



Avira

Internet Security Suite

Gebruikershandleiding

Handelsmerken en auteursrechten

Handelsmerken

Windows is een geregistreerd handelsmerk van Microsoft Corporation in de Verenigde Staten en andere landen. Alle anderen merk- en productnamen zijn handelsmerken of gedeponeerde handelsmerken van hun respectievelijke eigenaars. Beschermd handelsmerken worden niet als zodanig aangegeven in deze handleiding. Dit betekent echter niet dat deze vrijelijk mogen worden gebruikt.

Informatie auteursrecht

Voor Avira Internet Security Suite is code gebruikt die door derden ter beschikking is gesteld. Wij zijn de eigenaren van de auteursrechten dankbaar dat ze de code aan ons ter beschikking hebben gesteld. Voor meer informatie over auteursrechten, zie Third Party Licenses.

Licentieovereenkomst voor eindgebruikers - EULA

<http://www.avira.com/nl/license-agreement>

Privacybeleid

<http://www.avira.com/nl/general-privacy>

Inhoudsopgave

1. Introductie	10
1.1 Iconen en accentueringen	10
2. Productinformatie.....	12
2.1 Leveringsomvang	12
2.2 Systeemvereisten	13
2.2.1 Systeemvereisten Avira Internet Security Suite	13
2.2.2 Avira SearchFree Toolbar	14
2.2.3 Administrator-rechten (sinds Windows Vista)	14
2.2.4 Incompatibiliteit met andere programma's	15
2.3 Licenties en upgraden.....	16
2.3.1 Licenties	16
2.3.2 Verlengen van een licentie.....	16
2.3.3 Upgraden	16
2.3.4 Licentiebeheer.....	17
3. Installatie en de-installatie	19
3.1 Voorbereiden voor de installatie.....	19
3.2 Installeren vanaf cd indien online.....	20
3.3 Installeren vanaf cd indien offline.....	20
3.4 Software die van de Avira-winkel is gedownload, installeren.....	20
3.5 Incompatibele software verwijderen	21
3.6 Een installatietype kiezen	21
3.6.1 Een Express Installation uitvoeren	22
3.6.2 Een aangepaste installatie uitvoeren.....	23
3.7 Avira Internet Security Suite installeren	23
3.7.1 Een bestemmingsmap kiezen	24
3.7.2 Avira SearchFree Toolbar installeren	25
3.7.3 Installatieonderdelen kiezen	25
3.7.4 Snelkoppelingen maken voor Avira Internet Security Suite.....	28
3.7.5 Avira Internet Security Suite activeren	29
3.7.6 Proxy-instellingen definiëren.....	30
3.7.7 Het heuristische detectieniveau configureren (AHeAD)	32

3.7.8	Uitgebreide bedreigingscategorieën selecteren	33
3.7.9	Een scan starten na de installatie	33
3.8	De installatie wijzigen	34
3.8.1	Een installatie wijzigen onder Windows 8	34
3.8.2	Een installatie wijzigen onder Windows 7	35
3.8.3	Een installatie wijzigen onder Windows XP	36
3.9	De-installatie	36
3.9.1	Avira Internet Security Suite onder Windows 8 de-installeren	36
3.9.2	Avira Internet Security Suite onder Windows 7 de-installeren	37
3.9.3	Avira Internet Security Suite onder Windows XP de-installeren	38
3.9.4	Avira SearchFree Toolbar de-installeren	39
4.	Overzicht van Avira Internet Security Suite	42
4.1	Gebruikersinterface en werking	42
4.1.1	Control Center	42
4.1.2	Configuratie	45
4.1.3	Taakbalkicoon	49
4.2	Avira SearchFree Toolbar	50
4.2.1	Gebruik	51
4.2.2	Opties	54
4.2.3	Avira SearchFree Toolbar de-installeren onder Windows 7	58
4.3	Hoe te...?	58
4.3.1	Licentie activeren	58
4.3.2	Product activeren	59
4.3.3	Automatische updates uitvoeren	60
4.3.4	Start een handmatige update	62
4.3.5	Een scanprofiel gebruiken om te scannen op virussen en malware	62
4.3.6	Scan op virussen en malware door middel van slepen en neerzetten	64
4.3.7	Scan op virussen en malware via het contextmenu	64
4.3.8	Scan automatisch op virussen en malware	65
4.3.9	Gerichte scan naar Rootkits en actieve malware	67
4.3.10	Reageer op gedetecteerde virussen en malware	67
4.3.11	Bestanden in quarantaine afhandelen (*.qua):	72
4.3.12	Herstellen van bestanden in quarantaine	75
4.3.13	Verplaats verdachte bestanden naar quarantaine	76
4.3.14	Het bestandstype in een scanprofiel bewerken of verwijderen	77
4.3.15	Maak een bureaubladsnelkoppeling voor een scanprofiel	77
4.3.16	Filter gebeurtenissen	78
4.3.17	Sluit e-mailadressen uit van scan	79

5.	Detectie.....	80
5.1	Overzicht	80
5.2	Interactieve actiemodus	80
5.2.1	Waarschuwing.....	81
5.2.2	Detectie, Fouten, Waarschuwingen	81
5.2.3	Opties in het contextmenu.....	82
5.2.4	Speciale features wanneer geïnfecteerde bootsectors, rootkits en actieve malware wordt gedetecteerd.....	83
5.2.5	Knoppen en links.....	84
5.2.6	Speciale functies wanneer malware wordt gedetecteerd terwijl Web Protection inactief is	84
5.3	Bestanden versturen naar de Protection Cloud	84
5.3.1	Weergegeven informatie.....	85
5.3.2	Knoppen en links.....	85
5.4	Real-Time Protection.....	86
5.5	Verdacht gedrag	87
5.5.1	Waarschuwing van Real-Time Protection: Verdacht toepassingsgedrag gedetecteerd..	87
5.5.2	Naam en pad van het momenteel gedetecteerde verdachte programma.....	88
5.5.3	Opties.....	88
5.5.4	Knoppen en links.....	88
5.6	Inkomende e-mails	89
5.6.1	Waarschuwing.....	89
5.6.2	Detecties, Fouten, Waarschuwingen	89
5.6.3	Opties.....	90
5.6.4	Knoppen en links.....	91
5.7	Uitgaande e-mails.....	91
5.7.1	Waarschuwing.....	92
5.7.2	Detecties, Fouten, Waarschuwingen	92
5.7.3	Opties.....	92
5.7.4	Knoppen en links.....	93
5.8	Afzender	93
5.8.1	Waarschuwing.....	94
5.8.2	Gebruikt programma, gebruikte SMTP-server en het adres van de afzender van de e-mail	94
5.9	Server	94
5.9.1	Waarschuwing.....	95
5.9.2	Gebruikt programma, gebruikte SMTP-server.....	95

5.10	Web Protection	95
6.	Scanner.....	98
6.1	Scanner	98
6.2	Luke Filewalker.....	98
6.2.1	Luke Filewalker: scanstatus-venster	99
6.2.2	Luke Filewalker: Scanstatistieken.....	102
7.	Control Center	104
7.1	Control Center Overzicht	104
7.2	Bestand	107
7.2.1	Afsluiten.....	107
7.3	Weergave	107
7.3.1	Status	107
7.3.2	Spelmodus	121
7.3.3	Scanner	122
7.3.4	Handmatig kiezen	124
7.3.5	Real-Time Protection	127
7.3.6	FireWall	129
7.3.7	Web Protection	129
7.3.8	Mail Protection	131
7.3.9	Avira Free Android Security.....	133
7.3.10	Quarantaine	134
7.3.11	Planner	140
7.3.12	Rapporten.....	144
7.3.13	Gebeurtenissen.....	146
7.3.14	Vernieuwen	149
7.4	Extra's.....	149
7.4.1	Bootrecords scannen	149
7.4.2	Detectielijst.....	149
7.4.3	Herstel-cd downloaden.....	150
7.4.4	Configuratie.....	151
7.5	Update	151
7.5.1	Start update.....	151
7.5.2	Handmatige update.....	151
7.6	Help.....	151
7.6.1	Topics	151
7.6.2	Help me	151

7.6.3	Live ondersteuning	152
7.6.4	Forum.....	152
7.6.5	Handleiding downloaden.....	152
7.6.6	Licentiebeheer.....	152
7.6.7	Product aanbevelen.....	153
7.6.8	Feedback geven.....	153
7.6.9	Over Avira Internet Security Suite.....	154
8.	Bescherming van mobiele apparatuur	155
9.	Configuratie.....	156
9.1	Configuratie.....	156
9.2	Scanner	158
9.2.1	Scan	158
9.2.2	Rapport.....	167
9.3	Real-Time Protection.....	168
9.3.1	Scan	168
9.3.2	Rapport.....	179
9.4	Update	181
9.4.1	Webserver	181
9.5	FireWall.....	183
9.5.1	De FireWall configureren	183
9.5.2	Windows Firewall	183
9.6	Web Protection	186
9.6.1	Scan	186
9.6.2	Rapport.....	194
9.7	Mail Protection	195
9.7.1	Scan	195
9.7.2	Algemeen.....	202
9.7.3	Rapport.....	204
9.8	Algemeen	205
9.8.1	Dreigingscategorieën	205
9.8.2	Geavanceerde bescherming	206
9.8.3	Wachtwoord	210
9.8.4	Beveiliging	213
9.8.5	WMI	214
9.8.6	Gebeurtenissen.....	215
9.8.7	Rapporten.....	215

9.8.8	Mappen.....	216
9.8.9	Akoestische waarschuwingen	216
9.8.10	Waarschuwingen.....	217
10.	Taakbalkicoon	219
11.	In-productberichten	220
11.1.1	Product Message Subscription Center.....	220
11.1.2	Actuele informatie	220
12.	FireWall	221
12.1	Windows Firewall.....	221
13.	Updates.....	222
13.1	Updates	222
13.2	Updater.....	223
14.	FAQ, Tips.....	225
14.1	Hulp bij een probleem	225
14.2	Snelkoppelingen	229
14.2.1	In dialoogvensters.....	229
14.2.2	In help	230
14.2.3	In het Control Center.....	231
14.3	Windows Security Center	233
14.3.1	Algemeen.....	233
14.3.2	Het Windows Security Center en uw Avira-product	234
14.4	Windows Action Center.....	236
14.4.1	Algemeen.....	236
14.4.2	Het Windows Action Center en uw Avira-product.....	237

15. Virussen en meer.....	242
15.1 Dreigingscategorieën	242
15.2 Virussen en andere malware.....	246
16. Informatie en Service	250
16.1 Contactadres.....	250
16.2 Technische ondersteuning.....	250
16.3 Verdacht bestand.....	251
16.4 Valse positieven rapporteren.....	251
16.5 Uw feedback voor meer veiligheid.....	251

1. Introductie

Uw Avira-product beschermt uw computer tegen virussen, wormen, Trojaanse paarden, adware, spyware en andere risico's. In deze handleiding wordt hieraan gerefereerd als virussen of malware (schadelijke software) en ongewenste programma's.

De handleiding beschrijft de installatie en werking van het programma.

Voor meer opties en informatie, kunt u onze website bezoeken:

<http://www.avira.nl>

De Avira website biedt u:

- toegang tot informatie over andere Avira-desktopprogramma's
- het downloaden van de laatste Avira-desktopprogramma's
- het downloaden van de laatste producthandleidingen in PDF-formaat
- het downloaden van gratis ondersteunings- en reparatietools
- toegang tot onze uitgebreide kennisdatabase en FAQs voor probleemoplossing
- toegang tot landspecifieke ondersteuningsadressen.

Uw Avira Team

1.1 Iconen en accentueringen

De volgende iconen worden gebruikt:

Icoon / Bestemming	Uitleg
✓	Geplaatst voor een voorwaarde die vervuld moet worden voordat een actie wordt uitgevoerd.
▶	Geplaatst voor een actie-stap die u onderneemt.
→	Geplaatst voor een gebeurtenis die de vorige actie opvolgt.
Waarschuwing	Geplaatst voor een waarschuwing wanneer belangrijk dataverlies plaats kan vinden.

Opmerking	Geplaatst voor een link naar bijzonder belangrijke informatie of een tip die uw Avira-product makkelijker in het gebruik maakt.
------------------	---

De volgende accentueringen worden gebruikt:

Accentuering	Uitleg
<i>Cursief</i>	Bestandsnaam of gegevenspad.
	Weergegeven software interface-elementen (bijv. schermsectie of waarschuwing).
Vet	Aanklikbare software interface-elementen (bijv. menu-item, navigatiegebied, keuzevak of knop).

2. Productinformatie

Dit hoofdstuk bevat alle relevante informatie over de aanschaf en het gebruik van uw Avira-product:

- Zie Hoofdstuk: [Leveringsomvang](#)
- Zie Hoofdstuk: [Systeemvereisten](#)
- Zie Hoofdstuk: [Licenties en Upgrade](#)
- Zie Hoofdstuk: [Licentiemanager](#)

Avira-producten zijn uitgebreide en flexibele tools waarop u kunt vertrouwen om uw computer te beschermen tegen virussen, malware, ongewenste programma's en andere gevaren.

- ▶ Let alstublieft op de volgende informatie:

Waarschuwing

Verlies van waardevolle data heeft meestal dramatische consequenties. Zelfs het beste virusbeschermingsprogramma kan niet honderd procent bescherming bieden tegen gegevensverlies. Maak regelmatig kopieën (back-ups) van uw data voor veiligheidsdoeleinden.

Let op

Een programma kan alleen betrouwbare en effectieve bescherming tegen virussen, malware, ongewenste programma's en andere gevaren bieden als het up-to-date is. Zorg ervoor dat uw Avira-product up-to-date is met automatische updates. Configureer het programma dienovereenkomstig.

2.1 Leveringsomvang

Uw Avira-product heeft de volgende functies:

- Control Center voor het monitoren, beheren en controleren van het hele programma
- Centrale configuratie met gebruikersvriendelijke standaard- en geavanceerde opties en contextgevoelige help
- Scanner (scan op aanvraag) met profielgecontroleerde en configureerbare scan voor alle bekende soorten virussen en malware
- Integratie in de Windows User Account Control stelt u in staat taken uit te voeren die administrator-rechten vereisen.
- Real-Time Protection (scan bij toegang) voor continue bewaking van alle pogingen toegang te krijgen tot bestanden

- ProActiv-component voor de permanente bewaking van programma-acties (alleen voor 32-bitssystemen)
- Mail Protection (POP3 Scanner, IMAP Scanner en SMTP Scanner) voor de permanente controle van e-mails op virussen en kwaadaardige software, met inbegrip van de controle van e-mailbijlagen
- Avira SearchFree werkbalk, een zoek-werkbalk geïntegreerd in de webbrowser waarmee u snel en gemakkelijk zoekopties beschikbaar heeft. Het bevat ook elementen van de meest voorkomende internetfuncties.
- Web Protection voor het controleren van gegevens en bestanden overgedragen vanuit het internet met behulp van het HTTP-protocol (controle van de poorten 80, 8080, 3128)
- De Avira Free Android Security-app is niet alleen gericht op antidiefstalmaatregelen. De app helpt om uw mobiele apparaat terug te krijgen als het is verloren, of nog erger: als het is gestolen. Afgezien daarvan stelt de app u in staat inkomende oproepen of SMS te blokkeren. Avira Free Android Security beschermt mobiele telefoons en smartphones die draaien onder het Android-besturingssysteem.
- Geïntegreerd quarantainebeheer om verdachte bestanden te isoleren en te verwerken
- Rootkit Protection voor het opsporen van verborgen kwaadaardige software geïnstalleerd op uw computersysteem (rootkits) (Niet beschikbaar onder Windows XP 64-bit)
- Directe toegang tot gedetailleerde informatie over de gedetecteerde virussen en kwaadaardige software via het internet
- Eenvoudige en snelle updates van het programma, virusdefinities en zoekmachine door middel van Single File Update en incrementele VDF-updates via een webserver op het internet
- Gebruikersvriendelijk licentiëren met de Licentiemanager
- Geïntegreerde Planner voor het plannen van eenmalige of terugkerende taken zoals updates of scans
- Extreem hoge detectie van virussen en kwaadaardige software via innovatieve scantechnologie (scan-engine) met inbegrip van heuristische scanmethode
- Detectie van alle conventionele archieftypes inclusief detectie van geneste archieven en slimme extensiedetectie
- High-performance multithreadingfunctie (gelijktijdig met hoge-snelheidsscan van meerdere bestanden)

2.2 Systeemvereisten

2.2.1 Systeemvereisten Avira Internet Security Suite

Avira Internet Security Suite stelt de volgende eisen voor een succesvol gebruik van het systeem:

Besturingssysteem

- Windows 8, nieuwste SP (32- of 64-bits) of
- Windows 7, nieuwste SP (32- of 64-bits) of
- Windows XP, nieuwste SP (32- of 64-bits)

Hardware

- Computer met Pentium-processor, of later, tenminste 1 GHz
- Minimaal 150 MB beschikbare ruimte op de harddisk (meer, als quarantaine wordt gebruikt voor tijdelijk opslaan)
- Minimaal 1024 MB RAM onder Windows 8, Windows 7
- Minimaal 512 MB RAM onder Windows XP

Overige vereisten

- Voor de installatie van het programma: administrator-rechten
- Voor alle installaties: Windows Internet Explorer 6.0 of hoger
- Waar nodig een internetverbinding (zie [Vorbereiden voor de installatie](#))

2.2.2 Avira SearchFree Toolbar

- Besturingssysteem
 - Windows XP, nieuwste SP (32 of 64 bit) of
 - Windows 7, nieuwste SP (32 of 64 bit) of
 - Windows 8, nieuwste SP (32 of 64 bit)
- Webbrowser
 - Windows Internet Explorer 6.0 of hoger
 - Mozilla Firefox 3.0 of hoger
 - Google Chrome 18.0 of hoger

Let op

Indien nodig, verwijder eventuele eerder geïnstalleerde zoek-werkbalken voordat u de Avira SearchFree-werkbalk installeert. Anders bent u niet in staat de Avira SearchFree Toolbar te installeren.

2.2.3 Administrator-rechten (sinds Windows Vista)

Onder Windows XP werken veel gebruikers met administrator-rechten. Dit is echter niet wenselijk vanuit het oogpunt van beveiliging omdat dan gemakkelijk virussen en ongewenste programma's computers kunnen infiltreren.

Om deze reden introduceerde Microsoft het "Gebruikersaccountbeheer" (UAC = User Account Control). Gebruikersaccountbeheer is onderdeel van de volgende besturingssystemen:

- Windows Vista
- Windows 7
- Windows 8

Gebruikersaccountbeheer biedt meer bescherming voor gebruikers die zijn aangemeld als administrator. Op die manier heeft een administrator aanvankelijk alleen de bevoegdheden die een normale gebruiker heeft. Acties waarvoor administrator-rechten nodig zijn, worden duidelijk gemarkeerd door het besturingssysteem met een informatiepictogram. Bovendien moet de gebruiker expliciet de gevraagde actie bevestigen. Rechten worden alleen dan verhoogd en de administratieve taak wordt pas uitgevoerd door het besturingssysteem nadat deze toestemming is verkregen.

Avira Internet Security Suite vereist administrator-rechten voor sommige acties. Deze acties zijn gemarkeerd met het volgende symbool: . Als dit symbool ook verschijnt op een knop, zijn administrator-rechten vereist voor het uitvoeren van de actie. Als uw huidige gebruikersaccount geen administrator-rechten heeft, vraagt het Windows-dialogvenster van het Gebruikersaccountbeheer u om het administrator-wachtwoord in te voeren. Wanneer u geen administrator-wachtwoord heeft, kunt u de actie niet uitvoeren.

2.2.4 Incompatibiliteit met andere programma's

Avira Internet Security Suite

Avira Internet Security Suite kan op dit moment niet worden gebruikt met de volgende producten:

- PGP Desktop Home
- PGP Desktop Professional 9.0
- CyberPatrol

Een fout in deze producten kan ertoe leiden dat Avira Mail Protection POP3-scanner) in Avira Internet Security niet werkt of dat het systeem instabiel wordt. Avira werkt samen met PGP en CyberPatrol aan een oplossing voor dit probleem. Totdat er een oplossing is gevonden, raden we u echter aan deze producten te verwijderen voordat u Avira Internet Security Suite installeert.

Avira Web Protection

Avira Web Protection is niet compatibel met de volgende producten:

- Teleport Pro van Tennyson Maxwell, Inc
- CHIPDRIVE® Time Recording van SCM Microsystems
- MSN Messenger van Microsoft

Gegevens die door deze producten worden verzonden of aangevraagd, worden genegeerd door Avira Web Protection.

Opmerking

Avira Mail Protection werkt niet als er al een e-mailserver (zoals AVM KEN of Exchange) op de computer is geïnstalleerd.

2.3 Licenties en upgraden

2.3.1 Licenties

Om uw Avira-product te kunnen gebruiken, hebt u een licentie nodig. U accepteert daarmee de licentievoorwaarden.

De licentie wordt verstrekt in de vorm van een activeringscode. De activeringscode is een code bestaande uit letters en cijfers die u ontvangt na aankoop van het Avira-product. De activeringscode bevat de exacte gegevens van uw licentie, bijvoorbeeld welke programma's in licentie zijn gegeven voor welke periode.

De activeringscode wordt naar u verzonden via e-mail, als u uw Avira-product hebt gekocht op het internet of het wordt aangegeven op de verpakking van het product.

Om uw programma van de licentie te voorzien, gelieve uw activeringscode in te voeren om het programma te activeren. De productactivering kan worden uitgevoerd tijdens de installatie. U kunt uw Avira-product echter ook activeren na de installatie in de License Manager, onder [Help > Licentiebeheer](#).

2.3.2 Verlengen van een licentie

Als uw licentie bijna verlopen is, stuurt Avira een [schuifvenster](#) om u eraan te herinneren dat u uw licentie moet verlengen. Daarvoor hoeft u alleen maar een link aan te klikken, waarna u wordt doorgestuurd naar de Avira-onlineshop. U kunt de licentie voor uw Avira-product echter ook verlengen via de License Manager, onder [Help > Licentiebeheer](#)

Als u zich hebt laten registreren in het licentieportaal van Avira, kunt u bovendien uw licentie direct online via het **Licentie-overzicht** verlengen of de automatische vernieuwing van uw licentie selecteren.

2.3.3 Upgraden

In de License Manager heeft u de optie voor een product van de Avira-bureaubladproductenfamilie een upgrade te lanceren. Handmatige de-installatie van het oude product en handmatige installatie van het nieuwe product is niet vereist. Bij het upgraden met de License Manager voert u de activeringscode voor het product dat u wilt

upgraden in het License Manager-invoerveld in. Het nieuwe product wordt automatisch geïnstalleerd.

Om hoge betrouwbaarheid en beveiliging voor uw computer te bereiken, stuurt Avira een pop-up-item om u eraan te herinneren uw systeem te upgraden naar de nieuwste versie. Klik gewoon op de **Upgrade**-link op het pop-up-item en u wordt naar de specifieke upgrade site voor uw product geleid.

U hebt de mogelijkheid om uw huidige product te upgraden, of u kunt een uitgebreider product aanschaffen. De productoverzichtspagina toont welk soort product u momenteel gebruikt en biedt de kans om uw product te vergelijken met andere Avira-producten. Als u meer informatie nodig heeft, klikt u op het **informatie**-icoon rechts naast de naam van het product. Als u hetzelfde product wilt blijven gebruiken, klikt u op **Upgrade** en het downloaden van de nieuwe versie begint onmiddellijk. Wilt u een meer uitgebreid product aanschaffen dan klikt u op de **Kopen**-knop aan de onderkant van de productkolom. U wordt automatisch doorgestuurd naar de Avira-onlineshop waar u uw bestelling kunt plaatsen.

Let op

Afhankelijk van uw product en uw besturingssysteem heeft u mogelijk administrator-rechten nodig om de upgrade uit te voeren. Login als administrator voordat u een upgrade uitvoert.

2.3.4 Licentiebeheer

De Avira Internet Security Suite-licentiebeheer maakt een heel eenvoudige installatie van de Avira Internet Security Suite-licentie mogelijk.

Avira Internet Security Suite-licentiebeheer



U kunt de licentie installeren door het licentiebestand met een dubbelklik te selecteren in uw bestandsbeheer, of in de activatie e-mail, en de relevante instructies op het scherm te volgen.

Let op

De Avira Internet Security Suite-licentiebeheer kopieert automatisch de overeenkomstige licentie naar de relevante productmap. Indien er al een licentie bestaat, verschijnt een melding met de vraag of het bestaande licentiebestand moet worden vervangen. In dat geval wordt het bestaande bestand overschreven door het nieuwe licentiebestand.

3. Installatie en de-installatie

Dit hoofdstuk bevat informatie met betrekking tot de installatie van Avira Internet Security Suite.

- [Vorbereiden voor de installatie](#)
- [Installeren vanaf cd indien online](#)
- [Installeren vanaf cd indien offline](#)
- [Gedownload software installeren](#)
- [Incompatibele software verwijderen](#)
- [Een installatietype kiezen](#)
- [Avira Internet Security Suite installeren](#)
- [De installatie wijzigen](#)
- [Avira Internet Security Suite de-installeren](#)

3.1 Vorbereiden voor de installatie

- ✓ Controleer vóór de installatie of uw computer voldoet aan alle minimale systeemvereisten.
- ✓ Sluit alle actieve toepassingen.
- ✓ Zorg er voor dat geen andere virusbeschermingsprogramma's zijn geïnstalleerd. De automatische beschermingsfuncties van verschillende beveiligingsoplossingen kunnen elkaar verstoren (zie [Incompatibele software verwijderen](#) voor automatische opties).
- ✓ Verwijder, indien nodig, eventueel eerder geïnstalleerde zoekwerkbalken voordat u de Avira SearchFree Toolbar installeert. Anders kunt u de Avira SearchFree Toolbar niet installeren.
- ✓ Breng een internetverbinding tot stand.
- De verbinding is nodig voor het uitvoeren van de volgende stappen van de installatie:
 - Het downloaden van het huidige programmabestand en de scan-engine en de nieuwste virusdefinities via het installatieprogramma (voor op internet gebaseerde installatie)
 - Activeren van het programma
 - Registreren als gebruiker
 - Waar nodig, het uitvoeren van een update na voltooide installatie
- ✓ Houd de activeringscode of het licentiebestand voor uw Avira Internet Security Suite bij de hand als u het programma wilt activeren.
- ✓ Om uw product te activeren of te registreren, gebruikt uw Avira Internet Security Suite het HTTP-protocol en de poort 80 (webcommunicatie), evenals het coderingsprotocol SSL en poort 443, om te communiceren met de Avira-servers. Als u een firewall gebruikt, dient u ervoor te zorgen dat de vereiste verbindingen en/of

binnenkomende of uitgaande gegevens niet door de firewall worden geblokkeerd.

3.2 Installeren vanaf cd indien online

- ▶ Plaats de Avira Internet Security Suite-cd.

Als automatisch starten is ingeschakeld, klikt u op **Map openen** om bestanden weer te geven.

OF

Navigeer naar uw cd-station, klik met de rechtermuisknop op AVIRA en selecteer **Map openen** om bestanden weer te geven.

Dubbelklik op het bestand *autorun.exe*.

Kies de online versie die u wilt installeren in het cd-menu.

Het programma scant op incompatibele software (meer informatie hier: [Incompatibele software verwijderen](#)).

Klik op **Volgende** in het scherm *Welkom*.

Selecteer de taal en klik op **Volgende**. Alle bestanden die nodig zijn voor de installatie worden gedownload van de Avira-webservers.

Ga door met [Een installatietype kiezen](#).

3.3 Installeren vanaf cd indien offline

- ▶ Plaats de Avira Internet Security Suite-cd.

Als automatisch starten is ingeschakeld, klikt u op **Map openen** om bestanden weer te geven.

OF

Navigeer naar uw cd-station, klik met de rechtermuisknop op AVIRA en selecteer **Map openen** om bestanden weer te geven.

Dubbelklik op het bestand *autorun.exe*.

Kies de offline versie die u wilt installeren in het cd-menu.

Het programma scant op incompatibele software (meer informatie hier: [Incompatibele software verwijderen](#)).

Het installatiebestand wordt uitgepakt. De installatieprocedure wordt gestart.

Ga door met [Een installatietype kiezen](#).

3.4 Software die van de Avira-winkel is gedownload, installeren

- ▶ Ga naar www.avira.com/download.

Selecteer het product en klik op **Downloaden**.

Sla het gedownloade bestand op uw systeem op.

Dubbelklik op het installatiebestand `avira_internet_security_suite_en.exe`.

Klik op Ja in het venster Gebruikersaccountbeheer dat wordt weergegeven

Het programma scant op incompatibele software (meer informatie hier: [Incompatibele software verwijderen](#)).

Het installatiebestand wordt uitgepakt. De installatieprocedure wordt gestart.

Ga door met [Een installatietype kiezen](#).

3.5 Incompatibele software verwijderen

Avira Internet Security Suite zoekt naar mogelijke incompatibele software op uw computer. Als er potentieel incompatibele software wordt gedetecteerd, genereert Avira Internet Security Suite een lijst van deze programma's. Het wordt aanbevolen om deze programma's te verwijderen om te voorkomen dat de stabiliteit van uw computer in gevaar wordt gebracht.

- ▶ Selecteer de selectievakjes van alle programma's die automatisch moeten worden verwijderd van uw computer in de lijst en klik op **Volgende**.

Voor sommige producten moet de de-installatie handmatig worden bevestigd.

Selecteer die programma's en klik op **Volgende**.

De de-installatie van één of meer van de geselecteerde programma's kan vereisen dat de computer opnieuw wordt opgestart. Na het opnieuw opstarten wordt de installatie gestart.

3.6 Een installatietype kiezen

Tijdens de installatie kunt u een setuptype selecteren in de installatiewizard. De installatiewizard is ontworpen om u bij begeleiding bij de installatie te bieden.



Verwante onderwerpen:

- zie [Een Express Installation uitvoeren](#)
- zie [Een aangepaste installatie uitvoeren](#)

3.6.1 Een Express Installation uitvoeren

De *Express installation* is de aanbevolen installatiemethode.

- Deze installeert alle standaardonderdelen van Avira Internet Security Suite. De door Avira aanbevolen instellingen voor het beveiligingsniveau worden gebruikt.
- Standaard wordt een van de volgende installatiepaden gekozen:
 - `C:\Program Files\Avira` (voor Windows 32-bits versies) of
 - `C:\Program Files (x86)\Avira` (voor Windows 64-bits versies)
- Hier vindt u alle bestanden met betrekking tot Avira Internet Security Suite.
- Als u dit installatietype kiest, kunt u een installatie uitvoeren door gewoon op **Volgende** te klikken tot de installatie is voltooid.
- Deze installatiemethode is speciaal ontworpen voor gebruikers die niet goed op de hoogte zijn van softwarehulpprogramma's.

3.6.2 Een aangepaste installatie uitvoeren

Via *Aangepaste installatie* kunt u uw installatie configureren. Dit is alleen aanbevolen voor geavanceerde gebruikers die goed op de hoogte zijn van hard- en software en van beveiligingsproblemen.

- U kunt kiezen om individuele programmaonderdelen te installeren.
- Er kan een doelmap worden geselecteerd voor het installeren van de programmabestanden.
- U kunt **Creër een bureaubladpictogram en programmagroep in het menu Start** uitschakelen.
- Met de configuratiewizard kunt u aangepaste instellingen definiëren voor uw Avira Internet Security Suite. U kunt ook het beveiligingsniveau kiezen waarbij u zich op uw gemak voelt.
- Na de installatie kunt u een korte systeemscan starten die automatisch wordt uitgevoerd na de installatie.

3.7 Avira Internet Security Suite installeren



- ▶ Als u geen lid wilt worden van Avira, schakelt u het selectievakje **Ik wil mijn bescherming verbeteren door gebruik te maken van Avira ProActiv en Protection Cloud** dat standaard is ingeschakeld, uit.

Als u uw deelname aan de gemeenschap van Avira bevestigt, stuurt Avira Internet Security Suite de gegevens over gedetecteerde verdachte programma's naar het Avira Malware Research Center. De gegevens worden alleen gebruikt voor een geavanceerde online-scan en voor het uitbreiden en verfijnen van de detectietechnologie.

U kunt klikken op de koppelingen **ProActiv** en **Protection Cloud** om meer details over de uitgebreide online- en cloudscan te verkrijgen.

Bevestig dat u de **Eindgebruiker Licentie-Overeenkomst** accepteert. Voor het lezen van de gedetailleerde tekst van de **Eindgebruiker Licentie-Overeenkomst**, klikt u op de EULA-link.

3.7.1 Een bestemmingsmap kiezen

Met de aangepaste installatie kunt u de map kiezen waarin u Avira Internet Security Suite wilt installeren.



- ▶ Klik op **Bladeren** en navigeer naar de locatie waar u Avira Internet Security Suite wilt installeren.

Selecteer de map waarin u Avira Internet Security Suite wilt installeren in het venster **Bestemmingsmap kiezen**.

Klik op **Volgende**.

3.7.2 Avira SearchFree Toolbar installeren

Aan het einde van de setup kunt u de Avira SearchFree Toolbar installeren.

Avira SearchFree Toolbar bevat twee hoofdonderdelen: Avira SearchFree en de werkbalk.

Met Avira SearchFree kunt u op internet zoeken naar alle termen die u nodig hebt. Deze zoekmachine toont alle treffers in de browservensters met beoordeling van hun veiligheidsniveau. Hierdoor kunnen gebruikers van Avira veiliger navigeren op het internet.

De werkbalk biedt u drie widgets naar de belangrijkste met internet verwante functies. Met één klik heeft u direct toegang tot Facebook en uw email of kunt u zich verzekeren van veilig surfen op het web (alleen Firefox en Internet Explorer).

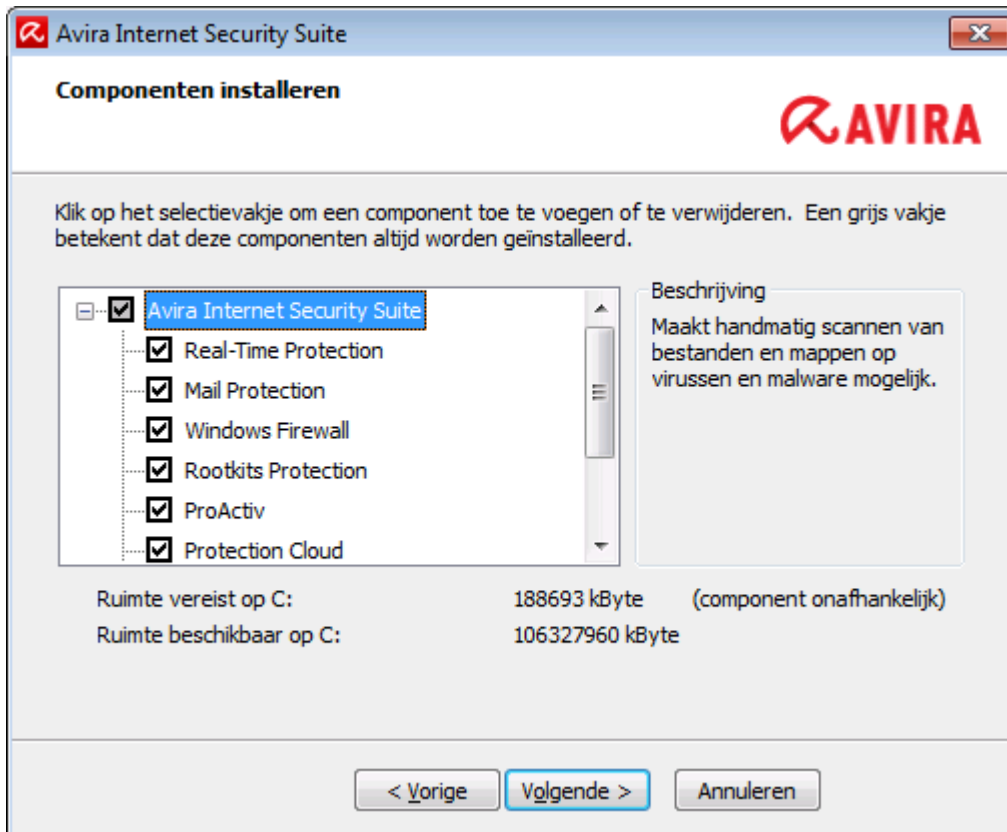


Als u Avira SearchFree Toolbar niet wilt installeren, schakelt u de selectievakjes uit van de opties **Stel Ask in als mijn standaard zoekmachine en behoud dit zo** en **Stel Avira SearchFree (avira.search.ask.com) in als startpagina en tabbladpagina van mijn browser en laat dit zo**.

Als u weigert, wordt de setup van Avira SearchFree Toolbar afgebroken. De installatie van Avira Internet Security Suite wordt echter voltooid.

3.7.3 Installatieonderdelen kiezen

In een aangepaste installatie of wijziging van de installatie kunnen de volgende installatieonderdelen worden geselecteerd, toegevoegd of verwijderd.



Selecteer of hef de selectie op van onderdelen in de lijst in het dialoogvenster Onderdelen installeren.

- **Avira Internet Security Suite**

Deze module bevat alle onderdelen die nodig zijn voor een succesvolle installatie van Avira Internet Security Suite.

- **Real-Time Protection**

De Avira Real-Time Protection draait op de achtergrond. Het bewaakt en repareert, indien mogelijk, bestanden tijdens bewerkingen zoals openen, schrijven en kopiëren in de "modus Bij toegang". De modus Bij toegang betekent dat, telkens wanneer een gebruiker een bestandsbewerking uitvoert (bijvoorbeeld document laden, uitvoeren, kopiëren), Avira Internet Security Suite het bestand automatisch scant. Het hernoemen van een bestand activeert echter geen scan door Avira Real-Time Protection.

- **Mail Protection**

Mail Protection is de interface tussen uw computer en de e-mailserver van waaruit uw e-mailprogramma (e-mailclient) e-mails downloadt. Mail Protection is verbonden als een zogenaamde proxy tussen het e-mailprogramma en de e-mailserver. Alle inkomende e-mails worden door deze proxy geleid, gescand op virussen en ongewenste programma's en doorgestuurd naar uw e-mailprogramma. Afhankelijk van de configuratie, verwerkt het programma de betrokken e-mails automatisch of vraagt het u een bepaalde actie uit te voeren.

- **Windows Firewall (vanaf Windows 7)**

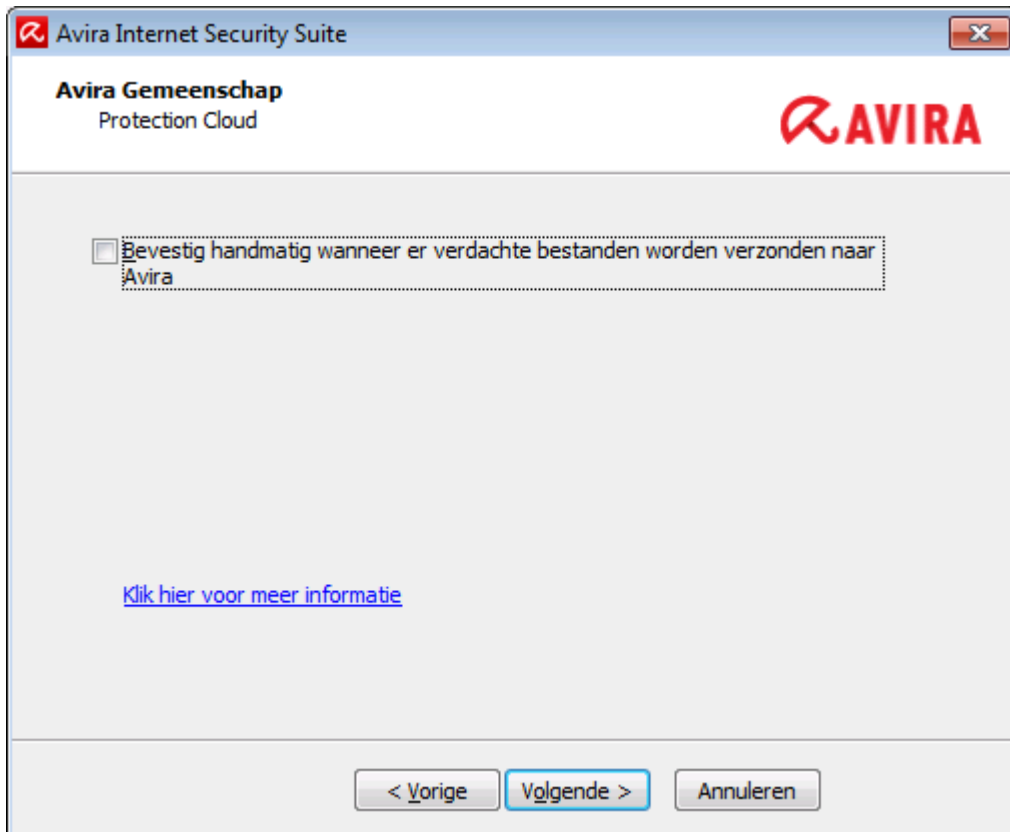
Dit onderdeel beheert de Windows Firewall vanaf Avira Internet Security Suite.

- **Rookits Protection**
Avira Rookits Protection controleert of er al software op uw computer is geïnstalleerd die niet meer met conventionele methoden van malwarebescherming kan worden gedetecteerd na het binnendringen van het computersysteem.
- **ProActiv**
Het ProActiv-onderdeel controleert de acties van programma's en waarschuwt gebruikers bij verdachte acties van toepassingen. Deze op gedrag gebaseerde herkenning stelt u in staat om uzelf te beschermen tegen onbekende malware. Het ProActiv-onderdeel is geïntegreerd in Avira Real-Time Protection.
- **Protection Cloud**
Het Protection Cloud-onderdeel is een module voor dynamische online detectie van nog onbekende malware. Dit betekent dat de bestanden worden geüpload naar een externe locatie en worden vergeleken met bekende bestanden evenals met andere bestanden die in real time worden geüpload en geanalyseerd (niet gepland en zonder vertraging). Op deze manier wordt de database voortdurend bijgewerkt en kan hierdoor een hoger beveiligingsniveau worden geleverd.
Als u er voor kiest om het onderdeel Protection Cloud te installeren, maar u wilt handmatig bevestigen welke bestanden moeten worden verzonden naar de Cloud voor analyse, kunt u de optie **Handmatig bevestigen bij het verzenden van verdachte bestanden naar Avira** activeren.
- **Web Protection**
Bij het surfen op internet, gebruikt u uw webbrowser om gegevens van een webserver te vragen. De gegevens die worden verplaatst vanaf de webserver (HTML-bestanden, script- en beeldbestanden, flashbestanden, video- en muziekstreams, enz.), worden normaliter rechtstreeks verplaatst naar de browsercache voor weergave in de webbrowser, wat betekent dat een scan bij toegang, zoals uitgevoerd door Avira Real-Time Protection, niet mogelijk is. Dit zou virussen en ongewenste programma's toegang tot uw computersysteem kunnen geven. Web Protection is wat bekend is als een HTTP-proxy die de poorten die gebruikt worden voor gegevensoverdracht bewaakt (80, 8080, 3128) en de overgedragen gegevens scant op virussen en ongewenste programma's. Afhankelijk van de configuratie, verwerkt het programma de betrokken bestanden automatisch of vraagt de gebruiker om een bepaalde actie.
- **Shelluitbreiding**
De Shelluitbreiding genereert een vermelding **Scan geselecteerde bestanden met Avira** in het contextmenu van Windows Explorer (rechtermuisknop). Met dit bericht kunt u bestanden of mappen direct scannen.

Verwante onderwerpen:

[Een installatie wijzigen](#)

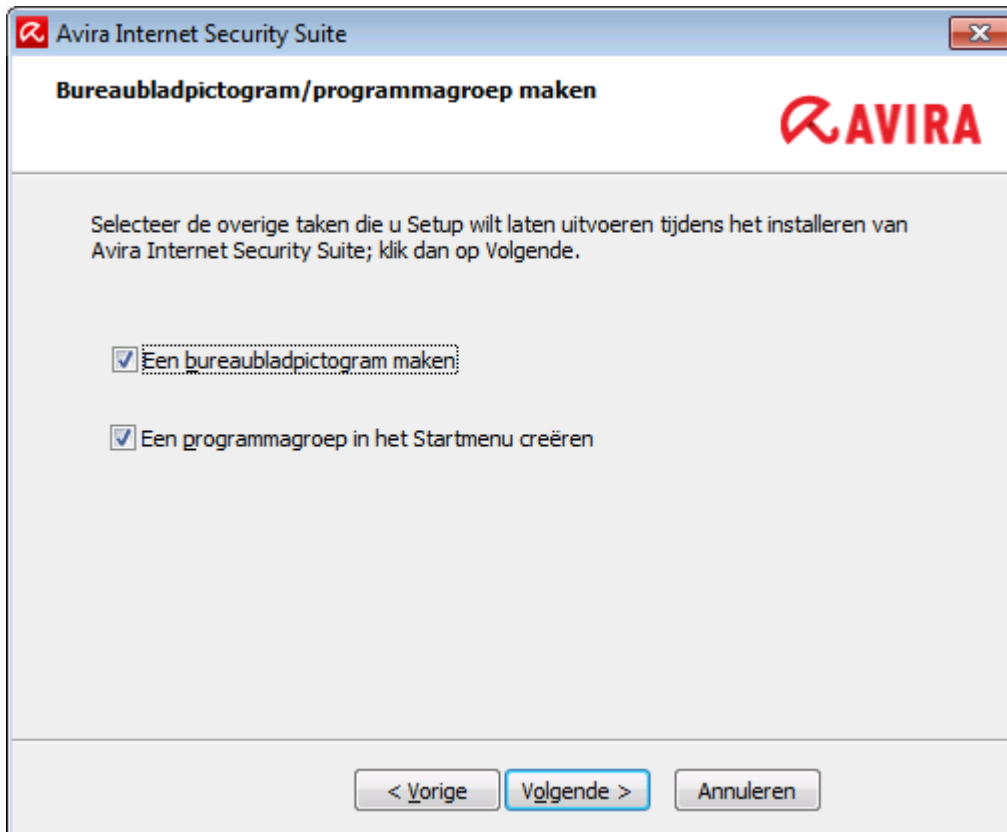
Als u hebt besloten om deel te nemen aan de Avira Community, kunt u ervoor kiezen de upload steeds handmatig te bevestigen als er een bestand wordt verzonden naar het Avira Malware Research Center.



- ▶ Als u wilt dat Avira Internet Security Suite iedere keer om een bevestiging vraagt, dient u de optie **Handmatig bevestigen bij het verzenden van verdachte bestanden naar Avira** te activeren.

3.7.4 Snelkoppelingen maken voor Avira Internet Security Suite

Via een bureaubladpictogram en of een programmagroep in het menu Start, krijgt u sneller en eenvoudiger toegang tot Avira Internet Security Suite.



- ▶ Om een bureaubladpictogram voor Avira Internet Security Suite en/of een programmagroep te maken in het **menu Start** laat u de optie(s) geactiveerd.

3.7.5 Avira Internet Security Suite activeren

Er zijn verschillende manieren om uw Avira Internet Security Suite te activeren.



Als u al een activeringscode hebt ontvangen, geeft u deze op in de hiervoor bestemde velden.

- ▶ Als u nog steeds een activeringscode moet verkrijgen, klikt u op de link [Koop een activeringscode](#).

U wordt doorgestuurd naar de website van Avira waar u een activeringscode kunt verkrijgen.

- ▶ Als u het product alleen wilt testen, selecteert u **Product testen** en geeft u uw gegevens op in de vereiste registratievelden.

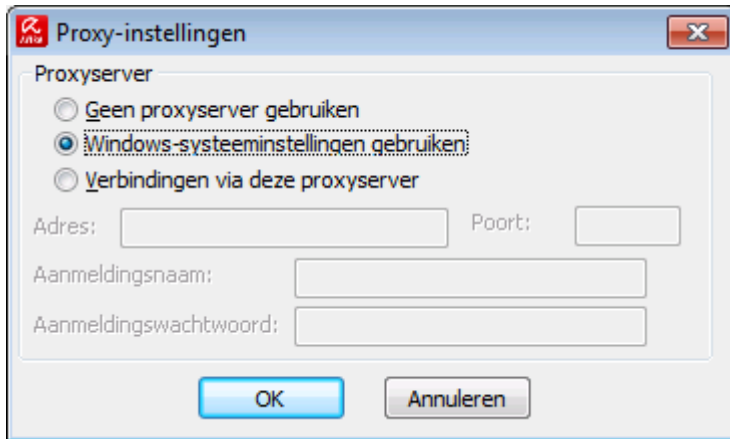
Uw evaluatielicentie is geldig voor 31 dagen.

- ▶ Als u al een product hebt geactiveerd en uw Avira-product opnieuw wilt installeren, selecteert u de optie **Ik heb al een geldig licentiebestand**.

Een browservenster wordt geopend en u kunt navigeren naar het bestand *hbedv.key* op uw systeem.

3.7.6 Proxy-instellingen definiëren

Het definiëren van proxy-instellingen is alleen aanbevolen voor geavanceerde gebruikers die goed op de hoogte zijn van hard- en software en van beveiligingsproblemen.



- ▶ Als Avira Internet Security Suite niet wordt verondersteld om een internetverbinding te maken via een proxyserver, activeert u de optie **Geen proxyserver gebruiken**.
- ▶ Als u wilt dat Avira Internet Security Suite op dezelfde manier als elke andere geïnstalleerde toepassing verbinding maakt met het internet, laat u **instellingen Windows-systeem** (standaard geactiveerd) ingeschakeld.

U kunt de Windows-systeeminstellingen configureren om een proxyserver te gebruiken onder **Configuratiescherm > Internetopties > Verbindingen > LAN-instellingen**. U heeft ook toegang tot de internetopties via het menu **Extra's** in Internet Explorer.

Let op

Als u een proxyserver gebruikt die authenticatie vereist, moet u alle vereiste gegevens invoeren onder de optie **Verbindingen via deze proxyserver**. De optie **Instellingen Windows-systeem gebruiken** kan alleen worden gebruikt voor proxyservers zonder authenticatie.

- ▶ Als u een proxyserver wilt instellen die speciaal gekoppeld is met Avira Internet Security Suite, schakelt u **Verbindingen via deze proxyserver** in en voert u de relevante informatie in:

Adres

Voer de computernaam of het IP-adres in van de proxyserver die u wilt gebruiken om een verbinding te maken met de webserver.

Voorbeelden:

Adres: proxy.domein.com

Adres: 192.168.1.100

Poort

Voer het poortnummer in van de proxyserver die u wilt gebruiken om een verbinding te maken met de webserver.

Voorbeelden:

Poort: 8080

Poort: 3128

Aanmeldingsnaam

Gebruikersnaam invoeren om in te loggen bij de proxyserver.

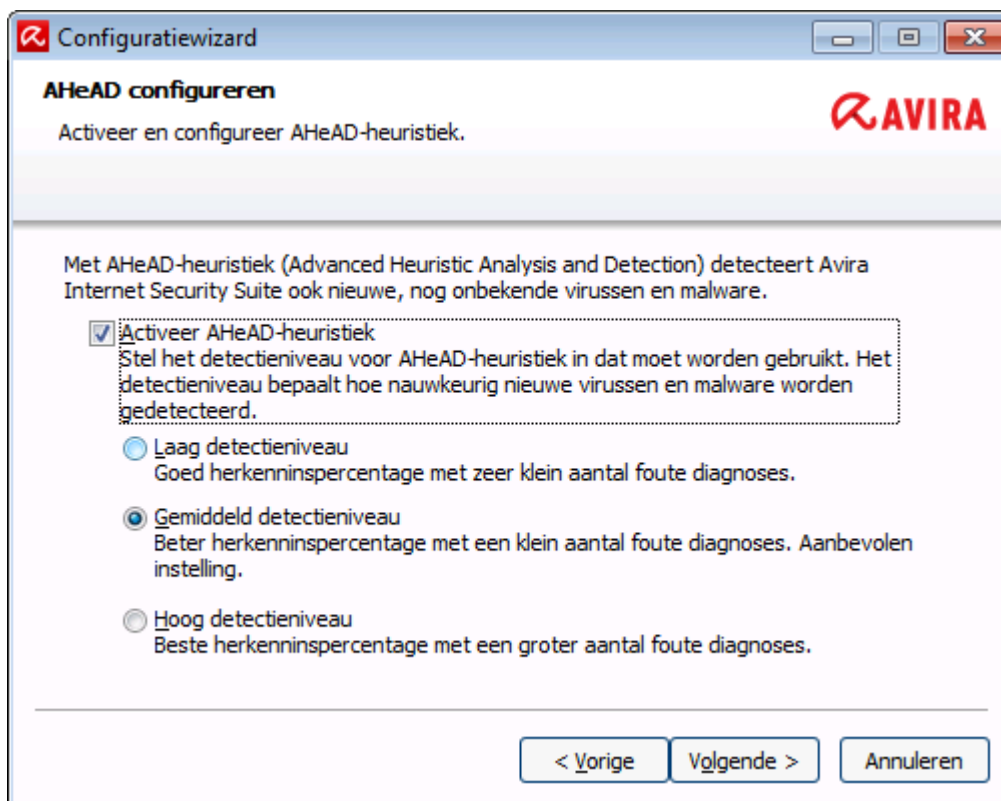
Aanmeldingswachtwoord

Voer hier het relevante wachtwoord in om in te loggen bij de proxyserver. Het wachtwoord wordt in gecodeerde vorm opgeslagen. Om veiligheidsredenen veranderen de feitelijke tekens die u op deze plaats typt, in asterisken (*).

