McAfee®

Total Protection

Gebruikershandleiding

Inhoud

HOOFDSTUK 1

McAfee Total Protection

Total Protection biedt uitgebreide virusvoorzieningen voor uw computer zodat u optimaal bent beschermd wanneer u online werkt of speelt. U kunt Total Protection gebruiken om uw computer te beschermen tegen virussen, hackers en spyware; internetverkeer te controleren op verdachte activiteiten; de privacy van uw gezin te beschermen; verdachte websites te blokkeren; en meer.

In dit hoofdstuk

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

Vereenvoudigde beveiligingsstatus	Hiermee kunt u gemakkelijk de beveiligingsstatus van de computer inspecteren, op updates controleren en beveiligingsproblemen oplossen.
Automatische updates en upgrades	SecurityCenter downloadt en installeert automatisch updates voor al uw programma´s. Wanneer er een nieuwe versie van een McAfee-programma beschikbaar is, ontvangt u die automatisch gedurende de looptijd van uw abonnement. Zo bent u er zeker van dat uw beveiliging altijd up-to-date is.
Realtimewaarschuwingen	Door middel van beveiligingswaarschuwingen wordt u op de hoogte gebracht van nieuwe virusuitbraken en veiligheidsrisico´s.

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

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.

Beveiligings-status	Beschrijving
Rood	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. 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.
Geel	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. 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.
Groen	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. In elke beveiligingscategorie worden de services vermeld die uw computer beveiligen.

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.

Klik op een categorienaam om de bijbehorende beveiligingsservices te configureren en eventuele beveiligingsproblemen weer te geven die voor deze services zijn gevonden. 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.

Beveiligingscategorie	Beschrijving
Computer en bestanden	In de categorie Computer en bestanden kunt u de volgende beveiligingsservices configureren: ▪ Virusbeveiliging ▪ Spywarebeveiliging ▪ SystemGuards ▪ Beveiliging van Windows ▪ Pc-status
Internet en netwerk	In de categorie Internet en netwerk kunt u de volgende beveiligingsservices configureren: ▪ Firewallbeveiliging ▪ Phishing-beveiliging ▪ Bescherming van de identiteit
E-mail en expresberichten	In de categorie E-mail en expresberichten kunt u de volgende beveiligingsservices configureren: ▪ E-mailvirusbeveiliging ▪ IM-virusbeveiliging ▪ E-mailspywarebeveiliging ▪ IM-spywarebeveiliging ▪ Spambeveiliging
Ouderlijk toezicht	In de categorie Ouderlijk toezicht kunt u de volgende beveiligingsservices configureren: ▪ Inhoud blokkeren

De beveiligingsservices begrijpen

Beveiligingsservices zijn de verschillende onderdelen 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, spywarebeveiliging, SystemGuards en scripts scannen. 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 Ouderlijk toezicht 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 abonnementen beheren

Bij elk beveiligingsproduct van McAfee dat u aanschaft, wordt een abonnement geleverd waarmee u het product op een bepaald aantal computers gedurende een bepaalde periode kunt gebruiken. De duur van uw abonnement hangt af van wat u hebt aangeschaft, maar begint gewoonlijk wanneer u het product activeert. Activeren is eenvoudig en gratis – u hebt alleen een internetverbinding nodig – maar is erg belangrijk, omdat u daarmee recht krijgt op regelmatige, automatische productupdates die uw computer beschermen tegen de nieuwste bedreigingen.

Activeren gebeurt normaal gesproken bij het installeren van het product, maar als u besluit te wachten (als u bijvoorbeeld geen internetverbinding hebt), hebt u 15 dagen de tijd om te activeren. Als u uw producten niet binnen 15 dagen activeert, ontvangt u geen belangrijke updates meer en worden er geen scans meer uitgevoerd. U wordt ook regelmatig gewaarschuwd (via schermmeldingen) voordat uw abonnement bijna afloopt. Zo vermijdt u hiaten in uw beveiliging door het product op tijd te verlengen of door automatische verlenging in te stellen op onze website.

Als u een koppeling in SecurityCenter ziet waarin u wordt gevraagd uw product te activeren, is uw abonnement nog niet geactiveerd. Als u de vervaldatum van uw abonnement wilt zien, bekijkt u de accountpagina.

Toegang tot uw McAfee-account

U hebt gemakkelijk toegang tot de McAfee-accountgegevens (uw accountpagina) vanuit SecurityCenter.

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

Uw product activeren

Activeren gebeurt normaal gesproken bij het installeren van uw product. Als dat niet is gebeurd, ziet u een koppeling in SecurityCenter waarin u wordt gevraagd te activeren. U krijgt regelmatig bericht hierover.

- Klik in het deelvenster SecurityCenter Home onder **SecurityCenter-informatie** op **Activeer uw abonnement**.

Tip: u kunt uw abonnement ook activeren via de waarschuwing die regelmatig verschijnt.

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**.

Uw abonnement verlengen

Vlak voordat uw abonnement afloopt, ziet u een koppeling in SecurityCenter waarin u wordt gevraagd te verlengen. U krijgt ook regelmatig bericht over een komende vervaldatum.

- Klik in het deelvenster SecurityCenter Home onder **SecurityCenter-informatie** op **Verlengen**.

Tip: u kunt uw product ook verlengen via de melding die regelmatig verschijnt. Of u gaat naar uw accountpagina waar u kunt verlengen of de functie Automatische verlenging kunt instellen.

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 geactiveerd, 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 voor het weergeven van een waarschuwing voordat updates worden gedownload of geïnstalleerd. U kunt het automatisch bijwerken ook uitschakelen.

Opmerking: als u uw McAfee-product hebt geïnstalleerd vanaf een cd, moet u het binnen 15 dagen activeren; anders ontvangt u geen belangrijke updates voor uw producten en worden er geen scans uitgevoerd.

In dit hoofdstuk

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 21) 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 13) 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**.

3 Klik op **Ja** in het bevestigingsdialoogvenster.

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

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 handtekeningbestanden 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 geactiveerd en kan daarom niet volledig worden beveiligd.	Activeer het programma op de McAfee-website.
Uw abonnement is verlopen.	Controleer uw accountstatus op de McAfee-website. Zie Uw abonnementen beheren (pagina 10) voor meer informatie.

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 27) 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 er geen Anti-Spam of Ouderlijk toezicht is 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

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 over virusuitbraken en andere beveiligingsrisico's binnen de online gemeenschap 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 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.

Beveiligingsberichten verbergen

U kunt beveiligingsberichten over het beveiligen van meerdere computers in uw thuisnetwerk verbergen. Die berichten bevatten informatie over uw abonnement, het aantal computers dat u kunt beschermen met uw abonnement en hoe u uw abonnement kunt uitbreiden om nog meer computers te beschermen.

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 het selectievakje **Virusadviezen of andere beveiligingsberichten weergeven** uit.

Tip: u kunt deze beveiligingsberichten op elk moment laten weergeven door het selectievakje **Virusadviezen of andere beveiligingsberichten weergeven** 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

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 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.

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

Uitgebreide virusbescherming

Bescherm uzelf en uw computer tegen de nieuwste beveiligingsrisico's, waaronder virussen, 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 ook bedreigingen voorkomen die via andere toegangspunten verlopen, waaronder e-mails, expresberichten en internet. Er is geen omslachtig beheer vereist.

Brongevoelige scanopties

U kunt scanopties aan uw wensen aanpassen, maar als u dat niet doet, blijft uw computer beschermd. 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.

Automatisch herstellen

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 bijvoorbeeld 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.

HOOFDSTUK 9

De computer scannen

Zelfs voordat u SecurityCenter voor het eerst start, beschermt de real-time virusbeveiliging van VirusScan 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 het instellen van scanopties Virusbeveiliging instellen (pagina 47).

VirusScan biedt een uitgebreidere verzameling scanopties voor virusbeveiliging, waarmee u regelmatig meer diepgaande scans kunt uitvoeren. U kunt een volledige, snelle, aangepaste of geplande scan uitvoeren vanuit SecurityCenter. U kunt ook tijdens uw werkzaamheden handmatige scans uitvoeren in Windows Verkenner. 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 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

Uw pc scannen

VirusScan biedt een complete verzameling scanopties voor virusbeveiliging, waaronder real-time scannen (waarmee uw pc voortdurend wordt gecontroleerd op bedreigingen), handmatig scannen vanuit Windows Verkenner en volledig, snel, aangepast of gepland scannen vanuit SecurityCenter.

Om...	Doet u het volgende...
Real-time virusbeveiliging te starten om uw computer voortdurend te laten controleren op virusactiviteit; bestanden worden telkens gescand als deze op uw computer worden geopend	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**. **Opmerking**: Real-time scannen is standaard ingeschakeld.
Een snelle scan te starten om uw computer snel op bedreigingen te controleren	1. Klik op **Scannen** in het menu Basis. 2. Klik in het deelvenster Scanopties onder Snel scannen op **Starten**.
Een volledige scan te starten om uw computer op bedreigingen te controleren	1. Klik op **Scannen** in het menu Basis. 2. Klik in het deelvenster Scanopties onder Volledig scannen op **Starten**.

Om...	Doet u het volgende...
Een aangepaste scan te starten op basis van uw eigen instellingen	1. Klik op **Scannen** in het menu Basis. 2. Klik in het deelvenster Scanopties onder Laat mij kiezen op **Starten**. 3. Een scan aanpassen door ongedaan maken of selecteren: **Alle bedreigingen in alle bestanden** **Onbekend virussen** **Archiefbestanden** **Spyware en mogelijke bedreigingen** **Trackingcookies** **Stealth-programma's** 4. Klik op **Start**.
Een handmatige scan te starten om bestanden, mappen of stations te controleren op bedreigingen	1. Open Windows Verkenner. 2. Klik met de rechtermuisknop op een bestand, een map of station en klik vervolgens op **Scannen**.

Om...	Doet u het volgende...
Een geplande scan te starten om uw computer regelmatig op bedreigingen te controleren	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**.

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.

Opmerking: zie Typen scans (pagina 41) als u meer wilt weten over scanopties.

Scanresultaten weergeven

Als een 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	1. Dubbelklik op het pictogram **Scan voltooid** in het systeemvak op de taakbalk. 2. Klik op **Details** in het deelvenster Volledige scan, Snelle scan, Aangepaste scan of Handmatige scan.
Informatie te bekijken over uw laatste scan	Dubbelklik op het pictogram **Scan voltooid** in het systeemvak op de taakbalk en bekijk informatie over uw laatste scan in het deelvenster Volledige scan, Snelle scan, Aangepaste scan of Handmatige scan.

HOOFDSTUK 10

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. VirusScan plaatst een bestand altijd in quarantaine voordat het wordt opgeschoond. Als het bestand geïnfecteerd is, wordt het in quarantaine geplaatst.

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 opschonen of in quarantaine plaatsen, wordt verdere toegang tot het bestand ontzegd. Als er trackingcookies worden vastgesteld, maar VirusScan de cookies niet kan opschonen 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

Als VirusScan een virus of een Trojaans paard in een bestand op de computer vaststelt, probeert het programma het bestand op te schonen. Als het bestand niet kan worden opgeschoond, probeert VirusScan het in quarantaine te plaatsen. Als ook dit 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 39) 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, kunt u het programma verwijderen of als vertrouwd aanmerken. Als u het programma niet herkent, raden we u aan om te overwegen het programma te verwijderen. 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.

Typen scans

VirusScan biedt een complete verzameling scanopties voor virusbeveiliging, waaronder real-time scannen (waarmee uw pc voortdurend wordt gecontroleerd op bedreigingen), handmatig scannen vanuit Windows Verkenner en de mogelijkheid om een volledige, snelle of aangepaste scan uit te voeren vanuit SecurityCenter of in te stellen wanneer geplande scans moeten worden uitgevoerd. Het scannen in SecurityCenter biedt het voordeel dat u mogelijkheden hebt om de scanopties op elk gewenst moment direct te wijzigen.

Real-time scannen:

Bij real-time virusbeveiliging wordt uw computer voortdurend gecontroleerd op virusactiviteit en worden bestanden telkens gescand als deze op uw computer worden geopend. 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.

U kunt standaardopties instellen voor real-time scannen, waaronder scannen op onbekende virussen, en controleren op bedreigingen in trackingcookies en op netwerkstations. U kunt ook gebruikmaken van bescherming voor overschrijding van de bufferlimiet, die standaard is ingeschakeld (behalve als u de 64-bits versie van het besturingsprogramma Windows Vista gebruikt). U vindt hierover meer informatie in Real-time scanopties instellen (pagina 48).

Snel scannen

Met Snel scannen kunt u controleren op bedreigende activiteiten in processen, kritieke Windows-bestanden en op andere verdachte plekken op uw computer.

Volledig scannen

Met Volledig scannen kunt u de hele computer grondig controleren op virussen, spyware en andere bedreigingen die zich ergens op uw pc bevinden.

Aangepast scannen

Met Aangepast scannen kunt u zelf instellingen kiezen om uw pc te controleren op verdachte activiteiten. De opties voor Aangepast scannen bestaan onder andere uit het controleren op bedreigingen in alle bestanden, in archiefbestanden en in cookies, naast scannen op onbekende virussen, spyware en stealth-programma's.

U kunt standaardopties instellen voor aangepast scannen, waaronder scannen op onbekende virussen, archiefbestanden en spyware, en mogelijke bedreigingen, trackingcookies en stealth-programma's. U kunt ook scannen met het gebruik van minimale computerbronnen. U vindt hierover meer informatie in Aangepaste scanopties instellen (pagina 51).

Handmatig scannen

Met Handmatig scannen kunt u bestanden, mappen en stations vanuit Windows Verkenner snel controleren op bedreigingen.

Scans 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. Zie voor meer informatie Een scan plannen (pagina 54)

Opmerking: als u wilt weten hoe u de geschiktste scanoptie voor u kunt starten, bekijkt u Uw pc scannen (pagina 32)

HOOFDSTUK 11

Aanvullende beveiliging gebruiken

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 of in uw webbrowser 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.

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

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 12

Virusbeveiliging instellen

U kunt verschillende opties instellen voor gepland, aangepast en real-time scannen. 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.

U bepaalt ook hoe VirusScan mogelijk onbevoegde of ongewenste wijzigingen op uw pc moet controleren en beheren met behulp van SystemGuards en Vertrouwde adressen. SystemGuards zorgen voor het bewaken en beheren van mogelijk niet-gemachtige 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. U kunt Vertrouwde adressen gebruiken om te bepalen wanneer u regels als vertrouwd wilt aanmerken of wilt verwijderen waarmee u bestands- of registerwijzigingen (SystemGuard) en programma- of bufferoverschrijdingen kunt opsporen. 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.

In dit hoofdstuk

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	Selecteer **Scannen op onbekende virussen**.
Cookies op te sporen	Selecteer **Trackingcookies scannen en verwijderen**.
Virussen en andere mogelijke bedreigingen vast te stellen op stations die met het netwerk verbonden zijn	Selecteer **Netwerkstations scannen**.
De computer te beschermen tegen overschrijdingen van bufferlimieten	Selecteer **Bescherming overschrijding bufferlimiet inschakelen**.
Aan te geven welke bestandstypen moeten worden gescand	Klik op **Alle bestanden (aanbevolen)** of op **Alleen programmabestanden en documenten**.

Real-time virusbeveiliging stoppen

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.

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 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 **Uit**.

3 Selecteer de optie voor het hervatten van real-time scannen in het dialoogvenster.

4 Klik op **OK**.

Aangepaste scanopties instellen

Bij aangepaste virusbeveiliging kunt u bestanden op verzoek scannen. Als u een aangepaste 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 aangepaste scans wilt wijzigen, moet u bepalen waar VirusScan tijdens een scan op controleert. U kunt bijvoorbeeld bepalen of VirusScan onbekende virussen zoekt, mogelijk ongewenste programma's zoals spyware of adware, stealth-programma's en 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 en alle netwerkstations als een aangepaste scan wordt uitgevoerd; u kunt echter de standaardlocaties geheel aan uw eisen en wensen aanpassen. U kunt bijvoorbeeld alleen kritieke pc-bestanden 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 aangepaste 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 bijvoorbeeld 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 aangepaste scans.

Opties voor aangepaste scans instellen

Via het instellen van de opties voor aangepast scannen, kunt u aanpassen welke items VirusScan zoekt tijdens een aangepaste 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. Via het instellen van de locaties voor aangepast scannen, bepaalt u ook waar VirusScan zoekt naar virussen en andere schadelijke items tijdens een aangepaste 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 Aangepast 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 aangepast scannen op en klik op **OK**.

Om...	Doet u het volgende...
Onbekende virussen en nieuwe varianten van bekende virussen vast te stellen	Selecteer **Scannen op onbekende virussen**.
Virussen in zip-bestanden en andere archiefbestanden vast te stellen en te verwijderen	Selecteer **Archiefbestanden scannen**.
Spyware, adware en andere mogelijk ongewenste programma's vast te stellen	Selecteer **Scannen op spyware en mogelijke bedreigingen**.
Cookies op te sporen	Selecteer **Trackingcookies scannen en verwijderen**.
Rootkits en stealth-programma's vast te stellen die bestaande systeembestanden van Windows kunnen wijzigen en uitbuiten	Selecteer **Scannen op verborgen programma's**.

Om...	Doet u het volgende...
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)	Selecteer **Scannen met minimale computerbronnen**.
Aan te geven welke bestandstypen moeten worden gescand	Klik op **Alle bestanden (aanbevolen)** of op **Alleen programmabestanden en documenten**.

3 Klik op **Standaardlocatie voor scannen** en selecteer of maak de selectie ongedaan van de locaties die u wilt scannen of overslaan en klik daarna op **OK**:

Om...	Doet u het volgende...
Alle bestanden en mappen op de computer te scannen	Selecteer **(Deze)Computer**.
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.

Plan scans om de gehele computer grondig te controleren op virussen en andere bedreigingen met behulp van uw standaardscanopties. Door VirusScan wordt standaard eenmaal per week een geplande scan uitgevoerd.

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-gemachtige 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 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 **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 58) 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-uitvoeringshooks	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 wijzigingen 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-opdrachten 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.

SystemGuard	Spoort de volgende items op...
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 bestuurde 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-softwaretoevoegingen	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 webbrowser kunnen beïnvloeden.
Internet Explorer-webbrowser	Onbevoegde registerwijzigingen in de Internet Explorer-webbrowser die de weergave en het gedrag van uw webbrowser kunnen beïnvloeden.

SystemGuard	Spoort de volgende items op...
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 63) 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	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. 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.

Optie	Beschrijving
SystemGuards voor Windows	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. 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.
SystemGuards voor browsers	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. 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.
Vertrouwde programma's	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.

Optie	Beschrijving
Overschrijding van limieten van vertrouwde buffers	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. 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.

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

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.
Realtime-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.
Gamebeveiliging	Hiermee verbergt u waarschuwingen over inbraakpogingen en verdachte activiteiten tijdens het spelen van schermvullende games.
Opstartbeveiliging	Bescherm uw computer tegen inbraakpogingen, ongewenste programma's en netwerkverkeer zodra u Windows® opstart.
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.
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 aangeven. Verder vindt u gedetailleerde contact- en eigenaargegevens en geografische gegevens van de bron-IP-adressen. Ook kunt u inkomend en uitgaand verkeer analyseren en de bandbreedte en activiteiten van programma's controleren.
Inbraakpreventie	Bescherm uw privacy tegen mogelijke internetbedreigingen. Met behulp van heuristische functionaliteit bieden we 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 Automatisch (met de ingeschakelde optie om programma's alleen uitgaande internettoegang te bieden) zijn automatisch ingeschakeld.

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

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

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.

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 **Nieuwe netwerkverbinding** verschijnt bijvoorbeeld als een computer waarop Firewall is geïnstalleerd, wordt aangesloten op een nieuw netwerk. U kunt het vertrouwensniveau opgeven dat u wilt toekennen aan dit nieuwe netwerk, waarna het in uw lijst met netwerken wordt weergegeven. Als Slimme aanbevelingen is ingeschakeld, worden bekende programma's automatisch 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 uigeschakeld.

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

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 Automatisch 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

Met de beveiligingsniveaus van Firewall kunt u bepalen in welke mate u waarschuwingen wit 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 Automatisch waarbij alleen uitgaande toegang is toegestaan.

Als het beveiligingsniveau is ingesteld op Automatisch 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. Hoewel groene waarschuwingen standaard zijn uitgeschakeld, verschijnen ze wanneer bekende programma's worden gedetecteerd en wordt er 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 Standaard), hoe meer opties en waarschuwingen er worden weergegeven, die u vervolgens moet afhandelen.

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

Niveau	Beschrijving
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.
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.

Niveau	Beschrijving
Automatisch	Programma's krijgen inkomende en uitgaande (volledige) internettoegang of alleen uitgaande internettoegang. Het standaardbeveiligingsniveau is Automatisch, 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.

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

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 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 Automatisch

U kunt het beveiligingsniveau van Firewall instellen op Automatisch 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 **Automatisch** 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.

Slimme aanbevelingen configureren voor waarschuwingen

U kunt Firewall instellen om waarschuwingen die worden gegenereerd als programma's proberen toegang tot internet te krijgen, toe te voegen, uit te sluiten of weer te geven. Slimme aanbevelingen bieden u hulp om te besluiten hoe u moet reageren op waarschuwingen.

Als Slimme aanbevelingen wordt toegepast (en als het beveiligingsniveau is ingesteld op Automatisch waarbij alleen uitgaande toegang is toegestaan), staat Firewall automatisch bekende programma's toe en worden mogelijk schadelijke programma's geblokkeerd.

Als Slimme aanbevelingen niet wordt toegepast, wordt internettoegang niet automatisch toegestaan of geblokkeerd en worden er ook geen aanbevelingen gedaan in de waarschuwing.

Als Slimme aanbevelingen is ingesteld op Weergeven, wordt u via een waarschuwing gevraagd om toegang te verlenen of te blokkeren en krijgt u aanbevelingen in de waarschuwing.

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 toepassen**.
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 niet toepassen**.
4. Klik op **OK**.

