firewall' op **Programmamachtigingen**.
- 4 Selecteer een programma onder **Programmamachtigingen**.
- 5 Klik onder **Actie** op **Programmamachtiging verwijderen**.
- 6 Klik op **OK**.

Opmerking: sommige programma's kunt u niet wijzigen.
Uitgeschakelde acties worden in dat geval lichter weergegeven.

Informatie over programma's

Als u onzeker bent over de keuze van de machtigingen voor een bepaald programma, kunt u op de HackerWatch-website van McAfee informatie over dat programma vinden.

Informatie over programma's raadplegen

U kunt via de website HackerWatch van McAfee informatie krijgen over programma's om te bepalen of u inkomende en uitgaande internettoegang wilt toestaan of blokkeren.

Opmerking: Controleer dat de computer is aangesloten op internet, zodat de browser succesvol de HackerWatch-website van McAfee kan openen. Deze site biedt actuele informatie over programma's, vereisten voor internettoegang en beveiligingsrisico's.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Klik in het deelvenster 'Firewall' op **Programmamachtigingen**.
- 4 Selecteer een programma onder **Programmamachtigingen**.
- 5 Klik onder **Actie** op **Meer informatie**.

Informatie over een programma opvragen vanuit het logboek voor uitgaande gebeurtenissen

U kunt via het logboek Uitgaande gebeurtenissen programmainformatie krijgen van de website HackerWatch van McAfee om te bepalen voor welke programma's u inkomende en uitgaande internettoegang wilt toestaan of blokkeren.

Opmerking: Controleer dat de computer is aangesloten op internet, zodat de browser succesvol de HackerWatch-website van McAfee kan openen. Deze site biedt actuele informatie over programma's, vereisten voor internettoegang en beveiligingsrisico's.

- 1 Klik in het deelvenster McAfee SecurityCenter op het menu **Geavanceerd**.
- 2 Klik op **Rapporten en logboeken**.
- 3 Selecteer een gebeurtenis onder Recente gebeurtenissen en klik vervolgens op **Logboek weergeven**.
- 4 Klik op **Internet en netwerk** en vervolgens op **Uitgaande gebeurtenissen**.
- 5 Selecteer een IP-adres en klik vervolgens op **Lees meer**.

HOOFDSTUK 19

Systemservices beheren

Bepaalde programma's (waaronder webservers en serverprogramma's voor het delen van bestanden) werken alleen als deze ongevraagde verbindingen van andere computers via toegewezen poorten van systemservices accepteren. Deze servicepoorten worden gewoonlijk door Firewall gesloten omdat deze het meest risicovolle element in de beveiliging van uw systeem vormen. Voor het accepteren van verbindingen van externe computers moeten de servicepoorten echter geopend zijn.

In dit hoofdstuk

Poorten voor systemservices configureren 106

Poorten voor systeemservices configureren

Systeemservicepoorten kunnen geconfigureerd worden om externe toegang tot een netwerkservice op uw computer toe te staan of te blokkeren.

De onderstaande lijst toont de gebruikelijke systeemservices en de bijbehorende poorten:

- Poort 20-21 voor File Transfer Protocol (FTP)
- Poort 143 voor e-mailserver (IMAP)
- Poort 110 voor e-mailserver (POP3)
- Poort 25 voor e-mailserver (SMTP)
- Poort 445 voor Microsoft Directory Server (MSFT DS)
- Poort 1433 voor Microsoft SQL-server (MSFT SQL)
- Poort 123 voor Network Time Protocol
- Poort 3389 voor Desktop / Hulp op afstand / Terminal Server (RDP)
- Poort 135 voor Remote Procedure Calls (RPC)
- Poort 443 voor beveiligde webserver (HTTPS)
- Poort 5000 voor Universal Plug and Play (UPnP)
- Poort 80 voor webserver (HTTP)
- Poort 137-139 voor NETBIOS (delen van bestanden in Windows)

Systeemservicepoorten kunnen ook geconfigureerd worden om toe te staan de internetverbinding van een computer te delen met andere computers die op hetzelfde netwerk zijn aangesloten. Deze verbinding, ook wel voorziening Internetverbinding delen (ICS) genoemd, staat de computer die de verbinding deelt toe om te functioneren als een gateway voor het internet voor de andere computer op het netwerk.

Opmerking: Als uw computer een applicatie heeft die web- of FTP-serververbindingen accepteert, dan moet de computer die de verbinding deelt wellicht de bijbehorende systeemservicepoort openen en doorgestuurde of inkomende verbindingen toestaan voor die poorten.

Toegang tot een bestaande poort voor een systeemservice toestaan

U kunt een bestaande poort openen om externe toegang tot een netwerkservice op uw computer toe te staan.

Opmerking: Een geopende poort voor een systeemservice kan uw computer kwetsbaar maken voor van internet afkomstige bedreigingen van de beveiliging. U moet daarom alleen poorten openen als dat echt nodig is.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld op Geavanceerd**.
- 3 Klik op **Systeemservices** in het deelvenster 'Firewall'.
- 4 Selecteer de servicepoort die u wilt openen onder **Poort voor systeemservice openen**.
- 5 Klik op **OK**.

De toegang tot een bestaande poort voor een systeemservice blokkeren

U kunt een bestaande poort sluiten om externe toegang tot een netwerkservice op uw computer te blokkeren.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld op Geavanceerd**.
- 3 Klik op **Systeemservices** in het deelvenster 'Firewall'.
- 4 Schakel onder **Poort voor systeemservice openen** het selectievakje uit van de servicepoort die u wilt sluiten.
- 5 Klik op **OK**.

Een nieuwe poort voor een systeemservice openen

U kunt een nieuwe netwerkservicepoort op uw computer configureren die u kunt openen of sluiten om externe toegang tot uw computer toe te staan of te blokkeren.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Klik op **Systeemservices** in het deelvenster 'Firewall'.
- 4 Klik op **Toevoegen**.
- 5 Voer in het deelvenster Systeemservices onder **Poorten en Systeemservices** het volgende in:
 - De programmaam
 - Inkomende TCP/IP-poorten
 - Uitgaande TCP/IP-poorten
 - Inkomende UDP-poorten
 - Uitgaande UDP-poorten
- 6 Selecteer **Netwerkactiviteit van deze poort doorsturen naar netwerkgebruikers die de voorziening Internetverbinding delen gebruiken** indien u de activiteitsinformatie van deze poort door wilt sturen naar een andere Windows-computer op het netwerk die uw internetverbinding deelt.
- 7 Voeg eventueel een beschrijving voor de nieuwe configuratie toe.
- 8 Klik op **OK**.

Opmerking: Als uw computer een applicatie heeft die web- of FTP-serververbindingen accepteert, dan moet de computer die de verbinding deelt wellicht de bijbehorende systeemservicepoort openen en doorgestuurde of inkomende verbindingen toestaan voor die poorten. Als u gebruik maakt van de voorziening Internetverbinding delen (ICS), dient u ook een vertrouwde internetverbinding toe te voegen aan de lijst Vertrouwde IP-adressen. Voor meer informatie zie Vertrouwde computerverbinding toevoegen:

Een poort voor een systeemservice wijzigen

U kunt informatie wijzigen over inkomende en uitgaande netwerktoegang van een bestaande systeemservicepoort.

Opmerking: Als de poortinformatie niet juist is ingevoerd, mislukt het uitvoeren van de systeemservice.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Klik op **Systeemservices** in het deelvenster 'Firewall'.
- 4 Selecteer een systeemservice en klik vervolgens op **Bewerken**.
- 5 Voer in het deelvenster Systeemservices onder **Poorten en Systeemservices** het volgende in:
 - De programmaam
 - Inkomende TCP/IP-poorten
 - Uitgaande TCP/IP-poorten
 - Inkomende UDP-poorten
 - Uitgaande UDP-poorten
- 6 Selecteer **Netwerkactiviteit van deze poort doorsturen naar netwerkgebruikers die de voorziening Internetverbinding delen gebruiken** indien u de activiteitsinformatie van deze poort door wilt sturen naar een andere Windows-computer op het netwerk die uw internetverbinding deelt.
- 7 Voeg eventueel een beschrijving voor de gewijzigde configuratie toe.
- 8 Klik op **OK**.

Een poort voor een systeemservice verwijderen

U kunt een bestaande systeemservicepoort van uw computer verwijderen. Na verwijdering hebben externe computers geen toegang meer tot de netwerkservice op uw computer.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Klik op **Systeemservices** in het deelvenster 'Firewall'.
- 4 Selecteer een systeemservice en klik vervolgens op **Verwijderen**.
- 5 Klik **Ja** op de opdrachtregel om te bevestigen.

HOOFDSTUK 20

Computerverbindingen beheren

U kunt Firewall configureren voor het beheren van specifieke externe verbindingen naar uw computer door middel van regels die zijn gebaseerd op IP-adressen (Internet Protocol) van externe computers. Computers waaraan een vertrouwd IP-adres is gekoppeld, kunnen worden vertrouwd om toegang te krijgen tot uw computer. Computers waaraan een onbekend, verdacht of onvertrouwd IP-adres is gekoppeld, kunnen worden uitgesloten van verbinding met uw computer.

Als u een verbinding toestaat, controleer dan of de computer die u vertrouwt, veilig is. Als een computer die u vertrouwt, is geïnfecteerd met een worm of een ander mechanisme, kan uw computer vatbaar zijn voor virusinfecties. Bovendien raadt McAfee u aan om te controleren of de computer(s) die u vertrouwt, zelf ook zijn beveiligd door middel van een firewall en een antivirusprogramma dat up-to-date is. Verkeer dat afkomstig is van IP-adressen uit de lijst met vertrouwde IP-adressen, wordt niet in het logboek geregistreerd. Ook worden voor deze adressen geen gebeurteniswaarschuwingen gegenereerd.

Computers waaraan een onbekend, verdacht of onvertrouwd IP-adres is gekoppeld, kunnen worden uitgesloten van verbinding met uw computer.

Aangezien Firewall al het ongewenste verkeer blokkeert, is het normaal gesproken niet nodig om een IP-adres te blokkeren. U moet een IP-adres alleen blokkeren wanneer u zeker weet dat een internetverbinding een specifieke bedreiging oplevert. Zorg ervoor dat u geen belangrijke IP-adressen blokkeert, zoals de DNS- of DHCP-server, of andere providergerelateerde servers. Afhankelijk van uw beveiligingsinstellingen, kan Firewall u waarschuwen wanneer er een gebeurtenis van een verboden computer wordt gedetecteerd.

In dit hoofdstuk

Computerverbindingen vertrouwen.....	112
Computerverbindingen verbieden	116

Computerverbindingen vertrouwen

In het deelvenster 'Vertrouwde en verboden IP-adressen' kunt u onder **Vertrouwde IP-adressen** vertrouwde IP-adressen toevoegen, bewerken en verwijderen.

Via de lijst **Vertrouwde IP-adressen** in het deelvenster 'Vertrouwde en verboden IP-adressen' kunt u alle verkeer van een specifieke computer toegang geven tot uw computer. Verkeer dat afkomstig is van IP-adressen uit de lijst **Vertrouwde IP-adressen**, wordt niet in het logboek geregistreerd. Ook worden voor deze adressen geen gebeurteniswaarschuwingen gegenereerd.

Alle geselecteerde IP-adressen in de lijst worden vertrouwd. Dat betekent dat verkeer vanaf een vertrouwd IP-adres via de firewall of via een van de poorten altijd wordt toegestaan. In Firewall worden activiteiten tussen uw computer en de computer met een vertrouwd IP-adres niet gefilterd of geanalyseerd. Standaard wordt bij de Vertrouwde IP-adressen het eerste privénetwerk vermeld dat Firewall vindt.

Als u een verbinding toestaat, controleer dan of de computer die u vertrouwt, veilig is. Als een computer die u vertrouwt, is geïnfecteerd met een worm of een ander mechanisme, kan uw computer vatbaar zijn voor virusinfecties. Bovendien raadt McAfee u aan om te controleren of de computer(s) die u vertrouwt, zelf ook zijn beveiligd door middel van een firewall en een antivirusprogramma dat up-to-date is.

Vertrouwde computerverbinding toevoegen

U kunt een vertrouwde computerverbinding en het bijbehorende IP-adres toevoegen.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Klik in het deelvenster 'Firewall' op **Vertrouwde en verboden IP-adressen**.
- 4 Selecteer **Vertrouwde IP-adressen** in het deelvenster Vertrouwde en verboden IP-adressen en klik vervolgens op **Toevoegen**.
- 5 Voer onder **Regel verboden IP-adres toevoegen** een van de volgende handelingen uit:
 - Selecteer **Enkelvoudig IP-adres** en voer vervolgens het IP-adres in.
 - Selecteer **IP-adresbereik** en voer vervolgens het eerste en laatste IP-adres in in de vakken **Eerste IP-adres** en **Laatste IP-adres**.

- 6 Indien een systeemservice gebruik maakt van de voorziening Internetverbinding delen (ICS), dan kunt u het volgende IP-adresbereik toevoegen: 192.168.0.1 tot 192.168.0.255.
- 7 Selecteer eventueel **Regel verloopt over** waarna u kunt invullen gedurende hoeveel dagen deze regel moet worden uitgevoerd.
- 8 Ook kunt u eventueel een beschrijving van de regel opgeven.
- 9 Klik op **OK**.
- 10 Klik in het dialoogvenster **Vertrouwde en verboden IP-adressen** op **Ja** om te bevestigen.

Opmerking: Zie Nieuwe systeemservice configureren voor meer informatie over de voorziening Internetverbinding delen (ICS).

Een vertrouwde computer toevoegen vanuit het logboek voor inkomende gebeurtenissen

U kunt een vertrouwde computerverbinding en het bijbehorende IP-adres toevoegen vanuit het logboek voor inkomende gebeurtenissen.

- 1 Klik in het deelvenster McAfee SecurityCenter onder het deelvenster Algemene taken op het menu **Geavanceerd**.
- 2 Klik op **Rapporten en logboeken**.
- 3 Klik onder **Recente gebeurtenissen** op **Logboek weergeven**.
- 4 Klik op **Internet en netwerk** en vervolgens op **Inkomende gebeurtenissen**.
- 5 Selecteer een bron-IP-adres en klik onder **Ik wil op Dit adres vertrouwen**.
- 6 Klik op **Ja** om te bevestigen.

Vertrouwde computerverbinding bewerken

U kunt een vertrouwde computerverbinding en het bijbehorende IP-adres bewerken.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Klik in het deelvenster 'Firewall' op **Vertrouwde en verboden IP-adressen**.
- 4 Selecteer **Vertrouwde IP-adressen** in het deelvenster 'Vertrouwde en verboden IP-adressen'.
- 5 Selecteer een IP-adres en klik vervolgens op **Bewerken**.
- 6 Voer onder **Vertrouwd IP-adres bewerken** een van de volgende handelingen uit:
 - Selecteer **Enkelvoudig IP-adres** en voer vervolgens het IP-adres in.
 - Selecteer **IP-adresbereik** en voer vervolgens het eerste en laatste IP-adres in in de vakken **Eerste IP-adres** en **Laatste IP-adres**.
- 7 Selecteer eventueel **Regel verloopt over**, waarna u kunt invullen gedurende hoeveel dagen deze regel moet worden uitgevoerd.
- 8 Ook kunt u eventueel een beschrijving van de regel opgeven.
- 9 Klik op **OK**.

Opmerking: U kunt de standaard computerverbinding(en) die Firewall automatisch heeft toegevoegd van een vertrouwd privé-netwerk niet bewerken.

Vertrouwde computerverbinding verwijderen

U kunt een vertrouwde computerverbinding en het bijbehorende IP-adres verwijderen.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Klik in het deelvenster 'Firewall' op **Vertrouwde en verboden IP-adressen**.
- 4 Selecteer **Vertrouwde IP-adressen** in het deelvenster 'Vertrouwde en verboden IP-adressen'.
- 5 Selecteer een IP-adres en klik vervolgens op **Verwijderen**.
- 6 Klik in het dialoogvenster **Vertrouwde en verboden IP-adressen** op **Ja** om te bevestigen.

Computerverbindingen verbieden

In het deelvenster 'Vertrouwde en verboden IP-adressen' kunt u onder **Verboden IP-adressen** verboden IP-adressen toevoegen, bewerken en verwijderen.

Computers waaraan een onbekend, verdacht of onvertrouwd IP-adres is gekoppeld, kunnen worden uitgesloten van verbinding met uw computer.

Aangezien Firewall al het ongewenste verkeer blokkeert, is het normaal gesproken niet nodig om een IP-adres te blokkeren. U moet een IP-adres alleen blokkeren wanneer u zeker weet dat een internetverbinding een specifieke bedreiging oplevert. Zorg ervoor dat u geen belangrijke IP-adressen blokkeert, zoals de DNS- of DHCP-server, of andere providergerelateerde servers. Afhankelijk van uw beveiligingsinstellingen, kan Firewall u waarschuwen wanneer er een gebeurtenis van een verboden computer wordt gedetecteerd.

Verboden computerverbinding toevoegen

U kunt een verboden computerverbinding en het bijbehorende IP-adres toevoegen.

Opmerking: Zorg ervoor dat u geen belangrijke IP-adressen blokkeert, zoals de DNS- of DHCP-server, of andere providergerelateerde servers.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Klik in het deelvenster 'Firewall' op **Vertrouwde en verboden IP-adressen**.
- 4 Selecteer **Verboden IP-adressen** in het deelvenster Vertrouwde en verbonden IP-adressen en klik vervolgens op **Toevoegen**.
- 5 Voer onder **Regel verboden IP-adres toevoegen** een van de volgende handelingen uit:
 - Selecteer **Enkelvoudig IP-adres** en voer vervolgens het IP-adres in.
 - Selecteer **IP-adresbereik** en voer vervolgens het eerste en laatste IP-adres in in de vakken **Eerste IP-adres** en **Laatste IP-adres**.

- 6 Selecteer eventueel **Regel verloopt over** waarna u kunt invullen gedurende hoeveel dagen deze regel moet worden uitgevoerd.
- 7 Ook kunt u eventueel een beschrijving van de regel opgeven.
- 8 Klik op **OK**.
- 9 Klik in het dialoogvenster **Vertrouwde en verboden IP-adressen** op **Ja** om te bevestigen.

Een verboden computerverbinding bewerken

U kunt een verboden computerverbinding en het bijbehorende IP-adres bewerken.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Klik in het deelvenster 'Firewall' op **Vertrouwde en verboden IP-adressen**.
- 4 Selecteer **Verboden IP-adressen** in het deelvenster Vertrouwde en verbonden IP-adressen en klik vervolgens op **Bewerken**.
- 5 Voer onder **Verboden IP-adres bewerken** een van de volgende handelingen uit:
 - Selecteer **Enkelvoudig IP-adres** en voer vervolgens het IP-adres in.
 - Selecteer **IP-adresbereik** en voer vervolgens het eerste en laatste IP-adres in in de vakken **Eerste IP-adres** en **Laatste IP-adres**.
- 6 Selecteer eventueel **Regel verloopt over** waarna u kunt invullen gedurende hoeveel dagen deze regel moet worden uitgevoerd.
- 7 Ook kunt u eventueel een beschrijving van de regel opgeven.
- 8 Klik op **OK**.

Een verbinding met een verboden computer verwijderen

U kunt een verboden computerverbinding en het bijbehorende IP-adres verwijderen.

- 1 Klik in het deelvenster McAfee SecurityCenter op **Internet en netwerk** en klik vervolgens op **Configuratie**.
- 2 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 3 Klik in het deelvenster 'Firewall' op **Vertrouwde en verboden IP-adressen**.
- 4 Selecteer **Verboden IP-adressen** in het deelvenster 'Vertrouwde en verboden IP-adressen'.
- 5 Selecteer een IP-adres en klik vervolgens op **Verwijderen**.
- 6 Klik in het dialoogvenster **Vertrouwde en verboden IP-adressen** op **Ja** om te bevestigen.

Een computer blokkeren vanuit het logboek voor inkomende gebeurtenissen

U kunt een vertrouwde computerverbinding en het bijbehorende IP-adres blokkeren vanuit het logboek voor inkomende gebeurtenissen.

IP-adressen die in het logboek voor inkomende gebeurtenissen worden weergegeven, zijn geblokkeerd. Het blokkeren van een adres resulteert dan ook niet in een verdergaande mate van bescherming, behalve als uw computer gebruikmaakt van poorten die opzettelijk zijn geopend of als er op uw computer een programma staat waaraan internettoegang is toegestaan.

Voeg alleen een IP-adres toe aan de lijst met **verboden IP-adressen** als een of meer poorten opzettelijk zijn geopend en als er aanleiding is om te voorkomen dat het adres toegang krijgt tot de geopende poorten.

De pagina Inkomende gebeurtenissen bevat u een lijst met al het inkomende internetverkeer, die u kunt gebruiken om een IP-adres te blokkeren dat u ervan verdenkt de bron te zijn van een verdachte of ongewenste internetactiviteit.