Klik op **OK**.

3.7.7 Het heuristische detectieniveau configureren (AHeAD)

Avira Internet Security Suite bevat een krachtig hulpmiddel in de vorm van Avira AHeAD-technologie (*Advanced Heuristic Analysis and Detection*). Deze technologie gebruikt patroonherkenningstechnieken, zodat deze onbekende (nieuwe) malware kan detecteren door andere malware vooraf te hebben geanalyseerd.

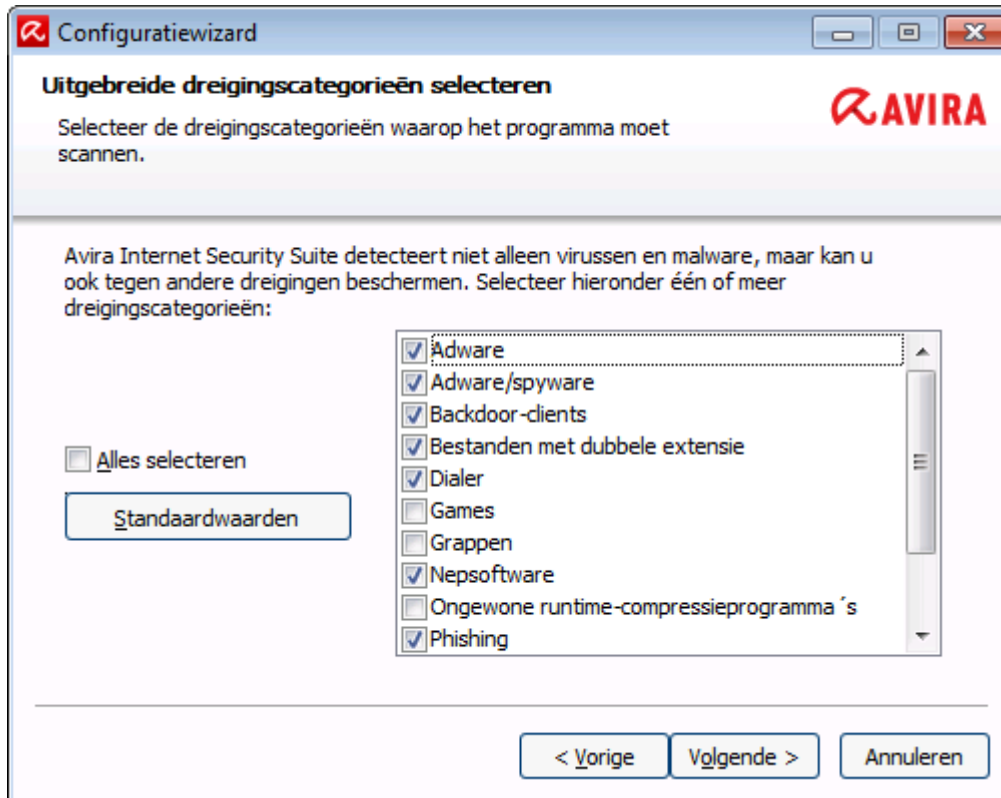


- ▶ Selecteer een detectieniveau in het dialoogvenster **Configureer AHeAD** en klik op **Volgende**.

Het geselecteerde detectieniveau wordt gebruikt voor de System Scanner (Scan op aanvraag) en Real-Time Protection (Scan bij toegang) AHeAD-technologie-instellingen.

3.7.8 Uitgebreide bedreigingscategorieën selecteren

Virus en malware zijn niet de enige bedreigingen die een gevaar betekenen voor uw computersysteem. We hebben een complete lijst van risico's gedefinieerd en deze voor u onderverdeeld in uitgebreide bedreigingscategorieën.



- Er zijn al enkele bedreigingscategorieën standaard vooraf geselecteerd.

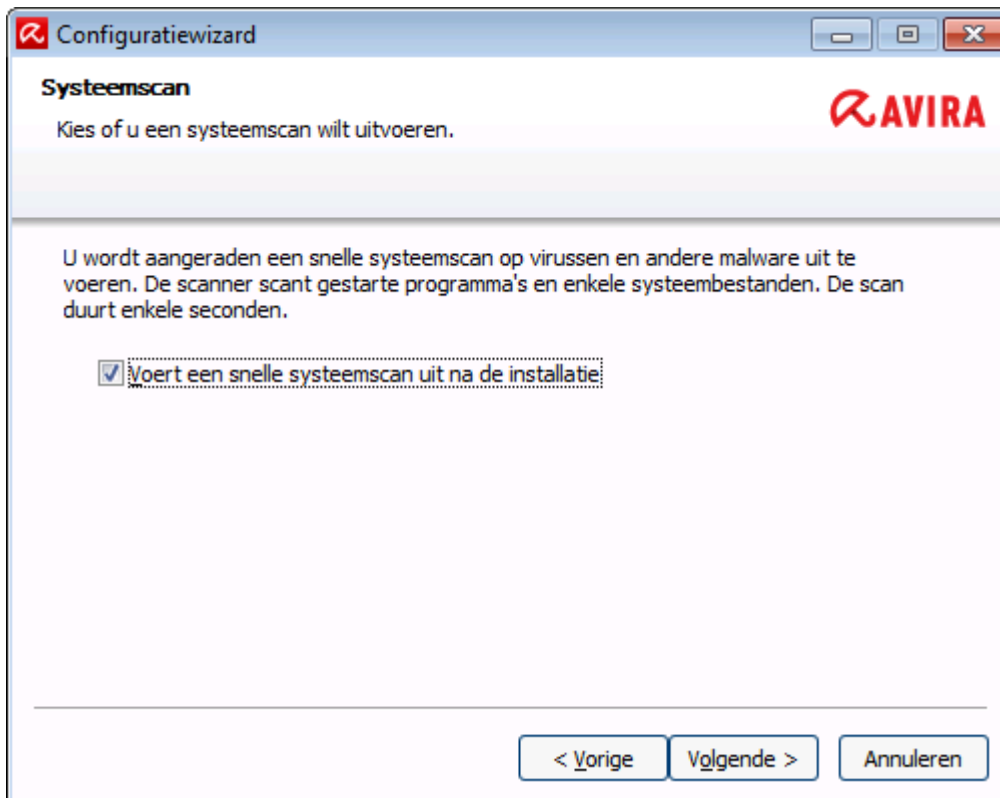
Activeer, indien nodig, andere bedreigingscategorieën in het dialoogvenster **Uitgebreide bedreigingscategorieën selecteren**.

Als u van gedacht verandert, kunt u terugkeren naar de aanbevolen waarden door te klikken op de knop **Standaardwaarden**.

Klik op **Volgende** om door te gaan met de installatie.

3.7.9 Een scan starten na de installatie

Om de huidige beveiligingsstatus van de computer te controleren, kan een snelle systeemscan worden uitgevoerd nadat de configuratie is voltooid en voordat de computer opnieuw wordt opgestart. De System Scanner scant actieve programma's en de belangrijkste systeembestanden op virussen en malware.



- ▶ Als u een snelle systeemscaan wilt uitvoeren, laat u de optie **Snelle systeemscaan** geactiveerd.
Klik op **Volgende**.
Klik op **Voltoeien** om de configuratie te voltooien.
Als u de optie **Snelle systeemscaan** niet hebt gedeactiveerd, wordt het venster *Luke Filewalker* geopend.
De System Scanner voert een snelle systeemscaan uit.

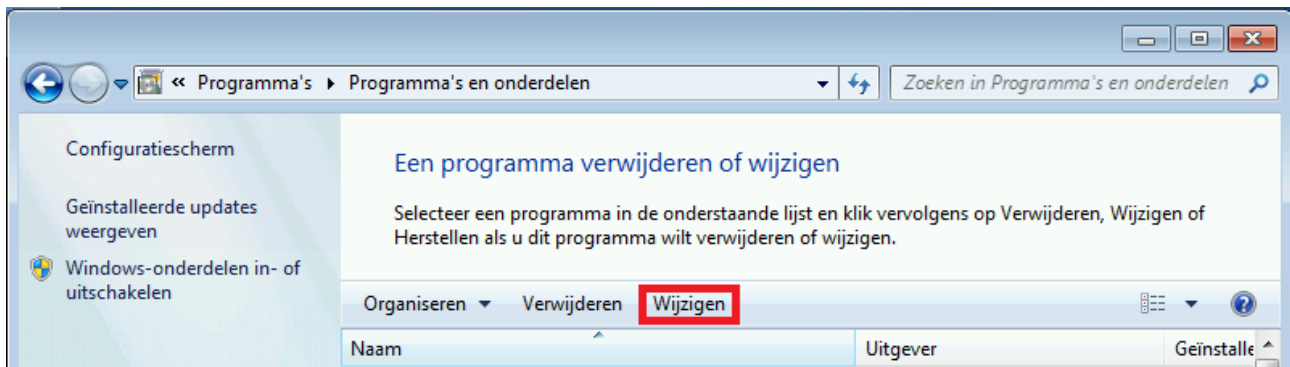
3.8 De installatie wijzigen

Als u modules van de huidige installatie wilt toevoegen of verwijderen, kunt u dat doen zonder dat u Avira Internet Security Suite hoeft te de-installeren. Zo gaat u te werk:

- [Een installatie wijzigen onder Windows 8](#)
- [Een installatie wijzigen onder Windows 7](#)
- [Een installatie wijzigen onder Windows XP](#)

3.8.1 Een installatie wijzigen onder Windows 8

U hebt de mogelijkheid om individuele programmaonderdelen van de installatie van Avira Internet Security Suite toe te voegen of te verwijderen (zie [Installatieonderdelen kiezen](#)).



Als u modules van de huidige installatie wilt toevoegen of verwijderen, kunt u gebruik maken van de optie **Programma's verwijderen** in het **Configuratiescherm van Windows** voor het **wijzigen/verwijderen** van programma's.

- ▶ Klik met de rechtermuisknop op het scherm.

Het symbool **Alle apps** verschijnt.

Klik op het symbool en zoek in de sectie *Apps - Systeem* naar het item **Configuratiescherm**.

Dubbelklik op het symbool **Configuratiescherm**.

Klik op **Programma's - Een programma de-installeren**.

Klik op **Programma's en onderdelen - Een programma de-installeren**.

Selecteer Avira Internet Security Suite en klik op **Wijzigen**.

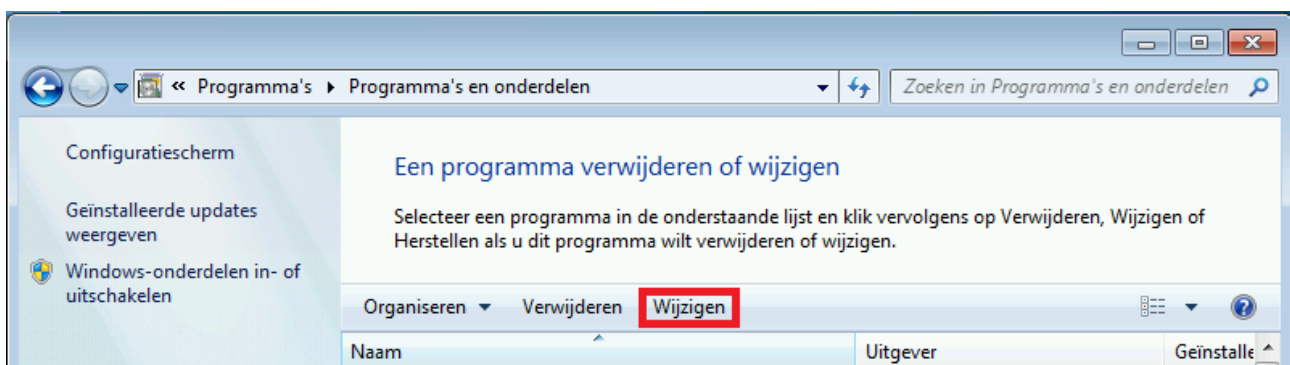
Selecteer in het **Welkom**-dialogvenster van het programma de optie **Wijzigen**. U wordt begeleid bij de installatiewijzigingen.

Verwante onderwerpen:

[Installatieonderdelen kiezen](#)

3.8.2 Een installatie wijzigen onder Windows 7

U hebt de mogelijkheid om individuele programmaonderdelen van de installatie van Avira Internet Security Suite toe te voegen of te verwijderen (zie [Installatieonderdelen kiezen](#)).



Indien u modules van de huidige installatie wilt toevoegen of verwijderen, kunt u gebruik maken van de optie **Programma's toevoegen of verwijderen** in het **Windows-configuratiescherm** voor **Wijzigen/Verwijderen** van programma's.

- ▶ Open het **Configuratiescherm** via het Windows-menu **Start**.
Dubbelklik op **Programma's en Onderdelen**.
Selecteer Avira Internet Security Suite en klik op **Wijzigen**.
Selecteer in het **Welkom**-dialoogvenster van het programma de optie **Wijzigen**. U wordt begeleid bij de installatiewijzigingen.

Verwante onderwerpen:

[Installatieonderdelen kiezen](#)

3.8.3 Een installatie wijzigen onder Windows XP

U hebt de mogelijkheid om individuele programmaonderdelen van de installatie van Avira Internet Security Suite toe te voegen of te verwijderen (zie [Installatiemodules kiezen](#)).

Indien u modules van de huidige installatie wilt toevoegen of verwijderen, kunt u gebruik maken van de optie **Programma's toevoegen of verwijderen** in het **Windows-configuratiescherm** voor **Wijzigen/Verwijderen** van programma's.

- ▶ Open het **Configuratiescherm** via het Windows-menu **Start > Instellingen**.
Dubbelklik op **Programma's toevoegen of verwijderen**.
Selecteer Avira Internet Security Suite en klik op **Wijzigen**.
Selecteer in het **Welkom**-dialoogvenster van het programma de optie **Wijzigen**. U wordt begeleid bij de installatiewijzigingen.

Verwante onderwerpen:

[Installatieonderdelen kiezen](#)

3.9 De-installatie

Als u Avira Internet Security Suite ooit wilt de-installeren, kunt u als volgt te werk gaan:

- [Avira Internet Security Suite onder Windows 8 de-installeren](#)
- [Avira Internet Security Suite onder Windows 7 de-installeren](#)
- [Avira Internet Security Suite onder Windows XP de-installeren](#)

3.9.1 Avira Internet Security Suite onder Windows 8 de-installeren

Om Avira Internet Security Suite van uw computer te de-installeren, gebruikt u de optie **Programma's en onderdelen** in het Configuratiescherm van Windows.



- ▶ Klik met de rechtermuisknop op het scherm.

Het symbool **Alle apps** verschijnt.

Klik op het symbool en zoek in de sectie *Apps - Systeem* naar het item **Configuratiescherm**.

Dubbelklik op het symbool **Configuratiescherm**.

Klik op **Programma's - Een programma verwijderen**.

Klik op **Programma's en onderdelen - Een programma verwijderen**.

Selecteer Avira Internet Security Suite in de lijst en klik op **Verwijderen**.

Wanneer u wordt gevraagd of u de toepassing en al zijn componenten werkelijk wilt verwijderen, klikt u op **Ja** om te bevestigen.

Wanneer u wordt gevraagd Windows Firewall te activeren (wordt Avira FireWall gedeïnstalleerd), klikt u op **Ja** om toch tenminste iets van bescherming over te houden voor uw systeem.

Alle onderdelen van het programma worden verwijderd.

Klik op **Afsluiten** om de de-installatie te voltooien.

Als een dialoogvenster verschijnt met de aanbeveling de computer opnieuw op te starten, klikt u op **Ja** om te bevestigen.

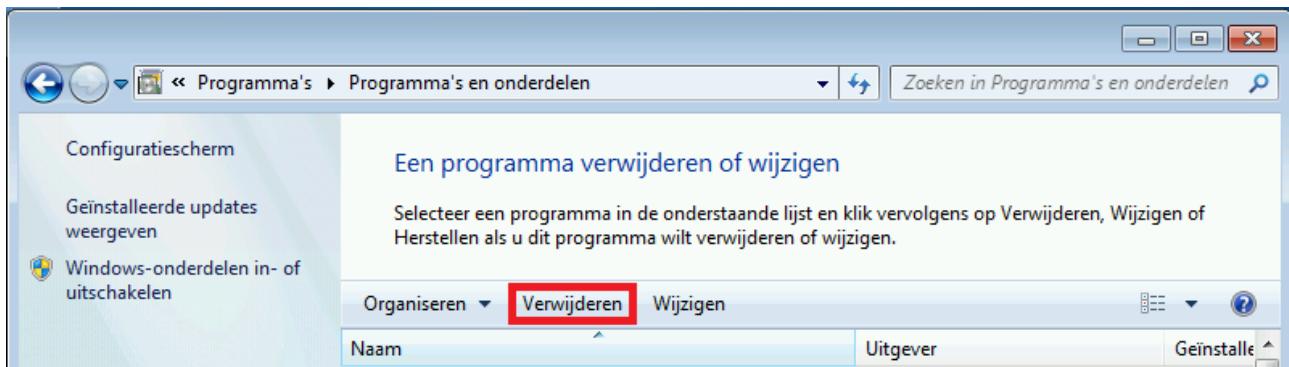
Avira Internet Security Suite is nu gedeïnstalleerd en alle mappen, bestanden en registervermeldingen voor het programma worden verwijderd als de computer opnieuw wordt opgestart.

Let op

De Avira SearchFree Toolbar is niet opgenomen in het de-installatieprogramma en moet afzonderlijk worden gedeïnstalleerd.

3.9.2 Avira Internet Security Suite onder Windows 7 de-installeren

Om Avira Internet Security Suite van uw computer te de-installeren, gebruikt u de optie **Programma's en onderdelen** in het Configuratiescherm van Windows.



- ▶ Open het **Configuratiescherm** via het Windows-menu **Start**.

Klik op **Programma's en Onderdelen**.

Selecteer Avira Internet Security Suite in de lijst en klik op **Verwijderen**.

Wanneer u wordt gevraagd of u de toepassing en al zijn componenten werkelijk wilt verwijderen, klikt u op **Ja** om te bevestigen.

Wanneer u wordt gevraagd Windows Firewall te activeren (wordt Avira FireWall gedeïnstalleerd), klikt u op **Ja** om toch minstens iets van bescherming over te houden voor uw systeem.

Alle onderdelen van het programma worden verwijderd.

Klik op **Afsluiten** om de de-installatie te voltooien.

Als een dialoogvenster verschijnt met de aanbeveling de computer opnieuw op te starten, klikt u op **Ja** om te bevestigen.

Avira Internet Security Suite is nu gedeïnstalleerd en alle mappen, bestanden en registervermeldingen voor het programma worden verwijderd als de computer opnieuw wordt opgestart.

Let op

De Avira SearchFree Toolbar is niet opgenomen in het de-installatieprogramma en moet afzonderlijk worden gedeïnstalleerd.

3.9.3 Avira Internet Security Suite onder Windows XP de-installeren

Om Avira Internet Security Suite van uw computer te de-installeren, gebruikt u de optie **Programma's wijzigen of verwijderen** in het Configuratiescherm van Windows.

- ▶ Open het **Configuratiescherm** via het Windows-menu **Start > Instellingen**.

Dubbelklik op **Programma's toevoegen of verwijderen**.

Selecteer Avira Internet Security Suite in de lijst en klik op **Verwijderen**.

Wanneer u wordt gevraagd of u de toepassing en al zijn componenten werkelijk wilt verwijderen, klikt u op **Ja** om te bevestigen.

Alle onderdelen van het programma worden verwijderd.

Klik op **Afsluiten** om de de-installatie te voltooien.

Als een dialoogvenster verschijnt met de aanbeveling de computer opnieuw op te starten, klikt u op **Ja** om te bevestigen.

Avira Internet Security Suite is nu gedeïnstalleerd en alle mappen, bestanden en registervermeldingen voor het programma worden verwijderd als de computer opnieuw wordt opgestart.

Let op

De Avira SearchFree Toolbar is niet opgenomen in het verwijderingsprogramma en moet afzonderlijk worden verwijderd.

3.9.4 Avira SearchFree Toolbar de-installeren

Als u Avira SearchFree Toolbar ooit wilt de-installeren, kunt u als volgt te werk gaan:

- [Avira SearchFree Toolbar de-installeren onder Windows 8](#)
- [Avira SearchFree Toolbar de-installeren onder Windows 7](#)
- [Avira SearchFree Toolbar de-installeren onder Windows XP](#)
- [Avira SearchFree Toolbar de-installeren via de webbrowser](#)
- [Avira SearchFree Toolbar de-installeren via Invoegtoepassingenbeheer](#)

Avira SearchFree Toolbar de-installeren onder Windows 8

Uw Avira SearchFree Toolbar de-installeren:

- ▶ Sluit de webbrowser.

Klik met de rechtermuisknop in een van de hoeken onderaan op het scherm.

Het symbool **Alle apps** verschijnt.

Klik op het symbool en zoek in de sectie *Apps - Systeem* naar het item **Configuratiescherm**.

Dubbelklik op het symbool **Configuratiescherm**.

Klik op **Programma's - Een programma de-installeren**.

Klik op **Programma's en onderdelen - Een programma de-installeren**.

Selecteer Avira SearchFree Toolbar plus Web Protection in de lijst en klik op **Verwijderen**.

U wordt gevraagd of u dit product daadwerkelijk wilt de-installeren.

Klik op **Ja** om te bevestigen.

Avira SearchFree Toolbar plus Web Protection zijn verwijderd en alle mappen, bestanden en registervermeldingen voor de Avira SearchFree Toolbar plus Web Protection worden verwijderd wanneer uw computer opnieuw wordt opgestart.

Avira SearchFree Toolbar de-installeren onder Windows 7

Uw Avira SearchFree Toolbar de-installeren:

- ▶ Sluit uw webbrowser.

Open het **Configuratiescherm** via het Windows-menu **Start**.

Dubbelklik op **Programma's en Onderdelen**.

Selecteer Avira SearchFree Toolbar plus Web Protection in de lijst en klik op **Verwijderen**.

U wordt gevraagd of u dit product daadwerkelijk wilt de-installeren.

Klik op **Ja** om te bevestigen.

Avira SearchFree Toolbar plus Web Protection zijn verwijderd en alle mappen, bestanden en registervermeldingen voor de Avira SearchFree Toolbar plus Web Protection worden verwijderd wanneer uw computer opnieuw wordt opgestart.

Avira SearchFree Toolbar de-installeren onder Windows XP

Uw Avira SearchFree Toolbar de-installeren:

- ▶ Sluit uw webbrowser.

Open het **Configuratiescherm** via het Windows-menu **Start > Instellingen**.

Dubbelklik op **Programma's toevoegen of verwijderen**.

Selecteer Avira SearchFree Toolbar plus Web Protection in de lijst en klik op **Verwijderen**.

U wordt gevraagd of u dit product daadwerkelijk wilt de-installeren.

Klik op **Ja** om te bevestigen.

Avira SearchFree Toolbar plus Web Protection zijn verwijderd en alle mappen, bestanden en registervermeldingen voor de Avira SearchFree Toolbar plus Web Protection worden verwijderd wanneer uw computer opnieuw wordt opgestart.

Avira SearchFree Toolbar de-installeren via de webbrowser

U kunt de Avira SearchFree Toolbar ook rechtstreeks in de browser verwijderen. Deze optie is alleen beschikbaar voor Firefox en Internet Explorer:

- ▶ Open uw webbrowser.

Open in de zoekwerkbalk het menu **Opties**.

Klik op **Werkbalk de-installeren vanaf browser**.

Wanneer u wordt gevraagd of u het product wilt installeren, klikt u op **Ja** om te bevestigen.

U wordt nu gevraagd om uw webbrowser te sluiten.

Sluit de webbrowser en klik op **Opnieuw**.

Avira SearchFree Toolbar plus Web Protection zijn verwijderd en alle mappen, bestanden en registervermeldingen voor de Avira SearchFree Toolbar plus Web Protection worden verwijderd wanneer uw computer opnieuw wordt opgestart.

Let op

Om Avira SearchFree Toolbar te de-installeren, moet de werkbalk ingeschakeld zijn in de Add-On Manager.

Avira SearchFree Toolbar de-installeren via Invoegtoepassingenbeheer

Omdat de werkbalk is geïnstalleerd als een invoegtoepassing, kan deze ook als zodanig worden gedeïnstalleerd:

Firefox

- ▶ Klik op **Tools > Add-ons > Extensies**. Van daaruit kunt u de invoegtoepassing van Avira beheren: activeren of deactiveren van de werkbalk en de-installeren.

Internet Explorer

- ▶ Ga naar **Beheren Add-ons > Toolbars en Extensies**. Hier kunt u uw Avira SearchFree Toolbar activeren en deactiveren of de-installeren.

Google Chrome

- ▶ Klik op **Opties > Extensies** en beheer eenvoudig uw toolbar: activeren, deactiveren of de-installeren.

4. Overzicht van Avira Internet Security Suite

Dit hoofdstuk bevat een overzicht van de functionaliteit en de werking van uw Avira-product.

- zie hoofdstuk [Gebruikersinterface en werking](#)
- zie hoofdstuk [Avira SearchFree Toolbar](#)
- zie hoofdstuk [Hoe te...?](#)

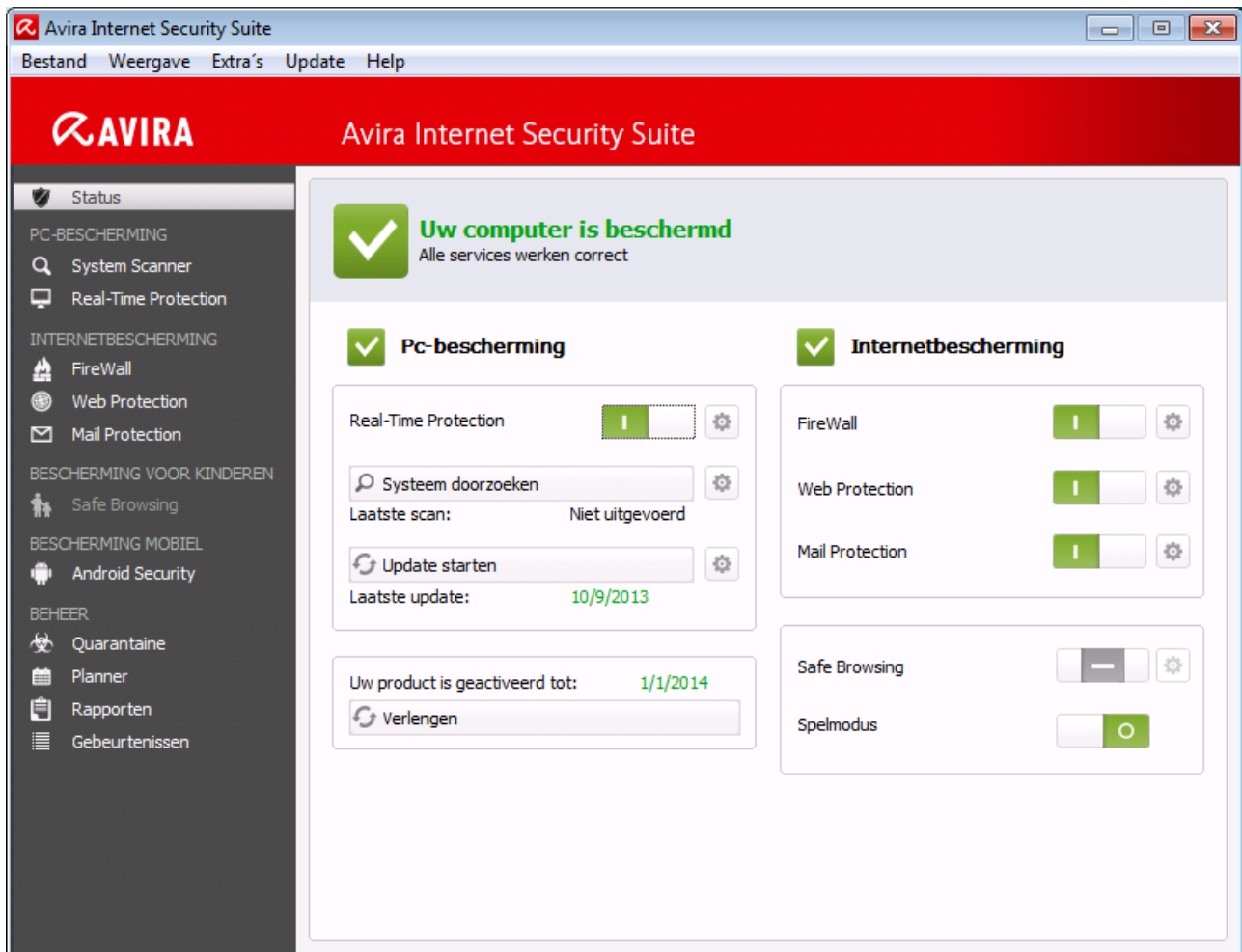
4.1 Gebruikersinterface en werking

U gebruikt uw Avira-product met behulp van drie programma-interface-elementen:

- **Control Center:** monitoren en beheren van het Avira-product
- **Configuratie:** Het Avira-product configureren
- **Taakbalkpictogram** in de systeemtaakbalk: openen van het Control Center en andere functies

4.1.1 Control Center

Het Control Center is ontworpen om de beveiligingsstatus van uw computersystemen te bewaken en voor het controleren en bedienen van de beveiligingscomponenten en -functies van uw Avira-product.



Het venster van het Control Center is onderverdeeld in drie gebieden: de **Menubalk**, het **Navigatiegebied** en het detailvenster **Status**:

- **Menubalk:** in de menubalk van het Control Center heeft u toegang tot algemene programmafuncties en informatie over het programma.
- **Navigatiegebied:** in het navigatiegebied kunt u eenvoudig wisselen tussen de afzonderlijke secties van het Control Center. De afzonderlijke secties bevatten informatie over en functies van de programmaonderdelen en zijn gerangschikt in de navigatiebalk volgens activiteit. Voorbeeld: Activiteit *PC PROTECTION* - Sectie **Real-Time Protection**.
- **Status:** Bij het openen van het Control Center wordt de **Status** weergegeven waarmee u in een oogopslag kunt zien of uw computer veilig is en bovendien heeft u een overzicht van de actieve modules, de datum van de laatste backup en de datum van de laatste systeemscaan. De **Status**-weergave bevat ook knoppen voor het starten van functies of acties, zoals het starten of stoppen van de **Real-Time Protection**.

Starten en afsluiten van het Control Center

Voor het starten van het Control Center zijn de volgende opties beschikbaar:

- Dubbelklikken op het programmaicoon op uw bureaublad

- Via de programmattoegang in het menu **Start > Programma's**.
- Via het [Taakbalkicoon](#) van uw Avira-product.

Sluit het Control Center via de menu-opdracht **Sluiten** in het menu **Bestand** of door te klikken op het tabblad Sluiten in het Control Center.

Bedienen van het Control Center

Navigeren in het Control Center

- ▶ Selecteer een activiteit in de navigatiebalk.
 - De activiteit wordt geopend en andere secties verschijnen. Het eerste sectie van de activiteit is geselecteerd en wordt weergegeven in het scherm.
- ▶ Klik indien nodig op een andere sectie om die weer te laten geven in het detailvenster.

Let op

U kunt de toetsenbordnavigatie in de menubalk activeren met de **[Alt]**-toets. Wanneer de navigatie is geactiveerd, kunt u door het menu lopen met de **pijljes**-toetsen. Met de **Return**-toets activeert u het actieve menu-item. Voor het openen of sluiten van menu's in het Control Center of om te navigeren in de menu's kunt u ook gebruik maken van de volgende toetsencombinaties: **[Alt]** + onderstreepte letter in het menu of de menu-opdracht. Houd de **[Alt]**-toets ingedrukt wanneer u een menu, een menu-opdracht of een submenu wilt openen.

Voor het bewerken van gegevens of objecten in het detailvenster:

- ▶ Markeer het gegeven of het object dat u wilt bewerken.
 - Om meerdere elementen tegelijk te markeren (elementen in kolommen) houdt u de **Ctrl**-toets of de **Shift**-toets ingedrukt terwijl u de elementen selecteert.
- ▶ Klik op de juiste knop in de bovenste balk van het detailvenster om het object te bewerken.

Overzicht Control Center

- **Status**: door te klikken op de **Status**-balk krijgt u een overzicht van de functionaliteit en de prestaties van het product (zie [Status](#)).
 - De **Status**-sectie toont u in een oogopslag welke modules actief zijn en geeft informatie over de laatst uitgevoerde update.
- **PC-BESCHERMING**: in deze sectie vindt u de componenten voor het controleren van de bestanden op virussen en malware op uw computersysteem.
 - De sectie Scanner stelt u in staat om op eenvoudige wijze een scan op aanvraag te configureren en te starten. Vooraf gedefinieerde profielen maken een scan mogelijk met reeds aangepaste standaardopties. Op dezelfde manier is het mogelijk om de

scan op virussen en ongewenste programma's aan te passen aan uw persoonlijke wensen met behulp van handmatige selectie (wordt opgeslagen) of door het aanmaken van gebruikersgedefinieerde profielen.

- De sectie Real-Time Protection toont informatie over gescande bestanden, evenals andere statistische gegevens, die op elk moment gereset kunnen worden, en geeft toegang tot het rapportagebestand. Uitgebreidere informatie over het laatst gedetecteerde virus of ongewenste programma kan praktisch worden verkregen "met een druk op de knop".
- **INTERNETBESCHERMING:** in deze sectie vindt u de componenten voor het beschermen van uw computersysteem tegen virussen en malware vanaf het internet en tegen ongevoegde toegang tot het netwerk.
 - Met de FireWall-sectie kunt u de basisinstellingen configureren voor de FireWall. Afgezien daarvan worden de huidige gegevensoverdrachtssnelheid en alle actieve toepassingen die een netwerkverbinding gebruiken, weergegeven.
 - De sectie Web Protection toont informatie over gescande URL's en gedetecteerde virussen, evenals andere statistische gegevens, die op elk moment gereset kunnen worden, en geeft toegang tot het rapportbestand. Uitgebreidere informatie over het laatst gedetecteerde virus of ongewenste programma kan praktisch worden verkregen "met een druk op de knop".
 - De sectie Mail Protection toont u alle e-mails die gescand zijn door Mail Protection, hun eigenschappen en andere statistische gegevens. U kunt ook e-mailadressen uitsluiten van toekomstige scannen op malware of spam. E-mails kunnen ook worden verwijderd uit de Mail Protection-buffer.
- **BESCHERMING VAN MOBIELE APPARATUUR.** Vanuit deze sectie wordt u doorgeleid naar de onlinetoegang voor Android-apparaten.
 - [Avira Free Android Security](#) beheert al uw op Android gebaseerde apparaten.
- **BEHEER:** in deze sectie vindt u tools voor het isoleren en beheren van verdachte of geïnfecteerde bestanden en voor het plannen van terugkerende taken.
 - De Quarantaine-sectie bevat de zogenaamde quarantainemanager. Dit is het centrale punt voor bestanden die al in quarantaine zijn geplaatst of voor verdachte bestanden die u in quarantaine wilt plaatsen. Het is ook mogelijk om een geselecteerd bestand per e-mail te verzenden naar het Avira Malware Research Center.
 - Met de Planner-sectie kunt u geplande scans, updates en backups configureren en bestaande taken aanpassen of verwijderen.
 - Met de Rapporten-sectie kunt u de resultaten van uitgevoerde acties bekijken.
 - De Gebeurtenissen-sectie stelt u in staat gebeurtenissen te bekijken die door bepaalde programma-modules zijn gegenereerd.

4.1.2 Configuratie

U kunt de instellingen van uw Avira-product wijzigen in Configuratie. Uw Avira-product is ingesteld met de standaardinstellingen na de installatie, zodat uw computersysteem

optimaal beschermd is. Wellicht moet u de beschermende onderdelen van het programma echter aanpassen aan uw computersysteem of de eisen die u aan uw Avira-product stelt.



De Configuratie opent een dialoogvenstervenster: u kunt hier uw configuratie-instellingen opslaan via de knoppen **OK** of **Toepassen**, uw instellingen verwijderen door op de knop Annuleren te drukken of de standaardinstellingen herstellen met de knop **Standaardwaarden**. U kunt individuele configuratiesecties selecteren in de linker navigatiebalk.

De Configuratie openen

U heeft verschillende opties om de configuratie te openen:

- via het Windows-configuratiescherm.
- via het Windows Security Center - vanaf Windows XP Service Pack 2.
- via het [Taakbalkicoon](#) van uw Avira-product.
- in het [Control Center](#) via het menu-item [Extra's -> Configuratie](#).
- in het [Control Center](#) via de [Configuratie](#)-knop.

Let op:

als u de configuratie opent via de **Configuratie**-knop in het Control Center, ga dan naar het Configuratieregister van de in het Control Center actieve sectie.

Configuratiewerking

Navigeer in het configuratiescherm op dezelfde manier als in Windows Explorer:

- ▶ Klik op een artikel in de boomstructuur om deze configuratiesectie weer te geven in het detailscherm.
- ▶ Klik op het plus-symbool bij een invoer om de configuratiesectie uit te breiden en configuratiesubsecties weer te geven in de boomstructuur.
- ▶ Klik op het minus-symbool bij de uitgebreide configuratiesectie om de configuratiesubsecties te verbergen.

Let op

Om Configuratie-opties te activeren of te deactiveren en de knoppen te gebruiken, kunt u ook de volgende toetsenbordcombinaties gebruiken: **[Alt] +** onderstreepte letter in de optienaam of knopbeschrijving.

Als u uw Configuratie-instellingen wilt bevestigen:

- ▶ Klik op **OK**.
 - Het configuratiescherm is gesloten en de instellingen zijn geaccepteerd.
- OF-
- ▶ Klik op **Toepassen**.
 - De instellingen worden toegepast. Het configuratiescherm blijft open.

Als u configuratie af wilt sluiten zonder uw instellingen te bevestigen:

- ▶ Klik op **Annuleren**.
 - Het configuratiescherm wordt gesloten en de instellingen worden verwijderd.

Als u alle configuratie-instellingen naar de standaardwaarden wilt herstellen:

- ▶ Klik op **Standaardwaarden**.
 - Alle instellingen van de configuratie zijn hersteld naar de standaardwaarden. Alle veranderingen en eigen toevoegingen worden gewist als de standaardinstellingen worden hersteld.

Overzicht van configuratieopties



De volgende configuratie-opties zijn beschikbaar:

- **Scanner:** Configuratie van een scan op aanvraag
 - Scanopties
 - Actie bij detectie
 - Archief-scanopties
 - Systeemsan uitzonderingen
 - Systeemsan heuristieken
 - Rapportfunctie-instelling
- **Real-Time Protection:** Configuratie van on-access scan
 - Scanopties
 - Actie bij detectie
 - Verdere acties
 - Uitzonderingen On-access-scan
 - Heuristieken On-access-scan
 - Rapportfunctie-instelling
- **Update:** Configuratie van de update-instellingen
 - Download via webserver
 - Proxy-instellingen
- **Web Protection:** Configuratie van Web Protection
 - Scan-opties, Web Protection activeren en deactiveren
 - Actie bij detectie
 - Geblokkeerde toegang: Ongewenste bestandstypen en MIME-typen, web filter voor bekende ongewenste URL's (kwaadaardige software, phishing, enz.)
 - Web Protection-scan uitzonderingen: URL's, bestandstypen, MIME-typen
 - Web Protection heuristieken
 - Rapportfunctie-instelling
- **Mail Protection:** Configuratie van Mail Protection
 - Scan-opties: Inschakelen van de monitoring van POP3-accounts, IMAP-accounts, uitgaande e-mails (SMTP)
 - Acties bij detectie
 - Verdere acties
 - Heuristieken Mail Protection-scan
 - AntiBot functie: Toegestane SMTP-servers, toegestane e-mail afzenders
 - Uitzonderingen Mail Protection-scan
 - Configuratie van cache, lege cache
 - Configuratie van een voettekst in verzonden e-mails
 - Rapportfunctie-instelling
- **Algemeen:**
 - Bedreigingscategorieën voor System Scanner en Real-Time Protection

- Geavanceerde bescherming: Opties om de ProActiv en Protection Cloud functies in te schakelen.
- Toepassingsfilter: Blokkeren of toestaan toepassingen
- Wachtwoordbeveiliging voor toegang tot het Control Center en de Configuratie
- Beveiliging: blokkeer autostartfunctie, productbescherming, bescherm Windows-hostsbestand
- WMI: schakel WMI-ondersteuning in
- Gebeurtenissenlog configuratie
- Configuratie van rapportfuncties
- Instellen van gebruikte mappen
- Configuratie van akoestische waarschuwingen wanneer kwaadaardige software wordt gedetecteerd

4.1.3 Taakbalkicoon

Het taakbalkicoon van uw Avira-product is zichtbaar na de installatie in de systeemtaakbalk van uw taakbalk:

Icoon	Beschrijving
	Avira Real-Time Protection is ingeschakeld
	Avira Real-Time Protection is uitgeschakeld

Het taakbalkpictogram geeft de status van de Real-Time Protection -service weer.

Belangrijke functies van uw Avira-product kunnen snel bereikt worden via het contextmenu van het **taakbalkicoon**. Open het contextmenu door op het **taakbalkicoon** te klikken met de rechtermuisknop.

Invoer in het contextmenu

- **Real-Time Protection inschakelen:** schakelt de Avira Real-Time Protection in of uit.
- **Mail Protection inschakelen:** schakelt de Avira Mail Protection in of uit.
- **Web Protection inschakelen:** schakelt de Avira Web Protection in of uit.
 - **Windows Firewall inschakelen:** schakelt de Windows Firewall in of uit (deze functie is beschikbaar vanaf Windows 8).
- **Start Avira Internet Security Suite:** opent het [Control Center](#).
- **Configureer Avira Internet Security Suite:** opent de [Configuratie](#).

- **Mijn berichten:** hiermee opent u een schuifvenster met de actuele informatie over uw Avira-product.
- **Mijn communicatie-instellingen:** opent het Product Message Subscription Center
- **Start update** Start een [update](#).
- **Help:** opent de Online Help.
- **Over Avira Internet Security Suite:** opent een dialoogvenster met informatie over uw Avira-product: productinformatie, versie-informatie, licentie-informatie.
- **Avira op internet:** opent het Avira webportaal op het internet. De voorwaarde hiervoor is dat u een actieve verbinding met het internet heeft.

4.2 Avira SearchFree Toolbar

Avira SearchFree Toolbar bevat twee hoofdcomponenten: Avira SearchFree en de toolbar.

De Avira SearchFree Toolbar is geïnstalleerd als add-on. Wanneer de browser de eerste keer wordt geopend (in Firefox en Internet Explorer) verschijnt er een pop-upbericht waarin u wordt gevraagd om toestemming voor het installeren van de toolbar. U moet accepteren om een succesvolle installatie van de Avira SearchFree Toolbar te voltooien.

Avira SearchFree is een zoekmachine en bevat een aanklikbaar Avira-logo dat gekoppeld is aan de Avira-website en web-, beeld- en videokanalen. Zodoende kunnen Avira-gebruikers veiliger navigeren op het internet.

De toolbar, die geïntegreerd is in uw webbrowser, bestaat uit een zoekvak, een Avira-logo dat gekoppeld is aan de Avira-website, twee statusweergaven, drie widgets en het menu **Opties**.

- **Zoek-toolbar**
Gebruik de zoek-toolbar voor gratis snel zoeken op internet met behulp van de Avira-zoekmachine.
- **Statusweergave**
De statusweergaven geven informatie over de status van de Web Protection en de huidige updatestatus van uw Avira-product en helpen u om te bepalen welke acties u moet ondernemen om uw pc te beschermen.
- **Widgets**
Avira biedt u drie widgets naar de belangrijkste internetgerelateerde functies. Met één klik heeft u direct toegang tot Facebook en uw e-mail of kunt u zich verzekeren van veilig surfen op het web (alleen Firefox en Internet Explorer).
- **Opties**
U kunt het menu **Opties** gebruiken voor toegang tot de toolbar-opties, de geschiedenis wissen, hulp voor de toolbar vinden en informatie en ook rechtstreeks de Avira SearchFree Toolbar de-installeren via de webbrowser (alleen Firefox en Internet Explorer).

4.2.1 Gebruik

Avira SearchFree

U kunt gebruik maken van Avira SearchFree om een willekeurig aantal termen te definiëren om op het internet te browsen.



Voer de term in het zoekvak in en druk op **Enter** of op **Zoeken**. De Avira SearchFree-engine zoekt vervolgens voor u op het internet en toont alle hits in het browservenster.



Om erachter te komen hoe u Avira SearchFree naar believen kunt configureren in Internet Explorer, Firefox en Chrome, ga naar [Opties](#).

Statusweergave

Web Protection

U kunt gebruikmaken van de volgende iconen en berichten om de acties te bepalen die u moet ondernemen om uw pc te beschermen:

Icoon	Statusweergave	Beschrijving
	<i>Web Protection</i>	Als u de cursor over het icoon beweegt, verschijnt het volgende bericht: <i>Avira Web Protection werkt, uw pc is beschermd.</i> Geen verdere actie vereist.
	<i>Web Protection uitgeschakeld</i>	Als u de cursor over het icoon beweegt, verschijnt het volgende bericht: <i>Avira Web Protection is uitgeschakeld. Klik om te leren hoe u de software inschakelt.</i> → U wordt doorgestuurd naar één van de artikelen in onze kennisbank.

	<i>Geen Web Protection</i>	<p>Als u de cursor over het icoon beweegt, verschijnt het volgende bericht:</p> <ul style="list-style-type: none"> • <i>U hebt Avira Web Protection niet geïnstalleerd. Klik om te ontdekken hoe u veilig kunt surfen.</i> <p>Dit bericht wordt weergegeven als u verkeerd installeert of Avira Antivirus de-installeert.</p> <ul style="list-style-type: none"> • <i>Web Protection krijgt u gratis bij Avira Anti-Virus. Klik om te leren hoe u Web Protection installeert.</i> <p>Dit bericht wordt weergegeven als u Web Protection niet installeert of de-installeert.</p> <ul style="list-style-type: none"> → In beide gevallen wordt u wordt doorgestuurd naar de Avira-homepage, waar u het Avira-product kunt downloaden.
	<i>Fout</i>	<p>Als u de cursor over het icoon beweegt, verschijnt het volgende bericht: <i>Avira heeft een fout gemeld. Klik om contact op te nemen met onze afdeling Ondersteuning.</i></p> <ul style="list-style-type: none"> ▶ Klik op het grijze icoon of de tekst om naar de Avira-ondersteuningspagina te gaan.

Widgets

Avira SearchFree bevat drie widgets met de belangrijkste functies voor het hedendaagse surfen op het internet: Facebook, e-mail en Beveiliging van browser.

Facebook

Met deze functie kunt u alle berichten van Facebook ontvangen en altijd up-to-date zijn.

E-mail

Als u het e-mailsymbool op de toolbar aanklikt, wordt er een keuzelijst getoond. U kunt kiezen uit de meest gebruikelijke e-mailproviders.

Beveiliging van browser

Deze widget is ontworpen om u met een enkele klik alle internet-beveiligingsopties die u

dagelijks nodig heeft, aan te bieden. Deze optie is alleen beschikbaar voor Firefox en Internet Explorer. Ook de namen van de functies verschillen soms van browser tot browser:

- *Pop-upblokker*

Wanneer deze optie is ingeschakeld, worden alle pop-upvensters geblokkeerd.

- *Cookies blokkeren*

Als u deze optie activeert, worden er geen cookies op uw computer opgeslagen.

- *Private Browsing (Firefox) / InPrivate Browsing (Internet Explorer)*

Schakel deze optie in als u niet wilt dat enige persoonlijke gegevens op het internet worden achtergelaten terwijl u surft. Deze optie is niet beschikbaar voor Internet Explorer 7 en 8.

- *Recente geschiedenis wissen (Firefox) / Browsergeschiedenis verwijderen (Internet Explorer)*

Met deze optie worden alle sporen van uw internetactiviteiten gewist.

Website Safety Advisor

De Website Safety Advisor verstrekt u een veiligheidsranking tijdens de navigatie.

U kunt de reputatie van de website die u bezoekt, beoordelen en controleren of zij een laag of een hoog risico voor de veiligheid vormt.

Deze widget bevat ook aanvullende informatie over de website, bijv. wie de eigenaar is van de domeinnaam of waarom de website gecategoriseerd is als veilig of riskant.

De status van de Website Safety Advisor wordt weergegeven in de Toolbar en in uw zoekresultaten door middel van een Avira-taakbalkicoon in combinatie met andere iconen:

Icoon	Statusweergave	Beschrijving
	<i>Safe</i>	Een groen vinkje voor veilige websites.
	<i>Laag risico</i>	Een geel uitroepteken voor websites die een laag risico vormen.
	<i>Hoog risico</i>	Een rood stopteken voor websites die een hoog risico voor uw veiligheid betekenen.
	<i>Onbekend</i>	Een grijs vraagteken verschijnt als de status onbekend is.

	<i>Verifiëren</i>	Dit teken verschijnt tijdens het verifiëren van de status van een website.
---	-------------------	--

Browser Tracking Blocker

Met de Browser Tracking Blocker kunt u trackers stoppen bij het verzamelen van informatie over u terwijl u surft.

Met behulp van de widget kunt u kiezen welke trackers geblokkeerd moeten worden en welke niet.

De trackingondernemingen worden ingedeeld in drie categorieën:

- Social Networks
- Advertentienetwerken
- Andere ondernemingen

4.2.2 Opties

Avira SearchFree Toolbar is compatibel met Internet Explorer, Firefox en Google Chrome en kan in de drie webbrowsers worden geconfigureerd:

- [Internet Explorer-configuratie-opties](#)
- [Firefox-configuratie-opties](#)
- [Google Chrome-configuratie-opties](#)

Internet Explorer

In Internet Explorer zijn de volgende configuratie-opties voor de Avira SearchFree Toolbar beschikbaar in het menu **Opties**:

Toolbar-opties

Zoeken

Avira-zoekmachine

In het menu **Avira-zoekmachine** kunt u selecteren welke zoekmachine u wilt gebruiken voor het zoeken. Zoekmachines zijn beschikbaar voor de Verenigde Staten, Brazilië, Duitsland, Spanje, Europa, Frankrijk, Italië, Nederland, Rusland en het Verenigd Koninkrijk.

Open zoekopdrachten in

In het optiemenu **Open zoekopdrachten in** kunt u selecteren waar het zoekresultaat moet worden weergegeven; in het huidige venster, in een nieuw venster of op een nieuw tabblad.

Recente zoekopdrachten weergeven

Wanneer de optie **Recente zoekopdrachten weergeven** is ingeschakeld, kunt u eerdere zoektermen weergeven in het tekstvak van de zoek-toolbar.

Recente zoekgeschiedenis automatisch wissen wanneer ik de browser sluit

Schakel de optie **Recente zoekgeschiedenis automatisch wissen wanneer ik de browser sluit** in, wanneer u eerdere zoekopdrachten niet wilt bewaren en de geschiedenis wilt wissen bij het sluiten van de webbrowser.

Meer opties

Selecteer toolbar taal

Onder **Selecteer toolbar taal** kunt u de taal selecteren waarin de Avira SearchFree Toolbar wordt weergegeven. De toolbar is beschikbaar in het Engels, Duits, Spaans, Frans, Italiaans, Portugees en Nederlands.

Let op

Waar mogelijk komt de standaardtaal van de Avira SearchFree Toolbar overeen met die van uw programma. Indien de toolbar niet beschikbaar is in uw taal, is de standaardtaal Engels.

Tekstlabels van knoppen weergeven

Schakel de optie **Tekstlabels van knoppen weergeven** uit wanneer u de tekst naast de iconen van de Avira SearchFree Toolbar wilt verbergen.

Geschiedenis wissen

Schakel de optie **Geschiedenis wissen** in wanneer u eerdere zoekopdrachten niet wilt bewaren en de geschiedenis onmiddellijk wilt wissen.

Help

Klik op **Help** voor toegang tot de website met veelgestelde vragen (FAQ's) met betrekking tot de toolbar.

Verwijderen

U kunt ook de Avira SearchFree Toolbar rechtstreeks in Internet Explorer de-installeren: [De-installatie via de webbrowser](#)

Info

Klik op **Info** om weer te geven welke versie van Avira SearchFree Toolbar is geïnstalleerd.

Firefox

In Firefox zijn de volgende configuratie-opties voor de Avira SearchFree Toolbar beschikbaar in het menu **Opties**:

Toolbar-opties

Zoeken

Avira-zoekmachine

In het menu **Avira-zoekmachine** kunt u selecteren welke zoekmachine u wilt gebruiken voor het zoeken. Zoekmachines zijn beschikbaar voor de Verenigde Staten, Brazilië, Duitsland, Spanje, Europa, Frankrijk, Italië, Nederland, Rusland en het Verenigd Koninkrijk.