Slimme aanbevelingen weergeven

U kunt instellen dat Slimme aanbevelingen alleen een aanbeveling weergeeft in de waarschuwingen, zodat u kunt besluiten 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 **Slimme aanbevelingen weergeven**.
4. Klik op **OK**.

Firewall-beveiliging optimaliseren

De veiligheid van uw computer kan op vele manieren in gevaar komen. Er zijn bijvoorbeeld programma's die proberen om toegang tot internet te krijgen wanneer Windows® wordt 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. Ze kunnen ook, met behulp van het UDP-protocol, informatie naar uw computer sturen in de vorm van berichteenheden (datagrammen). Firewall beschermt uw computer tegen dit type inbraken, doordat u programma's kunt blokkeren die toegang zoeken tot internet als Windows wordt gestart. U kunt daardoor pingaanvragen blokkeren die andere gebruikers helpen om uw computer in een netwerk te detecteren, waardoor u voorkomt dat andere gebruikers informatie naar uw computer sturen in de vorm van berichteenheden (datagrammen).

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.

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 **Beveiligingsinstellingende optie Beveiliging inschakelen tijdens het starten van Windows**.
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**.

UDP-instellingen configureren

U kunt gebruikers van andere netwerkcomputers toestaan berichteenheden (datagrammen) naar uw computer te sturen, met behulp van het UDP-protocol. Dat kan echter alleen als u een systeemservicepoort hebt gesloten om dit protocol 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. In het deelvenster 'Beveiligingsniveau', onder **Beveiligingsinstellingen**, gaat u op een van de volgende manieren te werk:
   - Selecteer **UDP-tracking inschakelen** om andere computergebruikers toe te staan berichteenheden (datagrammen) naar uw computer te sturen.
   - Schakel het selectievakje **UDP-tracking inschakelen** uit om te voorkomen dat andere computergebruikers berichteenheden (datagrammen) naar uw computer sturen.
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 configuratiedeelvenster van SecurityCenter onder **Beveiligingsstatus** op **Geavanceerd**.
3. Selecteer in het deelvenster Genegeerde problemen een of meer van de volgende opties:
   - **Firewallbescherming is uitgeschakeld.**
   - **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

Vergrendelen blokkeert alle inkomende en uitgaande netwerkverbindingen, waaronder toegang tot websites, e-mail en beveiligingsupdates. Vergrendelen heeft hetzelfde effect als het loskoppelen van de netwerkkabels op uw computer. U kunt deze instelling gebruiken om open poorten te blokkeren in het deelvenster Systeemservices en 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 elk netwerk, inclusief internet, te blokkeren.

1. Klik in het deelvenster McAfee SecurityCenter onder **Algemene taken** op **Firewall vergrendelen**.
2. Klik in het deelvenster Firewall vergrendelen op **Firewall vergrendelen inschakelen**.
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 toe te staan tussen uw computer en elk netwerk, inclusief internet.

1. Klik in het deelvenster McAfee SecurityCenter onder **Algemene taken** op **Firewall vergrendelen**.
2. Klik in het deelvenster Firewall vergrendelen op **Firewall vergrendelen uitschakelen**.
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 Automatisch 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.
4. Klik op **OK**.

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

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 117)

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 toegangrechten 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 McAfeeover 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

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 de lijst **Netwerken** geregistreerd.

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

In dit hoofdstuk

Computerverbindingen

Computerverbindingen zijn de verbindingen die u legt tussen andere computers in een netwerk en uw computer. U kunt IP-adressen toevoegen, bewerken en verwijderen in de lijst **Netwerken**. Deze IP-adressen worden gekoppeld aan netwerken waaraan u een vertrouwensniveau wilt toekennen wanneer er verbinding wordt gemaakt met uw computer: Vertrouwd, Standaard en Openbaar.

Niveau	Beschrijving
Vertrouwd	Firewall staat verkeer toe van een IP-adres via elke poort op uw computer. In Firewall worden activiteiten tussen uw computer en de computer met een vertrouwd IP-adres niet gefilterd of geanalyseerd. Het eerste privénetwerk dat Firewall vindt, wordt standaard als Vertrouwd opgenomen in de lijst **Netwerken**. Een voorbeeld van een vertrouwd netwerk is een computer of meerdere computers in uw lokale of thuisnetwerk.
Standaard	Firewall controleert het verkeer van een IP-adres (maar niet van een andere computer in dat netwerk) wanneer het verbinding maakt met uw computer. Het verkeer wordt toegestaan of geblokkeerd volgens de regels in de lijst **Systemservices**. Firewall registreert verkeer en genereert waarschuwingen bij gebeurtenissen van standaard IP-adressen. Een voorbeeld van een standaard netwerk is een computer of meerdere computers in een bedrijfsnetwerk.
Openbaar	Firewall controleert het verkeer van een openbaar netwerk volgens de regels in de lijst **Systeemservices**. Een voorbeeld van een openbaar netwerk is een internetnetwerk in een café, hotel of luchthaven.

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.

Een computerverbinding toevoegen

U kunt een vertrouwde, standaard of openbare computerverbinding en het bijbehorende IP-adres toevoegen.

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. Klik in het deelvenster Firewall op **Netwerken**.
4. Klik in het deelvenster Netwerken op **Toevoegen**.
5. Als de computer is verbonden via een IPv6-netwerk, selecteert u het vakje **IPv6**.
6. Voer onder **Regel toevoegen** een van de volgende handelingen uit:
   - Selecteer **Enkelvoudig** en voer daarna het IP-adres in het vak **IP-adres** in.
   - Selecteer **Bereik** en voer vervolgens het eerste en laatste IP-adres in in de vakken **Eerste IP-adres** en **Laatste IP-adres**. Als uw computer is verbonden via een IPv6-netwerk, typt u het eerste IP-adres en de lengte van het voorvoegsel in de vakken **Eerste IP-adres** en **Lengte voorvoegsel**.
7. Voer onder **Type** een van de volgende handelingen uit:
   - Selecteer **Vertrouwd** om aan te geven dat deze computerverbinding vertrouwd is (bijvoorbeeld een computer in een thuisnetwerk).
   - Selecteer **Standaard** om aan te geven dat deze computerverbinding (en niet de andere computers in het netwerk) vertrouwd is (bijvoorbeeld een computer in en bedrijfsnetwerk).
   - Selecteer **Openbaar** om aan te geven dat deze computerverbinding openbaar is (bijvoorbeeld een computer in een internetcafé, een hotel of een luchthaven).

8 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.

9 Selecteer eventueel **Regel verloopt over** waarna u kunt invullen gedurende hoeveel dagen deze regel moet worden uitgevoerd.

10 Ook kunt u eventueel een beschrijving van de regel opgeven.

11 Klik op **OK**.

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

Een computer toevoegen vanuit het logboek voor inkomende gebeurtenissen

U kunt een vertrouwde of standaard 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 voer onder **Ik wil** een van de volgende handelingen uit:

- Klik op **Dit IP-adres toevoegen als Vertrouwd** om deze computer als Vertrouwd toe te voegen aan uw lijst **Netwerken**.
- Klik op **Dit IP-adres toevoegen als Standaard** om deze computer als Standaard toe te voegen aan uw lijst **Netwerken**.

6 Klik op **Ja** om te bevestigen.

Een computerverbinding bewerken

U kunt een vertrouwde, standaard of openbare computerverbinding en het bijbehorende IP-adres bewerken.

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. Klik in het deelvenster Firewall op **Netwerken**.
4. Selecteer in het deelvenster Netwerken een IP-adres en klik vervolgens op **Bewerken**.
5. Als de computer is verbonden via een IPv6-netwerk, selecteert u het vakje **IPv6**.
6. Voer onder **Regel bewerken** een van de volgende handelingen uit:
   - Selecteer **Enkelvoudig** en voer daarna het IP-adres in het vak **IP-adres** in.
   - Selecteer **Bereik** en voer vervolgens het eerste en laatste IP-adres in in de vakken **Eerste IP-adres** en **Laatste IP-adres**. Als uw computer is verbonden via een IPv6-netwerk, typt u het eerste IP-adres en de lengte van het voorvoegsel in de vakken **Eerste IP-adres** en **Lengte voorvoegsel**.
7. Voer onder **Type** een van de volgende handelingen uit:
   - Selecteer **Vertrouwd** om aan te geven dat deze computerverbinding vertrouwd is (bijvoorbeeld een computer in een thuisnetwerk).
   - Selecteer **Standaard** om aan te geven dat deze computerverbinding (en niet de andere computers in het netwerk) vertrouwd is (bijvoorbeeld een computer in en bedrijfsnetwerk).
   - Selecteer **Openbaar** om aan te geven dat deze computerverbinding openbaar is (bijvoorbeeld een computer in een internetcafé, een hotel of een luchthaven).
8. Selecteer eventueel **Regel verloopt over**, waarna u kunt invullen gedurende hoeveel dagen deze regel moet worden uitgevoerd.
9. Ook kunt u eventueel een beschrijving van de regel opgeven.
10. Klik op **OK**.

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

Een computerverbinding verwijderen

U kunt een vertrouwde, standaard of openbare computerverbinding en het bijbehorende IP-adres verwijderen.

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. Klik in het deelvenster Firewall op **Netwerken**.
4. Selecteer in het deelvenster Netwerken een IP-adres en klik vervolgens op **Verwijderen**.
5. Klik op **Ja** om te bevestigen.

Computerverbindingen verbieden

U kunt verboden IP-adressen toevoegen, bewerken en verwijderen in het deelvenster Verboden IP-adressen.

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

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 **Configureren**.
2. Klik in het deelvenster Internet- en netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
3. Klik in het deelvenster Firewall op **Verboden IP-adressen**.

4 Klik in het deelvenster Verboden IP-adressen op **Toevoegen**.

5 Als de computer is verbonden via een IPv6-netwerk, selecteert u het vakje **IPv6**.

6 Voer onder **Regel toevoegen** een van de volgende handelingen uit:

- Selecteer **Enkelvoudig** en voer daarna het IP-adres in het vak **IP-adres** in.
- Selecteer **Bereik** en voer vervolgens het eerste en laatste IP-adres in in de vakken **Eerste IP-adres** en **Laatste IP-adres**. Als uw computer is verbonden via een IPv6-netwerk, typt u het eerste IP-adres en de lengte van het voorvoegsel in de vakken **Eerste IP-adres** en **Lengte voorvoegsel**.

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 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 **Configureren**.

2 Klik in het deelvenster Internet- en netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.

3 Klik in het deelvenster Firewall op **Verboden IP-adressen**.

4 Klik in het deelvenster Verboden IP-adressen op **Bewerken**.

5 Als de computer is verbonden via een IPv6-netwerk, selecteert u het vakje **IPv6**.

6 Voer onder **Regel bewerken** een van de volgende handelingen uit:

- Selecteer **Enkelvoudig** en voer daarna het IP-adres in het vak **IP-adres** in.
- Selecteer **Bereik** en voer vervolgens het eerste en laatste IP-adres in in de vakken **Eerste IP-adres** en **Laatste IP-adres**. Als uw computer is verbonden via een IPv6-netwerk, typt u het eerste IP-adres en de lengte van het voorvoegsel in de vakken **Eerste IP-adres** en **Lengte voorvoegsel**.

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**.

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 **Configureren**.

2 Klik in het deelvenster Internet- en netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.

3 Klik in het deelvenster Firewall op **Verboden IP-adressen**.

4 Selecteer in het deelvenster Verboden IP-adressen een IP-adres en klik vervolgens op **Verwijderen**.

5 Klik 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. Dit logboek 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.

Voeg een IP-adres toe aan de lijst **Verboden IP-adressen** als u al het ingaande internetverkeer vanaf dat IP-adres wilt blokkeren, ongeacht of uw systeemservicepoorten open of gesloten zijn.

1 Klik in het deelvenster McAfee SecurityCenter under **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 IP-adres blokkeren**.

6 Klik 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 under **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 IP-adres blokkeren**.
6. Klik op **Ja** om te bevestigen.

HOOFDSTUK 20

Systeemservices 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 systeemservices 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 systeemservices configureren

Systeemservicepoorten kunnen geconfigureerd worden om externe toegang tot een netwerkservice op uw computer toe te staan of te blokkeren. Deze systeemservicepoorten kunnen worden geopend of gesloten voor computers die aangemerkt zijn als Vertrouwd, Standaard of Openbaar in uw lijst **Netwerken**.

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

- Veelgebruikte besturingssysteempoort 5357
- 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 netwerktoegang tot een systeemservice 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 **Configureren**.
2. Klik in het deelvenster Internet- en 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 **Bewerken**.
6. Voer een van de volgende handelingen uit:
   - Als u de poort wilt openen voor een computer op een vertrouwd, standaard of openbaar netwerk (bijvoorbeeld een thuisnetwerk, bedrijfsnetwerk of internetnetwerk), selecteert u **Vertrouwd, Standaard en Openbaar**.
   - Als u de poort wilt openen voor een computer in een standaard netwerk (bijvoorbeeld een bedrijfsnetwerk), selecteert u **Standaard (omvat Vertrouwd)**.
7. Klik op **OK**.

De toegang tot een bestaande poort voor een systeemservice blokkeren

U kunt een bestaande poort sluiten om externe netwerktoegang tot een systeemservice op uw computer 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. Klik op **Systeemservices** in het deelvenster Firewall.
4. Onder **Poort voor systeemservice openen** schakelt u het selectievakje uit naast de systeemservicepoort 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 **Configureren**.
2. Klik in het deelvenster Internet- en 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 **Systeemserviceregel toevoegen** het volgende in:
   - Naam systeemservice
   - Categorie systeemservice
   - Lokale TCP/IP-poorten
   - Lokale UDP-poorten
6. Voer een van de volgende handelingen uit:
   - Als u de poort wilt openen voor een computer op een vertrouwd, standaard of openbaar netwerk (bijvoorbeeld een thuisnetwerk, bedrijfsnetwerk of internetnetwerk), selecteert u **Vertrouwd, Standaard en Openbaar**.
   - Als u de poort wilt openen voor een computer in een standaard netwerk (bijvoorbeeld een bedrijfsnetwerk), selecteert u **Standaard (omvat Vertrouwd)**.
7. Selecteer **Netwerkactiviteit van deze poort doorsturen naar netwerkcomputers die Internetverbinding delen gebruiken** indien u de activiteitsinformatie van deze poort door wilt sturen naar een andere Windows-netwerkcomputer op het netwerk die uw internetverbinding deelt.
8. Voeg eventueel een beschrijving voor de nieuwe configuratie toe.
9. Klik op **OK**.

Opmerking: als uw computer een programma heeft die web- of FTP-serververbindingen accepteert, 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 computerverbinding toe te voegen aan de lijst **Netwerken**. Zie voor meer informatie Een 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 **Configureren**.
2. Klik in het deelvenster Internet- en netwerkconfiguratie onder **Firewallbescherming is ingeschakeld** op **Geavanceerd**.
3. Klik op **Systeemservices** in het deelvenster Firewall.
4. Klik op het selectievakje naast een systeemservice en klik vervolgens op **Bewerken**.
5. Wijzig in het deelvenster Systeemservices onder **Systeemserviceregel toevoegen** het volgende:
   - Naam systeemservice
   - Lokale TCP/IP-poorten
   - Lokale UDP-poorten
6. Voer een van de volgende handelingen uit:
   - Als u de poort wilt openen voor een computer op een vertrouwd, standaard of openbaar netwerk (bijvoorbeeld een thuisnetwerk, bedrijfsnetwerk of internetnetwerk), selecteert u **Vertrouwd, Standaard en Openbaar**.
   - Als u de poort wilt openen voor een computer in een standaard netwerk (bijvoorbeeld een bedrijfsnetwerk), selecteert u **Standaard (omvat Vertrouwd)**.
7. Selecteer **Netwerkactiviteit van deze poort doorsturen naar netwerkcomputers die Internetverbinding delen gebruiken** indien u de activiteitsinformatie van deze poort door wilt sturen naar een andere Windows-netwerkcomputer op het netwerk die uw internetverbinding deelt.
8. Voeg eventueel een beschrijving voor de gewijzigde configuratie toe.
9. 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 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

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 IP-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 IP-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. Met de Verkeersmonitor geeft u de programma's op uw computer weer die de meeste netwerkverbindingen gebruiken en u geeft de IP-adressen weer die door deze programma's zijn benaderd.

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. Met de Verkeersmonitor geeft u de programma's op uw computer weer die de meeste netwerkverbindingen gebruiken en u geeft de IP-adressen weer die door deze programma's zijn benaderd.

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

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 Anti-Spam

AntiSpam (voorheen Spamkiller genoemd) zorgt ervoor dat ongevraagde e-mail niet in uw inbox kan komen door uw inkomende e-mail te controleren en te markeren als spam (e-mails die u proberen over te halen iets te kopen) of phishing (e-mails die proberen u persoonlijke informatie te ontlokken voor een potentieel frauduleuze website). Anti-Spam filtert de spam e-mail en verplaatst het naar de map McAfee Anti-Spam.

Als uw vrienden u soms legitieme e-mail sturen die als spam verschijnt, dan kunt u ervoor zorgen dat hun e-mail niet gefilterd wordt door hun e-mailadressen toe te voegen aan de Anti-Spam vriendenlijst. U kunt ook aanpassen hoe de spam gedetecteerd wordt. U kunt bijvoorbeeld berichten agressiever filteren, specificeren waarnaar moet worden gezocht in een bericht en uw eigen filters creëren.

Anti-Spam beschermt u ook als u een mogelijk frauduleuze website wilt bezoeken via een koppeling in een e-mailbericht. Als u op een koppeling klikt naar een mogelijke frauduleuze website, wordt u doorgestuurd naar de pagina Phishing-filter. Als er websites zijn waarvan u niet wilt dat ze gefilterd worden, dan kunt u deze toevoegen aan de witte lijst (de websites in deze lijst worden niet gefilterd).

Anti-Spam werkt met verschillende e-mailprogramma´s, zoals Yahoo®, MSN®/Hotmail®, Windows® Mail en Live™ Mail, Microsoft® Outlook® en Outlook Express, en Mozilla Thunderbird™, en met verschillende e-mailaccounts, zoals POP3, POP3 Webmail en MAPI (Microsoft Exchange Server). Als u een browser gebruikt om uw e-mail te lezen, dan moet u uw webmailaccount toevoegen aan Anti-Spam. Alle andere accounts worden automatisch geconfigureerd, u hoeft ze niet aan Anti-Spam toe te voegen.

U hoeft Anti-Spam niet te configureren na de installatie. Als u echter een gevorderde gebruiker bent, kunt u de geavanceerde functies voor spam- en phishing-bescherming op uw voorkeuren afstemmen.

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

Anti-Spam-functies

Antispamfilters	Voorkomen dat ongewenste e-mail in uw Postvak In belandt. De geavanceerde filters van Anti-Spam worden automatisch geüpdatet voor al uw e-mailaccounts. U kunt ook aangepaste filters creëren zodat alle spam gefilterd wordt, en u kunt spam aan McAfee rapporteren voor analyse.
Phishing-filter	Mogelijke phishing-websites (frauduleuze websites) herkennen die om persoonlijke gegevens vragen.
Aangepaste verwerking van spam	Markeer ongevraagde e-mail als spam en verplaats het naar de map McAfee Anti-Spam of markeer legitieme e-mail als geen spam en verplaats het naar uw Postvak IN.
Vrienden	Importeer de e-mailadressen van vrienden naar de vriendenlijst zodat hun e-mailberichten niet gefilterd worden.

HOOFDSTUK 24

Spamdetectie configureren

Met Anti-Spam kunt u de manier aanpassen waarop spam wordt vastgesteld. U kunt berichten op meer agressieve wijze filteren, opgeven waarnaar in een bericht moet worden gezocht of zoeken naar bepaalde tekensets bij het analyseren van spam. U kunt ook persoonlijke filters maken om Anti-Spam nauwkeurig af te stemmen op het type bericht dat als spam wordt aangeduid. Als ongewenste e-mail met het woord hypotheek bijvoorbeeld niet wordt gefilterd, kunt u een filter toevoegen dat het woord hypotheek bevat.

Als u problemen met e-mail ondervindt, kunt u de spambeveiliging uitschakelen als onderdeel van de probleemoplossingsstrategie.

In dit hoofdstuk

Filteropties instellen

U kunt de filteropties van Anti-Spam aanpassen als u berichten op meer agressieve wijze wilt filteren, wilt opgeven hoe u spam wilt verwerken of wilt zoeken naar bepaalde tekensets bij het analyseren van spam.

Filterniveau

Met het filterniveau wordt opgegeven hoe agressief e-mail wordt gefilterd. Als spam bijvoorbeeld niet wordt gefilterd en het filterniveau is ingesteld op Gemiddeld, kunt u het wijzigen in Gemiddeld-Hoog of Hoog. Als het filterniveau echter is ingesteld op Hoog, worden alleen e-mailberichten van afzenders in de vriendenlijst geaccepteerd: alle andere berichten worden gefilterd.

Verwerking van spam

Met Anti-Spam kunt u de manier aanpassen waarop spam wordt verwerkt. U kunt spam en phishing-berichten bijvoorbeeld opslaan in specifieke mappen, de naam van het label aanpassen dat wordt weergegeven in de opdrachtregel van de spam en phishing-berichten, een maximumgrootte opgeven om te filteren en opgeven hoe vaak u de spamregels wilt bijwerken.

Tekensets

Anti-Spam kan naar specifieke tekensets zoeken bij het analyseren van spam. Tekensets worden gebruikt om een taal voor te stellen, waaronder het alfabet, cijfers en andere symbolen van de taal. Als u spam ontvangt in het Grieks, kunt u alle berichten filteren die de tekenset voor het Grieks bevatten.

Filter echter geen tekensets voor talen waarin u regelmatig legitieme e-mail ontvangt. Als u bijvoorbeeld alleen berichten wilt filteren in het Italiaans, kunt u West-Europees inschakelen, omdat Italiaans een West-Europese taal is. Als u echter legitieme e-mail ontvangt in het Engels en u West-Europees selecteert, worden ook berichten in het Engels gefilterd en in de andere talen met de West-Europese tekenset. In dit geval kunt u niet alleen berichten in het Italiaans filteren.