- 1 Klik in het deelvenster McAfee SecurityCenter onder **Algemene taken** op het menu **Geavanceerd**.
- 2 Klik op **Rapporten en logboeken**.
- 3 Klik onder **Recente gebeurtenissen** op **Logboek weergeven**.
- 4 Klik op **Internet en netwerk** en vervolgens op **Inkomende gebeurtenissen**.
- 5 Selecteer een bron-IP-adres en klik onder **Ik wil** op **Dit adres blokkeren**.
- 6 Klik in het dialoogvenster **Regel verboden IP-adres toevoegen** op **Ja** om te bevestigen.

Een computer blokkeren vanuit het logboek voor gebeurtenissen van het inbraakdetectiesysteem

U kunt een computerverbinding en het bijbehorende IP-adres blokkeren vanuit het logboek voor gebeurtenissen van het inbraakdetectiesysteem.

- 1 Klik in het deelvenster McAfee SecurityCenter onder **Algemene taken** op het menu **Geavanceerd**.
- 2 Klik op **Rapporten en logboeken**.
- 3 Klik onder **Recente gebeurtenissen** op **Logboek weergeven**.
- 4 Klik op **Internet en netwerk** en klik vervolgens op **Gebeurtenissen inbraakdetectie**.
- 5 Selecteer een bron-IP-adres en klik onder **Ik wil** op **Dit adres blokkeren**.
- 6 Klik in het dialoogvenster **Regel verboden IP-adres toevoegen** op **Ja** om te bevestigen.

HOOFDSTUK 21

Logbestanden, controles en analyses

Firewall voorziet in veelomvattende en gebruikersvriendelijke mogelijkheden voor logboekregistratie, controles en analyses voor internetverkeer en gebeurtenissen. Inzicht in internetverkeer en -gebeurtenissen stelt u in staat om uw internetverbindingen beter te beheren.

In dit hoofdstuk

Logboekregistratie	122
Werken met statistieken	125
Internetverkeer traceren.....	126
Internetverkeer controleren.....	130

Logboekregistratie

Met Firewall kunt u gebeurtenisregistratie inschakelen of uitschakelen. Als u logboekregistratie inschakelt, kunt u bovendien instellen welke typen gebeurtenissen u wilt registreren. Het vastleggen van gebeurtenissen in logboeken stelt u in staat om recente inkomende en uitgaande gebeurtenissen weer te geven.

De instellingen voor het gebeurtenislogboek configureren

Specificeer en configureer de typen Firewall-gebeurtenissen die worden geregistreerd. Standaard is gebeurtenisregistratie ingeschakeld voor alle gebeurtenissen en activiteiten.

- 1 Klik in het deelvenster & Netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
- 2 Klik op **Instellingen gebeurtenislogboek** in het deelvenster Firewall.
- 3 Selecteer **Logboekregistratie inschakelen** als dit niet al is ingeschakeld.
- 4 Selecteer of verwijder onder **Logboekregistratie inschakelen** de gebeurtenistypen die u wel of niet wilt registreren. Het betreft de volgende gebeurtenistypen:
 - Geblokkeerde programma's
 - ICMP-pings
 - Verkeer van verboden IP-adressen
 - Gebeurtenissen op systeemservicepoorten
 - Gebeurtenissen op onbekende poorten
 - Gebeurtenissen in het inbraakdetectiesysteem (IDS)
- 5 Selecteer **Gebeurtenissen op de volgende poort(en) niet vastleggen** en voer afzonderlijke poortnummers gescheiden door komma's of poortbereiken gescheiden door streepjes in. Bijvoorbeeld 137-139, 445, 400-5000.
- 6 Klik op **OK**.

Recente gebeurtenissen weergeven

Als het logbestand is ingeschakeld, kunt u recente gebeurtenissen weergeven. In het deelvenster Recente gebeurtenissen worden datums en beschrijvingen van recente gebeurtenissen weergegeven. Hier worden alleen activiteiten weergegeven van programma's waarvoor de toegang tot internet nadrukkelijk is geblokkeerd.

- Klik in het menu **Geavanceerd** onder het deelvenster Algemene taken op **Rapporten en logboeken** of op **Recente gebeurtenissen weergeven**. U kunt ook in het menu Basis onder het deelvenster Algemene taken op **Recente gebeurtenissen weergeven** klikken.

Inkomende gebeurtenissen weergeven

Als het logbestand is ingeschakeld, kunt u inkomende gebeurtenissen weergeven. Inkomende gebeurtenissen bevatten datum en tijd, bron-IP-adres, hostnaam, informatie en gebeurtenistype.

- 1 Schakel het menu 'Geavanceerd' in. Klik in het deelvenster Algemene taken op **Rapporten & logboeken**.
- 2 Klik onder **Recente gebeurtenissen** op **Logboek weergeven**.
- 3 Klik op **Internet en netwerk** en vervolgens op **Inkomende gebeurtenissen**.

Opmerking: U kunt IP-adressen die in het logboek voor inkomende gebeurtenissen zijn vastgelegd, vertrouwen, blokkeren en traceren.

Uitgaande gebeurtenissen weergeven

Als het logbestand is ingeschakeld, kunt u uitgaande gebeurtenissen weergeven. In het logbestand voor uitgaande gebeurtenissen wordt onder meer het volgende vastgelegd: de naam van het programma dat heeft geprobeerd om een uitgaande verbinding tot stand te brengen, de datum en het tijdstip waarop de gebeurtenis plaatsvond en de locatie van het desbetreffende programma op uw computer.

- 1 Klik in het deelvenster Algemene taken op **Rapporten & logboeken**.
- 2 Klik onder **Recente gebeurtenissen** op **Logboek weergeven**.
- 3 Klik op **Internet en netwerk** en vervolgens op **Uitgaande gebeurtenissen**.

Opmerking: U kunt aan een programma in het logboek voor uitgaande gebeurtenissen volledige toegang of alleen uitgaande toegang toestaan. Daarnaast beschikt u over de mogelijkheid om aanvullende informatie over het desbetreffende programma weer te geven.

Gebeurtenissen van het inbraakdetectiesysteem weergeven

Als het logbestand is ingeschakeld, kunt u inkomende inbraakgebeurtenissen weergeven. Voor gebeurtenissen van het inbraakdetectiesysteem worden de datum en de tijd en het bron-IP-adres en de hostnaam van de gebeurtenis weergegeven.

- 1 Klik in het deelvenster Algemene taken op **Rapporten & logboeken**.
- 2 Klik onder **Recente gebeurtenissen** op **Logboek weergeven**.
- 3 Klik op **Internet en netwerk** en klik vervolgens op **Gebeurtenissen inbraakdetectie**.

Opmerking: U kunt IP-adressen die in het logboek voor gebeurtenissen van het inbraakdetectiesysteem zijn vastgelegd, vertrouwen, blokkeren en traceren.

Werken met statistieken

Firewall voorziet u via de HackerWatch-beveiligingswebsite van McAfee van mondiale statistieken over aan gerelateerde beveiligingsgebeurtenissen en poortactiviteiten.

Mondiale statistieken over beveiligingsgebeurtenissen weergeven

HackerWatch houdt wereldwijde beveiligingsgebeurtenissen met betrekking tot internet bij. U kunt deze gegevens weergeven via SecurityCenter. De informatie die u kunt weergeven omvat lijsten met incidenten die in de afgelopen 24 uur, 7 dagen of 30 dagen aan HackerWatch zijn gerapporteerd.

- 1 Schakel het menu Geavanceerd in en klik vervolgens op **Gereedschappen**.
- 2 Klik op **HackerWatch** in het deelvenster Gereedschappen.
- 3 Bekijk de statistieken over veiligheidsgebeurtenissen onder Tracering van gebeurtenissen.

Mondiale internetpoortactiviteiten weergeven

HackerWatch houdt wereldwijde beveiligingsgebeurtenissen met betrekking tot internet bij. U kunt deze gegevens weergeven via SecurityCenter. De weergegeven informatie omvat de belangrijkste gebeurtenissen met poorten die in de afgelopen zeven dagen aan HackerWatch zijn gerapporteerd. Hierbij wordt er standaard informatie weergegeven over HTTP-, TCP- en UDP-poorten.

- 1 Schakel het menu Geavanceerd in en klik vervolgens op **Gereedschappen**.
- 2 Klik op **HackerWatch** in het deelvenster Gereedschappen.
- 3 De belangrijkste gebeurtenissen worden weergegeven onder **Recente poortactiviteit**.

Internetverkeer traceren

Firewall biedt een aantal opties voor het traceren van internetverkeer. Deze opties stellen u in staat om een netwerkcomputer geografisch te traceren, om domein- en netwerkinformatie op te vragen en om computers vanuit de logboeken voor inkomende gebeurtenissen en voor gebeurtenissen in het inbraakdetectiesysteem te traceren.

Een netwerkcomputer geografisch traceren

Als u aan de hand van de naam of het IP-adres van een computer die verbinding maakt of die verbinding probeert te maken met uw computer de geografische locatie van de desbetreffende computer wilt achterhalen, kunt u de visuele traceerfunctie gebruiken. U kunt de visuele traceerfunctie ook gebruiken om netwerk- en registratie-informatie weer te geven. Als u de visuele traceerfunctie uitvoert, wordt er een wereldkaart weergegeven waarop de meest waarschijnlijke route van de broncomputer naar uw computer wordt afgebeeld.

- 1 Schakel het menu Geavanceerd in en klik vervolgens op **Gereedschappen**.
- 2 Klik op **Visual Tracer** in het deelvenster Gereedschappen.
- 3 Typ het IP-adres van de computer en klik op **Dit adres traceren**.
- 4 Selecteer onder **Visual Tracer** de optie **Weergave kaart**.

Opmerking: Het is niet mogelijk om gebeurtenissen met herhalende, privé- of ongeldige IP-adressen te traceren.

Computerregistratie-informatie ophalen

U kunt via SecurityCenter met Visual Trace computerregistratie-informatie ophalen. Deze informatie omvat de domeinnaam, de naam en het adres van de geregistreerd en de contactgegevens.

- 1 Schakel het menu Geavanceerd in en klik vervolgens op **Gereedschappen**.
- 2 Klik op **Visual Tracer** in het deelvenster Gereedschappen.
- 3 Typ het IP-adres van de desbetreffende computer en klik vervolgens op **Dit adres traceren**.
- 4 Selecteer onder **Visual Tracer** de optie **Weergave geregistreerde**.

De netwerkinformatie van een computer ophalen

U kunt via SecurityCenter met Visual Trace netwerkregistratie-informatie ophalen. Deze netwerkinformatie omvat details over het netwerk waarin het domein zich bevindt.

- 1 Schakel het menu Geavanceerd in en klik vervolgens op **Gereedschappen**.
- 2 Klik op **Visual Tracer** in het deelvenster Gereedschappen.
- 3 Typ het IP-adres van de desbetreffende computer en klik vervolgens op **Dit adres traceren**.
- 4 Selecteer onder **Visual Tracer** de optie **Weergave netwerk**.

Een computer traceren vanuit het logboek voor inkomende gebeurtenissen

U kunt vanuit het deelvenster Inkomende gebeurtenissen een IP-adres traceren dat wordt weergegeven in het logboek voor inkomende gebeurtenissen.

- 1 Schakel het menu 'Geavanceerd' in. Klik in het deelvenster Algemene taken op **Rapporten & logboeken**.
- 2 Klik onder **Recente gebeurtenissen** op **Logboek weergeven**.
- 3 Klik op **Internet en netwerk** en vervolgens op **Inkomende gebeurtenissen**.
- 4 Selecteer in het deelvenster Inkomende gebeurtenissen een bron-IP-adres en klik vervolgens op **Dit adres traceren**.
- 5 Klik in het deelvenster Visual Tracer op een van de volgende opties:
 - **Weergave kaart:** Hiermee kunt u een computer met het geselecteerde IP-adres geografisch traceren.
 - **Weergave geregistreerde:** Hiermee kunt u informatie weergeven over het domein dat het geselecteerde IP-adres gebruikt.
 - **Weergave netwerk:** Hiermee kunt u informatie weergeven over het netwerk dat het geselecteerde IP-adres gebruikt.
- 6 Klik op **Gereed**.

Een computer traceren vanuit het logboek voor gebeurtenissen van het inbraakdetectiesysteem

U kunt vanuit het deelvenster Gebeurtenissen inbraakdetectie een IP-adres traceren dat wordt weergegeven in het logboek voor gebeurtenissen van het inbraakdetectiesysteem.

- 1 Klik in het deelvenster Algemene taken op **Rapporten & logboeken**.
- 2 Klik onder **Recente gebeurtenissen** op **Logboek weergeven**.
- 3 Klik op **Internet en netwerk** en klik vervolgens op **Gebeurtenissen inbraakdetectie**. Selecteer in het deelvenster Gebeurtenissen inbraakdetectie een bron-IP-adres en klik vervolgens op **Dit adres traceren**.
- 4 Klik in het deelvenster Visual Tracer op een van de volgende opties:
 - **Weergave kaart:** Hiermee kunt u een computer met het geselecteerde IP-adres geografisch traceren.
 - **Weergave geregistreerde:** Hiermee kunt u informatie weergeven over het domein dat het geselecteerde IP-adres gebruikt.
 - **Weergave netwerk:** Hiermee kunt u informatie weergeven over het netwerk dat het geselecteerde IP-adres gebruikt.
- 5 Klik op **Gereed**.

Een gecontroleerd IP-adres traceren

U kunt een gecontroleerd IP-adres traceren. Als u het IP-adres traceert, wordt er een wereldkaart weergegeven waarop de meest waarschijnlijke route van de gegevens van de broncomputer naar uw computer wordt afgebeeld. Daarnaast kunt u registratie- en netwerkinformatie over het desbetreffende IP-adres ophalen.

- 1 Schakel het menu Geavanceerd in en klik vervolgens op **Gereedschappen**.
- 2 Klik op **Verkeersmonitor** in het deelvenster Gereedschappen.
- 3 Klik onder **Verkeersmonitor** op **Actieve programma's**.
- 4 Selecteer een programma en klik vervolgens op het IP-adres dat onder de naam van het programma wordt weergegeven.
- 5 Klik onder **Activiteit van programma** op **Dit IP-adres traceren**.
- 6 Er wordt vervolgens onder **Visual Tracer** een wereldkaart weergegeven waarop de meest waarschijnlijke route van de gegevens van de broncomputer naar uw computer wordt afgebeeld. Daarnaast kunt u registratie- en netwerkinformatie over het desbetreffende IP-adres ophalen.

Opmerking: Als u de meest actuele statistieken wilt weergeven, klikt u onder **Visual Tracer** op **Vernieuwen**.

Internetverkeer controleren

Firewall voorziet in een aantal methoden voor het controleren van het internetverkeer, waaronder:

- **De grafiek Verkeersanalyse:** Hiermee geeft u het recente inkomende en uitgaande internetverkeer weer.
- **De grafiek Verkeersgebruik:** Hiermee geeft u het percentage van de bandbreedte weer dat in de afgelopen 24 uur door de meest actieve toepassingen op uw computer is gebruikt.
- **Actieve Programma's:** Hiermee geeft u de programma's op uw computer weer die momenteel de meeste netwerkverbindingen gebruiken en u geeft de IP-adressen weer die door deze programma's zijn benaderd.

Informatie over de grafiek Verkeersanalyse

De grafiek Verkeersanalyse geeft een numerieke en een grafische weergave weer van inkomend en uitgaand internetverkeer. Bovendien geeft de Verkeersmonitor programma's weer die de meeste netwerkverbindingen op uw computer gebruiken en de IP-adressen die de programma's openen.

U kunt vanuit het deelvenster Verkeersanalyse recent inkomend en uitgaand internetverkeer en huidige, gemiddelde en maximale overdrachtssnelheden weergeven. U kunt bovendien het verkeersvolume weergeven (inclusief het verkeersvolume sinds u Firewall hebt gestart) en u kunt de totale hoeveelheid verkeer voor de huidige maand en de vorige maand weergeven.

Het deelvenster Verkeersanalyse geeft de realtime internetactiviteit op uw computer weer, inclusief het volume en de snelheid van het recente inkomende en uitgaande internetverkeer op uw computer. Daarnaast worden tevens de verbindingssnelheid en het aantal bytes dat via internet is overgedragen, weergegeven.

De groene lijn vertegenwoordigt de huidige overdrachtssnelheid voor inkomend verkeer. De groene stippellijn vertegenwoordigt de gemiddelde overdrachtssnelheid voor inkomend verkeer. Als de huidige en de gemiddelde overdrachtssnelheid gelijk zijn, wordt de stippellijn niet in de grafiek weergegeven. De weergegeven lijn vertegenwoordigt in een dergelijk geval zowel de gemiddelde als de huidige overdrachtssnelheid.

De rode lijn vertegenwoordigt de huidige overdrachtssnelheid voor uitgaand verkeer. De rode stippellijn vertegenwoordigt de gemiddelde overdrachtssnelheid voor uitgaand verkeer. Als de huidige en de gemiddelde overdrachtssnelheid gelijk zijn, wordt de stippellijn niet in de grafiek weergegeven. De weergegeven lijn vertegenwoordigt in een dergelijk geval zowel de gemiddelde als de huidige overdrachtssnelheid.

Het inkomende en uitgaande verkeer analyseren

De grafiek Verkeersanalyse geeft een numerieke en een grafische weergave weer van inkomend en uitgaand internetverkeer. Bovendien geeft de Verkeersmonitor programma's weer die de meeste netwerkverbindingen op uw computer gebruiken en de IP-adressen die de programma's openen.

- 1 Schakel het menu Geavanceerd in en klik vervolgens op **Gereedschappen**.
- 2 Klik op **Verkeersmonitor** in het deelvenster Gereedschappen.
- 3 Klik onder **Verkeersmonitor** op **Verkeersanalyse**.

Tip: Als u de meest actuele statistieken wilt weergeven, klikt u onder **Verkeersanalyse** op **Vernieuwen**.

De bandbreedte van programma's controleren

U kunt een cirkeldiagram weergeven waarin bij benadering het percentage aan bandbreedte wordt getoond dat in de afgelopen 24 uur door de meest actieve programma's op uw computer is gebruikt. Een cirkeldiagram voorziet in een grafische weergave van de relatieve hoeveelheid bandbreedte die door de programma's is gebruikt.

- 1 Schakel het menu Geavanceerd in en klik vervolgens op **Gereedschappen**.
- 2 Klik op **Verkeersmonitor** in het deelvenster Gereedschappen.
- 3 Klik onder **Verkeersmonitor** op **Verkeersgebruik**.

Tip: Als u de meest actuele statistieken wilt weergeven, klikt u onder **Verkeersgebruik** op **Vernieuwen**.

Activiteiten van programma's controleren

U kunt inkomende en uitgaande activiteiten van programma's weergeven. Hierbij worden de verbindingen met externe computers en poorten weergegeven.

- 1 Schakel het menu Geavanceerd in en klik vervolgens op **Gereedschappen**.
- 2 Klik op **Verkeersmonitor** in het deelvenster Gereedschappen.
- 3 Klik onder **Verkeersmonitor** op **Actieve programma's**.
- 4 U kunt de volgende informatie weergeven:
 - Een grafiek van de activiteiten van een programma: Selecteer een programma als u een grafiek van de activiteiten van het programma wilt weergeven.

- Luisterende verbindingen: Selecteer een item onder de naam van het programma.
- Computerverbindingen: Selecteer een IP-adres onder de naam van het programma, het systeemproces of de service.

Opmerking: Als u de meest actuele statistieken wilt weergeven, klikt u onder **Actieve programma's** op **Vernieuwen**.

HOOFDSTUK 22

Informatie over internetbeveiliging

Firewall voorziet u via de HackerWatch-beveiligingswebsite van McAfee van actuele informatie over programma's en mondiale internetactiviteiten. HackerWatch biedt daarnaast een HTML-zelfstudie over Firewall.

In dit hoofdstuk

De HackerWatch-zelfstudie starten..... 134

De HackerWatch-zelfstudie starten

Als u meer wilt leren over Firewall, kunt u de HackerWatch-zelfstudie starten vanuit SecurityCenter.

- 1 Schakel het menu Geavanceerd in en klik vervolgens op **Gereedschappen**.
- 2 Klik op **HackerWatch** in het deelvenster Gereedschappen.
- 3 Klik onder **HackerWatch-bronnen** op **Zelfstudie weergeven**.

HOOFDSTUK 23

McAfee QuickClean

Met QuickClean kunt u de prestaties van uw computer verbeteren door bestanden te verwijderen die de computer traag en onoverzichtelijk maken. U kunt niet alleen de Prullenbak legen, maar ook tijdelijke internetbestanden, snelkoppelingen, verloren bestandsfragmenten, registerbestanden, bestanden in de cache, cookies, de browsergeschiedenis, verzonden en verwijderde e-mailberichten, recent geopende bestanden, ActiveX-bestanden en systeemherstelpunten verwijderen. Uw privacy wordt ook gewaarborgd omdat items met gevoelige of persoonlijke informatie, bijvoorbeeld uw naam en adres, veilig en permanent worden verwijderd door McAfee Shredder. Zie McAfee Shredder voor informatie over het vernietigen van bestanden.