Recente zoekopdrachten weergeven

Wanneer de optie **Recente zoekopdrachten weergeven** is ingeschakeld, kunt u eerdere zoektermen weergeven door klikken op de pijl in de zoek-toolbar. Selecteer een term wanneer u het zoekresultaat opnieuw wilt weergeven.

Recente zoekgeschiedenis automatisch wissen wanneer ik de browser sluit

Schakel de optie **Recente zoekgeschiedenis automatisch wissen wanneer ik de browser sluit** in, wanneer u eerdere zoekopdrachten niet wilt bewaren en de geschiedenis wilt wissen bij het sluiten van de webbrowser.

Geef Ask-zoekresultaten weer wanneer ik trefwoorden of ongeldige URL's typ in de adresbalk van de browser

Wanneer deze optie is ingeschakeld, wordt een zoekopdracht gestart en het zoekresultaat weergegeven, elke keer als u zoekwoorden of een ongeldige URL invoert in de adresbalk van de webbrowser.

Meer opties

Selecteer toolbar taal

Onder **Selecteer toolbar taal** kunt u de taal selecteren waarin de Avira SearchFree Toolbar wordt weergegeven. De toolbar is beschikbaar in het Engels, Duits, Spaans, Frans, Italiaans, Portugees en Nederlands.

Let op

Waar mogelijk komt de standaardtaal van de Avira SearchFree Toolbar overeen met die van uw programma. Indien de toolbar niet beschikbaar is in uw taal, is de standaardtaal Engels.

Tekstlabels van knoppen weergeven

Schakel de optie **Tekstlabels van knoppen weergeven** uit wanneer u de tekst naast de iconen van de Avira SearchFree Toolbar wilt verbergen.

Geschiedenis wissen

Schakel de optie **Geschiedenis wissen** in wanneer u eerdere zoekopdrachten niet wilt bewaren en de geschiedenis onmiddellijk wilt wissen.

Help

Klik op **Help** voor toegang tot de website met veelgestelde vragen (FAQ's) met betrekking tot de toolbar.

Verwijderen

U kunt ook de Avira SearchFree Toolbar rechtstreeks in Firefox de-installeren: [De-installatie via de webbrowser](#).

Info

Klik op **Info** om weer te geven welke versie van Avira SearchFree Toolbar is geïnstalleerd.

Google Chrome

In de Chrome-webbrowser zijn de volgende configuratie-opties voor de Avira SearchFree Toolbar beschikbaar onder het menu van de rode Avira-paraplu:

Help

Klik op **Help** voor toegang tot de website met veelgestelde vragen (FAQ's) met betrekking tot de toolbar.

Instructies voor de-installeren

Hier wordt u doorgesluist naar de artikelen die alle informatie bevatten die u nodig heeft om de toolbar te de-installeren.

Info

Klik op **Info** om weer te geven welke versie van de Avira SearchFree Toolbar is geïnstalleerd.

Tonen/verbergen van de Avira SearchFree Toolbar

Klik hier voor het verbergen of tonen van de Avira SearchFree Toolbar in uw webbrowser.

4.2.3 Avira SearchFree Toolbar de-installeren onder Windows 7

Uw Avira SearchFree Toolbar de-installeren:

- ▶ Sluit uw webbrowser.

Open het **Configuratiescherm** via het Windows-menu **Start**.

Dubbelklik op **Programma's en Onderdelen**.

Selecteer Avira SearchFree Toolbar plus Web Protection in de lijst en klik op **Verwijderen**.

U wordt gevraagd of u dit product daadwerkelijk wilt de-installeren.

Klik op **Ja** om te bevestigen.

Avira SearchFree Toolbar plus Web Protection zijn verwijderd en alle mappen, bestanden en registervermeldingen voor de Avira SearchFree Toolbar plus Web Protection worden verwijderd wanneer uw computer opnieuw wordt opgestart.

4.3 Hoe te...?

De hoofdstukken "Hoe te ...?" bieden een korte handleiding over licentie- en productactivering, evenals informatie over de belangrijkste functies van uw Avira-product. De geselecteerde korte artikelen dienen als een overzicht van de functionaliteit van uw Avira-product. Ze zijn geen vervanging voor de gedetailleerde informatie van elke sectie van dit Help Center.

4.3.1 Licentie activeren

Om de licentie van uw Avira-product te activeren:

Activeer de licentie van uw Avira-product met het *.KEY*-licentiebestand. U kunt dit licentiebestand van Avira verkrijgen via e-mail. Het licentiebestand bevat de licentie voor alle producten die u heeft besteld in één bestelling.

Als u uw Avira-product nog niet heeft geïnstalleerd:

- ▶ Sla het licentiebestand op in een plaatselijke map op uw computer.
- ▶ Installeer uw Avira-product.
- ▶ Voer de opslaglocatie van het licentiebestand in tijdens de installatie.

Als u uw Avira-product al geïnstalleerd hebt:

- ▶ Dubbelklik op het licentiebestand in de bestandsmanager of in de activerings-email en volg de instructies op het scherm als het Licentiebeheer opent.

-OF-

In het Control Center van uw Avira-product selecteert u het menu-item **Help > License management**

Let op

Vanaf Windows Vista verschijnt het dialoogvenster Beheer Gebruikersaccount. Indien mogelijk, log in als administrator. Klik op **Doorgaan**.

- ▶ Markeer het licentiebestand en klik op **Open**.
 - Een bericht verschijnt.
- ▶ Klik op **OK** om te bevestigen.
 - De licentie is geactiveerd.
- ▶ Start uw systeem opnieuw op als dat nodig is.

4.3.2 Product activeren

Om uw Avira-product te activeren heeft u de volgende opties:

Activatie met een geldige volledige licentie

Om het programma te activeren met een volledige licentie, heeft u een geldige activeringscode nodig die gegevens bevat van de licentie die u heeft gekocht. U heeft van ons of per e-mail of afgedrukt op de verpakking van het product de activeringscode ontvangen.

Activatie met een evaluatielicentie

Uw Avira-product wordt geactiveerd met een automatisch gegenereerde evaluatielicentie, waarmee u het Avira-product kunt testen met de volledige functies voor een beperkte periode.

Let op

Om het product te activeren of voor een testlicentie is een actieve internetverbinding noodzakelijk.

Als er geen verbinding kan worden opgezet met de servers van Avira, controleer dan de instellingen van de gebruikte firewall: verbindingen via het HTTP-protocol en poort 80 (webcommunicatie) en via het coderingsprotocol SSL en poort 443 worden gebruikt voor productactivering. Wees er zeker van dat uw firewall geen inkomende en uitgaande gegevens blokkeert. Check allereerst of u toegang heeft tot websites met uw browser.

Hierna wordt beschreven hoe u uw Avira-product kunt activeren:

Als u uw Avira-product nog niet heeft geïnstalleerd:

- ▶ Installeer uw Avira-product.
 - Tijdens het installatieproces wordt u gevraagd een activeringsoptie te kiezen
- **Activeer product:** Activatie met een geldige volledige licentie
- **Test product:** Activatie met een evaluatielicentie


- ▶ Voer de activeringscode voor activering met een volledige licentie in.
- ▶ Bevestig de selectie van de activeringsprocedure door te klikken op **Volgende**.
- ▶ Indien en wanneer dat nodig is, voert u uw persoonlijke gegevens voor registratie in en bevestigt die door te klikken op **Volgende**.
 - ↪ De gegevens van uw licentie worden getoond in het volgende scherm. Uw Avira-product is ingeschakeld.
- ▶ Ga verder om te installeren.

Als u uw Avira-product al geïnstalleerd heeft:

- ▶ Selecteer het menu-item **Help > Licentiebeheer** in het Control Center.
 - ↪ De *licentiewizard* opent, waarin u een activeringsoptie kunt kiezen. De volgende stappen voor de productactivering zijn gelijk aan de hierboven beschreven procedure.

4.3.3 Automatische updates uitvoeren

Om een taak aan te maken met de Avira Planner om uw Avira-product automatisch te updaten:

- ▶ Selecteer in het Control Center de sectie *BEHEER* > **Planner**.
- ▶ Klik op het icoon  **Voeg nieuwe taak toe**.
 - ↪ Het dialoogvenster **Naam en beschrijving van de taak** verschijnt.
- ▶ Geef de taak een naam en, indien van toepassing, een beschrijving.
- ▶ Klik op **Volgende**.
 - ↪ Het dialoogvenster **Type taak** wordt getoond.
- ▶ Selecteer **Bewerk taak** uit de lijst.
- ▶ Klik op **Volgende**.
 - ↪ Het dialoogvenster **Tijdstip voor de taak** verschijnt.
- ▶ Selecteer een tijdstip voor de update:
 - **Onmiddellijk**
 - **Dagelijks**
 - **Wekelijks**
 - **Interval**
 - **Eenmalig**
 - **Aanmelding**

Let op

We adviseren regelmatige automatische updates. De aanbevolen update-interval is: 2 uur.


- ▶ Waar van toepassing, geeft u een datum op conform de selectie.
- ▶ Waar nodig, selecteert u aanvullende opties (beschikbaarheid hangt af van taaktype):
 - **Herhaal taak als de tijd is verstreken**
Taken uit het verleden die niet konden worden uitgevoerd op de gewenste tijd, bijvoorbeeld omdat de computer uitgeschakeld was, worden uitgevoerd.
 - **Start taak terwijl er verbinding met internet wordt gemaakt (inbellen)**
Afgezien van de gedefinieerde frequentie wordt de taak ook uitgevoerd als een internetverbinding tot stand is gekomen.
- ▶ Klik op **Volgende**.
 - ↳ Het dialoogvenster **Selecteer weergavemodus** verschijnt.
- ▶ Selecteer de weergavemodus van het taakvenster:
 - **Onzichtbaar**: geen taakvenster
 - **Geminimaliseerd**: alleen voortgangsindicator
 - **Gemaximaliseerd**: volledig taakvenster
- ▶ Klik op **Voltooien**.
 - ↳ Uw nieuw gemaakte taak verschijnt op de startpagina van de sectie **BEHEER > Planner** met de status ingeschakeld (vinkje).
- ▶ Waar nodig, de-activeert u taken die niet moeten worden uitgevoerd.

Gebruik de volgende iconen om taken nader te definiëren:

 Bekijk eigenschappen van een taak

 Taak bewerken

 Taak verwijderen

 Taak starten

 Taak stoppen

4.3.4 Start een handmatige update

Er zijn verschillende opties om een update handmatig te starten: als een update handmatig wordt gestart, worden het virusdefinitiebestand en de scan-engine altijd bijgewerkt.

Om een update van uw Avira-product handmatig te starten:

- ▶ Klik met de rechtermuisknop op het Avira-icoon in de taakbalk.
 - ↪ Een contextmenu verschijnt.
- ▶ Selecteer **Start update**.
 - ↪ Het **Updater**-dialoogvenster verschijnt.

-OF-

- ▶ Selecteer **Status** in het Control Center.
- ▶ In het veld **Laatste update**, klikt u op de link **Start update**.
 - ↪ Het dialoogvenster Updater verschijnt.

-OF-

- ▶ Selecteer in het Control Center, in het menu **Update** de opdracht **Start update**.
 - ↪ Het dialoogvenster Updater verschijnt.

Let op

We adviseren regelmatige automatische updates. De aanbevolen update-interval is: 2 uur.

Let op

U kunt ook rechtstreeks een handmatige update uitvoeren via het Windows Security Center.

4.3.5 Een scanprofiel gebruiken om te scannen op virussen en malware

Een scanprofiel is een set van stations en mappen die moeten worden gescand.

De volgende opties zijn beschikbaar voor scannen met een scanprofiel:

Gebruik een voorgedefinieerd scanprofiel

Als het voorgedefinieerde profiel overeenkomt met uw wensen.

Aanpassen en toepassen van een scanprofiel (handmatige selectie).

Als u wilt scannen met een aangepast scanprofiel.

Een nieuw scanprofiel maken en toepassen

Als u uw eigen scanprofiel wilt maken.

Afhankelijk van het besturingssysteem zijn verschillende iconen beschikbaar om een scanprofiel te starten:

- In Windows XP:



Dit pictogram start de scan via een scanprofiel.

- Sinds Windows Vista:

Sinds Microsoft Windows Vista heeft het Control Center slechts beperkte rechten, bijvoorbeeld voor toegang tot folders en bestanden. Bepaalde acties en bestandstoegang kunnen alleen worden uitgevoerd in het Control Center met uitgebreide administrator-rechten. Deze uitgebreide administrator-rechten moeten aan het begin van iedere scan worden toegewezen via een scanprofiel.



- Dit pictogram start een beperkte scan via een scanprofiel. Alleen folders en bestanden waarvoor het bedrijfssysteem toegangsrechten heeft verleend, worden gescand.



- Dit pictogram start de scan met uitgebreide administrator-rechten. Na bevestiging worden alle mappen en bestanden in het geselecteerde scanprofiel gescand.

Scannen naar virussen en malware met een scanprofiel:

- ▶ Ga naar het Control Center en selecteer de sectie *PC PROTECTION* > **System Scanner**.

→ Voorgedefinieerde scanprofielen verschijnen.

- ▶ Selecteer één van de voorgedefinieerde profielen.

-OF-

Pas het scanprofiel aan **Handmatige selectie**.

-OF-

Maak een nieuw scanprofiel

- ▶ Klik op het pictogram (in Windows XP:  , vanaf Windows Vista: ).

- ▶ Het **Luke Filewalker**-venster verschijnt en er wordt een systeemscan gestart.



→ Als de scan is voltooid, worden de resultaten getoond.

Wanneer u een scanprofiel wilt aanpassen:

- ▶ In het scanprofiel, open door **Handmatige selectie** de bestandsstructuur zodat alle stations en mappen die u wilt scannen zijn geopend.

- Klik op het +-pictogram: het volgende mapniveau wordt getoond.
- Klik op het --pictogram: het volgende mapniveau wordt verborgen.
- ▶ Markeer de knooppunten en mappen die gescand moeten worden door op het relevante vak te klikken van het desbetreffende mapniveau:
De volgende opties zijn beschikbaar om mappen te selecteren:
 - Map, inclusief onderliggende map (zwart vinkje)
 - Alleen onderliggende mappen van één map (grijs vinkje, onderliggende mappen hebben een zwart vinkje)
 - Geen map (geen vinkje)

Wanneer u een nieuw scanprofiel wilt maken:

- ▶ Klik op het  **Maak nieuw profiel**-pictogram.
 - Het profiel **Nieuw profiel** verschijnt onder de al eerder gecreëerde profielen.
- ▶ Indien van toepassing, hernoem dan het scanprofiel door te klikken op het pictogram .
- ▶ Markeer de knooppunten en mappen die bewaard moeten worden door het keuzevak van het desbetreffende mapniveau te activeren.
De volgende opties zijn beschikbaar om mappen te selecteren:
 - Map, inclusief onderliggende map (zwart vinkje)
 - Alleen onderliggende mappen van één map (grijs vinkje, onderliggende mappen hebben een zwart vinkje)
 - Geen map (geen vinkje)

4.3.6 Scan op virussen en malware door middel van slepen en neerzetten

Systematisch scannen op virussen en malware door middel van slepen en neerzetten:

- ✓ Het Control Center van uw Avira-product is geopend.
- ▶ Markeer het bestand of de map die u wilt scannen.
- ▶ Gebruik de linker muisknop om het gemarkeerde bestand of de map naar het **Control Center** te slepen.
 - Het **Luke-Filewalker**-venster verschijnt en er wordt een systeemsan gestart.
 - Wanneer de scan is voltooid, worden de resultaten weergegeven.

4.3.7 Scan op virussen en malware via het contextmenu

Systematisch scannen op virussen en malware via het contextmenu:

- ▶ Klik met de rechtermuisknop (bijv. in Windows Explorer op het bureaublad of in een geopende Windows-map) op het bestand of de map die u wilt scannen.


- Het contextmenu van Windows Explorer verschijnt.
- ▶ Selecteer **Geselecteerde bestanden scannen met Avira** in het contextmenu.
 - Het **Luke-Filewalker**-venster verschijnt en er wordt een systeemscan gestart.
 - Zo gauw de scan is voltooid, worden de resultaten weergegeven.

4.3.8 Scan automatisch op virussen en malware

Let op

Na installatie wordt de taak **Volledige systeemscan** aangemaakt in de Planner: een complete systeemscan wordt automatisch uitgevoerd volgens een aanbevolen interval.

Om een taak te maken voor het automatisch scannen op virussen en malware:






- ▶ Selecteer de sectie **BEHEER > Planner** in het Control Center.
- ▶ Klik op het icoon .
- Het dialoogvenster **Naam en beschrijving van de taak** verschijnt.
- ▶ Geef de taak een naam en, waar van toepassing, een beschrijving.
- ▶ Klik op **Volgende**.
 - Het dialoogvenster **Type taak** verschijnt.
- ▶ Selecteer **Scantaak**.
- ▶ Klik op **Volgende**.
 - Het dialoogvenster **Selectie van het profiel** verschijnt.
- ▶ Selecteer het profiel dat moet worden gescand.
- ▶ Klik op **Volgende**.
 - Het dialoogvenster **Tijdstip voor de taak** verschijnt.
- ▶ Selecteer een tijdstip voor de scan:
 - **Onmiddellijk**
 - **Dagelijks**
 - **Wekelijks**
 - **Interval**
 - **Eenmalig**
 - **Login**
- ▶ Waar nodig, geeft u een datum op conform de selectie.
- ▶ Waar van toepassing, selecteert u de volgende aanvullende opties (beschikbaarheid hangt af van taaktype):

Taak herhalen als tijd al is verlopen

Taken uit het verleden worden uitgevoerd die niet konden worden uitgevoerd op de gewenste tijd, bijvoorbeeld omdat de computer uitgeschakeld was.

- ▶ Klik op **Volgende**.
 - Het dialoogvenster **Selectie van de weergavemodus** verschijnt.
- ▶ Selecteer de weergavemodus voor het taakvenster:
 - **Onzichtbaar**: geen taakvenster
 - **Geminimaliseerd**: alleen voortgangsindicator.
 - **Gemaximaliseerd**: volledig taakvenster
- ▶ Selecteer de optie **Computer afsluiten als taak is voltooid** als u wilt dat de computer automatisch uitschakelt als de scan is voltooid. Deze optie is alleen beschikbaar als de weergavemodus is ingesteld op geminimaliseerd of gemaximaliseerd.
- ▶ Klik op **Voltooien**.
 - Uw nieuw gemaakte taak verschijnt op de startpagina van de sectie **BEHEER > Planner** met de status ingeschakeld (vinkje).
- ▶ Waar nodig, de-activeert u taken die niet moeten worden uitgevoerd.



Gebruik de volgende iconen om taken nader te definiëren:

Pictogram	Beschrijving
	Bekijk de eigenschappen van een taak
	Taak bewerken
	Taak verwijderen
	Taak starten
	Taak stoppen

4.3.9 Gerichte scan naar Rootkits en actieve malware

Om te scannen naar actieve rootkits gebruikt u het voorgedefinieerde scanprofiel **Scan naar Rootkits en actieve malware**.

Om systematisch te scannen naar actieve rootkits:

- ▶ Ga naar het Control Center en selecteer de sectie *PC PROTECTION* > **System Scanner**.
 - Voorgedefinieerde scanprofielen verschijnen.
- ▶ Selecteer het voorgedefinieerde scanprofiel **Scan naar Rootkits en actieve malware**.
- ▶ Voor zover nodig, markeert u andere knooppunten en directories die gescand moeten worden door het selectievakje op mapniveau aan te vinken.
- ▶ Klik op het pictogram (in Windows XP: , vanaf Windows Vista: ).
 - Het **Luke Filewalker**-venster verschijnt en er wordt een systeemscan gestart.
 - Als de scan is voltooid, worden de resultaten getoond.

4.3.10 Reageer op gedetecteerde virussen en malware

Voor de individuele Protectionscomponenten van uw Avira-product kunt u definiëren hoe uw Avira-product reageert op een gedetecteerd virus of ongewenst programma in de **Configuratie** onder de sectie **Actie bij detectie**.

Er zijn geen configureerbare actie-opties beschikbaar voor de ProActiv-component van de Real-Time Protection: mededeling van een detectie wordt altijd gedaan in het venster **Real-Time Protection: Verdacht applicatiegedrag**.

Actie-opties voor de Scanner:

Interactief

In de interactieve actiemodus worden de resultaten van de Scanner weergegeven in een dialoogvenster. Deze optie wordt ingeschakeld als de standaardinstelling.

In het geval van een **Scanner-scan**, krijgt u een waarschuwing met een lijst van de geïnfekteerde bestanden zo gauw de scan afgerond is. U kunt het contextgevoelige menu gebruiken om een uit te voeren actie te selecteren voor de verschillende geïnfekteerde bestanden. U kunt de standaardacties uitvoeren voor alle geïnfekteerde bestanden of de Scanner annuleren.

Automatisch

In de automatische actiemodus wordt, als een virus of een ongewenst programma wordt gedetecteerd, de actie die u geselecteerd heeft voor dit onderdeel, automatisch uitgevoerd.

Actie-opties voor de Real-Time Protection:

Interactief

In de interactieve actiemodus wordt toegang tot gegevens geweigerd en wordt er een bureaubladmededeling weergegeven. In de bureaubladmededeling kunt u de gedetecteerde malware verwijderen of de malware doorsturen met behulp van de knop **Details** naar de Scanner-component voor aanvullend virusmanagement. De Scanner opent een scherm met een mededeling van de detectie, die u verschillende opties geeft voor het behandelen van het betroffen bestand via een contextmenu (zie [Detectie > Scanner](#)):

Automatisch

In de automatische actiemodus wordt, als een virus of een ongewenst programma wordt gedetecteerd, de actie die u geselecteerd heeft in dit onderdeel, automatisch uitgevoerd.

Actie-opties voor Mail Protection, Web Protection:

Interactief

In de interactieve actiemodus verschijnt, als er een virus of een ongewenst programma wordt gedetecteerd, een dialoogvenster waarin u kunt selecteren wat u wilt doen met het geïnfecteerde object. Deze optie wordt ingeschakeld als de standaardinstelling.

Automatisch

In de automatische actiemodus wordt, als een virus of een ongewenst programma wordt gedetecteerd, de actie die u geselecteerd heeft voor dit onderdeel, automatisch uitgevoerd.

In de interactieve actiemodus kunt u reageren op gedetecteerde virussen of ongewenste programma's door een actie voor het geïnfecteerde object te kiezen in de waarschuwing en de geselecteerde actie uit te voeren door op **Bevestig** te klikken.

De volgende acties voor omgang met geïnfecteerde objecten zijn beschikbaar voor selectie:

Let op

Welke acties beschikbaar zijn voor selectie hangt af van het besturingssysteem, de beschermingsonderdelen (Avira Real-Time Protection, Avira Scanner, Avira Mail Protection, Avira Web Protection) die de detectie rapporteren, en het type gedetecteerde malware.

Acties van de Scanner en de Real-Time Protection (geen ProActiv-detecties):

Repareren

Het bestand is gerepareerd.

Deze optie is alleen beschikbaar als het geïnfekteerde bestand gerepareerd kan worden.

Hernoemen

Het bestand wordt hernoemd met een *.vir-extensie. Directe toegang tot deze bestanden (bijv. door dubbelklikken) is daarom niet meer mogelijk. Bestanden kunnen later gerepareerd worden en hun originele namen terugkrijgen.

Quarantaine

Het bestand wordt verpakt in een speciaal formaat (*.qua) en verplaatst naar de Quarantainemap **GEÏNFECTEERD** op uw harde schijf, zodat directe toegang niet langer mogelijk is. Bestanden in deze map kunnen gerepareerd worden in Quarantaine op een later tijdstip of, indien nodig, verstuurd worden naar Avira.

Verwijderen

Het bestand wordt verwijderd. Dit proces is veel sneller dan **Overschrijven en verwijderen**. Als een bootsectorvirus wordt gedetecteerd, kan het verwijderd worden door de bootsector te verwijderen. Een nieuwe bootsector wordt geschreven.

Negeren

Er wordt geen verdere actie ondernomen. Het geïnfekteerde bestand blijft actief op uw computer.

Overschrijven en verwijderen

Het bestand wordt overschreven met een standaard template en daarna verwijderd. Het kan niet hersteld worden.

Waarschuwing

Dit kan resulteren in dataverlies en schade aan het besturingssysteem!
Selecteer de **Negeren**-optie alleen in uitzonderlijke gevallen.

Altijd negeren

Actie-optie voor Real-Time Protection-detecties: er wordt geen verdere actie ondernomen door Real-Time Protection. Toegang tot het bestand is toegestaan. Alle verdere toegang tot dit bestand is toegestaan en er worden geen extra mededelingen gegeven totdat de computer opnieuw opgestart is of het virusdefinitiebestand is geüpdatet.

Naar quarantaine kopiëren

Actie-opties voor een rootkitsdetectie: de detectie wordt gekopieerd naar quarantaine.

Repareer bootsector | Download reparatie-tool

Actie-opties voor geïnfecteerde bootsectors zijn gedetecteerd: er zijn een aantal opties beschikbaar om geïnfecteerde diskettestations te repareren. Als uw Avira-product de reparatie niet uit kan voeren, kunt u een speciale tool downloaden om bootsectorvirussen te detecteren en te verwijderen.

Let op

Als u acties uitvoert op draaiende processen, worden de betrokken processen beëindigd voordat de acties worden uitgevoerd.

Acties van de Real-Time Protection voor detecties door de ProActiv-component (mededeling van verdachte acties van een toepassing):

Vertrouwd programma

De toepassing blijft actief. Het programma wordt toegevoegd aan de lijst van toegestane toepassingen en wordt uitgezonderd van controle door het ProActiv-onderdeel. Bij het toevoegen aan de lijst van toegestane toepassingen wordt het controletype ingesteld op *Inhoud*. Dit betekent dat de toepassing alleen uitgezonderd is van controle door het ProActiv-onderdeel als de inhoud onveranderd blijft (zie [Toepassingsfilter: Toegestane toepassingen](#)).

Programma eenmaal blokkeren

De toepassing wordt geblokkeerd, d.w.z. de toepassing wordt afgesloten. De acties van de toepassing worden verder gecontroleerd door het ProActiv-onderdeel.

Dit programma altijd blokkeren

De toepassing wordt geblokkeerd, d.w.z. de toepassing wordt afgesloten. Het programma wordt toegevoegd aan de lijst van geblokkeerde toepassingen en kan niet langer draaien (zie [Toepassingsfilter: Geblokkeerde toepassingen](#)).

Negeren

De toepassing blijft actief. De acties van de toepassing worden verder gecontroleerd door het ProActiv-onderdeel.

Mail Protection-acties: Inkomende e-mails

Naar quarantaine verplaatsen

De e-mail inclusief alle bijlagen wordt verplaatst naar [quarantaine](#). De geïnfecteerde mail wordt verwijderd. De inhoud van de tekst en alle bijlagen van de e-mail worden vervangen door een [standaardtekst](#).

E-mail verwijderen

De geïnfecteerde mail wordt verwijderd. De inhoud van de tekst en alle bijlages van de e-mail worden vervangen door een [standaardtekst](#).

Bijlage verwijderen

De geïnfecteerde bijlage wordt vervangen door een [standaardtekst](#). Als de inhoud van de e-mail geïnfecteerd is, wordt deze verwijderd en vervangen door een [standaardtekst](#). De e-mail zelf wordt afgeleverd.

Bijlage naar quarantaine verplaatsen

De geïnfecteerde bijlage wordt in [quarantaine](#) geplaatst en daarna verwijderd (vervangen door een [standaardtekst](#)). De body van de e-mail wordt afgeleverd. De geïnfecteerde bijlage kan later worden afgeleverd via de [quarantainemanager](#).

Negeren

De geïnfecteerde e-mail wordt afgeleverd.

Waarschuwing

Virussen en andere ongewenste programma's kunnen hierdoor uw computersysteem binnendringen. Selecteer de optie **Negeren** alleen in uitzonderlijke gevallen. Schakel de preview in uw e-mailprogramma uit; open nooit bijlages door dubbelklikken!

Mail Protection-acties: Uitgaande e-mails

E-mail in quarantaine plaatsen (niet verzenden)

De e-mail met alle bijlages wordt gekopieerd naar [Quarantaine](#) en niet verzonden. De e-mail blijft in de outbox van uw e-mailclient. U ontvangt een foutmelding in uw e-mailprogramma. Alle andere e-mails die worden verzonden vanaf uw account worden gecontroleerd op malware.

Blokkeer het versturen van e-mails (niet verzenden)

De e-mail wordt niet verzonden en blijft in de outbox van uw e-mailprogramma. U ontvangt een foutmelding in uw e-mailprogramma. Alle andere e-mails die worden verzonden vanaf uw account worden gecontroleerd op malware.

Negeren

De geïnfecteerde e-mail wordt verstuurd.

Waarschuwing

Virussen en ongewenste programma's kunnen zo het computersysteem van de e-mailontvanger binnendringen.

Web Protection-acties:

Toegang weigeren

De door de webserver opgevraagde website en/of willekeurige gegevens of bestanden die worden verplaatst, worden niet naar uw webbrowser verstuurd. Een foutmelding om u te informeren dat de toegang is geweigerd, wordt weergegeven in de webbrowser.

Naar quarantaine verplaatsen

De door de webserver opgevraagde website en/of willekeurige gegevens of bestanden die worden verplaatst, worden verplaatst naar quarantaine. Het geïnfecteerde bestand kan worden teruggehaald uit de quarantainemanager wanneer het een informatieve waarde heeft of - indien nodig - worden gestuurd naar het Avira Malware Research Center.

Negeren

De door de webserver opgevraagde website en/of willekeurige gegevens of bestanden die werden verplaatst, worden door Web Protection doorgestuurd naar uw webbrowser.

Waarschuwing

Virussen en andere ongewenste programma's kunnen hierdoor uw computersysteem binnendringen. Selecteer de optie **Negeren** alleen in uitzonderlijke gevallen.

Let op

Wij raden aan om alle verdachte bestanden die niet gerepareerd kunnen worden, naar quarantaine te verplaatsen.

Let op

U kunt ook bestanden gerapporteerd door de heuristiek, voor analyse naar ons toesturen.

U kunt bijvoorbeeld deze bestanden uploaden naar onze website:

<http://www.avira.nl/sample-upload>


U kunt door de heuristiek gerapporteerde bestanden herkennen aan de benaming *HEUR/* of *HEURISTIC/* die voorafgaat aan de bestandsnaam, bijv.: *HEUR/testfile.**.

4.3.11 Bestanden in quarantaine afhandelen (*.qua):

Omgaan met in quarantaine geplaatste bestanden:


- ▶ Selecteer de sectie *BEHEER* > **Quarantaine** in het Control Center.
- ▶ Controleer om welke bestanden het gaat, zodat u, indien nodig, de originele opnieuw op uw computer kunt plaatsen vanaf een andere locatie.

Wanneer u meer informatie over een bestand wilt zien:


- ▶ Markeer het bestand en klik op  .
 - ↳ Het dialoogvenster **Eigenschappen** verschijnt met meer informatie over het bestand.

Wanneer u een bestand opnieuw wilt scannen:


Het scannen van een bestand wordt aanbevolen wanneer het virusdefinitiebestand van uw Avira-product is geüpdatet en een foutief positief rapport wordt vermoed. Dit stelt u in staat een foutieve positief te bevestigen met een nieuwe scan en het bestand te herstellen.

- ▶ Markeer het bestand en klik op  .
 - ↳ Het bestand wordt gescand op virussen en malware door middel van de systeemscan-instellingen.
 - ↳ Na de scan verschijnt het dialoogvenster **Opnieuw scannen statistieken** waarin statistieken worden weergegeven over de status van het bestand voor en na de nieuwe scan.

Om een bestand te verwijderen:

- ▶ Markeer het bestand en klik op  .
- ▶ U moet uw keuze bevestigen met **Ja**.

Wanneer u het bestand wilt uploaden naar een Avira Malware Research Center-webserver voor analyse:

- ▶ Markeer het bestand dat u wilt uploaden.
- ▶ Klik op  .
 - ↳ Een dialoogvenster opent met een formulier voor het invoeren van uw contactgegevens.
- ▶ Voer alle gevraagde gegevens in.
- ▶ Selecteer een type: **Verdacht bestand** of **Verdenking van foutief positief**.
- ▶ Selecteer een antwoordformaat: **HTML**, **Tekst**, **HTML & Tekst**.
- ▶ Klik op **OK**.
 - ↳ Het bestand wordt in gecomprimeerde vorm geüpload naar de Avira Malware Research Center-webserver.

Let op

In de volgende gevallen wordt analyse door het Avira Malware Research Center aanbevolen:

heuristische hits (Verdacht bestand): tijdens een scan; door uw Avira-product is een bestand geclassificeerd als verdacht en in quarantaine geplaatst: analyse van het bestand door het Avira Malware Research Center werd aanbevolen in het dialoogvenster virusdetectie of in het rapportbestand gegenereerd door de scan

.Verdacht bestand: u beschouwt een bestand als verdacht en heeft het daarom in quarantaine geplaatst, maar een scan van het bestand op virussen en malware is negatief.

Verdenking van foutief positief: u veronderstelt dat een virusdetectie een foutief positief is: uw Avira-product rapporteert een detectie in een bestand waarvan het bijzonder onwaarschijnlijk is dat het geïnfecteerd werd door malware.


Let op

De omvang van de bestanden die u uploadt, is begrensd tot 20 MB niet-gecomprimeerd of 8 MB gecomprimeerd.

Let op

U kunt slechts één bestand per keer uploaden.


Wanneer u een in quarantaine geplaatst object van quarantaine wilt kopiëren naar een andere directory:

- ▶ Markeer het in quarantaine geplaatste object en klik op  .
 - ↳ Het dialoogvenster *Blader Naar Map* opent waarin u een directory kunt selecteren.
- ▶ Selecteer een directory waar u een kopie van het in quarantaine geplaatste object wilt bewaren en bevestig uw keuze.
 - ↳ Het geselecteerde in quarantaine geplaatste object wordt opgeslagen in de geselecteerde directory.

Let op

Het in quarantaine geplaatste object is niet identiek aan het herstelde bestand. Het in quarantaine geplaatste bestand is gecodeerd en kan niet worden uitgevoerd of gelezen in het oorspronkelijke formaat.


Wanneer u de eigenschappen van een in quarantaine geplaatst object naar een tekstbestand wilt exporteren:

- ▶ Markeer het in quarantaine geplaatste object en klik op  .
 - ↳ Het tekstbestand *quarantaine - Kladblok* opent met de gegevens van het geselecteerde in quarantaine geplaatste object.
- ▶ Sla het tekstbestand op.


U kunt de bestanden in quarantaine ook herstellen (zie Hoofdstuk: [Quarantaine: Bestanden in quarantaine herstellen](#)).

4.3.12 Herstellen van bestanden in quarantaine

Verschillende iconen voor de herstelprocedure, afhankelijk van het besturingssysteem:

- In Windows XP:
 -  Dit icoon herstelt het bestand naar de originele directory.
 -  Dit icoon herstelt het bestand naar een directory van uw keuze.
- Vanaf Windows Vista:

Vanaf Microsoft Windows Vista heeft het Control Center slechts beperkte rechten, bijvoorbeeld voor toegang tot mappen en bestanden. Bepaalde acties en bestandstoegang kunnen alleen worden uitgevoerd in het Control Center met uitgebreide administrator-rechten. Deze uitgebreide administrator-rechten moeten aan het begin van iedere scan worden toegewezen via een scanprofiel.

 -  Dit icoon herstelt het bestand naar een directory van uw keuze.
 -  Dit icoon herstelt het bestand naar de originele directory. Wanneer uitgebreide administrator-rechten zijn vereist voor toegang tot de directory, verschijnt een overeenkomstig verzoek.


Herstellen van bestanden in quarantaine:

Waarschuwing



Dit kan resulteren in verlies van data en schade aan het besturingssysteem van de computer! Gebruik de functie **Herstel geselecteerd object** alleen in uitzonderlijke gevallen. Herstel alleen bestanden die kunnen worden gerepareerd door een nieuwe scan.

- ✓ Bestand opnieuw gescand en gerepareerd.
- ▶ Selecteer de sectie *BEHEER* > **Quarantaine** in het Control Center.

Let op


E-mails en bijlagen bij e-mails kunnen met de optie  alleen worden hersteld als de extensie **.eml* is.

Om een bestand te herstellen naar de originele locatie:

- ▶ Markeer het bestand en klik op het pictogram (Windows XP: , Windows Vista ).


Deze optie is niet beschikbaar voor e-mails.

Let op

E-mails en bijlagen bij e-mails kunnen met de optie  alleen worden hersteld als de extensie **.eml* is.


- Er verschijnt een bericht waarin wordt gevraagd of u het bestand wilt herstellen.
- ▶ Klik op **Ja**.
 - Het bestand wordt hersteld in de directory waar het zich bevond voordat het in quarantaine werd geplaatst.

Om een bestand te herstellen naar een opgegeven directory:

- ▶ markeer het bestand en klik op  .
 - Er verschijnt een bericht waarin wordt gevraagd of u het bestand wilt herstellen.
- ▶ Klik op **Ja**.
 - Het standaard Windows-venster *Opslaan als* voor het selecteren van de directory verschijnt.
- ▶ Kies de directory om het bestand te herstellen en bevestig.
 - Het bestand wordt hersteld in de gekozen directory.

4.3.13 Verplaats verdachte bestanden naar quarantaine

Een verdacht bestand handmatig naar quarantaine verplaatsen:

- ▶ Selecteer in het Control Center de sectie *BEHEER* > **Sectie Quarantaine**.
- ▶ Klik op  .
 - Het standaardvenster van Windows voor het selecteren van een bestand verschijnt.

- ▶ Selecteer het bestand en bevestig met **Openen**.
 - ↳ Het bestand wordt verplaatst naar de quarantaine.

U kunt bestanden in quarantaine scannen met de Avira System Scanner (zie hoofdstuk: [Quarantaine: Behandeling van bestanden in quarantaine \(*.qua\)](#)).

4.3.14 Het bestandstype in een scanprofiel bewerken of verwijderen

Om aanvullende bestandstypen die moeten worden gescand te bepalen, of specifieke bestandstypen uit te sluiten van de scan in een scanprofiel (alleen mogelijk voor handmatige selectie en aangepaste scanprofielen):

- ✓ Ga in het Control Center naar de *PC PROTECTION* > **System Scanner**-sectie.
- ▶ Klik met de rechtermuisknop op het scanprofiel dat u wilt bewerken.
 - ↳ Een contextmenu verschijnt.
- ▶ Selecteer **Bestandsfilter**.
- ▶ Vergroot het contextmenu door aan de rechterkant van het contextmenu op de kleine driehoek te klikken.
 - ↳ De ingangen **Standaard**, **Scan alle bestanden** en **Gedefinieerd door gebruiker** verschijnen.
- ▶ Selecteer **Gedefinieerd door gebruiker**.
 - ↳ Het dialoogvenster **Bestandsextensies** verschijnt met een lijst van alle bestandstypen die met het scanprofiel moeten worden gescand.

Als u een bestandstype van de scan wilt uitsluiten:

- ▶ markeer het bestandstype en klik op **Verwijderen**.

Als u een bestandstype aan de scan wilt toevoegen:

- ▶ markeer een bestandstype.
- ▶ Klik op **Invoegen** en voer de bestandsextensie van het bestandstype in het invoervak in.


Gebruik maximaal 10 tekens en voer niet de punt vóór de extensie in. Wildcards (* en ?) zijn toegestaan.

4.3.15 Maak een bureaubladsnelkoppeling voor een scanprofiel

U kunt een systeemsan rechtstreeks starten vanaf uw bureaublad via een snelkoppeling op het bureaublad naar een scanprofiel, zonder dat u eerst het Control Center van uw Avira-product hoeft te openen.

Een snelkoppeling op het bureaublad maken naar het scanprofiel:

- ✓ Ga in het Control Center naar de sectie *PC-BEVEILIGING* > **System Scanner**.

- ▶ Selecteer het scanprofiel waarvoor u een snelkoppeling wilt maken.
- ▶ Klik op het pictogram  .
 - De snelkoppeling op het bureaublad wordt aangemaakt.

4.3.16 Filter gebeurtenissen

Gebeurtenissen die worden gegenereerd door programmaonderdelen van uw Avira-product worden weergegeven in het Control Center onder **BEHEER > Gebeurtenissen**. (vergelijkbaar met de gebeurtenisweergave van uw Windows-besturingssysteem). De programmaonderdelen, op alfabetische volgorde, zijn de volgende:

- Helper Service
- Mail Protection
- Real-Time Protection
- Planner
- Scanner
- Updater
- Web Protection
- ProActiv

De volgende gebeurtenistypen worden weergegeven:

- *Informatie*
- *Waarschuwing*
- *Fout*
- *Detectie*

Om weergegeven gebeurtenissen te filteren:

- ▶ Selecteer de sectie **BEHEER > Gebeurtenissen** in het Control Center.
- ▶ Markeer het vak van de programmaonderdelen om de gebeurtenissen van de geactiveerde onderdelen weer te geven.

-OF-

Haal de markering weg van het vak van de programmaonderdelen om de gebeurtenissen van de gedeactiveerde onderdelen te verbergen.


- ▶ Markeer het vak gebeurtenistype om deze gebeurtenissen weer te geven.

-OF-

Haal de markering weg van het vak gebeurtenistype om deze gebeurtenissen te verbergen.

4.3.17 Sluit e-mailadressen uit van scan

Om in te stellen welke e-mailadressen (afzenders) uitgesloten zijn van de Mail Protection-scan (white listing):

- ▶ Ga naar het Control Center en selecteer de sectie *INTERNETBESCHERMING* > **Mail Protection**.
 - ↳ De lijst toont binnenkomende e-mails.
- ▶ Markeer de e-mail die u wilt uitsluiten van de Mail Protection-scan.
- ▶ Klik op het icoon om de e-mail uit te sluiten van de Mail Protection-scan.
-  Het geselecteerde e-mailadres wordt niet langer gescand op virussen en ongewenste programma's.
 - ↳ Het e-mailadres van de afzender wordt opgenomen in de uitzonderingenlijst en niet langer gescand op virussen, malware .

Waarschuwing

Sluit e-mailadressen alleen uit van de Mail Protection-scan als de afzenders compleet betrouwbaar zijn.

Let op

U kunt andere e-mailadressen toevoegen of verwijderen van de uitzonderingenlijst in Configuratie, onder [Mail Protection > Algemeen > Uitzonderingen](#).

5. Detectie

5.1 Overzicht

Uw Avira kan automatisch bepaalde acties uitvoeren of interactief reageren als een virus wordt gedetecteerd. In de interactieve actiemodus opent een dialoogvenster als een virus wordt gedetecteerd waarin u de verdere afhandeling van het virus kunt beheren of initiëren (verwijderen, negeren, etc). Er is een optie in de automatische modus om een waarschuwing weer te geven als een virus wordt gedetecteerd. De actie die automatisch werd uitgevoerd, wordt weergegeven in het bericht.

Dit hoofdstuk bevat uitgebreide informatie, gerangschikt naar module, over detectieberichten.

- zie Hoofdstuk [Scanner](#): Interactieve actiemodus
- zie Hoofdstuk [Scanner](#): Bestanden versturen naar Protection Cloud
- zie Hoofdstuk [Real-Time Protection](#)
- zie Hoofdstuk [Real-Time Protection](#): Verdacht gedrag
- zie Hoofdstuk [Mail Protection](#): Inkomende e-mails
- zie Hoofdstuk [Mail Protection](#): Uitgaande e-mails
- zie Hoofdstuk [Verstuurde E-mail](#): Server
- zie Hoofdstuk [Verstuurde E-mail](#): Afzender
- zie Hoofdstuk [Web Protection](#)

5.2 Interactieve actiemodus

Als u de modus *Interactief* heeft geselecteerd als actiemodus als er een virus wordt gedetecteerd, ontvangt u een waarschuwing met daarin een lijst van de getroffen bestanden, zo gauw de scan is afgerond (zie de configuratiesectie [Scanner > Scan > Actie bij detectie](#)).

U kunt het contextgevoelige menu gebruiken om een uit te voeren actie te selecteren voor de verschillende geïnfecteerde bestanden. U kunt de standaardacties uitvoeren voor alle geïnfecteerde bestanden of de Scanner annuleren.

Let op

Als [rapporteren](#) is ingeschakeld, registreert de Scanner elke detectie in het [Rapport bestand](#).

5.2.1 Waarschuwing



5.2.2 Detectie, Fouten, Waarschuwingen

Gedetailleerde informatie, actie-opties voor de gedetecteerde virussen en berichten worden weergegeven in de tabbladen **Detectie**, **Fouten** en **Waarschuwingen**.

- **Detectie:**
 - *Object:* Bestandsnaam van het getroffen bestand
 - *Detectie:* Naam van het virus of ongewenste programma
 - *Actie:* Geselecteerde actie waarmee het getroffen bestand afgehandeld moet worden. U kunt andere acties kiezen voor het afhandelen van malware uit het contextgevoelige menu van de weergegeven actie.
- **Fout:** berichten over fouten die voorkwamen tijdens de scan
- **Waarschuwingen:** waarschuwingen met betrekking tot virussen die werden gedetecteerd

Let op

De volgende informatie wordt weergegeven in de tooltip van het object: Naam

van het getroffen bestand en het complete pad, naam van het virus en de actie die wordt uitgevoerd met de **Nu toepassen**-knop.

Let op

De standaardactie van de Scanner wordt weergegeven als de uit te voeren actie. De standaardactie van de Scanner voor het afhandelen van getroffen bestanden is om alle relevante bestanden naar quarantaine te verplaatsen.

5.2.3 Opties in het contextmenu

Let op

Als de detectie een heuristische hit (HEUR/), een uitzonderlijke runtimepacker (PCK/) of een bestand met een verborgen bestandsextensie (HEUR-DBLEXT/) is, zijn in [interactieve modus](#) alleen de opties [Naar quarantaine verplaatsen](#) en [Negeren](#) beschikbaar. In de [automatische modus](#) wordt de detectie automatisch verplaatst naar [quarantaine](#). Deze beperking voorkomt dat de gedetecteerde bestanden, die misschien een vals alarm zijn, rechtstreeks van uw computer worden verwijderd. Het bestand kan op elk moment worden hersteld met behulp van de [Quarantainemanager](#).

Repareren

Als deze optie is ingeschakeld, repareert de Scanner het getroffen bestand.

Let op

De optie **Repareren** kan alleen worden ingeschakeld als reparatie van het gedetecteerde bestand mogelijk is.

Quarantaine

Als deze optie is ingeschakeld, verplaatst de Scanner het bestand naar de [quarantaine](#). Het bestand kan worden teruggehaald uit de [Quarantainemanager](#) wanneer het een informatieve waarde heeft of - indien nodig - worden gestuurd naar het Avira Malware Research Center. Afhankelijk van het bestand, zijn meer selectie-opties beschikbaar in de [Quarantainemanager](#).

Verwijderen

Als deze optie is ingeschakeld, wordt het bestand verwijderd. Dit proces is veel sneller dan "overschrijven en verwijderen".

Overschrijven en verwijderen

Als deze optie is ingeschakeld, overschrijft de Scanner het bestand met een standaardpatroon en verwijdert het daarna. Het kan niet hersteld worden.

Hernoemen

Als deze optie is ingeschakeld, hernoemt de Scanner het bestand. Directe toegang tot deze bestanden (bijv. door dubbelklikken) is daarom niet meer mogelijk. Bestanden kunnen later worden gerepareerd en weer hun originele namen krijgen.

Negeren

Wanneer deze optie is ingeschakeld, is het bestand toegankelijk en blijft het bestand zoals het is.

Altijd negeren

Actie-optie voor Real-Time Protection-detecties: er wordt geen verdere actie ondernomen door Real-Time Protection. Toegang tot het bestand is toegestaan. Alle verdere toegang tot dit bestand is toegestaan en er worden geen extra mededelingen gegeven totdat de computer opnieuw opgestart is of het virusdefinitiebestand is geüpdatet.

Waarschuwing

As u de opties negeert of Altijd negeren selecteert, blijven de getroffen bestanden actief op uw computer! Het kan ernstige schade aan uw werkstation veroorzaken!

5.2.4 Speciale features wanneer geïnfecteerde bootsectors, rootkits en actieve malware wordt gedetecteerd

Actie-opties zijn beschikbaar om geïnfecteerde bootsectors te repareren wanneer die worden gedetecteerd:

Repareer 722 KB | 1,44 MB | 2,88 MB | 360 KB | 1,2 MB-bootsector

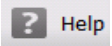
Deze opties zijn beschikbaar voor diskettestations.

Herstel-cd downloaden

Deze optie brengt u naar de Avira-website, waar u een speciale tool voor het detecteren en verwijderen van bootsectorvirussen kunt downloaden.

Als u acties uitvoert op draaiende processen, worden de betrokken processen beëindigd voordat de acties worden uitgevoerd.

5.2.5 Knoppen en links

Knop / Link	Beschrijving
Nu toepassen	De geselecteerde acties worden uitgevoerd om alle betrokken bestanden af te handelen.
Annuleren	De Scanner wordt afgesloten zonder verdere actie. De betrokken bestanden worden ongewijzigd op uw computersysteem achtergelaten.
 Help	Deze pagina van de onlinehelp wordt geopend via deze knop of link.

Waarschuwing

Voer de actie *Annuleren* alleen uit in uitzonderlijke gevallen. De getroffen bestanden blijven actief op uw werkstation nadat u annuleert! Het kan ernstige schade aan uw werkstation veroorzaken!

5.2.6 Speciale functies wanneer malware wordt gedetecteerd terwijl Web Protection inactief is

Als u Web Protection heeft uitgeschakeld, rapporteert de Scanner actieve malware die hij via een schuifvenster heeft gedetecteerd tijdens een systeemscan. Voordat u uw systeem repareert, kunt u een herstelpunt maken.

- ✓ Eerst moet u System Restore ingeschakeld hebben op uw Windows-systeem.
- ▶ Klik op **Details** in het schuifvenster.
 - Het scherm *Systeem wordt gescand* wordt weergegeven.
- ▶ Schakel **Maak systeemherstelpunt vóór reparatie** in.
- ▶ Klik op **Toepassen**.
 - Een systeemherstelpunt is gemaakt. Nu kunt u een systeemherstel uitvoeren via het Windows-configuratiescherm, mocht dat nodig zijn.

5.3 Bestanden versturen naar de Protection Cloud

Een lijst van bestandslocaties die vaak het doelwit van malware zijn, wordt gegenereerd als de taak **Snelle systeemscan** wordt uitgevoerd. De lijst bevat draaiende processen, programma's die draaien bij het opstarten, en services. Onbekende programmabestanden worden geüpload naar de Avira Protection Cloud voor analyse.

Als u de optie **Handmatige bevestiging bij het versturen van verdachte bestanden naar Avira** heeft ingeschakeld tijdens de installatie of later in de **Advanced Protection**-configuratie, ziet u de lijst van verdachte bestanden die verstuurd moeten worden naar de Protection Cloud, en kunt u kiezen welke bestanden u wilt versturen. Standaard worden alle verdachte bestanden geselecteerd die voor verdere analyse naar de Avira Protection Cloud worden gestuurd.

Let op

Als u de modus **Uitgebreide** rapportage heeft ingeschakeld, slaat de System Scanner elke detectie op in het Rapportbestand en voegt de *(Cloud)*-suffix toe aan de detecties die gemaakt zijn door de Protection Cloud.

5.3.1 Weergegeven informatie

De lijst van verdachte bestanden die naar Avira Protection Cloud verstuurd worden.

- *Versturen*: u kunt selecteren welke bestanden naar Avira Protection Cloud gestuurd worden.
- *Bestand*: de naam van het verdachte bestand.
- *Pad*: het pad naar het verdachte bestand.

Verzend bestanden altijd automatisch

Als deze optie ingeschakeld is, worden de verdachte bestanden naar de Protection Cloud gestuurd voor analyse na elke **Snelle systeemscan**, zonder te vragen naar handmatige bevestiging.

5.3.2 Knoppen en links

Knop / Link	Beschrijving
Verzenden	De geselecteerde bestanden worden verstuurd naar de Avira Protection Cloud.
Annuleren	De System Scanner wordt afgesloten zonder verdere actie. De verdachte bestanden worden onveranderd op uw computersysteem achtergelaten.
Help	Deze pagina van de onlinehelp wordt geopend.
Over Protection Cloud	De Protection Cloud-webpagina wordt geopend.

Gerelateerde onderwerpen:

- [Advanced Protection-configuratie](#)
- [Aangepaste installatie](#)
- [Rapport-configuratie](#)
- [Rapporten bekijken](#)

5.4 Real-Time Protection

Als virussen worden gedetecteerd door Real-Time Protection wordt toegang tot het bestand geweigerd en wordt er een bureaubladmededeling weergegeven, als u *interactieve* (zie de sectie Configuratie [Real-Time Protection > Scan > Actie bij detectie](#)).

Melding

De volgende informatie wordt weergegeven in de mededeling:

- Datum en tijd van de detectie
- Pad en naam van het getroffen bestand
- Naam van de malware

Let op

Als de standaard startmodus voor Real-Time Protection (Normale start) is gekozen en het aanmeldingsproces bij het opstarten wordt snel uitgevoerd, worden programma's die zijn geconfigureerd om automatisch te starten bij het opstarten, mogelijk niet gescand omdat ze wellicht al actief zijn voordat de Real-Time Protection volledig is gestart.