Opmerking: het opgeven van een tekensetfilter is voor gevorderde gebruikers.

Het filterniveau wijzigen

U kunt wijzigen hoe agressief u e-mail wilt filteren. Als bijvoorbeeld legitieme e-mailberichten worden gefilterd, kunt u het filterniveau verlagen.

1 Open het deelvenster Spambeveiliging.

Hoe?

1. Klik in het deelvenster Startpagina van SecurityCenter op **E-mail en expresberichten.**
2. In het e-mail- & IM-informatiegebied, klik op **Configuratie**.
3. Klik in het deelvenster e-mail- & IM-configuratie, onder **Spambeveiliging** op **Geavanceerd**.

2 Klik in het deelvenster Spambeveiliging op **Filteropties**.

3 Selecteer in de lijst **Een filterniveau voor spam opgeven** het gewenste niveau en klik daarna op **OK**.

Niveau	Beschrijving
Laag	De meeste e-mail wordt geaccepteerd.
Gemiddeld-Laag	Alleen overduidelijke spamberichten worden gefilterd.
Gemiddeld (aanbevolen)	E-mail wordt gefilterd op het aanbevolen niveau.
Gemiddeld-Hoog	Alle e-mail die op spam lijkt, wordt gefilterd.
Hoog	Alleen berichten van afzenders in uw vriendenlijst worden geaccepteerd.

Wijzigen hoe spam wordt verwerkt en gemarkeerd

U kunt een map opgeven om spam en phishing-berichten in op te slaan, het label [SPAM] of [PHISH] aanpassen dat wordt weergegeven in de onderwerpregel van het e-mailbericht, een maximumgrootte opgeven om te filteren en opgeven hoe vaak u de spamregels wilt bijwerken.

1 Open het deelvenster Spambeveiliging.

Hoe?

1. Klik in het deelvenster Startpagina van SecurityCenter op **E-mail en expresberichten.**
2. In het e-mail- & IM-informatiegebied, klik op **Configuratie**.
3. Klik in het deelvenster e-mail- & IM-configuratie, onder **Spambeveiliging** op **Geavanceerd**.

2 Klik in het deelvenster Spambeveiliging op **Filteropties**.

3 Selecteer de gewenste opties die hieronder staan en klik op **OK**.

Om...	Doet u het volgende...
De locatie op te geven waar spam en phishing-berichten moeten worden opgeslagen	Selecteer een map in de lijst **Ongewenste e-mail in deze map plaatsen**. De standaardmap is McAfee Anti-Spam.
De onderwerpregel van het spambericht te wijzigen	Geef in **Het onderwerp van de ongewenste e-mail markeren met** een label op dat moet worden toegevoegd aan de onderwerpregel van spamberichten. Het standaardlabel is [SPAM].
De onderwerpregel van het phishing-bericht te wijzigen	Geef in **Het onderwerp van het phishing-bericht markeren met** een label op dat moet worden toegevoegd aan de onderwerpregel van phishing-berichten. Het standaardlabel is [PHISH].
Op te geven wat de maximumgrootte van het e-mailbericht om te filteren is	Voer in **Maximale grootte opgeven voor berichten die worden gefilterd (grootte in kB)** de maximale grootte in van het e-mailbericht dat u wilt filteren.
De spamregels bij te werken	Selecteer **Regels voor spam bijwerken (in minuten)**, en voer daarna in hoe vaak u de spamregels wilt bijwerken. De aanbevolen frequentie is 30 minuten. Als u over een snelle netwerkverbinding beschikt kunt u voor een beter resultaat een hoger frequentie opgeven, bijvoorbeeld 5 minuten.
De spamregels niet bij te werken	Selecteer **Regels voor spam niet bijwerken**.

Tekensetfilters toepassen

Opmerking: het filteren van berichten met tekens van een specifieke tekenset is alleen bedoeld voor geavanceerde gebruikers.

U kunt tekensets van specifieke talen filteren. Filter echter geen tekensets voor talen waarin u regelmatig legitieme e-mail ontvangt.

1 Open het deelvenster Spambeveiliging.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **E-mail en expresberichten.**
   2. In het e-mail- & IM-informatiegebied, klik op **Configuratie**.
   3. Klik in het deelvenster e-mail- & IM-configuratie, onder **Spambeveiliging** op **Geavanceerd**.

2 Klik in het deelvenster Spambeveiliging op **Tekensets**.

3 Schakel de selectievakjes in naast de tekensets die u wilt filteren.

4 Klik op **OK**.

Persoonlijke filters gebruiken

In een persoonlijk filter geeft u op of e-mailberichten op basis van woorden of woordreeksen moeten worden toegestaan of geblokkeerd. Als een e-mailbericht een woord of een aantal woorden bevat dat in het filter is ingesteld om te worden geblokkeerd, wordt het bericht gemarkeerd als spam en blijft het in uw Postvak IN staan of wordt het verplaatst naar de map Anti-Spam van McAfee. Zie Wijzigen hoe een bericht wordt verwerkt en gemarkeerd (pagina 135) voor meer informatie over de manier waarop spam wordt afgehandeld.

Anti-Spam bevat een geavanceerd filter dat voorkomt dat er ongewenste e-mailberichten in uw Postvak IN terechtkomen. Als u echter precies wilt instellen welke berichten Anti-Spam als spam aanmerkt, kunt u een persoonlijk filter maken. Als u bijvoorbeeld een filter toevoegt met het woord hypotheek, worden berichten met dit woord door Anti-Spam gefilterd. Maak echter geen filters met veel voorkomende worden die in legitieme e-mailberichten voorkomen, omdat in dat geval zelfs berichten die geen spam zijn worden gefilterd. Nadat u een filter hebt gemaakt, kunt u het bewerken als u merkt dat het filter bepaalde spam nog steeds niet onderschept. Als u bijvoorbeeld een filter hebt gemaakt om te zoeken naar het woord viagra in het onderwerp van het bericht, maar u nog steeds berichten ontvangt die het woord viagra bevatten omdat het voorkomt in de hoofdtekst van het bericht, moet u het filter wijzigen en instellen dat ook wordt gezocht naar het woord in de hoofdtekst en niet alleen in het onderwerp.

Reguliere expressies (RegEx) zijn speciale tekens en reeksen die u ook in persoonlijke filters kunt gebruiken. McAfee raadt echter aan om alleen reguliere expressies te gebruiken als u een geavanceerde gebruiker bent. Als u niet bekend bent met reguliere expressies of u meer informatie wilt over het gebruik ervan, kunt u onderzoek doen naar reguliere expressies op het web (bezoek bijvoorbeeld http://en.wikipedia.org/wiki/Regular_expression - deze informatie is in het Engels).

Een persoonlijk filter toevoegen

U kunt filters toevoegen maken om Anti-Spam nauwkeurig af te stemmen op het type bericht dat als spam wordt aangeduid.

1. Open het deelvenster Spambeveiliging.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **E-mail en expresberichten.**
   2. In het e-mail- & IM-informatiegebied, klik op **Configuratie**.
   3. Klik in het deelvenster e-mail- & IM-configuratie, onder **Spambeveiliging** op **Geavanceerd**.

2. Klik in het deelvenster Spambeveiliging op **Persoonlijke filters**.
3. Klik op **Toevoegen.**
4. Geef op waarnaar het persoonlijke filter zoekt (pagina 140) in een e-mailbericht.
5. Klik op **OK**.

Een persoonlijk filter bewerken

U kunt bestaande filters bewerken om Anti-Spam nauwkeurig af te stemmen op het type bericht dat als spam wordt aangeduid.

1 Open het deelvenster Spambeveiliging.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **E-mail en expresberichten.**
   2. In het e-mail- & IM-informatiegebied, klik op **Configuratie**.
   3. Klik in het deelvenster e-mail- & IM-configuratie, onder **Spambeveiliging** op **Geavanceerd**.

2 Klik in het deelvenster Spambeveiliging op **Persoonlijke filters**.

3 Selecteer het filter dat u wilt bewerken en klik vervolgens op **Bewerken**.

4 Geef op waarnaar het persoonlijke filter zoekt (pagina 140) in een e-mailbericht.

5 Klik op **OK**.

Een persoonlijk filter verwijderen

U kunt filters permanent verwijderen die u niet langer wilt gebruiken.

1 Open het deelvenster Spambeveiliging.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **E-mail en expresberichten.**
   2. In het e-mail- & IM-informatiegebied, klik op **Configuratie**.
   3. Klik in het deelvenster e-mail- & IM-configuratie, onder **Spambeveiliging** op **Geavanceerd**.

2 Klik in het deelvenster Spambeveiliging op **Persoonlijke filters**.

3 Selecteer het filter dat u wilt verwijderen en klik vervolgens op **Verwijderen**.

4 Klik op **OK**.

Een persoonlijk filter opgeven

In de volgende tabel wordt beschreven waarnaar het persoonlijk filter zoekt in een e-mailbericht.

Om...	Doet u het volgende...
Op te geven welk deel van het e-mailbericht moet worden gefilterd	Klik in de lijst **E-mailonderdeel**op een item om te bepalen of het filter zoekt naar de woorden of woordreeksen in het onderwerp, de berichtteksten, de afzender, de kopteksten of de ontvanger van het bericht. Klik in de lijst **E-mailonderdeel** op een item om te bepalen of het filter zoekt naar een e-mailbericht dat de woorden of woordreeksen die u opgeeft wel of niet bevat.
De woorden of woordreeksen op te geven in uw filter	In **Woorden of zinsdelen** typt u waarnaar moet worden gezocht in een e-mailbericht. Als u bijvoorbeeld *hypotheek* opgeeft, worden alle berichten gefilterd die dit woord bevatten.
Op te geven dat het filter gebruikmaakt van reguliere expressies	Selecteer **Dit filter maakt gebruik van reguliere expressies**.
Te selecteren of e-mailberichten volgens de woorden of woordreeksen in uw filter moeten worden geblokkeerd of toegestaan	Selecteer in **Deze bewerking uitvoeren** de optie **Blokkeren** of **Toestaan** om e-mailberichten te blokkeren of toe te staan die de woorden of woordreeksen in uw filter bevatten.

Spambeveiliging uitschakelen

U kunt spambeveiliging uitschakelen en voorkomen dat e-mail wordt gefilterd door Anti-Spam.

1. Klik in het menu Geavanceerd op **Configureren**.
2. Klik in het configuratiedeelvenster op **E-mail en expresberichten**.
3. Klik onder **Spambeveiliging is ingeschakeld** op **Uit**.

Tip: denk er aan om op **Aan** te klikken onder **Spambeveiliging is ingeschakeld**, zodat u opnieuw wordt beveiligd tegen spam.

HOOFDSTUK 25

E-mail filteren

Anti-Spam onderzoekt de binnenkomende e-mail en categoriseert deze als spam (e-mails die u proberen over te halen iets te kopen) of phishing (e-mails die proberen u persoonlijke informatie te ontlokken voor een potentieel frauduleuze website). Anti-Spam duidt elk ongewenst e-mailbericht aan als spam of phishing (het label [SPAM] of [PHISH] wordt weergegeven in de onderwerpregel van het bericht), en verplaatst het bericht naar de map van McAfee Anti-Spam.

U kunt e-mail markeren als spam (of juist niet) vanaf de werkbalk van Anti-Spam, de locatie wijzigen waarnaar spamberichten worden verplaatst of het label wijzigen dat wordt weergegeven in de onderwerpregel.

U kunt ook de werkbalken van Anti-Spam uitschakelen als onderdeel van de probleemoplossingsstrategie als u problemen ondervindt met uw e-mailprogramma.

In dit hoofdstuk

Een bericht markeren vanaf de werkbalk van Anti-Spam

Wanneer u een bericht markeert als spam, wordt het onderwerp van het bericht gelabeld met [SPAM] of een eigen label naar keuze en blijft het staan in uw Postvak IN, de map van McAfee Anti-Spam (Outlook, Outlook Express, Windows Mail, Thunderbird) of de map Junk (Eudora®). Wanneer u een bericht markeert als zijnde geen spam, wordt het label van het bericht verwijderd en wordt het bericht verplaatst naar het Postvak IN.

Om een bericht te markeren in...	Selecteert u een bericht en voert u het volgende uit...
Outlook, Outlook Express, Windows Mail	Klik op **Markeren als Spam** of **Markeren als Geen spam**.
Eudora	Klik in het menu **Anti-Spam** op **Markeren als Spam** of **Markeren als Geen spam**.
Thunderbird	Wijs in de werkbalk **Anti-Spam** de optie **M** aan, wijs **Markeren als** aan en klik vervolgens op **Spam** of **Geen spam**.

De werkbalk van Anti-Spam uitschakelen

Als u Outlook, Outlook Express, Windows Mail, Eudora of Thunderbird gebruikt, kunt u de werkbalk van Anti-Spam uitschakelen.

1 Open het deelvenster Spambeveiliging.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **E-mail en expresberichten.**
   2. In het e-mail- & IM-informatiegebied, klik op **Configuratie**.
   3. Klik in het deelvenster e-mail- & IM-configuratie, onder **Spambeveiliging** op **Geavanceerd**.

2 Klik in het deelvenster Spambeveiliging op **E-mailwerkbalken**.

3 Schakel het selectievakje uit naast de werkbalk die u wilt uitschakelen.

4 Klik op **OK**.

Tip: u kunt de werkbalken van Anti-Spam op elk gewenst tijdstip opnieuw inschakelen door de bijbehorende selectievakjes in te schakelen.

HOOFDSTUK 26

Vrienden instellen

Door het verbeterde filter van Anti-Spam dat legitieme e-mailberichten herkent en toestaat, komt het zelden voor dat u het e-mailadres van uw vrienden moet toevoegen aan de vriendenlijst, of u ze nu handmatig toevoegt of uw adresboeken importeert. Als u toch het e-mailadres van een vriend toevoegt en iemand vervalst het, staat Anti-Spam berichten toe van dat e-mailadres in uw Postvak IN.

Wilt u toch uw adresboeken importeren en ze veranderen, dan moet u ze opnieuw importeren, omdat Anti-Spam uw vriendenlijst niet automatisch bijwerkt.

U kunt de vriendenlijst voor Anti-Spam ook handmatig bijwerken, of een volledig domein toevoegen als u wilt dat elke gebruiker in het domein wordt toegevoegd aan uw vriendenlijst. Als u bijvoorbeeld het domein bedrijf.com toevoegt, wordt geen e-mail die afkomstig is van deze organisatie gefilterd.

In dit hoofdstuk

Een adresboek importeren

Uw adresboeken importeren als u wilt dat Anti-Spam de e-mailadressen eruit toevoegt aan uw vriendenlijst.

1 Open het deelvenster Spambeveiliging.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **E-mail en expresberichten.**
   2. In het e-mail- & IM-informatiegebied, klik op **Configuratie**.
   3. Klik in het deelvenster e-mail- & IM-configuratie, onder **Spambeveiliging** op **Geavanceerd**.

2 Klik in het deelvenster Spambeveiliging op **Vrienden**.

3 Klik in het deelvenster Vrienden op **Importeren**.

4 Klik op het type adresboek dat u wilt importeren in de lijst **Een adresboek selecteren dat u wilt importeren**.

5 Klik op **Nu importeren**.

Vrienden handmatig instellen

U kunt uw vriendenlijst handmatig bewerken door de vermeldingen één voor één aan te passen. Als u bijvoorbeeld een e-mail ontvangt van een vriend van wie het adres zich niet in uw adresboek bevindt, kunt u het e-mailadres van uw vriend direct handmatig toevoegen. De gemakkelijkste manier om dit te doen is via de werkbalk van Anti-Spam. Als u de werkbalk van Anti-Spam niet wilt gebruiken, moet u de gegevens van uw vriend handmatig opgeven.

Een vriend toevoegen vanaf de werkbalk van Anti-Spam

Als u de e-mailprogramma's Outlook, Outlook Express, Windows Mail, Eudora™ of Thunderbird gebruikt, kunt u vrienden rechtstreeks toevoegen vanaf de werkbalk van Anti-Spam.

Om een vriend toe te voegen in...	Selecteert u een bericht en voert u het volgende uit...
Outlook, Outlook Express, Windows Mail	Klik op **Vriend toevoegen**.
Eudora	Klik in het menu **Anti-Spam** op **Vriend toevoegen**.
Thunderbird	Wijs in de werkbalk **Anti-Spam** de optie **M** aan, wijs **Markeren als** aan en klik vervolgens op **Vriend**.

Handmatig een vriend toevoegen

Als u een vriend niet rechtstreeks vanaf de werkbalk wilt toevoegen of u vergeten bent om dit te doen toen u het e-mailbericht ontving, kunt u alsnog een vriend toevoegen aan de vriendenlijst.

1 Open het deelvenster Spambeveiliging.

Hoe?

1. Klik in het deelvenster Startpagina van SecurityCenter op **E-mail en expresberichten.**
2. In het e-mail- & IM-informatiegebied, klik op **Configuratie**.
3. Klik in het deelvenster e-mail- & IM-configuratie, onder **Spambeveiliging** op **Geavanceerd**.

2 Klik in het deelvenster Spambeveiliging op **Vrienden**.

3 Klik in het deelvenster Vrienden op **Toevoegen**.

4 Typ de naam van de vriend in het vak **Naam**.

5 Selecteer **Eén e-mailadres** in de lijst **Type**.

6 Typ het e-mailadres van de vriend in het vak **E-mailadres**.

7 Klik op **OK**.

Een domein toevoegen

Voeg een volledig domein toe als u elke gebruiker binnen het domein wilt toevoegen aan de vriendenlijst. Als u bijvoorbeeld het domein bedrijf.com toevoegt, wordt geen e-mail die afkomstig is van deze organisatie gefilterd.

1 Open het deelvenster Spambeveiliging.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **E-mail en expresberichten.**
   2. In het e-mail- & IM-informatiegebied, klik op **Configuratie**.
   3. Klik in het deelvenster e-mail- & IM-configuratie, onder **Spambeveiliging** op **Geavanceerd**.

2 Klik in het deelvenster Spambeveiliging op **Vrienden**.

3 Klik in het deelvenster Vrienden op **Toevoegen**.

4 Typ de naam van de organisatie of groep in het vak **Naam**.

5 Selecteer **Volledig domein** in de lijst **Type**.

6 Typ de naam van het domein in het vak **E-mailadres**.

7 Klik op **OK**.

Een vriend bewerken

Als de gegevens van een vriend veranderen, kunt u de vriendenlijst bijwerken om te voorkomen dat Anti-Spam de van hen afkomstige berichten als spam aanduidt.

1 Open het deelvenster Spambeveiliging.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **E-mail en expresberichten.**
   2. In het e-mail- & IM-informatiegebied, klik op **Configuratie**.
   3. Klik in het deelvenster e-mail- & IM-configuratie, onder **Spambeveiliging** op **Geavanceerd**.

2 Klik in het deelvenster Spambeveiliging op **Vrienden**.

3 Selecteer de vriend die u wilt bewerken en klik vervolgens op **Bewerken**.

4 Wijzig de naam van de vriend in het vak **Naam**.

5 Typ het e-mailadres van de vriend in het vak **E-mailadres**.

6 Klik op **OK**.

Een domein bewerken

Als de gegevens van een domein veranderen, kunt u de vriendenlijst bijwerken om te voorkomen dat Anti-Spam de van het domein afkomstige berichten als spam aanduidt.

1 Open het deelvenster Spambeveiliging.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **E-mail en expresberichten.**
   2. In het e-mail- & IM-informatiegebied, klik op **Configuratie**.
   3. Klik in het deelvenster e-mail- & IM-configuratie, onder **Spambeveiliging** op **Geavanceerd**.

2 Klik in het deelvenster Spambeveiliging op **Vrienden**.

3 Klik in het deelvenster Vrienden op **Toevoegen**.

4 Wijzig de naam van de organisatie of groep in het vak **Naam**.

5 Selecteer **Volledig domein** in de lijst **Type**.

6 Typ de naam van het domein in het vak **E-mailadres**.

7 Klik op **OK**.

Een vriend verwijderen

Als u van een persoon of een domein in de vriendenlijst spam ontvangt, kunt u de persoon of het domein verwijderen uit de vriendenlijst van Anti-Spam, zodat de van de persoon of het domein afkomstige berichten opnieuw worden gefilterd.

1 Open het deelvenster Spambeveiliging.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **E-mail en expresberichten.**
   2. In het e-mail- & IM-informatiegebied, klik op **Configuratie**.
   3. Klik in het deelvenster e-mail- & IM-configuratie, onder **Spambeveiliging** op **Geavanceerd**.

2 Klik in het deelvenster Spambeveiliging op **Vrienden**.

3 Selecteer een vriend die u wilt verwijderen en klik vervolgens op **Verwijderen**.

HOOFDSTUK 27

Webmailaccounts instellen

Als u een browser gebruikt om uw e-mail te lezen, dan moet u Anti-Spam configureren om verbinding te maken met uw account en uw berichten te filteren. Om uw webmailaccount toe te voegen aan Anti-Spam, voegt u gewoon de accountinformatie toe zoals verstrekt door uw e-mailaanbieder.

Nadat u een webmailaccount heeft toegevoegd, kunt u uw accountinformatie bewerken en meer informatie krijgen over gefilterde webmail. Als u een webmailaccount niet meer gebruikt, of als u het niet wilt filteren, kunt u het verwijderen.

Anti-Spam werkt met verschillende e-mailprogramma´s, zoals Yahoo®, MSN®/Hotmail®, Windows® Mail en Live™ Mail, Microsoft® Outlook® en Outlook Express, en Mozilla Thunderbird™, en met verschillende e-mailaccounts, zoals POP3, POP3 Webmail en MAPI (Microsoft Exchange Server). POP3 is het meest voorkomende accounttype, en het is het standaardtype voor e-mail via internet. Als u een POP3-account hebt, maakt Anti-Spam direct verbinding met de e-mailserver en worden de berichten daar gefilterd voordat deze door uw webmailaccount worden opgehaald. POP3 webmail, Yahoo!, MSN/Hotmail en Windows Mail accounts maken gebruik van internet. Het filteren van POP3-webmailaccounts is vergelijkbaar met het filteren van POP3-accounts.