Met Schijfdefragmentatie worden bestanden en mappen opnieuw op uw computer gerangschikt zodat deze niet gefragmenteerd raken. Door regelmatig de vaste schijf te defragmenteren, zorgt u ervoor dat deze gefragmenteerde bestanden worden samengevoegd, zodat u ze later sneller kunt openen.

Als u uw computer niet handmatig wilt onderhouden, kunt u QuickClean en Schijfdefragmentatie automatisch zo vaak als u wilt laten uitvoeren als onafhankelijke taken.

Opmerking: SecurityCenter stelt u op de hoogte van kritieke en niet-kritieke beveiligingsproblemen zodra deze worden vastgesteld. Als u hulp nodig hebt bij het analyseren van beveiligingsproblemen, kunt u McAfee Virtual Technician uitvoeren.

In dit hoofdstuk

Functies van QuickClean.....	136
De computer opschonen.....	137
De computer defragmenteren.....	141
Taken plannen.....	142

Functies van QuickClean

Met QuickClean beschikt u over verschillende opschoonprogramma's waarmee u onnodige bestanden veilig en efficiënt kunt verwijderen. Hierdoor maakt u ruimte vrij op de vaste schijf en wordt uw computer sneller.

De computer opschonen

Hiermee worden bestanden verwijderd die de computer traag en onoverzichtelijk maken. U kunt niet alleen de Prullenbak legen, maar ook tijdelijke internetbestanden, snelkoppelingen, verloren bestandsfragmenten, registerbestanden, bestanden in de cache, cookies, de browsergeschiedenis, verzonden en verwijderde e-mailberichten, recent geopende bestanden, ActiveX-bestanden en systeemherstelpunten verwijderen. Deze items worden verwijderd zonder andere essentiële informatie te beschadigen.

U kunt elk gewenst opschoonprogramma gebruiken om onnodige bestanden te verwijderen. In de onderstaande tabel staan de opschoonprogramma's van QuickClean:

Naam	Functie
Prullenbak opschonen	Hiermee worden de bestanden in de Prullenbak verwijderd.
Tijdelijke bestanden opschonen	Hiermee worden bestanden verwijderd die zijn opgeslagen in tijdelijke mappen.
Snelkoppelingen opschonen	Hiermee worden niet alleen verbroken snelkoppelingen verwijderd, maar ook snelkoppelingen waaraan geen programma is gekoppeld.
Verloren bestandsfragmenten opschonen	Hiermee worden verloren bestandsfragmenten van de computer verwijderd.
Register opschonen	Hiermee wordt Windows®-registerinformatie verwijderd voor programma's die niet meer aanwezig zijn op de computer. Het register is een database waarin configuratie-informatie voor Windows wordt opgeslagen. Het bevat profielen voor elke gebruiker van de computer en informatie over de hardware, geïnstalleerde programma's en allerlei instellingen. Wanneer Windows wordt uitgevoerd, wordt deze informatie voortdurend geraadpleegd.
Cache opschonen	Hiermee worden bestanden in het cachegeheugen verwijderd die worden verzameld wanneer u op internet surft. Deze bestanden worden gewoonlijk als tijdelijke bestanden in een cachemap opgeslagen. Een cachemap is een tijdelijke opslagruimte op de computer. Om sneller en efficiënter op internet te kunnen surfen, worden webpagina's die u al eerder hebt bezocht, uit de cache opgehaald, niet van een externe server.

Cookies opschonen	<p>Hiermee worden cookies verwijderd. Deze bestanden worden gewoonlijk opgeslagen als tijdelijke bestanden.</p> <p>Een cookie is een klein bestand met informatie over de persoon die op internet surft en bevat meestal een gebruikersnaam en de huidige datum en tijd. Cookies worden gewoonlijk door websites gebruikt om gebruikers te herkennen die zich eerder hebben aangemeld bij de site. Ze kunnen echter ook een bron van informatie zijn voor hackers.</p>
Browsergeschiedenis en opschonen	<p>Hiermee wordt uw browsergeschiedenis verwijderd.</p>
Opschonen van verwijderde en verzonden e-mail in Outlook Express en Outlook	<p>Hiermee worden verzonden en verwijderde e-mailberichten in Outlook® en Outlook Express verwijderd.</p>
Recent gebruikte items opschonen	<p>Hiermee worden recent geopende bestanden verwijderd die zijn gemaakt met een van de onderstaande programma's:</p> <ul style="list-style-type: none"> ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Windows History ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®
ActiveX opschonen	<p>Hiermee worden ActiveX-besturingselementen verwijderd.</p> <p>ActiveX is een programmaonderdeel dat in programma's of op webpagina's wordt gebruikt om extra functionaliteit toe te voegen en verschijnt als een normaal onderdeel van het programma of de webpagina. De meeste ActiveX-besturingselementen zijn onschuldig, maar sommige zijn ontworpen om informatie op uw computer te zoeken.</p>

Systeemherstelpunten opschonen	<p>Hiermee worden oude systeemherstelpunten (behalve het meest recente) van de computer verwijderd.</p> <p>Met systeemherstelpunten worden in Windows wijzigingen in het systeem gemarkeerd, zodat u bij problemen een eerdere, goed werkende configuratie kunt herstellen.</p>
--------------------------------	---

De computer opschonen

U kunt elk gewenst opschoonprogramma gebruiken om onnodige bestanden te verwijderen. Wanneer u klaar bent, wordt onder **Overzicht van QuickClean** de hoeveelheid vrijgemaakte schijfruimte, het aantal verwijderde bestanden en de datum en tijd van de vorige opschoonactie weergegeven.

- 1 Klik in het deelvenster McAfee SecurityCenter onder **Algemene taken** op **Computer onderhouden**.
- 2 Klik onder **McAfee QuickClean** op **Start**.
- 3 Voer een van de volgende handelingen uit:
 - Klik op **Volgende** om de standaardopschoonprogramma's in de lijst te accepteren.
 - Selecteer de gewenste opschoonprogramma's en klik op **Volgende**. Als u Recent gebruikte items opschonen selecteert, kunt u op **Eigenschappen** klikken om de bestanden te selecteren die u recent hebt gemaakt met de programma's in de lijst of om de selectie van bestanden ongedaan te maken. Klik vervolgens op **OK**.
 - Klik op **Standaardwaarden herstellen** als u de standaardopschoonprogramma's wilt herstellen en klik vervolgens op **Volgende**.
- 4 Nadat de analyse is voltooid, klikt u op **Volgende**.
- 5 Klik op **Volgende** om het verwijderen te bevestigen.
- 6 Voer een van de volgende handelingen uit:
 - Klik op **Volgende** om de standaardoptie **Nee, ik wil bestanden op de standaardmanier van Windows verwijderen** te accepteren.
 - Klik op **Ja, ik wil mijn bestanden veilig wissen met Shredder**, geef het aantal cyclussen op (maximaal 10) en klik vervolgens op **Volgende**. Bestanden vernietigen kan lang duren als er een grote hoeveelheid informatie moet worden gewist.

- 7 Als bestanden tijdens het opschonen geblokkeerd waren, wordt u misschien gevraagd de computer opnieuw te starten. Klik op **OK** om het venster te sluiten.
- 8 Klik op **Voltoeien**.

Opmerking: Bestanden die met Shredder worden verwijderd, kunnen niet meer worden hersteld. Zie McAfee Shredder voor informatie over het vernietigen van bestanden.

De computer defragmenteren

Met Schijfdefragmentatie worden bestanden en mappen opnieuw op uw computer gerangschikt zodat deze niet gefragmenteerd raken. Door regelmatig de vaste schijf te defragmenteren, zorgt u ervoor dat deze gefragmenteerde bestanden worden samengevoegd, zodat u ze later sneller kunt openen.

De computer defragmenteren

U kunt de computer defragmenteren om het openen en ophalen van bestanden en mappen te verbeteren.

- 1 Klik in het deelvenster McAfee SecurityCenter onder **Algemene taken** op **Computer onderhouden**.
- 2 Klik onder **Schijfdefragmentatie** op **Analyseren**.
- 3 Volg de instructies op het scherm.

Opmerking: zie de Help van Windows voor meer informatie over Schijfdefragmentatie.

Taken plannen

Met de taakplanner kunt u instellen hoe vaak QuickClean en Schijfdefragmentatie op de computer moeten worden uitgevoerd. U kunt bijvoorbeeld instellen dat elke zondag om 9:00 de Prullenbak door QuickClean wordt geleegd en dat elke laatste dag van de maand de vaste schijf van de computer wordt gedefragmenteerd. U kunt taken op elk gewenst moment maken, wijzigen of verwijderen. Geplande taken kunnen alleen worden uitgevoerd als u bent aangemeld bij de computer. Als een taak om welke reden dan ook niet wordt uitgevoerd, wordt deze vijf minuten nadat u zich weer hebt aangemeld, opnieuw uitgevoerd.

QuickClean-taken plannen

U kunt een QuickClean-taak plannen om de computer automatisch te laten opschonen met een of meer opschoonprogramma's. Wanneer de taak is voltooid, wordt onder **Overzicht van QuickClean** de datum en tijd weergegeven wanneer de taak weer wordt uitgevoerd.

1 Open het deelvenster Taakplanner.

Hoe?

1. Klik in het deelvenster McAfee SecurityCenter onder **Algemene taken** op **Computer onderhouden**.
2. Klik onder **Taakplanner** op **Start**.

2 Klik in de lijst **Selecteer de bewerking die u wilt plannen** op **McAfee QuickClean**.

3 Typ een naam voor de taak in het vak **Taaknaam** en klik op **Maken**.

4 Voer een van de volgende handelingen uit:

- Klik op **Volgende** om de opschoonprogramma's in de lijst te accepteren.
- Selecteer de gewenste opschoonprogramma's of maak de selectie ervan ongedaan en klik op **Volgende**. Als u Recent gebruikte items opschonen selecteert, kunt u op **Eigenschappen** klikken om de bestanden te selecteren die u recent hebt gemaakt met de programma's in de lijst of om de selectie van bestanden ongedaan te maken. Klik vervolgens op **OK**.
- Klik op **Standaardwaarden herstellen** als u de standaardopschoonprogramma's wilt herstellen en klik vervolgens op **Volgende**.

5 Voer een van de volgende handelingen uit:

- Klik op **Plannen** om de standaardoptie **Nee, ik wil bestanden op de standaardmanier van Windows verwijderen** te accepteren.

- Klik op **Ja, ik wil mijn bestanden veilig wissen met Shredder**, geef het aantal cyclussen op (maximaal 10) en klik vervolgens op **Plannen**.
- 6 Selecteer in het dialoogvenster **Plannen** hoe vaak de taak moet worden uitgevoerd en klik op **OK**.
 - 7 Als u wijzigingen hebt aangebracht in de eigenschappen van Recent gebruikte items opschonen, wordt u misschien gevraagd de computer opnieuw op te starten. Klik op **OK** om het venster te sluiten.
 - 8 Klik op **Voltooien**.

Opmerking: Bestanden die met Shredder worden verwijderd, kunnen niet meer worden hersteld. Zie McAfee Shredder voor informatie over het vernietigen van bestanden.

QuickClean-taken wijzigen

U kunt voor geplande QuickClean-taken andere opschoonprogramma's instellen of de taken met een andere frequentie op de computer laten uitvoeren. Wanneer de taak is voltooid, wordt onder **Overzicht van QuickClean** de datum en tijd weergegeven wanneer de taak weer wordt uitgevoerd.

- 1 Open het deelvenster Taakplanner.

Hoe?

 1. Klik in het deelvenster McAfee SecurityCenter onder **Algemene taken** op **Computer onderhouden**.
 2. Klik onder **Taakplanner** op **Start**.
- 2 Klik in de lijst **Selecteer de bewerking die u wilt plannen** op **McAfee QuickClean**.
- 3 Selecteer de taak in de lijst **Selecteer een bestaande taak** en klik op **Wijzigen**.
- 4 Voer een van de volgende handelingen uit:
 - Klik op **Volgende** om de opschoonprogramma's te accepteren die voor de taak zijn geselecteerd.
 - Selecteer de gewenste opschoonprogramma's of maak de selectie ervan ongedaan en klik op **Volgende**. Als u Recent gebruikte items opschonen selecteert, kunt u op **Eigenschappen** klikken om de bestanden te selecteren die u recent hebt gemaakt met de programma's in de lijst of om de selectie van bestanden ongedaan te maken. Klik vervolgens op **OK**.
 - Klik op **Standaardwaarden herstellen** als u de standaardopschoonprogramma's wilt herstellen en klik vervolgens op **Volgende**.

- 5 Voer een van de volgende handelingen uit:
 - Klik op **Plannen** om de standaardoptie **Nee, ik wil bestanden op de standaardmanier van Windows verwijderen** te accepteren.
 - Klik op **Ja, ik wil mijn bestanden veilig wissen met Shredder**, geef het aantal cyclussen op (maximaal 10) en klik vervolgens op **Plannen**.
- 6 Selecteer in het dialoogvenster **Plannen** hoe vaak de taak moet worden uitgevoerd en klik op **OK**.
- 7 Als u wijzigingen hebt aangebracht in de eigenschappen van Recent gebruikte items opschonen, wordt u misschien gevraagd de computer opnieuw op te starten. Klik op **OK** om het venster te sluiten.
- 8 Klik op **Voltooien**.

Opmerking: bestanden die met Shredder worden verwijderd, kunnen niet meer worden hersteld. Zie McAfee Shredder voor informatie over het vernietigen van bestanden.

QuickClean-taken verwijderen

U kunt geplande QuickClean-taken verwijderen als u deze niet meer automatisch wilt laten uitvoeren.

- 1 Open het deelvenster Taakplanner.
Hoe?
 1. Klik in het deelvenster McAfee SecurityCenter onder **Algemene taken** op **Computer onderhouden**.
 2. Klik onder **Taakplanner** op **Start**.
- 2 Klik in de lijst **Selecteer de bewerking die u wilt plannen** op **McAfee QuickClean**.
- 3 Selecteer de taak in de lijst **Selecteer een bestaande taak**.
- 4 Klik op **Verwijderen** en klik vervolgens op **Ja** om het verwijderen te bevestigen.
- 5 Klik op **Voltooien**.

Schijfdefragmentatie-taken plannen

U kunt Schijfdefragmentatie-taken plannen om de frequentie in te stellen waarmee de vaste schijf van de computer automatisch wordt gedefragmenteerd. Wanneer de taak is voltooid, wordt onder **Schijfdefragmentatie** de datum en tijd weergegeven wanneer de taak weer wordt uitgevoerd.

- 1 Open het deelvenster Taakplanner.
Hoe?

1. Klik in het deelvenster McAfee SecurityCenter onder **Algemene taken** op **Computer onderhouden**.
2. Klik onder **Taakplanner** op **Start**.
- 2 Klik in de lijst **Selecteer de bewerking die u wilt plannen** op **Schijfdefragmentatie**.
- 3 Typ een naam voor de taak in het vak **Taaknaam** en klik op **Maken**.
- 4 Voer een van de volgende handelingen uit:
 - Klik op **Plannen** om de standaardinstelling **Defragmentatie uitvoeren, zelfs bij weinig schijfruimte** te accepteren.
 - Schakel de optie **Defragmentatie uitvoeren, zelfs bij weinig schijfruimte** uit en klik op **Plannen**.
- 5 Selecteer in het dialoogvenster **Plannen** hoe vaak de taak moet worden uitgevoerd en klik op **OK**.
- 6 Klik op **Voltoeien**.

Schijfdefragmentatie-taken wijzigen

U kunt voor geplande Schijfdefragmentatie-taken de frequentie wijzigen waarmee de taken op de computer worden uitgevoerd. Wanneer de taak is voltooid, wordt onder **Schijfdefragmentatie** de datum en tijd weergegeven wanneer de taak weer wordt uitgevoerd.

- 1 Open het deelvenster Taakplanner.

Hoe?

 1. Klik in het deelvenster McAfee SecurityCenter onder **Algemene taken** op **Computer onderhouden**.
 2. Klik onder **Taakplanner** op **Start**.
- 2 Klik in de lijst **Selecteer de bewerking die u wilt plannen** op **Schijfdefragmentatie**.
- 3 Selecteer de taak in de lijst **Selecteer een bestaande taak** en klik op **Wijzigen**.
- 4 Voer een van de volgende handelingen uit:
 - Klik op **Plannen** om de standaardinstelling **Defragmentatie uitvoeren, zelfs bij weinig schijfruimte** te accepteren.
 - Schakel de optie **Defragmentatie uitvoeren, zelfs bij weinig schijfruimte** uit en klik op **Plannen**.
- 5 Selecteer in het dialoogvenster **Plannen** hoe vaak de taak moet worden uitgevoerd en klik op **OK**.
- 6 Klik op **Voltoeien**.

Schijfdefragmentatie-taken verwijderen

U kunt geplande Schijfdefragmentatie-taken verwijderen als u deze niet meer automatisch wilt laten uitvoeren.

- 1 Open het deelvenster Taakplanner.
Hoe?
 1. Klik in het deelvenster McAfee SecurityCenter onder **Algemene taken** op **Computer onderhouden**.
 2. Klik onder **Taakplanner** op **Start**.
- 2 Klik in de lijst **Selecteer de bewerking die u wilt plannen** op **Schijfdefragmentatie**.
- 3 Selecteer de taak in de lijst **Selecteer een bestaande taak**.
- 4 Klik op **Verwijderen** en klik vervolgens op **Ja** om het verwijderen te bevestigen.
- 5 Klik op **Voltooien**.

HOOFDSTUK 24

McAfee Shredder

Met McAfee Shredder worden items permanent van de vaste schijf van uw computer verwijderd (vernietigd). Zelfs als u handmatig bestanden en mappen verwijdert, de Prullenbak leegmaakt of de map met tijdelijke internetbestanden verwijdert, is het nog steeds mogelijk deze informatie te herstellen met speciale opsporingsprogramma's. Verwijderde bestanden kunnen daarnaast ook worden hersteld doordat in sommige toepassingen tijdelijke, verborgen kopieën van geopende bestanden worden gemaakt. Met Shredder verwijdert u ongewenste bestanden veilig en definitief, waardoor uw privacy wordt gewaarborgd. U moet wel bedenken dat vernietigde bestanden niet kunnen worden hersteld.

Opmerking: SecurityCenter stelt u op de hoogte van kritieke en niet-kritieke beveiligingsproblemen zodra deze worden vastgesteld. Als u hulp nodig hebt bij het analyseren van beveiligingsproblemen, kunt u McAfee Virtual Technician uitvoeren.

In dit hoofdstuk

Functies van Shredder	148
Bestanden, mappen en schijven vernietigen	149

Functies van Shredder

Met Shredder verwijdert u items definitief van de vaste schijf van uw computer, zodat de informatie in deze items niet kan worden hersteld. Uw privacy wordt gewaarborgd doordat bestanden en mappen, items in de Prullenbak en de map met tijdelijke internetbestanden veilig en definitief worden verwijderd. Dit geldt ook als u de gehele inhoud van vaste of verwisselbare schijven verwijdert, zoals herschrijfbare cd's, externe vaste schijven en diskettes.

Bestanden, mappen en schijven vernietigen

Met Shredder kunt u er zeker van zijn dat de informatie in verwijderde bestanden en mappen in de Prullenbak en in de map met tijdelijke internetbestanden niet kan worden hersteld, zelfs niet met speciale programma's. U kunt in Shredder opgeven hoe vaak items moeten worden vernietigd (maximaal 10 keer). Door een groter aantal vernietigingscyclussen op te geven, wordt het niveau van veilige bestandsverwijdering verhoogd.

Bestanden en mappen vernietigen

U kunt bestanden en mappen op de vaste schijf van uw computer vernietigen, ook items in de Prullenbak en in de map met tijdelijke internetbestanden.

1 Open **Shredder**.

Hoe?

1. Klik in het deelvenster McAfee SecurityCenter onder **Algemene taken** op het menu **Geavanceerd**.
2. Klik in het linkerdeelvenster op **Extra**.
3. Klik op **Shredder**.

2 Klik in het deelvenster Bestanden en mappen vernietigen onder **Ik wil** op **Bestanden en mappen wissen**.

3 Klik onder **Vernietigingsniveau** op een van de volgende opties:

- **Snel:** hiermee worden de geselecteerde items eenmaal vernietigd.
- **Grondig:** hiermee worden de geselecteerde items 7 keer vernietigd.
- **Aangepast:** hiermee worden de geselecteerde items maximaal 10 keer vernietigd.