U heeft de volgende opties in interactieve modus:

Verwijderen

Het getroffen bestand wordt verplaatst naar de Scanner-component en verwijderd door de Scanner. Er verschijnt geen verder bericht.

Details

Het getroffen bestand wordt verplaatst naar de Scanner-component. De Scanner opent een scherm met een mededeling van de detectie en verschillende opties voor het behandelen van het getroffen bestand.

Let op

Graag notie nemen van de informatie over virusmanagement onder [Detectie > Scanner](#).

Let op

De actie *Quarantaine* is standaard voorgeselecteerd in de berichtgeving van de Scanner. Aanvullende acties kunnen worden geselecteerd via een contextmenu.

Sluiten

Het bericht wordt gesloten. Virusmanagement wordt afgesloten.

5.5 Verdacht gedrag

Als u het ProActiv-onderdeel van de Real-Time Protection activeert, worden applicatie-acties gecontroleerd en gescand op typisch verdacht gedrag van malware. U ontvangt een waarschuwing als verdacht gedrag wordt gedetecteerd in een toepassing. U heeft verschillende opties om de detectie af te handelen.

5.5.1 Waarschuwing van Real-Time Protection: Verdacht toepassingsgedrag gedetecteerd



5.5.2 Naam en pad van het momenteel gedetecteerde verdachte programma

De naam en het pad van de toepassing die verdachte acties uitvoert, worden weergegeven in het middelste scherm van het bericht.

5.5.3 Opties

Vertrouwd programma

Als deze optie is ingeschakeld, blijft de toepassing draaien. Het programma wordt toegevoegd aan de lijst van toegestane toepassingen en wordt uitgezonderd van controle door het ProActiv-onderdeel. Bij het toevoegen aan de lijst van toegestane toepassingen wordt het controletype ingesteld op *Inhoud*. Dit betekent dat de toepassing alleen uitgezonderd is van controle door het ProActiv-onderdeel als de inhoud onveranderd blijft (zie [Configuratie > Algemeen > Gevorderde protectie > Toepassingsfilter: Toegestane toepassingen](#)).

Programma eenmaal blokkeren

Als deze optie is geactiveerd, wordt de toepassing geblokkeerd, d.w.z. de toepassing wordt afgesloten. De acties van de toepassing worden verder gecontroleerd door het ProActiv-onderdeel.


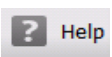
Dit programma altijd blokkeren

Als deze optie is geactiveerd, wordt de toepassing geblokkeerd, d.w.z. de toepassing wordt afgesloten. Het programma wordt toegevoegd aan de lijst van geblokkeerde toepassingen en kan niet langer draaien (zie [Configuratie > Algemeen > Gevorderde protectie > Toepassingsfilter: Geblokkeerde toepassingen](#)).

Negeren

Als deze optie is ingeschakeld, blijft de toepassing draaien. De acties van de toepassing worden verder gecontroleerd door het ProActiv-onderdeel.

5.5.4 Knoppen en links

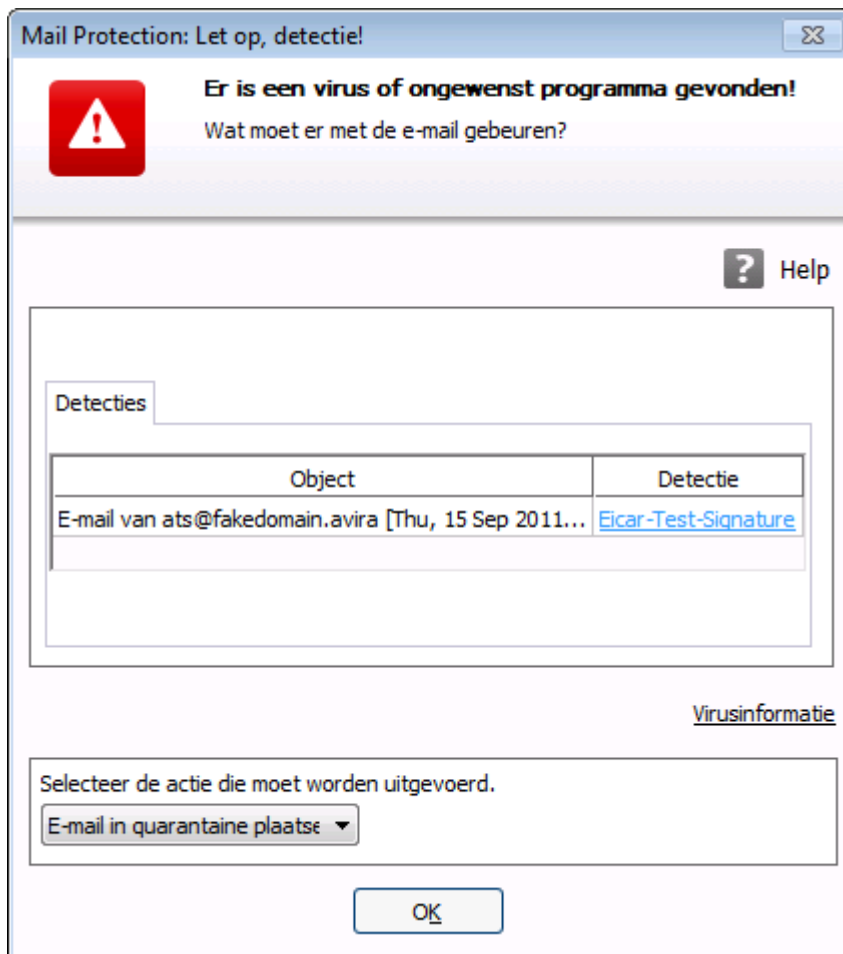
Knop / Link	Beschrijving
	Met deze link - en met een actieve internetverbinding - heeft u toegang tot een internetpagina met meer informatie over dit virus of ongewenste programma.
	Deze pagina van de onlinehelp wordt geopend via deze knop of link.

5.6 Inkomende e-mails

Als er een virus wordt gedetecteerd door Mail Protection krijgt u een waarschuwing als u de *interactieve* modus als de actiemodus voor het detecteren van een virus heeft geselecteerd (zie configuratiesectie [Mail Protection > Scan > Actie bij detectie](#)). In de interactieve modus kunt u kiezen wat u doet met de e-mail of de bijlage in het dialoogschermb.

U krijgt de waarschuwing die beneden wordt weergegeven als er een virus is gedetecteerd in een inkomende e-mail.

5.6.1 Waarschuwing



5.6.2 Detecties, Fouten, Waarschuwingen

Berichten en meer gedetailleerde informatie over de e-mails in kwestie worden weergegeven in de tabbladen **Detecties**, **Fouten** en **Waarschuwingen**:

- **Detecties:** Object: e-mail in kwestie, laat de naam van de afzender zien en de tijd waarop de e-mail werd verzonden.

Detectie: naam van het gedetecteerde virus of ongewenste programma

- **Fout:** berichten met fouten die zich voordeden tijdens de Mail Protection-scan.
- **Waarschuwingen:** waarschuwingen met betrekking tot de getroffen objecten.

5.6.3 Opties

Let op

Als een detectie een heuristische hit (HEUR/), een uitzonderlijke runtimepacker (PCK/) of een bestand met een verborgen bestandsextensie (HEUR-DBLEXT/) is, zijn alleen de opties [Naar quarantaine verplaatsen](#) en [Negeren](#) beschikbaar in de [interactieve modus](#). In de [automatische modus](#) wordt de detectie automatisch verplaatst naar [quarantaine](#).

.Deze beperking voorkomt dat de gedetecteerde bestanden, die misschien een vals alarm zijn, rechtstreeks van uw computer worden verwijderd. Het bestand kan op elk moment worden hersteld met behulp van de [Quarantainemanager](#).

Naar quarantaine verplaatsen

Als deze optie is ingeschakeld, wordt de e-mail inclusief alle bijlagen verplaatst naar [quarantaine](#). Deze kan later worden afgeleverd via de [quarantainemanager](#). De getroffen e-mail is verwijderd. De inhoud van de tekst en alle bijlages van de e-mail worden vervangen door een [standaardtekst](#).

E-mail verwijderen

Als deze optie is ingeschakeld, wordt de geïnfecteerde e-mail verwijderd wanneer er een virus of een ongewenst programma is gedetecteerd. De inhoud van de tekst en alle bijlages van de e-mail worden vervangen door een [standaardtekst](#).

Bijlage verwijderen

Wanneer deze optie is ingeschakeld, wordt de geïnfecteerde bijlage vervangen door een [standaardtekst](#). Als de inhoud van de e-mail geïnfecteerd is, wordt deze verwijderd en vervangen door een [standaardtekst](#). De e-mail zelf wordt afgeleverd.

Bijlage naar quarantaine verplaatsen

Wanneer deze optie is ingeschakeld, wordt de geïnfecteerde bijlage verplaatst naar [quarantaine](#) en vervolgens verwijderd (vervangen door een [standaardtekst](#)). De inhoud van de e-mail wordt afgeleverd. De geïnfecteerde bijlage kan later worden afgeleverd via de [quarantaine-manager](#).

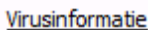
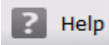
Negeren

Wanneer deze optie is ingeschakeld, wordt de geïnfecteerde e-mail afgeleverd, ondanks de detectie van een virus of een ongewenst programma.

Waarschuwing

Virussen en andere ongewenste programma's kunnen hierdoor uw computersysteem binnendringen. Selecteer de optie **Negeren** alleen in uitzonderlijke gevallen. Schakel de preview in uw e-mailprogramma uit; open nooit bijlages door dubbelklikken.

5.6.4 Knoppen en links

Knop / Link	Beschrijving
	Met deze link - en met een actieve internetverbinding - heeft u toegang tot een internetpagina met meer informatie over dit virus of ongewenste programma.
	Deze pagina van de online hulp wordt geopend via deze knop of link.

5.7 Uitgaande e-mails

Als er een virus wordt gedetecteerd door Mail Protection krijgt u een waarschuwing als u de *interactieve* modus als de actiemodus voor het detecteren van een virus heeft geselecteerd (zie configuratiesectie [Mail Protection > Scan > Actie bij detectie](#)). In de interactieve modus kunt u kiezen wat u doet met de e-mail of de bijlage in het dialoogscherf.

5.7.1 Waarschuwing



5.7.2 Detecties, Fouten, Waarschuwingen

Berichten en meer gedetailleerde informatie over de e-mails in kwestie worden weergegeven in de tabbladen **Detecties**, **Fouten** en **Waarschuwingen**:

- **Detecties:** Object: e-mail in kwestie, laat de naam van de afzender zien en de tijd waarop de e-mail werd verzonden.
Detectie: naam van het gedetecteerde virus of ongewenste programma
- **Fout:** berichten met fouten die zich voordeden tijdens de Mail Protection-scan.
- **Waarschuwingen:** waarschuwingen met betrekking tot de getroffen objecten.

5.7.3 Opties

E-mail in quarantaine plaatsen (niet verzenden)

Als deze optie actief is wordt de e-mail met alle bijlagen gekopieerd naar [Quarantaine](#) en niet verzonden. De e-mail blijft in de outbox van uw e-mailclient. U ontvangt een foutmelding in uw e-mailprogramma. Alle andere e-mails die worden verzonden vanaf uw account worden gecontroleerd op malware.

Blokkeer het versturen van e-mails (niet verzenden)

De e-mail wordt niet verzonden en blijft in de outbox van uw e-mailprogramma. U ontvangt een foutmelding in uw e-mailprogramma. Alle andere e-mails die worden verzonden vanaf uw account worden gecontroleerd op malware.

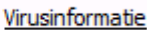
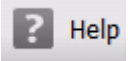
Negeren

Als deze optie is ingeschakeld, wordt de geïnfecteerde e-mail verzonden ondanks de detectie van een virus of ongewenst programma.

Waarschuwing

Virussen en ongewenste programma's kunnen zo het computersysteem van de e-mailontvanger binnendringen..

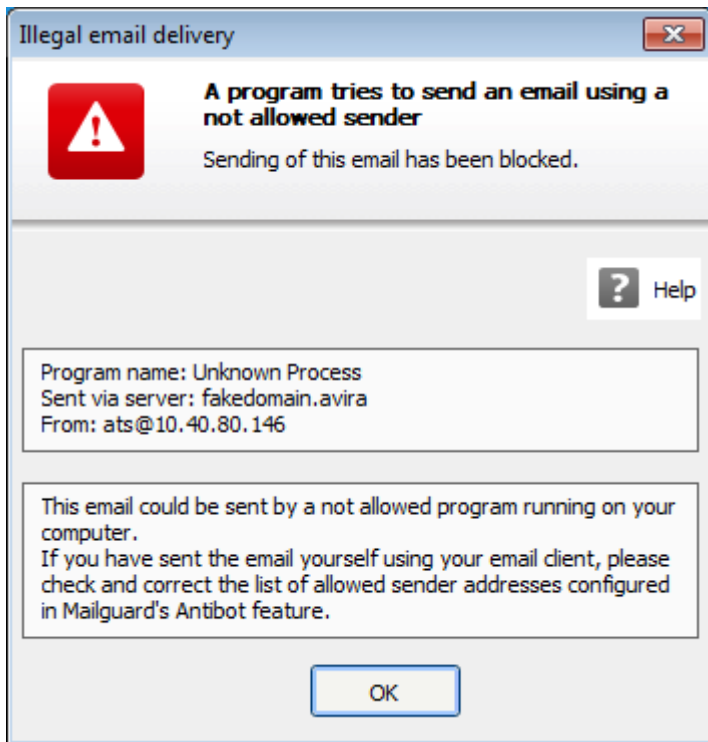
5.7.4 Knoppen en links

Knop / Link	Beschrijving
	Met deze link - en met een actieve internetverbinding - heeft u toegang tot een internetpagina met meer informatie over dit virus of ongewenste programma.
	Deze pagina van de onlinehelp wordt geopend via deze knop of link.

5.8 Afzender

As u de AntiBot-functie van Mail Protection gebruikt, worden e-mails van ongeautoriseerde afzenders geblokkeerd door Mail Protection. De afzender wordt gecontroleerd aan de hand van de lijst van toegestane afzenders die u gemaakt heeft in de configuratie onder [Mail Protection > Scan > AntiBot](#). De geblokkeerde e-mail wordt weergegeven in een dialoogschermb.

5.8.1 Waarschuwing



5.8.2 Gebruikt programma, gebruikte SMTP-server en het adres van de afzender van de e-mail

De volgende informatie wordt weergegeven in het middelste venster van het bericht:

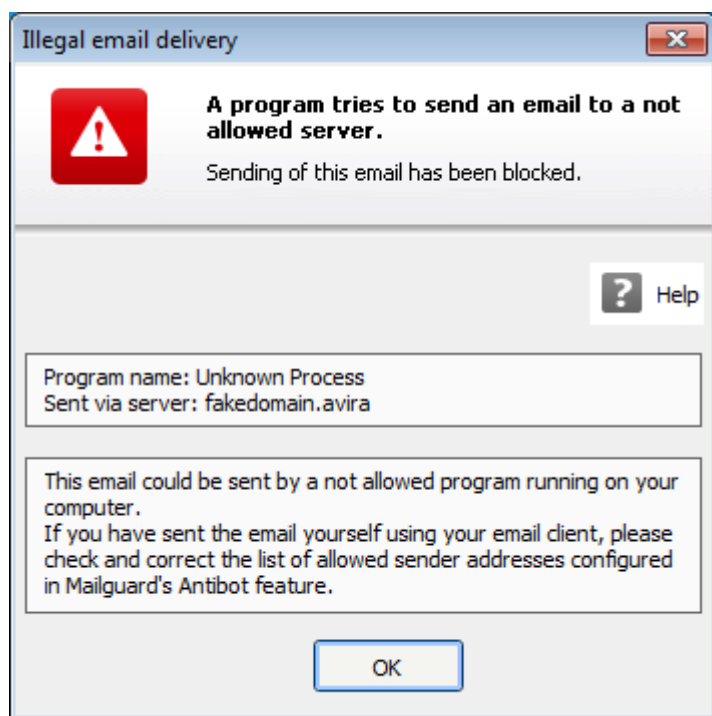
- Naam van het programma dat gebruikt is om de e-mail te versturen.
- Naam van de SMTP-server die gebruikt is om de e-mail te versturen
- Adres van de afzender van de e-mail

Als u de e-mail in kwestie verstuurt met uw eigen e-mailprogramma, vergelijk dan de lijst van toegestane afzenders in de configuratie onder [Mail Protection > Scan > AntiBot](#) met de adressen van afzenders die u gebruikt in de e-mailaccounts van uw e-mailprogramma. Als de lijst van toegestane afzenders incompleet is in de configuratie, voeg dan de andere afzenderadressen die u gebruikt, toe aan de lijst. U vindt de geblokkeerde e-mail in de outbox van uw e-mailprogramma. Om de geblokkeerde e-mail te versturen, rondt u de configuratie af en verstuurt u de e-mail opnieuw.

5.9 Server

As u de AntiBot-functie van Mail Protection gebruikt, worden e-mails die zijn verzonden door ongeautoriseerde SMTP-servers geblokkeerd door Mail Protection. Controleren welke SMTP-server werd gebruikt, vindt plaats op basis van de lijst van toegestane servers die u heeft toegevoegd aan de configuratie onder [Mail Protection > Scan > AntiBot](#). De geblokkeerde e-mail wordt weergegeven in een dialoogscherm.

5.9.1 Waarschuwing



5.9.2 Gebruikt programma, gebruikte SMTP-server

De volgende informatie wordt weergegeven in het middelste venster van het bericht:

- Naam van het programma dat gebruikt is om de e-mail te versturen.
- Naam van de SMTP-server die gebruikt is om de e-mail te versturen.

Als u de e-mail in kwestie verstuurt met uw eigen e-mailprogramma, vergelijk dan de lijst van toegestane afzenders in de configuratie onder [Mail Protection > Scan > AntiBot](#) met de SMTP-servers die u gebruikt om e-mails te versturen. U kunt de SMTP-servers die gebruikt worden in uw e-mailprogramma vinden onder de gebruikte e-mailaccounts. Als de lijst van geautoriseerde servers incompleet is in de configuratie, voeg dan de andere SMTP-servers die u gebruikt, toe aan de lijst. U vindt de geblokkeerde e-mail in de outbox van uw e-mailprogramma. Om de geblokkeerde e-mail te versturen, rondt u de configuratie af en verstuurt u de e-mail opnieuw.

5.10 Web Protection

Als virussen worden gedetecteerd door Web Protection, ontvangt u een waarschuwing als u de *interactieve* (zie de configuratiesectie [Web Protection > Scan > Actie bij detectie](#)). In de interactieve modus kunt u in het dialoogvenster kiezen wat er gedaan moet worden met de door de webserver verzonden gegevens.

Waarschuwing



Detectie, Fouten, Waarschuwingen

Berichten en gedetailleerde informatie over de gedetecteerde virussen worden weergegeven in de tabbladen **Detectie**, **Fouten** en **Waarschuwingen**:

- **Detectie:** URL en de naam van het gedetecteerde virus of ongewenste programma
- **Fout:** berichten over fouten die voorkwamen tijdens de Web Protection-scan
- **Waarschuwingen:** waarschuwingen met betrekking tot de virussen die zijn gedetecteerd

Mogelijke acties

Let op

Als een detectie een heuristische hit (HEUR/), een uitzonderlijke runtimepacker (PCK/) of een bestand met een verborgen bestandsextensie (HEUR-DBLEXT/) is, zijn alleen de opties [Naar quarantaine verplaatsen](#) en [Negeren](#) beschikbaar in de [interactieve modus](#).

Deze beperking voorkomt dat de gedetecteerde bestanden, die misschien een

vals alarm zijn, rechtstreeks van uw computer worden verwijderd. Het bestand kan op elk moment worden hersteld met behulp van de [Quarantainemanager](#).

Toegang weigeren

De door de webserver opgevraagde website en/of willekeurige gegevens of bestanden die worden verplaatst, worden niet naar uw webbrowser verstuurd. Een foutmelding om u te informeren dat de toegang is geweigerd, wordt weergegeven in de webbrowser. Web Protection slaat de detectie op in het rapportbestand als de rapportfunctie is ingeschakeld.

In quarantaine plaatsen

Als er een virus of malware wordt gedetecteerd, worden de door de webserver opgevraagde website en/of de overgedragen gegevens en bestanden in quarantaine geplaatst. Het geïnfecteerde bestand kan worden teruggehaald uit de quarantainemanager wanneer het een informatieve waarde heeft of - indien nodig - worden gestuurd naar het Avira Malware Research Center.

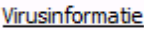
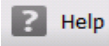
Negeren

De door de webserver opgevraagde website en/of willekeurige gegevens of bestanden die werden verplaatst, worden door Web Protection doorgestuurd naar uw webbrowser.

Waarschuwing

Virussen en andere ongewenste programma's kunnen hierdoor uw computersysteem binnendringen. Selecteer de **Negeren**-optie alleen in uitzonderlijke gevallen.

Knoppen en links

Knop / Link	Beschrijving
	Met deze link - en met een actieve internetverbinding - heeft u toegang tot een internetpagina met meer informatie over dit virus of ongewenste programma.
	Deze pagina van de onlinehelp wordt geopend via deze knop of link.

6. Scanner

6.1 Scanner

Met de component Scanner kunt u doelgericht scans (scans op aanvraag) op virussen en ongewenste programma's uitvoeren. De volgende opties zijn beschikbaar voor het scannen op geïnfecteerde bestanden:

- **Systemscan via contextmenu**

De systemscan via het contextmenu (rechter muisknop - toegang tot **Geselecteerde bestanden scannen met Avira**) wordt aanbevolen als u bijvoorbeeld afzonderlijke bestanden en mappen wilt scannen. Een ander voordeel is dat het niet nodig is om eerst het [Control Center](#) te starten voor een systemscan via het contextmenu.

- **Systemscan via slepen en neerzetten**

Wanneer een bestand of map in het programmavenster van het [Control Center](#) wordt geslept, scant de Scanner het bestand of de map en alle submappen die de map bevat. Deze procedure wordt aanbevolen als u afzonderlijke bestanden en mappen wilt scannen die u heeft opgeslagen, bijvoorbeeld op uw bureaublad.

- **Systemscan via profielen**

Deze procedure wordt aanbevolen wanneer u regelmatig bepaalde mappen en drives wilt scannen (bijv. uw werkmap of drives waarop u regelmatig nieuwe bestanden opslaat). U hoeft dan niet opnieuw deze mappen en drives te selecteren voor elke nieuwe scan, u selecteert alleen het betreffende profiel.

- **Systemscan via de Planner**

Met de Planner kunt u tijdgestuurde scans uitvoeren.

Speciale processen zijn nodig bij het scannen op rootkits, bootsectorvirussen en bij het scannen van actieve processen. De volgende opties zijn beschikbaar:

- Scannen op rootkits via het scanprofiel **Scannen op rootkits en actieve malware**
- Actieve processen scannen via het scanprofiel **Actieve processen**
- Scannen op bootsectorvirussen via de menu-opdracht **Bootrecords-scan ...** in het menu **Extra's**

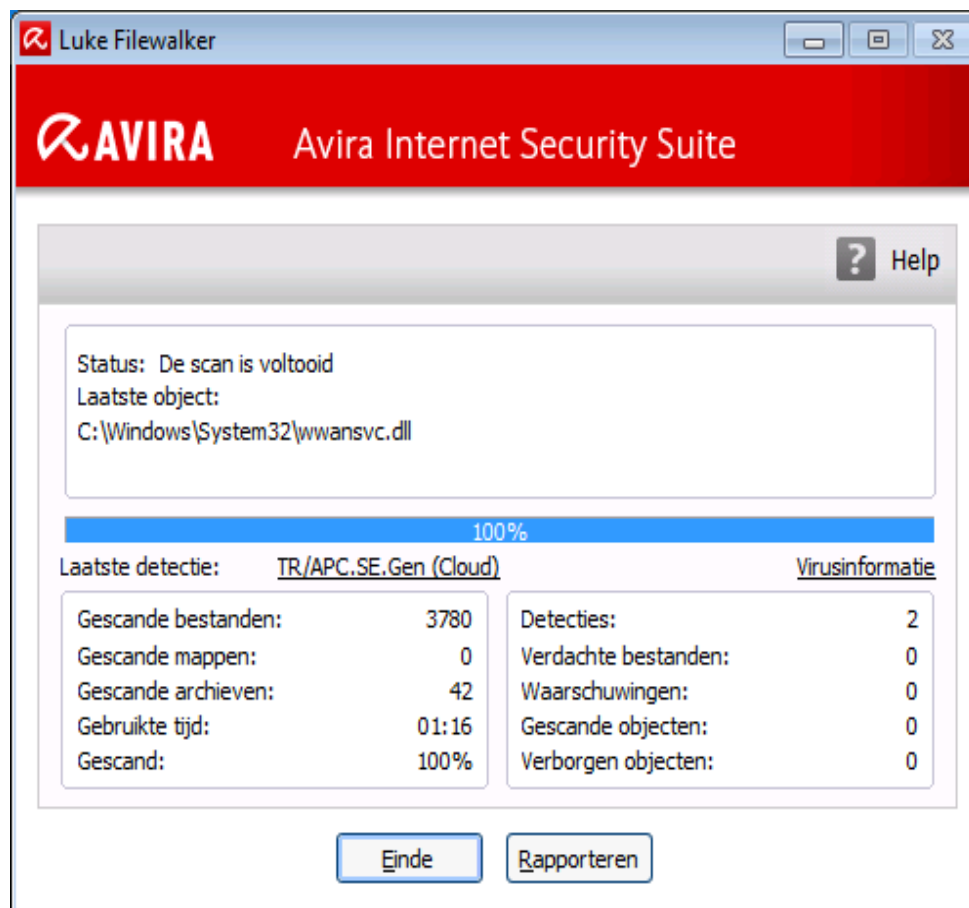
6.2 Luke Filewalker

Tijdens een systemscan verschijnt het statusvenster **Luke Filewalker**, dat u voorziet van exacte informatie over de status van de scan.

Als de optie **interactief** is geselecteerd in de configuratie van de [System Scanner](#) in de groep **Actie bij detectie**, wordt u gevraagd wat er moeten worden gedaan met een gedetecteerd virus of ongewenst programma. Wanneer de optie **automatisch** is geselecteerd, worden alle detecties weergegeven in het [Scanrapport](#).

Wanneer de scan is voltooid, worden de resultaten (statistieken), waarschuwingen en foutmeldingen weergegeven in een nieuw dialoogvenster.

6.2.1 Luke Filewalker: scanstatus-venster



Weergegeven informatie

Status: er zijn verschillende statusberichten:

- *Het programma wordt geïnitieerd*
- *Er wordt gezocht naar verborgen objecten!*
- *De gestarte processen worden gescand*
- *Bestand wordt gescand*
- *Archief initialiseren*
- *Beschikbaar geheugen*
- *Het bestand wordt uitgepakt*
- *Opstartsectoren worden gescand*
- *Hoofd-opstartsectoren worden gescand*
- *Register wordt gescand*

- *Het programma wordt beëindigd!*
- *De scan is voltooid*

Laatste object: naam en het pad van het bestand dat momenteel wordt gescand of dat het laatst is gescand

Laatste detectie: er zijn verschillende berichten voor de laatste detectie:

- *Geen detectie!*
- Naam van het laatst gedetecteerde virus of ongewenste programma

Gescande bestanden: aantal gescande bestanden

Gescande mappen: aantal gescande mappen

Gescande archieven: aantal gescande archieven

Gebruikte tijd: duur van de systeemsan

Gescand: percentage van reeds voltooide scans

Detecties: aantal gedetecteerde virussen of ongewenste programma's

Verdachte bestanden: aantal door de heuristiek gerapporteerde bestanden

Waarschuwingen: aantal alarmen in verband met gedetecteerde virussen


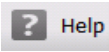
Gescande objecten: aantal gescande objecten tijdens de rootkits-scan

Verborgene objecten: totaal aantal gedetecteerde verborgen objecten

Let op

Rootkits hebben de mogelijkheid processen en objecten te verbergen, zoals registervermeldingen of bestanden. Niet elk verborgen object is echter noodzakelijkerwijs het bewijs van de aanwezigheid van een rootkit. Verborgene objecten kunnen ook onschadelijk objecten zijn. Wanneer een scan een verborgen object detecteert maar geen viruswaarschuwingalarm geeft, moet u het rapport gebruiken om te bepalen aan welk object wordt gerefereerd en dient u meer informatie over het gedetecteerde object te verkrijgen.

Knoppen en links

Knop / Link	Beschrijving
	Met deze link - en met een actieve internetverbinding - heeft u toegang tot een internetpagina met meer informatie over dit virus of ongewenste programma.
	Deze pagina van de onlinehelp wordt geopend via deze knop of link.
Stoppen	Het scanproces wordt gestopt.
Pauze	De scan wordt onderbroken en kan worden voortgezet door te klikken op de knop Hervatten .
Hervatten	De onderbroken scan wordt voortgezet.
Beëindigen	De System Scanner wordt gesloten.

Rapporteren	Het rapportbestand van de scan wordt getoond.
--------------------	---

6.2.2 Luke Filewalker: Scanstatistieken



Weergegeven informatie: Statistieken

Bestanden: aantal gescande bestanden

Mappen: aantal gescande mappen

Archieven: aantal gescande archieven

Waarschuwingen: aantal alarmen in verband met gedetecteerde virussen

Doorzochte objecten: aantal gescande objecten tijdens de rootkits-scan

Verborgene objecten: aantal gedetecteerde verborgene objecten (rootkits)

Detecties: aantal gedetecteerde virussen of ongewenste programma's

Verdacht: aantal door de heuristiek gerapporteerde bestanden

Gerepareerd: aantal gerepareerde bestanden

Geëlimineerd: aantal overschreven bestanden

Verwijderd: aantal verwijderde bestanden

Verplaatst: aantal bestanden dat naar quarantaine is verplaatst

Knoppen en links

Knop / Link	Beschrijving
	Deze pagina van de onlinehelp wordt geopend via deze knop of link.
Sluiten	Het samenvattingvenster wordt gesloten.
Rapporteren	Het rapportbestand van de scan wordt getoond.

7. Control Center

7.1 Control Center Overzicht

Het Control Center is een informatie-, configuratie- en managementcentrum. Behalve de [secties](#) die individueel geselecteerd kunnen worden, biedt het ook een groot aantal opties waarvoor u toegang krijgt vanuit de [menubalk](#).

Menubalk

Alle functies van het Control Center vindt u in de menubalk.

Bestand

- [Afsluiten](#) (Alt + F4)

Weergave

- [Status](#)
- Pc-bescherming
 - [Scanner](#)
 - [Real-Time Protection](#)
- Internetbescherming
 - [FireWall](#)
 - [Web Protection](#)
 - [Mail Protection](#)
- Bescherming van mobiele apparatuur
 - [Avira Free Android Security](#)
- Beheer
 - [Quarantaine](#)
 - [Planner](#)
 - [Rapporten](#)
 - [Gebeurtenissen](#)
- [Opnieuw laden](#) (F5)

Extra's

- [Scan bootrecords...](#)
- [Detectielijst...](#)
- [Herstel-cd downloaden](#)

- [Configuratie \(F8\)](#)

Update

- [Start update...](#)
- [Handmatige update...](#)

Help

- [Topics](#)
- [Leesmij](#)
- [Help mij](#)
- [Live ondersteuning](#)
- [Forum](#)
- [Handleiding downloaden](#)
- [Licentiebeheer](#)
- [Product aanbevelen](#)
- [Feedback versturen](#)
- [Over Avira Internet Security Suite](#)

Let op

U kunt de toetsenbordnavigatie in de menubalk activeren met behulp van de [ALT]-toets. Wanneer de navigatie is geactiveerd, kunt u door het menu lopen met de pijltjestoetsen. Met de Enter-toets activeert u het actieve menu-item.

Navigatiesecties

In de navigatiebalk aan de linkerkant vindt u de volgende secties:

- **Status**

PC-BESCHERMING

- [Scanner](#)
- [Real-Time Protection](#)

INTERNETBESCHERMING

- [FireWall](#)
- [Web Protection](#)
- [Mail Protection](#)

BESCHERMING VAN MOBIELE APPARATUUR

- [Avira Free Android Security](#)

BEHEER

- [Quarantaine](#)
- [Planner](#)
- [Rapporten](#)
- [Gebeurtenissen](#)

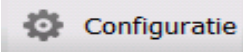
Navigatiebeschrijving

- **Status:** door te klikken op de **Status**-balk krijgt u een overzicht van de functionaliteit en de prestaties van het product (zie [Status](#)).
 - De **Status**-sectie toont u in een oogopslag welke modules actief zijn en geeft informatie over de laatst uitgevoerde update.
- **PC-BESCHERMING:** in deze sectie vindt u de componenten voor het controleren van de bestanden op virussen en malware op uw computersysteem.
 - De sectie [Scanner](#) stelt u in staat om op eenvoudige wijze een scan op aanvraag te configureren en te starten. [Vooraf gedefinieerde profielen](#) maken een scan mogelijk met reeds aangepaste standaardopties. Op dezelfde manier is het mogelijk om de scan op virussen en ongewenste programma's aan te passen aan uw persoonlijke wensen met behulp van [handmatige selectie](#) (wordt opgeslagen) of door het aanmaken van [gebruikergedefinieerde profielen](#).
 - De sectie [Real-Time Protection](#) toont [informatie over gescande bestanden](#), evenals andere [statistische gegevens](#), die op elk moment [gereset](#) kunnen worden, en geeft toegang tot het [rapportagebestand](#). Uitgebreidere [informatie](#) over het laatst gedetecteerde virus of ongewenste programma kan praktisch worden verkregen "met een druk op de knop".
- **INTERNETBESCHERMING:** in deze sectie vindt u de componenten voor het beschermen van uw computersysteem tegen virussen en malware vanaf het internet en tegen onbevoegde toegang tot het netwerk.
 - Met de [FireWall](#)-sectie kunt u de basisinstellingen configureren voor de FireWall. Afgezien daarvan worden de huidige gegevensoverdrachtssnelheid en alle actieve toepassingen die een netwerkverbinding gebruiken, weergegeven.
 - De sectie [Web Protection](#) toont [informatie over gescande URL's en gedetecteerde virussen](#), evenals andere statistische gegevens, die op elk moment [gereset](#) kunnen worden, en geeft toegang tot het [rapportbestand](#). Uitgebreidere [informatie](#) over het laatst gedetecteerde virus of ongewenste programma kan praktisch worden verkregen "met een druk op de knop".
 - De sectie [Mail Protection](#) toont u alle e-mails die gescand zijn door Mail Protection, hun eigenschappen en andere statistische gegevens. U kunt ook e-mailadressen uitsluiten van toekomstige scannen op malware of spam. E-mails kunnen ook worden verwijderd uit de Mail Protection-buffer.
- **BESCHERMING VAN MOBIELE APPARATUUR.** Vanuit deze sectie wordt u doorgeleid naar de onlinetoegang voor Android-apparaten.

- [Avira Free Android Security](#) beheert al uw op Android gebaseerde apparaten.
- **BEHEER**: in deze sectie vindt u tools voor het isoleren en beheren van verdachte of geïnfekteerde bestanden en voor het plannen van terugkerende taken.
 - De [Quarantaine](#)-sectie bevat de zogenaamde quarantainemanager. Dit is het centrale punt voor bestanden die al in quarantaine zijn geplaatst of voor verdachte bestanden die u in quarantaine wilt plaatsen. Het is ook mogelijk om een geselecteerd bestand per e-mail te verzenden naar het Avira Malware Research Center.
 - Met de [Planner](#)-sectie kunt u geplande scans, updates en backups configureren en bestaande taken aanpassen of verwijderen.
 - Met de [Rapporten](#)-sectie kunt u de resultaten van uitgevoerde acties bekijken.
 - De [Gebeurtenissen](#)-sectie stelt u in staat gebeurtenissen te bekijken die door bepaalde programma-modules zijn gegenereerd.

Knoppen en links

De volgende knoppen en links kunnen beschikbaar zijn.

Knop / link	Snelkoppeling	Beschrijving
		Deze knop of link wordt gebruikt voor toegang tot het overeenkomstige configuratiedialoogvenster voor de sectie.
	F1	Deze knop of link opent het overeenkomstige onlinehelp-onderwerp voor de sectie.

7.2 Bestand

7.2.1 Afsluiten

Het menu-onderdeel **Afsluiten** in het menu **Bestand** sluit het Control Center.

7.3 Weergave

7.3.1 Status

Met het startscherm van het Control Center, de sectie **Status**, kunt u in één blik zien of uw computersysteem wordt beschermd en welke Avira-modulen actief zijn. Het venster **Status** biedt ook informatie over de laatst uitgevoerde update. U kunt ook zien of u een geldige licentie bezit.

- **Pc-bescherming:** [Real-Time Protection](#), [Laatste scan](#), [Laatste update](#), [Uw product is geactiveerd](#)
- **Internetbescherming:** [Web Protection](#), [Mail Protection](#), [FireWall](#), [Spelmodus](#),

Let op

De gebruikersaccountcontrole (UAC) zal u toestemming vragen voor het in- of uitschakelen van de services Real-Time Protection, Web Protection en Mail Protection in besturingssystemen vanaf Windows Vista.

PC-bescherming

In deze sectie wordt informatie weergegeven over de huidige status van de service en beschermingsfuncties die uw computer lokaal tegen virussen en malware van het internet beschermen.


Real-Time Protection


In dit veld wordt informatie over de huidige status van de Real-Time Protection weergegeven.


U kunt de Real-Time Protection in- of uitschakelen door op de knop **AAN/UIT** te klikken. Voor de Real-Time Protection kunnen meer opties worden geopend door in de navigatiebalk op **Real-Time Protection** te klikken. U krijgt eerst informatie over de status van de laatst gevonden malware en geïnfecteerde bestanden. Klik op **Configuratie** om meer instellingen te definiëren.

- **Configuratie:** Ga naar Configuratie om de instellingen voor de Real-Time Protection-componenten te definiëren.

De volgende mogelijkheden zijn beschikbaar:

Icoon	Status	Optie	Beschrijving
	<i>Geactiveerd</i>	Deactiveren	<p>De Real-Time Protection-service is actief, d.w.z. uw systeem wordt continu op virussen en ongewenste programma's gecontroleerd.</p> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p>Let op U kunt de Real-Time Protection-service uitschakelen. Houd er echter rekening mee dat als Real-Time Protection is uitgeschakeld, u niet langer tegen virussen en ongewenste programma's bent beschermd. Alle bestanden kunnen ongemerkt door het systeem passeren en mogelijk schade veroorzaken.</p> </div>

	<p><i>Gedeactiveerd</i></p>	<p>Activeren</p>	<p>De Real-Time Protection-service is uitgeschakeld, d.w.z. de service is geladen maar niet actief.</p> <div data-bbox="1107 414 1399 1099" style="background-color: #cccccc; padding: 10px;"> <p>Waarschuwing Er wordt geen scan uitgevoerd op virussen en ongewenste programma's. Alle bestanden kunnen ongemerkt het systeem passeren. U bent niet beschermd tegen virussen en ongewenste programma's.</p> </div> <div data-bbox="1107 1137 1399 1715" style="background-color: #cccccc; padding: 10px;"> <p>Let op Om opnieuw tegen virussen en ongewenste programma's te worden beschermd, dient u op de knop AAN/UIT te klikken naast Real-Time Protection in de sectie <i>PC-bescherming</i>.</p> </div>
---	-----------------------------	-------------------------	---

	<p><i>Service gestopt</i></p>	<p>Service starten</p>	<p>De Real-Time Protection-service is gestopt.</p> <div data-bbox="1107 338 1399 1025" style="background-color: #e0e0e0; padding: 10px;"> <p>Waarschuwing Er wordt geen scan uitgevoerd op virussen en ongewenste programma's. Alle bestanden kunnen ongemerkt het systeem passeren. U bent niet beschermd tegen virussen en ongewenste programma's.</p> </div> <div data-bbox="1107 1066 1399 1899" style="background-color: #e0e0e0; padding: 10px;"> <p>Let op Om opnieuw tegen virussen en ongewenste programma's te worden beschermd, dient u op de knop AAN/UIT te klikken naast Real-Time Protection in de sectie <i>PC-bescherming</i>. De huidige status moet in de kleur groen worden weergegeven. Dit betekent Geactiveerd.</p> </div>
---	-------------------------------	-------------------------------	--

	<i>Onbekend</i>	Help	Deze status wordt weergegeven als zich een onbekende fout voordoet. Neem in dit geval contact op met onze Ondersteuning .
--	-----------------	-------------	---

Laatste scan

In dit veld wordt informatie weergegeven over de laatst uitgevoerde systeemscan. Als een volledige systeemcontrole wordt uitgevoerd, worden alle vaste schijven op uw computer grondig gescand. Alle scanprocessen, met uitzondering van de integriteitscontroles van systeembestanden, worden uitgevoerd: standaardscan van bestanden, controle van het register en bootsectors, scan voor rootkits, enz.

De volgende details worden weergegeven:

- Datum van laatste volledige systeemscan

De volgende mogelijkheden zijn beschikbaar:

Systemscan	Optie	Beschrijving
<i>Niet uitgevoerd</i>	Systeem scannen	<p>Sinds de installatie is geen volledige systeemcontrole uitgevoerd.</p> <div style="background-color: #cccccc; padding: 10px; margin: 10px 0;"> <p>Waarschuwing De status van het systeem is ongecontroleerd. Er bestaat een mogelijkheid dat er op uw computer virussen of ongewenste programma's worden gevonden.</p> </div> <div style="background-color: #cccccc; padding: 10px; margin: 10px 0;"> <p>Let op Klik op de koppeling Systeem scannen om uw computer te controleren.</p> </div>
Datum van laatste systeemscan, bijv. <i>18-9-2011</i>	Systeem scannen	<p>U hebt op de aangegeven datum een volledige systeemscan uitgevoerd.</p> <div style="background-color: #cccccc; padding: 10px; margin: 10px 0;"> <p>Let op Wij raden u aan de standaard scantaak <i>Volledige systeemscan</i> te gebruiken. Gebruik de Planner om de taak Volledige systeemscan uit te voeren.</p> </div>
<i>Onbekend</i>	Help	<p>Deze status wordt weergegeven als zich een onbekende fout voordoet. Neem in dit geval contact op met onze Ondersteuning.</p>


Laatste update


Hier wordt informatie over de status van de laatst uitgevoerde update weergegeven.


De volgende details worden weergegeven:

- Datum van de laatste update
 - ▶ Klik op de knop **Configuratie openen** om meer instellingen voor automatische updates te definiëren.

De volgende mogelijkheden zijn beschikbaar:

Icoon	Status	Optie	Beschrijving
	<i>Datum van laatste update, bijv. 18-7-2011</i>	Start update	<p>Het programma is gedurende de afgelopen 24 uur bijgewerkt.</p> <div data-bbox="1058 506 1267 1010" style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p>Let op U kunt uw Avira-product via de knop Update starten tot de nieuwste versie bijwerken.</p> </div>

	<p><i>Datum van laatste update, bijv. 18-7-2011</i></p>	<p>Start update</p>	<p>Sinds de update zijn al 24 uur voorbij gegaan, maar u bent nog steeds binnen de herinneringscyclus voor updates die u hebt gekozen. Dit is afhankelijk van de instelling in de configuratie.</p> <div data-bbox="1058 674 1267 1173" style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p>Let op U kunt uw Avira-product via de knop Update starten tot de nieuwste versie bijwerken.</p> </div>
---	---	----------------------------	---



	<p><i>Niet uitgevoerd</i></p>	<p>Start update</p>	<p>Sinds de installatie is geen update uitgevoerd</p> <p>-of-</p> <p>De door u gekozen herinneringscyclus voor updates is verlopen (zie Configuratie) en er zijn geen updates uitgevoerd</p> <p>-of-</p> <p>het bestand met virusdefinities is ouder dan de herinneringscyclus voor updates die u hebt geselecteerd (zie Configuratie).</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Let op U kunt uw Avira-product via de knop Update starten tot de nieuwste versie bijwerken.</p> </div>
		<p>Niet beschikbaar</p>	<p>Als de licentie is verlopen, kunnen geen updates worden uitgevoerd.</p>

Uw product is geactiveerd




In dit veld wordt informatie over de huidige status van uw licentie weergegeven.

De volgende mogelijkheden zijn beschikbaar:

Volledige versie

Icoon	Status	Optie	Betekenis
	<i>Geldigheidsdatum van de huidige licentie voor een volledige versie, bijv. 31-10-2011</i>	Vernieuwen	U hebt een geldige licentie voor uw Avira-product. U kunt via de knop Verlengen naar de online Avira-shop gaan. Daar hebt u de mogelijkheid om uw huidige licentie aan uw behoeften aan te passen en een upgrade uit te voeren naar Avira Premium.
	<i>Geldigheidsdatum van de huidige licentie voor een volledige versie, bijv. 31-10-2011</i>	Vernieuwen	U hebt een geldige licentie voor uw Avira-product. De licentieperiode is echter dertig of minder dagen. Gebruik de knop Verlengen om naar de online Avira-shop te gaan. Daar hebt u de optie om de huidige licentie te verlengen.
	<i>De licentie is verlopen op: bijv. 31-8-2011</i>	Kopen	Uw licentie voor uw Avira-product is verlopen. Gebruik de knop Kopen om naar de online Avira-shop te gaan. Daar hebt u de optie om een geldige licentie te kopen. <div style="background-color: #cccccc; padding: 10px; border: 1px solid #000;"> <p>Waarschuwing Als uw licentie is verlopen, zijn er geen updates meer mogelijk. De beschermingsfuncties van het programma zijn gedeactiveerd en kunnen niet meer worden geactiveerd.</p> </div>

Evaluatielicentie

Icoon	Status	Optie	Betekenis
	<i>Geldigheidsdatum van de evaluatielicentie, bijv. 31-10-2011</i>	Kopen	U hebt een evaluatielicentie waarmee u gedurende een bepaalde tijdsperiode de volledige reeks functies van uw Avira-product kunt testen. Gebruik de knop Kopen om naar de online Avira-shop te gaan. Daar hebt u de optie om een geldige licentie te kopen.
	<i>Geldigheidsdatum van de evaluatielicentie, bijv. 31-10-2011</i>	Vernieuwen	U hebt een evaluatielicentie. De licentieperiode is echter dertig of minder dagen. Gebruik de knop Verlengen om naar de online Avira-shop te gaan. Daar hebt u de optie om een geldige licentie te kopen.
	<i>De evaluatielicentie is verlopen op: 31-10-2011</i>	Kopen	Uw licentie voor uw Avira-product is verlopen. Gebruik de knop Kopen om naar de online Avira-shop te gaan. Daar hebt u de optie om een geldige licentie te kopen. <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Waarschuwing Als uw licentie is verlopen, zijn er geen updates meer mogelijk. De beschermingsfuncties van het programma zijn gedeactiveerd en kunnen niet meer worden geactiveerd.</p> </div>

Internetbescherming

In deze sectie wordt informatie weergegeven over de huidige status van de service die uw computer tegen virussen en malware van het internet beschermen.



- **FireWall:** deze service controleert de communicatiekanalen van en naar uw computer.


- **Web Protection:** deze service controleert de gegevens die in uw webbrowser werden overgedragen en geladen terwijl u op het internet aan het surfen bent (controle van poorten 80, 8080, 3128).
- **Mail Protection:** deze service controleert e-mails en hun bijlagen op virussen en malware.
- **Spelmodus:** wanneer op automatisch ingesteld, schakelt uw Avira-product voor elke toepassing die in volledig scherm actief is, automatisch over naar de [Spelmodus](#).

Andere opties voor deze processen kunnen vanuit een contextmenu worden geopend door op het configuratieicoon te klikken naast de knop **AAN/UIT**.

- **Configureren:** ga naar Configuratie om voor het procesonderdeel instellingen te definiëren.

De volgende mogelijkheden zijn beschikbaar: *Services*

Icoon	Status	Processtatus	Optie	Betekenis
	OK	<i>Geactiveerd</i>	Deactiveren	<p>Alle services voor Internetbescherming zijn actief.</p> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p>Let op U kunt een service deactiveren door op de knop AAN/UIT te klikken. Let er echter op dat u, zodra een service is gedeactiveerd, niet meer volledig bent beschermd tegen virussen en malware.</p> </div>
	<i>Beperkt</i>	<i>Gedeactiveerd</i>	Activeren	<p>Een service is gedeactiveerd, d.w.z. de service is gestart maar is niet actief.</p> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p>Waarschuwing Uw computersysteem wordt niet volledig gecontroleerd. Er bestaat een mogelijkheid dat virussen en ongewenste programma's uw computersysteem binnen kunnen komen.</p> </div> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc; margin-top: 10px;"> <p>Let op Om de service te activeren, klikt u op de knop AAN/UIT.</p> </div>

	<i>Waarschuwing</i>	<i>Service gestopt</i>	Service starten	Er is een service gestopt <div style="background-color: #cccccc; padding: 10px;"> <p>Waarschuwing Uw computersysteem wordt niet volledig gecontroleerd. Er bestaat een mogelijkheid dat virussen en ongewenste programma's uw computersysteem binnen kunnen komen.</p> </div> <div style="background-color: #cccccc; padding: 10px; margin-top: 10px;"> <p>Let op Klik op de knop AAN/UIT om de service te starten zodat uw computersysteem wordt gecontroleerd. De service is gestart en geactiveerd.</p> </div>
		<i>Onbekend</i>	Help	Deze status wordt weergegeven als zich een onbekende fout voordoet. Neem in dit geval contact op met onze Ondersteuning .

7.3.2 Spelmodus

Als een toepassing wordt uitgevoerd in full-screenmodus op uw computersysteem, dan kunt u opzettelijk bureaubladmededelingen in de vorm van pop-upvensters en in-productboodschappen annuleren door de Spelmodus te activeren.

U kunt de Spelmodus in werking stellen of hem in de de automatische modus houden door op de **AAN/UIT**-knop te klikken. Standaard is de Spelmodus ingesteld op **automatisch** en

deze wordt weergegeven in groen. De standaardinstellingen staan ingesteld op automatisch, zodat, elke keer wanneer u een toepassing draait die de full-screenmodus vereist, uw Avira-product automatisch naar Spelmodus wisselt.

- ▶ Klik op de knop aan de linkerkant naast de **UIT**-knop om de Spelmodus te activeren.
 - De Spelmodus is ingesteld en wordt weergegeven in geel.

Let op

Wij bevelen u aan om de standaardinstelling **UIT** met haar automatische full-screenmoduserkenning alleen tijdelijk te wijzigen omdat u geen zichtbare bureaubladmededelingen en waarschuwingen over netwerkgebeurtenissen en mogelijke bedreigingen, ontvangt.

7.3.3 Scanner

Met de sectie **Scanner** kunt u gemakkelijk configureren en een systeemscan starten. [Vooraf gedefinieerde profielen](#) maken een systeemscan met al aangepaste standaardopties mogelijk. Op dezelfde wijze is het met behulp van [handmatige selectie](#) of via het maken van [gebruikergedefinieerde profielen](#), mogelijk de systeemscan voor virussen en ongewenste programma's aan te passen op uw persoonlijke vereisten. De vereiste handeling kan via het icoon in de [toolbar](#), via [snelkoppeling](#) of via het [contextmenu](#) worden geselecteerd. Start een systeemscan via het item [Scan starten met het geselecteerde profiel](#).

De weergave en hantering van de bewerkbare profielen komt overeen met die van Windows Explorer. Elke map in de hoofdmap komt met één profiel overeen. Mappen of bestanden die gescand moeten worden, worden geselecteerd of kunnen met een vinkje voor de map of het bestand voor een scan worden geselecteerd.

- Om mappen te veranderen, dubbelklikt u op de gewenste map.
- Om stations te veranderen, dubbelklikt u op de letter van het gewenste station.
- Om mappen en stations te selecteren, kunt u in het vak voor de map of het stationsicoon klikken of via het [contextmenu](#) selecteren.
- U kunt met behulp van de schuifbalk en de schuifpijlen door de menustructuur navigeren.

Vooraf gedefinieerde profielen

Indien nodig, zijn vooraf gedefinieerde scanprofielen beschikbaar.

Let op

Deze profielen zijn alleen-lezen en kunnen niet worden gewijzigd of verwijderd. Om een profiel op uw vereisten aan te passen, selecteert u een eenmalige [scan](#) de map [Handmatig kiezen](#) of [Nieuw profiel maken](#) om een [gebruikergedefinieerd profiel](#) te maken die kunnen worden opgeslagen.

Let op

De scanopties voor de vooraf gedefinieerde profielen kunnen worden ingesteld in [Configuratie > Scanner > Scan > Bestanden](#). U kunt deze instellingen op uw vereisten aanpassen.

Lokale stations

Alle lokale stations op uw systeem worden op virussen en ongewenste programma's gescand.

Lokale vaste schijven

Alle lokale vaste schijven op uw systeem worden op virussen of ongewenste programma's gescand.

Verwijderbare stations

Alle beschikbare, verwijderbare stations van uw systeem worden op virussen of ongewenste programma's gescand.