In dit hoofdstuk

Een webmailaccount toevoegen

Voeg een POP3 (bijvoorbeeld Yahoo), MSN/Hotmail of Windows Mail (alleen betaalde versies worden volledig ondersteund) webmailaccount toe als u de berichten in die account wilt filteren op spam.

1 Open het deelvenster Spambeveiliging.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **E-mail en expresberichten.**
   2. In het e-mail- & IM-informatiegebied, klik op **Configuratie**.
   3. Klik in het deelvenster e-mail- & IM-configuratie, onder **Spambeveiliging** op **Geavanceerd**.

2 Klik in het deelvenster Spambeveiliging op **Webmailaccounts**.

3 Klik in het deelvenster Webmailaccounts op **Toevoegen**.

4 Specificeer de accountinformatie (pagina 152) en klik vervolgens op **Volgende**.

5 Onder **Controleopties**, specificeer als Anti-Spam uw account op spam controleert (pagina 152).

6 Als u een inbelverbinding gebruikt, specificeer hoe Anti-Spam verbinding maakt met het internet (pagina 152).

7 Klik op **Voltooien**.

Een webmailaccount wijzigen

U moet uw webmailaccount-informatie bewerken als er veranderingen in uw account zijn. Bijvoorbeeld, bewerk uw webmailaccount als u uw wachtwoord wijzigt of als u wilt dat Anti-Spam vaker op spam controleert.

1 Open het deelvenster Spambeveiliging.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **E-mail en expresberichten.**
   2. In het e-mail- & IM-informatiegebied, klik op **Configuratie**.
   3. Klik in het deelvenster e-mail- & IM-configuratie, onder **Spambeveiliging** op **Geavanceerd**.

2 Klik in het deelvenster Spambeveiliging op **Webmailaccounts**.

3 Selecteer de account die u wilt wijzigen en klik vervolgens op **Bewerken**.

4 Specificeer de accountinformatie (pagina 152) en klik vervolgens op **Volgende**.

5 Onder **Controleopties**, specificeer als Anti-Spam uw account op spam controleert (pagina 152).

6 Als u een inbelverbinding gebruikt, specificeer hoe Anti-Spam verbinding maakt met het internet (pagina 152).

7 Klik op **Voltooien**.

Een webmailaccount verwijderen

Verwijder een webmailaccount als u de e-mail niet langer wilt filteren op spam. Als u account bijvoorbeeld niet meer actief is, of indien u problemen ondervindt, kunt u de account verwijderen terwijl u het probleem oplost.

1 Open het deelvenster Spambeveiliging.

   Hoe?

1. Klik in het deelvenster Startpagina van SecurityCenter op **E-mail en expresberichten.**
2. In het e-mail- & IM-informatiegebied, klik op **Configuratie**.
3. Klik in het deelvenster e-mail- & IM-configuratie, onder **Spambeveiliging** op **Geavanceerd**.

2 Klik in het deelvenster Spambeveiliging op **Webmailaccounts**.

3 Selecteer de account die u wilt verwijderen en klik vervolgens op **Verwijderen**.

Informatie over de accountinformatie voor webmail

In de volgende tabellen wordt de informatie beschreven die u moet opgeven als u webmailaccounts toevoegt of bewerkt.

Accountinformatie

Informatie	Beschrijving
Beschrijving	Beschrijf de account voor uzelf. U kunt zelf bepalen welke informatie u hier invoert.
E-mailadres	Geef het e-mailadres op van deze e-mailaccount.
Type account	Geef het type e-mailaccount op dat u toevoegt. (bijvoorbeeld POP3-webmail of MSN/Hotmail).
Server	Geef de naam op van de server die als host fungeert voor deze account. Als u de naam van de server niet weet, moet u de informatie raadplegen die u hebt ontvangen van uw internetaanbieder.
Gebruikersnaam	Geef de gebruikersnaam op voor deze e-mailaccount. Als uw e-mailadres bijvoorbeeld *gebruikersnaam*@hotmail.com is, is de gebruikersnaam waarschijnlijk *gebruikersnaam*.
Wachtwoord	Geef het wachtwoord op voor deze e-mailaccount.
Wachtwoord bevestigen	Bevestig het wachtwoord voor deze e-mailaccount.

Controleopties

Optie	Beschrijving
Controleer elke	Anti-Spam controleert deze account met het opgegeven interval (aantal minuten) op spam. Het interval moeten tussen 5 en 3600 minuten liggen.
Controleer bij het starten	Anti-Spam controleert de account elke keer dat u de computer opnieuw opstart.

Verbindingsopties

Optie	Beschrijving
Nooit inbellen	Anti-Spam brengt niet automatisch een internetverbinding voor u tot stand. U moet de inbelverbinding handmatig tot stand brengen.
Inbellen wanneer er geen verbinding beschikbaar is	Wanneer er geen internetverbinding beschikbaar is, probeert Anti-Spam verbinding te maken met de inbelverbinding die u hebt opgegeven.
Altijd inbellen bij de opgegeven verbinding	Anti-Spam probeert verbinding te maken via de inbelverbinding die u opgeeft. Als u momenteel verbonden bent via een andere inbelverbinding dan de verbinding die u opgeeft, wordt deze verbroken.
Inbellen bij deze verbinding	Geef de inbelverbinding op die door Anti-Spam wordt gebruikt om verbinding te maken met internet.
Verbinding behouden nadat het filteren is voltooid	De computer blijft verbonden met internet nadat het filteren is voltooid.

HOOFDSTUK 28

Werken met gefilterde e-mail

Bepaalde spam wordt soms mogelijk niet gedetecteerd. U kunt spam rapporteren aan McAfee als dit gebeurt. De spam wordt vervolgens geanalyseerd om filterupdates te maken.

Als u een webmailaccount gebruikt, kunt u gefilterde e-mailberichten bekijken, exporteren en verwijderen. Dit is handig als u niet zeker weet of een legitiem bericht is gefilterd, of u wilt nagaan wanneer het bericht is gefilterd.

In dit hoofdstuk

E-mailberichten rapporteren aan McAfee

U kunt e-mailberichten aan McAfee rapporteren wanneer u ze markeert als spam of geen spam, zodat we ze kunnen analyseren om filterupdates te maken.

1 Open het deelvenster Spambeveiliging.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **E-mail en expresberichten.**
   2. In het e-mail- & IM-informatiegebied, klik op **Configuratie**.
   3. Klik in het deelvenster e-mail- & IM-configuratie, onder **Spambeveiliging** op **Geavanceerd**.

2 Klik in het deelvenster Spambeveiliging op **E-mailwerkbalken**.

3 Schakel onder **Help Anti-Spam te verbeteren** de gewenste selectievakjes in of uit en klik op **OK**.

Om...	Doet u het volgende...
Een e-mailbericht te rapporteren aan McAfee wanneer u het markeert als spam	Selecteer **U markeert e-mail als spam**.
Een e-mailbericht te rapporteren aan McAfee wanneer u het markeert als geen spam	Selecteer **U markeert e-mail als 'geen spam'**.

Om...	Doet u het volgende...
Het volledige e-mailbericht, niet alleen de koptekst, naar McAfee te sturen wanneer u een e-mailbericht rapporteert als 'geen spam'.	Selecteer **Volledig e-mailbericht verzenden (niet alleen koptekst)**.

Opmerking: wanneer u een e-mailbericht als 'geen spam' rapporteert en het volledige bericht naar McAfee stuurt, wordt het bericht niet gecodeerd.

Gefilterde webmail bekijken, exporteren of verwijderen

U kunt berichten die zijn gefilterd in uw webmailaccount bekijken, exporteren of verwijderen.

1. Klik op **Rapporten en logboeken** onder **Algemene taken.**
2. Klik in het deelvenster Rapporten en logboeken op **Gefilterde webmail**.
3. Selecteer een bericht.
4. Ga op een van de volgende manieren te werk onder **Ik wil**:
   - Klik op **Weergeven** om het bericht te bekijken in uw standaard-e-mailprogramma.
   - Klik op **Exporteren** als u het bericht naar uw computer wilt kopiëren.
   - Klik op **Verwijderen** als u het bericht wilt verwijderen.

Een gebeurtenis bekijken voor gefilterde webmail

U kunt bijvoorbeeld bekijken op welke datum en op welk tijdstip e-mailberichten werden gefilterd en op welke account de berichten zijn binnengekomen.

1. Klik onder **Algemene taken** op **Recente gebeurtenissen weergeven**.
2. Klik in het deelvenster Recente gebeurtenissen op **Logboek weergeven**.
3. Vouw in het linkerdeelvenster de lijst **E-mail en expresberichten** uit en klik vervolgens op **Gebeurtenissen voor het filteren van webmail**.
4. Selecteer het logboek dat u wilt weergeven.

HOOFDSTUK 29

Phishing-beveiliging configureren

Ongevraagde mail wordt door Anti-Spam gecategoriseerd als spam (e-mail die u probeert over te halen iets te kopen) of phishing (e-mail die probeert u persoonlijke informatie te ontlokken voor een bekende of potentieel frauduleuze website). Phising-beveiliging blokkeert uw toegang tot frauduleuze websites. Als u op een koppeling in een e-mailbericht klikt naar een website waarvan bekend is of vermoed wordt dat deze frauduleus is, wordt u door Anti-Spam omgeleid naar de veilige pagina van het phising-filter.

Als er websites zijn die u niet wilt filteren, moet u deze toevoegen aan de witte lijst voor phising. U kunt ook sites in de witte lijst bewerken of hieruit verwijderen. U hoeft geen sites toe te voegen als Google®, Yahoo of McAfee, omdat deze websites niet als frauduleus worden beschouwd.

Opmerking: als u SiteAdvisor hebt geïnstalleerd, ontvangt u geen phising-beveiliging van Anti-Spam, omdat SiteAdvisor al over phising-beveiliging beschikt die vergelijkbaar is met die van Anti-Spam.

In dit hoofdstuk

Een website toevoegen aan de witte lijst

Als er websites zijn die u niet wilt filteren, moet u deze toevoegen aan de witte lijst.

1. Open het deelvenster Phising-beveiliging.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **Internet en netwerk**.
   2. Klik in het gebied met gegevens van Internet en netwerk op **Configureren**.

2. Klik in het deelvenster Phising-beveiliging op **Geavanceerd**.
3. Klik onder **Witte lijst** op **Toevoegen**.
4. Typ het adres van de website en klik op **OK**.

Sites in de witte lijst bewerken

Als u een website hebt toegevoegd aan de witte lijst en het adres van de website wordt gewijzigd, kunt u de lijst op elk gewenst moment bijwerken.

1 Open het deelvenster Phising-beveiliging.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **Internet en netwerk**.
   2. Klik in het gebied met gegevens van Internet en netwerk op **Configureren**.

2 Klik in het deelvenster Phising-beveiliging op **Geavanceerd**.

3 Selecteer de website die u wilt bijwerken onder **Witte lijst** en klik op **Bewerken**.

4 Bewerk het adres van de website en klik op **OK**.

Een website verwijderen uit de witte lijst

Als u een website hebt toegevoegd aan de witte lijst omdat u hiertoe toegang wilde hebben, maar u deze site nu wilt filteren, moet u de site verwijderen uit de witte lijst.

1 Open het deelvenster Phising-beveiliging.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **Internet en netwerk**.
   2. Klik in het gebied met gegevens van Internet en netwerk op **Configureren**.

2 Klik in het deelvenster Phising-beveiliging op **Geavanceerd**.

3 Selecteer de website die u wilt verwijderen onder **Witte lijst** en klik op **Verwijderen**.

Phishing-beveiliging uitschakelen

Als u al beschikt over phishing-software van een andere leverancier dan McAfee en er een conflict optreedt, kunt u de phishing-beveiliging van Anti-Spam uitschakelen.

1. Klik in het deelvenster Startpagina van SecurityCenter op **Internet en netwerk**.
2. Klik in het gebied met gegevens van Internet en netwerk op **Configureren**.
3. Klik onder **Phishing-beveiliging is ingeschakeld** op **Uit**.

Tip: denk er aan om op **Aan** te klikken onder **Phishing-beveiliging is ingeschakeld** als u klaar bent, zodat u wordt beveiligd tegen frauduleuze websites.

HOOFDSTUK 30

McAfee Parental Controls

Parental Controls biedt uitgebreide beveiliging voor u, uw gezinsleden, uw persoonlijke bestanden en uw computer. U kunt uzelf hiermee beveiligen tegen diefstal van uw identiteitsgegevens via het internet, de overdracht van persoonlijke gegevens blokkeren en mogelijk aanstootgevende online inhoud (waaronder afbeeldingen) filteren. U kunt ook onbevoegd surfgedrag controleren en vastleggen en het biedt veilige opslagruimte voor persoonlijke wachtwoorden.

Voordat u begint met het gebruik van Parental Controls kunt u kennismaken met enkele van de meest gebruikte functies. Meer informatie over het configureren en gebruik van deze functies vindt u in de Help van Parental Controls.

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 Ouderlijk toezicht

Parental Controls	Hiermee kunt u voor SecurityCenter-gebruikers mogelijk ongepaste afbeeldingen blokkeren, zoeken op basis van leeftijdsgeschiktheid inschakelen, groepen voor inhoudsrestricties (leeftijdsgroepen waarmee de websites en inhoud worden gedefinieerd die een gebruiker kan bekijken) configureren en tijdslimieten voor surfen op internet instellen, dat wil zeggen, op welke dagen en uren een gebruiker toegang heeft tot internet. Met de opties van Parental Controls kunt u ook de toegang tot specifieke websites beperken en toegang verlenen en blokkeren op basis van trefwoorden.
Beveiliging van persoonlijke gegevens	De verzending van vertrouwelijke of gevoelige gegevens (zoals creditcard- en bankrekeningnummers en adressen) via internet blokkeren.
Wachtwoordkluis	Wachtwoorden opslaan met de zekerheid dat geen enkele andere gebruiker (zelfs een beheerder niet) ze kan bekijken.

HOOFDSTUK 31

Uw kinderen beschermen

Als uw kinderen uw computer gebruiken, kunt u Parental Controls gebruiken om te bepalen wat een kind kan zien en doen bij het surfen op internet. U kunt bijvoorbeeld zoeken op basis van leeftijdsgeschiktheid en afbeeldingen filteren, een groep voor inhoudsrestricties kiezen en tijdslimieten voor surfen op internet instellen.

Zoeken op basis van leeftijdsgeschiktheid zorgt ervoor dat de veiligheidsfilters van bepaalde populaire zoekmachines worden ingeschakeld, zodat mogelijk ongeschikte zoekresultaten niet worden opgenomen in de lijst met zoekresultaten. Met het filteren van afbeeldingen wordt het weergeven van mogelijk ongepaste afbeeldingen geblokkeerd als een kind op internet surft. De groep voor inhoudsrestricties bepaalt het soort inhoud waartoe het kind toegang heeft, op basis van de leeftijdsgroep van het kind, en met de tijdslimieten voor surfen worden de dagen en uren ingesteld waarop het kind toegang heeft tot internet. U kunt ook bepaalde websites filteren (blokkeren of toestaan) voor alle kinderen.

Opmerking: als u Parental Controls wilt configureren om uw kinderen te beschermen, moet u zich als Windows-beheerder aanmelden op uw computer. Als u een upgrade hebt uitgevoerd van een eerdere versie van dit McAfee-product waarin met McAfee-gebruikers werd gewerkt, moet u ook zijn aangemeld als McAfee-beheerder.

In dit hoofdstuk

Websites filteren met trefwoorden

Met filteren met trefwoorden kunt u websites die mogelijk aanstootgevende woorden bevatten, blokkeren voor minderjarige gebruikers. Als filteren met trefwoorden is ingeschakeld, wordt met een standaardlijst met trefwoorden en bijbehorende regels inhoud geclassificeerd op basis van de groepen voor inhoudsrestricties waartoe gebruikers behoren. Gebruikers moeten tot een bepaalde leeftijdsgroep behoren om toegang te krijgen tot websites die bepaalde trefwoorden bevatten. Alleen leden van de groep volwassenen kunnen bijvoorbeeld websites bezoeken die het woord *porno* bevatten en alleen leden van de groep kinderen (en ouderen) kunnen websites bezoeken die het woord *drugs* bevatten (leden van de groep jonge kinderen kunnen dergelijke sites dus niet bezoeken).

U kunt echter eigen trefwoorden toevoegen aan de standaardlijst en die aan bepaalde leeftijdsgroepen koppelen. Trefwoordregels die u zelf toevoegt, hebben voorrang op regels die eventueel al zijn gekoppeld aan dat trefwoord in de standaardlijst.

Websites blokkeren op basis van trefwoorden

Als u websites wilt blokkeren wegens ongepaste inhoud, maar de precieze webadressen niet weet, kunt u de sites blokkeren op basis van trefwoorden. Voer een trefwoord in en geef dan aan welke leeftijdsgroepen websites met dit trefwoord al dan niet kunnen bezoeken.

1. Open het deelvenster Ouderlijk toezicht.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **Ouderlijk toezicht**.
   2. Klik in het gedeelte voor gegevens over ouderlijk toezicht op **Configureren**.
   3. Controleer in het deelvenster voor configuratie van ouderlijk toezicht of Ouderlijk toezicht is ingeschakeld en klik op **Geavanceerd**.

2. Klik in het deelvenster Ouderlijk toezicht op **Trefwoorden** en controleer of filteren op trefwoorden is ingeschakeld.
3. Typ een trefwoord in het vak **Zoeken naar** onder **Trefwoordlijst**.
4. Verplaats de schuifregelaar **Minimumleeftijd** om de minimumleeftijd aan te geven.
   Gebruikers in deze leeftijdsgroep en ouder kunnen websites met dit trefwoord bezoeken.
5. Klik op **OK**.

Filteren op trefwoorden uitschakelen

Filteren met trefwoorden is standaard ingeschakeld. Dit houdt in dat met een standaardlijst met trefwoorden en bijbehorende regels inhoud wordt geclassificeerd op basis van de groepen voor inhoudsrestricties waartoe gebruikers behoren. U kunt filteren op trefwoorden op elk moment uitschakelen, hoewel dit niet wordt aangeraden.

1 Open het deelvenster Ouderlijk toezicht.

Hoe?

1. Klik in het deelvenster Startpagina van SecurityCenter op **Ouderlijk toezicht**.
2. Klik in het gedeelte voor gegevens over ouderlijk toezicht op **Configureren**.
3. Controleer in het deelvenster voor configuratie van ouderlijk toezicht of Ouderlijk toezicht is ingeschakeld en klik op **Geavanceerd**.

2 Klik in het deelvenster Ouderlijk toezicht op **Trefwoorden**.

3 Klik in het deelvenster Trefwoorden op **Uit**.

4 Klik op **OK**.

Websites filteren

U kunt websites filteren (blokkeren of toestaan) voor alle gebruikers, behalve de leden van de groep volwassenen. U blokkeert een website om te voorkomen dat uw kinderen toegang tot de site krijgen als zij op internet surfen. Als een kind toegang tot een geblokkeerde website probeert te krijgen, verschijnt een bericht waarin wordt aangegeven dat de site niet toegankelijk is omdat deze met McAfee is geblokkeerd.

U kunt een website toestaan als deze standaard door McAfee is geblokkeerd, maar u uw kinderen wel toegang tot de site wilt bieden. Zie Websites filteren met trefwoorden (pagina 164) voor meer informatie over websites die standaard door McAfee worden geblokkeerd. U kunt een gefilterde website ook op elk moment bijwerken of verwijderen.

Opmerking: gebruikers (onder wie beheerders) die behoren tot de groep volwassenen, hebben toegang tot alle websites, ook tot geblokkeerde websites. Als u geblokkeerde websites wilt testen, moet u zich aanmelden als minderjarige gebruiker, maar vergeet niet de geschiedenis in uw webbrowser te verwijderen wanneer u klaar bent met testen.

Gefilterde websites verwijderen

U kunt een gefilterde website uit de lijst verwijderen als u de website niet langer wilt blokkeren of toestaan.

1. Open het deelvenster Ouderlijk toezicht.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **Ouderlijk toezicht**.
   2. Klik in het gedeelte voor gegevens over ouderlijk toezicht op **Configureren**.
   3. Controleer in het deelvenster voor configuratie van ouderlijk toezicht of Ouderlijk toezicht is ingeschakeld en klik op **Geavanceerd**.

2. Klik in het deelvenster Ouderlijk toezicht op **Gefilterde websites**.
3. Klik in het deelvenster Gefilterde websites op een item in de lijst **Gefilterde websites** en klik vervolgens op **Verwijderen**.
4. Klik op **OK**.

Een gefilterde website bijwerken

Als het adres van een website wordt gewijzigd of als u het adres onjuist hebt ingevoerd toen u de site blokkeerde of toestond, kunt u het adres bijwerken.

1 Open het deelvenster Ouderlijk toezicht.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **Ouderlijk toezicht**.
   2. Klik in het gedeelte voor gegevens over ouderlijk toezicht op **Configureren**.
   3. Controleer in het deelvenster voor configuratie van ouderlijk toezicht of Ouderlijk toezicht is ingeschakeld en klik op **Geavanceerd**.

2 Klik in het deelvenster Ouderlijk toezicht op **Gefilterde websites**.

3 Klik in het deelvenster Gefilterde websites op een item in de lijst **Gefilterde websites**, wijzig het adres van de website in het vak **http://** en klik op **Bijwerken**.

4 Klik op **OK**.

Websites toestaan

U staat een website toe om te zorgen dat alle gebruikers toegang hebben tot de site. Als u een website toestaat die standaard door McAfee is geblokkeerd, vervangt u de standaardinstelling.

1 Open het deelvenster Ouderlijk toezicht.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **Ouderlijk toezicht**.
   2. Klik in het gedeelte voor gegevens over ouderlijk toezicht op **Configureren**.
   3. Controleer in het deelvenster voor configuratie van ouderlijk toezicht of Ouderlijk toezicht is ingeschakeld en klik op **Geavanceerd**.