4 Klik op **Volgende**.

5 Voer een van de volgende handelingen uit:

- Klik in de lijst **Selecteer te vernietigen bestand(en)** op **Prullenbak-inhoud** of op **Tijdelijke internetbestanden**.
- Klik op **Bladeren**, ga naar het bestand dat u wilt vernietigen, selecteer het en klik op **Openen**.

- 6 Klik op **Volgende**.
- 7 Klik op **Start**.
- 8 Klik op **Klaar** wanneer het proces is voltooid.

Opmerking: doe niets met bestanden totdat deze taak is voltooid.

Volledige schijfinhoud vernietigen

U kunt de volledige inhoud van een schijf vernietigen. U kunt alleen verwisselbare schijven, zoals externe vaste schijven, herschrijfbaar cd's en diskettes vernietigen.

- 1 Open **Shredder**.
Hoe?
 1. Klik in het deelvenster McAfee SecurityCenter onder **Algemene taken** op het menu **Geavanceerd**.
 2. Klik in het linkerdeelvenster op **Extra**.
 3. Klik op **Shredder**.
- 2 Klik in het deelvenster Bestanden en mappen vernietigen onder **Ik wil** op **Volledige schijf wissen**.
- 3 Klik onder **Vernietigingsniveau** op een van de volgende opties:
 - **Snel:** hiermee wordt de geselecteerde schijf eenmaal vernietigd.
 - **Grondig:** hiermee wordt de geselecteerde schijf 7 keer vernietigd.
 - **Aangepast:** hiermee wordt de geselecteerde schijf maximaal 10 keer vernietigd.
- 4 Klik op **Volgende**.
- 5 Klik in de lijst **Selecteer de schijf** op de schijf die u wilt vernietigen.
- 6 Klik op **Volgende** en klik vervolgens ter bevestiging op **Yes**.
- 7 Klik op **Start**.
- 8 Klik op **Klaar** wanneer het proces is voltooid.

Opmerking: doe niets met bestanden totdat deze taak is voltooid.

HOOFDSTUK 25

McAfee Network Manager

McAfee Network Manager biedt een grafische weergave van de computers en onderdelen in uw thuisnetwerk. Met Network Manager kunt u de beveiligingsstatus van elke beheerde computer in het netwerk op afstand controleren en gerapporteerde beveiligingsproblemen van deze computers op afstand oplossen.

Voordat u Network Manager gebruikt, kunt u kennismaken met enkele functies. Meer informatie over de configuratie en het gebruik van deze functies vindt u in de Help bij Network Manager.

Opmerking: SecurityCenter stelt u op de hoogte van kritieke en niet-kritieke beveiligingsproblemen zodra deze worden vastgesteld. Als u hulp nodig hebt bij het analyseren van beveiligingsproblemen, kunt u McAfee Virtual Technician uitvoeren.

In dit hoofdstuk

Functies van Network Manager	152
Informatie over pictogrammen van Network Manager	153
Een beheerd netwerk instellen.....	155
Het netwerk op afstand beheren.....	163

Functies van Network Manager

Network Manager biedt de volgende functies.

Grafisch netwerkoverzicht

Het netwerkoverzicht van Network Manager biedt een grafisch overzicht van de beveiligingsstatus van de computers en onderdelen waaruit uw thuisnetwerk bestaat. Wanneer u wijzigingen aanbrengt in uw netwerk (als u bijvoorbeeld een computer toevoegt), herkent het netwerkoverzicht deze wijzigingen. U kunt het netwerkoverzicht vernieuwen, de naam van het netwerk wijzigen of uw weergave wijzigen door componenten van het netwerkoverzicht weer te geven of te verbergen. U kunt ook de details bekijken van elk onderdeel dat in het netwerkoverzicht wordt weergegeven.

Extern beheer

Gebruik het netwerkoverzicht van Network Manager om de beveiligingsstatus te beheren van de computers waaruit uw thuisnetwerk bestaat. U kunt een computer uitnodigen om lid te worden van het beheerde netwerk, de beveiligingsstatus van de beheerde computer controleren, en bekende zwakke punten in de beveiliging repareren vanaf een externe computer in het netwerk.

Informatie over pictogrammen van Network Manager

In de volgende tabel worden de pictogrammen beschreven die worden gebruikt in het netwerkoverzicht van Network Manager.

Pictogram	Beschrijving
	Een online, beheerde computer
	Een offline, beheerde computer
	Een niet-beheerde computer waarop SecurityCenter is geïnstalleerd
	Een offline, niet-beheerde computer
	Een online computer waarop SecurityCenter niet is geïnstalleerd of een onbekend netwerkapparaat
	Een offline computer waarop SecurityCenter niet is geïnstalleerd of een offline, onbekend netwerkapparaat
	Het bijbehorende item is beveiligd en aangesloten
	Het bijbehorende item vereist mogelijk uw aandacht
	Het bijbehorende item vereist uw onmiddellijke aandacht
	Een draadloze thuisrouter
	Een standaardthuisrouter
	Het internet, als u verbinding hebt
	Het internet, als u geen verbinding hebt

HOOFDSTUK 26

Een beheerd netwerk instellen

Als u een beheerd netwerk wilt instellen, werkt u met de items in het netwerkoverzicht en voegt u leden (computers) aan het netwerk toe. U kunt een computer alleen op afstand beheren of deze machtigen om andere computers in het netwerk op afstand te beheren als deze computer een vertrouwd lid van het netwerk is. Lidmaatschap van het netwerk wordt aan nieuwe computers verleend door bestaande netwerkleden (computers) met beheerdersrechten.

U kunt gedetailleerde informatie weergeven over elk onderdeel van het netwerkoverzicht, zelfs nadat u wijzigingen hebt aangebracht in het netwerk (als u bijvoorbeeld een computer hebt toegevoegd).

In dit hoofdstuk

Werken met het netwerkoverzicht	156
Lid worden van het beheerde netwerk	158

Werken met het netwerkoverzicht

Als u een computer op het netwerk aansluit, wordt het netwerk geanalyseerd met Network Manager om te bepalen of er beheerde of niet-beheerde leden zijn en wat de routerkenmerken en de internetstatus zijn. Als er geen leden worden gevonden, wordt aangenomen dat de momenteel aangesloten computer de eerste computer in het netwerk is en wordt de computer een beheerd lid met beheerdersrechten. De naam van het netwerk bestaat standaard uit de werkgroep- of domeinnaam van de eerste computer met SecurityCenter die op het netwerk wordt aangesloten. U kunt de naam van het netwerk echter op elk moment wijzigen.

Als u wijzigingen in het netwerk aanbrengt (als u bijvoorbeeld een computer toevoegt), kunt u het netwerkoverzicht aanpassen. Zo kunt u het netwerkoverzicht vernieuwen, de naam van het netwerk wijzigen, en onderdelen van het netwerkoverzicht weergeven of verbergen om de weergave aan te passen. U kunt ook de details bekijken van elk onderdeel dat in het netwerkoverzicht wordt weergegeven.

Het netwerkoverzicht openen

Het netwerkoverzicht biedt een grafische weergave van de computers en onderdelen in uw thuisnetwerk.

- Klik in het menu Basis of Geavanceerd op **Netwerk beheren**.

Opmerking: de eerste keer dat u het netwerkoverzicht opent, wordt u gevraagd de andere computers in het netwerk te vertrouwen.

Het netwerkoverzicht vernieuwen

U kunt het netwerkoverzicht altijd vernieuwen, bijvoorbeeld nadat u een andere computer aan het beheerde netwerk hebt toegevoegd.

- 1 Klik in het menu Basis of Geavanceerd op **Netwerk beheren**.
- 2 Klik op **Het netwerkoverzicht vernieuwen** onder **Ik wil**.

Opmerking: de koppeling **Het netwerkoverzicht vernieuwen** is alleen beschikbaar als u geen items hebt geselecteerd in het netwerkoverzicht. Als u een item wilt wissen, klikt u op het geselecteerde item of op een leeg gedeelte in het netwerkoverzicht.

De naam van het netwerk wijzigen

De naam van het netwerk bestaat standaard uit de werkgroep- of domeinnaam van de eerste computer die op het netwerk wordt aangesloten en waarop SecurityCenter is geïnstalleerd. Als u liever een andere naam gebruikt, kunt u de naam wijzigen

- 1 Klik in het menu Basis of Geavanceerd op **Netwerk beheren**.
- 2 Klik op **De naam van het netwerk wijzigen** onder **Ik wil**.
- 3 Typ de gewenste naam van het netwerk in het vak **Netwerknnaam**.
- 4 Klik op **OK**.

Opmerking: de koppeling **De naam van het netwerk wijzigen** is alleen beschikbaar als u geen items hebt geselecteerd in het netwerkoverzicht. Als u een item wilt wissen, klikt u op het geselecteerde item of op een leeg gedeelte in het netwerkoverzicht.

Een item in het netwerkoverzicht weergeven of verbergen

Standaard worden alle computers en onderdelen in uw thuisnetwerk weergegeven in het netwerkoverzicht. Als u items hebt verborgen, kunt u deze op elk moment opnieuw weergeven. U kunt alleen niet-beheerde items verbergen. Beheerde computers worden altijd weergegeven.

Om...	Klikt u in het menu Basis of Geavanceerd op Netwerk beheren en voert u een van de volgende handelingen uit...
Een item in het netwerkoverzicht te verbergen	Klik op een item in het netwerkoverzicht en vervolgens op Dit item verbergen onder Ik wil . Klik op Ja in het bevestigingsdialoogvenster.
Verborgen items in het netwerkoverzicht weer te geven	Klik op Verborgen items weergegeven onder Ik wil .

Gedetailleerde informatie over een item weer te geven

U kunt gedetailleerde informatie over elk onderdeel in uw netwerk bekijken door het onderdeel in het netwerkoverzicht te selecteren. Deze informatie bestaat uit de naam van het onderdeel, de beveiligingsstatus en andere gegevens die nodig zijn om het onderdeel te beheren.

- 1 Klik op het pictogram van een item in het netwerkoverzicht.
- 2 Bekijk de informatie over het item onder **Details**.

Lid worden van het beheerde netwerk

U kunt een computer alleen op afstand beheren of machtigen om andere computers in het netwerk op afstand te beheren als deze computer een vertrouwd lid van het netwerk is. Lidmaatschap van het netwerk wordt aan nieuwe computers verleend door bestaande netwerkleden (computers) met beheerdersrechten. Gebruikers van de verlenende computer en de computer die wordt toegevoegd, moeten elkaar verifiëren om ervoor te zorgen dat alleen vertrouwde computers lid van het netwerk worden.

Als een computer aan het netwerk wordt toegevoegd, wordt de computer gevraagd de McAfee-beveiligingsstatus zichtbaar te maken voor andere computers in het netwerk. Zodra een computer de beveiligingsstatus beschikbaar maakt, wordt de computer een beheerd lid van het netwerk. Als een computer de beveiligingsstatus niet beschikbaar maakt, wordt de computer een niet-beheerd lid van het netwerk. Niet-beheerde leden van het netwerk zijn doorgaans gastcomputers die willen gebruikmaken van andere netwerkvoorzieningen (bijvoorbeeld het verzenden van bestanden of delen van printers).

Opmerking: zodra een computer met andere netwerkprogramma's van McAfee (zoals EasyNetwork) aan het netwerk is toegevoegd, wordt de computer eveneens herkend als beheerde computer in deze programma's. Het machtigingsniveau dat aan een computer wordt toegewezen in Network Manager, wordt toegepast op alle McAfee-netwerkprogramma's. Raadpleeg de documentatie bij een programma voor meer informatie over de betekenis van gast-, beheer- en volledige machtigingen in het betreffende programma.

Lid worden van een beheerd netwerk

Als u een uitnodiging krijgt om lid te worden van een beheerd netwerk, kunt u deze accepteren of weigeren. U kunt ook aangeven of u wilt dat deze computer en andere computers in het netwerk elkaars beveiligingsinstellingen controleren (bijvoorbeeld nagaan of de virusbeveiligingsservices van een computer up-to-date zijn).

- 1 Controleer of het selectievakje **Elke computer in dit netwerk toestaan om beveiligingsinstellingen te controleren** in het dialoogvenster Beheerd netwerk is ingeschakeld.
- 2 Klik op **Aanmelden**.
Als u de uitnodiging accepteert, worden twee speelkaarten weergegeven.
- 3 Bevestig dat de speelkaarten overeenkomen met de speelkaarten op de computer die de uitnodiging heeft verstuurd om lid te worden van het beheerde netwerk.
- 4 Klik op **OK**.

Opmerking: als op de computer die u heeft uitgenodigd lid te worden van het beheerde netwerk niet dezelfde speelkaarten worden weergegeven als in het bevestigingsdialoogvenster, is er sprake van een lek in de beveiliging van het beheerde netwerk. Als u lid wordt van het netwerk, kunt u uw computer in gevaar brengen. Klik daarom op **Annuleren** in het dialoogvenster Beheerd netwerk.

Een computer uitnodigen om lid te worden van het beheerde netwerk

Als een computer wordt toegevoegd aan het beheerde netwerk of als het netwerk een andere, niet-beheerde computer bevat, kunt u deze computer uitnodigen om lid te worden van het beheerde netwerk. Alleen computers met beheerdersrechten voor het netwerk kunnen andere computers uitnodigen om lid te worden. In de uitnodiging kunt u tevens aangeven welk machtigingsniveau u wilt toewijzen aan de computer die wordt toegevoegd.

- 1 Klik op het pictogram van een niet-beheerde computer in het netwerkoverzicht.
- 2 Klik op **Deze computer controleren** onder **Ik wil**.
- 3 Voer in het dialoogvenster Een computer uitnodigen om lid te worden van dit beheerde netwerk het volgende uit:
 - Klik op **Gasttoegang verlenen aan programma's in een beheerd netwerk** om de computer toegang te verlenen tot het netwerk (u kunt deze optie gebruiken voor tijdelijke gebruikers bij u thuis).

- Klik op **Volledige toegang verlenen aan programma's in een beheerd netwerk** om de computer toegang te verlenen tot het netwerk.
 - Klik op **Beheerderstoegang verlenen aan programma's in een beheerd netwerk** om de computer toegang te verlenen tot het netwerk met beheerdersrechten. De computer kan dan tevens toegang verlenen aan andere computers die lid van het beheerde netwerk willen worden.
- 4** Klik op **OK**.
Een uitnodiging om lid te worden van het beheerde netwerk wordt naar de computer verzonden. Zodra de computer de uitnodiging accepteert, worden twee speelkaarten weergegeven.
- 5** Bevestig dat de speelkaarten overeenkomen met de speelkaarten op de computer die u hebt uitgenodigd om lid te worden van het beheerde netwerk.
- 6** Klik op **Toegang verlenen**.

Opmerking: als op de computer die u hebt uitgenodigd lid te worden van het beheerde netwerk niet dezelfde speelkaarten worden weergegeven als in het bevestigingsdialoogvenster, is er sprake van een lek in de beveiliging van het beheerde netwerk. Als u de computer toestaat om lid te worden van het netwerk, kunt u andere computers in gevaar brengen. Klik daarom op **Toegang weigeren** in het bevestigingsdialoogvenster.

Computers op het netwerk niet meer vertrouwen

Als u computers op het netwerk per abuis hebt vertrouwd, kunt u het vertrouwen opheffen.

- Klik op **Computers op dit netwerk niet meer vertrouwen** onder **Ik wil**.

Opmerking: de koppeling **Computers op dit netwerk niet meer vertrouwen** is alleen beschikbaar als u over beheerdersrechten beschikt en andere beheerde computers lid zijn van het netwerk.

HOOFDSTUK 27

Het netwerk op afstand beheren

Nadat u het beheerde netwerk hebt ingesteld, kunt u de computers en onderdelen van het netwerk op afstand beheren. Zo kunt u de status en machtigingsniveaus van de computers en onderdelen op afstand controleren en de meeste beveiligingsproblemen op afstand oplossen.

In dit hoofdstuk

Status en machtigingen controleren	164
Beveiligingsproblemen oplossen	167

Status en machtigingen controleren

Een beheerd netwerk heeft beheerde en niet-beheerde leden. Beheerde leden staan andere computers in het netwerk toe hun McAfee-beveiligingsstatus te controleren. Niet-beheerde leden staan dit niet toe. Niet-beheerde leden zijn doorgaans gastcomputers die willen gebruikmaken van andere netwerkvoorzieningen (bijvoorbeeld het verzenden van bestanden of het delen van printers). Een beheerde computer in het netwerk kan een niet-beheerde computer op elk willekeurig moment uitnodigen om een beheerd lid te worden. Evenzo kan een beheerde computer niet-beheerd worden gemaakt.

Beheerde computers hebben beheer-, gast- of volledige machtiging voor het netwerk. Met een beheerdersmachtiging kan de beheerde computer de beveiligingsstatus van alle andere beheerde computers in het netwerk beheren en andere computers lid van het netwerk maken. Met een gast- of volledige machtiging heeft een computer alleen toegang tot het netwerk. U kunt het machtigingsniveau van een computer op elk moment wijzigen.

Omdat een beheerd netwerk ook apparaten kan bevatten (zoals routers), kunt u deze eveneens met Network Manager beheren. Tevens kunt u de weergave-eigenschappen van een apparaat in het netwerkoverzicht configureren en wijzigen.

De beveiligingsstatus van een computer controleren

Als de beveiligingsstatus van een computer niet wordt gecontroleerd in het netwerk (de computer is geen lid of een onbeheerd lid), kunt u een verzoek indienen om de computer te controleren.

- 1 Klik op het pictogram van een niet-beheerde computer in het netwerkoverzicht.
- 2 Klik op **Deze computer controleren** onder **Ik wil**.

De controle van de beveiligingsstatus van een computer stoppen

U kunt het controleren van beveiligingsstatus van een beheerde computer in het netwerk stoppen. De computer is dan echter voortaan een niet-beheerde computer, waarvan u de beveiligingsstatus niet extern kunt beheren.

- 1 Klik op het pictogram van een beheerde computer in het netwerkoverzicht.
- 2 Klik op **Controle van deze computer stoppen** onder **Ik wil**.
- 3 Klik op **Ja** in het bevestigingsdialoogvenster.

Machtigingen van een beheerde computer wijzigen

U kunt de machtigingen van een beheerde computer op elk moment wijzigen. Zo kunt u de computers wijzigen die de beveiligingsstatus van andere computers in het netwerk kunnen controleren.

- 1 Klik op het pictogram van een beheerde computer in het netwerkoverzicht.
- 2 Klik op **Machtigingen voor deze computer wijzigen** onder **Ik wil**.
- 3 Schakel in het dialoogvenster Machtigingen wijzigen het selectievakje in of uit om te bepalen of deze computer en andere computers in het beheerde netwerk elkaars beveiligingsstatus kunnen controleren.
- 4 Klik op **OK**.

Een apparaat beheren

U kunt een apparaat beheren door de beheerwebpagina van het apparaat te openen vanuit Network Manager.

- 1 Klik op het pictogram van een apparaat in het netwerkoverzicht.
- 2 Klik op **Dit apparaat beheren** onder **Ik wil**.
De webbrowser wordt geopend, waarin de beheerwebpagina van het apparaat wordt weergegeven.
- 3 Geef in de webbrowser uw aanmeldingsgegevens op en configureer de beveiligingsinstellingen van het apparaat.

Opmerking: als het apparaat een draadloze router of een draadloos toegangspunt is die of dat is beveiligd met Wireless Network Security, moet u de beveiligingsinstellingen van het apparaat configureren in Wireless Network Security.

De weergave-eigenschappen van een apparaat wijzigen

Als u de weergave-eigenschappen van een apparaat wijzigen, kunt u de apparaatnaam wijzigen die wordt weergegeven in het netwerkoverzicht en aangeven of het apparaat een draadloze router is.

- 1 Klik op het pictogram van een apparaat in het netwerkoverzicht.
- 2 Klik op **Apparaateigenschappen wijzigen** onder **Ik wil**.
- 3 Typ een naam in het vak **Naam** om de weergavenaam van het apparaat op te geven.
- 4 Geef het type apparaat op: klik op **Standaardrouter** als het apparaat geen draadloze router is, of op **Draadloze router** als het een draadloos apparaat betreft.
- 5 Klik op **OK**.

Beveiligingsproblemen oplossen

Vanaf beheerde computers met beheerdersrechten kunt u de McAfee-beveiligingsstatus van andere beheerde computers in het netwerk op afstand controleren en gerapporteerde beveiligingsproblemen op afstand oplossen. Wanneer de McAfee-beveiligingsstatus van een beheerde computer bijvoorbeeld aangeeft dat VirusScan is uitgeschakeld, kunt u VirusScan extern inschakelen vanaf een andere beheerde computer met beheerdersrechten.