Windows-systeemmap

De Windows-systeemmap van uw systeem wordt op virussen of ongewenste programma's gescand.

Volledige systeemsan

Alle lokale vaste schijven op uw computer worden op virussen of ongewenste programma's gescand. Tijdens de scan worden, met uitzondering van de integriteitscontrole van systeembestanden, alle scanprocessen ingezet: standaardscan van bestanden, scan van register en bootsectors, scan voor rootkits, enz. (zie [Scanner > Overzicht](#)). De scanprocessen worden, ongeacht de instellingen van de scanner in de configuratie onder [Scanner > Scannen: Overige instellingen](#), uitgevoerd.

Snelle systeemsan

De belangrijkste mappen van uw systeem (de mappen *Windows*, *Programma's*, *Documenten en Instellingen\Lokale gebruiker*, *Documenten en Instellingen\Alle gebruikers*) worden op virussen en ongewenste programma's gescand.

Mijn documenten

De standaardlocatie van "*Mijn documenten*" van de aangemelde gebruiker wordt op virussen en ongewenste programma's gescand.

Let op

Onder Windows is "*Mijn documenten*" een map in het profiel van de gebruiker die voor documenten die zijn opgeslagen als standaardlocatie wordt gebruikt.

De standaardinstelling voor de map is *C:\Documenten en Instellingen\gebruikersnaam\Mijn documenten*.

Actieve processen

Alle huidige processen worden op virussen of ongewenste programma's gescand.

Scan op rootkits en actieve malware

De computer wordt op rootkits en actieve (werkzame) malwareprogramma's gescand. Alle actieve processen worden gecontroleerd.

Let op

In de [interactieve modus](#) kunt u op verschillende manieren op een detectie reageren. In de [automatische modus](#) wordt de detectie in het rapportbestand opgenomen.

Let op

De scan op rootkits is niet beschikbaar voor Windows XP 64 bit !

7.3.4 Handmatig kiezen

Selecteer deze map als u de scan op uw individuele vereisten wilt aanpassen. Markeer de vereiste mappen en bestanden die moeten worden gescand.

Let op



Het profiel **Handmatig kiezen** wordt gebruikt om gegevens te sannen zonder eerst een nieuw profiel aan te maken.

Gebruikergedefinieerde profielen

Een nieuw profiel kan via de [toolbar](#), via [snelkoppeling](#) of via het [contextmenu](#) worden gemaakt.

Nieuwe profielen kunnen onder de door u gewenste naam worden opgeslagen en zijn naast de [handmatig beheerde scan](#) nuttig om met behulp van de [Planner](#) geplande scans te maken.

Toolbar en snelkoppelingen

Icoon	Snelkoppeling	Beschrijving
	F3	Scan starten met het geselecteerde profiel Het geselecteerde profiel wordt op virussen of ongewenste programma's gescand.
	F6	Scan starten met het geselecteerde icoon als administrator Het geselecteerde profiel wordt met administrator-rechten gescand
	Ins	Nieuw profiel maken Er wordt een nieuw profiel gemaakt.
	F2	Geselecteerd profiel hernoemen Voor het geselecteerde profiel wordt een nieuwe naam opgeslagen.
	F4	Bureaubladkoppeling maken voor het geselecteerde profiel Op het bureaublad wordt een koppeling naar het geselecteerde profiel gemaakt.
	Del	Geselecteerd profiel verwijderen Het geselecteerde profiel wordt onherstelbaar verwijderd.

Contextmenu

Voor deze sectie kan het contextmenu worden verkregen door met de muis een vereist profiel te selecteren en de rechtermuisknop ingedrukt te houden.

Scan starten

Het geselecteerde profiel wordt op virussen of ongewenste programma's gescand.

Scan starten (admin)

(Deze functie is alleen beschikbaar vanaf Windows Vista. Om deze handeling uit te voeren, worden administrator-rechten vereist.)

Het geselecteerde profiel wordt op virussen of ongewenste programma's gescand.

Nieuw profiel maken

Er wordt een nieuw profiel gemaakt. Selecteer de te scannen mappen en bestanden.

Profiel hernoemen

Geeft het geselecteerde profiel een door u gekozen naam.

Let op

Deze invoering kan niet in het contextmenu worden geselecteerd als een [vooraf gedefinieerd profiel](#) is geselecteerd.

Profiel verwijderen

Het geselecteerde profiel wordt onherstelbaar verwijderd.

Let op

Deze invoering kan niet in het contextmenu worden geselecteerd als een [vooraf gedefinieerd profiel](#) is geselecteerd.

Bestandsfilter

Standaard:

Betekent dat de bestanden volgens de instelling in de groep [Bestanden](#) van Configuratie worden gescand. U kunt deze [instelling](#) in Configuratie op uw vereisten aanpassen. U kunt via de knop of koppeling [Configuratie](#) naar Configuratie gaan.

Alle bestanden scannen:

Alle bestanden worden gescand, ongeacht de instelling in [Configuratie](#).

Gebruikergedefinieerd:

Er wordt een dialoogvenster geopend waarin alle bestandsextensies worden weergegeven die worden gescand. Voor de extensies worden standaardinvoeringen gedefinieerd. De invoeringen kunnen echter worden toegevoegd of verwijderd.

Let op

Deze invoering kan alleen in het contextmenu worden geselecteerd als de muis op een keuzevak is geplaatst.
De optie is niet beschikbaar bij [vooraf gedefinieerde profielen](#).

Selecteren

Met submappen:

Alles wordt in het geselecteerde knooppunt gescand (zwart vinkje).

Zonder submappen:

Alleen de bestanden in het geselecteerde knooppunt worden gescand (groen vinkje).

Alleen submappen:

Alleen de submappen in het geselecteerde knooppunt worden gescand en niet de bestanden die in het knooppunt zijn (grijs vinkje, submappen hebben een zwart vinkje).

Geen selectie:

De selectie is geannuleerd, het huidig geselecteerde knooppunt wordt niet gescand (geen vinkje).

Let op

Deze invoering kan alleen in het contextmenu worden geselecteerd als de muis op een keuzevak is geplaatst.

De optie is niet beschikbaar bij [vooraf gedefinieerde profielen](#).

Bureaubladkoppeling maken

Maakt op het bureaublad een koppeling naar het geselecteerde profiel.

Let op

Deze invoering kan niet in het contextmenu worden geselecteerd als het profiel [Handmatig kiezen](#) is geselecteerd. De instellingen van [Handmatig kiezen](#) worden namelijk niet permanent opgeslagen.

7.3.5 Real-Time Protection

De sectie **Real-Time Protection** geeft [informatie over gescande bestanden](#) weer, en ook andere [statistische gegevens](#), die op elk moment [gereset](#) kunnen worden, en verleent toegang tot het [rapportbestand](#). Uitgebreidere [informatie](#) over het laatst gedetecteerde virus of ongewenste programma kan praktisch worden verkregen "met een druk op de knop".

Let op

Als de [Real-Time Protection-service](#) niet is gestart, wordt de knop naast de module weergegeven in de kleur geel. Het [rapportbestand](#) van de Real-Time Protection kan echter wel worden weergegeven.

Toolbar

Icoon	Beschrijving
	<p>Rapportbestand weergeven</p> <p>Het rapportbestand van de Real-Time Protection wordt weergegeven.</p>
	<p>Statistische gegevens resetten</p> <p>De statistische informatie in deze sectie wordt ingesteld op nul.</p>

Weergegeven informatie

Laatste gevonden bestand

Geeft de naam en de locatie van het laatste door de Real-Time Protection gevonden bestand weer.

Het laatst gevonden virus of ongewenste programma

Toont de naam van het laatst gevonden virus of ongewenste programma.

Icoon/Link	Beschrijving
 Virusinformatie	<p>Klik op het icoon of de koppeling om gedetailleerde informatie weer te geven over het virus of het ongewenste programma als een internetverbinding aanwezig is.</p>

Laatste gescande bestand

Geeft de naam en de locatie van het laatste door de Real-Time Protection gescande bestand weer.

Statistieken

Aantal bestanden

Geeft het aantal tot nu toe gescande bestanden weer.

Aantal detecties

Toont het aantal virussen en ongewenste programma's dat tot nu toe is gevonden.

Aantal verdachte bestanden

Toont het aantal bestanden gerapporteerd door de heuristieken.

Aantal verwijderde bestanden

Toont het aantal verwijderde bestanden tot nu toe.

Aantal gerepareerde bestanden

Toont het aantal gerepareerde bestanden tot nu toe.

Aantal verplaatste bestanden

Toont het aantal verplaatste bestanden tot nu toe.

Aantal hernoemde bestanden

Toont het aantal hernoemde bestanden tot nu toe.

7.3.6 FireWall

Windows Firewall (Windows 7 of hoger)


Vanaf Windows 7 bevat Avira Internet Security Suite niet langer de Avira FireWall. In plaats daarvan beheert Avira de Windows Firewall vanuit het Control en Configuratie Center.

De FireWall-sectie stelt u in staat om de status van de Windows Firewall te controleren en de aanbevolen instellingen te herstellen door op de knop **Probleem oplossen** te klikken.

7.3.7 Web Protection

De sectie **Web Protection** toont [informatie over gescande URL's](#), evenals andere [statistische gegevens](#) die op elk moment kunnen worden [gereset](#), en maakt toegang mogelijk tot het [rapportbestand](#). Meer gedetailleerde [informatie](#) over het laatste virus of ongewenst programma die werd gedetecteerd, kunnen praktisch door "een druk op de knop" worden verkregen.

Werkbalk

Pictogram	Beschrijving
	<p>Rapportbestand tonen</p> <p>Het rapportbestand van de Web Protection wordt weergegeven.</p>
	<p>Statistische gegevens resetten</p> <p>De statistische informatie in deze sectie wordt op nul ingesteld.</p>

Weergegeven informatie

Laatste gerapporteerde URL

Geeft de laatste URL weer die door Web Protection is gedetecteerd.

Laatst gedetecteerde virus of ongewenst programma

Geeft de naam van het laatst gevonden virus of ongewenste programma.

Pictogram/koppeling	Beschrijving
 Virusinformatie	Klik op het pictogram of de koppeling om gedetailleerde informatie weer te geven over het virus of het ongewenste programma als een internetverbinding aanwezig is.

Laatst gescande URL

Toont de naam en het pad van de laatste URL die door Web Protection werd gecontroleerd.

Statistieken

Aantal URL's

Toont het aantal URL's dat tot op dit punt is gecontroleerd.

Aantal detecties

Toont het aantal virussen en ongewenste programma's dat tot nu toe is gevonden.

Aantal geblokkeerde URL's

Toont het aantal eerder geblokkeerde URL's.

Aantal genegeerde URL's

Toont het aantal eerder genegeerde URL's.

7.3.8 Mail Protection

De sectie **Mail Protection** toont u alle e-mails die gescand zijn door Mail Protection, hun eigenschappen en andere statistische gegevens.

Let op


Als de [Mail Protection-service](#) niet is gestart, wordt de knop naast de module weergegeven in de kleur geel. Het [rapportbestand](#) van de Mail Protection kan echter wel worden weergegeven. Als de module niet beschikbaar is in uw Avira-product, zijn de vakken van dit onderdeel grijs gemaakt en kunnen niet geselecteerd worden.

Let op

Uitsluiting van individuele e-mailadressen van de malware-scan geldt logischerwijs alleen voor binnenkomende e-mails. Om het scannen van uitgaande e-mails uit te schakelen, deactiveert u de scan in de configuratie onder [Mail Protection > Scan](#).



Werkbalk

Icoon	Beschrijving
	<p>Rapportbestand weergeven</p> <p>Het rapportbestand van de Mail Protection wordt weergegeven.</p>
	<p>Geef de eigenschappen van de geselecteerde e-mail weer</p> <p>Opent een dialoogscherf met meer informatie over de geselecteerde e-mail.</p>
	<p>E-mailadres niet op malware scannen</p> <p>Het geselecteerde e-mailadres wordt in de toekomst niet langer gescand op virussen en ongewenste programma's. U kunt deze instelling ongedaan maken in de configuratie bij Mail Protection > Algemeen > Uitzonderingen.</p>
	<p>Geselecteerde e-mail(s) verwijderen</p> <p>De geselecteerde e-mail wordt verwijderd uit de cache. De e-mail blijft echter wel in uw e-mailprogramma.</p>

	<p>Statistische gegevens resetten</p> <p>De statistische informatie in deze sectie wordt ingesteld op 0.</p>
---	---

Gescande e-mails:

Dit gebied toont de door Mail Protection gescande e-mails.

Icoon	Beschrijving
	Er is geen virus of ongewenst programma gevonden.
	Er is een virus of ongewenst programma gevonden.

Type:

Toont het protocol dat gebruikt is om de e-mail te versturen of te ontvangen:

- POP 3: e-mail ontvangen via POP 3
- IMAP: e-mail ontvangen via IMAP
- SMTP: e-mail verstuurd via SMTP

Van/Naar

Geeft het e-mailadres van de afzender weer.

Onderwerp:

Toont het onderwerp van de ontvangen e-mail.

Datum/tijd:

Geeft aan wanneer de e-mail gescand is op spam.

Let op

U kunt meer informatie over de e-mail krijgen door te dubbelklikken op de relevante e-mail.

Statistieken

E-mailactie

Geeft de uitgevoerde actie weer als Mail Protection een virus of een ongewenst programma in een e-mail vindt. In [interactieve modus](#) is hier geen weergave beschikbaar, omdat u zelf kunt selecteren welke procedure gevolgd moet worden in het geval van een detectie.

Let op

U kunt deze [instelling](#) aanpassen aan uw eisen in de Configuratie. U kunt Configuratie openen met de knop of link [Configuratie](#).

Getroffen bijlagen

Toont de uitgevoerde actie wanneer Mail Protection een virus of een ongewenst programma in een e-mail vindt. In [interactieve modus](#) is hier geen weergave beschikbaar, omdat u zelf kunt selecteren welke procedure gevolgd moet worden in het geval van een detectie.

Let op

U kunt deze [instelling](#) aanpassen aan uw eisen in de Configuratie. U kunt Configuratie openen met de knop of link [Configuratie](#).

Aantal e-mails

Toont het aantal e-mails dat gescand is door Mail Protection.

Laatste detectie

Toont de naam van het laatst gevonden virus of ongewenste programma.

Aantal detecties

Geeft het aantal virussen en ongewenste programma's weer dat eerder gedetecteerd en gerapporteerd is.

Verdachte e-mails

Toont het aantal e-mails dat gerapporteerd is door de heuristieken.

Aantal inkomende e-mails

Geeft het aantal ontvangen e-mails weer.

Aantal uitgaande e-mails

Geeft het aantal verzonden e-mails weer.

7.3.9 Avira Free Android Security

Avira Free Android Security-app is niet alleen gericht op antidiefstalmaatregelen die u helpen om uw mobieltje terug te krijgen als u niet meer weet waar u het gelaten heeft, of erger nog, als het gestolen is. Deze toepassing maakt het mogelijk om binnenkomende gesprekken en sms'en te blokkeren. Avira Free Android Security beschermt mobiele telefoons en smartphones die draaien onder het Android-besturingssysteem.

Avira Free Android Security bestaat uit twee componenten:

- De toepassing zelf, geïnstalleerd op uw Android-apparatuur
- De Avira Android Web Console voor registratie en featurecontrole

Avira Free Android Security is een gratis app waarvoor u geen licentie nodig heeft. Alle prominente merken worden ondersteund door Avira Free Android Security, zoals Samsung, HTC, LG en Motorola.

Meer informatie kunt u vinden op onze website:

<http://www.avira.com/android>



7.3.10 Quarantaine




De **Quarantainemanager** beheert aangetaste objecten (bestanden en e-mails). Uw Avira-product kan aangetaste objecten in een speciaal formaat naar de quarantainemap verplaatsen. Zij kunnen niet worden uitgevoerd of geopend.





Let op

Om objecten naar de Quarantainemanager te verplaatsen, selecteert u in **Configuratie** onder **System Scanner** en **Real-Time Protection** en **Mail Protection - Scannen > Actie bij detectie** de relevante optie terwijl u in **automatische modus** werkt. Als alternatief kunt u de relevante quarantaine-optie in de **interactieve modus** selecteren.

Toolbar, snelkoppelingen en contextmenu

Icoon	Snelkoppeling	Beschrijving
	F2	<p>Object(en) opnieuw scannen</p> <p>Een geselecteerd object wordt opnieuw op virussen en ongewenste programma's gescand. De instellingen van de scan op verzoek worden hiervoor gebruikt.</p>
	Terug	<p>Eigenschappen</p> <p>Opent een dialoogvenster met meer gedetailleerde informatie over het geselecteerde object.</p> <div style="background-color: #e0e0e0; padding: 10px; margin-top: 10px;"> <p>Let op U kunt gedetailleerde informatie ook verkrijgen door op een object dubbel te klikken.</p> </div>

  (Windows Vista)	F3	<p>Object(en) herstellen</p> <p>Een geselecteerd object wordt hersteld. Daarna wordt het object in de oorspronkelijke locatie geplaatst.</p> <div style="background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p>Let op Deze optie is niet beschikbaar voor objecten van het type e-mail.</p> </div> <div style="background-color: #d0d0d0; padding: 5px; margin: 10px 0;"> <p>Waarschuwing Enorme schade aan het systeem wegens virussen en ongewenste programma's! Als u bestanden herstelt, dient u er zeker van te zijn dat alleen bestanden worden hersteld die door een andere scan konden worden schoongemaakt.</p> </div> <div style="background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p>Opmerking Sinds Windows Vista moet u administrator-rechten hebben om objecten te herstellen.</p> </div>
	F6	<p>Object(en) herstellen naar...</p> <p>Een geselecteerd object kan naar een door u gedefinieerde locatie worden hersteld. Als u deze optie selecteert, gaat het dialoogvenster "Opslaan als" open, waarin u de opslaglocatie kunt selecteren.</p> <div style="background-color: #d0d0d0; padding: 5px; margin: 10px 0;"> <p>Waarschuwing Enorme schade aan het systeem wegens virussen en ongewenste programma's! Als u bestanden herstelt, dient u er zeker van te zijn dat alleen bestanden worden hersteld die door een andere scan konden worden schoongemaakt.</p> </div>

	Ins	<p>Bestand aan quarantaine toevoegen</p> <p>Als u een bestand als verdacht beschouwt, kunt u dit via deze optie handmatig aan de quarantainemanager toevoegen. Indien van toepassing, uploadt u het bestand met de optie Object verzenden voor onderzoek naar een webserver van het Avira Malware Research Center.</p>
	F4	<p>Object(en) verzenden</p> <p>Het object wordt voor onderzoek door het Avira Malware Research Center naar een webserver van het Avira Malware Research Center geüpload. Als u op de knop Object verzenden klikt, gaat een dialoogvenster open dat een formulier bevat waarin u uw contactgegevens kunt invoeren. Voer alle vereiste gegevens in. Selecteer een type: Verdacht bestand of Fout positief. Klik op OK om het verdachte bestand te uploaden.</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Let op De omvang van de bestanden die u uploadt, is begrensd tot 20 MB niet-gecomprimeerd of 8 MB gecomprimeerd.</p> <p>Let op U kunt per keer maar één bestand uploaden.</p> </div>
	Del	<p>Object(en) verwijderen</p> <p>Een geselecteerd object wordt uit de quarantainemanager verwijderd. Het object kan niet worden hersteld.</p>
		<p>Object(en) kopiëren naar</p> <p>Het gemarkeerde object in quarantaine wordt naar de geselecteerde map opgeslagen.</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Let op Het in quarantaine geplaatste object is niet identiek aan het herstelde bestand. Het object in quarantaine is gecodeerd en kan niet in de oorspronkelijke indeling worden uitgevoerd of gelezen.</p> </div>

	F7	<p>Alle eigenschappen exporteren</p> <p>De eigenschappen van het gemarkeerde object in quarantaine worden in een tekstbestand geëxporteerd.</p>
	F10	<p>Quarantainemap openen</p> <p>Opent de map GEÏNFECTEERD.</p>




Let op

U hebt de optie om op meerdere gemarkeerde objecten acties uit te voeren. Om meerdere objecten (objecten in kolommen) te markeren, houdt u de Ctrl-toets of Shift-toets ingedrukt terwijl u in de quarantainemanager objecten selecteert. Druk op **Ctrl + A** om alle weergegeven objecten te selecteren. Tijdens het uitvoeren van de handeling **Eigenschappen weergeven** kunnen er geen meerdere objecten worden geselecteerd. Met de handeling **Object verzenden** zijn meervoudige selecties niet mogelijk omdat per keer maar één bestand kan worden geüpload.

Tabel

Status

Een object dat in quarantaine is geplaatst, kan verschillende statussen hebben:

Icoon	Beschrijving
	Er is geen virus of ongewenst programma gevonden, het object is "schoon".
	Er is een virus of ongewenst programma gevonden.
	Als met de optie Bestand toevoegen een verdacht bestand aan de quarantainemanager is toegevoegd, heeft het dit waarschuwingsicoon.

Type

Bestemming	Beschrijving
E-mail	Het object is als een e-mail gedetecteerd.
Bestand	Het object is als een bestand gedetecteerd.

Detectie

Toont de naam van de gevonden malware.
Heuristische vondsten worden met de afkorting HEUR/ geïdentificeerd.

Bron

Toont het pad waaronder het object is gevonden.

Datum/Tijd

Toont de datum en tijd van de detectie.

Gedetailleerde informatie**Bestandsnaam**

Volledig pad en bestandsnaam van het object.

Object in quarantaine

Bestandsnaam van het object in quarantaine.

Hersteld

JA/NEE

JA: het geselecteerde object is hersteld.

NEE: het geselecteerde object is niet hersteld.

Geüpload naar Avira

JA/NEE

JA: het object is al naar een Avira Malware Research Center webserver van Avira Malware Research Center geüpload voor onderzoek.

NEE: het object is nog niet naar een Avira Malware Research Center webserver van Avira Malware Research Center geüpload voor onderzoek.

Besturingssysteem

Windows XP: de malware is geïdentificeerd door een Avira-desktopproduct.

Scan-engine

Versienummer van scan-engine

Virusdefinitiebestand

Versienummer van het virusdefinitiebestand

Detectie

Naam van de gedetecteerde malware.

Datum/Tijd

Datum en tijd van de detectie





7.3.11 Planner

De **Planner** geeft u de optie geplande scan- en update-taken te maken en bestaande taken aan te passen of te verwijderen.

De volgende taak wordt standaard na installatie gemaakt:

- Scantaak **Snelle systeemscan** (standaard ingeschakeld): een wekelijkse snelle systeemscan wordt automatisch uitgevoerd. Tijdens de snelle systeemscan worden op uw computer alleen belangrijke bestanden en mappen op virussen of ongewenste programma's gescand. U kunt de taak **Snelle systeemscan** wijzigen, maar wij raden aan om andere scantaken te maken die beter uw behoeften weergeven.



Werkbalk, snelkoppelingen en contextmenu

Pictogram	Snelkoppeling	Beschrijving
	Ins	Nieuwe taak invoegen Maakt een nieuwe taak aan. Een wizard leidt u duidelijk door de benodigde instellingen.
	Return	Eigenschappen Opent een dialoogvenster met meer informatie over de geselecteerde taak.
	F2	Taak bewerken Opent de wizard om een taak te maken en te wijzigen.
	Del	Taak verwijderen Verwijdert de geselecteerde taken uit de lijst.

		Rapportbestand weergeven Het rapportbestand van de Planner wordt weergegeven.
	F3	Taak starten Start een gemarkeerde taak uit de lijst.
	F4	Taak stoppen Stopt een gestarte en gemarkeerde taak.

Tabel

Type taak

Pictogram	Beschrijving
	De taak is een update-taak.
	De taak is een scantaaak.

Naam

Naam van de taak.

Actie

Geeft aan of de taak een **scan** of een **update** is.

Frequentie

Geeft aan hoe vaak en wanneer een taak wordt gestart.

Weergavemodus

De volgende weergavemodi zijn beschikbaar:

Onzichtbaar: de taak wordt op de achtergrond uitgevoerd maar is niet zichtbaar. Dit is van toepassing op scantaken en update-taken.

Minimaliseren: het taakvenster wordt alleen in een voortgangsbalk weergegeven.

Maximaliseren: het taakvenster is volledig zichtbaar.

Ingeschakeld

De taak wordt geactiveerd als u het keuzevakje inschakelt.

Let op

als de frequentie van de taak op onmiddellijk is ingesteld, start de taak zodra hij wordt geactiveerd. Dit geeft u de mogelijkheid de taak te herstarten als dit nodig is.

Status

Geeft de status van de taak weer:

Gereed: de taak is gereed voor uitvoering.

Actief: de taak is gestart en wordt uitgevoerd.

Taken met de Planner maken

De wizard Planning ondersteunt u bij het plannen, configureren en aanmaken van

- een getimedede scan voor virussen en ongewenste programma's
- een getimedede update via het internet

Voor beide taaktypes moet u het volgende invoeren:

- de naam en beschrijving van de taak
- wanneer de taak moet worden gestart
- hoe vaak de taak moet worden uitgevoerd
- de weergavemodus van de taak

Frequentie van de taak

Frequentie van de taak	Beschrijving
Onmiddellijk	De taak wordt onmiddellijk na beëindiging van de wizard Planning gestart.
Dagelijks	De taak wordt dagelijks op een bepaalde tijd gestart, bijv. 22:00.

Wekelijks	De taak wordt wekelijks op een bepaalde dag of op diverse weekdays op een bepaalde tijd gestart, bijv. dinsdag en vrijdag om 16:26.
Interval	De taak wordt op specifieke intervallen uitgevoerd, bijv. elke 24 uur.
Eenmalig	De taak wordt één keer op een gedefinieerd tijdstip uitgevoerd, bijv. op 04-10-04 om 10:04.
Aanmelding	De taak wordt bij elke aanmelding van een Windows-gebruiker uitgevoerd.

Starttijd van de taak

U kunt voor de starttijd van de taak een weekday, datum, tijdstip of interval definiëren. Dit wordt niet weergegeven als u als starttijd **Onmiddellijk** hebt ingevoerd.

Afhankelijk van het taaktype zijn er diverse aanvullende opties

Ook taak starten bij verbinding met internet (inbellen)

Afgezien van de gedefinieerde frequentie wordt de taak ook uitgevoerd als een internetverbinding wordt ingesteld.

Deze optie kan met een update-taak worden geselecteerd die dagelijks, wekelijks of op andere intervallen wordt uitgevoerd.

Taak herhalen als de tijd al is verlopen

Taken uit het verleden die niet op het vereiste tijdstip konden worden uitgevoerd, bijv. omdat de computer was uitgeschakeld.

Deze optie kan zowel bij een update- als een scantaak worden geselecteerd als deze dagelijks, wekelijks, op intervallen of één keer wordt uitgevoerd.

Computer uitschakelen als de taak is voltooid

De computer wordt uitgeschakeld als de taak is voltooid. Scantaken kunnen geminimaliseerd of gemaximaliseerd worden weergegeven.

Let op

Bij een scantaak is het mogelijk om [vooraf gedefinieerde profielen](#) en [door gebruikers gedefinieerde profielen](#) te selecteren in het dialoogvenster **Selectie van het profiel**. Het profiel [Handmatig kiezen](#) wordt altijd met de huidige selectie uitgevoerd.

7.3.12 Rapporten



Met de sectie **Rapporten** kunt u de resultaten openen van acties die door het programma zijn uitgevoerd.



Werkbalk, snelkoppelingen en contextmenu

Pictogram	Snelkoppeling	Beschrijving
	Return	Rapport weergeven Opent een venster waarin de resultaten van de geselecteerde handeling worden weergegeven. Bijvoorbeeld de resultaten van een scan .
	F3	Rapportbestand weergeven Geeft het rapportbestand van het geselecteerde rapport weer.
	F4	Rapportbestand afdrukken Opent het dialoogvenster Afdrukken van Windows om het rapportbestand af te drukken.
	Del	Rapport(en) verwijderen Verwijdert het geselecteerde rapport en het relevante rapportbestand.

Tabel

Status

Pictogram	Beschrijving
	Actie scan: succesvol voltooid zonder een virus te detecteren.
	Actie scan: virus gedetecteerd of niet succesvol voltooid.

	Actie update: succesvol voltooid.
	Actie update: niet succesvol voltooid.

- **Actie**
Toont de uitgevoerde actie.
- **Resultaat**
Toont het resultaat van de actie.
- **Datum/tijd**
Toont de datum en tijd waarop het rapport werd gemaakt.

Inhoud van een rapport voor een scan

- *Datum van de scan:*
de datum van de scan.
- *Starttijd van de scan:*
de starttijd van de scan in uu:mm.
- *Vereiste scantijd:*
de tijdsduur van de scan in mm:ss-notatie.
- *Scanstatus:*
toont of de scan werd voltooid.
- *Laatste detectie:*
naam van het laatst gevonden virus of het ongewenste programma.
- *Gescande mappen:*
totaal aantal gescande mappen.
- *Gescande bestanden:*
totaal aantal gescande bestanden.
- *Gescande archieven:*
aantal gescande archieven.
- *Verborgene objecten:*
totaal aantal gedetecteerde verborgene objecten
- *Detecties:*
totaal aantal gedetecteerde virussen en ongewenste programma's.
- *Verdacht:*
aantal verdachte bestanden.
- *Waarschuwingen:*

aantal waarschuwingen over gedetecteerde virussen.

- *Informatie:*
aantal uitgegeven informatie-items, bijvoorbeeld aanvullende informatie die gedurende een scan kan opkomen.
- *Gerepareerd:*
totaal aantal gerepareerde bestanden
- *Quarantaine:*
totaal aantal bestanden in quarantaine geplaatst.
- *Hernoemd:*
totaal aantal hernoemde bestanden.
- *Verwijderd:*
totaal aantal verwijderde bestanden.
- *Gewist:*
totaal aantal overgeschreven bestanden.

Let op

Rootkits hebben de mogelijkheid om processen en objecten te verbergen zoals registerinvoeringen of bestanden. Niet elk verborgen object is echter per se bewijs voor het bestaan van een rootkit. Verborgene objecten kunnen ook onschadelijke objecten zijn. Als een scan verborgene objecten detecteert, maar hij geeft geen waarschuwing voor virusdetectie uit, dient u het rapport te gebruiken om vast te stellen naar welk object wordt verwezen en om meer informatie over het gedetecteerde object te verkrijgen.

7.3.13 Gebeurtenissen




Gebeurtenissen die gegenereerd zijn door de verschillende programmacomponenten worden weergegeven onder **Gebeurtenissen**.

De gebeurtenissen worden opgeslagen in een database. U kunt de grootte van de gebeurtenissendatabase beperken of de restrictie op de grootte van de database uitschakelen (zie). Alleen de gebeurtenissen van de laatste 30 dagen worden opgeslagen in de standaardinstelling. De gebeurtenissenweergave wordt automatisch bijgewerkt wanneer u de **Gebeurtenissen**-sectie selecteert.

Let op

De weergave wordt niet automatisch bijgewerkt als de sectie geselecteerd wordt, als er meer dan 20.000 gebeurtenissen in de gebeurtenissendatabase zijn opgeslagen. In dat geval drukt u op **F5** om de gebeurtenis-viewer bij te werken.

Toolbar, snelkoppelingen en contextmenu

Icoon	Snelkoppeling	Beschrijving
	Terug	Geef de geselecteerde gebeurtenis weer Opent een venster waarin het resultaat van de geselecteerde actie wordt weergegeven. Bijvoorbeeld het resultaat van een scan .
	F3	Exporteer geselecteerde gebeurtenis(sen) Exporteert geselecteerde gebeurtenissen.
	Del	Verwijder geselecteerde gebeurtenis(sen) Verwijdert de geselecteerde gebeurtenis.

Let op

U heeft de optie om acties uit te voeren op een aantal geselecteerde gebeurtenissen. Om een aantal gebeurtenissen te selecteren, houdt u de **Ctrl-toets** of de **Shift-toets** (selecteert opvolgende gebeurtenissen) ingedrukt terwijl u de gewenste gebeurtenissen selecteert. Om alle weergegeven gebeurtenissen te selecteren, drukt u op **Ctrl + A**.

In het geval van de actie **Geef geselecteerde gebeurtenis weer**, is het uitvoeren van de actie op een selectie van meerdere objecten niet mogelijk.

Modules

De gebeurtenissen van de volgende modules (hier in alfabetische volgorde) kunnen weergegeven worden door de gebeurtenis-viewer:

Naam module
Helper Service
Mail Protection
Real-Time Protection
Planner


Scanner
Updater
Web Protection

Door het aanvinken van het vakje **Alle** kunt u de gebeurtenissen van alle beschikbare modules weergeven. Om alleen de gebeurtenissen van een specifieke module weer te geven, vinkt u het vakje aan naast de gewenste module.

Filter

De volgende gebeurtenisclassificatie kan weergegeven worden door de gebeurtenis-viewer.

Icoon	Beschrijving
	Informatie
	Waarschuwing
	Fout
	Detectie

Door het vakje **Filter**  aan te vinken, kunt u alle gebeurtenissen weergeven. Om alleen bepaalde gebeurtenissen weer te geven, vinkt u het vakje aan naast de gewenste gebeurtenis.

Tabel

De gebeurtenissenlijst bevat de volgende informatie:

- **Icoon**
Het icoon van de gebeurtenisclassificatie.
- **Type**
Een classificatie van de striktheid van de gebeurtenis: *Informatie*, *Waarschuwing*, *Fout*, *Detectie*.
- **Module**
De module die de gebeurtenis geregistreerd heeft. Bijvoorbeeld de Real-Time Protection-module die de detectie uitgevoerd heeft.

- **Actie**

Gebeurtenisbeschrijving van de respectieve module.

- **Datum/Tijd**

De datum en de plaatselijke tijd waarop de gebeurtenis plaatsvond.

7.3.14 Vernieuwen

Updatet het beeld van de geopende sectie.

7.4 Extra's

7.4.1 Bootrecords scannen

U kunt ook de bootsectors van de drives van uw werkstation scannen met een systeemscan. We raden dit bijvoorbeeld aan als bij het scannen een virus is ontdekt en u er zeker van wilt zijn dat de opstartsectoren niet aangetast zijn.

U kunt meer dan één bootsector selecteren door de Shift-knop ingedrukt te houden en de gewenste stations met de muis te selecteren.

Let op

Het is mogelijk om de bootsectors automatisch te laten scannen met een systeemscan (zie [Scan bootsectors van geselecteerde stations](#)).

Let op

Sinds Windows Vista moet u administratorrechten hebben om de bootsectors te scannen.

7.4.2 Detectielijst

Deze functie vermeldt in een lijst de namen van de virussen en ongewenste programma's die door uw Avira-produkt herkend worden. Een gemakkelijke zoekfunctie voor de namen is geïntegreerd.

Detectielijst doorzoeken

Voer een zoekwoord of tekenvolgorde in het *Zoeken naar:* vak.

Zoeken naar tekenreeks binnen een naam

U kunt hier een opeenvolgende reeks letters of tekens op het toetsenbord invoeren en de marker verschuift dan naar het eerste punt in de lijst met namen die deze reeks bevat, zelfs in het midden van een naam (bijvoorbeeld: "raxa" vindt "Abraxas").

Zoeken vanaf het eerste teken van een naam

U kunt hier de beginletter en de volgende tekens op het toetsenbord invoeren en de marker loopt dan alfabetisch door de lijst met namen (bijvoorbeeld: "Ko" vindt "Konijn").

Als de naam of de volgorde van tekens waarop gezocht wordt, beschikbaar is, wordt de gevonden positie gemarkeerd in de lijst.

Voorwaarts zoeken

Begint met voorwaarts zoeken in alfabetische volgorde.

Achterwaarts zoeken

Begint met achterwaarts zoeken in alfabetische volgorde.

Eerste match

Beweegt binnen de lijst naar de eerste gevonden invoer.

Ingaven in de detectielijst

Onder deze titel bevindt zich een lijst met de namen van virussen of ongewenste programma's die herkend kunnen worden. De meeste invoeren in deze lijst kunnen ook met uw Avira-produkt verwijderd worden. Deze zijn in alfabetische volgorde opgesteld (eerst speciale tekens en nummers, dan de letters). Gebruik de schuifbalk om naar boven of beneden te schuiven in de lijst.

7.4.3 Herstel-cd downloaden

Menu-opdracht **Herstel-cd downloaden** start het downloaden van het pakket Avira-herstel-cd. Het pakket bevat een opstartbaar livesysteem voor pc's en een Avira antivirusscanner met de meest actuele virusdefinities en scannersoftware. U kunt de Avira-herstel-cd gebruiken om uw pc vanaf de cd of dvd op te starten als het besturingssysteem beschadigd is, om gegevens te redden of om een antivirusscan/malware-scan uit te voeren.

Wanneer het herstel-cd-pakket van Avira is gedownload, verschijnt er een dialoogvenster waarin u een cd/dvd-drive selecteert om de herstel-cd te branden. U heeft ook de optie om het herstel-cd-pakket van Avira op te slaan en de cd op een later tijdstip te branden.

Let op

Om het herstel-cd-pakket van Avira te downloaden, moet u beschikken over

een actieve internetverbinding. Om de herstel-cd te branden, heeft u een cd/dvd-drive en een beschrijfbare cd of dvd nodig.

7.4.4 Configuratie

Het menu-onderdeel **Configuratie** in het menu **Extra's** opent de **Configuratie**.

7.5 Update

7.5.1 Start update...

Het menu-onderdeel **Update starten...** in het menu **Update** start een directe update. Het virusdefinitiebestand en de scan-engine worden geüpdatet. .

7.5.2 Handmatige update...

Het menu-onderdeel **Handmatige update...** in het menu **Update** opent een dialoogvenster voor het selecteren en laden van een VDF/zoekmachine-updatepakket. Het updatepakket kan worden gedownload van de website van de producent en bevat het huidige virusdefinitiebestand en de scan-engine:

<http://www.avira.nl>

Let op

Sinds Windows Vista moet u administrator-rechten hebben om een handmatige update uit te kunnen voeren.

7.6 Help

7.6.1 Topics

Het menu-onderdeel **Topics** in het menu **Help** opent de inhoudslijst van de online-hulpfunctie.

7.6.2 Help me

Als er een internetverbinding actief is, opent het onderdeel **Help me** in het menu **Help** de betreffende ondersteuningspagina voor uw product op de Avira-website. Daar kunt u de antwoorden op veel gestelde vragen lezen, de kennisbank raadplegen en contact opnemen met de ondersteuning van Avira.

7.6.3 Live ondersteuning

Als er een internetverbinding actief is, opent de menu-opdracht **Live ondersteuning** in het menu **Help** een pagina op de Avira-website. Download de klantmodule Avira-ondersteuning. De klantmodule is noodzakelijk voor een externe verbinding met de Avira-ondersteuning. Nadat u de module heeft gedownload en geïnstalleerd, neemt u telefonisch contact op met de Avira-ondersteuning om ons uw module-ID door te geven en een ondersteuningssessie op afstand te plannen.

7.6.4 Forum

Als er een internetverbinding actief is, opent de menu-opdracht **Forum** in het menu **Help** een webpagina die u toegang geeft tot het Avira-forum.

7.6.5 Handleiding downloaden

Als er een internetverbinding actief is, opent de menu-opdracht **Handleiding downloaden** in het menu **Help** de download-pagina van uw Avira-product. Hier vindt u de link voor het downloaden van de huidige versie van de handleiding van uw Avira-product.

7.6.6 Licentiebeheer

Het menu-item **Licentiebeheer** in het menu **Help** wordt de licentiewizard geopend. Deze assistent helpt u op gemakkelijke wijze uw Avira-product te licenseren of te activeren.

Product activeren

Activeer deze optie als u al een activeringscode hebt en uw Avira-product nog niet hebt geactiveerd. Tijdens de activering van het product wordt u als klant geregistreerd en wordt uw Avira-product met uw licentie geactiveerd. U heeft van ons of per e-mail of afgedrukt op de verpakking van het product de activeringscode ontvangen.

Let op

Als dit door een nieuwe installatie van het systeem wordt vereist, kan de activering van het programma herhaaldelijk met een geldige activeringscode worden uitgevoerd.

Let op

Voor productvalidatie gebruikt het programma het HTTP-protocol en poort 80 (webcommunicatie), evenals coderingsprotocol SSL en poort 443 om met de Avira-servers te communiceren. Als u een firewall gebruikt, dient u ervoor te zorgen dat de vereiste verbindingen en/of binnenkomende of uitgaande gegevens niet door de firewall worden geblokkeerd.

Let op

U heeft de optie voor een product van de Avira-bureaubladproductenfamilie een upgrade te lanceren (zie [Productinformatie > Licenties en upgraden](#)). Voer in het invoervak **Activeringscode** de activeringscode in voor het product waarvoor u een upgrade wilt uitvoeren. Als een upgrade beschikbaar is, wordt het product automatisch geïnstalleerd.

Licentie kopen/verlengen

Deze optie wordt weergegeven als uw licentie nog geldig is, is verlopen of als u net een evaluatielicentie heeft. Gebruik deze optie om uw productlicentie te verlengen of om een licentie van een volledige versie te kopen. Dit vereist een actieve internetverbinding. Selecteer de optie **Licentie kopen/verlengen** en klik op **Volgende**. Uw internetbrowser opent en uw bereikt de online Avira-shop waar u een licentie kunt kopen.

Geldig licentiebestand

U kunt via de koppeling **licentiebestand** een geldig licentiebestand laden.

Tijdens de productactivering met een geldige activeringscode wordt de licentiesleutel gegenereerd, in de programmamap van uw Avira-product opgeslagen en geladen. Gebruik deze optie als u al een product hebt geactiveerd.

Proxy-instellingen ...

Er wordt een dialoogvenster geopend als u op deze knop klikt. Indien en wanneer vereist, kunt u hier instellen dat u voor productactivering via een proxyserver de internetverbinding wilt instellen.

7.6.7 Product aanbevelen

Als er een internetverbinding actief is, opent het onderdeel **Product aanbevelen** in het menu **Help** een website voor Avira-klanten. Gebruik deze pagina om uw Avira-product aan te bevelen en te profiteren van Avira-kortingen.

7.6.8 Feedback geven

Als er een internetverbinding actief is, opent de menu-opdracht **Feedback geven** in het menu **Help** een feedback-pagina voor uw Avira-producten. Hier vindt u een product-evaluatieformulier dat u naar Avira kunt sturen met uw beoordeling van de productkwaliteit en andere suggesties.

7.6.9 Over Avira Internet Security Suite

- **Algemeen**

Adressen en informatie over uw Avira-produkt.

- **Versie-informatie**

Versie-informatie voor bestanden in het Avira-produktpakket.

- **Licentie-informatie**

Licentiegegevens voor de huidige licentie en links naar de onlineshop (kopen of verlengen van een licentie).

Let op

U kunt de licentiegegevens in de cache bewaren. Rechtsklik op het gebied *Licentiegegevens*. Een contextmenu opent. In het contextmenu, klikt u op de menuopdracht **Kopiëren naar klembord**. Uw licentiegegevens worden nu opgeslagen naar het klembord en kunnen toegevoegd worden aan e-mails, formulieren of documenten via de Windows-opdracht **Toevoegen**.

8. Bescherming van mobiele apparatuur

Avira beschermt niet alleen uw computer tegen malware en virussen, maar ook uw smartphone, die op het Android-besturingssysteem draait, tegen verlies en diefstal. Met behulp van Avira Free Android Security kunt u ook ongewenste telefoontjes of sms-berichten blokkeren. Voeg eenvoudigweg telefoonnummers van het telefoonlogboek, sms-logboek en uw lijst met contactpersonen toe aan de zwarte lijst of maak handmatig een contactpersoon aan die u wilt blokkeren.

Meer informatie kunt u vinden op onze website:

<http://www.avira.com/android>

9. Configuratie

9.1 Configuratie

- [Overzicht van configuratieopties](#)
- [Knoppen](#)

Overzicht van configuratieopties

De volgende configuratie-opties zijn beschikbaar:

- **System Scanner:** Configuratie van een systeemscan (op aanvraag)
 - Scanopties
 - Actie bij detectie
 - Archief-scanopties
 - Systeemscan uitzonderingen
 - Systeemscan heuristieken
 - Rapportfunctie-instelling
- **Real-Time Protection:** Configuratie van een realtime-scan (on-access)
 - Scanopties
 - Actie bij detectie
 - Verdere acties
 - Uitzonderingen On-access-scan
 - Heuristieken On-access-scan
 - Rapportfunctie-instelling
- **Update:** Configuratie van de update-instellingen, set-up van de productupdates
 - Download via webserver
 - Proxy-instellingen
- **Web Protection:** Configuratie van Web Protection
 - Scan-opties, Web Protection activeren en deactiveren
 - Actie bij detectie
 - Geblokkeerde toegang: Ongewenste bestandstypen en MIME-typen, web filter voor bekende ongewenste URL's (kwaadaardige software, phishing, enz.)
 - Web Protection-scan uitzonderingen: URL's, bestandstypen, MIME-typen
 - Web Protection heuristieken
 - Rapportfunctie-instelling
- **Mail Protection:** Configuratie van Mail Protection
 - Scan-opties: Inschakelen van de monitoring van POP3-accounts, IMAP-accounts, uitgaande e-mails (SMTP)

- Acties bij detectie
- Verdere acties
- Heuristische Mail Protection-scan
- AntiBot functie: Toegestane SMTP-servers, toegestane e-mail afzenders
- Uitzonderingen Mail Protection-scan
- Configuratie van cache, lege cache
- Configuratie van een voettekst in verzonden e-mails
- Rapportfunctie-instelling
- **Algemeen:**
 - Bedreigingscategorieën voor System Scanner en Real-Time Protection
 - Toepassingsfilter: Blokkeren of toestaan toepassingen
 - Geavanceerde bescherming: Opties om de ProActiv en Protection Cloud functies in te schakelen.
 - Wachtwoordbeveiliging voor toegang tot het Control Center en de Configuratie
 - Beveiliging: blokkeer autostartfunctie, statusweergave van volledige systeemscan, productbescherming, bescherm Windows-hostsbestand
 - WMI: schakel WMI-ondersteuning in
 - Gebeurtenissenlog configuratie
 - Configuratie van rapportfuncties
 - Instellen van gebruikte mappen

Knoppen

Knop	Beschrijving
Standaardwaarden	Alle instellingen van de configuratie zijn hersteld naar de standaardwaarden. Alle veranderingen en eigen toevoegingen worden gewist als de standaardinstellingen worden hersteld.
OK	Alle uitgevoerde instellingen zijn opgeslagen. De configuratie wordt gesloten. De gebruikersaccountcontrole (UAC) zal u toestemming vragen voor het toepassen van veranderingen in besturingssystemen vanaf Windows Vista.
Annuleren	De configuratie wordt gesloten zonder uw instellingen in de configuratie op te slaan.
Toepassen	Alle uitgevoerde instellingen zijn opgeslagen. De gebruikersaccountcontrole (UAC) zal u toestemming vragen voor het toepassen van veranderingen in besturingssystemen vanaf Windows Vista.

9.2 Scanner

De sectie **System Scanner** onder Configuratie is verantwoordelijk voor de configuratie van de scan op aanvraag.

9.2.1 Scan

U kunt het gedrag bepalen van de scanroutine op aanvraag . Als u bepaalde mappen selecteert, scant de Scanner afhankelijk van de configuratie:

- met een bepaalde scanprioriteit,
- ook bootsectors en hoofdgeheugen,
- alle of geselecteerde bestanden in de map.

Bestanden

De Scanner kan een filter gebruiken om alleen de bestanden met een bepaalde extensie te scannen (soort).

Alle bestanden

Als deze optie is ingeschakeld, worden alle bestanden gescand op virussen of ongewenste programma's, ongeacht hun inhoud en bestandsextensie. De filter wordt niet gebruikt.

Let op

Indien **Alle bestanden** is ingeschakeld, kan de knop **Bestandsextensies** niet worden geselecteerd.

Gebruik slimme extensies

Als deze optie is ingeschakeld, wordt de selectie van de bestanden die worden gescand op virussen of ongewenste programma's, automatisch gekozen door het programma. Dit betekent dat uw Avira-programma beslist of de bestanden gescand worden of niet, gebaseerd op hun inhoud. Deze procedure is iets trager dan **Gebruik bestandsextensielijst**, maar zekerder, omdat er niet alleen op basis van de bestandsextensie wordt gescand. Deze optie is ingeschakeld als standaardinstelling en wordt aanbevolen.

Let op

Indien **Gebruik slimme extensies** is ingeschakeld, kan de knop **Bestandsextensies** niet worden geselecteerd.

Bestandsextensielijst gebruiken

Als deze optie is ingeschakeld, worden alleen bestanden met een bepaalde extensie gescand. Alle bestandstypen die virussen en ongewenste programma's kunnen bevatten, zijn vooraf ingesteld. De lijst kan handmatig worden bewerkt via de knop "**Bestandsextensies**".

Let op

Als deze optie is ingeschakeld en u hebt alle gegevens verwijderd uit de lijst met bestandsextensies, wordt dit aangegeven met de tekst "*Geen bestandsextensies*" onder de knop **Bestandsextensies**.

Bestandsextensies

Deze knop opent een dialoogvenster waarin alle gescande bestandsextensies worden getoond in de modus "**Gebruik bestandsextensielijst**". Standaardinstellingen worden voor de extensies ingesteld, maar instellingen kunnen worden toegevoegd of verwijderd.

Let op

Houd er rekening mee dat de standaardlijst kan variëren van versie tot versie.

Extra instellingen

Bootsectors van geselecteerde stations scannen

Als deze optie is ingeschakeld, scant de Scanner de bootsectors van de stations die u selecteert voor de systeemscan. Deze optie wordt ingeschakeld als de standaardinstelling.

Hoofdbootsectors scannen

Als deze optie is ingeschakeld, scant de Scanner de hoofdbootsectors van de harddisk(s) die worden gebruikt in het systeem.

Offline bestanden negeren

Als deze optie is ingeschakeld, negeert de directe scan volledig de zogenaamde offlinebestanden tijdens het scannen. Dit houdt in dat deze bestanden niet worden gescand op virussen en ongewenste programma's. Offlinebestanden zijn bestanden die fysiek door een Hierarchical Storage Management System (HSMS) zijn verplaatst van een harde schijf naar een tape bijvoorbeeld. Deze optie wordt ingeschakeld als de standaardinstelling.

Integriteitscontrole van systeembestanden

Als deze optie is ingeschakeld, worden de belangrijkste systeembestanden van Windows onderworpen aan een bijzonder veilige controle op wijzigingen door malware tijdens elke scan op aanvraag. Als een gewijzigd bestand wordt gedetecteerd, wordt

dit als verdacht gemeld. Deze functie gebruikt veel computercapaciteit. Dat is de reden waarom de optie is uitgeschakeld als standaardinstelling.

Let op

Deze optie is alleen beschikbaar bij Windows Vista en hoger.

Let op

Deze optie mag niet worden gebruikt als u tools van derden gebruikt die systeembestanden wijzigen en het boot- of startscherm aanpassen aan uw eisen. Voorbeelden van dergelijke tools zijn skinpacks, TuneUp-hulpprogramma's of Vista Customization.

Geoptimaliseerde scan

Als de optie is ingeschakeld, wordt de processorcapaciteit optimaal benut tijdens een Scanner-scan. Om redenen van performance wordt een geoptimaliseerde scan alleen op standaardniveau geregistreerd.

Let op

Deze optie is alleen beschikbaar op multiprocessorsystemen.

Symbolische koppelingen volgen

Als deze optie is ingeschakeld, voert de Scanner een scan uit die alle symbolische koppelingen in het scanprofiel of de geselecteerde map volgt en scant de gekoppelde bestanden op virussen en malware.

Let op

De optie bevat geen snelkoppelingen, maar heeft uitsluitend betrekking op symbolische links (gegenereerd door mklink.exe) of Junction Points (gegenereerd door junction.exe) die transparant zijn in het bestandssysteem.

Zoeken naar rootkits vóór scan

Als deze optie is ingeschakeld en er een scan is gestart, scant de Scanner de Windows-systeemmap op actieve rootkits in een zogenaamde snelkoppeling. Dit proces scant uw computer niet zo volledig op actieve rootkits zoals bij het scanprofiel "**Scan op rootkits**", maar het is aanzienlijk sneller qua uitvoering. Deze optie verandert alleen de instellingen van door u gecreëerde profielen.

Let op

Rootkits scannen is niet beschikbaar voor Windows XP 64 bit

Register scannen

Als deze optie is ingeschakeld, wordt het register gescand op verwijzingen naar malware. Deze optie verandert alleen de instellingen van door u gecreëerde profielen.

Bestanden en paden op Network Drives negeren

Als deze optie is ingeschakeld, worden de op de computer aangesloten Network Drives uitgesloten van de scan op aanvraag. Deze optie wordt aanbevolen wanneer de servers of andere werkstations zelf al zijn beschermd met antivirussoftware. Deze optie is uitgeschakeld als standaardinstelling.

*Scanproces***Stoppen van de scanner toestaan**

Als deze optie is ingeschakeld, kan de scan op virussen of ongewenste programma's op elk moment worden beëindigd met de toets "**Stop**" in het "Luke Filewalker"-venster. Als u deze optie heeft uitgeschakeld dan heeft de knop **Stop** in het "Luke Filewalker"-venster een grijze achtergrond. Voortijdige beëindiging van een scanproces is dus niet mogelijk! Deze optie wordt ingeschakeld als de standaardinstelling.