2 Klik in het deelvenster Ouderlijk toezicht op **Gefilterde websites**.

3 Typ in het deelvenster Gefilterde websites het adres van een website in het vak **http://** en klik vervolgens op **Toestaan**.

4 Klik op **OK**.

Tip: U kunt een website die u eerder hebt geblokkeerd, toestaan door in de lijst **Gefilterde websites** op het adres van de website te klikken en vervolgens op **Toestaan** te klikken.

Websites blokkeren

U blokkeert een website om te voorkomen dat uw kinderen toegang tot de site krijgen als zij op internet surfen. Als een kind toegang tot een geblokkeerde website probeert te krijgen, verschijnt een bericht waarin wordt aangegeven dat de site niet toegankelijk is omdat deze met McAfee is geblokkeerd.

1 Open het deelvenster Ouderlijk toezicht.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **Ouderlijk toezicht**.
   2. Klik in het gedeelte voor gegevens over ouderlijk toezicht op **Configureren**.
   3. Controleer in het deelvenster voor configuratie van ouderlijk toezicht of Ouderlijk toezicht is ingeschakeld en klik op **Geavanceerd**.

2 Klik in het deelvenster Ouderlijk toezicht op **Gefilterde websites**.

3 Typ in het deelvenster Gefilterde websites het adres van een website in het vak **http://** en klik vervolgens op **Blokkeren**.

4 Klik op **OK**.

Tip: U kunt een website die u eerder hebt toegestaan, blokkeren door in de lijst **Gefilterde websites** op het adres van de website te klikken en vervolgens op **Blokkeren** te klikken.

Tijdslimieten voor surfen op internet instellen

Als u zich zorgen maakt over onverantwoord of excessief internetgebruik van uw kinderen, kunt u passende tijdslimieten instellen voor hun surfgedrag. Als u surfen voor uw kinderen tot bepaalde tijden beperkt, kunt u ervan op aan dat die beperkingen door SecurityCenter worden gehandhaafd, ook als u niet thuis bent.

Standaard mogen kinderen 24 uur per dag en 7 dagen van de week op internet surfen. U kunt surfen echter beperken tot bepaalde uren of dagen of helemaal verbieden. Als een kind op het internet probeert te surfen tijdens een uitgesloten periode, ontvangt het een melding dat dat niet is toegestaan. Als u surfen op internet volledig verbiedt, kan het kind zich aanmelden op de computer en die gebruiken. Het kan met andere programma's werken zoals e-mailprogramma's, programma's voor expresberichten, ftp-programma's, games enzovoort, maar het kan niet op internet surfen.

Tijdslimieten voor surfen op internet instellen

Op de pagina Tijdslimieten voor internet kunt u internetactiviteiten van kinderen beperken tot bepaalde dagen en uren.

1 Open het deelvenster Gebruikersinstellingen.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **Ouderlijk toezicht**.
   2. Klik in het gedeelte voor gegevens over ouderlijk toezicht op **Configureren**.
   3. Klik in het deelvenster voor configuratie van ouderlijk toezicht op **Geavanceerd**.
   4. Klik in het deelvenster Ouderlijk toezicht op **Gebruikersinstellingen**.

2 Klik in het deelvenster Gebruikersinstellingen op een gebruikersnaam en klik vervolgens op **Bewerken**.

3 Sleep onder **Tijdslimieten voor internetten** in het dialoogvenster Gebruikersaccount bewerken met de muis om de dagen en uren op te geven gedurende welke de gebruiker niet op internet kan surfen.

4 Klik op **OK**.

De groep voor inhoudsrestricties instellen

Een gebruiker kan tot een van de volgende groepen voor inhoudrestricties behoren:

- Jong kind
- Kind
- Jongere tiener
- Oudere tiener
- Volwassene

Webinhoud wordt door Parental Controls geclassificeerd (geblokkeerd of toegestaan) op basis van de groep waartoe de gebruiker behoort. Op deze manier kunt u bepaalde websites blokkeren of toestaan voor bepaalde gebruikers binnen uw gezin. U kunt bepaalde inhoud op een website bijvoorbeeld blokkeren voor gebruikers die behoren tot de groep jonge kinderen maar dezelfde site toestaan voor gebruikers die behoren tot de groep jonge tieners. Als u strengere inhoudsrestricties voor een gebruiker wilt instellen, kunt u instellen dat de gebruiker alleen websites kan bekijken die voorkomen in de lijst **Gefilterde websites**. Zie Websites filteren (pagina 166) voor meer informatie.

Inhoudrestricties voor gebruikers instellen

Nieuwe gebruikers worden standaard toegevoegd aan de groep volwassenen. Leden van deze groep hebben toegang tot alle webinhoud. U kunt de gebruiker vervolgens toewijzen aan een andere groep voor inhoudsrestricties, op grond van de leeftijd en rijpheid van de desbetreffende persoon.

1 Open het deelvenster Gebruikersinstellingen.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **Ouderlijk toezicht**.
   2. Klik in het gedeelte voor gegevens over ouderlijk toezicht op **Configureren**.
   3. Klik in het deelvenster voor configuratie van ouderlijk toezicht op **Geavanceerd**.
   4. Klik in het deelvenster Ouderlijk toezicht op **Gebruikersinstellingen**.

2 Klik in het deelvenster Gebruikersinstellingen op een gebruikersnaam en klik vervolgens op **Bewerken**.

3 Klik in het dialoogvenster Gebruikersaccount bewerken onder **Inhoudsrestricties** op de leeftijdsgroep waaraan u de gebruiker wilt toewijzen.

   Als u wilt dat de gebruiker alleen websites in de lijst **Gefilterde websites** kan bezoeken, schakelt u het selectievakje **Deze gebruiker heeft alleen toegang tot websites uit de lijst met toegestane websites** in.

4 Klik op **OK**.

Mogelijk ongepaste webafbeeldingen filteren

Wegens de leeftijd of rijpheid van een gebruiker kunt u instellen dat mogelijk ongepaste afbeeldingen worden gefilterd (geblokkeerd of toegestaan) als de gebruiker op internet surft. U kunt bijvoorbeeld de weergave van mogelijk ongepaste afbeeldingen blokkeren op momenten dat uw jongere kinderen op internet surfen, maar de weergave ervan wel toestaan voor de oudere tieners en de volwassenen in het gezin. Standaard is het filteren van afbeeldingen uitgeschakeld voor alle leden van de groep volwassenen. Dat wil zeggen dat mogelijk ongepaste afbeeldingen worden weergegeven als de leden van deze groep op internet surfen. Zie De groep voor inhoudsrestricties instellen (pagina 169) voor meer informatie over het instellen van de leeftijdsgroep van een gebruiker.

Mogelijk ongepaste webafbeeldingen filteren

Standaard worden nieuwe gebruikers toegevoegd aan de groep volwassenen en is het filteren van afbeeldingen uitgeschakeld. Als u de weergave van mogelijk ongepaste afbeeldingen wilt blokkeren als een bepaalde gebruiker op internet surft, kunt u het filteren van afbeeldingen inschakelen. Elke mogelijk ongepaste webafbeelding wordt automatisch vervangen door een statische McAfee-afbeelding.

1 Open het deelvenster Gebruikersinstellingen.

   Hoe?

   1. Klik in het deelvenster Startpagina van SecurityCenter op **Ouderlijk toezicht**.
   2. Klik in het gedeelte voor gegevens over ouderlijk toezicht op **Configureren**.
   3. Klik in het deelvenster voor configuratie van ouderlijk toezicht op **Geavanceerd**.
   4. Klik in het deelvenster Ouderlijk toezicht op **Gebruikersinstellingen**.

2 Klik in het deelvenster Gebruikersinstellingen op een gebruikersnaam en klik vervolgens op **Bewerken**.

3 Klik op **Aan** onder **Afbeeldingsfilter** in het dialoogvenster Gebruikersaccount bewerken.

4 Klik op **OK**.

Zoeken op basis van leeftijdsgeschiktheid inschakelen

Sommige populaire zoekmachines (zoals Yahoo! en Google) bieden "veilig zoeken": een zoekinstelling die voorkomt dat er mogelijk ongepaste zoekresultaten worden opgenomen in de lijsten met resultaten. In die zoekmachines kunt u gewoonlijk instellen hoe strikt het zoekfilter moet zijn, maar u of een andere gebruiker kan deze functie op elk moment uitschakelen.

In Parental Controls is zoeken op basis van leeftijdsgeschiktheid een makkelijke manier om ervoor te zorgen dat "veilig zoeken" altijd is ingeschakeld voor een gebruiker wanneer hij een van de volgende zoekmachines gebruikt:

- Google™
- MSN®
- Windows® Live Search
- Yahoo!®

Als u zoeken op basis van leeftijdsgeschiktheid inschakelt, zorgen wij ervoor dat het filter voor veilig zoeken van de zoekmachine wordt ingeschakeld voor die gebruiker en dat het filter zo strikt mogelijk is ingesteld. Als een gebruiker het filter probeert uit te schakelen (in de voorkeurs- of geavanceerde instellingen van de zoekmachine), schakelen wij het filter automatisch weer in.

Standaard is zoeken op leeftijdsgeschiktheid ingeschakeld voor alle gebruikers, behalve voor beheerders en gebruikers in de groep Volwassenen. Zie De groep voor inhoudsrestricties instellen (pagina 169) voor meer informatie over het instellen van de leeftijdsgroep van een gebruiker.

Leeftijdsafhankelijk zoeken inschakelen

Nieuwe gebruikers worden standaard toegevoegd aan de groep volwassenen, en leeftijdsafhankelijk zoeken is uitgeschakeld. Als u er voor wilt zorgen dat optie voor "veilig zoeken" die door sommige populaire zoekmachines wordt aangeboden, wordt ingeschakeld voor een volwassen gebruiker, kunt u leeftijdsafhankelijk zoeken inschakelen.

1 Open het deelvenster Gebruikersinstellingen.

Hoe?

1. Klik in het deelvenster Startpagina van SecurityCenter op **Ouderlijk toezicht**.
2. Klik in het gedeelte voor gegevens over ouderlijk toezicht op **Configureren**.
3. Klik in het deelvenster voor configuratie van ouderlijk toezicht op **Geavanceerd**.
4. Klik in het deelvenster Ouderlijk toezicht op **Gebruikersinstellingen**.

2 Klik in het deelvenster Gebruikersinstellingen op een gebruikersnaam en klik vervolgens op **Bewerken**.

3 Klik in het venster Gebruikersaccount bewerken onder **Leeftijdsafhankelijk zoeken** op **Aan**.

4 Klik op **OK**.

HOOFDSTUK 32

Gebruikers configureren

Als u Parental Controls wilt configureren om uw kinderen te beschermen, kunt u de kinderen bepaalde machtigingen toekennen in SecurityCenter. Deze machtigingen bepalen wat een kind kan zien en doen op internet.

Standaard komen de SecurityCenter-gebruikers overeen met de Windows-gebruikers die u op uw computer hebt ingesteld. Als u echter een upgrade hebt uitgevoerd van een eerdere versie van SecurityCenter waarin McAfee-gebruikers werden gebruikt, worden uw McAfee-gebruikers en hun machtigingen behouden.

Opmerking: als u gebruikers wilt configureren, moet u zich op uw computer aanmelden als Windows-beheerder. Als u een upgrade hebt uitgevoerd van een eerdere versie van dit McAfee-product waarin met McAfee-gebruikers werd gewerkt, moet u ook zijn aangemeld als McAfee-beheerder.

In dit hoofdstuk

Werken met McAfee-gebruikers

Als u een upgrade hebt uitgevoerd van een eerdere versie van SecurityCenter waarin McAfee-gebruikers werden gebruikt, worden uw McAfee-gebruikers en hun machtigingen automatisch behouden. U kunt McAfee-gebruikers blijven configureren en beheren. McAfee raadt u echter aan om over te stappen op Windows-gebruikers. Als u bent overgestapt op Windows-gebruikers, kunt u niet meer teruggaan naar McAfee-gebruikers.

Als u McAfee-gebruikers blijft gebruiken, kunt u gebruikers toevoegen, bewerken en verwijderen en het wachtwoord van de McAfee-beheerder wijzigen en opzoeken.

Het wachtwoord van de McAfee-beheerder opzoeken

Als u het beheerderswachtwoord bent vergeten, kunt u het nog terugvinden.

1. Klik met de rechtermuisknop op het pictogram van SecurityCenter, en klik vervolgens op **Andere gebruiker**.
2. Klik in de lijst **Gebruikersnaam** op **Beheerder** en klik vervolgens op **Wachtwoord vergeten?**.
3. Typ het antwoord op uw geheime vraag in het vak **Antwoord**.
4. Klik op **Verzenden**.

Het wachtwoord van de McAfee-beheerder wijzigen

Als u er moeite mee hebt om het McAfee-beheerderswachtwoord te onthouden of vermoedt dat dit wachtwoord bekend is geworden bij derden, kunt u het wijzigen.

1. Meld u bij SecurityCenter aan als beheerder.
2. Open het deelvenster Gebruikersinstellingen.

   Hoe?

   1. Klik op **Startpagina** onder **Algemene taken**.
   2. Klik in het deelvenster Startpagina van SecurityCenter op **Ouderlijk toezicht**.
   3. Klik in het gedeelte voor gegevens over ouderlijk toezicht op **Configureren**.
   4. Klik in het deelvenster voor configuratie van ouderlijk toezicht op **Geavanceerd**.

3 Selecteer **Beheerder** onder **McAfee-gebruikersaccounts** in het deelvenster Gebruikersinstellingen en klik vervolgens op **Bewerken**.

4 Typ een nieuw wachtwoord in het vak **Nieuw wachtwoord** in het dialoogvenster Gebruikersaccount bewerken en typ het vervolgens nogmaals in het vak **Wachtwoord opnieuw invoeren**.

5 Klik op **OK**.

Een McAfee-gebruiker verwijderen

U kunt een McAfee-gebruiker op elk moment verwijderen.

Ga als volgt te werk om een McAfee-gebruiker te verwijderen:

1 Meld u bij SecurityCenter aan als beheerder.

2 Open het deelvenster Gebruikersinstellingen.

Hoe?

1. Klik op **Startpagina** onder **Algemene taken**.
2. Klik in het deelvenster Startpagina van SecurityCenter op **Ouderlijk toezicht**.
3. Klik in het gedeelte voor gegevens over ouderlijk toezicht op **Configureren**.
4. Klik in het deelvenster voor configuratie van ouderlijk toezicht op **Geavanceerd**.

3 Selecteer een gebruikersnaam onder **McAfee-gebruikersaccounts** in het deelvenster Gebruikersinstellingen en klik vervolgens op **Verwijderen**.

Accountgegevens van McAfee-gebruikers bewerken

U kunt het wachtwoord, het accounttype en de mogelijkheid om zich automatisch aan te melden wijzigen voor een McAfee-gebruiker.

1 Meld u bij SecurityCenter aan als beheerder.

2 Open het deelvenster Gebruikersinstellingen.

Hoe?

1. Klik op **Startpagina** onder **Algemene taken**.
2. Klik in het deelvenster Startpagina van SecurityCenter op **Ouderlijk toezicht**.
3. Klik in het gedeelte voor gegevens over ouderlijk toezicht op **Configureren**.
4. Klik in het deelvenster voor configuratie van ouderlijk toezicht op **Geavanceerd**.

3 Klik in het deelvenster Gebruikersinstellingen op een gebruikersnaam en klik vervolgens op **Bewerken**.

4 Volg de instructies op het scherm om het wachtwoord en accounttype en de opties voor Parental Controls voor de gebruiker te bewerken.

5 Klik op **OK**.

Een McAfee-gebruiker toevoegen

Als u een McAfee-gebruiker hebt gemaakt, kunt u Parental Controls configureren voor de gebruiker. Raadpleeg de Help van Parental Controls voor meer informatie.

1 Meld u bij SecurityCenter aan als beheerder.

2 Open het deelvenster Gebruikersinstellingen.

   Hoe?

   1. Klik op **Startpagina** onder **Algemene taken**.
   2. Klik in het deelvenster Startpagina van SecurityCenter op **Ouderlijk toezicht**.
   3. Klik in het gedeelte voor gegevens over ouderlijk toezicht op **Configureren**.
   4. Klik in het deelvenster voor configuratie van ouderlijk toezicht op **Geavanceerd**.

3 Klik op **Toevoegen** in het deelvenster Gebruikersinstellingen.

4 Volg de instructies op het scherm om een gebruikersnaam, wachtwoord en accounttype en de opties voor Parental Controls in te stellen.

5 Klik op **Maken**.

Overstappen op Windows-gebruikers

Om het beheer te vereenvoudigen, raadt McAfee aan om over te stappen op Windows-gebruikers. U kunt daarna echter niet meer teruggaan naar McAfee-gebruikers.

1 Open het deelvenster Gebruikersinstellingen.

   Hoe?

   1. Klik op **Startpagina** onder **Algemene taken**.
   2. Klik in het deelvenster Startpagina van SecurityCenter op **Ouderlijk toezicht**.
   3. Klik in het gedeelte voor gegevens over ouderlijk toezicht op **Configureren**.
   4. Klik in het deelvenster voor configuratie van ouderlijk toezicht op **Geavanceerd**.

2 Klik op **Overschakelen** in het deelvenster Configuratie.

3 Bevestig de bewerking.

Werken met Windows-gebruikers

Standaard komen de SecurityCenter-gebruikers overeen met de Windows-gebruikers die u op uw computer hebt ingesteld. U voegt gebruikers toe, bewerkt de accountgegevens van gebruikers en verwijdert gebruikers met Computerbeheer in Windows. U kunt vervolgens Parental Controls voor deze gebruikers instellen in SecurityCenter.

Zie Werken met McAfee-gebruikers (pagina 176) als u een upgrade hebt uitgevoerd van een eerdere versie van SecurityCenter waarin met McAfee-gebruikers werd gewerkt.

HOOFDSTUK 33

Informatie op het internet beveiligen

U kunt ook voorkomen dat uw persoonlijke gegevens (zoals naam, adres en nummers van creditcards en bankrekeningen) via internet worden overgebracht door deze gegevens toe te voegen aan het gebied met beschermde gegevens.

Opmerking: de overdracht van persoonlijke gegevens door veilige websites (dat wil zeggen websites die met het protocol https:// werken, zoals sites van banken) wordt niet geblokkeerd door Parental Controls.

In dit hoofdstuk

Persoonlijke gegevens beveiligen

Voorkom dat uw persoonlijke gegevens (zoals naam, adres en nummers van creditcards en bankrekeningen) via het internet worden overgebracht door deze gegevens te blokkeren. Als McAfee ontdekt dat persoonlijke gegevens die zijn opgenomen in bijvoorbeeld een veld in een formulier of in een bestand, op het punt staan om via het internet te worden verzonden, gebeurt het volgende:

- Als u beheerder bent, moet u bevestigen dat de informatie moet worden verzonden.
- Als u geen beheerder bent, wordt de geblokkeerde informatie vervangen door sterretjes (*). Als bijvoorbeeld een poging wordt ondernomen om uw creditcardnummer naar een andere computer te verzenden, wordt het nummer vervangen door sterretjes.

Persoonlijke gegevens beveiligen

U kunt de volgende soorten persoonlijke gegevens blokkeren: naam, adres, postcode, sofinummer, telefoonnummer, creditcardnummers, bankrekeningen, courtagerekeningen en telefoonkaarten. Als u een ander soort persoonlijke gegevens wilt blokkeren, kiest u **overige**.

1 Open het deelvenster Beschermde gegevens.

   Hoe?

   1. Klik op **Startpagina** onder **Algemene taken**.
   2. Klik in het deelvenster Startpagina van SecurityCenter op **Internet en netwerk**.
   3. Klik in het gedeelte Internet en netwerk op **Configureren**.
   4. Controleer in het deelvenster voor configuratie van internet en netwerk of de optie Beveiliging van persoonlijke gegevens is ingeschakeld en klik op **Geavanceerd**.

2 Klik in het deelvenster Beschermde gegevens op **Toevoegen**.

3 Selecteer in de lijst het soort gegevens dat u wilt blokkeren.

4 Voer de persoonlijke gegevens in en klik op **OK**.

HOOFDSTUK 34

Wachtwoorden beveiligen

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

In dit hoofdstuk

De wachtwoordkluis instellen

Voordat u de wachtwoordkluis gaat gebruiken, moet u een wachtwoord voor de wachtwoordkluis instellen. Alleen gebruikers die dit wachtwoord kennen, hebben toegang tot uw wachtwoordkluis. Als u het wachtwoord van uw wachtwoordkluis vergeet, kunt u dit opnieuw instellen. Alle wachtwoorden die u hebt opgeslagen in de wachtwoordkluis worden dan echter verwijderd.

Als u een wachtwoord voor de wachtwoordkluis hebt ingesteld, kunt u wachtwoorden toevoegen aan, bewerken in of verwijderen uit de kluis. Ook kunt u op elk moment het wachtwoord van uw wachtwoordkluis wijzigen.

Het wachtwoord voor uw wachtwoordkluis opnieuw instellen

Als u uw wachtwoord voor de wachtwoordkluis vergeet, kunt u dit opnieuw instellen. Alle wachtwoorden die u hebt opgeslagen, worden dan echter verwijderd.

1 Open het deelvenster Wachtwoordkluis.

   Hoe?

   1. Klik op **Startpagina** onder **Algemene taken**.
   2. Klik in het deelvenster Startpagina van SecurityCenter op **Internet en netwerk**.
   3. Klik in het gedeelte Internet en netwerk op **Configureren**.
   4. Klik in het deelvenster Internet en netwerk op **Geavanceerd** onder **Wachtwoordkluis**.

2 Klik op **Wachtwoord vergeten?**

3 Typ een nieuw wachtwoord in het vak **Wachtwoord** in het dialoogvenster Wachtwoordkluis opnieuw instellen en typ het vervolgens nogmaals in het vak **Wachtwoord opnieuw invoeren**.