Als u beveiligingsproblemen op afstand oplost, worden de meeste gerapporteerde problemen hersteld met Network Manager. Voor bepaalde beveiligingsproblemen kan echter handmatige interventie op de lokale computer zijn vereist. In dit geval worden door Network Manager de problemen opgelost die op afstand kunnen worden hersteld, en wordt u vervolgens gevraagd de resterende problemen op te lossen door u aan te melden bij SecurityCenter op de kwetsbare computer en de aanbevolen handelingen uit te voeren. Soms wordt als mogelijke oplossing aanbevolen SecurityCenter op de externe computer of computers in uw netwerk te installeren.

Beveiligingsproblemen oplossen

Met Network Manager kunt u de meeste beveiligingsproblemen op externe beheerde computers oplossen. Als VirusScan bijvoorbeeld is uitgeschakeld op een externe computer, kunt u het programma inschakelen.

- 1 Klik op het pictogram van een item in het netwerkoverzicht.
- 2 Bekijk de beveiligingsstatus van het item onder **Details**.
- 3 Klik op **Beveiligingsproblemen oplossen** onder **Ik wil**.
- 4 Klik op **OK** als u de beveiligingsproblemen hebt opgelost.

Opmerking: hoewel met Network Manager de meeste beveiligingsproblemen automatisch worden opgelost, vereisen bepaalde problemen mogelijk dat u SecurityCenter opent op de kwetsbare computer en de aanbevolen handelingen uitvoert.

McAfee-beveiligingssoftware installeren op externe computers

Als op een of meer computers in het netwerk niet de meest recente versie van SecurityCenter wordt uitgevoerd, kan de beveiligingsstatus van deze computers niet op afstand worden gecontroleerd. Als u deze computers op afstand wilt controleren, moet u de meest recente versie van SecurityCenter ter plaatse op elke computer installeren.

- 1 Open SecurityCenter op de computer waarop u de beveiligingssoftware wilt installeren.
- 2 Klik op **Mijn account** onder **Algemene taken**.
- 3 Meld u aan met behulp van het e-mailadres en het wachtwoord dat u hebt gebruikt om de beveiligingssoftware te registreren toen u deze voor het eerst installeerde.
- 4 Selecteer het gewenste product, klik op het pictogram **Installeren/Downloaden** en voer de instructies op het scherm uit.

HOOFDSTUK 28

McAfee EasyNetwork

Met EasyNetwork kunt u bestanden veilig delen, bestanden gemakkelijk overdragen en printers delen tussen vertrouwde computers in uw thuisnetwerk. Op de computers in het netwerk moet echter EasyNetwork zijn geïnstalleerd als u toegang wilt krijgen tot deze programmafuncties.

Voordat u EasyNetwork gebruikt, kunt u kennismaken met enkele functies. Meer informatie over het configureren en gebruik van deze functies vindt u in de Help van EasyNetwork.

Opmerking: SecurityCenter stelt u op de hoogte van kritieke en niet-kritieke beveiligingsproblemen zodra deze worden vastgesteld. Als u hulp nodig hebt bij het analyseren van beveiligingsproblemen, kunt u McAfee Virtual Technician uitvoeren.

In dit hoofdstuk

Functies van EasyNetwork	170
EasyNetwork instellen	171
Bestanden delen en versturen.....	177
Printers delen	183

Funcities van EasyNetwork

EasyNetwork biedt de volgende functies:

Bestanden delen

Met EasyNetwork kunt u op eenvoudige wijze bestanden delen met andere computers in het netwerk. Wanneer u bestanden deelt, verleent u daarmee andere computers toestemming om deze bestanden te lezen (alleen-lezen). Alleen computers met volledige of beheerderstoegang tot het beheerde netwerk (leden) kunnen bestanden delen of openen die door andere leden worden gedeeld.

Bestandsoverdracht

U kunt bestanden verzenden aan andere computers met volledige of beheerderstoegang op het beheerde netwerk (leden). Wanneer u een bestand ontvangt, verschijnt dit in uw Postvak IN van EasyNetwork. Het Postvak IN is een tijdelijke opslagplaats voor alle bestanden die door andere computers in het netwerk naar u worden verzonden.

Automatisch delen van printers

Nadat u zich hebt aangemeld bij een beheerd netwerk, kunt u automatisch de beschikbare lokale printers delen die met uw computer zijn verbonden met andere leden. Hierbij wordt de huidige naam van de printer gebruikt als naam voor de gedeelde printer. EasyNetwork controleert ook of er printers beschikbaar zijn die worden gedeeld door andere computers in uw netwerk, en staat u toe om deze printers te configureren en te gebruiken.

HOOFDSTUK 29

EasyNetwork instellen

Voordat u EasyNetwork kunt gebruiken, moet u het programma starten en lid worden van een beheerd netwerk. Nadat u lid bent geworden van een beheerd netwerk, kunt u bestanden delen, zoeken en verzenden aan andere computers op het netwerk. U kunt ook printers delen. U kunt op elk gewenst tijdstip uw lidmaatschap voor het netwerk opzeggen.

In dit hoofdstuk

EasyNetwork openen	171
Lid worden van een beheerd netwerk	172
U afmelden bij een beheerd netwerk.....	176

EasyNetwork openen

Standaard wordt u na het installeren van EasyNetwork gevraagd of u dit programma wilt openen. U kunt EasyNetwork echter ook op een later tijdstip openen.

- Wijs in het menu **Start** de optie **Programma's** aan, wijs **McAfee** aan klik vervolgens op **McAfee EasyNetwork**.

Tip: als u tijdens de installatie een bureaubladpictogram en een snelstartpictogram hebt gemaakt, kunt u EasyNetwork ook openen door te dubbelklikken op het pictogram van McAfee EasyNetwork op uw bureaublad of in het systeemvak van Windows, geheel rechts op de taakbalk.

Lid worden van een beheerd netwerk

Als op geen van de computers op het netwerk waarmee u verbonden bent SecurityCenter is geïnstalleerd, krijgt u lidmaatschap van het netwerk en wordt u gevraagd om aan te geven of het netwerk vertrouwd is. Als uw computer de eerste is die lid wordt van het netwerk, wordt de naam van uw computer automatisch opgenomen in de netwerknaam. U kunt dit netwerk echter altijd een andere naam geven.

Wanneer een computer verbinding maakt met het netwerk, wordt een aanmeldingsverzoek gestuurd naar de andere computers op het netwerk. Het verzoek kan worden ingewilligd door elke computer die over de juiste beheerdersrechten voor het netwerk beschikt. De toegangsverlener kan ook het machtigingsniveau bepalen voor de computer die lid wordt van het netwerk. Machtigingsniveaus zijn bijvoorbeeld: gast (uitsluitend bestandsoverdracht) of volledige/beheerdersrechten (bestandsoverdracht en het uitwisselen van bestanden). In EasyNetwork kunnen computers met beheerdersrechten toegang verlenen aan andere computers en machtigingen beheren (computers hoger of lager in de hiërarchie plaatsen); computers met volledige toegangsrechten mogen deze beheerderstaken niet uitvoeren.

Opmerking: zodra een computer met andere netwerkprogramma's van McAfee (zoals Network Manager) aan het netwerk is toegevoegd, wordt de computer eveneens herkend als beheerde computer in deze programma's. Het machtigingsniveau dat aan een computer in EasyNetwork is toegewezen, geldt voor alle McAfee-netwerkprogramma's. Raadpleeg de documentatie bij een programma voor meer informatie over de betekenis van gast-, beheer- en volledige machtigingen in het betreffende programma.

Lid worden van het netwerk

De eerste keer dat een computer waarop EasyNetwork is geïnstalleerd verbinding maakt met een vertrouwd netwerk, wordt er gevraagd of u lid wil worden van het beheerde netwerk. Wanneer de computer lid wil worden, wordt een aanmeldingsverzoek gestuurd naar alle andere computers met beheerdersrechten. Dit verzoek moet worden verleend voordat de computer printers of bestanden kan delen, of bestanden kan versturen of kopiëren over het netwerk. Aan de eerste computer op het netwerk worden automatisch beheerdersrechten verleend.

- 1 Klik in het venster Gedeelde bestanden op **Aanmelden bij dit netwerk**.
Wanneer een computer met beheerdersrechten uw verzoek inwilligt, verschijnt een bericht waarin u wordt gevraagd of u deze computer en andere computers in het netwerk wilt toestaan om elkaars beveiligingsinstellingen te beheren.
- 2 Als u wilt toestaan dat deze computer en andere computers in het netwerk elkaars beveiligingsinstellingen beheren, klikt u op **OK**; zo niet, dan klikt u op **Annuleren**.
- 3 Bevestig dat de computer die toegang verleent de speelkaarten toont die worden weergegeven in het bevestigingsdialoogvenster, en klik vervolgens op **OK**.

Opmerking: als op de computer die u heeft uitgenodigd lid te worden van het beheerde netwerk niet dezelfde speelkaarten worden weergegeven als in het bevestigingsdialoogvenster, is er sprake van een lek in de beveiliging van het beheerde netwerk. Als u lid wordt van het netwerk, kunt u uw computer in gevaar brengen. Klik daarom op **Annuleren** in het bevestigingsdialoogvenster.

Toegang verlenen tot het netwerk

Wanneer een computer een verzoek indient om lid te worden van het beheerde netwerk, wordt een bericht gestuurd naar de andere computers in het netwerk die over beheerdersrechten beschikken. De eerste computer die reageert, wordt de computer die toegang verleent. Als toegangsverlener bent u verantwoordelijk voor het besluit welk type toegang aan de computer in kwestie wordt verleend: gast, volledig of beheerder.

- 1 Klik op het gewenste toegangsniveau in de waarschuwing.
- 2 Voer in het dialoogvenster Een computer uitnodigen om lid te worden van dit beheerde netwerk het volgende uit:
 - Klik op **Gasttoegang verlenen aan programma's in een beheerd netwerk** om de computer toegang te verlenen tot het netwerk (u kunt deze optie gebruiken voor tijdelijke gebruikers bij u thuis).

- Klik op **Volledige toegang verlenen aan programma's in een beheerd netwerk** om de computer toegang te verlenen tot het netwerk.
- Klik op **Beheerderstoegang verlenen aan programma's in een beheerd netwerk** om de computer toegang te verlenen tot het netwerk met beheerdersrechten. De computer kan dan tevens toegang verlenen aan andere computers die lid van het beheerde netwerk willen worden.

3 Klik op **OK**.

4 Bevestig dat de computer de speelkaarten toont die worden weergegeven in het bevestigingsdialoogvenster, en klik vervolgens op **Toegang verlenen**.

Opmerking: als er op de computer niet dezelfde speelkaarten worden weergegeven als in het bevestigingsdialoogvenster, is er sprake van een inbreuk op de beveiliging van het beheerde netwerk. Door deze computer toegang te verlenen tot het netwerk kunt u uw computer blootstellen aan een beveiligingsrisico. We raden u dan ook aan om te klikken op **Verzoek afwijzen** in het bevestigingsdialoogvenster.

De naam van het netwerk wijzigen

Standaard wordt de naam van de eerste computer die zich bij het netwerk heeft aangemeld opgenomen in de naam van het netwerk. U kunt de naam van het netwerk echter altijd nog wijzigen. Wanneer u het netwerk een andere naam geeft, wijzigt u de netwerksomgeving die wordt weergegeven in EasyNetwork.

- 1 Klik in het menu **Opties** op **Configureren**.
- 2 In het dialoogvenster Configureren typt u de naam van het netwerk in het vak **Netwerknaam**.
- 3 Klik op **OK**.

U afmelden bij een beheerd netwerk

Als u zich hebt aangemeld bij een beheerd netwerk en vervolgens besluit dat u niet langer lid wenst te zijn, kunt u het netwerk verlaten. Als u een beheerd netwerk hebt verlaten, kunt u op elk gewenst moment opnieuw lid worden. Hiervoor moet u echter opnieuw toestemming ontvangen. Zie Lid worden van een beheerd netwerk (pagina 172) voor meer informatie over het aanmelden.

U afmelden bij een beheerd netwerk

U kunt zich afmelden bij een beheerd netwerk waarbij u zich eerder hebt aangemeld.

- 1 Klik in het menu **Extra** op **Netwerk verlaten**.
- 2 In het dialoogvenster Netwerk verlaten selecteert u de naam van het netwerk waarvoor u zich wilt afmelden.
- 3 Klik op **Netwerk verlaten**.

HOOFDSTUK 30

Bestanden delen en versturen

Met EasyNetwork wordt het eenvoudig om bestanden te delen met en te versturen naar andere computers in het netwerk. Wanneer u bestanden deelt, verleent u daarmee andere computers toestemming om deze bestanden te lezen (alleen-lezen). Alleen computers die lid zijn van het beheerde netwerk (met volledige of beheerdersrechten) kunnen bestanden delen of bestanden openen die door andere lidcomputers worden gedeeld.

Opmerking: het delen van grote hoeveelheden bestanden is mogelijk van invloed op uw computerbronnen.

In dit hoofdstuk

Bestanden delen.....	178
Bestanden naar andere computers verzenden	181

Bestanden delen

Alleen computers die lid zijn van het beheerde netwerk (met volledige of beheerdersrechten) kunnen bestanden delen of bestanden openen die door andere lidcomputers worden gedeeld. Als u een map deelt, worden alle bestanden in die map en in de submappen daarvan gedeeld. Als u vervolgens bestanden toevoegt aan die map worden deze echter niet automatisch gedeeld. Als een gedeeld bestand of een gedeelde map wordt verwijderd, wordt deze ook verwijderd uit het venster Gedeelde bestanden. U kunt het delen van een bestand op elk gewenst moment opheffen.

U kunt een gedeeld bestand rechtstreeks openen vanuit EasyNetwork of het naar uw computer kopiëren en het daarop openen. Als de lijst met gedeelde bestanden erg groot is en u niet gemakkelijk kunt zien waar het bestand zich bevindt, kunt u het zoeken.

Opmerking: bestanden die zijn gedeeld met EasyNetwork kunnen niet vanaf andere computers worden geopend met Windows Verkenner omdat de functie voor het delen van bestanden van EasyNetwork via een beveiligde verbinding moet worden gebruikt.

Een bestand delen

Wanneer u een bestand deelt, wordt dit beschikbaar gesteld aan alle leden met volledige of beheerdersrechten voor het beheerde netwerk.

- 1 Zoek in Windows Verkenner het bestand dat u wilt delen.
- 2 Sleep het bestand vanuit de locatie in Windows Verkenner naar het venster Gedeelde bestanden in EasyNetwork.

Tip: u kunt een bestand ook delen door te klikken op **Bestanden delen** in het menu **Extra**. Navigeer in het dialoogvenster Delen naar de map waarin het bestand dat u wilt delen is opgeslagen, selecteer het bestand en klik vervolgens op **Delen**.

Het delen van een bestand opheffen

Als u een bestand deelt op het beheerde netwerk, kunt u het delen van dat bestand op elk gewenst moment opheffen. Wanneer u stopt met het delen van een bestand kunnen andere leden van het beheerde netwerk dat bestand niet openen.

- 1 Klik in het menu **Extra** op **Stoppen met bestanden delen**.
- 2 Selecteer in het dialoogvenster Stoppen met bestanden delen het bestand dat u niet langer wilt delen.
- 3 Klik op **OK**.

Een gedeeld bestand kopiëren

U kopieert een gedeeld bestand om er over te kunnen beschikken als het niet langer wordt gedeeld. U kunt gedeelde bestanden vanaf elke computer in het beheerde netwerk kopiëren.

- Sleep een bestand vanuit het venster Gedeelde bestanden in EasyNetwork naar een locatie in Windows Verkenner of naar het Windows-bureaublad.

Tip: u kunt een gedeeld bestand ook kopiëren door het bestand te selecteren in EasyNetwork, en vervolgens te klikken op **Kopiëren naar** in het menu **Extra**. Navigeer in het dialoogvenster Kopiëren naar map naar de map waarnaar u het bestand wilt kopiëren, selecteer de betreffende map en klik vervolgens op **Opslaan**.

Een gedeeld bestand zoeken

U kunt zoeken naar een bestand dat door u of door een ander lid van het netwerk is gedeeld. Terwijl u uw zoekcriteria typt, geeft EasyNetwork de bijbehorende resultaten weer in het venster Gedeelde bestanden.

- 1 Klik in het venster Gedeelde bestanden op **Zoeken**.
- 2 Klik op de gewenste optie (pagina 179) in de lijst **Bevat**.
- 3 Typ een deel van de bestandsnaam of van het pad of de gehele bestandsnaam of het gehele pad in de lijst **Bestandsnaam of pad**.
- 4 Klik op het gewenste bestandstype (pagina 179) in de lijst **Type**.
- 5 Klik in de lijsten **Van** en **t/m** op datums die het datumbereik aangeven waarbinnen het gezochte bestand is aangemaakt.

Zoekcriteria

In de volgende tabellen vindt u zoekcriteria die u kunt opgeven bij het zoeken naar gedeelde bestanden.

Naam van het bestand of het pad

Bevat	Beschrijving
Bevat alle volgende woorden	Zoekt een naam van het bestand of het pad die alle woorden bevat die u opgeeft in de lijst Bestandsnaam of pad , in willekeurige volgorde.
Bevat een of meer van de volgende woorden	Zoekt een naam van het bestand of het pad die een of meer van de woorden bevat die u opgeeft in de lijst Bestandsnaam of pad .
Bevat exact de volgende tekenreeks	Zoekt een naam van het bestand of het pad die exact dezelfde woordenreeks bevat die u opgeeft in de lijst Bestandsnaam of pad .

Type bestand

Type	Beschrijving
Willekeurig	Doorzoekt alle gedeelde bestandstypen.
Document	Doorzoekt alle gedeelde documenten.
Afbeelding	Doorzoekt alle gedeelde afbeeldingsbestanden.
Video	Doorzoekt alle gedeelde videobestanden.
Audio	Doorzoekt alle gedeelde audiobestanden.
Gecomprimeerd	Doorzoekt alle gecomprimeerde bestanden (bijvoorbeeld .zip-bestanden).

Bestanden naar andere computers verzenden

U kunt bestanden verzenden naar andere computers die lid zijn van het beheerde netwerk. Voordat u een bestand verstuurt, bevestigt EasyNetwork dat er voldoende vrije schijfruimte beschikbaar is op de computer die het bestand ontvangt.

Wanneer u een bestand ontvangt, verschijnt dit in uw Postvak IN van EasyNetwork. Het Postvak IN is een tijdelijke opslagplaats voor alle bestanden die andere computers in het netwerk naar u verzenden. Als u EasyNetwork geopend hebt wanneer u een bestand ontvangt, verschijnt het bestand direct in uw Postvak IN. Als u EasyNetwork niet geopend hebt, verschijnt er een bericht in het systeemvak van Windows, geheel rechts op de taakbalk. Als u geen meldingen wilt ontvangen (omdat deze u bijvoorbeeld in uw werkzaamheden storen), kunt u deze functie uitschakelen. Als er in het Postvak IN al een bestand voorkomt met dezelfde naam, krijgt het nieuwe bestand een nummer achter de naam. Bestanden blijven in uw Postvak IN staan totdat u deze accepteert (totdat u deze naar een locatie op uw computer kopieert).

Een bestand naar een andere computer verzenden

U kunt een bestand naar een andere computer op het beheerde netwerk sturen zonder dat u het bestand hoeft te delen. Voordat een gebruiker op de ontvangende computer het bestand kan bekijken, moet deze het bestand eerst opslaan op een lokale locatie. Zie Een bestand van een andere computer accepteren (pagina 182) voor meer informatie.

- 1 Zoek in Windows Verkenner het bestand dat u wilt verzenden.
- 2 Sleep het bestand vanuit de locatie in Windows Verkenner naar het pictogram van een actieve computer in EasyNetwork.

Tip: u kunt meerdere bestanden tegelijk naar een computer verzenden door de toets Ctrl (Control) ingedrukt te houden terwijl u de bestanden selecteert. U kunt ook bestanden verzenden door te klikken op **Verzenden** in het menu **Extra**, de bestanden te selecteren en vervolgens te klikken op **Verzenden**.

Een bestand van een andere computer accepteren

Als een andere computer in het beheerde netwerk u een bestand stuurt, moet u dit accepteren door het bestand op te slaan in een map op uw computer. Als EasyNetwork niet wordt uitgevoerd wanneer er een bestand naar uw computer wordt gestuurd, ontvangt u een bericht hierover in het systeemvak van Windows, geheel rechts op de taakbalk. Klik op dit bericht om EasyNetwork te openen en toegang te krijgen tot het bestand.

- Klik op **Ontvangen** en sleep vervolgens het bestand vanuit uw Postvak IN van EasyNetwork naar een map in Windows Verkenner.

Tip: u kunt ook een bestand van een andere computer ontvangen door het bestand te selecteren in uw Postvak IN van EasyNetwork, en vervolgens te klikken op **Accepteren** in het menu **Extra**. Blader in het dialoogvenster Accepteren in map naar de map waarin u de bestanden die u ontvangt wilt opslaan, selecteer de gewenste map en klik vervolgens op **Opslaan**.