Scannerprioriteit

Bij de scan op aanvraag maakt de Scanner een onderscheid tussen prioriteitsniveaus. Dit is alleen effectief als er meerdere processen gelijktijdig worden uitgevoerd op het werkstation. De selectie beïnvloedt de scansnelheid.

laag

De Scanner wordt alleen processortijd toegekend door het besturingssysteem als er geen andere processen rekentijd vragen, d.w.z. zolang alleen de Scanner draait, is de snelheid maximaal. In het algemeen is samenwerking met andere programma's optimaal: de computer reageert sneller als andere programma's processortijd nodig hebben, terwijl de Scanner blijft draaien op de achtergrond.

normaal

De Scanner wordt uitgevoerd met normale prioriteit. Aan alle processen wordt dezelfde hoeveelheid processortijd toegewezen door het besturingssysteem. Deze optie is ingeschakeld als standaardinstelling en wordt aanbevolen. Onder bepaalde omstandigheden kan het werken met andere toepassingen worden beïnvloed.

hoog

De Scanner heeft de hoogste prioriteit. Gelijktijdig werken met andere toepassingen is bijna onmogelijk. De Scanner voltooit de scan echter op maximale snelheid.

Actie bij detectie

U kunt de acties vastleggen die door System Scanner moeten worden uitgevoerd wanneer een virus of ongewenst programma wordt gedetecteerd.

Interactief

Wanneer deze optie is ingeschakeld, worden de resultaten van de scan van de System Scanner weergegeven in een dialoogvenster. Bij het uitvoeren van een scan met de System Scanner krijgt u aan het einde van de scan een waarschuwing met een lijst van de geïnfekteerde bestanden. U kunt het contextgevoelige menu gebruiken om een uit te voeren actie te selecteren voor de verschillende geïnfekteerde bestanden. U kunt de standaardacties uitvoeren voor alle geïnfekteerde bestanden of de Scanner annuleren.

Let op

De actie **Quarantaine** is standaard voorgeselecteerd in de berichtgeving van de System Scanner. Aanvullende acties kunnen worden geselecteerd via een contextmenu.

Automatisch

Wanneer deze optie is ingeschakeld, verschijnt er geen dialoogvenster bij de detectie van een virus. De System Scanner reageert volgens de instellingen die u vooraf definieert in dit gedeelte als primaire en secundaire actie.

Bestand vóór actie naar quarantaine kopiëren

Als deze optie is ingeschakeld, maakt de System Scanner eerst een backupkopie voordat de gevraagde primaire of secundaire actie wordt uitgevoerd. De backupkopie wordt opgeslagen in **Quarantaine**, waar het bestand kan worden hersteld indien het van informatieve waarde is. U kunt de backupkopie ook naar het Avira Malware Research Center sturen voor verder onderzoek.

Primaire actie

De primaire actie is de actie die wordt uitgevoerd wanneer de System Scanner een virus of ongewenst programma vindt. Als de optie "**Repareren**" is geselecteerd, maar het geïnfekteerde bestand niet kan worden gerepareerd, wordt de onder "**Secundaire actie**" geselecteerde actie uitgevoerd.

Let op

De optie **Secundaire actie** kan alleen worden geselecteerd wanneer de instelling **Repareren** is geselecteerd onder **Primaire actie**.

Repareren

Als deze optie is ingeschakeld, repareert de System Scanner automatisch geïnfekteerde bestanden. Als de System Scanner een geïnfekteerd bestand niet kan repareren, wordt de onder **Secundaire actie** geselecteerde actie uitgevoerd.

Let op

Een automatische reparatie wordt aanbevolen, maar betekent wel dat de System Scanner bestanden op het werkstation aanpast.

Hernoemen

Als deze optie is ingeschakeld, hernoemt de System Scanner het bestand. Directe toegang tot deze bestanden (bijv. door dubbelklikken) is daarom niet meer mogelijk. Bestanden kunnen later worden gerepareerd en weer hun originele namen krijgen.

Quarantaine

Als deze optie is ingeschakeld, verplaatst de System Scanner het bestand naar de quarantaine. Deze bestanden kunnen later worden gerepareerd of - indien nodig - worden gestuurd naar het Avira Malware Research Center.

Verwijderen

Wanneer deze optie is ingeschakeld wordt het bestand verwijderd. Dit proces is veel sneller dan "overschrijven en verwijderen".

Negeren

Wanneer deze optie is ingeschakeld, is het bestand toegankelijk en blijft het bestand zoals het is.

Waarschuwing

Het aangetaste bestand blijft actief op uw werkstation! Het kan ernstige schade aan uw werkstation veroorzaken!

Overschrijven en verwijderen

Als deze optie is ingeschakeld, overschrijft de System Scanner het bestand met een standaardpatroon en verwijdert het vervolgens. Het kan niet hersteld worden.

Secundaire actie

De optie "**Secundaire actie**" kan alleen worden geselecteerd als de instelling **Repareren** is geselecteerd onder "**Primaire actie**". Door middel van deze optie kan nu worden bepaald wat er moet worden gedaan met het geïnfecteerde bestand als het niet gerepareerd kan worden.

Hernoemen

Als deze optie is ingeschakeld, hernoemt de System Scanner het bestand. Directe toegang tot deze bestanden (bijv. door dubbelklikken) is daarom niet meer mogelijk. Bestanden kunnen later worden gerepareerd en weer hun originele namen krijgen.

Quarantaine

Als deze optie is ingeschakeld, verplaatst de System Scanner het bestand naar [Quarantaine](#). Deze bestanden kunnen later worden gerepareerd of - indien nodig - worden gestuurd naar het Avira Malware Research Center.

Verwijderen

Wanneer deze optie is ingeschakeld wordt het bestand verwijderd. Dit proces is veel sneller dan "overschrijven en verwijderen".

Negeren

Wanneer deze optie is ingeschakeld, is het bestand toegankelijk en blijft het bestand zoals het is.

Waarschuwing

Het aangetaste bestand blijft actief op uw werkstation! Het kan ernstige schade aan uw werkstation veroorzaken!

Overschrijven en verwijderen

Als deze optie is ingeschakeld, overschrijft de System Scanner het bestand met een standaardpatroon en verwijdert (wist) het vervolgens. Het kan niet hersteld worden.

Let op

Wanneer u **Verwijderen** of **Overschrijven en verwijderen** als de primaire of secundaire actie heeft geselecteerd, let dan op het volgende: in geval van heuristische hits worden de geïnfecteerde bestanden niet verwijderd, maar in plaats daarvan in quarantaine gezet.

Archieven

Bij het scannen van archieven maakt de System Scanner gebruik van een recursieve scan: archieven binnen archieven worden ook uitgepakt en gescand op virussen en ongewenste programma's. De bestanden worden gescand, gedecomprimeerd en opnieuw gescand.

Archieven scannen

Als deze optie is ingeschakeld, worden de geselecteerde archieven in de archieflijst gescand. Deze optie wordt ingeschakeld als de standaardinstelling.

Alle archieftypen

Als deze optie is ingeschakeld, worden alle archieftypes in de archieflijst geselecteerd en gescand.

Slimme extensies

Als deze optie is ingeschakeld, detecteert de System Scanner of een bestand een ingepakte bestandsopmaak (archief) heeft, zelfs als de bestandsextensie verschilt van de gebruikelijke extensies, en scant het archief. Elk bestand moet hiervoor echter worden geopend, wat de scansnelheid verlaagt. Voorbeeld: als een *.zip-archief de extensie *.xyz heeft, pakt de System Scanner ook dit archief uit en scant het. Deze optie wordt ingeschakeld als de standaardinstelling.

Let op

Alleen die archieftypen die in de archieflijst zijn gemarkeerd, worden ondersteund.

Recursie-diepte beperken

Uitpakken en scannen van recursieve archieven kan een grote aanslag doen op de computertijd en de resources. Als deze optie is ingeschakeld, beperkt u de diepte van de scan in multi-packed-archieven tot een bepaald aantal verpakkingsniveaus (maximale recursie-diepte). Dit bespaart tijd en computerresources.

Let op

Om een virus of een ongewenst programma in een archief te vinden, moet de System Scanner scannen tot het recursie-niveau waarin het virus of het ongewenste programma zich bevindt.

Maximale recursie-diepte

Om de maximale recursie-diepte in te voeren, moet de optie [Recursie-diepte beperken](#) worden ingeschakeld.

U kunt de vereiste recursie-diepte hetzij rechtstreeks invoeren, hetzij met behulp van de rechter pijltoets van het invoerveld. De toegestane waarden zijn 1 tot en met 99. De standaardwaarde is 20, en deze wordt aanbevolen.

Standaardwaarden

De knop herstelt de vooraf gedefinieerde waarden voor het scannen van archieven.

Archieven

In dit weergavegebied kunt u instellen welke archieven de System Scanner moet scannen. Hiervoor moet u de relevante invoer selecteren.

Uitzonderingen*Bestandsobjecten die moeten worden overgeslagen voor de Scanner*

De lijst in dit venster bevat de bestanden en paden die niet moeten worden opgenomen door de Scanner in de scan naar virussen en ongewenste programma's.

Vul hier een zo gering mogelijk aantal uitzonderingen in en eigenlijk alleen bestanden die, om welke reden dan ook, niet in een normale scan moeten worden opgenomen. We raden u aan deze bestanden altijd te scannen op virussen of ongewenste programma's voordat ze in deze lijst worden opgenomen!

Let open

De items in de lijst mogen niet resulteren in meer dan 6000 tekens in totaal.

Waarschuwing

Deze bestanden worden niet in een scan opgenomen!

Let op

De bestanden die in deze lijst zijn opgenomen, worden geregistreerd in het [rapportbestand](#). Controleer het rapportbestand van tijd tot tijd op niet-gescande bestanden, omdat de reden dat u hier een bestand heeft uitgesloten misschien niet meer van toepassing is. In dit geval moet u de naam van dit bestand opnieuw uit deze lijst verwijderen.

Input-box

In dit invoervak kunt u de naam van het bestandsobject invoeren dat niet is opgenomen in de scan op verzoek. Er is geen bestandsobject ingevoerd als de standaardinstelling.



De knop opent een venster waarin u het vereiste bestand of het vereiste pad kunt selecteren.

Wanneer u een bestandsnaam heeft ingevoerd met het volledige pad, wordt alleen dit bestand niet op infecties gescand. Als u een bestandsnaam zonder een pad heeft ingevoerd, worden alle bestanden met deze naam (ongeacht het pad of het station) niet gescand.

Toevoegen

Met deze knop kunt u het bestandsobject dat is ingevoerd in het invoervak, toevoegen aan het weergavevenster.

Verwijderen

De knop verwijdert een geselecteerd item uit de lijst. De knop is inactief als er geen item is geselecteerd.

Heuristiek

Dit configuratiegedeelte bevat de instellingen voor de heuristiek van de scan-engine.

Avira-producten bevatten zeer krachtige heuristieken die proactief onbekende malware kunnen detecteren, d.w.z. voordat een speciale virusdefinitie ter bestrijding van het schadelijke element is gecreëerd en voordat een update van de controle op virussen is verzonden. Virusdetectie omvat een uitgebreide analyse en onderzoek van de geïnfecteerde codes voor functies die kenmerkend zijn voor malware. Indien de code die gescand wordt deze kenmerken vertoont, wordt hij gerapporteerd als verdacht. Dit betekent niet per se dat de code inderdaad malware is. Soms doen zich valse positieven voor. De beslissing over de wijze van behandeling van de geïnfecteerde code moet door

de gebruiker worden genomen, bijv. op basis van zijn of haar kennis van de vraag of de bron van de code betrouwbaar is of niet.

Macrovirus-heuristiek

Macrovirus-heuristiek

Uw Avira-product bevat een zeer krachtige macrovirus-heuristiek. Als deze optie is ingeschakeld, worden alle macro's in het betreffende document gewist in geval van een reparatie, in het andere geval worden verdachte documenten alleen gerapporteerd, d.w.z. dat u een waarschuwing ontvangt. Deze optie is ingeschakeld als standaardinstelling en wordt aanbevolen.

Advanced Heuristic Analysis and Detection (AHeAD)

AHeAD inschakelen

Uw Avira-programma bevat een zeer krachtige heuristiek in de vorm van Avira-AHeAD-technologie, die ook onbekende (nieuwe) malware kan detecteren. Als deze optie is ingeschakeld, kunt u vastleggen hoe "agressief" deze heuristiek moet zijn. Deze optie wordt ingeschakeld als de standaardinstelling.

Laag detectieniveau

Als deze optie is ingeschakeld, wordt iets minder onbekende malware gedetecteerd; de kans op een vals alarm is in dat geval laag.

Gemiddeld detectieniveau

Deze optie combineert een sterk detectieniveau met een laag risico op vals alarm. De standaardinstelling is medium indien u heeft gekozen voor gebruik van deze heuristiek.

Hoog detectieniveau

Als deze optie is ingeschakeld, wordt aanzienlijk meer onbekende malware gedetecteerd, maar dan is er waarschijnlijk ook sprake van valse positieven.

9.2.2 Rapport

De System Scanner heeft een uitgebreide rapportagefunctie. U krijgt op deze manier exacte informatie over de resultaten van een scan op aanvraag. Het rapportagebestand bevat alle invoer van het systeem en ook waarschuwingen en berichten van de scan op aanvraag.

Let op

Om in staat te zijn om te bepalen welke acties de System Scanner heeft ondernomen als er virussen of ongewenste programma's gedetecteerd werden, moet u het rapportagebestand in de configuratie activeren.

Rapporteren

Uit

Als deze optie is ingeschakeld, rapporteert de System Scanner de acties en resultaten van de scan op aanvraag niet.

Standaard

Als deze optie is ingeschakeld, registreert de System Scanner het pad en de namen van de betreffende bestanden. Afgezien daarvan worden de configuratie van de huidige scan en informatie over de versie en de licentiehouder opgenomen in het rapportagebestand.

Uitgebreid

Als deze optie is ingeschakeld, registreert de System Scanner ook waarschuwingen en tips, afgezien van de standaardinformatie. Het rapport bevat ook een '(cloud)'-achtervoegsel om de detecties van de Protection Cloud te identificeren.

Volledig

Als deze optie is ingeschakeld, registreert de System Scanner ook alle gescande bestanden. Bovendien worden in het rapportagebestand ook alle betrokken bestanden vermeld, evenals waarschuwingen en tips.

Let op

Wanneer u ons op een willekeurig tijdstip een rapportagebestand stuurt (voor probleemoplossing), maak dan a.u.b. het rapportagebestand in deze modus aan.

9.3 Real-Time Protection

De sectie **Real-Time Protection** onder Configuratie is verantwoordelijk voor de configuratie van de scan bij toegang.

9.3.1 Scan

Normaal gesproken wilt u uw systeem constant controleren. Dat doet u door de Real-Time Protection (= on-access System Scanner) te gebruiken. Geopende of gekopieerde bestanden op uw computer worden op die manier vanzelf gescand op virussen of ongewenste programma's.

Bestanden

De Real-Time Protection kan een filter gebruiken om alleen de bestanden met een bepaalde extensie te scannen (type).

Alle bestanden

Als deze optie is ingeschakeld, worden alle bestanden gescand op virussen of ongewenste programma's, ongeacht hun inhoud en bestandsextensie.

Let op

Indien **Alle bestanden** is ingeschakeld dan kan de knop **Bestandsextensies** niet worden geselecteerd.

Gebruik slimme extensies

Als deze optie is ingeschakeld, wordt de selectie van de bestanden die worden gescand op virussen of ongewenste programma's, automatisch gekozen door het programma. Dit betekent dat uw programma beslist wanneer de bestanden gescand worden of niet, gebaseerd op hun inhoud. Deze procedure is iets trager dan **Gebruik bestandsextensielijst**, maar zekerder, omdat er niet alleen op basis van de bestandsextensie wordt gescand.

Let op

Indien **Gebruik Slimme extensies** is ingeschakeld, kan de knop **Bestandsextensies** niet worden geselecteerd.

Bestandsextensielijst gebruiken

Als deze optie is ingeschakeld, worden alleen bestanden met een bepaalde extensie gescand. Alle bestandstypen die virussen en ongewenste programma's kunnen bevatten, zijn vooraf ingesteld. De lijst kan handmatig worden bewerkt via de knop "**Bestandsextensies**". Deze optie is ingeschakeld als standaardinstelling en wordt aanbevolen.

Let op

Als deze optie is ingeschakeld en u heeft alle gegevens verwijderd uit de lijst met bestandsextensies, wordt dit aangegeven met de tekst "Geen bestandsextensies" onder de knop **Bestandsextensies**.

Bestandsextensies

Deze knop opent een dialoogvenster waarin alle gescande bestandsextensies worden getoond in de modus "**Gebruik bestandsextensielijst**". Standaardinstellingen worden voor de extensies ingesteld, maar instellingen kunnen worden toegevoegd of verwijderd.

Let op

Houd er rekening mee dat de bestandsextensielijst kan variëren van versie tot versie.

Stations

Network Drives controleren

Als deze optie is ingeschakeld, worden bestanden gescand die staan op Network Drives (mapped drives) zoals servervolumes, peer drives enz.

Let op

Gebruik de optie **Network Drives controleren** alleen in uitzonderlijke gevallen om te voorkomen dat de performance van uw computer vermindert.

Waarschuwing

Als deze optie is uitgeschakeld, worden Network Drives **niet** gecontroleerd. Ze zijn niet langer beschermd tegen virussen of ongewenste programma's!

Let op

Wanneer bestanden worden uitgevoerd op netwerkstations, worden ze door Real-Time Protection gescand, onafhankelijk van de instelling voor de optie **Netwerkstations controleren**. In sommige gevallen worden bestanden gescand op Network Drives bij het openen, ook al is de optie **Network Drives controleren** uitgeschakeld. Reden: toegang tot deze bestanden vindt plaats op basis van 'Execute File'-rechten. Indien u deze bestanden of zelfs uitgevoerde bestanden op netwerkstations wilt uitsluiten van scannen door de Real-Time Protection, voeg de bestanden dan toe aan de lijst van bestandsobjecten die uitgesloten moeten worden (zie: [Real-Time Protection > Scan > Uitzonderingen](#)).

Opslaan in cache inschakelen

Als deze optie is ingeschakeld, komen gecontroleerde bestanden op netwerkstations beschikbaar in de Real-Time Protection-cache. Network Drives controleren zonder de cachefunctie is zekerder, maar werkt niet zo goed als Network Drives controleren met opslaan in cache.

Archieven

Archieven scannen

Als deze functie is ingeschakeld, worden archieven gescand. Gecomprimeerde bestanden worden gescand, vervolgens gedecomprimeerd en dan opnieuw gescand. Deze optie is standaard uitgeschakeld. De archiefscan is beperkt door de recursie-diepte, het aantal te scannen bestanden en de grootte van het archief. Maximale recursie-diepte, het aantal te scannen bestanden en de maximale archiefgrootte kunt u instellen.

Let op

Deze optie is standaard uitgeschakeld omdat het proces een groot deel van de performance van de computer in beslag neemt. In het algemeen wordt aanbevolen om archieven te controleren met een scan op aanvraag.

Max. recursie-diepte

Real-Time Protection gebruikt een recursieve scan bij het scannen van archieven: archieven binnen archieven worden ook uitgepakt en gescand op virussen en ongewenste programma's. U kunt de recursie-diepte definiëren. De aanbevolen standaardwaarde voor de recursie-diepte is 1: alle bestanden die zich direct in het hoofdarchief bevinden, worden gescand.

Max. aantal bestanden

U kunt de scan beperken tot een maximum aantal bestanden in het archief wanneer u archieven scant. De aanbevolen standaardwaarde voor het maximum aantal te scannen bestanden is 10.

Max. grootte (kB)

Als u archieven scant, kunt u de scan beperken tot een maximale archiefgrootte die moet worden uitgepakt. De standaardwaarde van 1000 kB wordt aanbevolen.

Actie bij detectie

U kunt acties definiëren die Real-Time Protection moet ondernemen als een virus of ongewenst programma wordt gedetecteerd.

Interactief

Als deze optie is ingeschakeld, verschijnt er een bureaubladmededeling als Real-Time Protection een virus of ongewenst programma detecteert. U kunt de gedetecteerde malware verwijderen of andere mogelijke antivirusacties ondernemen via de knop "**Details**". De acties worden weergegeven in een dialoogvenster. Deze optie wordt ingeschakeld als de standaardinstelling.

Toegestane acties

In dit weergavevak kunt u de virusmanagement-acties specificeren die beschikbaar moeten zijn als aanvullende acties in het dialoogvenster. Om dat te doen moet u de bijbehorende opties activeren.

Repareren

Real-Time Protection repareert het geïnfecteerde bestand indien mogelijk.

Hernoemen

Real-Time Protection hernoemt het bestand. Directe toegang tot deze bestanden (bijv. door dubbelklikken) is daarom niet meer mogelijk. Het bestand kan worden gerepareerd op een later tijdstip en weer worden hernoemd.

Quarantaine

Real-Time Protection verplaatst het bestand naar [Quarantaine](#). Het bestand kan uit de [Quarantainemanager](#) worden hersteld indien het een informatieve waarde heeft of - indien nodig - naar het Avira Malware Research Center worden verzonden. Afhankelijk van het bestand, zijn meer opties beschikbaar in de [Quarantainemanager](#).

Verwijderen

Het bestand wordt verwijderd. Dit proces is veel sneller dan **Overschrijven en verwijderen** (zie hieronder).

Negeren

Toegang tot het bestand is toegestaan en het bestand wordt genegeerd.

Overschrijven en verwijderen

Real-Time Protection overschrijft het bestand met een standaardpatroon vóór het verwijderen. Het kan niet hersteld worden.

Waarschuwing

Als Real-Time Protection is ingesteld op **Scan tijdens schrijven**, wordt het getroffen bestand niet geschreven.

Standaard

Met deze knop kunt u een actie selecteren die in het dialoogvenster standaard geactiveerd is wanneer er een virus wordt gedetecteerd. Selecteer de actie die standaard moet worden geactiveerd en klik op de "**Standaard**"-knop.

Let op

De actie **Repareren** kan niet worden geselecteerd als standaardactie.

Klik [hier](#) voor meer informatie.

Automatisch

Wanneer deze optie is ingeschakeld, verschijnt er geen dialoogvenster bij de detectie van een virus. Real-Time Protection reageert volgens de instellingen die u vooraf definieert in dit gedeelte als primaire en secundaire actie.

Bestand vóór actie naar quarantaine kopiëren

Als deze optie is ingeschakeld, maakt de Real-Time Protection eerst een backupkopie voordat de gevraagde primaire of secundaire actie wordt uitgevoerd. De backupkopie wordt opgeslagen in quarantaine. Ze kan hersteld worden vanaf de [Quarantainemanager](#) als ze een informatieve waarde heeft. U kunt de backupkopie ook naar het Avira Malware Research Center sturen. Afhankelijk van het object zijn er meer opties beschikbaar in de [Quarantainemanager](#).

Primaire actie

De primaire actie is de actie die wordt uitgevoerd wanneer Real-Time Protection een virus of ongewenst programma vindt. Als de optie "**Repareren**" is geselecteerd, maar het geïnfecteerde bestand niet kan worden gerepareerd, wordt de onder "**Secundaire actie**" geselecteerde actie uitgevoerd.

Let op

De optie **Secundaire actie** kan alleen worden geselecteerd indien de instelling **Repareren** is geselecteerd onder **Primaire actie**.

Repareren

Als deze optie is ingeschakeld, reparaert de Real-Time Protection automatisch geïnfecteerde bestanden. Als de Real-Time Protection een geïnfecteerd bestand niet kan repareren, wordt de onder **Secundaire actie** geselecteerde actie uitgevoerd.

Let op

Een automatische reparatie wordt aanbevolen, maar betekent wel dat de Real-Time Protection bestanden op het werkstation aanpast.

Hernoemen

Als deze optie is ingeschakeld, hernoemt de Real-Time Protection het bestand. Directe toegang tot deze bestanden (bijv. door dubbelklikken) is daarom niet meer mogelijk. Bestanden kunnen later worden gerepareerd en weer hun originele namen krijgen.

Quarantaine

Als deze optie is ingeschakeld, plaatst Real-Time Protection het bestand in Quarantaine. De bestanden in deze map kunnen later worden gerepareerd of - indien nodig - worden gestuurd naar het Avira Malware Research Center.

Verwijderen

Wanneer deze optie is ingeschakeld wordt het bestand verwijderd. Dit proces is veel sneller dan **Overschrijven en verwijderen**.

Negeren

Wanneer deze optie is ingeschakeld, is het bestand toegankelijk en blijft het bestand zoals het is.

Waarschuwing

Het aangetaste bestand blijft actief op uw werkstation! Het kan ernstige schade aan uw werkstation veroorzaken!

Overschrijven en verwijderen

Als deze optie is ingeschakeld, overschrijft de Real-Time Protection het bestand met een standaardpatroon en verwijdert het daarna. Het kan niet hersteld worden.

Toegang weigeren

Als deze optie is ingeschakeld, voert Real-Time Protection de detectie alleen in het [rapportbestand](#) in, als de rapportfunctie is ingeschakeld. Bovendien voegt de Real-Time Protection een vermelding toe in het [Gebeurtenissenlogboek](#), als deze optie is ingeschakeld.

Waarschuwing

Als Real-Time Protection is ingesteld op **Scan tijdens schrijven**, wordt het geïnfecteerde bestand niet geschreven.

Secundaire actie

De optie **Secundaire actie** kan alleen worden geselecteerd als de optie **Repareren** werd geselecteerd onder **Primaire actie**. Door middel van deze optie kan nu worden bepaald wat er moet worden gedaan met het geïnfecteerde bestand als het niet gerepareerd kan worden.

Hernoemen

Als deze optie is ingeschakeld, hernoemt de Real-Time Protection het bestand. Directe toegang tot deze bestanden (bijv. door dubbelklikken) is daarom niet meer mogelijk. Bestanden kunnen later worden gerepareerd en weer hun originele namen krijgen.

Quarantaine

Als deze optie is ingeschakeld, plaatst Real-Time Protection het bestand in [Quarantaine](#). De bestanden kunnen later gerepareerd worden of - indien nodig - verzonden worden naar het Avira Malware Research Center.

Verwijderen

Wanneer deze optie is ingeschakeld wordt het bestand verwijderd. Dit proces is veel sneller dan **Overschrijven en verwijderen**.

Negeren

Wanneer deze optie is ingeschakeld, is het bestand toegankelijk en blijft het bestand zoals het is.

Waarschuwing

Het betrokken bestand blijft actief op uw werkstation! Het kan ernstige schade aan uw werkstation veroorzaken!

Overschrijven en verwijderen

Als deze optie is ingeschakeld, overschrijft de Real-Time Protection het bestand met een standaardpatroon en verwijdert het daarna. Het kan niet hersteld worden.

Toegang weigeren

Als deze optie is ingeschakeld, wordt het betrokken bestand niet geschreven; Real-Time Protection vermeldt de detectie alleen in het [rapportbestand](#) als de rapportfunctie is ingeschakeld. Bovendien voegt de Real-Time Protection een vermelding toe in het [Gebeurtenissenlogboek](#), als deze optie is ingeschakeld.

Let op

Indien u **Verwijderen** of **Overschrijven en verwijderen** als primaire of secundaire actie heeft geselecteerd, let dan op het volgende: in geval van heuristische hits worden de geïnfekteerde bestanden niet verwijderd, maar in plaats daarvan in quarantaine gezet.

Verdere acties

Gebeurtenissenlogboek gebruiken

Wanneer deze optie is ingeschakeld wordt voor elke detectie een vermelding toegevoegd aan het Windows-gebeurtenissenlogboek. De gebeurtenissen kunnen worden opgeroepen in de Windows-gebeurtenissenviewer. Deze optie is ingeschakeld als de standaardinstelling.

Uitzonderingen

Met deze opties kunt u uitzonderingsobjecten instellen voor de Real-Time Protection (on-access-scan). De desbetreffende objecten worden dan niet opgenomen in de on-access-scan. De Real-Time Protection kan bestandstoegang tot deze objecten negeren tijdens de on-access-scan op basis van de lijst met processen die moeten worden overgeslagen. Dit is nuttig, bijvoorbeeld bij databases of backupoplossingen.

Let op het volgende bij het opgeven van processen en bestandsobjecten die moeten worden overgeslagen: de lijst wordt van boven naar beneden verwerkt. Hoe langer de lijst, des te meer processtijd is nodig voor het verwerken van de lijst voor elke toegang. Vandaar dat het verstandig is de lijst zo kort mogelijk te houden.

Processen die moeten worden overgeslagen door de Real-Time Protection

Alle procesbestandstoegangen in deze lijst worden uitgesloten van controle door Real-Time Protection.

Input-box

In dit veld voert u de naam in van het proces dat moet worden genegeerd door de realtime-scan. Er wordt geen proces ingevoerd als de standaardinstelling.

Het opgegeven pad en de bestandsnaam van het proces mogen maximaal uit 255 tekens bestaan. U kunt tot maximaal 128 processen invoeren. De vermeldingen in de lijst mogen in totaal niet meer dan 6000 karakters bevatten.

Bij het invoeren van het proces worden Unicode-symbolen geaccepteerd. U kunt dus proces- of mapnamen invoeren die speciale symbolen bevatten.

Drive-informatie moet als volgt worden ingevoerd: [Drive-letter]:\

Het dubbele-puntsymbool (:) wordt alleen gebruikt om drives te specificeren.

Bij het specificeren van het proces kunt u gebruik maken van de jokertekens * (een willekeurig aantal tekens) en ? (één enkel karakter).

```
C:\Program Files\Application\application.exe
C:\Program Files\Application\ applicatio?.exe
C:\Program Files\Application\ applic*.exe
C:\Program Files\Application\*.exe
```

Om te voorkomen dat het proces volledig wordt uitgesloten van controle door Real-Time Protection, zijn specificaties die uitsluitend bestaan uit de volgende tekens, ongeldig: * (asterisk), ? (vraagteken), / (slash), \ (backslash), . (punt),: (dubbele punt).

U heeft de mogelijkheid processen uit te sluiten van controle door de Real-Time Protection, zonder volledig details over het pad. Bijvoorbeeld: application.exe

Dit geldt echter alleen voor processen waarbij de uitvoerbare bestanden zich bevinden op de harde schijven.

Het volledige pad is nodig voor processen waarbij de uitvoerbare bestanden zich bevinden op aangesloten stations, zoals Network Drives. Let op de algemene informatie over de notatie van [Uitzonderingen op aangesloten Network Drives](#).

Specificeer geen uitzonderingen voor processen waarvan de uitvoerbare bestanden zich bevinden op dynamische stations. Dynamische stations worden gebruikt voor verwijderbare schijven, zoals cd's, dvd's of USB-sticks.

Waarschuwing

Houd er rekening mee dat alle procesbestandstoegangen die in de lijst zijn opgenomen, worden uitgesloten van de scan op virussen en ongewenste programma's!



De knop opent een venster waarin u een uitvoerbaar bestand kunt selecteren.

Processen

De knop "**Processen**" opent het venster "**Processelectie**", waarin de lopende processen worden weergegeven.

Toevoegen

Met deze knop kunt u het proces dat is ingevoerd in het invoervak, toevoegen aan het weergavevenster.

Verwijderen

Met deze knop kunt u een geselecteerd proces verwijderen uit het weergavevenster.

Bestandsobjecten die moeten worden overgeslagen door de Real-Time Protection

Alle bestandstoegangen van processen in deze lijst worden uitgesloten van controle door Real-Time Protection.

Input-box

In dit vak kunt u de naam invoeren van het bestandsobject dat niet is opgenomen in de on-access-scan. Er is geen bestandsobject ingevoerd als de standaardinstelling.

De vermeldingen in de lijst mogen in totaal niet meer dan 6000 karakters bevatten.

Bij het specificeren van bestandsobjecten die overgeslagen moeten worden, kunt u gebruik maken van de jokertekens* (een willekeurig aantal tekens) en ? (een enkel teken): individuele bestandsextensies kunnen ook worden uitgesloten (inclusief jokertekens):

```
C:\Directory\*.mdb
*.mdb
*md?
*.xls *
C:\Directory\*.log
```

Mapnamen moeten eindigen met een backslash \.

Als een map is uitgesloten, worden alle sub-mappen automatisch ook uitgesloten.

Voor elk station kunt u een maximum van 20 uitzonderingen opgeven door het invoeren van het volledige pad (beginnend met de stationsletter). Bijvoorbeeld:

```
C;\Program Files\Application\Name.log
```

Het maximum aantal uitzonderingen zonder een compleet pad is 64. Bijvoorbeeld:

```
*.log
\computer1\C\directory1
```

In het geval van dynamische schijven die zijn aangesloten als een map op een ander station, moet de alias van het besturingssysteem voor het geïntegreerde station in de uitzonderingenlijst worden gebruikt, bijvoorbeeld:

```
\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\
```

Als u het koppelpunt als zodanig gebruikt, bijvoorbeeld C: \ DynDrive, wordt de dynamische drive desondanks gescand. U kunt de alias van het besturingssysteem die moet worden gebruikt, ophalen uit het Real-Time Protection-rapportbestand.



De knop opent een venster waarin u het bestand kunt selecteren dat moet worden uitgesloten.

Toevoegen

Met deze knop kunt u het bestandsobject dat is ingevoerd in het invoervak, toevoegen aan het weergavevenster.

Verwijderen

Met deze knop kunt u een geselecteerd bestandsobject verwijderen uit het weergavevenster.

Let alstublieft op de volgende informatie wanneer u uitzonderingen specificeert:

Om ook objecten uit te sluiten wanneer deze worden geopend met korte DOS-bestandsnamen (DOS-naamconventie 8.3), moet de desbetreffende korte bestandsnaam ook worden opgenomen in de lijst.

Een bestandsnaam die jokertekens bevat, mag niet worden afgesloten met een backslash. Bijvoorbeeld:

```
C:\ Program Files\Application\application*exe\
```

Deze invoer is niet geldig en wordt niet behandeld als een uitzondering!

Let op het volgende met betrekking tot **uitzonderingen op aangesloten netwerkstations**: als u de stationsletter van het aangesloten netwerkstation gebruikt, worden de opgegeven bestanden en mappen NIET uitgesloten van de Real-Time Protection-scan. Als het UNC-pad in de uitzonderingenlijst verschilt van het UNC-pad gebruikt voor de verbinding met de netwerkdrive (IP-adresspecificatie in de uitzonderingenlijst - specificatie van de computernaam voor de verbinding met de netwerkdrive), worden de opgegeven mappen en bestanden NIET uitgesloten van de Real-Time Protection-scan. Zoek het relevante UNC-pad in het Real-Time Protection-rapportbestand:

```
\\<Computernaam>\<Enable>\ - OF - \\<IP-adres>\<Enable>\
```

U kunt het pad dat Real-Time Protection gebruikt om te scannen op geïnfecteerde bestanden vinden in het Real-Time Protection-rapportbestand. Geef precies hetzelfde pad op in de uitzonderingenlijst. Ga als volgt te werk: stel de protocolfunctie van de Real-Time Protection in op **Compleet** in de configuratie onder [Real-Time Protection > Rapport](#). Benader nu de bestanden, mappen, gekoppelde stations of verbonden netwerkstations met de geactiveerde Real-Time Protection. U kunt nu het pad dat moet worden gebruikt, lezen in het Real-Time Protection-rapportbestand. U krijgt toegang tot het rapportbestand in het Control Center onder [Lokale bescherming > Real-Time Protection](#).

Heuristiek

Dit configuratiegedeelte bevat de instellingen voor de heuristiek van de scan-engine.

Avira-producten bevatten zeer krachtige heuristieken die proactief onbekende malware kunnen detecteren, d.w.z. voordat een speciale virusdefinitie ter bestrijding van het schadelijke element is gecreëerd en voordat een update van de controle op virussen is verzonden. Virusdetectie omvat een uitgebreide analyse en onderzoek van de

geïnfecteerde codes voor functies die kenmerkend zijn voor malware. Indien de code die gescand wordt deze kenmerken vertoont, wordt hij gerapporteerd als verdacht. Dit betekent niet per se dat de code inderdaad malware is. Soms doen zich valse positieven voor. De beslissing over de wijze van behandeling van de geïnfecteerde code moet door de gebruiker worden genomen, bijv. op basis van zijn of haar kennis van de vraag of de bron van de code betrouwbaar is of niet.

Macrovirus-heuristiek

Macrovirus-heuristiek

Uw Avira-product bevat een zeer krachtige macrovirus-heuristiek. Als deze optie is ingeschakeld, worden alle macro's in het betreffende document gewist in geval van een reparatie, in het andere geval worden verdachte documenten alleen gerapporteerd, d.w.z. dat u een waarschuwing ontvangt. Deze optie is ingeschakeld als standaardinstelling en wordt aanbevolen.

Advanced Heuristic Analysis and Detection (AHeAD)

AHeAD inschakelen

Uw Avira-programma bevat een zeer krachtige heuristiek in de vorm van Avira-AHeAD-technologie, die ook onbekende (nieuwe) malware kan detecteren. Als deze optie is ingeschakeld, kunt u vastleggen hoe "agressief" deze heuristiek moet zijn. Deze optie wordt ingeschakeld als de standaardinstelling.

Laag detectieniveau

Als deze optie is ingeschakeld, wordt iets minder onbekende malware gedetecteerd; de kans op een vals alarm is in dat geval laag.

Gemiddeld detectieniveau

Deze optie combineert een sterk detectieniveau met een laag risico op vals alarm. De standaardinstelling is medium indien u heeft gekozen voor gebruik van deze heuristiek.

Hoog detectieniveau

Als deze optie is ingeschakeld, wordt aanzienlijk meer onbekende malware gedetecteerd, maar dan is er waarschijnlijk ook sprake van valse positieven.

9.3.2 Rapport

Real-Time Protection omvat een uitgebreide logboekregistratiefunctie om de gebruiker of administrator exacte notities te geven over het type en de manier van een detectie.

Rapporteren

Met deze groep kunt u de inhoud van het rapportbestand bepalen.

Uit

Als deze optie is ingeschakeld, creëert Real-Time Protection geen logboekregistratie. We raden aan om de logboekregistratiefunctie alleen in uitzonderlijke gevallen uit te schakelen, bijvoorbeeld bij het uitvoeren van testen met meerdere virussen of ongewenste programma's.

Standaard

Als deze optie is ingeschakeld, registreert Real-Time Protection belangrijke informatie (over detecties, waarschuwingen en fouten) in het rapportbestand, en minder belangrijke informatie wordt genegeerd voor meer helderheid. Deze optie wordt ingeschakeld als de standaardinstelling.

Uitgebreid

Als deze optie is ingeschakeld, registreert Real-Time Protection ook minder belangrijke informatie in het rapportbestand.

Volledig

Als deze optie is ingeschakeld, registreert Real-Time Protection alle beschikbare informatie in het rapportbestand, inclusief bestandsgrootte, bestandstype, datum, enz.

Rapportbestand beperken

Grootte beperken tot n MB

Als deze optie is ingeschakeld, kan het rapportbestand beperkt worden tot een zekere grootte. Toegestane waarden liggen tussen 1 en 100 MB. Ongeveer 50 kilobytes extra ruimte wordt toegestaan bij de beperking van het rapportbestand om het gebruik van de systeembronnen zo laag mogelijk te houden. Als het rapportbestand de geïndiceerde grootte met meer dan 50 kilobyte overschrijdt, worden oude invoeren verwijderd totdat de geïndiceerde grootte minus 50 kilobytes is bereikt.

Backup van rapportbestand maken vóór verkleinen

Als deze optie is ingeschakeld, wordt een backup gemaakt van het rapportbestand vóór verkleinen.

Configuratie naar rapportbestand schrijven

Als deze optie is ingeschakeld, wordt de configuratie van de on-access-scan in het rapportbestand geregistreerd.

Let op

Als u geen rapportbestandsbeperking heeft ingesteld, wordt automatisch een nieuw rapportbestand gecreëerd als het rapportbestand een grootte van 100 MB bereikt. Er wordt een backup gemaakt van het oude rapportbestand. Er kunnen maximaal drie backups van oude rapportbestanden worden opgeslagen. De oudste backups worden eerst verwijderd.

9.4 Update

In het **Update**-gedeelte kunt u de automatische ontvangst van updates. U kunt verschillende update-intervallen.

Automatische update

Elke n dag(en) / uur (uren) / minuut (minuten)

In dit venster kunt u het interval specificeren waarmee de automatische update wordt uitgevoerd. Om de update-interval te wijzigen, markeert u een van de tijdopties in het vak en wijzigt u deze met behulp van de pijltoets rechts van het invoervak.

Taak starten tijdens verbinding maken met internet (inbellen)

Wanneer deze optie is ingeschakeld, wordt behalve het gespecificeerde update-interval de update-taak uitgevoerd, telkens wanneer er een internetverbinding tot stand komt.

Taak herhalen als de tijd reeds verlopen is

Als deze optie is ingeschakeld, worden verstreken update-taken uitgevoerd die niet konden worden uitgevoerd op het aangegeven tijdstip, bijvoorbeeld omdat de computer was uitgeschakeld.

9.4.1 Webserver

Webserver

De update kan rechtstreeks worden uitgevoerd via een webserver op het internet.

Webserver-verbinding

Bestaande verbinding gebruiken (netwerk)

Deze instelling wordt weergegeven wanneer uw verbinding wordt gebruikt via een netwerk.

Gebruik de volgende verbinding

Deze instelling wordt weergegeven wanneer u uw verbinding individueel definieert.

De Updater detecteert automatisch welke verbindingsopties beschikbaar zijn. Verbindingsopties die niet beschikbaar zijn, worden grijs weergegeven en kunnen niet worden geactiveerd. Een inbelverbinding kan handmatig worden ingesteld met behulp van bijvoorbeeld een telefoonboekinvoer in Windows.

Gebruiker

Voer de gebruikersnaam in voor het geselecteerde account.

Wachtwoord

Voer het wachtwoord in voor dit account. Om veiligheidsredenen veranderen de feitelijke tekens die u op deze plaats typt, in asterisken (*).

Let op

Wanneer u een bestaand internet-account of wachtwoord bent vergeten, neem dan contact op met uw Internet Service Provider.

Let op

De automatische inbelverbinding van de updater via zogenaamde inbel-tools (bijv. SmartSurfer, Oleco, enz.) is momenteel nog niet beschikbaar.

Een inbelverbinding verbreken die is ingesteld voor de update

Wanneer deze optie is ingeschakeld, wordt de inbelverbinding die gemaakt is voor de update, automatisch weer onderbroken zodra de download met succes is uitgevoerd.

Let op

Deze optie is alleen beschikbaar bij Windows XP. Bij nieuwere besturingssystemen wordt de voor de update geopende inbelverbinding altijd beëindigd zodra de download is uitgevoerd.

Proxy-instellingen*Proxyserver***Geen proxyserver gebruiken**

Als deze optie is ingeschakeld, wordt uw verbinding met de webserver niet tot stand gebracht via een proxyserver.

Gebruik proxy-systeeminstellingen

Als deze optie is ingeschakeld, wordt uw verbinding met de webserver niet tot stand gebracht via een proxyserver. Configureer de Windows-systeeminstellingen om een proxyserver te gebruiken onder **Configuratiescherm > Internetopties > Verbindingen > LAN-instellingen**. U heeft ook toegang tot de internetopties via het menu **Extra's** in Internet Explorer.

Waarschuwing

Als u een proxyserver gebruikt die authenticatie vereist, voer dan alle vereiste gegevens in onder de optie **Gebruik deze proxyserver**. De optie **Gebruik proxy-systeeminstellingen** kan alleen gebruikt worden voor proxyservers zonder authenticatie.

Deze proxyserver gebruiken

Als uw webserver-verbinding tot stand komt via een proxyserver, kunt u hier de relevante gegevens invoeren.

Adres

Voer de computernaam of het IP-adres in van de proxyserver die u wilt gebruiken om u te verbinden met de webserver.

Poort

Hier graag het poortnummer invoeren van de proxyserver die u wilt gebruiken om u te verbinden met de webserver.

Inlognaam

Gebruikersnaam invoeren om in te loggen bij de proxyserver.

Inlogwachtwoord

Voer hier het relevante wachtwoord in om in te loggen bij de proxyserver. Om veiligheidsredenen veranderen de feitelijke tekens die u op deze plaats typt, in asterisken (*).

Voorbeelden:

Adres: `proxy.domein.com` Poort: 8080

Adres: `192.168.1.100` Poort: 3128

9.5 FireWall

9.5.1 De FireWall configureren

Met Avira Internet Security Suite kunt u de Avira FireWall configureren of de Windows Firewall beheren (vanaf Windows 8):

- [Windows Firewall](#)

9.5.2 Windows Firewall

De **FireWall**-sectie onder **Configuratie > Internetbescherming** is verantwoordelijk voor de configuratie van de Windows Firewall, vanaf Windows 8.

Netwerkprofielen**Netwerkprofielen**

Windows Firewall blokkeert ongeautoriseerde toegang tot uw computer door programma's en apps op basis van drie netwerklocatieprofielen:

- **Particulier netwerk:** voor netwerken thuis of op kantoor
- **Openbaar netwerk:** voor netwerken op openbare plekken
- **Domeinnetwerk:** voor netwerken met een domeincontroller

U kunt deze profielen beheren via de configuratie van uw Avira-product onder **Internetbescherming > Windows Firewall > Netwerkprofielen**.

Ga naar de officiële Microsoft-website voor nadere informatie over deze netwerkprofielen.

Waarschuwing

Windows Firewall hanteert dezelfde regels voor alle netwerken die tot dezelfde netwerklocatie behoren; dat wil zeggen dat wanneer u een programma of toepassing toestaat, dit programma of deze toepassing ook toegang verkrijgt in alle netwerken die hetzelfde profiel hebben.

Particulier netwerk

Particulier netwerk-instellingen

De particulier netwerk-instellingen beheren de toegang van andere computers of apparaten tot uw computer in uw netwerk thuis of op kantoor. Deze instellingen staan standaard toe dat de gebruikers van het particuliere netwerk uw computer zien en daartoe toegang hebben.

Inschakelen

Als deze optie wordt ingeschakeld, wordt de Windows Firewall geactiveerd en functioneert deze via het Avira-product.

Alle inkomende verbindingen blokkeren

Als deze optie wordt ingeschakeld, wijst Windows Firewall alle ongevraagde pogingen om verbinding te maken met uw computer af, inclusief de inkomende verbindingen van toegestane toepassingen.

Informeer mij als een nieuwe app geblokkeerd is

Als deze optie is ingeschakeld, krijgt u elke keer dat Windows Firewall een nieuw programma of een nieuwe app blokkeert een melding.

Uitschakelen (niet aanbevolen)

Als deze optie wordt ingeschakeld, wordt de Windows Firewall gedeactiveerd. Deze optie wordt niet aanbevolen; het levert risico's op voor uw computer.

Openbaar netwerk

Openbaar netwerk-instellingen

De openbaar netwerk-instellingen beheren de toegang van andere computers of apparaten tot uw computer in netwerken op openbare plekken. Deze instellingen staan

niet standaard toe dat de gebruikers van het openbare netwerk uw computer zien of daartoe toegang hebben.

Inschakelen

Als deze optie wordt ingeschakeld, wordt de Windows Firewall geactiveerd en functioneert deze via het Avira-product.

Alle inkomende verbindingen blokkeren

Als deze optie wordt ingeschakeld, wijst Windows Firewall alle ongevraagde pogingen om verbinding te maken met uw computer af, inclusief de inkomende verbindingen van toegestane toepassingen.

Informeer mij als een nieuwe app geblokkeerd is

Als deze optie is ingeschakeld, krijgt u elke keer dat Windows Firewall een nieuw programma of een nieuwe app blokkeert een melding.

Uitschakelen (niet aanbevolen)

Als deze optie wordt ingeschakeld, wordt de Windows Firewall gedeactiveerd. Deze optie wordt niet aanbevolen; het levert risico's op voor uw computer.

Domeinnetwerk

Domeinnetwerk-instellingen

De domeinnetwerk-instellingen beheren de toegang van andere computers of apparaten tot uw computer in een netwerk dat via een domeincontroller authenticaceert. Deze instellingen staan standaard toe dat geauthenticeerde gebruikers van het domein uw computer zien of daartoe toegang hebben.

Inschakelen

Als deze optie wordt ingeschakeld, wordt de Windows Firewall geactiveerd en functioneert deze via het Avira-product.

Alle inkomende verbindingen blokkeren

Als deze optie wordt ingeschakeld, wijst Windows Firewall alle ongevraagde pogingen om verbinding te maken met uw computer af, inclusief de inkomende verbindingen van toegestane toepassingen.

Informeer mij als een nieuwe app geblokkeerd is

Als deze optie is ingeschakeld, krijgt u elke keer dat Windows Firewall een nieuw programma of een nieuwe app blokkeert een melding.

Uitschakelen (niet aanbevolen)

Als deze optie wordt ingeschakeld, wordt de Windows Firewall gedeactiveerd. Deze optie wordt niet aanbevolen; het levert risico's op voor uw computer.

Let op

Deze optie is alleen beschikbaar als uw computer verbonden is met een netwerk met domeincontroller.

Toepassingsregels

Als u de link onder **Windows Firewall > Toepassingsregels** aanklikt, gaat u terug naar het menu **Toegestane apps en onderdelen** van de Windows Firewall configuratie.

Geavanceerde instellingen

Als u de link onder **Windows Firewall > Geavanceerde instellingen** aanklikt, gaat u terug naar het menu **Windows Firewall met geavanceerde beveiliging** van de Windows Firewall configuratie.

9.6 Web Protection

De sectie **Web Protection** onder **Configuratie > Internetbeveiliging** is verantwoordelijk voor de configuratie van de webbeveiliging.

9.6.1 Scan

Web Protection beschermt u tegen virussen of malware die uw computer bereiken door webpagina's die u in uw webbrowser laadt vanaf internet. De **Scan**-opties kunnen gebruikt worden om het gedrag van de Web Protection-component in te stellen

Scan

IPv6-ondersteuning inschakelen

Is deze optie ingeschakeld, dan wordt Internet Protocol versie 6 ondersteund door Web Protection. Deze optie is niet beschikbaar voor nieuwe of gewijzigde installaties onder Windows 8.

Drive-by-bescherming

Drive-by-bescherming geeft u de mogelijkheid om instellingen te maken om I-Frames, ook bekend als inline-frames, te blokkeren. I-Frames zijn HTML-elementen, d.w.z. elementen van internetpagina's die een gebied van een webpagina afbakenen. I-Frames kunnen worden gebruikt om verschillende webinhoud te laden en weer te geven - meestal andere URL's - als onafhankelijke documenten in een subvenster van de browser. I-Frames worden meestal gebruikt voor banners. In sommige gevallen worden I-Frames gebruikt om

malware te verbergen. In deze gevallen is het I-Frame-gebied meestal onzichtbaar of bijna onzichtbaar in de browser. De optie **Blokkeer verdachte I-frames** geeft u de mogelijkheid om I-Frames te controleren en te blokkeren.

Verdachte I-frames blokkeren

Als deze optie is ingeschakeld, worden I-Frames op de door u aangevraagde webpagina 's gescand volgens bepaalde criteria. Als er verdachte I-Frames zijn op een aangevraagde webpagina, wordt de I-Frame geblokkeerd. Een foutmelding wordt weergegeven in het I-Frame-venster.

Actie bij detectie

U kunt de acties definiëren die Web Protection moet uitvoeren als een virus of ongewenst programma wordt gedetecteerd.

Interactief

Als deze optie is ingeschakeld, verschijnt er een dialoogvenster wanneer een virus of ongewenst programma wordt gedetecteerd tijdens een scan op aanvraag, waarin u kunt kiezen wat er moet gebeuren met het getroffen bestand. Deze optie wordt ingeschakeld als de standaardinstelling.

Voortgangsbalk weergeven

Als deze optie is ingeschakeld, verschijnt er een bureaubladmededeling met een downloadvoortgangsbalk als het downloaden van website-inhoud een time-out van 20 seconden overschrijdt. Deze bureaubladmededeling is specifiek ontworpen voor het downloaden van websites met grotere gegevensvolumes: als u surft met Web Protection wordt website-inhoud niet stapsgewijs gedownload in de internetbrowser, omdat die inhoud wordt gescand op virussen en malware voordat hij wordt weergegeven in de internetbrowser. Deze optie is uitgeschakeld als standaardinstelling.

Klik [hier](#) voor meer informatie.

Automatisch

Wanneer deze optie is ingeschakeld, verschijnt er geen dialoogvenster bij de detectie van een virus. Web Protection reageert volgens de instellingen die u vooraf definieert in dit gedeelte als primaire en secundaire actie.

Primaire actie

De primaire actie is de actie die wordt uitgevoerd wanneer Web Protection een virus of ongewenst programma vindt.

Toegang weigeren

De door de webserver opgevraagde website en/of willekeurige gegevens of bestanden die worden verplaatst, worden niet naar uw webbrowserserver verstuurd. Een foutmelding om u te informeren dat de toegang is geweigerd, wordt weergegeven in de webbrowsers. Web Protection slaat de detectie op in het rapportbestand als de [rapportfunctie](#) is geactiveerd.