4 Klik op **Opnieuw instellen**.

5 Klik in het bevestigingsdialoogvenster op **Ja**.

Uw wachtwoord voor de wachtwoordkluis wijzigen

U kunt op elk moment het wachtwoord van uw wachtwoordkluis wijzigen.

1 Open het deelvenster Wachtwoordkluis.

   Hoe?

   1. Klik op **Startpagina** onder **Algemene taken**.
   2. Klik in het deelvenster Startpagina van SecurityCenter op **Internet en netwerk**.
   3. Klik in het gedeelte Internet en netwerk op **Configureren**.
   4. Klik in het deelvenster Internet en netwerk op **Geavanceerd** onder **Wachtwoordkluis**.

2 Typ in het deelvenster Wachtwoordkluis uw huidige wachtwoord in het vak **Wachtwoord** en klik vervolgens op **Openen**.

3 Klik in het deelvenster Wachtwoordkluis beheren op **Wachtwoord wijzigen**.

4 Typ een nieuw wachtwoord voor uw wachtwoordkluis in het vak **Wachtwoord** en typ dit nogmaals in het vak **Wachtwoord opnieuw invoeren**.

5 Klik op **OK**.

6 Klik in het dialoogvenster Het wachtwoord voor de wachtwoordkluis is gewijzigd op **OK**.

Een wachtwoord verwijderen

U kunt op elk moment een wachtwoord verwijderen uit de wachtwoordkluis. U kunt een verwijderd wachtwoord echter niet herstellen.

1 Open het deelvenster Wachtwoordkluis.

   Hoe?

   1. Klik op **Startpagina** onder **Algemene taken**.
   2. Klik in het deelvenster Startpagina van SecurityCenter op **Internet en netwerk**.
   3. Klik in het gedeelte Internet en netwerk op **Configureren**.
   4. Klik in het deelvenster Internet en netwerk op **Geavanceerd** onder **Wachtwoordkluis**.

2 Typ het wachtwoord voor uw wachtwoordkluis in het vak **Wachtwoord**.

3 Klik op **Openen**.

4 Klik in het deelvenster Wachtwoordkluis beheren op het desbetreffende wachtwoord en klik op **Verwijderen**.

5 Klik op **Ja** in het dialoogvenster Verwijdering bevestigen.

Een wachtwoord wijzigen

U kunt wachtwoorden in de wachtwoordkluis bijwerken als ze veranderen, zodat uw wachtwoordkluis altijd betrouwbaar en up-to-date is.

1 Open het deelvenster Wachtwoordkluis.

   Hoe?

   1. Klik op **Startpagina** onder **Algemene taken**.
   2. Klik in het deelvenster Startpagina van SecurityCenter op **Internet en netwerk**.
   3. Klik in het gedeelte Internet en netwerk op **Configureren**.
   4. Klik in het deelvenster Internet en netwerk op **Geavanceerd** onder **Wachtwoordkluis**.

2 Typ het wachtwoord voor uw wachtwoordkluis in het vak **Wachtwoord**.

3 Klik op **Openen**.

4 Klik in het deelvenster Wachtwoordkluis beheren op een wachtwoord en klik op **Bewerken**.

5 Wijzig de beschrijving van het wachtwoord (bijvoorbeeld het doel) in het vak **Beschrijving** of wijzig het wachtwoord zelf in het vak **Wachtwoord**.

6 Klik op **OK**.

Een wachtwoord toevoegen

Als u moeite hebt uw wachtwoorden te onthouden, kunt u ze toevoegen aan de wachtwoordkluis. De wachtwoordkluis is een veilige locatie die alleen toegankelijk is voor gebruikers die het wachtwoord van uw wachtwoordkluis weten.

1 Open het deelvenster Wachtwoordkluis.

Hoe?

1. Klik op **Startpagina** onder **Algemene taken**.
2. Klik in het deelvenster Startpagina van SecurityCenter op **Internet en netwerk**.
3. Klik in het gedeelte Internet en netwerk op **Configureren**.
4. Klik in het deelvenster Internet en netwerk op **Geavanceerd** onder **Wachtwoordkluis**.

2 Typ het wachtwoord voor uw wachtwoordkluis in het vak **Wachtwoord**.

3 Klik op **Openen**.

4 Klik in het deelvenster Wachtwoordkluis beheren op **Toevoegen**.

5 Typ een beschrijving van het wachtwoord (bijvoorbeeld het doel) in het vak **Beschrijving** en typ het wachtwoord zelf in het vak **Wachtwoord**.

6 Klik op **OK**.

HOOFDSTUK 35

McAfee Backup and Restore

Gebruik McAfee® Backup and Restore om ongewild gegevensverlies te voorkomen door bestanden te archiveren op cd, dvd, een USB-station, een externe vaste schijf of een netwerkstation. Met lokaal archiveren kunt u uw persoonlijke gegevens archiveren (een back-up maken) op cd, dvd, een USB-station, een externe vaste schijf of een netwerkstation. Zo bent u voorzien van een lokale reservekopie van uw gegevens, documenten en andere belangrijke materialen als u deze onbedoeld zou verliezen.

Voordat u begint met het gebruik van Backup and Restore kunt u kennis maken met de populairste functies. Meer informatie over het configureren en gebruik van deze functies vindt u in de Help van Backup and Restore. Als u de functies van het programma hebt bekeken, moet u controleren of u over geschikte archiveringsmedia beschikt om een back-up te maken van lokale archieven.

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 Backup and Restore

Lokaal gepland archiveren	Bescherm uw gegevens door bestanden en mappen te archiveren op cd, dvd, USB-station, externe vaste schijf of netwerkstation. Nadat u de eerste archivering hebt gestart, worden volgende archiveringen automatisch uitgevoerd.
Met één klik herstellen	Als bestanden of mappen op uw computer per ongeluk zijn verwijderd of beschadigd, kunt u de meest recent gearchiveerde versies herstellen vanaf de gebruikte archiefmedia.
Compressie en codering	Uw gearchiveerde bestanden worden standaard gecomprimeerd. Dit scheelt ruimte op uw archiefmedium. Als extra beveiligingsmaatregel worden uw archieven standaard gecodeerd.

HOOFDSTUK 36

Bestanden archiveren

U kunt McAfee Backup and Restore gebruiken om een kopie van uw bestanden op te slaan op cd, dvd, een USB-station, een externe vaste schijf of een netwerkschijf. Als u uw bestanden op deze manier archiveert, zijn de gegevens eenvoudig terug te vinden als u onopzettelijk gegevens verliest of beschadigt.

Voordat u begint met het archiveren van bestanden, moet u een standaard archiveerlocatie selecteren (cd, dvd, een USB-station, externe vaste schijf of een netwerkschijf). McAfee heeft enkele instellingen vooraf ingesteld (bijvoorbeeld mappen en bestandstypen), maar u kunt deze instellingen aanpassen.

U kunt de standaardinstellingen voor de frequentie van volledige of snelle archivering door Backup and Restore wijzigen nadat u de lokale archiefopties hebt ingesteld. U kunt ook te allen tijde handmatig archiveren.

In dit hoofdstuk

Lokaal archiveren in- en uitschakelen

De eerste keer dat u Backup and Restore start, bepaalt u of u lokaal archiveren wilt in- of uitschakelen, afhankelijk van hoe u Backup and Restore wilt gebruiken. Zodra u zich aanmeldt en Backup and Restore begint te gebruiken, kunt u op elk moment lokaal archiveren in- of uitschakelen.

Als u geen kopie van uw bestanden wilt opslaan op cd, dvd, een USB-station, een externe vaste schijf of een netwerkschijf, kunt u lokaal archiveren uitschakelen.

Lokaal archiveren inschakelen

U schakelt lokaal archiveren in als u een kopie van uw bestanden wilt opslaan op cd, dvd, een USB-station, een externe vaste schijf of een netwerkschijf.

1. Klik in SecurityCenter in het menu **Geavanceerd** op **Configureren**.
2. Klik in het configuratiedeelvenster op **Computer en bestanden**.
3. Klik in het deelvenster Internet- en netwerkconfiguratie onder **Lokaal archiveren is uitgeschakeld** op **Aan**.

Lokaal archiveren uitschakelen

U schakelt lokaal archiveren uit als u geen kopie van uw bestanden wilt opslaan op cd, dvd, een USB-station, een externe vaste schijf of een netwerkschijf.

1. Klik in SecurityCenter in het menu **Geavanceerd** op **Configureren**.
2. Klik in het configuratiedeelvenster op **Computer en bestanden**.
3. Klik in het deelvenster Internet- en netwerkconfiguratie onder **Lokaal archiveren is ingeschakeld** op **Aan**.

Archiefopties instellen

Voordat u begint met het archiveren van uw bestanden, moet u enkele lokale archiefopties instellen. U moet bijvoorbeeld de bewaakte locaties en bewaakte bestandstypen instellen. Bewaakte locaties zijn de mappen op uw computer die door Backup and Restore worden gecontroleerd op nieuwe bestanden of gewijzigde bestanden. Bewaakte bestandstypen zijn de bestandstypen (bijvoorbeeld .doc, .xls, etc.) op de bewaakte locaties die Backup and Restore archiveert. Standaard worden de volgende bestandstypen gearchiveerd, maar u kunt ook andere bestandtypen archiveren.

- Microsoft® Word-documenten (.doc, .docx)
- Microsoft Excel®-spreadsheets (.xls, .xlsx)
- Microsoft PowerPoint®-presentaties (.ppt, .pptx)
- Microsoft Project®-bestanden (.mpp)
- Adobe® PDF-bestanden (.pdf)
- Platte tekstbestanden (.txt)
- HTML-bestanden (.html)
- Joint Photographic Experts Group-bestanden (.jpg, .jpeg)
- Tagged Image Format-bestanden (.tif)
- MPEG Audio Stream III-bestanden (.mp3)
- Videobestanden (.vdo)

Opmerking: van de volgende bestandstypen kunt u geen back-up maken: .ost, en .pst.

U kunt twee typen bewaakte locaties instellen: mappen en submappen op het hoogste niveau en alleen mappen op het hoogste niveau. Als u een locatie instelt voor mappen en submappen op het hoogste niveau, archiveert Backup and Restore bewaakte bestandstypen in die map en de bijbehorende submappen. Als u een locatie voor mappen op het hoogste niveau instelt, archiveert Backup and Restore uitsluitend de bewaakte bestandstypen in die map (en niet in de submappen). U kunt ook locaties opgeven die u wilt uitsluiten uit het lokale archief. Standaard zijn de locaties Bureaublad en Mijn documenten ingesteld als op het hoogste niveau bewaakte map- en submaplocaties.

Nadat u de bewaakte bestandstypen en locaties hebt ingesteld, moet u de archieflocatie (d.w.z. het cd-, dvd- of USB-station, de externe vaste schijf of het netwerkstation waarop de gearchiveerde gegevens worden opgeslagen) opgeven. U kunt de archieflocatie te allen tijde wijzigen.

Codering en compressie zijn standaard ingeschakeld voor uw gearchiveerde bestanden in verband met beveiliging en bestandsgrootte. De inhoud van gecodeerde bestanden wordt omgezet in code. Hierdoor worden de gegevens gemaskeerd zodat deze onleesbaar wordt voor iedereen die niet weet hoe de informatie moet worden gedecodeerd. Gecomprimeerde bestanden worden gecomprimeerd naar een formaat dat minder ruimte inneemt bij het opslaan of versturen. Het is te allen tijde mogelijk de codering of compressie uit te schakelen, maar McAfee raadt dit af.

Een locatie in het archief opnemen

U kunt twee verschillende typen bewaakte locaties instellen voor het archiveren: mappen en submappen op het hoogste niveau en alleen mappen op het hoogste niveau. Als u een locatie voor mappen en submappen op het hoogste niveau instelt, controleert Backup and Restore de inhoud van de map en de bijbehorende submappen op wijzigingen. Als u een locatie voor mappen op het hoogste niveau instelt, controleert Backup and Restore uitsluitend de inhoud van de map (niet de subfolders).

1 Open het dialoogvenster Instellingen voor lokaal archief.

   Hoe?

   1. Klik op het tabblad **Lokaal archiveren**.
   2. Klik in het linker deelvenster op **Instellingen**.

2 Klik op **Bewaakte locaties**.

3 Voer een van de volgende handelingen uit:

   - Als u de inhoud van een map inclusief de inhoud van de bijbehorende submappen wilt archiveren, klikt u op **Map toevoegen** onder **Archivering van mappen en submappen op het hoogste niveau**.
   - Als u de inhoud van een map, maar niet de inhoud van de bijbehorende submappen wilt archiveren, klikt u op **Map toevoegen** onder **Archivering van mappen op het hoogste niveau**.
   - Als u een volledig bestand wilt archiveren, klikt u op **Bestand toevoegen** onder **Archivering van mappen op het hoogste niveau**.

4 Navigeer in het dialoogvenster Zoeken naar map (of Openen) naar de map die (of een bestand dat) u wilt bewaken en klik vervolgens op **OK**.

5 Klik op **OK**.

Tip: als u Backup and Restore een map wilt laten bewaken die u nog niet hebt gemaakt, klik dan op **Nieuwe map maken** in het dialoogvenster Zoeken naar map, voeg een map toe en stel deze tegelijkertijd in als bewaakte locatie.

Bestandstypen voor archivering instellen

U kunt opgeven welke typen bestanden worden gearchiveerd binnen uw mappen en submappen op het hoogste niveau of uw mappen op het hoogste niveau. U kunt selecteren in een bestaande lijst met bestandtypen of een nieuw type toevoegen aan de lijst.

1 Open het dialoogvenster Instellingen voor lokaal archief.

   Hoe?

   1. Klik op het tabblad **Lokaal archiveren**.
   2. Klik in het linker deelvenster op **Instellingen**.

2 Klik op **Bestandstypen**.

3 Vouw de lijst met bestandstypen uit en selecteer de selectievakjes naast de bestandstypen die u wilt archiveren.

4 Klik op **OK**.

Tip: als u een nieuw bestandstype wilt toevoegen aan de lijst met **Geselecteerde bestandstypen**, typt u de bestandsextensie in het vak **Aangepast bestandstype aan Overige toevoegen**, klikt u op **Toevoegen** en vervolgens op **OK**. Het nieuwe bestandstype wordt automatisch een bewaakt bestandstype.

Een locatie uit het archief uitsluiten

U kunt een locatie uitsluiten uit het archief als u niet wilt dat die locatie (map) en de inhoud ervan wordt gearchiveerd.

1 Open het dialoogvenster Instellingen voor lokaal archief.

   Hoe?

   1. Klik op het tabblad **Lokaal archiveren**.
   2. Klik in het linker deelvenster op **Instellingen**.

2 Klik op **Bewaakte locaties**.

3 Klik op **Map toevoegen** onder **Mappen die uitgesloten zijn van de back-up**.

4 Navigeer in het dialoogvenster Zoeken naar map naar de map die u wilt uitsluiten, selecteer de map en klik vervolgens op **OK**.

5 Klik op **OK**.

Tip: als u Backup and Restore een map wilt laten uitsluiten die u nog niet hebt gemaakt, klik dan op **Nieuwe map maken** in het dialoogvenster Zoeken naar map, voeg een map toe en sluit deze tegelijkertijd uit.

Archieflocatie wijzigen

Als u de archieflocatie wijzigt, worden de bestanden die eerder op een andere locatie zijn gearchiveerd weergegeven als *Nooit gearchiveerd*.

1. Open het dialoogvenster Instellingen voor lokaal archief.

   Hoe?

   1. Klik op het tabblad **Lokaal archiveren**.
   2. Klik in het linker deelvenster op **Instellingen**.

2. Klik op **Archieflocatie wijzigen**.
3. Ga op een van de volgende manieren te werk in het dialoogvenster Archieflocatie:
   - Klik op **Cd/dvd-writer selecteren**, klik op het cd- of dvd-station van uw computer in de lijst **Writer** en klik vervolgens op **OK**.
   - Klik op **Stationslocatie selecteren** en navigeer naar een USB-station, een lokaal station of een externe vaste schijf. Selecteer het station en klik vervolgens op **OK**.
   - Klik op **Netwerklocatie selecteren** en navigeer naar een netwerkmap. Selecteer de map en klik vervolgens op **OK**.
4. Controleer de nieuwe archieflocatie onder **Geselecteerde archieflocatie** en klik vervolgens op **OK**.
5. Klik in het bevestigingsdialoogvenster op **OK**.
6. Klik op **OK**.

Opmerking: wanneer u de archieflocatie wijzigt, worden eerder gearchiveerde bestanden weergegeven als **Niet gearchiveerd** in de kolom **Status**.

Codering en compressie voor archief uitschakelen

Coderen van gearchiveerde bestanden beschermt de vertrouwelijkheid van uw gegevens door de inhoud van de bestanden te maskeren zodat de bestanden onleesbaar zijn. Door comprimeren van gearchiveerde bestanden nemen deze minder ruimte in. Standaard zijn codering en compressie beide ingeschakeld. U kunt deze opties echter te allen tijde uitschakelen.

1 Open het dialoogvenster Instellingen voor lokaal archief.

   Hoe?

   1. Klik op het tabblad **Lokaal archiveren**.
   2. Klik in het linker deelvenster op **Instellingen**.

2 Klik op **Geavanceerde instellingen**.

3 Verwijder het vinkje uit het selectievakje **Codering activeren om beveiliging te vergroten**.

4 Verwijder het vinkje uit het selectievakje **Compressie inschakelen om opslagruimte te reduceren**.

5 Klik op **OK**.

Opmerking: McAfee raadt u aan de codering en compressie niet uit te schakelen terwijl u uw bestanden archiveert.

Volledige en snelle archivering uitvoeren

U kunt twee soorten archiveerbewerkingen uitvoeren: snel of volledig. Als u een volledige archivering uitvoert, archiveert u een volledige gegevensset die is gebaseerd op de bewaakte bestandstypen en locaties die u hebt ingesteld. Als u een snelle archivering uitvoert, worden alleen de bewaakte bestanden gearchiveerd die zijn gewijzigd sinds de laatste volledige of snelle archivering.

Backup and Restore is voorzien van een standaardplanning waarbij er elke maandag om 09.00 uur een volledige archivering plaatsvindt van de bewaakte bestandstypen en er een snelle archivering plaatsvindt elke 48 uur na een volledige of snelle archivering. Hierdoor bent u steeds verzekerd van een recente archivering van uw bestanden. Als u echter niet elke 48 uur wilt archiveren, kunt u de planning naar wens aanpassen.

Als u tussentijds de inhoud van uw bewaakte locaties wilt archiveren, kunt u dit te allen tijde doen. Als u bijvoorbeeld een bestand wijzigt en het wilt archiveren maar Backup and Restore heeft pas weer over 60 minuten een volledige of snelle archivering gepland, kunt u het bestand handmatig archiveren. Als u bestanden handmatig archiveert, wordt het interval voor de automatische archivering opnieuw ingesteld.

U kunt een automatische of handmatige archivering ook onderbreken als deze plaatsvindt op een ongelegen ogenblik. Als er bijvoorbeeld een automatische archivering begint terwijl u een taak aan het uitvoeren bent die veel geheugenruimte vergt, kunt u de archivering stoppen. Als u een automatische archivering stopt, wordt het interval voor de automatische archiveringen opnieuw ingesteld.

Automatische archiveringen plannen

U kunt de frequentie instellen voor volledige en snelle archiveringen om ervoor te zorgen dat uw gegevens altijd beschermd zijn.

1 Open het dialoogvenster Instellingen voor lokaal archief.

   Hoe?

   1. Klik op het tabblad **Lokaal archiveren**.
   2. Klik in het linker deelvenster op **Instellingen**.

2 Klik op **Algemeen**.

3 Klik op een van de mogelijkheden onder **Volledige archivering elke:** om elke dag, elke week of elke maand een volledige archivering uit te voeren.

   - **Dag**
   - **Week**
   - **Maand**

4 Selecteer het selectievakje naast de dag waarop u de volledige archivering wilt laten uitvoeren.

5 Klik op een waarde in de lijst **Om** om de tijd op te geven waarop u wilt dat de volledige archivering wordt uitgevoerd.

6 Klik op een van de mogelijkheden onder **Snelle archivering** om elke dag of elk uur een snelle archivering uit te voeren:

   - **Uren**
   - **Dagen**

7 Typ een getal dat de frequentie aangeeft in het vak **Snelle archivering elke:**.

8 Klik op **OK**.

Opmerking: u kunt een geplande archivering uitschakelen door **Handmatig** te selecteren onder **Volledige archivering elke:**.

Automatisch archiveren onderbreken

Backup and Restore archiveert automatisch de bestanden en mappen op uw bewaakte locaties volgens de door u gedefinieerde planning. Als er een automatische archivering wordt uitgevoerd, kunt u deze op elk moment onderbreken.

1 Klik in het linker deelvenster op **Archiveren stoppen**.

2 Klik op **Ja** in het bevestigingsdialoogvenster.

Opmerking: de koppeling **Archiveren stoppen** verschijnt uitsluitend als er een archivering wordt uitgevoerd.

Handmatig archiveren

Automatisch archiveren wordt volgens een vooraf gedefinieerd schema uitgevoerd, maar u kunt ook te allen tijde handmatig volledige of een snelle archivering uitvoeren. Met een snelle archivering worden alleen de bestanden gearchiveerd die zijn gewijzigd sinds de laatste volledige of snelle archivering. Bij een volledige archivering worden de bewaakte bestandstypen op alle bewaakte locaties gearchiveerd.

1. Klik op het tabblad **Lokaal archiveren**.
2. Voer een van de volgende handelingen uit:
   - Klik in het linker deelvenster op **Snelle archivering** om een snelle archivering uit te voeren.
   - Klik in het linker deelvenster op **Volledige archivering** om een volledige archivering uit te voeren.
3. Controleer in het dialoogvenster Beginnen met archiveren uw opslagruimte en instellingen en klik vervolgens op **Doorgaan**.