Bericht ontvangen wanneer een bestand wordt verzonden

U kunt desgewenst bericht ontvangen telkens wanneer een andere computer op het beheerde netwerk u een bestand stuurt. Als EasyNetwork niet wordt uitgevoerd, wordt het bericht weergegeven in het systeemvak van Windows, geheel rechts op de taakbalk.

- 1 Klik in het menu **Opties** op **Configureren**.
- 2 Schakel in het dialoogvenster Configureren het selectievakje **Waarschuwen wanneer een andere computer mij bestanden stuurt** in.
- 3 Klik op **OK**.

HOOFDSTUK 31

Printers delen

Nadat u zich hebt aangemeld bij een beheerd netwerk, deelt EasyNetwork de beschikbare lokale printers die met uw computer zijn verbonden. Hierbij wordt de huidige naam van de printer gebruikt als naam voor de gedeelde printer. EasyNetwork controleert ook of er printers beschikbaar zijn die worden gedeeld door andere computers in uw netwerk, en staat u toe om deze te configureren en te gebruiken.

Als u een printer zodanig hebt geconfigureerd dat deze afdrukt via een netwerk-afdrukservers (zoals een draadloze USB-afdrukservers), beschouwt EasyNetwork de printer als een lokale printer en zal EasyNetwork de printer delen in het netwerk. U kunt het delen van een printer op elk gewenst moment opheffen.

In dit hoofdstuk

Werken met gedeelde printers 184

Werken met gedeelde printers

EasyNetwork stelt de printers vast die door de computers op het netwerk worden gedeeld. Als EasyNetwork een externe printer aantreft die niet met uw computer verbonden is, verschijnt de koppeling **Beschikbare netwerkprinters** in het venster Gedeelde bestanden wanneer u EasyNetwork voor het eerst opent. Vervolgens kunt u de beschikbare printers installeren of de installatie opheffen van printers die al met uw computer zijn verbonden. U kunt ook de lijst met printers vernieuwen en ervoor zorgen dat u de meeste recente informatie weergeeft.

Als u zich niet hebt aangemeld bij het beheerde netwerk maar er wel op bent aangesloten, kunt u de gedeelde printers openen via het onderdeel Printers en faxapparaten van het Configuratiescherm van Windows.

Het delen van een printer opheffen

Als u het delen van een printer opheft, kunnen leden deze niet gebruiken.

- 1 Klik in het menu **Extra** op **Printers**.
- 2 Selecteer in het dialoogvenster Netwerkprinters beheren de printer die u niet langer wilt delen.
- 3 Klik op **Niet delen**.

Een beschikbare netwerkprinter installeren

Als u lid bent van een beheerd netwerk, hebt u toegang tot de gedeelde printers. U moet echter wel het printerstuurprogramma installeren dat de printer gebruikt. Als de eigenaar van de printer het delen stopt, kunt u de printer niet gebruiken.

- 1 Klik in het menu **Extra** op **Printers**.
- 2 Klik in het dialoogvenster Beschikbare netwerkprinters op de naam van een printer.
- 3 Klik op **Installeren**.

Naslag

De Verklarende woordenlijst van termen geeft een overzicht en definitie van de beveiligingstermen die in McAfee-producten het meeste worden gebruikt.

Verklarende woordenlijst

8

802.11

Een verzameling IEEE-standaarden voor het verzenden van gegevens via een draadloos netwerk. 802.11 staat beter bekend als Wi-Fi.

802.11a

Een uitbreiding van 802.11 waarbij gegevens worden verzonden met een maximumsnelheid van 54 Mbps in de 5-GHz band. De transmissiesnelheid is weliswaar hoger dan bij 802.11b, maar de maximumafstand is veel kleiner.

802.11b

Een uitbreiding van 802.11 waarbij gegevens worden verzonden met een maximumsnelheid van 11 Mbps in de 2,4-GHz band. De transmissiesnelheid is weliswaar lager dan bij 802.11b, maar de maximumafstand is veel groter.

802.1x

Een IEEE-standaard voor verificatie op draadloze en niet-draadloze netwerken. 802.1x wordt veel gebruikt in combinatie met draadloze netwerken van het type 802.11.

A

Aanval met grof geweld

Een methode voor het decoderen van gecodeerde gegevens, zoals wachtwoorden, via een grote inzet (grof geweld) in plaats van met een intelligente strategie. Deze methode neemt weliswaar veel tijd in beslag, maar wordt als onfeilbaar beschouwd. Een aanval met grof geweld wordt ook wel kraken met grof geweld genoemd.

ActiveX-besturingselement

Een software-onderdeel dat in programma's of op webpagina's wordt gebruikt om extra functionaliteit toe te voegen en dat verschijnt als een normaal onderdeel van het programma of de webpagina. De meeste ActiveX-besturingselementen zijn onschuldig, maar sommige zijn ontworpen om informatie op uw computer te zoeken.

Afbeeldingsfilter

Een optie voor ouderlijk toezicht waarbij mogelijk ongewenste webafbeeldingen voor weergave worden geblokkeerd.

Archiveren

Een lokale kopie maken van belangrijke bestanden op cd, dvd, een USB-station, een externe vaste schijf of een netwerkschijf.

B

Back-up maken

Een kopie maken van uw belangrijke bestanden op een beveiligde online server.

Bandbreedte

De hoeveelheid gegevens die binnen een bepaalde periode kan worden verzonden of ontvangen.

Beheerd netwerk

Een thuisnetwerk dat twee typen leden kan hebben: beheerde leden en niet-beheerde leden. Beheerde leden staan andere computers in het netwerk toe hun beveiligingsstatus te controleren. Niet-beheerde leden staan dit niet toe.

Bestandsfragmenten

Bestanden die niet definitief zijn verwijderd en die zich overal op een schijf kunnen bevinden. Bestandsfragmentatie vindt plaats tijdens het toevoegen of verwijderen van bestanden en kan de prestaties van de computer beïnvloeden.

Bewaakte bestandstypen

De bestandstypen (bijvoorbeeld .doc, .xls, enzovoort) waarvan met Data Backup een back-up wordt gemaakt of die worden gearchiveerd in de bewaakte locaties.

Bewaakte locaties

De mappen op uw computer die door Data Backup worden bewaakt.

Bibliotheek

Een online opslagruimte voor bestanden waarvan u een back-up hebt gemaakt en die u hebt gepubliceerd. De Data Backup-bibliotheek is een website op internet die toegankelijk is voor iedereen met toegang tot internet.

Browser

Een programma voor het weergeven van webpagina's op internet. Populaire webbrowsers zijn onder andere Microsoft Internet Explorer en Mozilla Firefox.

C

Cache

Een tijdelijke opslagruimte op de computer. Om sneller en efficiënter op internet te kunnen surfen, worden bijvoorbeeld webpagina's die u al eerder hebt bezocht, uit de cache opgehaald, niet van een externe server.

Client

Een toepassing die op een pc of werkstation wordt uitgevoerd en afhankelijk is van een server voor de uitvoering van bepaalde acties. Bijvoorbeeld: een e-mailclient is een toepassing waarmee u e-mail kunt verzenden en ontvangen.

Codering

Een proces waarbij tekst wordt omgezet in code. Hierdoor worden de gegevens gemaskeerd zodat deze onleesbaar wordt voor iedereen die niet weet hoe de informatie moet worden gedecodeerd. Gecodeerde gegevens worden ook codetekst genoemd.

Codetekst

Gecodeerde tekst. Codetekst is onleesbaar totdat deze is geconverteerd (gedecodeerd) naar normale tekst.

Compressie

Een proces waarbij bestanden worden gecomprimeerd naar een formaat dat minder ruimte inneemt bij het opslaan of versturen.

Cookie

Een klein bestand met informatie dat bevat meestal een gebruikersnaam en de huidige datum en tijd bevat en dat wordt opgeslagen op de computer van een persoon die op het web surft. Cookies worden gewoonlijk door websites gebruikt om gebruikers te herkennen die zich eerder hebben aangemeld bij de site. Ze kunnen echter ook een bron van informatie zijn voor hackers.

D

DAT

(Virusdefinitiebestanden) Bestanden met de definities die worden gebruikt bij het detecteren van virussen, Trojaanse paarden, spyware, adware en andere mogelijk ongewenste programma's op uw computer of USB-station.

Delen

Ontvangers van een e-mailbericht tijdens een beperkte periode toestaan om geselecteerde back-upbestanden te openen. Als u een bestand deelt, verstuurt u een back-upexemplaar van het bestand aan de e-mailontvangers die u opgeeft. De ontvangers ontvangen een e-mailbericht van Data Backup met de melding dat er bestanden met hen worden gedeeld. Het e-mailbericht bevat ook een koppeling naar de gedeelde bestanden.

Denial of Service (DoS)

Een type aanval waarbij het verkeer op een netwerk wordt vertraagd of wordt gestopt. Een DoS-aanval (Denial of Service-aanval) vindt plaats als een netwerk wordt overspoeld met zoveel aanvullende aanvragen dat het gewone verkeer wordt vertraagd of volledig wordt onderbroken. Dit resulteert normaal gesproken niet in gegevensdiefstal of andere veiligheidsrisico's.

Dialer

Software waarmee u een internetverbinding tot stand kunt brengen. Als dergelijke software op kwaadwillende wijze wordt gebruikt, kan uw internetverbinding worden omgeleid naar een andere provider dan uw gewone internetaanbieder (ISP) zonder dat u daarbij op de hoogte bent van de extra kosten.

DNS

(Domain Name System) Een systeem voor het omzetten van hostnamen of domeinnamen in IP-adressen. Op het web wordt DNS gebruikt voor het omzetten van het gemakkelijk leesbare webadres (bijvoorbeeld www.myhostname.com) in IP-adressen (bijvoorbeeld 111.2.3.44), zodat de website kan worden gedownload en weergegeven. Zonder DNS zou u zelf het IP-adres in de adresbalk van de browser moeten typen.

DNS-server

(Domain Name System-server) Een computer die IP-adressen retourneert die zijn gekoppeld aan een host- of domeinnaam. Zie ook DNS.

Domein

Een lokaal subnetwerk of een lokale descriptor voor sites op internet.

Op een LAN (Local Area Network) is een domein een subnetwerk dat bestaat uit client- en servercomputers die worden beheerd door één beveiligingsdatabase. In deze context kunnen domeinen de prestaties verbeteren. Op internet is een domein onderdeel van elk webadres (in www.abc.com is abc bijvoorbeeld het domein).

Draadloze adapter

Een apparaat dat mogelijkheden voor draadloze communicatie biedt voor een computer of PDA. De draadloze adapter wordt aangesloten via een USB-poort, PC Card (CardBus)-sleuf of geheugenkaartsleuf of intern op de PCI-bus.

Draadloze PCI-adapterkaarten

(Peripheral Component Interconnect) Een draadloze adapterkaart die u in een PCI-uitbreidingsleuf kunt plaatsen in de computer.

Draadloze USB-adapterkaart

Een draadloze adapterkaart die wordt aangesloten op een USB-poort van de computer.

E

E-mail

(Electronic mail) Berichten die elektronisch worden verzonden en ontvangen op een computernetwerk. Zie ook [webmail](#).

E-mailclient

Een programma dat u uitvoert op een computer voor het verzenden en ontvangen van e-mail (bijvoorbeeld Microsoft Outlook).

ESS

(Extended Service Set) Een set van twee of meer netwerken die één subnetwerk vormen.

Externe vaste schijf

Een vaste schijf die zich buiten de computer bevindt.

F

Firewall

Een systeem (hardwaredatig, softwarematig of beide) dat is ontworpen om ongeoorloofde toegang tot of vanaf een privénetwerk onmogelijk te maken. Firewalls worden vaak gebruikt om niet-geautoriseerde internetgebruikers de toegang te weigeren tot privénetwerken (vooral intranetten) die met internet zijn verbonden. Alle berichten die het intranet binnenkomen of verlaten, verlopen via de firewall, die alle berichten controleert en berichten blokkeert die niet voldoen aan de ingestelde beveiligingscriteria.

G

Gebeurtenis

Een actie die wordt geïnitieerd door de gebruiker, een apparaat of de computer zelf, en die een reactie veroorzaakt. McAfee legt gebeurtenissen vast in het bijbehorende gebeurtenislogboek.

Gedeeld geheim

Een tekenreeks of een sleutel (meestal een wachtwoord) dat wordt gedeeld tussen twee met elkaar communicerende partijen vóórdat de communicatie werd geïnitieerd. Een gedeeld geheim wordt gebruikt voor het beveiligen van vertrouwelijke gedeelten van RADIUS-berichten.

Geïntegreerde gateway

Een apparaat dat de functies van een toegangspunt, router en firewall combineert. Sommige apparaten kunnen ook beveiligingsfuncties en bridgingvoorzieningen bieden.

Groep met inhoudsrestricties

Bij ouderlijk toezicht: een leeftijdsgroep waartoe een gebruiker behoort. Inhoud wordt beschikbaar gesteld of geblokkeerd op basis van de groep met inhoudsrestricties waartoe een gebruiker behoort. De groepen met inhoudsrestricties zijn: jong kind, kind, jongere tiener, oudere tiener en volwassene.

H

Hotspot

Een geografisch bereik dat wordt gedekt door een Wi-Fi-toegangspunt (802.11). Gebruikers die een hotspot binnengaan met een laptop met een draadloze verbinding kunnen een internetverbinding maken, mits de hotspot zichzelf adverteert en verificatie niet is vereist. Hotspots bevinden zich meestal in dichtbevolkte of drukke gebieden, zoals vliegvelden.

I

Internet

Internet bestaat uit een groot aantal onderling verbonden netwerken die de TCP/IP-protocollen gebruiken om gegevens te vinden en over te zetten. Internet is voortgekomen uit een aantal aan elkaar gekoppelde computers op universiteiten en colleges (aan het eind van de jaren zestig en aan het begin van de jaren zeventig van de vorige eeuw) die waren gefinancierd door het Amerikaanse ministerie van defensie. Dit netwerk werd het ARPANET genoemd. Vandaag de dag is internet een wereldwijd netwerk dat bestaat uit bijna 100.000 onafhankelijke netwerken.

Intranet

Een privécomputernetwerk, meestal binnen een organisatie, waartoe alleen gemachtigde gebruikers toegang hebben.

IP-adres

Een identificatie voor een computer of apparaat op een TCP/IP-netwerk. Netwerken die gebruikmaken van het TCP/IP-protocol, routeren berichten op basis van het IP-adres van de bestemming. De notatie van een IP-adres is een 32-bits adres dat bestaat uit vier getallen die met een punt van elkaar worden gescheiden. Elk getal kan tussen 0 en 255 liggen (bijvoorbeeld 192.168.1.100).

IP-spoofing

De IP-adressen in een IP-pakket vervalsen. Dit wordt toegepast in vele typen aanvallen, inclusief session hijacking (kapen van een sessie). Het wordt ook vaak gebruikt om de e-mailheader van spam te vervalsen, zodat de afzender niet goed kan worden opgespoord.

K

Knooppunt

Eén computer die met een netwerk is verbonden.

L

LAN

(Local Area Network) Een computernetwerk dat een relatief klein gebied omvat (bijvoorbeeld één gebouw). Computers op een LAN kunnen met elkaar communiceren en bronnen zoals printers en bestanden delen.

Launchpad (platform)

Een U3-interfacecomponent die fungeert als startpunt voor het starten en beheren van USB-programma's via het U3-platform.

Lijsten met vertrouwde items

Bevat items die u als vertrouwd hebt aangeduid en die niet worden vastgesteld. Als u een item per ongeluk als vertrouwd hebt aangemerkt (bijvoorbeeld een mogelijk ongewenst programma) of als u wilt dat het wordt gedetecteerd, moet u het uit deze lijst verwijderen.

Locatie voor grondige bewaking

Een map op uw computer die door Data Backup worden gecontroleerd op wijzigingen. Als u een locatie voor grondige bewaking instelt, maakt Data Backup back-ups van de bewaakte bestandstypen in die map en de bijbehorende submappen.

Locaties voor oppervlakkige bewaking

Een map op uw computer die door Data Backup wordt gecontroleerd op wijzigingen. Als u een locatie voor oppervlakkige bewaking instelt, maakt Data Backup back-ups van de bewaakte bestandstypen in die map, maar niet van de bijbehorende submappen.

M

MAC (Message Authentication Code)

Een beveiligingscode die wordt gebruikt voor het coderen van berichten die tussen computers worden verzonden. Het bericht wordt geaccepteerd als de computer de gedecodeerde code als geldig aanmerkt.

MAC-adres

(Media Access Control-adres) Een uniek serienummer dat wordt toegewezen aan een fysiek apparaat dat toegang heeft tot het netwerk.

Man-in-het-midden-aanval

Een methode voor het onderscheppen en mogelijk wijzigen van berichten tussen twee partijen zonder dat een van de partijen op de hoogte is van het doorbreken van de communicatieverbinding.

MAPI

(Messaging Application Programming Interface) Een Microsoft-interfacespecificatie waarmee verschillende bericht- en werkgroep-toepassingen (inclusief e-mail, voicemail en fax) via één enkele client kunnen werken, zoals de Exchange-client.

Mogelijk ongewenst programma (MOP)

Een programma dat zonder uw toestemming persoonlijke gegevens verzamelt en verzendt (bijvoorbeeld spyware en adware).

MSN

(Microsoft Network) Een groep of webservices die door Microsoft Corporation worden geboden, waaronder een zoekprogramma, e-mail, expresberichten en een portaal.

N

Netwerk

Een verzameling toegangspunten en de hieraan gekoppelde gebruikers, vergelijkbaar met een ESS.

Netwerkoverzicht

Een grafisch overzicht van de beveiligingsstatus van de computers en componenten waaruit uw thuisnetwerk bestaat.

Netwerkstation

Een station of schijf die is verbonden met een server op een netwerk met meerdere gebruikers. Netwerkstations worden soms externe stations genoemd.

NIC

(Network Interface Card) Een kaart die in een laptopcomputer of een ander apparaat wordt geplaatst om verbinding te maken met het LAN.

Normale tekst

Tekst die niet is gecodeerd. Zie ook codering.

O

Onbetrouwbare toegangspunten

Een niet-gemachtigd toegangspunt. Onbetrouwbare toegangspunten kunnen op een beveiligd bedrijfsnetwerk worden geïnstalleerd voor het verlenen van toegang aan niet-gemachtigde partijen. Een aanvaller kan deze ook maken om een man-in-het-midden-aanval uit te voeren.

Online opslagplaats

De locatie op de online server waarop uw bestanden worden opgeslagen nadat er een back-up van is gemaakt.

Overschrijding van de bufferlimiet

De situatie waarin verdachte programma's of processen proberen om meer gegevens in een buffer (een tijdelijke opslagruimte) op de computer op te slaan dan deze kan bevatten. Bij overschrijdingen van de bufferlimiet worden gegevens in naastgelegen buffers overschreven.

P

Parental Controls

Instellingen waarmee u kunt beheren wat uw kinderen te zien krijgen en wat ze mogen doen als zij op het web surfen. Voor het instellen van Parental Controls kunt u afbeeldingsfilters in- of uitschakelen, een groep met inhoudsrestricties kiezen en tijdslimieten voor internetgebruik vastleggen.

Phishing

Oplichting op internet die is gericht op het verkrijgen van waardevolle gegevens (zoals creditcardnummers en sofinummers, gebruikers-id's en wachtwoorden) van nietsvermoedende gebruikers en die voor frauduleuze doeleinden worden gebruikt.

Plugin

Een klein softwareprogramma dat wordt gebruikt in combinatie met een groter programma voor meer uitgebreide functionaliteit. Dankzij invoegtoepassingen kan de webbrowser bijvoorbeeld bestanden openen en uitvoeren die zijn ingesloten in HTML-documenten en een indeling hebben die de browser normaal gesproken niet zou herkennen (zoals animatie-, video- en audiobestanden).

Poort

Een plaats waarop informatie de computer binnengaat of verlaat. Een conventionele analoge modem wordt bijvoorbeeld op een seriële poort aangesloten.

Pop-ups

Kleine vensters die op de voorgrond voor andere vensters worden weergegeven op het beeldscherm van de computer. Pop-upvensters worden vaak gebruikt om advertenties weer te geven in webbrowsers.

POP3

(Post Office Protocol 3) Een interface tussen een e-mailclientprogramma en de e-mailserver. De meeste thuisgebruikers hebben een POP3-e-mailaccount, die ook wel standaard-e-mailaccount wordt genoemd.

PPPoE

(Point-to-Point Protocol Over Ethernet) Een methode voor het gebruiken van het PPP-inbelprotocol (Point-to-Point Protocol) met Ethernet als het transport.

Protocol

Een indeling (hardwarematig of softwarematig) voor de gegevenstransmissie tussen twee apparaten. Uw computer of apparaat moet het juiste protocol ondersteunen als u wilt communiceren met andere computers.