Naar quarantaine verplaatsen

Als er een virus of malware wordt gedetecteerd, worden de door de webserver opgevraagde website en/of de overgedragen gegevens en bestanden in quarantaine geplaatst. Het getroffen bestand kan worden teruggehaald uit de quarantaine-manager wanneer het een informatieve waarde heeft of - indien nodig - naar het Avira Malware Research Center worden gestuurd.

Negeren

De door de webserver opgevraagde website en/of willekeurige gegevens of bestanden die werden verplaatst, worden door Web Protection doorgestuurd naar uw webbrowswer. Toegang tot het bestand is toegestaan en het bestand wordt genegeerd.

Waarschuwing

Het aangetaste bestand blijft actief op uw werkstation! Het kan ernstige schade aan uw werkstation veroorzaken!

Geblokkeerde aanvragen

Bij **Geblokkeerde aanvragen** kunt u aangeven welke bestands- en MIME-types (inhoudstypes voor de overgedragen gegevens) moeten worden geblokkeerd door Web Protection. Met de Webfilter kunt u bekende phishing- en malware-URL's blokkeren. Web Protection voorkomt overdracht van gegevens van het internet naar uw computersysteem.

Web Protection blokkeert de volgende bestandstypes / MIME-types

Alle bestands- en MIME-types (inhoudstypes voor de overgedragen gegevens) in de lijst worden door Web Protection geblokkeerd.

Input-box

Geef in dit invoervak de namen in van de MIME- en bestandstypes waarvan u wilt dat Web Protection deze blokkeert. Voer voor bestandstypes de extensie in, bijv. **.htm**. Geef voor MIME-types het mediatype en, indien van toepassing, het subtype aan. De twee instructies worden van elkaar gescheiden door een slash, bijv. **video/mpeg** of **audio/x-wav**.

Let op

Bestanden die al op uw systeem zijn opgeslagen als tijdelijke internetbestanden en zijn geblokkeerd door Web Protection, kunnen echter plaatselijk van internet worden gedownload door de internetbrowser van uw computer. Tijdelijke internetbestanden zijn bestanden die op uw computer worden opgeslagen door de internetbrowser zodat websites sneller benaderd kunnen worden.

Let op

De items op de lijst van geblokkeerde bestands- en MIME-types worden genegeerd, als deze voorkomen op de lijst van uitgesloten bestands- en MIME-types onder [Web Protection > Scan > Uitzonderingen](#).

Let op

Gebruik geen jokertekens (* voor een willekeurig aantal tekens, of ? voor een enkel teken) bij het invoeren van bestandstypes en MIME-types.

MIME-types: voorbeelden van mediatypes:

- `text` = voor tekstbestanden
- `image` = voor grafische bestanden
- `video` = voor video bestanden
- `audio` = voor audiobestanden
- `application` = voor bestanden die aan een specifiek programma gekoppeld zijn

Voorbeelden van uitgesloten bestands- en MIME-types

- `application/octet-stream` = `application/octet-stream` MIME-bestandstypes (uitvoerbare bestanden `*.bin`, `*.exe`, `*.com`, `*.dll`, `*.class`) worden geblokkeerd door Web Protection.
- `application/olescript` = `application/olescript` MIME-bestandstypes (ActiveX-scriptbestanden `*.axs`) worden geblokkeerd door Web Protection.
- `.exe` = alle bestanden met de extensie `.exe` (uitvoerbare bestanden) worden geblokkeerd door Web Protection.
- `.msi` = alle bestanden met de extensie `.msi` (Windows-installatiebestanden) worden geblokkeerd door Web Protection.

Toevoegen

Met deze knop kunt u MIME- en bestandstypes kopiëren van het invoerveld naar het weergavevenster.

Verwijderen

De knop verwijdert een geselecteerd item uit de lijst. De knop is inactief als er geen item is geselecteerd.

Webfilter

De webfilter is gebaseerd op een interne database die dagelijks wordt geüpdatet en URL's op basis van inhoud rangschikt.

Webfilter activeren

Als de optie is ingeschakeld, worden alle URL's die overeenkomen met de geselecteerde categorieën in de webfilter, geblokkeerd.

Webfilterlijst

In de webfilterlijst kunt u de inhoudscategorieën selecteren waarvan de URL's moeten worden geblokkeerd door Web Protection.

Let op

De webfilter wordt genegeerd voor invoer in de lijst van uitgesloten URL's onder [Web Protection > Scan > Uitzonderingen](#).

Let op

Spam-URL's zijn URL's verzonden met spam-e-mails. De categorie **Fraude / Misleiding** gaat in op webpagina's met "Abonnement verloopt" en andere aanbiedingen van diensten waarvan de kosten door de provider worden verborgen.

Uitzonderingen

Met deze opties kunt u uitzonderingen instellen op basis van MIME-types (inhoudstypes voor de overgedragen gegevens) en bestandstypes voor URL's (internetadressen) om te worden gescand door Web Protection. Web Protection negeert de ingestelde MIME-types en URL's, d.w.z. dat de gegevens niet op virussen en malware worden gescand bij de overdracht naar uw computersysteem.

MIME-types die Web Protection overslaat

In dit veld kunt u MIME-types (inhoudstypes van overgedragen gegevens) selecteren die Web Protection moet negeren tijdens het scannen.

Bestandstypes/MIME-types, overgeslagen door Web Protection (gebruikersgedefinieerd)

Alle MIME-types (inhoudstypes van overgedragen gegevens) uit de lijst worden door Web Protection tijdens het scannen genegeerd.

Input-box

In dit vak kunt u de naam van MIME-types en bestandstypes invoeren die Web Protection moet negeren tijdens het scannen. Voer voor bestandstypes de extensie in, bijv. **.htm**. Geef voor MIME-types het mediatype en, indien van toepassing, het subtype aan. De twee instructies worden van elkaar gescheiden door een slash, bijv. **video/mpeg** of **audio/x-wav**.

Let op

Gebruik geen jokertekens (* voor een willekeurig aantal tekens, of ? voor een enkel teken) bij het invoeren van bestandstypes en MIME-types.

Waarschuwing

Alle bestandstypes en inhoudstypes op de lijst met uitzonderingen worden naar de internetbrowser gedownload zonder verder scannen van geblokkeerde aanvragen (lijst van te blokkeren bestands- en MIME-types in [Web Protection > Scan > Geblokkeerde aanvragen](#)) of door Web Protection: voor alle items op de lijst van uitzonderingen, worden de items op de lijst met geblokkeerde bestands- en MIME-types, genegeerd. Er wordt geen scan uitgevoerd op virussen en malware.

MIME-types: voorbeelden van mediatypes:

- `text` = voor tekstbestanden
- `image` = voor grafische bestanden
- `video` = voor video bestanden
- `audio` = voor audiobestanden
- `application` = voor bestanden die aan een specifiek programma gekoppeld zijn

Voorbeelden van uitgesloten bestands- en MIME-types:

- `audio/` = Alle bestandstypes van het soort audio/media worden uitgesloten van Web Protection-scans
- `video/quicktime` = Alle Quicktime subtype-videobestanden (*.qt, *.mov) worden uitgesloten van Web Protection-scans
- `.pdf` = Alle Adobe PDF-bestanden worden uitgesloten van Web Protection-scans.

Toevoegen

Met deze knop kunt u MIME- en bestandstypes kopiëren van het invoerveld naar het weergavevenster.

Verwijderen

De knop verwijdert een geselecteerd item uit de lijst. De knop is inactief als er geen item is geselecteerd.

URL's die Web Protection overslaat

Alle URL's van deze lijst worden uitgesloten van Web Protection-scans.

Input-box

Voer in dit vak URL's in (internetadressen) die moeten worden uitgesloten bij Web Protection-scans, bijv. `www.domeinnaam.com`. U kunt delen van de URL specificeren, door met voorafgaande en volgende punt-teken het domeinniveau aan te geven: `.domainname.com` voor alle pagina's en alle subdomeinen van het domein. Geef websites met een willekeurig topdomein (`.com` of `.net`) aan met een punt-teken er achter: `domainname.`. Als u een tekenreeks zonder punt-teken ervoor of erachter opgeeft, wordt de tekenreeks geïnterpreteerd als een topdomein, bijv. `net` voor alle NET-domeinen (`www.domain.net`).

Let op

U kunt ook het jokerteken `*` gebruiken voor elk willekeurig aantal tekens bij het opgeven van URL's. U kunt ook voorafgaande en volgende punt-teken gebruiken in combinatie met jokertekens om het domeinniveau aan te geven:

`.domainname.*`

`*.domainname.com`

`.*name*.com` (geldig maar niet aan te raden)

specificaties zonder punt-teken zoals `*name*`, worden geïnterpreteerd als deel van een topdomein en worden afgeraden.

Waarschuwing

Alle websites op de lijst met uitgezonderde URL's worden naar de internetbrowser gedownload zonder verder scannen door de webfilter of door Web Protection: voor alle items op de lijst van uitgesloten URL's, worden de items van de webfilter (zie [Web Protection > Scan > Geblokkeerde aanvragen](#)) genegeerd. Er wordt geen scan uitgevoerd op virussen en malware. Sluit daarom alleen betrouwbare URL's uit van Web Protection-scans.

Toevoegen

Met deze knop kunt u de URL (internetadres) kopiëren van het invoerveld naar het weergavevenster.

Verwijderen

De knop verwijdert een geselecteerd item uit de lijst. De knop is inactief als er geen item is geselecteerd.

Voorbeelden: overgeslagen URL's

- `www.avira.com -OF- www.avira.com/*`
= Alle URL's met het domein `www.avira.com` worden uitgesloten van Web Protection-scans: `www.avira.com/en/pages/index.php`, `www.avira.com/en/support/index.html`, `www.avira.com/en/download/index.html`, enz. URL's met het domein `www.avira.nl` worden niet uitgesloten van Web Protection-scans.

- `avira.com -OF- *.avira.com`
= Alle URL's met het tweede en topdomein `avira.com` worden uitgesloten van Web Protection-scans: de specificatie omvat alle bestaande subdomeinen voor `.avira.com`: `www.avira.com`, `forum.avira.com`, enz.
- `avira. -OF- *.avira.*`
= Alle URL's met het domein van het tweede niveau `avira` worden uitgesloten van Web Protection-scans: de specificatie omvat alle bestaande top- of subdomeinen voor `.avira`: `www.avira.com`, `www.avira.nl`, `forum.avira.com`, enz.
- `.*domain*.*`
Alle URL's die een domein van het tweede niveau bevatten met de tekenreeks `domain` worden uitgesloten van Web Protection-scans: `www.domain.com`, `www.new-domain.de`, `www.sample-domain1.de`, ...
- `net -OF- *.net`
= Alle URL's met het topdomein `net` worden uitgesloten van Web Protection-scans: `www.name1.net`, `www.name2.net`, enz.

Waarschuwing

Voer de URL's die u wilt uitsluiten van Web Protection-scans, zo nauwkeurig mogelijk in. Vermijd het opgeven van een volledig topdomein of delen van een domein van het tweede niveau, omdat het risico bestaat dat internetpagina's die malware en ongewenste programma's verspreiden, uitgesloten worden van Web Protection-scans op basis van algemene specificaties en uitzonderingen. We raden u aan om tenminste het volledige domein van het tweede niveau en het topdomein op te geven: `domainname.com`

Heuristiek

Dit configuratiegedeelte bevat de instellingen voor de heuristiek van de scan-engine.

Avira-producten bevatten zeer krachtige heuristieken die proactief onbekende malware kunnen detecteren, d.w.z. voordat een speciale virusdefinitie ter bestrijding van het schadelijke element is gecreëerd en voordat een update van de controle op virussen is verzonden. Virusdetectie omvat een uitgebreide analyse en onderzoek van de geïnfecteerde codes voor functies die kenmerkend zijn voor malware. Indien de code die gescand wordt deze kenmerken vertoont, wordt hij gerapporteerd als verdacht. Dit betekent niet per se dat de code inderdaad malware is. Soms doen zich valse positieven voor. De beslissing over de wijze van behandeling van de geïnfecteerde code moet door de gebruiker worden genomen, bijv. op basis van zijn of haar kennis van de vraag of de bron van de code betrouwbaar is of niet.

Macrovirus-heuristiek

Uw Avira-product bevat een zeer krachtige macrovirus-heuristiek. Als deze optie is ingeschakeld, worden alle macro's in het betreffende document gewist in geval van een reparatie, in het andere geval worden verdachte documenten alleen

gerapporteerd, d.w.z. dat u een waarschuwing ontvangt. Deze optie is ingeschakeld als standaardinstelling en wordt aanbevolen.

Advanced Heuristic Analysis and Detection (AHeAD)

AHeAD inschakelen

Uw Avira-programma bevat een zeer krachtige heuristiek in de vorm van Avira-AHeAD-technologie, die ook onbekende (nieuwe) malware kan detecteren. Als deze optie is ingeschakeld, kunt u vastleggen hoe "agressief" deze heuristiek moet zijn. Deze optie wordt ingeschakeld als de standaardinstelling.

Laag detectieniveau

Als deze optie is ingeschakeld, wordt iets minder onbekende malware gedetecteerd; de kans op een vals alarm is in dat geval laag.

Gemiddeld detectieniveau

Deze optie combineert een sterk detectieniveau met een laag risico op vals alarm. De standaardinstelling is medium indien u heeft gekozen voor gebruik van deze heuristiek.

Hoog detectieniveau

Als deze optie is ingeschakeld, wordt aanzienlijk meer onbekende malware gedetecteerd, maar dan is er waarschijnlijk ook sprake van valse positieven.

9.6.2 Rapport

Web Protection omvat een uitgebreide logboekregistratiefunctie om de gebruiker of administrator exacte notities te geven over het type en de manier van een detectie.

Rapporteren

Met deze groep kunt u de inhoud van het rapportbestand bepalen.

Uit

Als deze optie is ingeschakeld, creëert Web Protection geen logboekregistratie. We raden aan om de logboekregistratiefunctie alleen in uitzonderlijke gevallen uit te schakelen, bijvoorbeeld bij het uitvoeren van testen met meerdere virussen of ongewenste programma's.

Standaard

Als deze optie is ingeschakeld, registreert Web Protection belangrijke informatie (over detecties, waarschuwingen en fouten) in het rapportbestand, en minder belangrijke informatie wordt genegeerd voor meer helderheid. Deze optie is ingeschakeld als standaardinstelling.

Geavanceerd

Als deze optie is ingeschakeld, registreert Web Protection ook minder belangrijke informatie in het rapportbestand.

Volledig

Als deze optie is ingeschakeld, registreert Web Protection alle beschikbare informatie in het rapportbestand, inclusief bestandsgrootte, bestandstype, datum, enz.

Rapportbestand beperken

Grootte beperken tot n MB

Als deze optie is ingeschakeld, kan het rapportbestand beperkt worden tot een zekere grootte; mogelijke waarden: toegestane waarden liggen tussen 1 en 100 MB. Ongeveer 50 kilobytes extra ruimte wordt toegestaan bij de beperking van het rapportbestand om het gebruik van de systeembronnen zo laag mogelijk te houden. Als het rapportbestand de geïndiceerde grootte met meer dan 50 kilobytes overschrijdt, worden oude invoeren verwijderd totdat de geïndiceerde grootte verminderd is met 20 %.

Configuratiebestand in rapportbestand schrijven

Als deze optie is ingeschakeld, wordt de configuratie van de on-access-scan in het rapportbestand geregistreerd.

Let op

Als u geen rapportbestandsbeperking heeft ingesteld, wordt oude invoer automatisch verwijderd als het rapportbestand een grootte van 100 MB bereikt. Bestanden worden gewist tot de grootte van het rapportbestand 80 MB is.

9.7 Mail Protection

De sectie **Mail Protection** onder Configuratie is verantwoordelijk voor de configuratie van de Mail Protection.

9.7.1 Scan

Gebruik Mail Protection om inkomende e-mails op virussen, malware te scannen. Uitgaande e-mails kunt u met Mail Protection scannen op virussen en malware. Uitgaande e-mails bestaande uit spam, gestuurd vanaf een onbekende **bot** op uw computer, kunnen door Mail Protection worden geblokkeerd om spam te voorkomen.

Inkomende e-mails scannen

Wanneer deze optie is ingeschakeld, worden inkomende e-mails gescand op virussen, malware en. Mail Protection ondersteunt POP3- en IMAP-protocollen. Schakel de

inbox-account in die uw e-mailclient gebruikt om e-mails te ontvangen die moeten worden gecontroleerd door Mail Protection.

POP3-accounts bewaken

Wanneer deze optie is ingeschakeld, worden POP3-accounts op de opgegeven poorten bewaakt.

Bewaakte poorten

Geef in dit veld de poort op die als vak voor inkomende berichten onder het POP3-protocol moet worden gebruikt. Meerdere poorten worden gescheiden door komma's.

Standaard

Deze knop stelt de opgegeven poort opnieuw in op de standaard POP3-poort.

IMAP-accounts bewaken

Wanneer deze optie is ingeschakeld, worden de IMAP-accounts bewaakt op de opgegeven poorten.

Bewaakte poorten

Geef in dit veld de poort op die als vak voor inkomende berichten onder het IMAP-protocol moet worden gebruikt. Meerdere poorten worden gescheiden door komma's.

Standaard

Deze knop stelt de opgegeven poort opnieuw in op de standaard IMAP-poort.

Uitgaande e-mails scannen (SMTP)

Als deze optie is ingeschakeld, worden uitgaande e-mails gescand op virussen en malware. Spam-e-mails van onbekende bots worden geblokkeerd.

Bewaakte poorten

Geef in dit veld de poort op die als vak voor uitgaande berichten onder het SMTP-protocol moet worden gebruikt. Meerdere poorten worden gescheiden door komma's.

Standaard

Deze knop stelt de opgegeven poort opnieuw in op de standaard SMTP-poort.

Let op

Kijk de instellingen van uw e-mailaccounts in uw e-mailclientprogramma na om de gebruikte protocollen en poorten te verifiëren. Meestal worden standaardpoorten gebruikt.

IPv6-ondersteuning inschakelen

Als deze optie is ingeschakeld, wordt Internet Protocol versie 6 ondersteund door Mail Protection. (Deze optie is niet beschikbaar voor nieuwe of gewijzigde installaties onder Windows 8.)

Actie bij detectie

Dit configuratiegedeelte bevat instellingen voor acties die worden uitgevoerd wanneer Mail Protection een virus of ongewenst programma vindt in een e-mail of in een bijlage.

Let op

Deze acties worden zowel uitgevoerd wanneer een virus wordt gedetecteerd in inkomende e-mails als wanneer een virus wordt gedetecteerd in uitgaande e-mails.

Interactief

Als deze optie is ingeschakeld, verschijnt er een dialoogvenster wanneer een virus of ongewenst programma wordt gedetecteerd in een e-mail of bijlage, waarin u kunt kiezen wat er moet gebeuren met de betreffende e-mail of bijlage. Deze optie wordt ingeschakeld als de standaardinstelling.

Voortgangsbalk weergeven

Als deze optie is ingeschakeld, toont de Mail Protection een voortgangsbalk tijdens het downloaden van e-mails. Deze optie kan alleen worden ingeschakeld wanneer de optie "**Interactief**" is geselecteerd.

Automatisch

Wanneer deze optie is ingeschakeld, wordt u niet meer geïnformeerd als er een virus of ongewenst programma is gevonden. Mail Protection reageert volgens de instellingen die u definieert in dit gedeelte.

Geïnfecteerde e-mails

De gekozen actie voor "*Geïnfecteerde e-mails*" wordt uitgevoerd wanneer Mail Protection een virus of ongewenst programma in een e-mail vindt. Wanneer de optie "**Negeren**" is geselecteerd is het ook mogelijk onder "*Geïnfecteerde bijlagen*" het proces te selecteren voor de behandeling van een virus of ongewenst programma dat in een bijlage is gedetecteerd.

Verwijderen

Wanneer deze optie is ingeschakeld, wordt de geïnfecteerde e-mail automatisch verwijderd als er een virus of een ongewenst programma is gevonden. De body van de e-mail wordt vervangen door de [standaardtekst](#), zoals hieronder weergegeven. Hetzelfde is van toepassing op alle aangehechte bijlagen; deze worden eveneens vervangen door een [standaardtekst](#).

Negeren

Wanneer deze optie is ingeschakeld, wordt de geïnfecteerde e-mail genegeerd, ondanks de detectie van een virus of een ongewenst programma. U kunt echter beslissen wat er moet gebeuren met de geïnfecteerde bijlage.

Naar quarantaine verplaatsen

Wanneer deze optie is ingeschakeld, wordt de gehele e-mail, inclusief alle bijlagen, in [Quarantaine](#) geplaatst als er een virus of een ongewenst programma is gevonden. Desgewenst kan deze later worden teruggezet. De geïnfekteerde mail zelf wordt verwijderd. De body van de e-mail wordt vervangen door de [standaardtekst](#), zoals hieronder weergegeven. Hetzelfde is van toepassing op alle aangehechte bijlagen; deze worden eveneens vervangen door een [standaardtekst](#).

Getroffen bijlagen

De optie "*Geïnfekteerde bijlagen*" kan alleen worden geselecteerd wanneer de instelling "**Negeren**" is geselecteerd onder "*Geïnfekteerde bijlagen*". Met deze optie is het nu mogelijk te bepalen wat er moet worden gedaan wanneer er een virus of ongewenst programma in een bijlage is gevonden.

Verwijderen

Wanneer deze optie is ingeschakeld, wordt de geïnfekteerde bijlage verwijderd als er een virus of een ongewenst programma is gevonden en vervangen door een [standaardtekst](#).

Negeren

Wanneer deze optie is ingeschakeld, wordt de bijlage genegeerd en afgeleverd, ondanks de detectie van een virus of een ongewenst programma.

Waarschuwing

Wanneer u deze optie selecteert, heeft u geen bescherming tegen virussen en ongewenste programma's door Mail Protection. Selecteer dit item alleen wanneer u er zeker van bent wat u doet. Schakel de preview in uw e-mail-programma uit, open nooit bijlagen met dubbelklikken!

Naar quarantaine verplaatsen

Wanneer deze optie is ingeschakeld, wordt de geïnfekteerde bijlage verplaatst naar [Quarantaine](#) en vervolgens verwijderd (vervangen door een [standaardtekst](#)). Desgewenst kan/kunnen de geïnfekteerde bijlage(n) later worden teruggezet.

Verdere acties

Dit configuratiegedeelte bevat aanvullende instellingen voor acties die worden uitgevoerd wanneer Mail Protection een virus of ongewenst programma vindt in een e-mail of in een bijlage.

Let op

Deze acties worden uitsluitend uitgevoerd wanneer een virus wordt gedetecteerd in inkomende e-mails.

Standaardtekst voor verwijderde en verplaatste e-mails

De tekst in dit vak wordt ingevoegd in de e-mail als bericht in plaats van de geïnficeerde e-mail. U kunt dit bericht bewerken. Een tekst kan maximaal 500 tekens bevatten.

U kunt gebruik maken van de volgende toetsencombinatie voor de opmaak:

Ctrl + Enter = voegt een regeleinde in.

Standaard

De knop voegt een vooraf gedefinieerde standaardtekst in in het invoervak.

Standaardtekst voor verwijderde en verplaatste bijlagen

De tekst in dit vak wordt ingevoegd in de e-mail als bericht in plaats van de geïnficeerde bijlage. U kunt dit bericht bewerken. Een tekst kan maximaal 500 tekens bevatten.

U kunt gebruik maken van de volgende toetsencombinatie voor de opmaak:

Ctrl + Enter = voegt een regeleinde in.

Standaard

De knop voegt een vooraf gedefinieerde standaardtekst in in het invoervak.

Heuristiek

Dit configuratiegedeelte bevat de instellingen voor de heuristiek van de scan-engine.

Avira-producten bevatten zeer krachtige heuristieken die proactief onbekende malware kunnen detecteren, d.w.z. voordat een speciale virusdefinitie ter bestrijding van het schadelijke element is gecreëerd en voordat een update van de controle op virussen is verzonden. Virusdetectie omvat een uitgebreide analyse en onderzoek van de geïnficeerde codes voor functies die kenmerkend zijn voor malware. Indien de code die gescand wordt deze kenmerken vertoont, wordt hij gerapporteerd als verdacht. Dit betekent niet per se dat de code inderdaad malware is. Soms doen zich valse positieven voor. De beslissing over de wijze van behandeling van de geïnficeerde code moet door de gebruiker worden genomen, bijv. op basis van zijn of haar kennis van de vraag of de bron van de code betrouwbaar is of niet.

Macrovirus-heuristiek

Uw Avira-product bevat een zeer krachtige macrovirus-heuristiek. Als deze optie is ingeschakeld, worden alle macro's in het betreffende document gewist in geval van een reparatie, in het andere geval worden verdachte documenten alleen gerapporteerd, d.w.z. dat u een waarschuwing ontvangt. Deze optie is ingeschakeld als standaardinstelling en wordt aanbevolen.

Advanced Heuristic Analysis and Detection (AHeAD)

AHeAD inschakelen

Uw Avira-programma bevat een zeer krachtige heuristiek in de vorm van Avira-AHeAD-technologie, die ook onbekende (nieuwe) malware kan detecteren. Als deze optie is ingeschakeld, kunt u vastleggen hoe "agressief" deze heuristiek moet zijn. Deze optie wordt ingeschakeld als de standaardinstelling.

Laag detectieniveau

Als deze optie is ingeschakeld, wordt iets minder onbekende malware gedetecteerd; de kans op een vals alarm is in dat geval laag.

Gemiddeld detectieniveau

Deze optie combineert een sterk detectieniveau met een laag risico op vals alarm. De standaardinstelling is medium indien u heeft gekozen voor gebruik van deze heuristiek.

Hoog detectieniveau

Als deze optie is ingeschakeld, wordt aanzienlijk meer onbekende malware gedetecteerd, maar dan is er waarschijnlijk ook sprake van valse positieven.

AntiBot

De functie AntiBot van Mail Protection voorkomt dat uw computer onderdeel wordt van een zogenaamd **bot-net** en wordt gebruikt om spam-e-mails te versturen: om spam te verzenden via een bot-net, infecteert een aanvaller meestal een aantal computers met een bot die vervolgens verbinding maakt met een IRC-server, dan een bepaald kanaal opent en wacht op het commando om de spam e-mails te sturen. Om spam-e-mails van een onbekende bot te onderscheiden van echte e-mails, controleert Mail Protection of de SMTP-server en de e-mailafzender van een uitgaande e-mail zijn opgenomen in de lijsten van toegestane servers en afzenders. Indien dit niet het geval is, worden uitgaande emails geblokkeerd, d.w.z. de e-mail wordt niet verzonden. De geblokkeerde e-mail wordt weergegeven in een dialoogvenster.

Let op

De functie AntiBot kan alleen worden gebruikt als de Mail Protection-scan van uitgaande e-mails is ingeschakeld (zie de optie **Uitgaande e-mails scannen** onder [Mail Protection > Scannen](#)).

Toegestane servers

Alle servers in deze lijst worden geautoriseerd door Mail Protection om e-mails te versturen: e-mails verstuurd aan deze servers worden **niet** geblokkeerd door Mail Protection. Als er geen servers in de lijst zijn opgenomen, wordt de SMTP-server die wordt gebruikt om uitgaande e-mails te versturen, niet gescand. Als de lijst is ingevuld, blokkeert Mail Protection e-mails die worden verzonden naar een SMTP-server die niet in de lijst staat.

Input-box

Voer in dit vak de hostnaam of het IP-adres van de SMTP-server in, dat/die u gebruikt om uw e-mails te versturen.

Let op

U vindt de details van de SMTP-server die door uw e-mailprogramma wordt gebruikt voor het versturen van e-mails, in uw e-mailprogramma onder de datum dat de gebruikersaccount werd gecreëerd.

Toevoegen

U kunt deze knop gebruiken om servers toe te voegen die zijn opgegeven in het invoervak, aan de lijst van toegestane servers.

Verwijderen

Deze knop verwijdert een gemarkeerd item uit de lijst van toegestane servers. De knop is inactief als er geen item is geselecteerd.

Alles wissen

Deze knop verwijdert alle items uit de lijst van toegestane servers.

Toegestane afzender(s)

Alle verzenders in deze lijst zijn geautoriseerd door Mail Protection om e-mails te versturen: e-mails verstuurd vanaf dit e-mailadres worden **niet** geblokkeerd door Mail Protection. Als er geen afzenders in de lijst zijn opgenomen, wordt het e-mailadres dat wordt gebruikt om uitgaande e-mails te versturen, niet gescand. Als de lijst is ingevuld, blokkeert Mail Protection e-mails die worden verzonden door afzenders die niet in de lijst staan.

Input-box

Voer in dit invoervak uw e-mailzendadres in.

Toevoegen

U kunt deze knop gebruiken om verzenders toe te voegen die zijn opgegeven in het invoervak, aan de lijst van toegestane verzenders.

Verwijderen

Deze knop verwijdert een gemarkeerd item uit de lijst van toegestane verzenders. De knop is inactief als er geen item is geselecteerd.

Alles wissen

Deze knop verwijdert alle items uit de lijst van toegestane verzenders.

9.7.2 Algemeen

Uitzonderingen

Scan-uitzonderingen

Deze tabel geeft de lijst met e-mailadressen weer die zijn uitgesloten van scannen door Mail Protection (white list).

Let op

De lijst met uitzonderingen wordt uitsluitend gebruikt door Mail Protection voor inkomende e-mails.

Scan-uitzonderingen

Input-box

In dit vak voert u het e-mailadres in dat u wilt toevoegen aan de lijst met e-mailadressen die niet moeten worden gescand. Afhankelijk van uw instellingen wordt het e-mailadres in de toekomst niet langer gescand door de Mail Protection.

Toevoegen

Met deze knop kunt u het e-mailadres toevoegen dat is ingevoerd in het invoervak, aan de lijst met e-mailadressen die niet moeten worden gescand.

Verwijderen

Deze knop verwijdert een gemarkeerd e-mailadres uit de lijst.

E-mailadres

E-mail die niet langer gescand moet worden.

Malware

Wanneer deze optie is ingeschakeld, wordt het e-mailadres niet meer op malware gescand.

Omhoog

U kunt deze knop gebruiken om een gemarkeerd e-mailadres naar een hogere positie te verplaatsen. Als er geen item is gemarkeerd of het gemarkeerde adres op de eerste positie in de lijst staat, wordt deze knop niet ingeschakeld.

Omlaag

U kunt deze knop gebruiken om een gemarkeerd e-mailadres naar een lagere positie te verplaatsen. Als er geen item is gemarkeerd of het gemarkeerde adres op de laatste positie in de lijst staat, wordt deze knop niet ingeschakeld.

Cache

De Mail Protection-cache bevat gegevens over de gescande e-mails die worden weergegeven als statische gegevens in het Control Center onder **Mail Protection**.

Maximum aantal e-mails dat in de cache moet worden opgeslagen

Dit veld wordt gebruikt om het maximum aantal e-mails in te stellen dat door Mail Protection in de cache wordt opgeslagen. De oudste e-mails worden het eerst verwijderd.

Maximaal aantal dagen dat een e-mail wordt opgeslagen

De maximale opslagperiode in dagen van een e-mail wordt in dit vak ingevoerd. De e-mail wordt daarna verwijderd uit de cache.

Cache leegmaken

Klik op deze knop om de e-mails te verwijderen die zijn opgeslagen in de cache.

Voettekst

Onder **Voettekst** kunt u een e-mailvoettekst instellen die wordt weergegeven in de e-mails die u verstuurt.

Deze functie vereist het activeren van de Mail Protection-scan van uitgaande e-mails (zie optie **Scan uitgaande e-mails (SMTP)** onder [Configuratie > Mail Protection > Scan](#)). U kunt de gedefinieerde voettekst van Avira Mail Protection gebruiken om te bevestigen dat de uitgaande e-mail gescand is door een antivirusprogramma. U heeft ook de mogelijkheid om zelf tekst in te voeren voor een gebruikergedefinieerde voettekst. Als u beide voettekst-opties gebruikt, wordt de gebruikergedefinieerde tekst voorafgegaan door de Avira Mail Protection-voettekst.

Voettekst voor uitgaande e-mails

Mail Protection-voettekst bijvoegen

Wanneer deze optie is ingeschakeld, wordt de Avira Mail Protection-voettekst weergegeven onder de tekst van de verzonden e-mail. De Avira Mail Protection-voettekst bevestigt dat de verzonden e-mail is gescand op virussen en ongewenste programma's door Avira Mail Protection en niet afkomstig is van een onbekende bot. De Avira Mail Protection-voettekst bevat de volgende tekst: "*Gescand met Avira Mail Protection [productversie] [initialen en versienummer van zoekmachine] [initialen en versienummer van virusdefinitiebestand]*".

De volgende voettekst bijvoegen

Als deze optie is ingeschakeld, wordt de tekst die u in het invoervak getypt heeft, weergegeven als voettekst in verzonden e-mails.

Input-box

In dit invoervak kunt u een tekst typen die als voettekst wordt weergegeven in verzonden e-mails.

9.7.3 Rapport

De Mail Protection omvat een uitgebreide logboekregistratiefunctie om de gebruiker of administrator exacte notities te geven over het type en de manier van een detectie.

Rapporteren

Met deze groep kunt u de inhoud van het rapportbestand bepalen.

Uit

Als deze optie is ingeschakeld, creëert Mail Protection geen logboekregistratie. We raden aan om de logboekregistratiefunctie alleen in uitzonderlijke gevallen uit te schakelen, bijvoorbeeld bij het uitvoeren van testen met meerdere virussen of ongewenste programma's.

Standaard

Als deze optie is ingeschakeld, registreert Mail Protection belangrijke informatie (over detecties, waarschuwingen en fouten) in het rapportbestand, en minder belangrijke informatie wordt genegeerd voor meer helderheid. Deze optie wordt ingeschakeld als de standaardinstelling.

Uitgebreid

Als deze optie is ingeschakeld, registreert Mail Protection ook minder belangrijke informatie in het rapportbestand.

Volledig

Als deze optie is ingeschakeld, registreert Mail Protection alle informatie in het rapportbestand.

Rapportbestand beperken

Grootte beperken tot n MB

Als deze optie is ingeschakeld, kan het rapportbestand beperkt worden tot een zekere grootte; mogelijke waarden: toegestane waarden liggen tussen 1 en 100 MB. Ongeveer 50 kilobytes extra ruimte wordt toegestaan bij de beperking van het rapportbestand om het gebruik van de systeembronnen zo laag mogelijk te houden. Als het rapportbestand de geïndiceerde grootte met meer dan 50 kilobyte overschrijdt, worden oude invoeren verwijderd totdat de geïndiceerde grootte minus 50 kilobytes is bereikt.

Backup maken van rapportbestand vóór verkleinen

Als deze optie is ingeschakeld, wordt een backup gemaakt van het rapportbestand vóór verkleinen.

Configuratie naar rapportbestand schrijven

Als deze optie is ingeschakeld, wordt de Mail Protection-configuratie naar het rapportbestand geschreven.

Let op

Als u geen rapportbestandsbeperking heeft ingesteld, wordt automatisch een nieuw rapportbestand gecreëerd als het rapportbestand een grootte van 100 MB bereikt. Er wordt een backup gemaakt van het oude rapportbestand. Er kunnen maximaal drie backups van oude rapportbestanden worden opgeslagen. De oudste backups worden eerst verwijderd.

9.8 Algemeen

9.8.1 Dreigingscategorieën

Selectie van uitgebreide dreigingscategorieën

Uw Avira-product beschermt u tegen computervirussen. Afgezien daarvan kunt u scannen op basis van de volgende uitgebreide dreigingscategorieën.

- [Adware](#)
- [Adware/Spyware](#)
- [Toepassingen](#)
- [Backdoor-clients](#)
- [Dialer](#)
- [Bestanden met dubbele extensie](#)
- [Frauduleuze software](#)
- [Games](#)
- [Grappen](#)
- [Phishing](#)
- [Programma's die het privédomein schenden](#)
- [Ongebruikelijke runtime-compressie](#)

Door te klikken op het betreffende vakje wordt het geselecteerde type ingeschakeld (met vinkje) of uitgeschakeld (geen vinkje).

Alles selecteren

Als deze optie is ingeschakeld, zijn alle types ingeschakeld.

Standaardwaarden

Deze knop herstelt de vooraf gedefinieerde standaardwaarden.

Let op

Als een type is uitgeschakeld, worden bestanden die herkend worden als relevant programmatype, niet meer aangegeven. Er wordt geen melding van gemaakt in het rapportagebestand.

9.8.2 Geavanceerde bescherming

ProActiv

ProActiv inschakelen

Als deze optie is ingeschakeld, worden programma's op uw systeem bewaakt en gecontroleerd op verdachte acties. U ontvangt een bericht als typisch malware-gedrag wordt gedetecteerd. U kunt het programma blokkeren of u kunt "**Negeren**"selecteren om het programma verder te gebruiken. De bewaking wordt niet toegepast op: programma's die als betrouwbaar zijn geclassificeerd, vertrouwde en ondertekende programma's die standaard worden opgenomen in de filter toegestane applicaties, en alle programma's die u heeft toegevoegd aan het applicatiefilter voor toegestane programma's.

ProActiv beschermt u tegen nieuwe en onbekende bedreigingen waarvoor nog geen antivirusdefinities of heuristieken beschikbaar zijn. ProActiv-technologie is geïntegreerd in de Real-Time Protection-component en observeert en analyseert de uitgevoerde programma-acties. Het gedrag van het programma wordt afgezet tegen typische malware-actiepatronen: actiotype en actievolgordes. Als een programma typisch malware-gedrag vertoont, wordt dit behandeld als een virusdetectie: U kunt het programma blokkeren of de melding negeren en het programma verder gebruiken. U kunt het programma als vertrouwd classificeren en toevoegen aan het applicatiefilter voor toegestane programma's. U heeft de mogelijkheid om het programma toe te voegen aan het applicatiefilter voor geblokkeerde programma's met behulp van het commando **Altijd blokkeren**.

Het onderdeel ProActiv maakt gebruik van regelsets ontwikkeld door het Avira Malware Research Center om verdacht gedrag te identificeren. De regelsets worden door Avira-databases geleverd. ProActiv stuurt informatie over verdachte programma's naar de Avira-databases voor logboekregistratie. Tijdens de Avira-installatie heeft u de mogelijkheid om gegevensoverdracht naar de Avira-databases uit te schakelen.

Let op

ProActiv-technologie is nog niet beschikbaar voor 64-bitssystemen!

Protection Cloud

Protection Cloud inschakelen

Vingerafdrukken van alle verdachte bestanden worden verzonden naar de Protection Cloud voor dynamische online-inspectie. Uitvoerbare bestanden worden direct geïdentificeerd als schoon, geïnfected of onbekend.

De Protection Cloud fungeert als een centrale locatie om pogingen tot cyberaanvallen binnen onze gebruikersdatabase te observeren. De bestanden die op uw computer worden geopend, worden vergeleken met de vingerafdrukken van bestanden die zijn opgeslagen in de cloud. Naarmate er meer gescand wordt in de cloud, is er minder processorvermogen nodig voor de antivirusapplicatie.

Een lijst van bestandslocaties die vaak het doelwit van malware zijn, wordt gegenereerd als de taak **Snelle systeemscan** wordt uitgevoerd. De lijst bevat lopende processen, programma's die worden uitgevoerd bij het opstarten en diensten. De vingerafdruk van elk bestand wordt gegenereerd en verzonden naar de Protection Cloud die vervolgens wordt gecategoriseerd als "schoon" of "malware". Onbekende programmabestanden worden geüpload naar de Protection Cloud voor analyse.

Bevestig handmatig als u verdachte bestanden naar Avira stuurt

U kunt een lijst zien met de verdachte bestanden die moeten worden toegezonden aan de Protection Cloud en u kunt kiezen welke bestanden u wilt verzenden.

Real-time scannen van bestanden

Als deze optie is ingeschakeld, worden onbekende bestanden voor analyse naar de Protection Cloud gestuurd zodra ze worden geopend.

Geef voortgang weer voor uploads naar de Avira Protection Cloud

Een scherm geeft de volgende informatie over het (de) geüploadde bestand(en) in de vorm van een voortgangsbalk:

- bestandslocatie
- bestandsnaam
- status (uploaden/analyseren)
- resultaat (schoon/geïnfected)

Geblokkeerde toepassingen

Onder *Te blokkeren toepassingen* kunt u toepassingen invoeren die u als schadelijk beschouwt en waarvan u wilt dat Avira ProActiv ze standaard blokkeert. De toegevoegde

toepassingen kunnen niet worden uitgevoerd op uw computersysteem. U kunt ook programma's toevoegen aan de applicatiefilter voor het blokkeren door Real-Time Protection van mededelingen over verdacht programmagedrag, door het selecteren van de **Dit programma altijd blokkeren**-optie.

Te blokkeren toepassingen

Toepassing

De lijst omvat alle toepassingen die u geklasseerd heeft als schadelijk en heeft ingevoerd via de configuratie of door melding aan het ProActiv-onderdeel. Avira ProActiv blokkeert de toepassingen op de lijst en deze kunnen niet worden uitgevoerd op uw computersysteem. Een bericht van het besturingssysteem verschijnt als een geblokkeerd programma opstart. Avira ProActiv herkent de te blokkeren toepassingen op basis van het opgegeven pad en de bestandsnaam en ze worden geblokkeerd ongeacht hun inhoud.

Input-box

Voer in dit vak de toepassing in die u wilt blokkeren. Teneinde de toepassing te identificeren, dient u het volledige pad, de bestandsnaam en de bestandsextensie op te geven. Het pad moet hetzij het station vermelden waarop de applicatie zich bevindt, hetzij beginnen met een omgevingsvariabele.



De knop opent een venster waarin u de te blokkeren toepassing kunt selecteren.

Toevoegen

Met de knop "**Toevoegen**" kunt u de toepassing die is opgegeven in het invoervak overbrengen naar de lijst te blokkeren toepassingen.

Let op

Toepassingen die nodig zijn voor het correct werken van het besturingssysteem kunnen niet worden toegevoegd.

Verwijderen

Met de knop "**Verwijderen**" kunt u een gemarkeerde toepassing verwijderen uit de lijst te blokkeren toepassingen.

Toegestane toepassingen

Het onderdeel *Toepassingen die moeten worden overgeslagen* somt de toepassingen op die uitgesloten zijn van monitoring door de ProActiv-component: ondertekende programma's in de categorie betrouwbaar en standaard inbegrepen in de lijst, alle betrouwbare toepassingen, en alle die zijn toegevoegd aan de toepassingsfilter : U kunt toegestane toepassingen toevoegen aan de lijst in Configuratie. U heeft ook de mogelijkheid om toepassingen toe te voegen aan verdacht programmagedrag via Real-

Time Protection-mededelingen, met de optie **Vertrouwd programma** in de Real-Time Protection-mededelingen.

Toepassingen die moeten worden overgeslagen

Toepassing

De lijst bevat toepassingen die zijn uitgesloten van controle door de ProActiv-component. In de standaard installatie-instellingen, bevat de lijst ondertekende toepassingen van betrouwbare leveranciers. U heeft de optie om toepassingen toe te voegen waarvan u vindt dat ze betrouwbaar zijn, hetzij via de configuratie, hetzij via Real-Time Protection-mededelingen. De ProActiv-component identificeert toepassingen op basis van het pad, de bestandsnaam en de inhoud. We raden aan dat het controleren van de inhoud als malware, kan worden toegevoegd aan een programma, door wijzigingen zoals updates. U kunt bepalen of er een inhoudscontrole moet worden uitgevoerd van het gespecificeerde **Type**: Voor het type "*Inhoud*", worden de toepassingen die gespecificeerd zijn met pad en bestandsnaam, gecontroleerd op veranderingen van de bestandsinhoud vóór dat ze worden uitgesloten van bewaking door de ProActiv-component. Wanneer de bestandsinhoud is veranderd, wordt de toepassing opnieuw bewaakt door de ProActiv-component. Voor het type "*Pad*" wordt geen inhoudscontrole doorgevoerd voordat de toepassing is uitgesloten van Real-Time Protection-bewaking. Klik op het weergegeven type om het type uitsluiting te veranderen.

Waarschuwing

Gebruik het type *Pad* alleen in uitzonderingsgevallen. Door een update kan schadelijke code worden toegevoegd aan een toepassing. De oorspronkelijk onschadelijke toepassing is nu malware.

Let op

Sommige vertrouwde toepassingen, inclusief bijvoorbeeld alle toepassingscomponenten van uw Avira-product, worden standaard uitgesloten van bewaking door de ProActiv-component, ook al zijn ze niet in de lijst vermeld.

Input-box

Voer in dit vak de toepassing in die u wilt uitsluiten van bewaking door de ProActiv-component. Teneinde de toepassing te identificeren, dient u het volledige pad, de bestandsnaam en de bestandsextensie op te geven. Het pad moet hetzij het station vermelden waarop de applicatie zich bevindt, hetzij beginnen met een omgevingsvariabele.



De knop opent een venster waarin u de uit te sluiten toepassing kunt selecteren.

Toevoegen

Met de knop "**Toevoegen**" kunt u de toepassing die is opgegeven in het invoervak, overbrengen naar de lijst te blokkeren toepassingen.

Verwijderen

Met de knop "**Verwijderen**" kunt u een gemarkeerde toepassing verwijderen uit de lijst te blokkeren toepassingen.

9.8.3 Wachtwoord

U kunt uw Avira-product in [verschillende gebieden](#) met een wachtwoord beschermen. Als er een wachtwoord is verstrekt, wordt u elke keer dat u het beschermde gebied wilt openen om dit wachtwoord gevraagd.

Wachtwoord

Wachtwoord invoeren

Voer hier uw verplichte wachtwoord in. Om veiligheidsredenen veranderen de feitelijke tekens die u op deze plaats typt, in asterisken (*). Het wachtwoord kan maximaal 20 tekens bevatten. Zodra het wachtwoord is verstrekt, weigert het programma toegang als er een verkeerd wachtwoord wordt ingevoerd. Een leeg vak betekent "Geen wachtwoord".

Bevestiging

Bevestig het boven ingevoerde wachtwoord door het hier nogmaals in te voeren. Om veiligheidsredenen veranderen de feitelijke tekens die u op deze plaats typt, in asterisken (*).

Let op

Het wachtwoord is hoofdlettergevoelig!

Gebieden beschermd door wachtwoord

Uw Avira-product kan individuele gebieden met een wachtwoord beschermen. Door op het relevante vak te klikken, kan het verzoek om een wachtwoord naar believen worden in- of uitgeschakeld voor individuele gebieden.

Met wachtwoord beveiligd gebied	Functie
Control Center	Als deze optie is ingeschakeld, is het vooraf gedefinieerde wachtwoord verplicht voor het starten van het Control Center.
Real-Time Protection activeren/deactiveren	Als deze optie is ingeschakeld, is het vooraf gedefinieerde wachtwoord verplicht voor het in- of uitschakelen van Avira Real-Time Protection.
Mail Protection activeren/deactiveren	Als deze optie is ingeschakeld, is het vooraf gedefinieerde wachtwoord verplicht voor het in- of uitschakelen van Mail Protection.
Web Protection activeren/deactiveren	Als deze optie is ingeschakeld, is het vooraf gedefinieerde wachtwoord verplicht voor het in- of uitschakelen van Web Protection.
Quarantaine	Als deze optie is ingeschakeld, worden alle gebieden van de quarantinemanager die beveiligd zijn met een wachtwoord, ingeschakeld. Door op het relevante vak te klikken, kan de wachtwoordnavraag op verzoek weer worden uit- of ingeschakeld voor afzonderlijke gebieden.
Betreffende objecten herstellen	Als deze optie is ingeschakeld, is het vooraf gedefinieerde wachtwoord verplicht voor het herstellen van een object.

Betreffende objecten opnieuw scannen	Als deze optie is ingeschakeld, is het vooraf gedefinieerde wachtwoord verplicht voor het opnieuw scannen van een object.
Eigenschappen betreffende objecten	Als deze optie is ingeschakeld, is het vooraf gedefinieerde wachtwoord verplicht voor het weergeven van de eigenschappen van een object.
Betreffende objecten verwijderen	Als deze optie is ingeschakeld, is het vooraf gedefinieerde wachtwoord verplicht voor het verwijderen van een object.
E-mail sturen naar Avira	Als deze optie is ingeschakeld, is het vooraf gedefinieerde wachtwoord verplicht voor het versturen van een object naar het Avira Malware Research Center voor inspectie.
Getroffen objecten kopiëren	Als deze optie is ingeschakeld, is het vooraf gedefinieerde wachtwoord verplicht voor het kopiëren van een betreffend object.
Opdrachten toevoegen en wijzigen	Als deze optie is ingeschakeld, is het vooraf gedefinieerde wachtwoord verplicht voor het toevoegen en wijzigen van opdrachten in de Planner.
Configuratie	Als deze optie is ingeschakeld, is configuratie van het programma alleen mogelijk na het invoeren van het vooraf gedefinieerde wachtwoord.
Installatie / de-installatie	Als deze optie is ingeschakeld, is het vooraf gedefinieerde wachtwoord verplicht voor installatie of de-installatie van het programma.

9.8.4 Beveiliging

Automatisch starten

Functie "Automatisch starten" blokkeren

Wanneer deze optie is ingeschakeld wordt de functie "Automatisch starten" van Windows geblokkeerd op alle aangesloten drives, inclusief USB-sticks, cd- en dvd-drives en Network Drives. Met de functie "Automatisch starten" van Windows worden bestanden op gegevensdragers of Network Drives direct bij het laden of verbinden gelezen en zodoende kunnen bestanden automatisch worden gestart en gekopieerd. Deze functionaliteit brengt echter een hoog veiligheidsrisico met zich mee, omdat malware en ongewenste programma's met de automatische start kunnen worden geïnstalleerd. De functie "Automatisch starten" is vooral kritiek voor USB-sticks omdat gegevens op een stick op elk moment kunnen worden gewijzigd.

Cd's en dvd's uitsluiten

Wanneer deze optie is ingeschakeld is de functie "Automatisch starten" toegestaan op cd- en dvd-drives.

Waarschuwing

Schakel de functie "Automatisch starten" voor cd- en dvd-drives alleen uit wanneer u er zeker van bent dat u uitsluitend vertrouwde gegevensdragers gebruikt.

Systeembeveiliging

Windows-hostbestanden tegen wijzigingen beschermen

Wanneer deze optie is ingeschakeld zijn de Windows-host-bestanden beveiligd tegen schrijven. Manipuleren is niet meer mogelijk. U kunt bijvoorbeeld door malware niet meer omgeleid worden naar ongewenste websites. Deze optie is ingeschakeld als standaardinstelling.

Productbeveiliging

Let op

De opties voor productbeveiliging zijn niet beschikbaar als de realtime-bescherming niet is geïnstalleerd met behulp van de gebruikersgedefinieerde installatie-optie.

Processen tegen ongewenste beëindiging beschermen

Wanneer deze optie is ingeschakeld worden alle processen van het programma beschermd tegen ongewenste beëindiging door virussen en malware of tegen 'ongecontroleerde' beëindiging door een gebruiker, bijvoorbeeld via Task-Manager. Deze optie wordt ingeschakeld als de standaardinstelling.

Geavanceerde procesbeveiliging

Wanneer deze optie is ingeschakeld worden alle processen van het programma met geavanceerde opties beschermd tegen ongewenste beëindiging. Geavanceerde procesbeveiliging vereist aanzienlijk meer computercapaciteiten dan eenvoudige procesbeveiliging. De optie is ingeschakeld als de standaardinstelling. Om deze optie uit te schakelen, moet u de computer opnieuw opstarten.

Let op

Procesbeveiliging is niet beschikbaar voor Windows XP 64 bit !

Waarschuwing

Als procesbeveiliging is ingeschakeld, kunnen zich interactieproblemen voordoen met andere softwareproducten. Schakel in deze gevallen procesbeveiliging uit.

Bestanden en registervermeldingen tegen manipuleren beveiligen

Wanneer deze optie is ingeschakeld, worden alle registervermeldingen van het programma en alle programmabestanden (binaire- en configuratiebestanden) beveiligd tegen manipulatie. Beveiliging tegen manipulatie brengt het voorkomen van schrijven, verwijderen en, in sommige gevallen, lezen van de registervermeldingen of programmabestanden met zich mee door gebruikers of externe programma's. Om deze optie in te schakelen, moet u de computer opnieuw opstarten.

Waarschuwing

Houd er rekening mee dat, als deze optie is uitgeschakeld, de reparatie van computers die besmet zijn met bepaalde typen malware kan mislukken.

Let op

Wanneer deze optie is geactiveerd, kunnen alleen wijzigingen worden aangebracht in de configuratie, inclusief wijzigingen in scans of updateverzoeken, door de gebruikersinterface.

Let op

Beveiliging voor bestanden en registervermeldingen is niet beschikbaar voor Windows XP 64 bit !