HOOFDSTUK 37

Werken met gearchiveerde bestanden

Nadat u bestanden hebt gearchiveerd, kunt u Backup and Restore gebruiken om met deze bestanden te werken. Uw gearchiveerde bestanden worden aangeboden in een traditionele weergave in de verkenner zodat u uw bestanden snel kunt vinden. Als uw archief groter wordt, kunt u de bestanden sorteren of naar bestanden zoeken. U kunt ook bestanden rechtstreeks in de verkennerweergave openen om de inhoud te bekijken zonder dat u de bestanden hoeft op te halen.

U kunt bestanden ophalen uit een archief als uw lokale exemplaar van het bestand verouderd is, ontbreekt of is beschadigd. Met Backup and Restore beschikt u over de informatie die u nodig hebt om uw lokale archieven en opslagmedia te beheren.

In dit hoofdstuk

De lokale archiefverkenner gebruiken

Met de lokale archiefverkenner kunt u de bestanden die u lokaal hebt gearchiveerd bekijken en bewerken. U kunt van elk bestand de naam, het type, de locatie, de grootte, de status (gearchiveerd, niet gearchiveerd of archivering in voortgang) en de datum waarop het bestand voor het laatst is gearchiveerd bekijken. U kunt de bestanden ook volgens een van deze criteria sorteren.

Als u een groot archief hebt, kunt u een bestand snel vinden door ernaar te zoeken. U kunt zoeken op een gedeelte van of de volledige bestandsnaam of het pad en vervolgens de zoekopdracht beperken door de geschatte bestandsgrootte op te geven en de datum waarop het bestand voor het laatst is gearchiveerd.

Nadat u een bestand hebt gevonden, kunt u het rechtstreeks in de lokale archiefverkenner openen. Backup and Restore opent het bestand in het oorspronkelijke programma, waardoor u wijzigingen kunt aanbrengen zonder dat u de lokale archiefverkenner hoeft te verlaten. Het bestand wordt opgeslagen op de oorspronkelijke bewaakte locatie op uw computer en wordt automatisch gearchiveerd volgens de ingestelde archiefplanning.

Gearchiveerde bestanden sorteren

U kunt uw gearchiveerde bestanden en mappen sorteren op de volgende criteria: naam, bestandstype, grootte, status (bijvoorbeeld: gearchiveerd, niet gearchiveerd of archivering in voortgang), de datum waarop de bestanden voor het laatst zijn gearchiveerd of de locatie van de bestanden op uw computer (het pad).

Archiefbestanden sorteren:

1. Klik op het tabblad **Lokaal archiveren**.
2. Klik in het rechter deelvenster op een naam van een kolom.

Een gearchiveerd bestand zoeken

Als u een grote opslagplaats met gearchiveerde bestanden hebt, kunt u een bestand snel vinden door ernaar te zoeken. U kunt zoeken op een gedeelte van of de volledige bestandsnaam of het pad en vervolgens de zoekopdracht beperken door de geschatte bestandsgrootte op te geven en de datum waarop het bestand voor het laatst is gearchiveerd.

1. Typ de volledige of een gedeelte van de bestandsnaam in het vak **Zoeken** boven aan het scherm en druk vervolgens op ENTER.
2. Typ de volledige of een gedeelte van het pad in het vak **Gehele of gedeeltelijke pad**.
3. Geef op een van de volgende manieren de geschatte bestandsgrootte op van het bestand dat u zoekt:
   - Klik op **Kleiner dan 100 KB**, **Kleiner dan 1 MB** of **Groter dan 1 MB**.
   - Klik op **Grootte in KB** en geef de juiste grootte op in de vakken.
4. Geef op een van de volgende manieren de geschatte datum van de laatste archivering van het bestand op:
   - Klik op **Deze week**, **Deze maand** of **Dit jaar**.
   - Klik op **Datums opgeven** en op **Gearchiveerd** in de lijst en klik vervolgens op de datum in de datumlijst.
5. Klik op **Zoeken**.

Opmerking: als u de grootte en datum van de laatste archivering niet weet, klik dan op **Onbekend**.

Een gearchiveerd bestand openen

U kunt de inhoud van een archiefbestand bekijken door het bestand rechtstreeks te openen in de lokale archiefverkenner.

Archiefbestanden openen:

1. Klik op het tabblad **Lokaal archiveren**.
2. Klik in het rechterdeelvenster op een bestandsnaam en klik vervolgens op **Openen**.

Tip: U kunt een archiefbestand ook openen door te dubbelklikken op de bestandsnaam.

Gearchiveerde bestanden terugzetten

Als een bewaakt bestand beschadigd raakt, ontbreekt, of per ongeluk is verwijderd, kunt u een kopie van dit bestand vanuit een lokaal archief herstellen. Daarom is het belangrijk dat u uw bestanden regelmatig archiveert. U kunt ook oudere versies vanuit een lokaal archief herstellen. Als u bijvoorbeeld een bestand regelmatig archiveert maar wilt terugkeren naar een vorige versie van het bestand, kunt u dit doen door het bestand in de archieflocatie te zoeken. Als de archieflocatie een lokaal station of een netwerkstation is, kunt u het bestand meteen zoeken. Als de archieflocatie een externe vaste schijf of een USB-station is, moet u eerst de schijf of het station aansluiten op de computer en kunt u daarna het bestand zoeken. Als de archieflocatie een cd of dvd is, moet u de cd of dvd in de computer plaatsen en vervolgens kunt u het bestand zoeken.

U kunt ook bestanden herstellen op een computer die u hebt gearchiveerd vanaf een andere computer. Als u bijvoorbeeld een verzameling bestanden archiveert op een externe vaste schijf op computer A, kunt u deze bestanden herstellen op computer B. Hiervoor moet u Backup and Restore op computer B installeren en de externe vaste schijf aansluiten. Vervolgens zoekt u in Backup and Restore naar de bestanden die zijn toegevoegd aan de lijst **Ontbrekende bestanden** om ze terug te zetten.

Zie Bestanden archiveren voor meer informatie over het archiveren van bestanden. Als u opzettelijk een bewaakt bestand uit uw archief verwijdert, kunt u dit bestand ook verwijderen uit de lijst **Ontbrekende bestanden**.

Ontbrekende bestanden uit een lokaal archief herstellen

Met het lokale archief van Backup and Restore kunt u gegevens terugzetten die ontbreken uit een bewaakte map op uw lokale computer. Als er bijvoorbeeld een reeds gearchiveerd bestand uit een bewaakte map is verplaatst of is verwijderd, kunt u het bestand herstellen vanuit het lokale archief.

1. Klik op het tabblad **Lokaal archiveren**.
2. Schakel het selectievakje in naast de naam van het bestand dat u wilt terugzetten op het tabblad **Ontbrekende bestanden** onderin het scherm.
3. Klik op **Herstellen**.

Tip: u kunt alle bestanden in de lijst **Ontbrekende bestanden** herstellen door op **Alles herstellen** te klikken.

Een oudere versie van een bestand uit een lokaal archief herstellen

Als u een oudere versie van een gearchiveerd bestand wilt herstellen, kunt u het bestand zoeken en toevoegen aan de lijst **Ontbrekende bestanden**. Vervolgens kunt u het bestand op dezelfde manier herstellen als u dat met een willekeurig ander bestand in de lijst **Ontbrekende bestanden** zou doen.

1 Klik op het tabblad **Lokaal archief**.

2 Klik op het tabblad **Ontbrekende bestanden**, onderin het scherm, op **Bladeren** en blader naar de locatie waarop het archief is opgeslagen.

   Gearchiveerde mapnamen hebben de volgende indeling: `cre ddmmjj_uu-mm-ss_***`, waarbij `ddmmjj` de datum is waarop de bestanden zijn gearchiveerd en `uu-mm-ss` de tijd waarop de bestanden zijn gearchiveerd. `***` kan `Volledig` zijn of `Snel`. Dit hangt er van af of er een volledige of snelle archivering is uitgevoerd.

3 Selecteer een locatie en klik vervolgens op **OK**.

   De bestanden die zich op de geselecteerde locatie bevinden, verschijnen in de lijst **Ontbrekende bestanden** en staan klaar om te worden opgehaald. Zie Ontbrekende bestanden uit een lokaal archief herstellen (pagina 204) voor meer informatie.

Bestanden verwijderen uit de lijst Ontbrekende bestanden

Als een archiefbestand uit een bewaakte map wordt verplaatst of wordt verwijderd, verschijnt dit bestand automatisch in de lijst **Ontbrekende bestanden**. Zo wordt u erop gewezen dat er een verschil bestaat tussen de archiefbestanden en de bestanden die zich in de bewaakte mappen bevinden. Als u het bestand opzettelijk hebt verplaatst of verwijderd, kunt u het bestand verwijderen uit de lijst **Ontbrekende bestanden**.

Een bestand verwijderen uit de lijst Ontbrekende bestanden:

1 Klik op het tabblad **Lokaal archiveren**.

2 Schakel het selectievakje in naast de naam van het bestand dat u wilt verwijderen op het tabblad **Ontbrekende bestanden** onderin het scherm.

3 Klik op **Verwijderen**.

Tip: U kunt alle bestanden in de lijst **Ontbrekende bestanden** verwijderen door op **Alles verwijderen** te klikken.

Archieven beheren

U kunt te allen tijde een overzicht met gegevens over uw volledige en snelle archieven bekijken. U kunt bijvoorbeeld informatie bekijken over de hoeveelheid gegevens die momenteel wordt bewaakt, de hoeveelheid gegevens die is gearchiveerd en de hoeveelheid gegevens die worden bewaakt, maar die nog niet zijn gearchiveerd. U kunt ook gegevens bekijken over de archiveringsplanning, zoals de datum waarop de laatste archivering heeft plaatsgevonden en wanneer de volgende archivering zal plaatsvinden.

Een overzicht van de archiefactiviteiten bekijken

U kunt te allen tijde gegevens over de archiefactiviteiten bekijken. U kunt bijvoorbeeld bekijken welk percentage van de bestanden is gearchiveerd, de grootte bekijken van de bewaakte bestanden, de grootte bekijken van de gegevens die zijn gearchiveerd en de grootte bekijken van de gegevens die worden bewaakt maar die nog niet zijn gearchiveerd. U kunt ook de datums bekijken waarop de laatste archivering heeft plaatsgevonden en waarop de volgende archivering plaatsvindt.

1 Klik op het tabblad **Lokaal archief**.

2 Klik bovenaan het scherm op **Accountoverzicht**.

HOOFDSTUK 38

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

Bestanden opschonen Onnodige bestanden veilig en efficiënt verwijderen met verschillende opschoonprogramma's. Hierdoor maakt u ruimte vrij op de vaste schijf en wordt uw computer sneller.

HOOFDSTUK 39

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 uit 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.

Naam	Functie
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	Hiermee worden cookies verwijderd. Deze bestanden worden gewoonlijk opgeslagen als tijdelijke bestanden. 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 website. Ze kunnen echter ook een bron van informatie zijn voor hackers.
Browsergeschiedeniss en opschonen	Hiermee wordt uw browsergeschiedenis verwijderd.
Opschonen van verwijderde en verzonden e-mail in Outlook Express en Outlook	Hiermee worden verzonden en verwijderde e-mailberichten in Outlook® en Outlook Express verwijderd.
Recent gebruikte items opschonen	Hiermee worden recent geopende bestanden verwijderd die zijn gemaakt met een van de onderstaande programma's: ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Windows History ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®

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

In dit hoofdstuk

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 **Voltooien**.

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

HOOFDSTUK 40

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.

HOOFDSTUK 41

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 **Voltooien**.

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 **Voltooien**.

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 42

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

Bestanden en mappen permanent verwijderen

Hiermee 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, herschrijfbare 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 venietigd.
- **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 43

McAfee Network Manager

McAfee Network Manager biedt een grafische weergave van de computers en andere apparaten in uw thuisnetwerk. Met Network Manager kunt u de beveiligingsstatus van elke beheerde computer in het netwerk op afstand beheren en gerapporteerde beveiligingsproblemen van deze computers op afstand oplossen. Als u McAfee Total Protection hebt geïnstalleerd, kan Network Manager uw netwerk ook controleren op indringers (computers of apparaten die u niet herkent of vertrouwt) die er verbinding mee proberen te maken.

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

Grafisch netwerkoverzicht

Een grafisch overzicht bekijken 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 apparaat dat in het netwerkoverzicht wordt weergegeven.

Extern beheer

De beveiligingsstatus 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 voor een externe computer in het netwerk.

Netwerkbewaking

Laat Network Manager, indien beschikbaar, uw netwerken controleren en u op de hoogte brengen wanneer Vrienden of Indringers verbinding maken. Netwerkbewaking is alleen beschikbaar als u McAfee Total Protection hebt aangeschaft.

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 44

Een beheerd netwerk instellen

Als u een beheerd netwerk wilt instellen, merkt u het netwerk aan als vertrouwd (als u dat nog niet hebt gedaan) en voegt u leden (computers) toe aan het netwerk. 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 item 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

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 naam 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 items van het netwerkoverzicht weergeven of verbergen om de weergave aan te passen. U kunt ook de details bekijken van elk item dat in het netwerkoverzicht wordt weergegeven.

Het netwerkoverzicht openen

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

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

Opmerking: als u het netwerk nog niet als vertrouwd hebt aangemerkt (met behulp van McAfee Personal Firewall), wordt u gevraagd dat te doen bij de eerste keer dat u het netwerkoverzicht opent.

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 **Netwerkoverzicht vernieuwen** onder **Ik wil**.

Opmerking: de koppeling **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 naam 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 **Naam van netwerk wijzigen** onder **Ik wil**.
3. Typ de gewenste naam van het netwerk in het vak **Netwerknaam**.
4. Klik op **OK**.

Opmerking: de koppeling **Naam van 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 apparaten 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 weergeven

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

1. Controleer of het selectievakje **Elke computer in dit netwerk toestaan om beveiligingsinstellingen te beheren** 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 beheren** 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 45

Het netwerk op afstand beheren

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

In dit hoofdstuk

Status en machtigingen beheren

Een beheerd netwerk heeft beheerde en niet-beheerde leden. Beheerde leden staan andere computers in het netwerk toe hun McAfee-beveiligingsstatus te beheren. 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 met een beheerdersmachtiging in het netwerk kan een niet-beheerde computer op elk willekeurig moment uitnodigen om een beheerd lid te worden. Een beheerde computer met beheerdersmachtiging kan op een vergelijkbare manier ook op elk moment een andere beheerde computer onbeheerd maken.

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 beheren

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

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

Het beheer van de beveiligingsstatus van een computer stoppen

U kunt het beheren 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 **Beheren 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 beheren.

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 beheren.
4. Klik op **OK**.

Een apparaat beheren

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

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 McAfee 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 beheren 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 beheerd. Als u deze computers op afstand wilt beheren, moet u een recente versie van SecurityCenter ter plaatse op elke computer installeren.

1. Volg deze instructies op de computer die u op afstand wilt beheren.
2. Houd uw aanmeldingsgegevens voor McAfee bij de hand. Dit zijn het e-mailadres en het wachtwoord die u hebt gebruikt toen u de McAfee-ssoftware voor het eerst hebt geactiveerd.
3. Ga in een browser naar de website van McAfee en klik op **Mijn account**.
4. Zoek het product dat u wilt installeren, klik op de knop **Downloaden** ervan en volg daarna de aanwijzingen op het scherm.

Tip: u kunt ook leren hoe u McAfee-beveiligingssoftware installeert op een externe computer door het netwerkoverzicht te openen en te klikken op **Mijn pc's beschermen** onder **Ik wil**.

HOOFDSTUK 46

Uw netwerken controleren

Als u McAfee Total Protection hebt geïnstalleerd, controleert Network Manager uw netwerken ook op indringers. Als een onbekende computer of een onbekend apparaat verbinding maakt met uw netwerk, ontvangt u daar een melding over, zodat u kunt aangeven of die computer of dat apparaat een Vriend of een Indringer is. Een Vriend is een computer die of een apparaat dat u herkent en vertrouwt, en een Indringer is een computer die of een apparaat dat u niet herkent of vertrouwt. Als u een computer of apparaat markeert als Vriend, kunt u bepalen of u telkens een melding wilt krijgen wanneer die Vriend verbinding maakt met het netwerk. Als u een computer of apparaat markeert als Indringer, krijgt u automatisch een melding wanneer deze verbinding maakt.

De eerste keer dat u verbinding maakt met een netwerk na het installeren of upgraden van deze versie van Total Protection, markeren we automatisch elke computer of elk apparaat als Vriend en krijgt u geen melding als er in de toekomst verbinding wordt gemaakt met het netwerk. Na drie dagen begint u meldingen te krijgen over alle onbekende computers of apparaten die verbinding maken, zodat u deze zelf kunt markeren als Vriend of Indringer.

Opmerking: Netwerkbewaking is een functie van Network Manager die alleen beschikbaar is in McAfee Total Protection. Ga naar onze website voor meer informatie over Total Protection.

In dit hoofdstuk

Bewaking van netwerken stoppen

Als u netwerkbewaking uitschakelt, waarschuwen we u niet meer als indringers verbinding willen maken met uw thuisnetwerk of een ander netwerk waarmee u verbinding maakt.

1 Open het deelvenster Internet- en netwerkconfiguratie.

Hoe?

1. Klik op **Startpagina** onder **Algemene taken**.
2. Klik in het deelvenster Startpagina van SecurityCenter op **Internet en netwerk**.
3. Klik in het gedeelte Internet en netwerk op **Configureren**.

2 Klik op **Uit** onder **Netwerkbewaking**.

Meldingen voor netwerkbewaking opnieuw inschakelen

Hoewel u meldingen voor netwerkbewaking kunt uitschakelen, raden we dat niet aan. Als u dat doet, kunt u namelijk niet meer zien wanneer onbekende computers of Indringers verbinding maken met uw netwerk. Als u deze meldingen per ongeluk hebt uitgeschakeld (bijvoorbeeld als u in een melding het vakje **Deze waarschuwing niet meer tonen** hebt ingeschakeld), kunt u ze op elk moment weer inschakelen.

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 deelvenster voor configuratie van SecurityCenter op **Informatiewaarschuwingen**.

3 Zorg ervoor dat in het deelvenster Informatiewaarschuwingen de volgende selectievakjes uitgeschakeld zijn:

- **Geen waarschuwingen tonen wanneer nieuwe pc's of apparaten verbinding maken met het netwerk**
- **Geen waarschuwingen tonen wanneer Indringers verbinding maken met het netwerk**
- **Geen waarschuwingen tonen voor Vrienden waar ik gewoonlijk wel een melding over wil krijgen**
- **Geen herinnering weergeven wanneer onbekende pc's of apparaten worden gedetecteerd**

- **Geen herinnering weergeven wanneer McAfee klaar is met het detecteren van nieuwe Vrienden**

4 Klik op **OK**.

Markeren als Indringer

Markeer een computer of apparaat in uw netwerk als Indringer als u ze niet herkent of vertrouwt. Wij waarschuwen u automatisch als ze verbinding maken met uw netwerk.

1 Klik in het menu Basis of Geavanceerd op **Netwerk beheren**.
2 Klik op een item in het netwerkoverzicht.
3 Klik op **Markeren als Vriend of Indringer** onder **Ik wil**.
4 Klik in het dialoogvenster op **Een Indringer**.

Markeren als Vriend

Markeer een computer of apparaat in uw netwerk alleen als Vriend als u ze herkent en vertrouwt. Als u een computer of apparaat markeert als Vriend, kunt u ook bepalen of u telkens een melding wilt krijgen wanneer die Vriend verbinding maakt met het netwerk.

1 Klik in het menu Basis of Geavanceerd op **Netwerk beheren**.
2 Klik op een item in het netwerkoverzicht.
3 Klik op **Markeren als Vriend of Indringer** onder **Ik wil**.
4 Klik in het dialoogvenster op **Een Vriend**.
5 Als u een melding wilt krijgen wanneer een Vriend verbinding maakt met het netwerk, schakelt u het selectievakje **Waarschuwen wanneer deze computer of dit apparaat verbinding maakt met het netwerk** in.

Stoppen met opsporen van nieuwe vrienden

De eerste drie dagen nadat u verbinding maakt met een netwerk met deze versie van Total Protection geïnstalleerd, markeren we automatisch alle computers en apparaten als Vriend waarover u geen melding wilt krijgen. U kunt deze automatische functie wanneer u maar wilt uitschakelen binnen die drie dagen, maar dan kunt u de functie later niet meer inschakelen.

1 Klik in het menu Basis of Geavanceerd op **Netwerk beheren**.
2 Klik op **Stoppen met opsporen van nieuwe Vrienden** onder **Ik wil**.

HOOFDSTUK 47

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

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 48

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

U opent EasyNetwork vanuit het menu Start van Windows of door te klikken op het pictogram ervan op het bureaublad.

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

Tip: u kunt EasyNetwork ook openen door te dubbelklikken op het pictogram van McAfee EasyNetwork op het bureaublad.

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 netwerkomschrijving 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 246) 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. Verbreek de verbinding van uw computer met het netwerk.
2. Klik in EasyNetwork in het menu **Extra** op **Netwerk verlaten**.
3. In het dialoogvenster Netwerk verlaten selecteert u de naam van het netwerk waarvoor u zich wilt afmelden.
4. Klik op **Netwerk verlaten**.

HOOFDSTUK 49

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

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 253) 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 253) 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 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 255) 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 ín 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 50

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-afdrukserver (zoals een draadloze USB-afdrukserver), 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

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 geeft een overzicht en definitie van de beveiligingstermen die in McAfee-producten het meest worden gebruikt.

Verklarende woordenlijst

8

802.11

Een verzameling 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 waarmee 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 waarmee 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 standaard voor verificatie op draadloze en niet-draadloze netwerken. 802.1x wordt veel gebruikt in combinatie met draadloze netwerken van het type 802.11. Zie ook verificatie (pagina 271).

A

Aanval met grof geweld

Een hackingmethode die wordt gebruikt om wachtwoorden of coderingssleutels te achterhalen door alle mogelijke tekencombinaties te proberen tot de code is gekraakt.