Proxy

Een computer (of de software die erop wordt uitgevoerd) die fungeert als een barrière tussen een netwerk en het internet door slechts één netwerkadres door te geven aan externe sites. Doordat de proxy alle interne computers vertegenwoordigt, worden de netwerkidenties beveiligd, terwijl er wel internettoegang wordt verschaft. Zie ook proxyserver.

Proxyserver

Een onderdeel van een firewall waarmee het internetverkeer van en naar een LAN (Local Area Network) wordt beheerd. Een proxyserver kan de prestaties verbeteren, doordat deze veelgevraagde gegevens levert (zoals een populaire webpagina) en aanvragen kan filteren en negeren die door de eigenaar als ongewenst worden beschouwd, zoals aanvragen voor ongeoorloofde toegang tot bestanden.

Prullenbak

Een gesimuleerde prullenbak voor verwijderde bestanden en mappen in Windows.

Publiceren

Een back-upbestand openbaar beschikbaar maken op internet. U hebt toegang tot gepubliceerde bestanden in de Data Backup-bibliotheek.

Q

Quarantaine

Isoleren of afzonderen. In VirusScan worden verdachte bestanden bijvoorbeeld vastgesteld en in quarantaine geplaatst, zodat deze geen schade kunnen toebrengen aan uw computer of bestanden.

R

RADIUS

(Remote Access Dial-In User Service) Een protocol dat gebruikersverificatie mogelijk maakt, doorgaans bij externe toegang. Het RADIUS-protocol is oorspronkelijk gedefinieerd voor gebruik bij servers voor inbeltoegang, maar wordt nu voor een heel gamma van verificatieomgevingen gebruikt, inclusief 802.1x-verificatie van het gedeelde geheim van WLAN-gebruikers.

Real-time scannen

Bestanden en mappen op virussen en andere activiteiten scannen wanneer deze op uw computer worden geopend.

Register

Een database waarin configuratie-informatie voor Windows wordt opgeslagen. Het bevat profielen voor elke gebruiker van de computer en informatie over de hardware, geïnstalleerde programma's en allerlei instellingen. Wanneer Windows wordt uitgevoerd, wordt deze informatie voortdurend geraadpleegd.

Roaming

Van het ene toegangspunt naar een ander gaan zonder onderbreking van de service of verbreking van de verbinding.

Rootkit

Een verzameling hulpprogramma's waarmee een gebruiker toegang op beheerdersniveau kan krijgen tot een computer of een computernetwerk. Rootkits kunnen bijvoorbeeld bestaan uit spyware en andere mogelijk ongewenste programma's die extra beveiligings- of privacyrisico's kunnen veroorzaken in uw computergegevens en persoonlijke gegevens.

Router

Een netwerkapparaat dat gegevenspakketten doorstuurt van het ene netwerk naar een ander. Routers kunnen op basis van interne routingstabellen binnenkomende pakketten lezen en besluiten hoe deze moeten worden doorgestuurd op basis van een willekeurige combinatie van bron- en doeladres en de huidige omstandigheden van het netwerkverkeer (zoals de belasting, kosten per regel en ongeldige regels). Een router wordt soms toegangspunt genoemd.

S

Scan-op-verzoek

Een scan die op verzoek wordt gestart (dat wil zeggen wanneer u de bewerking initieert). Anders dan bij real-time scans, worden scans-op-verzoek niet automatisch gestart.

Script

Een lijst met opdrachten die automatisch kunnen worden uitgevoerd (dat wil zeggen zonder tussenkomst van de gebruiker). In tegenstelling tot programma's, worden scripts meestal opgeslagen in gewone tekst en worden deze gecompileerd als ze worden uitgevoerd. Macro's en batchbestanden worden ook scripts genoemd.

Server

Een computer of programma dat verbindingen aanvaardt van andere computers of programma's en relevante antwoorden retourneert. Uw e-mailprogramma maakt bijvoorbeeld telkens verbinding met een e-mailserver als u een e-mailbericht verzendt of ontvangt.

Sleutel

Een reeks letters en cijfers voor de verificatie van de communicatie tussen twee apparaten. Beide apparaten moeten over de sleutel beschikken. Zie ook WEP, WPA, WPA2, WPA-PSK en WPA2-PSK.

Slim station

Zie USB-apparaat.

SMTP

(Simple Mail Transfer Protocol) Een TCP/IP-protocol voor het verzenden van berichten van de ene computer naar de andere in een netwerk. Dit protocol wordt op internet gebruikt voor het routeren van e-mail.

Snelkoppeling

Een bestand dat slechts de locatie van een andere bestand op uw computer bevat.

Snelle archivering

Alleen de bestanden archiveren die zijn gewijzigd sinds de vorige volledige of snelle archivering. Zie ook volledige archivering.

SSID

(Service Set Identifier) Een token (geheime sleutel) waarmee een Wi-Fi-netwerk (802.11) wordt geïdentificeerd. De SSID wordt ingesteld door de netwerkbeheerder en moet worden opgegeven door gebruikers die toegang willen krijgen tot het netwerk.

SSL

(Secure Sockets Layer) Een protocol dat door Netscape is ontwikkeld voor het verzenden van privédocumenten op internet. SSL werkt met een openbare sleutel voor het coderen van gegevens die via de SSL-verbinding worden overgebracht. URL's waarvoor een SSL-verbinding is vereist, beginnen met https in plaats van http.

Standaard-e-mailaccount

Zie POP3.

Synchroniseren

Verschillen oplossen tussen de back-up bestanden en de bestanden op uw lokale computer. U synchroniseert de bestanden wanneer de versie van het bestand in de online opslagplaats nieuwer is dan de versie van het bestand die zich op de andere computers bevindt.

Systeemherstelpunt

Een momentopname (afbeelding) van de inhoud van het geheugen van een computer of van een database. Windows maakt regelmatig herstelpunten ten tijde van belangrijke systeemgebeurtenissen (zoals wanneer een programma of stuurprogramma wordt geïnstalleerd). U kunt tevens op elk gewenst moment uw eigen herstelpunten maken en een naam geven.

SystemGuard

McAfee-waarschuwingen die onbevoegde wijzigingen op uw computer detecteren en u melden wanneer deze zich voordoen.

T

Terugzetten

Een kopie van het bestand ophalen uit de online opslagplaats of uit een archief.

Thuisnetwerk

Twee of meer computers die in een thuissituatie met elkaar zijn verbonden voor het delen van bestanden en internettoegang. Zie ook LAN.

Tijdelijk bestand

Een bestand dat in het geheugen of op schijf wordt gemaakt door het besturingssysteem of een ander programma en dat alleen tijdens een sessie wordt gebruikt en vervolgens wordt verwijderd.

TKIP

(Temporal Key Integrity Protocol) Een protocol om de zwakke plekken van WEP-beveiliging te versterken, met name bij het opnieuw gebruiken van coderingssleutels. TKIP wijzigt de tijdelijke sleutels elke 10.000 pakketten en biedt op die manier een dynamische distributiemethode die de beveiliging van het netwerk aanzienlijk verbetert. Het TKIP-(beveiligings)proces begint met een tijdelijke 128-bits sleutel die wordt gedeeld tussen clients en toegangspunten. TKIP combineert de tijdelijke sleutel met het MAC-adres van de client en voegt vervolgens een relatief grote 16-byte initialisatievector toe om de sleutel voor het coderen van de gegevens te genereren. Deze procedure garandeert dat elk station andere sleutelstromen gebruikt om de gegevens te coderen. TKIP gebruikt RC4 voor het uitvoeren van de codering.

Toegangspunt

Een netwerkapparaat (meestal een draadloze router genoemd) die wordt aangesloten op een Ethernet-hub of -switch om het fysieke servicebereik uit te breiden voor een draadloze gebruiker. Als draadloze gebruikers hun mobiele apparatuur op verschillende locaties gebruiken, gaat de transmissie over van het ene toegangspunt naar het andere, zodat connectiviteit gewaarborgd blijft.

Trefwoord

Een woord dat u kunt toewijzen aan een back-upbestand om duidelijk te maken dat het bestand hoort bij de andere bestanden met hetzelfde trefwoord. Door het toewijzen van trefwoorden wordt het eenvoudiger om bestanden te vinden die u op internet hebt gepubliceerd.

Trojaans paard

Een programma dat een legitiem programma lijkt, maar dat waardevolle bestanden kan beschadigen, de werking van uw computer onderbreken en toegang tot uw computer verlenen aan onbevoegde personen.

U

U3

(slogan: "You: Simplified, Smarter, Mobile") Een platform waarmee Windows 2000- of XP-programma's rechtstreeks vanaf een USB-station kunnen worden gestart. Het U3-initiatief is in 2004 opgericht door M-Systems en SanDisk en biedt gebruikers de mogelijkheid om U3-programma's uit te voeren op een Windows-computer zonder dat zij hiervoor gegevens of instellingen op hun computer hoeven te installeren.

URL

(Uniform Resource Locator) De standaardindeling voor internetadressen.

USB

(Universal Serial Bus) Een gestandaardiseerde seriële computerinterface waarmee u randapparatuur, zoals toetsenborden, joysticks en printers, aan uw computer kunt koppelen.

USB-station

Een klein geheugenstation dat u aansluit op de USB-poort van een computer. Een USB-station fungeert als een klein schijfstation waarmee u eenvoudig bestanden van de ene computer naar de andere kunt overzetten.

V

Verificatie

Het proces waarbij een persoon wordt geïdentificeerd, doorgaans op basis van een unieke naam en een uniek wachtwoord.

Virussen

Zichzelf vermenigvuldigende programma's waarmee uw bestanden of gegevens kunnen worden gewijzigd. Vaak lijken deze programma's afkomstig te zijn van een vertrouwde afzender of bonafide inhoud te bevatten.

Volledige archivering

Hiermee archiveert u een volledige gegevensset die is gebaseerd op de bestandstypen en locaties die u hebt ingesteld. Zie ook snelle archivering.

VPN

(Virtual Private Network) Een privé-netwerk dat is geconfigureerd binnen een openbaar netwerk zodat het de beheerfaciliteiten van het openbare netwerk kan benutten. VPN's worden door bedrijven gebruikt om WAN's (wide area network) te maken die grote geografische gebieden beslaan, om verbindingen met nevenvestigingen te leveren en om mobiele gebruikers in te laten bellen op het LAN van het bedrijf.

W

Wachtwoord

Een code (meestal bestaande uit letters en getallen) waarmee u toegang krijgt tot uw computer, een programma of een website.

Wachtwoordkluis

Een veilig opslaggebied voor uw persoonlijke wachtwoorden. Hierin kunt u wachtwoorden opslaan met de zekerheid dat geen enkele andere gebruiker (zelfs een beheerder niet) ze kan bekijken.

Wardriver

Iemand die uitgerust met een Wi-Fi-computer en speciale hardware of software door steden rijdt op zoek naar Wi-Fi (802.11)-netwerken.

Webbugs

Kleine grafische bestanden die kunnen worden ingesloten in uw HTML-pagina's en waarmee een onbevoegde bron cookies kan instellen op uw computer. Deze cookies worden vervolgens gebruikt om informatie naar de onbevoegde bronnen over te brengen. Webbugs worden ook wel webbeacons, pixeltags, doorzichtige GIF's of onzichtbare GIF's genoemd.

Webmail

Berichten die elektronisch via het internet worden verzonden en ontvangen. Zie ook e-mail.

WEP

WEP (Wired Equivalent Privacy) Een coderings- en verificatieprotocol dat is gedefinieerd in de Wi-Fi (802.11)-standaard. De eerste versies waren gebaseerd op RC4-codeertekst en vertoonden belangrijke zwakheden. WEP probeert de beveiliging te verbeteren door gegevens via radiogolven te coderen, zodat ze veilig zijn tijdens het transport van het ene eindpunt naar het andere. WEP blijkt echter niet zo veilig als men oorspronkelijk dacht.

Wi-Fi

(Wireless Fidelity) Een term waarmee de Wi-Fi Alliance 802.11-netwerken van alle mogelijke typen aanduidt.

Wi-Fi Alliance

Een organisatie die bestaat uit toonaangevende leveranciers van draadloze hardware en software. De Wi-Fi Alliance streeft ernaar alle op 802.11 gebaseerde producten te certificeren voor compatibiliteit en het gebruik van de term Wi-Fi te stimuleren als wereldwijde merknaam in alle markten voor alle mogelijke op 802.11 gebaseerde draadloze LAN-producten. De organisatie fungeert als consortium, testlaboratorium en coördinatiecentrum voor leveranciers die de groei van de industrie willen bevorderen.

Wi-Fi Certified

Getest en goedgekeurd door de Wi-Fi Alliance. Producten met de aanduiding Wi-Fi Certified worden als compatibel beschouwd, ook als ze van verschillende fabrikanten afkomstig zijn. Een gebruiker met een Wi-Fi Certified-product kan een toegangspunt van een willekeurig merk gebruiken in combinatie met clienthardware van een willekeurig ander merk, op voorwaarde dat ook deze hardware is gecertificeerd.

Witte lijst

Een lijst met websites die mogen worden bezocht omdat ze niet als frauduleus worden beschouwd.

WLAN

(Wireless Local Area Network) Een LAN (local area network) waarvoor draadloze verbindingen worden gebruikt. In een WLAN worden hoogfrequente radiogolven in plaats van kabels gebruikt voor de communicatie tussen computers.

Woordenboekaanval

Een type aanval met grof geweld waarbij gewone uitdrukkingen worden gebruikt om een wachtwoord te ontdekken.

Worm

Een zichzelf vermenigvuldigend virus dat zich in het actieve geheugen nestelt en via e-mailberichten kopieën van zichzelf kan verspreiden. Wormen vermenigvuldigen zich en gebruiken systeembronnen, waardoor de computer langzamer wordt of taken worden gestopt.

WPA

(Wi-Fi Protected Access) Een specificatiestandaard die de gegevensbeveiliging en toegangscontrole voor bestaande en toekomstige draadloze LAN-systemen aanzienlijk verbetert. WPA, dat is ontworpen om als software-upgrade te worden geïnstalleerd op bestaande hardware, is afgeleid van en compatibel met de IEEE-standaard 802.11i. Wanneer WPA correct is geïnstalleerd, biedt het gebruikers van draadloze LAN's een hoog niveau van garantie dat hun gegevens veilig zijn en dat alleen geautoriseerde gebruikers toegang hebben tot het netwerk.

WPA-PSK

Een speciale WPA-modus die is ontworpen voor particuliere gebruikers die geen sterke beveiliging op bedrijfsniveau nodig hebben en geen toegang hebben tot verificatieservers. In deze modus moet de particuliere gebruiker handmatig het initiële wachtwoord invoeren om WPA (Wi-Fi Protected Access) in de modus PSK (Pre-Shared Key, oftewel vooraf-gedeelde sleutel) te activeren. Vervolgens moet de wachtzin op elke draadloze computer en elk draadloos toegangspunt regelmatig worden gewijzigd. Zie ook WPA2-PSK en TKIP.

WPA2

Een update van de beveiligingsstandaard WPA, gebaseerd op de 802.11i IEEE-standaard.

WPA2-PSK

Een speciale WPA-modus die vergelijkbaar is met WPA-PSK en is gebaseerd op de WPA2-standaard. Een veelvoorkomende eigenschap van WPA2-PSK is dat apparaten vaak meerdere coderingsmodi (bijvoorbeeld AES, TKIP) tegelijkertijd ondersteunen, terwijl oudere apparaten doorgaans slechts één enkele coderingsmodus tegelijk ondersteunen (dat wil zeggen dat alle clients dezelfde coderingsmodus moeten gebruiken).

Z

Zwarte lijst

Bij anti-phising: een lijst met websites die als frauduleus worden beschouwd.

McAfee

McAfee, Inc. is gevestigd in Santa Clara, Californië en is de wereldwijde marktleider op het gebied van inbraakpreventie en beveiligingsrisicobeheer. McAfee levert proactieve, bewezen oplossingen en diensten waarmee systemen en netwerken over de hele wereld worden beveiligd. Dankzij de ongeëvenaarde expertise op het gebied van beveiliging en het continue streven naar innovatie geeft McAfee thuisgebruikers, bedrijven, de publieke sector en serviceproviders de mogelijkheid om aanvallen te weren, uitval te voorkomen en doorlopend de beveiliging te controleren en te verbeteren.

Copyright

Copyright © 2007-2008, McAfee, Inc. Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, uitgezonden, overgezet, opgeslagen in een geautomatiseerd gegevensbestand, of vertaald in om het even welke taal in enige vorm of op enige wijze, zonder schriftelijke toestemming van McAfee, Inc. McAfee en andere handelsmerken die hierin worden genoemd, zijn gedeponeerde handelsmerken of handelsmerken van McAfee, Inc. en/of dochtermaatschappijen in de VS en/of andere landen. McAfee Red in verband met beveiliging is een kenmerk van producten van het McAfee-merk. Alle overige gedeponeerde en niet-gedeponeerde handelsmerken en materialen waarop auteursrechten berusten, zijn het eigendom van hun respectieve eigenaren.

HANDELSMERKEN

AVERT, EPO, EPOLICY ORCHESTRATOR, FLASHBOX, FOUNDSTONE, GROUPSHIELD, HERCULES, INTRUSHIELD, INTRUSION INTELLIGENCE, LINUXSHIELD, MANAGED MAIL PROTECTION, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, MCAFEE.COM, NETSHIELD, PORTALSHIELD, PREVENTSYS, PROTECTION-IN-DEPTH STRATEGY, PROTECTIONPILOT, SECURE MESSAGING SERVICE, SECURITYALLIANCE, SITEADVISOR, THREATSCAN, TOTAL PROTECTION, VIREX, VIRUSSCAN.

Licentie

KENNISGEVING VOOR ALLE GEBRUIKERS: LEES DE JURIDISCHE OVEREENKOMST BEHOREND BIJ DE LICENTIE DIE U HEBT AANGESCHAFT ZORGVULDIG DOOR. DEZE OVEREENKOMST BEVAT DE ALGEMENE BEPALINGEN EN VOORWAARDEN VOOR HET GEBRUIK VAN DE SOFTWARE ONDER LICENTIE. ALS U NIET WEET WELK TYPE LICENTIE U HEBT AANGESCHAFT, RAADPLEEGT U DE VERKOOPDOCUMENTEN EN ANDERE GERELATEERDE LICENTIE- OF INKOOPORDERDOCUMENTEN DIE BIJ HET SOFTWAREPAKKET ZIJN GELEVERD OF DIE U AFZONDERLIJK HEBT ONTVANGEN ALS ONDERDEEL VAN DE AANKOOP (IN DE VORM VAN EEN BOEKJE, EEN BESTAND OP DE PRODUCT-CD OF EEN BESTAND BESCHIKBAAR OP DE WEBSITE VANAF WAAR U HET SOFTWAREPAKKET HEBT GEDOWNLOAD). INDIEN U NIET INSTEMT MET EEN OF MEERDERE BEPALINGEN IN DEZE OVEREENKOMST, MAG U DE SOFTWARE NIET INSTALLEREN. INDIEN VAN TOEPASSING, KUNT U HET PRODUCT RETOURNEREN AAN MCAFEE, INC. OF TERUGBRENGEN NAAR DE PLAATS WAAR U DIT HEBT AANGESCHAFT, WAARNA HET VOLLEDIGE AANKOOPBEDRAG ZAL WORDEN GERESTITUEERD.

HOOFDSTUK 3 2

Klant- en technische ondersteuning

SecurityCenter stelt u op de hoogte van kritieke en niet-kritieke beveiligingsproblemen zodra deze worden vastgesteld. Voor kritieke beveiligingsproblemen is onmiddellijk actie vereist omdat deze uw beveiligingsstatus in gevaar brengen (de kleur wordt gewijzigd in rood). Voor niet-kritieke problemen is geen onmiddellijke actie vereist; deze kunnen de beveiligingsstatus in gevaar brengen, maar dat hoeft niet het geval te zijn (dit is afhankelijk van het type probleem). Als u een groene beveiligingsstatus wilt bereiken, moet u alle kritieke problemen oplossen en alle niet-kritieke problemen oplossen of negeren. Als u hulp nodig hebt bij het analyseren van beveiligingsproblemen, kunt u McAfee Virtual Technician uitvoeren. Raadpleeg de Help van McAfee Virtual Technician voor meer informatie over McAfee Virtual Technician.

Als u de beveiligingssoftware hebt gekocht bij een partner van of een andere leverancier dan McAfee, moet u via uw webbrowser naar www.mcafeehelp.com gaan. Selecteer vervolgens onder Partner Links de partner of leverancier om toegang te krijgen tot McAfee Virtual Technician.

Opmerking: voor het installeren en uitvoeren van McAfee Virtual Technician moet u zich bij de computer aanmelden als Windows-beheerder. Als u dit niet doet, kunnen eventuele problemen mogelijk niet door MVT worden opgelost. Raadpleeg Windows Help voor informatie over het aanmelden als Windows-beheerder. In Windows Vista™ krijgt u een waarschuwing als u MVT uitvoert. Klik op **Accepteren** als dit gebeurt. Virtual Technician werkt niet in combinatie met Mozilla® Firefox.

In dit hoofdstuk

McAfee Virtual Technician gebruiken	204
Ondersteuning en downloads	205

McAfee Virtual Technician gebruiken

Virtual Technician verzamelt informatie over uw SecurityCenter-programma's als een persoonlijke medewerker van de technische ondersteuning, zodat deze informatie kan worden gebruikt om beveiligingsproblemen op uw computer op te lossen. Als u Virtual Technician uitvoert, controleert het programma of de SecurityCenter-programma's correct werken. Als er problemen worden vastgesteld, stelt Virtual Technician u voor om deze voor u op te lossen of kunt u hierover meer gedetailleerde informatie krijgen. Na deze controle worden door Virtual Technician de resultaten van de analyse weergegeven en hebt u de mogelijkheid om aanvullende technische ondersteuning te krijgen van McAfee als dit gewenst is.

Virtual Technician verzamelt geen persoonlijke informatie aan de hand waarvan uw identiteit kan worden vastgesteld, waardoor de veiligheid en de integriteit van uw computer en bestanden gewaarborgd zijn.

Opmerking: klik op het pictogram **Help** in Virtual Technician voor meer informatie over het programma.

Virtual Technician starten

Virtual Technician verzamelt informatie over uw SecurityCenter-programma's, zodat deze informatie kan worden gebruikt om beveiligingsproblemen op uw computer op te lossen. Deze informatie bevat geen persoonlijke gegevens waarmee u kunt worden geïdentificeerd, zodat uw privacy is gewaarborgd.

- 1 Klik op **McAfee Virtual Technician** onder **Algemene taken**.
- 2 Volg de instructies voor het downloaden en uitvoeren van Virtual Technician op het scherm op.

Ondersteuning en downloads

Raadpleeg de volgende tabellen voor de sites van Ondersteuning en downloads (waaronder gebruikershandleidingen) van McAfee in uw land.

Ondersteuning en downloads

Land	Ondersteuning van McAfee	Downloads van McAfee
Australië	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brazilië	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Canada (Engels)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Canada (Frans)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
China (chn)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
China (tw)	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Tsjechische Republiek	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Denemarken	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Finland	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
Frankrijk	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Duitsland	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Groot-Brittannië	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
Italië	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Japan	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
Korea	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
Mexico	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
Noorwegen	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
Polen	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp

Portugal	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
Spanje	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Zweden	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Turkije	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
Verenigde Staten	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

Gebruikershandleidingen voor McAfee Total Protection

Land	McAfee-gebruikershandleidingen
Australië	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brazilië	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Canada (Engels)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
Canada (Frans)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
China (chn)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
China (tw)	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Tsjechische Republiek	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Denemarken	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
Frankrijk	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Duitsland	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Groot-Brittannië	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
Nederland	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
Italië	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf

Korea	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Mexico	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Noorwegen	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Polen	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
Spanje	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Zweden	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Turkije	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
Verenigde Staten	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

Gebruikershandleidingen voor McAfee Internet Security

Land	McAfee-gebruikershandleidingen
Australië	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brazilië	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Canada (Engels)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
Canada (Frans)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
China (chn)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
China (tw)	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Tsjechische Republiek	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Denemarken	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
Frankrijk	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf

Duitsland	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf
Groot-Brittannië	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Nederland	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Italië	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Mexico	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Noorwegen	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Polen	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
Spanje	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Zweden	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Turkije	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
Verenigde Staten	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

Gebruikershandleidingen voor McAfee VirusScan Plus

Land	McAfee-gebruikershandleidingen
Australië	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brazilië	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Canada (Engels)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
Canada (Frans)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
China (chn)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
China (tw)	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf

Tsjechische Republiek	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf
Denemarken	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
Frankrijk	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Duitsland	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Groot-Brittannië	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Nederland	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Italië	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Mexico	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Noorwegen	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Polen	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
Spanje	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Zweden	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Turkije	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
Verenigde Staten	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

Gebruikershandleidingen voor McAfee VirusScan

Land	McAfee-gebruikershandleidingen
Australië	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brazilië	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf

Canada (Engels)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf
Canada (Frans)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
China (chn)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
China (tw)	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Tsjechische Republiek	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Denemarken	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fin/VS_userguide_2008.pdf
Frankrijk	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Duitsland	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Groot-Brittannië	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Nederland	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Italië	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Mexico	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Noorwegen	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
Polen	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
Spanje	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Zweden	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Turkije	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
Verenigde Staten	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

Raadpleeg de volgende tabel voor het McAfee Threat Center en sites met virusinformatie voor uw land.

Land	Beveiliging	Virusinformatie
Australië	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brazilië	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Canada (Engels)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Canada (Frans)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
China (chn)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
China (tw)	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Tsjechische Republiek	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Denemarken	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Finland	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
Frankrijk	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Duitsland	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Groot-Brittannië	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Nederland	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Italië	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japan	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
Korea	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Mexico	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Noorwegen	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
Polen	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo

Portugal	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
Spanje	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Zweden	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Turkije	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
Verenigde Staten	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

Raadpleeg de volgende tabel voor HackerWatch-sites in uw land.

Land	HackerWatch
Australië	www.hackerwatch.org
Brazilië	www.hackerwatch.org/?lang=pt-br
Canada (Engels)	www.hackerwatch.org
Canada (Frans)	www.hackerwatch.org/?lang=fr-ca
China (chn)	www.hackerwatch.org/?lang=zh-cn
China (tw)	www.hackerwatch.org/?lang=zh-tw
Tsjechische Republiek	www.hackerwatch.org/?lang=cs
Denemarken	www.hackerwatch.org/?lang=da
Finland	www.hackerwatch.org/?lang=fi
Frankrijk	www.hackerwatch.org/?lang=fr
Duitsland	www.hackerwatch.org/?lang=de
Groot-Brittannië	www.hackerwatch.org
Nederland	www.hackerwatch.org/?lang=nl
Italië	www.hackerwatch.org/?lang=it
Japan	www.hackerwatch.org/?lang=jp
Korea	www.hackerwatch.org/?lang=ko
Mexico	www.hackerwatch.org/?lang=es-mx
Noorwegen	www.hackerwatch.org/?lang=no
Polen	www.hackerwatch.org/?lang=pl
Portugal	www.hackerwatch.org/?lang=pt-pt
Spanje	www.hackerwatch.org/?lang=es
Zweden	www.hackerwatch.org/?lang=sv

Turkije	www.hackerwatch.org/?lang=tr
Verenigde Staten	www.hackerwatch.org

Index

8

802.11	186
802.11a.....	186
802.11b	186
802.1x.....	186

A

Aanval met grof geweld	186
Aanvullende beveiliging starten	37
ActiveX-besturingselement.....	186
Activiteiten van programma's controleren	131
Afbeeldingsfilter	186
Alle gebeurtenissen weergeven	30
Alleen uitgaande toegang toestaan vanuit het logboek voor recente gebeurtenissen	97
Alleen uitgaande toegang toestaan vanuit het logboek voor uitgaande gebeurtenissen	98
Alleen uitgaande toegang voor een programma toestaan.....	97
Alleen uitgaande toegang voor programma's toestaan.....	97
Archiveren.....	186
Automatische updates configureren.....	14
Automatische updates uitschakelen	15

B

Back-up maken.....	187
Bandbreedte	187
Beheerd netwerk.....	187
Bericht ontvangen wanneer een bestand wordt verzonden	182
Bestanden delen	178
Bestanden delen en versturen	177
Bestanden en mappen vernietigen	149
Bestanden naar andere computers verzenden	181
Bestanden, mappen en schijven vernietigen.....	149
Bestandsfragmenten	187
Beveiliging van expresberichten starten.....	39
Beveiliging via Scripts scannen starten.....	38
Beveiliging via SystemGuards inschakelen	49

Beveiligingsniveau instellen op Open ...	84
Beveiligingsniveau instellen op Standaard	83
Beveiligingsniveau instellen op Stealth ..	82
Beveiligingsniveau instellen op Strikt....	82
Beveiligingsniveau instellen op Vergrendelen	81
Beveiligingsniveau instellen op Vertrouwend	83
Beveiligingsniveaus van Firewall beheren	80
Beveiligingsproblemen automatisch herstellen	18
Beveiligingsproblemen handmatig herstellen	19
Beveiligingsproblemen negeren	20
Beveiligingsproblemen oplossen 8, 18, 167	
Beveiligingsproblemen oplossen of negeren	8, 17
Bewaakte bestandstypen	187
Bewaakte locaties	187
Bibliotheek.....	187
Browser	187

C

Cache.....	187
Client.....	187
Codering	188
Codetekst	188
Compressie	188
Computer beveiligen tijdens het opstarten	87
Computerregistratie-informatie ophalen	126
Computers op het netwerk niet meer vertrouwen	161
Computerverbindingen beheren	111
Computerverbindingen verbieden	116
Computerverbindingen vertrouwen....	112
Controleren op updates.....	14, 15
Cookie	188
Copyright	201

D

DAT.....	188
De bandbreedte van programma's controleren.....	131

- De beveiligingscategorieën begrijpen. 7, 9, 29
- De beveiligingsservices begrijpen 10
- De beveiligingsstatus begrijpen 7, 8, 9
- De beveiligingsstatus van een computer controleren 164
- De computer defragmenteren 141
- De computer opschonen 137, 139
- De computer scannen 34, 59, 60
- De controle van de beveiligingsstatus van een computer stoppen 164
- De HackerWatch-zelfstudie starten 134
- De instellingen van de beveiligingsstatus van Firewall configureren 89
- De instellingen voor het gebeurtenislogboek configureren 122
- De naam van het netwerk wijzigen 157, 175
- De netwerkinformatie van een computer ophalen 127
- De toegang tot een bestaande poort voor een systeemservice blokkeren 107
- De toegang tot internet blokkeren vanuit het logboek voor recente gebeurtenissen 100
- De weergave-eigenschappen van een apparaat wijzigen 166
- Delen 188
- Denial of Service (DoS) 188
- Dialer 188
- DNS 189
- DNS-server 189
- Domein 189
- Draadloze adapter 189
- Draadloze PCI-adapterkaarten 189
- Draadloze USB-adapterkaart 189
- E**
- EasyNetwork instellen 171
- EasyNetwork openen 171
- Een apparaat beheren 165
- Een beheerd netwerk instellen 155
- Een beschikbare netwerkprinter installeren 184
- Een bestand delen 178
- Een bestand naar een andere computer verzenden 181
- Een bestand van een andere computer accepteren 181, 182
- Een beveiligingsprobleem negeren 20
- Een computer blokkeren vanuit het logboek voor gebeurtenissen van het inbraakdetectiesysteem 120
- Een computer blokkeren vanuit het logboek voor inkomende gebeurtenissen 119
- Een computer traceren vanuit het logboek voor gebeurtenissen van het inbraakdetectiesysteem 128
- Een computer traceren vanuit het logboek voor inkomende gebeurtenissen 127
- Een computer uitnodigen om lid te worden van het beheerde netwerk ... 159
- Een gecontroleerd IP-adres traceren ... 129
- Een gedeeld bestand kopiëren 179
- Een gedeeld bestand zoeken 179
- Een geluid afspelen bij waarschuwingen 26
- Een item in het netwerkoverzicht weergeven of verbergen 157
- Een netwerkcomputer geografisch traceren 126
- Een nieuwe poort voor een systeemservice openen 108
- Een poort voor een systeemservice verwijderen 110
- Een poort voor een systeemservice wijzigen 109
- Een scan plannen 47
- Een verbinding met een verboden computer verwijderen 118
- Een verboden computerverbinding bewerken 117
- Een vertrouwde computer toevoegen vanuit het logboek voor inkomende gebeurtenissen 113
- E-mail 189
- E-mailbeveiliging starten 39
- E-mailclient 189
- ESS 189
- Externe vaste schijf 189
- F**
- Firewall 190
- Firewall onmiddellijk ontgrendelen 90
- Firewall onmiddellijk vergrendelen 90
- Firewall opnieuw op de standaardwaarden instellen 91
- Firewall starten 71
- Firewall vergrendelen en problemen oplossen 90
- Firewallbescherming starten 71
- Firewallbescherming stoppen 72
- Firewall-beveiliging optimaliseren 87
- Functies van EasyNetwork 170
- Functies van Network Manager 152

- Functies van Personal Firewall68
 Functies van QuickClean136
 Functies van Shredder148
- G**
- Gebeurtenis.....190
 Gebeurtenissen van het
 inbraakdetectiesysteem weergeven..124
 Gebeurtenissen weergeven..... 18, 29
 Gedeeld geheim190
 Gedetailleerde informatie over een item
 weer te geven157
 Geïntegreerde gateway.....190
 Genegeerde problemen weergeven of
 verbergen20
 Groep met inhoudsrestricties190
- H**
- Het beveiligingsniveau van Firewall
 configureren79
 Het delen van een bestand opheffen ...178
 Het delen van een printer opheffen184
 Het inkomende en uitgaande verkeer
 analyseren.....131
 Het netwerk op afstand beheren163
 Het netwerkoverzicht openen156
 Het netwerkoverzicht vernieuwen156
 Het opstartscherm verbergen bij het
 opstarten.....26
 Hotspot.....190
- I**
- Inbraakdetectie configureren88
 Informatie over de grafiek
 Verkeersanalyse.....130
 Informatie over een programma
 opvragen vanuit het logboek voor
 uitgaande gebeurtenissen103
 Informatie over internetbeveiliging133
 Informatie over pictogrammen van
 Network Manager.....153
 Informatie over programma's102
 Informatie over programma's raadplegen
 102
 Informatie over typen lijsten met
 vertrouwde items56
 Informatie over typen SystemGuards51
 Informatie over waarschuwingen74
 Informatieve waarschuwingen beheren 77
 Informatieve waarschuwingen verbergen
 78
 Informatiewaarschuwingen weergeven en
 verbergen24
- Informatiewaarschuwingen weergeven of
 verbergen.....24
 Informatiewaarschuwingen weergeven of
 verbergen bij het spelen van spelletjes
 25
 Inkomende gebeurtenissen weergeven
 123
 Inleiding.....3
 Instellingen voor pingaanvragen
 configureren.....88
 Internet190
 Internettoegang voor programma's
 blokkeren.....99
 Internettoegang voor programma's
 toestaan94
 Internetverkeer controleren130
 Internetverkeer traceren.....126
 Intranet191
 IP-adres191
 IP-spoofing191
- K**
- Klant- en technische ondersteuning...203
 Knooppunt.....191
- L**
- LAN.....191
 Launchpad (platform).....191
 Licentie.....202
 Lid worden van een beheerd netwerk 159,
 172, 176
 Lid worden van het beheerde netwerk 158
 Lid worden van het netwerk.....173
 Lijsten met vertrouwde items.....191
 Lijsten met vertrouwde items beheren..55
 Lijsten met vertrouwde items gebruiken
 55
 Locatie voor grondige bewaking191
 Locaties voor handmatige scans instellen
 46
 Locaties voor oppervlakkige bewaking 191
 Logbestanden, controles en analyses ..121
 Logboekregistratie.....122
- M**
- MAC (Message Authentication Code)..192
 MAC-adres192
 Machtigingen van een beheerde
 computer wijzigen165
 Man-in-het-midden-aanval192
 MAPI.....192
 McAfee201
 McAfee EasyNetwork169
 McAfee Network Manager151

- McAfee Personal Firewall.....67
 McAfee QuickClean.....135
 McAfee SecurityCenter5
 McAfee Shredder147
 McAfee Virtual Technician gebruiken .204
 McAfee VirusScan.....31
 McAfee-beveiligingssoftware installeren
 op externe computers168
 Mogelijk ongewenst programma (MOP)
192
 Mondiale internetpoortactiviteiten
 weergeven125
 Mondiale statistieken over
 beveiligingsgebeurtenissen weergeven
125
 MSN192
- N**
- Naslag185
 Netwerk192
 Netwerkoverzicht192
 Netwerkstation192
 NIC.....192
 Normale tekst.....192
- O**
- Onbetrouwbare toegangspunten193
 Ondersteuning en downloads205
 Online opslagplaats.....193
 Opties voor handmatige scans instellen
44, 45
 Opties voor real-time scannen instellen 42
 Opties voor SystemGuards configureren
50
 Overschrijding van de bufferlimiet193
- P**
- Parental Controls.....193
 Phishing.....193
 Plugin193
 Poort193
 Poorten voor systeemservices
 configureren106
 POP3193
 Pop-ups193
 PPPoE194
 Printers delen.....183
 Programmamachtigingen verwijderen 101
 Programma's en toegangsregels beheren
93
 Protocol194
 Proxy194
 Proxyserver.....194
 Prullenbak.....194
- Publiceren194
- Q**
- Quarantaine.....194
 QuickClean-taken plannen142
 QuickClean-taken verwijderen144
 QuickClean-taken wijzigen143
- R**
- RADIUS194
 Real-time scannen194
 Real-time virusbeveiliging starten34
 Real-time virusbeveiliging stoppen35
 Recente gebeurtenissen weergeven.....29,
 123
 Register195
 Roaming.....195
 Rootkit.....195
 Router.....195
- S**
- Scan-op-verzoek.....195
 Scanresultaten weergeven.....61
 Schijfdefragmentatie-taken plannen... 144
 Schijfdefragmentatie-taken verwijderen
146
 Schijfdefragmentatie-taken wijzigen... 145
 Script195
 SecurityCenter bijwerken13
 SecurityCenter gebruiken7
 SecurityCenter-functies.....6
 Server195
 Sleutel.....195
 Slim station195
 Slimme aanbevelingen alleen weergeven
86
 Slimme aanbevelingen configureren voor
 waarschuwingen85
 Slimme aanbevelingen inschakelen85
 Slimme aanbevelingen uitschakelen86
 SMTP196
 Snelkoppeling.....196
 Snelle archivering.....196
 Spywarebeveiliging starten.....38
 SSID196
 SSL196
 Standaard-e-mailaccount.....196
 Status en machtigingen controleren... 164
 Synchroniseren.....196
 Systeemherstelpunt196
 Systeemservices beheren.....105
 SystemGuard196
 SystemGuard-opties gebruiken48

T

Taken plannen	142
Terugzetten	196
Thuisnetwerk	197
Tijdelijk bestand	197
TKIP	197
Toegang tot een bestaande poort voor een systeemservice toestaan	107
Toegang verlenen tot het netwerk.....	173
Toegang voor een nieuw programma blokkeren	99
Toegang voor een programma blokkeren	99
Toegangspunt	197
Toegangsrechten voor programma's verwijderen	101
Trefwoord.....	197
Trojaans paard.....	197

U

U afmelden bij een beheerd netwerk...176	
U3	197
Uitgaande gebeurtenissen weergeven ..95, 124	
URL.....	197
USB	198
USB-station.....	198
Uw abonnement controleren	11
Uw McAfee-account beheren.....	11

V

Verboden computerverbinding toevoegen	116
Verificatie	198
Vertrouwde computerverbinding bewerken	114
Vertrouwde computerverbinding toevoegen.....	112
Vertrouwde computerverbinding verwijderen	115
Virtual Technician starten	204
Virusbeveiliging instellen.....	41, 59
VirusScan-functies	33
Virussen.....	198
Volledige archivering.....	198
Volledige schijfinhoud vernietigen	150
Volledige toegang toestaan vanuit het logboek voor recente gebeurtenissen..95	
Volledige toegang toestaan vanuit het logboek voor uitgaande gebeurtenissen	96
Volledige toegang voor een nieuw programma toestaan.....	95

Volledige toegang voor een programma toestaan	94
VPN.....	198

W

Waarschuwingen voor virusuitbraken verbergen.....	27
Waarschuwingen weergeven tijdens het spelen van games	77
Waarschuwingsopties configureren	26
Wachtwoord	198
Wachtwoordkluis	198
Wardriver	198
Webbugs	199
Webmail.....	199
WEP	199
Werken met bestanden en cookies in quarantaine	65
Werken met gedeelde printers	184
Werken met het netwerkoverzicht	156
Werken met in quarantaine geplaatste bestanden.....	64, 65
Werken met mogelijk ongewenste programma's	64
Werken met scanresultaten	63
Werken met statistieken	125
Werken met virussen en Trojaanse paarden.....	64
Werken met waarschuwingen	14, 23, 73
Wi-Fi.....	199
Wi-Fi Alliance	199
Wi-Fi Certified	199
Witte lijst	199
WLAN	199
Woordenboekaanval	199
Worm.....	200
WPA	200
WPA2	200
WPA2-PSK.....	200
WPA-PSK.....	200

Z

Zoekcriteria.....	179
Zwarte lijst	200