ActiveX-besturingselement

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

Adapter voor draadloze netwerken

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

Archiveren

Een lokale kopie van belangrijke bestanden maken op een cd, dvd, een USB-station, een externe vaste schijf of een netwerkschijf. Vergelijken met back-up (pagina 260).

B

Back-up maken

Een kopie maken van uw belangrijke bestanden, meestal op een beveiligde server in het netwerk. Vergelijken met archiveren (pagina 260).

Bandbreedte

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

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 bestandtypen (bijvoorbeeld bestanden met de extensie .doc of .xls) waarvan met Backup and Restore een back-up wordt gemaakt of die worden gearchiveerd op bewaakte locaties.

Bewaakte locaties

De mappen op uw computer die door Backup and Restore worden bewaakt.

Browser

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

buffer overflow

De situatie waarin verdachte programma's of processen proberen om meer gegevens in de buffer (een tijdelijke opslaglocatie) van een besturingssysteem op te slaan dan deze kan bevatten. Bij overschrijdingen van de bufferlimiet worden gegevens in aangrenzende buffers overschreven of worden andere bestanden in het geheugen beschadigd.

C

Cache

Een tijdelijke opslaglocatie waar veelgebruikte of recent gebruikte gegevens worden opgeslagen op een 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 programma dat 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 methode om gegevens onleesbaar te maken voor onbevoegden. Gegevens worden gecodeerd met behulp van een 'sleutel' en wiskundige algoritmen. Gecodeerde gegevens kunnen alleen worden gedecodeerd met de juiste sleutel. Ook virussen worden soms gecodeerd om te voorkomen dat ze worden gedetecteerd.

Codetekst

Gecodeerde tekst. Codetekst is onleesbaar totdat deze is geconverteerd (gedecodeerd) naar normale tekst. Zie ook codering (pagina 261).

Compressie

Het kleiner maken van bestanden, zodat ze minder ruimte innemen bij het opslaan of verzenden.

Cookie

Een klein tekstbestand dat door veel websites wordt gebruikt om informatie over bezochte websites op te slaan op de computer van mensen die op internet surfen. In een cookie staan bijvoorbeeld aanmeld- en registratiegegevens, de inhoud van winkelwagentjes of gebruikersvoorkeuren. 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

In detectiebestanden, ook wel virusdefinitiebestanden, staan de definities die nodig zijn om virussen, Trojaanse paarden, spyware, adware en andere mogelijk ongewenste programma's te herkennen, detecteren en verwijderen.

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 Backup and Restore met de melding dat er bestanden met hen worden gedeeld. In het e-mailbericht staat ook een koppeling naar de gedeelde bestanden.

Dialers

Software die internetverbindingen omleidt naar een partij die niet de standaardinternetprovider van de gebruiker is, met de bedoeling de gebruiker extra te laten betalen voor de verbinding of inhoud.

DNS

Afkorting voor Domain Name System. Dit is een databasesysteem waarmee IP-adressen, bijvoorbeeld 11.2.3.44, worden omgezet in domeinnamen, zoals www.mcafee.com.

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. Op internet is een domein een onderdeel van elk webadres. Zo is in www.mcafee.com 'mcafee' het domein.

DoS-aanval (Denial of Service)

Een aanval op een computer, server of netwerk waarmee het verkeer op het netwerk wordt vertraagd of gestopt. Van een DoS-aanval is sprake wanneer een netwerk wordt overspoeld met zoveel extra aanvragen dat het gewone verkeer wordt vertraagd of volledig wordt onderbroken. Een DoS-aanval blokkeert het doelwit met een overvloed van verbindingsaanvragen, zodat normale aanvragen niet worden afgehandeld.

Draadloze PCI-adapterkaart

PCI staat voor Peripheral Component Interconnect. Een adapterkaart die in een PCI-uitbreidingssleuf in de computer wordt gestoken voor draadloos netwerkverkeer.

E

E-mail

Elektronische post. Berichten die elektronisch worden verzonden en ontvangen in een computernetwerk. Zie ook webmail (pagina 271).

E-mailclient

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

ESS

Afkorting van 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 (hardwarematig, softwarematig of beide) dat is ontworpen om ongeoorloofde toegang tot of vanaf een particulier netwerk onmogelijk te maken. Firewalls worden vaak gebruikt om niet-geautoriseerde internetgebruikers de toegang te weigeren tot particuliere netwerken (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

In een computersysteem of -programma: een incident of voorval dat kan worden gedetecteerd met beveiligingssoftware op basis van vooraf gedefinieerde criteria. Doorgaans wordt na een gebeurtenis een actie gestart, zoals het verzenden van een melding of het toevoegen van een item aan een gebeurtenissenlogboek.

Gedeeld geheim

Een tekenreeks of sleutel (meestal een wachtwoord) die wordt gedeeld door twee met elkaar communicerende partijen voordat de communicatie werd geïnitieerd. Dit dient voor de beveiliging van vertrouwelijke gedeelten van RADIUS-berichten. Zie ook RADIUS (pagina 267).

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

In Parental Controls: 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 als de hotspot zichzelf adverteert. Verificatie is hierbij niet vereist. Hotspots bevinden zich meestal in dichtbevolkte of drukke gebieden, zoals vliegvelden.

I

Intranet

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

Invoegtoepassing

Een stukje software dat extra voorzieningen toevoegt aan een programma. Dankzij invoegtoepassingen kan een 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).

IP-adres

Internet Protocol-adres. Een adres voor een computer of apparaat in een TCP/IP-netwerk. 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 of lokaal netwerk. Een computernetwerk dat een relatief klein gebied omvat (bijvoorbeeld één gebouw). Computers in 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 gescand. Als u een item per ongeluk als vertrouwd hebt aangemerkt (bijvoorbeeld een mogelijk ongewenst programma) of als u wilt dat het weer wordt gescand, moet u het uit deze lijst verwijderen.

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 elk fysiek apparaat, zoals een netwerkkaart (NIC), met toegang 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 werkgroepprogramma's (e-mail, voicemail en fax) via één enkele client kunnen werken, zoals de Exchange-client.

Mogelijk ongewenst programma (MOP)

Een programma dat mogelijk ongewenst is, ook al heeft de gebruiker het misschien zelf gedownload, omdat het de beveiligings- of privacyinstellingen kan veranderen op de computer waarop het wordt geïnstalleerd. MOP's kunnen (dit is niet altijd zo) spyware, adware en inbelprogramma's bevatten en worden soms ongemerkt, samen met gewenste programma's, gedownload.

MSN

Microsoft Network. Een verzameling internetservices die door Microsoft worden geboden, waaronder een zoekprogramma, e-mail, expresberichten en een portaal.

N

Netwerk

Een verzameling systemen op basis van het internetprotocol (IP), zoals routers, switches, servers en firewalls, die als logische eenheid zijn gegroepeerd. Zo kan bijvoorbeeld 'Netwerk Financieel' bestaan uit alle servers, routers en systemen op een financiële afdeling. Zie ook thuisnetwerk (pagina 270).

Netwerkoverzicht

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

Netwerkstation

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

NIC

Netwerkkaart. 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 (pagina 261).

O

Onbetrouwbare toegangspunt

Een niet-gemachtigd toegangspunt. Onbetrouwbare toegangspunten kunnen op een beveiligd bedrijfsnetwerk worden geïnstalleerd voor het verlenen van toegang aan niet-gemachtigde partijen. Via dergelijke punten kunnen ook man-in-het-midden-aanvallen worden uitgevoerd.

P

Phishing

Een vorm van fraude waarbij persoonlijke gegevens, zoals wachtwoorden, sofinummers en creditcardgegevens, worden gevraagd in vervalste e-mailberichten die eruitzien alsof ze van vertrouwde afzenders komen, zoals banken of legitieme bedrijven. Meestal staat in phishing-e-mails een verzoek om op een koppeling te klikken of om uw contactgegevens dan wel creditcardgegevens te geven of bij te werken.

Poort

Een hardwareadres voor het doorsturen van gegevens (in- en uitgaand). Pc's hebben diverse poorten: interne poorten voor het aansluiten van schijfstations, een beeldscherm en een toetsenbord; en externe poorten voor het aansluiten van modems, printers, een muis en andere randapparatuur.

Pop-up

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-mailclient 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 met Ethernet als transportlaag.

Protocol

Een verzameling regels voor het uitwisselen van gegevens tussen computers en andere apparaten. In een gelaagde netwerkarchitectuur (het Open Systems Interconnection-model) heeft elke laag zijn eigen protocollen, die bepalen hoe de communicatie op dat niveau moet plaatsvinden. Uw computer of apparaat moet het juiste protocol ondersteunen voor de communicatie met andere computers. Zie ook OSI (Open Systems Interconnection).

Proxy

Een computer (of de software die erop wordt uitgevoerd) die fungeert als een barrière tussen een netwerk en internet door slechts één netwerkadres door te geven aan externe sites. Doordat de proxy alle interne computers vertegenwoordigt, wordt de identiteit van apparaten in het netwerk niet buiten het LAN prijsgegeven en is er toch internettoegang mogelijk. Zie ook proxyserver (pagina 267).

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 virtuele prullenbak voor verwijderde bestanden en mappen in Windows.

Publiceren

Een back-upbestand via internet beschikbaar maken. U hebt toegang tot gepubliceerde bestanden in de Backup and Restore-bibliotheek.

Q

Quarantaine

Afgedwongen isolatie van een bestand of map waarvan vermoed wordt dat er een virus, spam, verdachte inhoud of MOP's (mogelijk ongewenste programma's) in voorkomen, zodat die bestanden of mappen niet meer kunnen worden uitgevoerd of geopend.

R

RADIUS

Remote Access Dial-In User Service. Een protocol dat gebruikersverificatie biedt, doorgaans bij externe toegang. Het is oorspronkelijk ontworpen voor servers waarop wordt ingebeld, maar wordt tegenwoordig voor een scala van verificatieomgevingen gebruikt, bijvoorbeeld voor 802.1x-verificatie van het gedeelde geheim van WLAN-gebruikers. Zie ook gedeeld geheim.

Real-time scannen

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

Register

Een Windows-database waarin instellingen van elke computergebruiker en van de hardware, geïnstalleerde programma's en eigenschappen worden opgeslagen. De database bestaat uit allerlei 'sleutels' waarvoor waarden worden ingesteld. Ongewenste programma's kunnen de waarden van registersleutels wijzigen of nieuwe sleutels maken om schadelijke code uit te voeren.

Roaming

Van het ene toegangspunt naar een ander gaan zonder services te stoppen of de verbinding te verbreken.

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 voor uw computergegevens en persoonlijke gegevens.

Router

Een netwerkapparaat dat gegevenspakketten doorstuurt van het ene netwerk naar een ander. Routers 'lezen' elk binnenkomend pakket en sturen het door op basis van het bron- en doeladres, en van het netwerkverkeer. Routers worden soms ook 'toegangspunt' genoemd.

S

Scannen op verzoek

Een gepland onderzoek van geselecteerde bestanden, toepassingen of netwerkapparaten om bedreigingen, kwetsbare punten en andere ongewenste code op te sporen. Het kan direct, op één gepland tijdstip of regelmatig met een bepaald interval worden uitgevoerd. Vergelijken met scannen bij toegang. Zie ook 'kwetsbare punten'.

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 die of dat verbindingen aanvaardt van andere computers of programma's en relevante antwoorden terugstuurt. 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 (pagina 272), WPA (pagina 273), WPA2 (pagina 273), WPA2-PSK (pagina 273), WPA-PSK (pagina 273).

Slim station

Zie USB-station (pagina 271).

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.

SSID

Serviceset-id. 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 via 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 wordt vereist, beginnen met https in plaats van http.

Standaard-e-mailaccount

Zie POP3 (pagina 266).

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 bij belangrijke systeemgebeurtenissen (bijvoorbeeld wanneer een programma of stuurprogramma wordt geïnstalleerd). U kunt ook 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

Thuisnetwerk

Twee of meer computers die in een thuissituatie met elkaar zijn verbonden voor het delen van bestanden en internettoegang. Zie ook LAN (pagina 264).

Tijdelijk bestand

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

TKIP

Temporal Key Integrity Protocol. Een gedeelte van de 802.11i coderingsstandaard voor draadloze LAN's. TKIP is de nieuwste generatie WEP en dient ter beveiliging van draadloze LAN's op basis van het 802.11 protocol. TKIP voorziet in de tekortkomingen van WEP met een voorziening voor berichtintegriteit, een mechanisme voor het wijzigen van sleutels en een methode om sleutels per pakket te combineren.

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 draadloze gebruikers. Als draadloze gebruikers hun mobiele apparatuur op verschillende locaties gebruiken, gaat de transmissie over van het ene toegangspunt naar het andere, zodat de verbinding niet wegvalt.

Trojaans paard

Een programma dat zich niet vermenigvuldigt maar wel schade veroorzaakt of de beveiliging van computers in gevaar brengt. Trojaanse paarden worden meestal door een ander per e-mail verzonden; ze verzenden zichzelf niet. Ook kunt u ongemerkt Trojaanse paarden van een website of een peer-to-peer-netwerk downloaden.

U

U3

Staat voor driemaal 'You': vereenvoudigd voor u, slimmer voor u, mobiel als u. Een platform waarmee Windows 2000- of XP-programma's vanaf een USB-station kunnen worden uitgevoerd. 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. Dit is de standaardindeling voor internetadressen.

USB

Universal Serial Bus. Een gestandaardiseerde aansluiting op de meeste computers, waarmee onder meer toetsenborden, muizen, webcams scanners en printers kunnen worden aangesloten.

USB-adapter voor draadloze netwerken

Een adapter voor draadloos netwerkverkeer die wordt aangesloten op een USB-poort van de computer.

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 controleren van de digitale identiteit van de afzender van een elektronisch bericht.

Virus

Een computerprogramma dat zichzelf kan kopiëren en computers kan infecteren zonder dat de gebruiker het merkt.

VPN

Virtual Private Network (virtueel particulier netwerk). Een particulier netwerk dat tot stand wordt gebracht op een openbaar netwerk met hosts, zoals internet. De gegevens die via de VPN-verbinding worden verzonden, zijn met sterke codering versleuteld.

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

E-mail via internet. Een service om online e-mail te beheren in een browser, en niet in een e-mailclient, zoals Microsoft Outlook. Zie ook e-mail (pagina 263).

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 zekere tekortkomingen. WEP draagt bij aan betere beveiliging 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 of e-mailadressen die veilig worden geacht. Gebruikers mogen websites op een witte lijst openen. E-mailadressen op een witte lijst zijn vertrouwde afzenders van wie u de berichten wilt ontvangen. Vergelijken met zwarte lijst (pagina 273).

WLAN

Wireless Local Area Network. Een lokaal netwerk (LAN) via een draadloze verbinding. In een WLAN worden hoogfrequente radiogolven in plaats van kabels gebruikt voor de communicatie tussen computers.

Woordenboekaanval

Een type aanval met grof geweld waarbij veelgebruikte woorden worden gebruikt om een wachtwoord te ontdekken.

Worm

Een virus dat zich verspreidt door duplicaten van zichzelf te maken op andere stations, systemen of netwerken. Een bulkmailworm verspreidt zich dankzij een handeling van de gebruiker. De gebruiker moet bijvoorbeeld een bijlage openen of een gedownload bestand uitvoeren. De meeste e-mailvirussen zijn tegenwoordig wormen. Er zijn ook wormen die zich zonder handeling van de gebruiker verspreiden. Voorbeelden van zichzelf verspreidende wormen zijn Blaster en Sasser.

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 standaard 802.11i. Wanneer WPA correct is geïnstalleerd, biedt het gebruikers van draadloze LAN's een vrij grote zekerheid 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 het wachtwoord op elke draadloze computer en elk draadloos toegangspunt regelmatig worden gewijzigd. Zie ook WPA2-PSK (pagina 273), TKIP (pagina 270).

WPA2

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

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-spam: een lijst met e-mailadressen waarvan u geen berichten wilt ontvangen omdat u van deze adressen spam verwacht. Bij anti-phising: een lijst met websites die als frauduleus worden beschouwd. Vergelijken met witte lijst (pagina 272).

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.

Licentie

Copyright

HOOFDSTUK 51

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

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.

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

Ondersteuning en downloads

Land/regio	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

Land/regio	Ondersteuning van McAfee	Downloads van McAfee
Canada (Frans)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp?langid=48
China (vereenvoudigd Chinees)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
Denemarken	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Duitsland	www.mcafeehilfe.com	de.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
Griekenland	www.mcafeehelp.com	el.mcafee.com/root/downloads.asp
Hongarije	www.mcafeehelp.com	hu.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
Rusland	www.mcafeehelp.com	ru.mcafee.com/root/downloads.asp
Slowakije	www.mcafeehelp.com	sk.mcafee.com/root/downloads.asp
Spanje	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Taiwan	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Tsjechië	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Turkije	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp

Land/regio	Ondersteuning van McAfee	Downloads van McAfee
Verenigd Koninkrijk	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
Verenigde Staten	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp
Zweden	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp

Gebruikershandleidingen voor McAfee Total Protection

Land/regio	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 (vereenvoudigd Chinees)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
Denemarken	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Duitsland	download.mcafee.com/products/manuals/de/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
Griekenland	download.mcafee.com/products/manuals/el/MTP_userguide_2008.pdf
Hongarije	download.mcafee.com/products/manuals/hu/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
Nederland	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
Noorwegen	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf

Land/regio	McAfee-gebruikershandleidingen
Polen	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
Rusland	download.mcafee.com/products/manuals/ru/MTP_userguide_2008.pdf
Slowakije	download.mcafee.com/products/manuals/sk/MTP_userguide_2008.pdf
Spanje	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Tsjechië	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Turkije	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
Verenigd Koninkrijk	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
Verenigde Staten	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf
Zweden	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf

Gebruikershandleidingen voor McAfee Internet Security

Land/regio	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 (vereenvoudigd Chinees)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
Denemarken	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Duitsland	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf

Land/regio	McAfee-gebruikershandleidingen
Finland	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
Frankrijk	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Griekenland	download.mcafee.com/products/manuals/el/MIS_userguide_2008.pdf
Hongarije	download.mcafee.com/products/manuals/hu/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
Nederland	download.mcafee.com/products/manuals/nl/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
Rusland	download.mcafee.com/products/manuals/ru/MIS_userguide_2008.pdf
Slowakije	download.mcafee.com/products/manuals/sk/MIS_userguide_2008.pdf
Spanje	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Tsjechië	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Turkije	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
Verenigd Koninkrijk	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Verenigde Staten	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf
Zweden	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf

Gebruikershandleidingen voor McAfee VirusScan Plus

Land/regio	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 (vereenvoudigd Chinees)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
Denemarken	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Duitsland	download.mcafee.com/products/manuals/de/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
Griekenland	download.mcafee.com/products/manuals/el/VSP_userguide_2008.pdf
Hongarije	download.mcafee.com/products/manuals/hu/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
Nederland	download.mcafee.com/products/manuals/nl/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
Rusland	download.mcafee.com/products/manuals/ru/VSP_userguide_2008.pdf

Land/regio	McAfee-gebruikershandleidingen
Slowakije	download.mcafee.com/products/manuals/sk/VSP_userguide_2008.pdf
Spanje	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Tsjechië	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf
Turkije	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
Verenigd Koninkrijk	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Verenigde Staten	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf
Zweden	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf

Gebruikershandleidingen voor McAfee VirusScan

Land/regio	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 (vereenvoudigd Chinees)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
Denemarken	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Duitsland	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
Frankrijk	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Griekenland	download.mcafee.com/products/manuals/el/VS_userguide.2008.pdf
Hongarije	download.mcafee.com/products/manuals/hu/VS_userguide.2008.pdf

Land/regio	McAfee-gebruikershandleidingen
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
Nederland	download.mcafee.com/products/manuals/nl/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
Rusland	download.mcafee.com/products/manuals/ru/VS_userguide_2008.pdf
Slowakije	download.mcafee.com/products/manuals/sk/VS_userguide_2008.pdf
Spanje	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Tsjechië	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Turkije	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
Verenigd Koninkrijk	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Verenigde Staten	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf
Zweden	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf

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

Land/regio	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 (vereenvoudigd Chinees)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
Denemarken	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Duitsland	www.mcafee.com/us/threat_center	de.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
Griekenland	www.mcafee.com/us/threat_center	gr.mcafee.com/virusInfo
Hongarije	www.mcafee.com/us/threat_center	hu.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
Nederland	www.mcafee.com/us/threat_center	nl.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
Rusland	www.mcafee.com/us/threat_center	ru.mcafee.com/virusInfo
Slowakije	www.mcafee.com/us/threat_center	sk.mcafee.com/virusInfo
Spanje	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Taiwan	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Tsjechië	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo

Turkije	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
Verenigd Koninkrijk	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Verenigde Staten	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo
Zweden	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo

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

Land/regio	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 (vereenvoudigd Chinees)	www.hackerwatch.org/?lang=zh-cn
Denemarken	www.hackerwatch.org/?lang=da
Duitsland	www.hackerwatch.org/?lang=de
Finland	www.hackerwatch.org/?lang=fi
Frankrijk	www.hackerwatch.org/?lang=fr
Griekenland	www.hackerwatch.org/?lang=el
Hongarije	www.hackerwatch.org/?lang=hu
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
Nederland	www.hackerwatch.org/?lang=nl
Noorwegen	www.hackerwatch.org/?lang=no
Polen	www.hackerwatch.org/?lang=pl
Portugal	www.hackerwatch.org/?lang=pt-pt
Rusland	www.hackerwatch.org/?lang=ru
Slowakije	www.hackerwatch.org/?lang=sk
Spanje	www.hackerwatch.org/?lang=es
Taiwan	www.hackerwatch.org/?lang=zh-tw
Tsjechië	www.hackerwatch.org/?lang=cs

Turkije	www.hackerwatch.org/?lang=tr
Verenigd Koninkrijk	www.hackerwatch.org
Verenigde Staten	www.hackerwatch.org
Zweden	www.hackerwatch.org/?lang=sv

Index

D

E

F

G

H

U

V

W

Z