9.8.5 WMI

Ondersteuning voor Windows Management Instrumentation

Windows Management Instrumentation is een eenvoudige Windows-managementtechnologie die script- en programmeertalen gebruikt om lees- en schrijftoegang toe te staan, zowel plaatselijk als op afstand, voor instellingen op Windows-systemen. Uw Avira-product ondersteunt WMI en voorziet in zowel gegevens (statusinformatie, statistische gegevens, geplande aanvragen, enz.) als gebeurtenissen via een interface. Met WMI kunt u besturingsgegevens downloaden van het programma

WMI-ondersteuning inschakelen

Als deze optie is ingeschakeld, kunt u besturingsgegevens van het programma via WMI downloaden.

9.8.6 Gebeurtenissen

Grootte van gebeurtenissendatabase beperken

Grootte beperken tot max. n items

Als deze optie is ingeschakeld, kan het maximum aantal gebeurtenissen in de gebeurtenissendatabase worden beperkt tot een bepaalde grootte; mogelijke waarden: 100-10.000 items. Als het aantal ingevoerde items wordt overschreden, worden de oudste items verwijderd.

Alle gebeurtenissen ouder dan n dag(en) verwijderen

Als deze optie is ingeschakeld, worden gebeurtenissen in de gebeurtenissendatabase na een bepaalde periode verwijderd; mogelijke waarden: 1 tot 90 dagen. Deze optie is standaard ingeschakeld met een waarde van 30 dagen.

Geen limiet

Wanneer deze optie is geactiveerd, is de grootte van de gebeurtenissendatabase niet beperkt. Er is echter een maximum van 20.000 weergegeven items in de programma-interface onder Gebeurtenissen.

9.8.7 Rapporten

Rapporten beperken

Aantal beperken tot max. n stuks

Als deze optie is ingeschakeld, kan het maximum aantal rapporten worden beperkt tot een bepaalde hoeveelheid. Er zijn waarden tussen 1 en 300 toegestaan. Wanneer het gespecificeerde aantal wordt overschreden, wordt het op dat moment oudste rapport verwijderd.

Alle rapporten ouder dan n dag(en) verwijderen

Als deze optie is ingeschakeld worden rapporten automatisch na een bepaald aantal dagen verwijderd. Toegestane waarden zijn: 1 tot 90 dagen. Deze optie is standaard ingeschakeld met een waarde van 30 dagen.

Geen limiet

Wanneer deze optie is ingeschakeld, is het aantal rapporten onbeperkt.

9.8.8 Mappen

Tijdelijk pad

Standaardsteeminstellingen gebruiken

Als deze optie is ingeschakeld, worden de instellingen van het systeem gebruikt voor de omgang met tijdelijke bestanden.

Let op

U kunt zien waar uw systeem tijdelijke bestanden opslaat - bijvoorbeeld, in Windows XP - onder: **Start > Instellingen > Configuratiescherm > Systeem > Indexkaart "Gevorderd"** Knop "Omgevingsvariabelen". De tijdelijke variabelen (TEMP, TMP) voor de huidige geregistreerde gebruiker en voor systeemvariabelen (TEMP, TMP) worden hier met hun relevante waarden weergegeven.

Volgende map gebruiken

Als deze optie is ingeschakeld, wordt het pad gebruikt dat wordt weergegeven in het invoervak.

Input-box

Voer in dit invoervakje het pad in waar het programma de tijdelijke bestanden zal opslaan.



De knop opent een venster waarin u het vereiste bestand of het vereiste tijdelijke pad kunt selecteren.

Standaard

De knop herstelt de vooraf gedefinieerde map voor het tijdelijke pad.

9.8.9 Akoestische waarschuwingen

Wanneer een virus of malware wordt gedetecteerd door de System Scanner of Real-Time Protection, wordt in interactieve actiemodus een akoestische waarschuwing afgespeeld. U kunt nu de akoestische waarschuwing activeren of deactiveren en een alternatief WAVE-bestand voor de waarschuwing selecteren.

Let op

De actiemodus van de Scanner is ingesteld in de configuratie onder [Scanner >](#)

[Scan > Actie bij detectie](#). De actiemodus van de Real-Time Protection wordt ingesteld in de configuratie onder [Real-Time Protection > Scan > Actie bij detectie](#).

Geen waarschuwing

Als deze optie is ingeschakeld, is er geen akoestische waarschuwing wanneer er een virus wordt gedetecteerd door de System Scanner of Real-Time Protection.

Gebruik pc-luidsprekers (alleen in interactieve modus)

Als deze optie is ingeschakeld, wordt er een akoestische waarschuwing afgegeven met het standaardsignaal wanneer er een virus wordt gedetecteerd door de System Scanner of Real-Time Protection. De akoestische waarschuwing wordt afgespeeld op de interne luidspreker van de pc.

Gebruik het volgende WAVE-bestand (alleen in interactieve modus)

Als deze optie is ingeschakeld, wordt er een akoestische waarschuwing afgegeven met het geselecteerde WAVE-bestand wanneer er een virus wordt gedetecteerd door de System Scanner of Real-Time Protection. Het geselecteerde WAVE-bestand wordt via een aangesloten externe luidspreker afgespeeld.

WAVE-bestand

In dit invoervak kunt u de naam en het bijbehorende pad of een audiobestand naar keuze invoeren. De standaard akoestische waarschuwing van het programma wordt als standaard ingevoerd.



De knop opent een venster waarin u het vereiste bestand kunt selecteren met behulp van de bestandsverkenner.

Test

Deze knop wordt gebruikt om het geselecteerde WAVE-bestand te testen.

9.8.10 Waarschuwingen

Uw Avira-product genereert zogenaamde slide-ups, bureaubladmededelingen voor bepaalde gebeurtenissen, die informatie geven over geslaagde of mislukte programmavolgorde zoals updates. Onder **Waarschuwingen** kunt u mededelingen voor bepaalde gebeurtenissen in- of uitschakelen.

Met bureaubladmededelingen heeft u de mogelijkheid om de mededeling direct in de slide-up uit te schakelen. U kunt de mededeling opnieuw activeren, in het configuratievenster **Waarschuwingen**.

Update

Waarschuwen als laatste update ouder is dan n dag(en)

In dit venster kunt u het maximale aantal toegestane dagen invoeren dat sinds de laatste update mag zijn verlopen. Als dit aantal dagen voorbij is, wordt er een rood icoon weergegeven voor de updatestatus onder **Status** in het Control Center.

Toon bericht als het virusdefinitiebestand verouderd is

Als deze optie is ingeschakeld, krijgt u een waarschuwing als het virusdefinitiebestand niet actueel meer is. Met behulp van de waarschuwingsoptie kunt u het tijdelijke interval configureren voor een mededeling als de laatste update ouder is dan n dag (en).

Waarschuwingen / Opmerkingen bij de volgende situaties

Er wordt een inbelverbinding gebruikt

Als deze optie is ingeschakeld, ontvangt u een bureaubladmededeling als een kiezer een inbelverbinding op uw computer creëert via de telefoon of ISDN-netwerk. Het gevaar bestaat dat de verbinding kan zijn gemaakt door een onbekende en ongewenste inbeller en dat de verbinding in rekening kan worden gebracht. (zie [Virussen en meer > Dreigingscategorieën: Inbeller](#))

Bestanden zijn met succes geüpdatet

Als deze optie is ingeschakeld, ontvangt u een bureaubladmededeling wanneer er een update met succes wordt uitgevoerd en bestanden worden geüpdatet.

Update mislukt



Als deze optie is ingeschakeld, ontvangt u een bureaubladmededeling wanneer er een update mislukt: er kon geen verbinding met de downloadserver worden gemaakt, de updatebestanden konden niet worden geïnstalleerd.

Geen update nodig

Als deze optie is ingeschakeld, ontvangt u een bureaubladmededeling wanneer er een update wordt gestart, maar installatie van de bestanden is niet nodig, omdat uw programma actueel is.

10. Taakbalkicoon

Het pictogram in het systeemvak van de taakbalk geeft de status van de Real-Time Protection -service aan.

Icoon	Beschrijving
	Avira Real-Time Protection is ingeschakeld
	Avira Real-Time Protection is uitgeschakeld

Invoer in het contextmenu

- **Real-Time Protection inschakelen:** schakelt de Avira Real-Time Protection in of uit.
- **Mail Protection inschakelen:** schakelt de Avira Mail Protection in of uit.
- **Web Protection inschakelen:** schakelt de Avira Web Protection in of uit.
 - **Windows Firewall inschakelen:** schakelt de Windows Firewall in of uit (deze functie is beschikbaar vanaf Windows 8).
- **Start Avira Internet Security Suite:** opent het [Control Center](#).
- **Configureer Avira Internet Security Suite:** opent de [Configuratie](#).
- **Mijn berichten:** hiermee opent u een schuifvenster met de [actuele informatie](#) over uw Avira-product.
- **Mijn communicatie-instellingen:** opent het [Product Message Subscription Center](#)
- **Start update** Start een [update](#).
- **Help:** opent de Online Help.
- **Over Avira Internet Security Suite:** opent een dialoogvenster met informatie over uw Avira-product: productinformatie, versie-informatie, licentie-informatie.
- **Avira op internet:** opent het Avira webportaal op het internet. De voorwaarde hiervoor is dat u een actieve verbinding met het internet heeft.

11. In-productberichten

11.1.1 Product Message Subscription Center

U kunt het *Product Message Subscription Center* bereiken door te klikken op **Mijn communicatie-instellingen** in het contextmenu van het Avira-taakbalkpictogram of door te klikken op het symbool voor **Configuratie** in het schuifvenster van **Mijn berichten**.

- ▶ U kunt invloed uitoefenen op de informatiestroom door te klikken op de betreffende **ON/OFF**-knop.
- ▶ Klik op **Profiel bijwerken** om uw persoonlijke berichtenprofiel te configureren.
 - ↪ U ontvangt het bericht dat uw profiel succesvol is bijgewerkt.

Voeg u online bij ons door te klikken op een van de links.

11.1.2 Actuele informatie

Het schuifvenster *Mijn berichten* wordt als communicatiekanaal gebruikt. Het brengt u op de hoogte van de nieuwste ontwikkelingen op het gebied van internetbeveiliging, nieuws over Avira-producten (updates, upgrades en licentieberichten) en virusinformatie.

Als er geen nieuwe berichten zijn, ontvangt u de informatie *Geen nieuwe berichten beschikbaar*. Klik op **OK** om het schuifvenster te sluiten.

Wanneer er nieuwe berichten beschikbaar zijn, heeft u volgende opties:

- ▶ Klik op **Herinner mij later**, indien u het bericht op een later tijdstip wilt lezen.
- ▶ Klik op **+ Lees meer**, om alle details van het bericht te lezen.
 - ↪ Afhankelijk van het soort bericht wordt u doorgestuurd naar onze homepage of wordt een nieuw venster uitgekapt om u de informatie te leveren.
- ▶ Klik op het kleine **x**-symbool om afzonderlijke berichten te sluiten.
- ▶ Klik op het symbool voor **Configuratie** in de kop van het schuifvenster om uw persoonlijke [berichtenprofiel](#) aan te maken.

12. FireWall

Met Avira Internet Security Suite kunt u het binnenkomend en uitgaand dataverkeer afhankelijk van de computerinstellingen beheren:

- [Windows Firewall](#)

Vanaf Windows 7 bevat Avira Internet Security Suite niet langer de Avira FireWall. De Windows Firewall wordt nu beheerd via het Avira-product.

12.1 Windows Firewall

Vanaf Windows 8 bevat Avira Internet Security Suite niet langer de Avira FireWall, maar biedt u de mogelijkheid om de Windows Firewall direct te beheren via het Avira Control en Configuratie Center. De volgende opties zijn beschikbaar voor de Windows Firewall:

de Windows Firewall inschakelen via het Control Center

Met de *FireWall*-optie onder **Status > Internetbescherming** kunt u de Windows Firewall in- of uitschakelen door op de knop **ON/OFF** te klikken.

de status van de Windows Firewall controleren via het Control Center

U kunt de status van de Windows Firewall controleren onder de sectie **INTERNETBESCHERMING > FireWall** en de aanbevolen instellingen herstellen door op de knop **Probleem oplossen** te klikken.

13. Updates

13.1 Updates

De effectiviteit van antivirussoftware is afhankelijk van hoe up-to-date het programma is, in het bijzonder het virusdefinitiebestand en de scan-engine. Voor het uitvoeren van regelmatige updates, wordt de Updater-component geïntegreerd in uw Avira-product. De Updater zorgt ervoor dat uw Avira-product altijd up-to-date is en in staat is, om te gaan met de nieuwe virussen die elke dag opdagen. Updater werkt de volgende onderdelen bij:

- Virusdefinitiebestand:
Het virusdefinitiebestand bevat de viruspatronen van de schadelijke programma's die worden gebruikt door uw Avira-product voor het scannen op virussen en malware en reparatie van geïnfecteerde objecten.
- Scan-engine:
De scan-engine bevat de methoden die worden gebruikt door uw Avira-product voor het scannen op virussen en malware.
- Programmabestanden (productupdate):
Updatepakketten voor productupdates maken extra functies beschikbaar voor de afzonderlijke programmaonderdelen.

Een update controleert of het virusdefinitiebestand, de scan-engine en het product up-to-date zijn en voert indien nodig een update uit. Na een productupdate, moet u mogelijk uw computersysteem opnieuw opstarten. Als alleen het virusdefinitiebestand en de scan-engine worden bijgewerkt, hoeft de computer niet opnieuw te worden opgestart.

Wanneer een productupdate een herstart nodig heeft, kunt u beslissen om verder te gaan met de update of om later opnieuw te worden herinnerd aan de update. Als u onmiddellijk met het productupdate doorgaat, bent u nog steeds in staat om te kiezen wanneer het opnieuw opstarten moet plaatsvinden.

Als u later aan de update wilt worden herinnerd, zullen het virusdefinitiebestand en de scanengine toch bijgewerkt worden, maar de productupdate wordt niet uitgevoerd.

Let op

De productupdate wordt niet voltooid tot een herstart heeft plaatsgevonden.

Let op

Om veiligheidsredenen controleert de Updater of het Windows-hostsbestand van uw computer werd gewijzigd, en of de update-URL, bijvoorbeeld, werd gemanipuleerd door malware om de Updater om te leiden naar ongewenste downloadsites. Als het Windows-hostsbestand is gemanipuleerd, wordt dit weergegeven in het Updater rapportbestand.

Een update wordt automatisch uitgevoerd in de volgende interval: 2 uur.

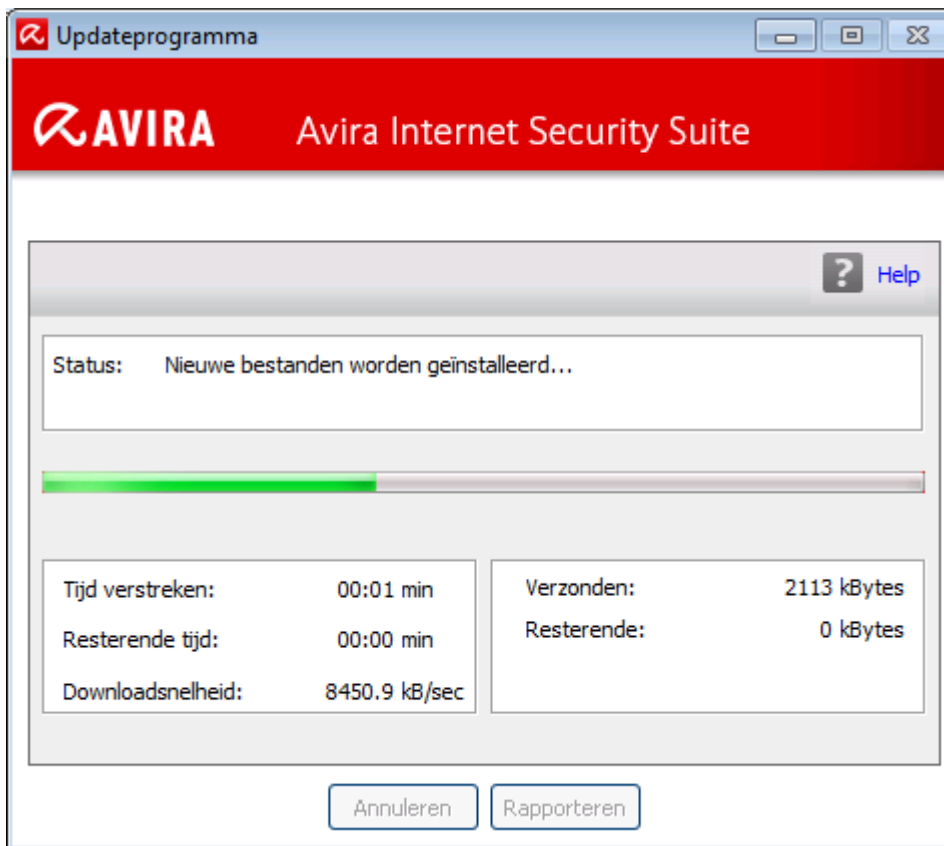
In het Control Center onder **Planner**, kunt u aanvullende updatetaken creëren die door Updater uitgevoerd worden op de gekozen tijdstippen. U hebt ook de mogelijkheid een update handmatig te starten:

- in het Control Center: in het menu **Bijwerken** en in de sectie **Status**
- via het contextmenu van het systeempictogram

Updates kunnen worden verkregen via internet via een webserver van de fabrikant. De bestaande netwerkverbinding is de standaardverbinding met de downloadservers van Avira. U kunt deze standaardinstelling wijzigen onder [Configuratie > Update](#).

13.2 Updater

Het Updater-venster opent bij de start van een update.



Let op

Voor updatetaken die zijn gemaakt in Planner, kunt u de weergavemodus voor het updatevenster definiëren. U kunt **Verbergen**, **Minimaliseren** of **Maximaliseren** selecteren.

Let op

Als u een programma in de modus Volledig scherm gebruikt (bijvoorbeeld spellen) en de **weergavemodus** van de updater is ingesteld op gemaximaliseerd of geminimaliseerd, schakelt de updater over naar het bureaublad. Om dit te voorkomen, start u de updater met de **weergavemodus** ingesteld op verbergen. In deze modus wordt u niet meer geïnformeerd over updates door het updatevenster.

Status: toont de voortgang van de updater.

Verstreken tijd: de tijd die is verstreken sinds de download is gestart.

Resterende tijd: tijd tot het downloaden is voltooid.

Downloadsnelheid: snelheid van de download.

Overgebracht: reeds gedownloadte bytes.

Resterend: aantal bytes dat nog gedownload moet worden.

Knoppen en links

Knop / link	Beschrijving
 Help	Deze pagina van de onlinehelp wordt geopend via deze knop of link.
Verkleinen	Het weergavevenster van de updater verschijnt in een verkleind formaat.
Vergroten	Het weergavevenster van de updater wordt hersteld naar de oorspronkelijke grootte.
Afbreken	De updateprocedure wordt geannuleerd. De updater wordt gesloten.
Sluiten	De updateprocedure is voltooid. Het weergavevenster wordt gesloten.
Rapport	Het rapportagebestand van de update wordt getoond.

14. FAQ, Tips

Dit hoofdstuk bevat belangrijke informatie over het oplossen van problemen en andere tips voor het gebruik van uw Avira-product.

- zie hoofdstuk [Hulp in geval van een probleem](#)
- zie hoofdstuk [Snelkoppelingen](#)
- zie hoofdstuk [Windows Security Center](#) (Windows XP) of [Windows Action Center](#) (vanaf Windows 7)

14.1 Hulp bij een probleem

Hier vindt u informatie over oorzaken en oplossingen van mogelijke problemen.

- [De foutmelding *Het licentiebestand kan niet worden geopend* verschijnt.](#)
- [De foutmelding *Verbinding mislukt tijdens het downloaden van het bestand ...* verschijnt bij een poging om een update te starten.](#)
- [Virussen en malware kunnen niet worden verplaatst of verwijderd.](#)
- [De status van het taakbalkicoon is uitgeschakeld.](#)
- [De computer is buitengewoon langzaam als ik een gegevensbackup maak.](#)
- [Mijn firewall meldt Avira Real-Time Protection en Avira Mail Protection direct na het inschakelen.](#)
- [Avira Mail Protection werkt niet.](#)
- [Een e-mail verstuurd via een TLS-verbinding is geblokkeerd door Mail Protection.](#)
- [Webchat werkt niet: Chat berichten worden niet weergegeven](#)

De foutmelding *Het licentiebestand kan niet worden geopend* verschijnt.

Reden: het bestand is versleuteld.

- ▶ Om de licentie te activeren, hoeft u het bestand niet te openen, maar het alleen maar op te slaan in de programmamap. .

De foutmelding *Verbinding mislukt tijdens het downloaden van het bestand ...* verschijnt bij een poging om een update te starten.

Reden: uw internetverbinding is inactief. Er kan dus geen verbinding met de webserver op het internet gemaakt worden.

- ▶ Test of andere internetdiensten zoals WWW of e-mail werken. Breng de internetverbinding opnieuw tot stand als dat niet het geval is.

Reden: de proxyserver is onbereikbaar.

- ▶ Controleer of de login voor de proxyserver is veranderd en wijzig eventueel uw configuratie.

Reden: het *update.exe*-bestand wordt niet volledig geaccepteerd door uw persoonlijke firewall.

- ▶ Zorg dat het *update.exe*-bestand volledig geaccepteerd wordt door uw firewall.

Anders:

- ▶ Controleer uw instellingen in de configuratie onder [Pc-bescherming > Update](#).

Virussen en malware kunnen niet worden verplaatst of verwijderd.

Reden: het bestand is geladen door Windows en is actief.

- ▶ Update uw Avira-product.
- ▶ Als u het Windows XP-besturingssysteem gebruikt, deactiveer dan System Restore.
- ▶ Start de computer in Safe Mode.
- ▶ Start de configuratie van uw Avira-product).
- ▶ Selecteer [Scanner > Scan > Bestanden > Alle bestanden](#) en bevestig het venster met **OK**.
- ▶ Start een scan van alle lokale drives.
- ▶ Start de computer in Normal Mode.
- ▶ Voer een scan uit in Normal Mode.
- ▶ Als er geen andere virussen of malware worden gevonden, activeer dan System Restore als dat beschikbaar en operationeel is.

De status van het taakbalkicoon is uitgeschakeld.

Reden: Avira Real-Time Protection is uitgeschakeld.

- ▶ In het Control Center, klikt u op [Status](#) en schakelt u de **Real-Time Protection** in in het onderdeel *PC Protection*.

-OF-

- ▶ Open het contextmenu door met de rechtermuisknop op het taakbalkicoon te klikken. Klik op **Real-Time Protection inschakelen**.

Reden: Avira Real-Time Protection wordt geblokkeerd door een firewall.

- ▶ Stel een algemene goedkeuring in voor Avira Real-Time Protection in de configuratie van uw firewall. Avira Real-Time Protection werkt alleen met het adres 127.0.0.1 (localhost). Er is geen internetverbinding tot stand gebracht. Hetzelfde geldt voor Avira Mail Protection.

Anders:

- ▶ Controleer het opstarttype van de Avira Real-Time Protection-service. Indien nodig, schakelt u de service in: selecteer in de taakbalk **Start > Instellingen > Configuratiescherm**. Open het configuratiepaneel **Services** door te dubbelklikken (onder Windows XP bevindt zich het services-applet in de onderliggende map *Administrative Tools*). Zoek de invoer *Avira Real-Time Protection*. *Automatisch* moet ingesteld zijn als het opstarttype en *Gestart* als de status. Indien nodig, start u de service handmatig door de betreffende regel te selecteren en de knop **Start**. Controleer gebeurtenissenweergave als er een foutmelding verschijnt.

De computer is buitengewoon langzaam als ik een gegevensbackup maak.

Reden: tijdens de backupprocedure scant Avira Real-Time Protection alle bestanden die gebruikt worden door de backupprocedure.

- ▶ Selecteer **Real-Time Protection > Scan > Uitzonderingen** in de configuratie en voer de procesnamen van de backupsoftware in.

Mijn firewall meldt Avira Real-Time Protection en Avira Mail Protection direct na het inschakelen.

Reden: communicatie met Avira Real-Time Protection en Avira Mail Protection vindt plaats via het TCP/IP-internetprotocol. Een firewall monitort alle verbindingen via dit protocol.

- ▶ Stel een algemene goedkeuring in voor Avira Real-Time Protection en Avira Mail Protection. Avira Real-Time Protection werkt alleen met het adres 127.0.0.1 (localhost). Er is geen internetverbinding tot stand gebracht. Hetzelfde geldt voor Avira Mail Protection.

Avira Mail Protection werkt niet.

Controleer de juiste werking van Avira Mail Protection met behulp van de volgende checklists als zich problemen voordoen met Avira Mail Protection.

Checklist

- ▶ Controleer of uw mailclient inlogt op de server via Kerberos, APOP of RPA. Deze verificatiemethoden worden momenteel niet ondersteund.
- ▶ Controleer of uw mailclient naar de server rapporteert met SSL (ook vaak TLS - Transport Layer Security - genoemd). Avira Mail Protection ondersteunt SSL niet, en sluit daarom alle versleutelde SSL-verbindingen. Als u versleutelde SSL-verbindingen wilt gebruiken zonder deze te beschermen door Mail Protection, moet u een poort gebruiken die niet wordt gemonitord door Mail Protection. De poorten die gemonitord worden door Mail Protection kunnen geconfigureerd worden onder **Mail Protection > Scan**.
- ▶ Is de Avira Mail Protection-service actief? Indien nodig, schakelt u de service in: selecteer in de taakbalk **Start > Instellingen > Configuratiescherm**. Open het configuratiepaneel **Services** door te dubbelklikken (onder Windows XP bevindt zich

het services-applet in de onderliggende map *Administrative Tools*). Zoek de invoer *Avira Mail Protection*. `Automatisch` moet ingesteld zijn als het opstarttype en `Gestart` als de status. Indien nodig, start u de service handmatig door de betreffende regel te selecteren en de knop **Start**. Controleer gebeurtenissenweergave als er een foutmelding verschijnt. Als dit niet werkt, moet u wellicht uw Avira-product compleet de-installeren via **Start > Instellingen > Configuratiescherm > Programma's toevoegen of verwijderen**, uw computer herstarten en daarna uw Avira-product opnieuw installeren.

Algemeen

POP3-verbindingen versleuteld via SSL (Secure Sockets Layer, ook vaak TSL (Transport Layer Security) genoemd) kunnen momenteel niet worden beschermd en worden genegeerd.

Verificatie met de mailserver wordt momenteel alleen ondersteund met behulp van wachtwoorden. "Kerberos" en "RPA" worden momenteel niet ondersteund.

Uw Avira-product controleert uitgaande e-mails niet op virussen en ongewenste programma's.

Let op

Wij bevelen u aan om regelmatig Microsoft-updates te installeren om gaten in de beveiliging te dichten.

Een e-mail verstuurd via een TLS-verbinding is geblokkeerd door Mail Protection.

Reden: Transport Layer Security (TSL: versleutelingsprotocol voor gegevensoverdracht op het internet) wordt momenteel niet ondersteund door Mail Protection. De volgende opties zijn beschikbaar om de e-mail te versturen:

- ▶ Gebruik een andere poort dan poort 25, die gebruikt wordt door SMTP. Dit ontwijkt het monitoren door Mail Protection.
- ▶ Zet uw TSL-versleutelde encryptie uit en deactiveer TSL-ondersteuning in uw e-mailclient.
- ▶ Deactiveer (tijdelijk) de monitoring van uitgaande e-mails door Mail Protection in de configuratie onder **Mail Protection > Scan**.

Webchat werkt niet: chatberichten worden niet weergegeven; gegevens worden niet geladen in de browser.

Dit fenomeen kan zich voordoen tijdens chats die gebaseerd zijn op het HTTP-protocol met 'transfer-encoding: chunked'.

Reden: Web Protection controleert eerst de verstuurde gegevens compleet op virussen en ongewenste programma's, voordat de gegevens in de browser geladen worden. Web

Protection kan de berichtlengte of de hoeveelheid gegevens niet vaststellen tijdens een gegevensoverdracht met 'transfer-encoding: chunked'.

- ▶ Stel de configuratie van de URL van de webchats in als een uitzondering (zie Configuratie: [Web Protection > Scan > Uitzonderingen](#)).

14.2 Snelkoppelingen

Toetsenbordopdrachten - ook 'shortcuts' genoemd - bieden een snelle mogelijkheid om door het programma te navigeren, om individuele modules te vinden en om acties te starten.

Hieronder vindt u een overzicht van alle beschikbare toetsenbordopdrachten. U kunt meer aanwijzingen over de functionaliteit vinden in het relevante hoofdstuk onder help.

14.2.1 In dialoogvensters

Shortcut	Beschrijving
Ctrl + Tab Ctrl + Page down	Navigeer in het Control Center Ga naar de volgende sectie.
Ctrl + Shift + Tab Ctrl + Page up	Navigeer in het Control Center Ga naar de vorige sectie.
← ↑ → ↓	Navigeer in de configuratiesecties Gebruik eerst de muis om de focus te leggen op een configuratiesectie. Wissel tussen de opties in een gemarkeerde dropdownlijst of tussen meerdere opties in een groep van opties.
Tab	Wissel naar de volgende groep of groep van opties.
Shift + Tab	Wissel naar de vorige opties of groep van opties.
Space	Activeer of deactiveer een opdrachtvak als de actieve optie een opdrachtvak is.

Alt + onderlijnde letter	Selecteer optie of start opdracht.
Alt + &darr; F4	Open de geselecteerde dropdownlijst.
Esc	Kies geselecteerde dropdownlijst. Annuleer opdracht en sluit dialoogvenster.
Enter	Start opdracht voor de actieve optie of knop.

14.2.2 In help

Shortcut	Beschrijving
Alt + Space	Systeemmenu weergeven.
Alt + Tab	Wissel tussen help en de andere geopende vensters.
Alt + F4	Sluit help.
Shift + F10	Geef het contextmenu van help weer.
Ctrl + Tab	Ga naar de volgende sectie in het navigatievenster.
Ctrl + Shift + Tab	Ga naar de vorige sectie in het navigatievenster.
Page up	Ga naar het onderwerp dat wordt weergegeven boven in de inhoud, in de index of in de lijst van zoekresultaten.
Page down	Ga naar het onderwerp dat wordt weergegeven beneden het actuele onderwerp in de inhoud, in de index of in de lijst van zoekresultaten.

Page up Page down	Blader door een onderwerp.
------------------------------------	----------------------------

14.2.3 In het Control Center

Algemeen

Shortcut	Beschrijving
F1	Help weergeven
Alt + F4	Sluit Control Center
F5	Vernieuw
F8	Open configuratie
F9	Start update

Scan sectie

Shortcut	Beschrijving
F2	Geselecteerd profiel hernoemen
F3	Scan starten met het geselecteerde profiel
F4	Bureaubladkoppeling maken voor het geselecteerde profiel
Ins	Nieuw profiel maken

Del	Geselecteerd profiel verwijderen
------------	----------------------------------

Quarantaine-sectie

Shortcut	Beschrijving
F2	Object opnieuw scannen
F3	Object herstellen
F4	Object verzenden
F6	Object herstellen naar...
Return	Eigenschappen
Ins	Bestand toevoegen
Del	Object verwijderen

Plannersectie

Shortcut	Beschrijving
F2	Taak bewerken
Return	Eigenschappen
Ins	Nieuwe taak invoegen
Del	Taak verwijderen

Rapportsectie

Shortcut	Beschrijving
F3	Rapportbestand weergeven
F4	Rapportbestand afdrukken
Return	Rapportbestand weergeven
Del	Rapport(en) verwijderen

Evenementensectie

Shortcut	Beschrijving
F3	Gebeurtenis(sen) exporteren
Return	Gebeurtenis tonen
Del	Gebeurtenis(sen) verwijderen

14.3 Windows Security Center

- Windows XP Service Pack 2 -

14.3.1 Algemeen

Het Windows Security Center controleert de status van een computer op belangrijke beveiligingsaspecten.

Als er een probleem wordt gevonden bij een van deze belangrijke punten (bijv. een verlopen antivirusprogramma), geeft het Security Center een waarschuwing, samen met aanbevelingen over hoe u uw computer beter kunt beschermen.

14.3.2 Het Windows Security Center en uw Avira-product

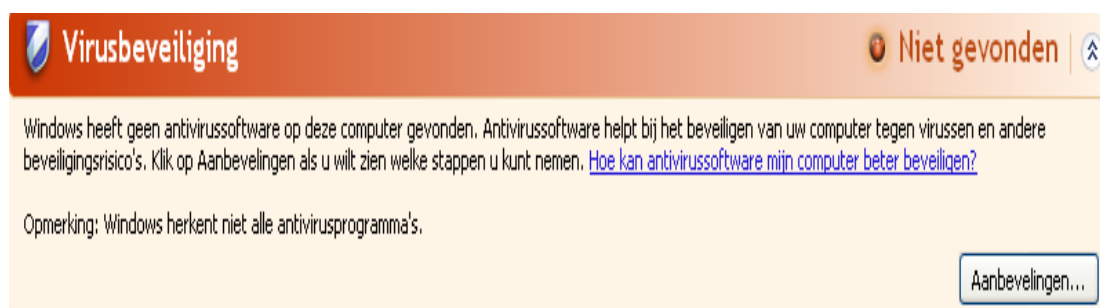
Virusbeschermingssoftware / Bescherming tegen schadelijke software

U kunt de volgende informatie ontvangen van het Windows Security Center over uw virusbescherming:

- [Virusbescherming NIET GEVONDEN](#)
- [Virusbescherming VERLOPEN](#)
- [Virusbescherming AAN](#)
- [Virusbescherming UIT](#)
- [Virusbescherming NIET GECONTROLEERD](#)

Virusbescherming NIET GEVONDEN

Deze informatie van het Windows Security Center wordt weergegeven als het Windows Security Center geen antivirussoftware op uw computer heeft gevonden.

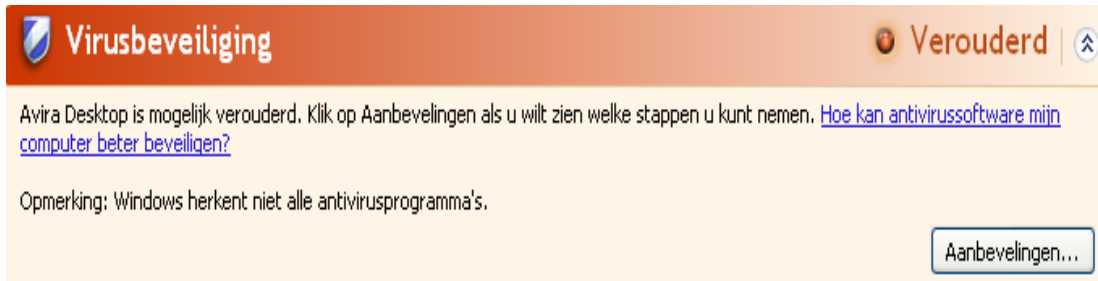


Opmerking

Installeer uw Avira-product op uw computer om deze tegen virussen en andere ongewenste programma's te beschermen!

Virusbescherming VERLOPEN

Als u Windows XP Service Pack 2 al heeft geïnstalleerd en dan uw Avira-product installeert, of als u Windows XP Service Pack 2 op een computer installeert waarop uw Avira-product al is geïnstalleerd, dan ontvangt u het volgende bericht:



Virusbeveiliging Verouderd

Avira Desktop is mogelijk verouderd. Klik op Aanbevelingen als u wilt zien welke stappen u kunt nemen. [Hoe kan antivirussoftware mijn computer beter beveiligen?](#)

Opmerking: Windows herkent niet alle antivirusprogramma's.

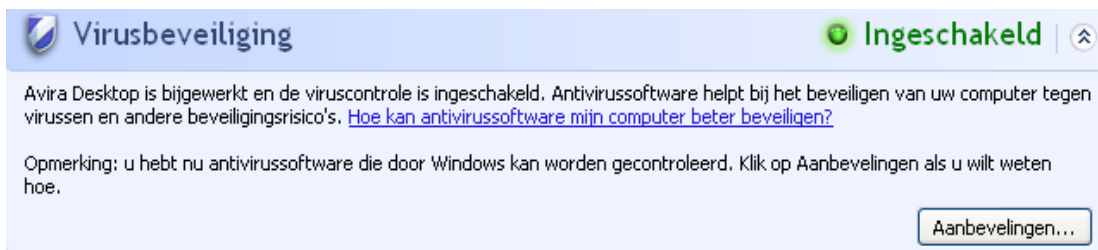
Aanbevelingen...

Opmerking

Er moet een update worden uitgevoerd na installatie, zodat het Windows Security Center uw Avira-product kan herkennen. Update uw computer door een [update](#) uit te voeren.

Virusbescherming AAN

Nadat u uw Avira-product heeft geïnstalleerd en de opvolgende update heeft uitgevoerd, wordt het volgende bericht weergegeven:



Virusbeveiliging Ingeschakeld

Avira Desktop is bijgewerkt en de viruscontrole is ingeschakeld. Antivirussoftware helpt bij het beveiligen van uw computer tegen virussen en andere beveiligingsrisico's. [Hoe kan antivirussoftware mijn computer beter beveiligen?](#)

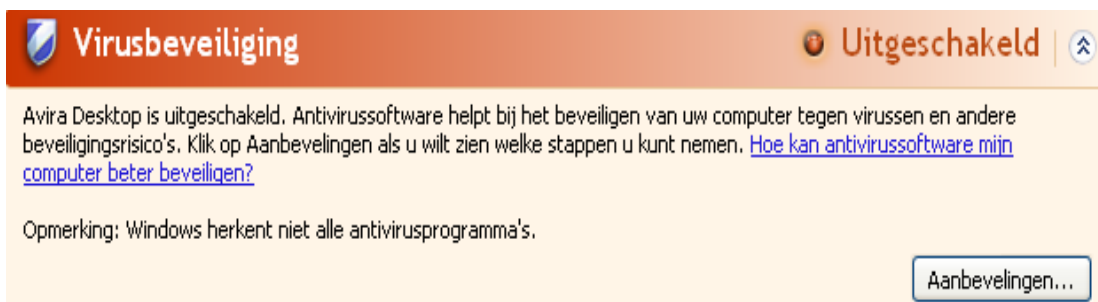
Opmerking: u hebt nu antivirussoftware die door Windows kan worden gecontroleerd. Klik op Aanbevelingen als u wilt weten hoe.

Aanbevelingen...

uw Avira-product is nu actueel en de Avira Real-Time Protection is geactiveerd.

Virusbescherming UIT

U ontvangt het volgende bericht zodra u de Avira Real-Time Protection uitschakelt of de Real-Time Protection-service beëindigt.



Virusbeveiliging Uitgeschakeld

Avira Desktop is uitgeschakeld. Antivirussoftware helpt bij het beveiligen van uw computer tegen virussen en andere beveiligingsrisico's. Klik op Aanbevelingen als u wilt zien welke stappen u kunt nemen. [Hoe kan antivirussoftware mijn computer beter beveiligen?](#)

Opmerking: Windows herkent niet alle antivirusprogramma's.

Aanbevelingen...

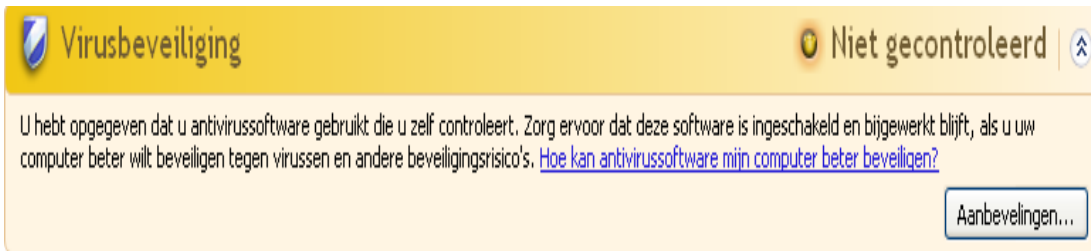
Opmerking

U kunt Avira Real-Time Protection in- of uitschakelen in de [Status](#)-sectie van

het **Control Center**. U kunt ook zien dat de Avira Real-Time Protection is ingeschakeld als het rode parapluutje in uw **taakbalk** open is.

Virusbescherming NIET GECONTROLEERD

Als u het volgende bericht ontvangt van het Windows Security Center, heeft u besloten dat u uw antivirussoftware zelf wilt controleren.



Opmerking

Het Windows Security Center wordt ondersteund door uw Avira-product. U kunt deze optie te allen tijde inschakelen via de knop **Aanbevelingen**.

Opmerking

Zelfs als u Windows XP Service Pack 2 heeft geïnstalleerd, heeft u nog steeds een oplossing nodig voor bescherming tegen virussen. Hoewel Windows uw antivirussoftware controleert, bevat het zelf geen enkele antivirusfunctie. Vandaar dat u geen bescherming tegen virussen en andere malware heeft zonder een extra antivirusoplossing!

14.4 Windows Action Center

- Windows 7 en Windows 8 -

14.4.1 Algemeen

Let op:

Vanaf Windows 7 is de naam **Windows Security Center** veranderd in **Windows Action Center**. In dit gedeelte vindt u de status van al uw beveiligingsopties.

Het Windows Action Center controleert de status van een computer op belangrijke beveiligingsaspecten. U bereikt het door te klikken op het vlaggetje in uw taakbalk of onder **Configuratiescherm > Action Center**.

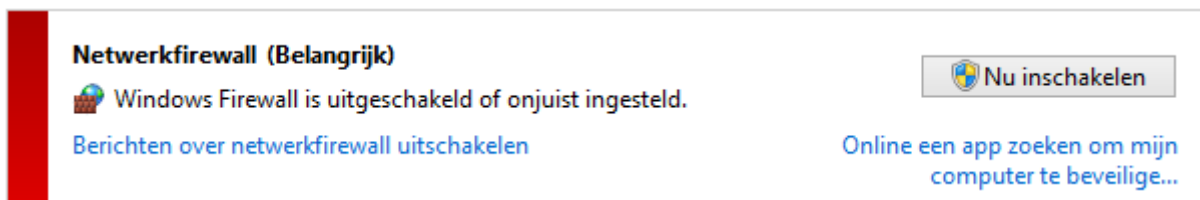
Als er een probleem wordt gevonden bij een van deze belangrijke punten (bijv. een verlopen antivirusprogramma), geeft het Action Center een waarschuwing, samen met aanbevelingen over hoe u uw computer beter kunt beschermen. Dit betekent dat, indien alles juist werkt, u niet met berichten wordt lastiggevallen. U kunt de beveiligingsstatus van uw computer nog steeds bekijken in het **Windows Action Center**, onder het item **Beveiliging**.

Het **Windows Action Center** biedt u ook de mogelijkheid om de geïnstalleerde programma's te beheren en om uit deze te kiezen (bijv. *Geïnstalleerde antispymwareprogramma's weergeven*).

U kunt de waarschuwingsberichten zelfs uitschakelen onder **Instellingen Action Center veranderen** (bijv. *Berichten uitschakelen over spyware en gerelateerde bescherming*).

14.4.2 Het Windows Action Center en uw Avira-product

De Windows Firewall is uitgeschakeld of verkeerd ingesteld



- **Windows Firewall**

Vanaf Windows 7 bevat Avira Internet Security Suite niet langer de Avira FireWall, maar biedt u de mogelijkheid om de Windows Firewall direct te beheren vanuit het Avira Control en Configuratie Center.

Virusbescherming

U kunt de volgende informatie ontvangen van het Windows Action Center over uw virusbescherming:

- [Avira Desktop meldt dat deze up to date is en dat viruscontrole is ingeschakeld.](#)
- [Avira Desktop rapporteert dat het is uitgeschakeld.](#)
- [Avira Desktop rapporteert dat het verouderd is.](#)
- [Windows heeft geen antivirussoftware op deze computer gevonden.](#)
- [De computer wordt niet meer beveiligd door Avira Desktop.](#)

Avira Desktop meldt dat deze up to date is en dat viruscontrole is ingeschakeld.

Na installatie van uw Avira product en een daarop volgende update ontvangt u geen berichten van het Windows Action Center. Maar als u naar **Action Center > Beveiliging** gaat, wordt het volgende weergegeven: *Avira Desktop meldt dat het actueel is en dat viruscontrole is ingeschakeld*. Dit betekent dat uw Avira-product nu actueel is en dat de Avira Real-Time Protection is geactiveerd.

Avira Desktop rapporteert dat het is uitgeschakeld.

U ontvangt het volgende bericht zodra u de Avira Real-Time Protection uitschakelt of de Real-Time Protection-service beëindigt.

Virusbeveiliging (Belangrijk)

Avira Desktop rapporteert dat het is uitgeschakeld.

[Berichten over virusbeveiliging uitschakelen](#)

Nu inschakelen

[Een ander antivirusprogramma downloaden](#)

Let op

U kunt Avira Real-Time Protection in- of uitschakelen in de sectie **Status** in het **Avira Control Center**. U kunt ook zien dat de Avira Real-Time Protection is ingeschakeld als het rode parapluutje in uw **taakbalk** open is. Het is ook mogelijk om het Avira-product te activeren door te klikken op de knop *Nu inschakelen* in het bericht van het Windows Action Center. U krijgt een melding waarin uw permissie wordt gevraagd om Avira uit te voeren. Klik op *Ja, ik vertrouw de uitgever en wil dit programma uitvoeren* en Real-Time Protection wordt dan weer ingeschakeld.

Avira Desktop rapporteert dat het verouderd is.

Als u Avira zojuist hebt geïnstalleerd of indien om één of andere reden het bestand met virusdefinities, de scan-engine of de programmabestanden van uw Avira-product niet automatisch zijn bijgewerkt (bijvoorbeeld als u een upgrade van een ouder Windows-besturingssysteem hebt uitgevoerd, waarop uw Avira product is al is geïnstalleerd), ontvangt u het volgende bericht:

Virusbeveiliging (Belangrijk)

Avira Desktop rapporteert dat het verouderd is.

[Berichten over virusbeveiliging uitschakelen](#)

Nu bijwerken

[Een ander antivirusprogramma downloaden](#)

Let op

Er moet een update worden uitgevoerd na installatie, zodat het Windows Action Center uw Avira-product kan herkennen. Update uw Avira-product door een [update](#) uit te voeren.

Windows heeft geen antivirussoftware op deze computer gevonden.

Deze informatie van het Windows Action Center wordt weergegeven als het Windows Action Center geen antivirussoftware op uw computer heeft gevonden.

Virusbeveiliging (Belangrijk)

Er is geen antivirussoftware op deze computer gevonden.

[Online naar programma zoeken](#)[Berichten over virusbeveiliging uitschakelen](#)**Let op**

Hou er rekening mee dat deze optie niet verschijnt in Windows 8, omdat Windows Defender nu ook de vooraf ingestelde virusbeschermingsfunctie is.

Let op

Installeer uw Avira-product op uw computer om deze tegen virussen en andere ongewenste programma's te beschermen!

De computer wordt niet meer beveiligd door Avira Desktop.

Deze informatie van het Windows Action Center wordt weergegeven wanneer de licentie van uw Avira product is verlopen.

Als u klikt op de knop **Vernieuw licentie**, wordt u doorgestuurd naar de website van Avira, waar u een nieuwe licentie kunt aanschaffen.

Virusbeveiliging (Belangrijk)

De computer wordt niet meer beveiligd door Avira Desktop.

[Actie ondernemen](#)[Berichten over virusbeveiliging uitschakelen](#)[Geïnstalleerde antivirusprogramma's weergeven](#)**Let op**

Houd er rekening mee dat deze optie alleen beschikbaar is voor Windows 8.

Bescherming tegen spyware en ongewenste software

U kunt de volgende informatie ontvangen van het Windows Action Center over uw spywarebescherming:

- [Avira Desktop meldt dat het is ingeschakeld.](#)
- [Windows Defender en Avira Desktop rapporteren beide dat deze zijn uitgeschakeld.](#)
- [Avira Desktop rapporteert dat het verouderd is.](#)
- [Windows Defender is verouderd.](#)
- [Windows Defender is uitgeschakeld.](#)

Avira Desktop meldt dat het is ingeschakeld

Na installatie van uw Avira-product en een daarop volgende update ontvangt u geen berichten van het Windows Action Center. Maar als u naar **Action Center > Beveiliging** gaat, wordt het volgende weergegeven: *Avira Desktop meldt dat het is ingeschakeld*. Dit betekent dat uw Avira-product nu actueel is en dat de Avira Real-Time Protection is geactiveerd.

Windows Defender en Avira Desktop rapporteren beide dat deze zijn uitgeschakeld.

U ontvangt het volgende bericht zodra u de Avira Real-Time Protection uitschakelt of de Real-Time Protection-service beëindigt.

Beveiliging tegen spyware en ongewenste software (Belangrijk)

Windows Defender en Avira Desktop rapporteren beide dat deze zijn uitgeschakeld.

[Berichten over beveiliging tegen spyware en dergelijke uitschakelen](#)

Antispywareprogramma's weergev...

Let op

U kunt Avira Real-Time Protection in- of uitschakelen in de sectie **Status** in het **Avira Control Center**. U kunt ook zien dat de Avira Real-Time Protection is ingeschakeld als het rode parapluutje in uw **taakbalk** open is. Het is ook mogelijk om het Avira-product te activeren door te klikken op de knop *Nu inschakelen* in het bericht van het Windows Action Center. U krijgt een melding waarin uw permissie wordt gevraagd om Avira uit te voeren. Klik op *Ja, ik vertrouw de uitgever en wil dit programma uitvoeren* en Real-Time Protection wordt dan weer ingeschakeld.

Avira Desktop rapporteert dat het verouderd is.

Als u Avira zojuist hebt geïnstalleerd of indien om één of andere reden het bestand met virusdefinities, de scan-engine of de programmabestanden van uw Avira-product niet automatisch zijn bijgewerkt (bijvoorbeeld als u een upgrade van een ouder Windows-besturingssysteem hebt uitgevoerd, waarop uw Avira product is al is geïnstalleerd), ontvangt u het volgende bericht:

Beveiliging tegen spyware en ongewenste software (Belangrijk)

Avira Desktop rapporteert dat het verouderd is.

[Berichten over beveiliging tegen spyware en dergelijke uitschakelen](#)

Nu bijwerken

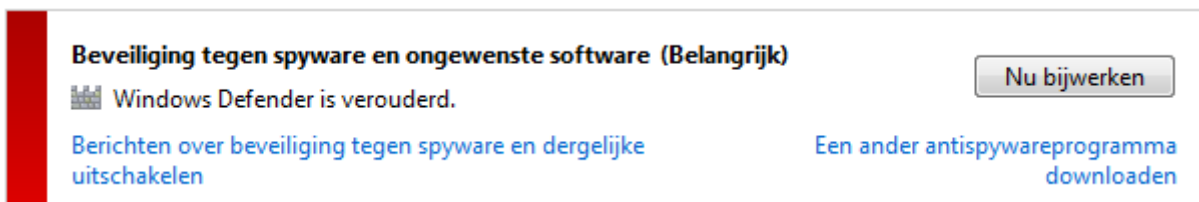
[Een ander antispywareprogramma downloaden](#)

Let op


Er moet een update worden uitgevoerd na installatie, zodat het Windows Action Center uw Avira-product kan herkennen. Update uw Avira-product door een [update](#) uit te voeren.

Windows Defender is verouderd

U kunt het volgende bericht ontvangen als Windows Defender is geactiveerd. Als u het Avira-product al heeft geïnstalleerd, zou dit bericht niet moeten worden weergegeven. Controleer of de installatie goed is verlopen.



Beveiliging tegen spyware en ongewenste software (Belangrijk) Nu bijwerken

 Windows Defender is verouderd.

[Berichten over beveiliging tegen spyware en dergelijke uitschakelen](#) [Een ander antispyswareprogramma downloaden](#)

Let op

Windows Defender is de vooraf ingestelde spyware en virusprotectie-oplossing van Windows.

Windows Defender is uitgeschakeld

Deze informatie van het Windows Action Center wordt weergegeven als het Windows Action Center geen andere antivirussoftware op uw computer heeft gevonden dan de software die standaard is geïntegreerd in het besturingsprogramma: Windows Defender. Indien er voorheen enige antivirussoftware op uw computer was geïnstalleerd, wordt deze toepassing uitgeschakeld. Als u het Avira-product al heeft geïnstalleerd, zou dit bericht niet moeten worden weergegeven: Avira zou automatisch moeten worden gevonden. Controleer of de installatie goed is verlopen.



Beveiliging tegen spyware en ongewenste software (Belangrijk) Nu inschakelen

 Windows Defender is uitgeschakeld.

[Berichten over beveiliging tegen spyware en dergelijke uitschakelen](#) [Een ander antispyswareprogramma downloaden](#)

15. Virussen en meer

Avira Internet Security Suite detecteert niet alleen virussen en malware, maar kan u ook tegen andere dreigingen beschermen. In dit hoofdstuk vindt u een overzicht van de verschillende soorten malware en andere bedreigingen, dat hun herkomst, gedrag en de onaangename verrassingen beschrijft die ze voor u in petto hebben.

Gerelateerde onderwerpen:

- [Dreigingscategorieën](#)
- [Virussen en andere malware](#)

15.1 Dreigingscategorieën

Adware

Adware is software die banner-advertenties in beeld brengt of deze in pop-upvensters door middel van een balk die op een computerscherm verschijnt, laat zien. Deze reclames kunnen meestal niet worden verwijderd en zijn dus altijd zichtbaar. De verbindingsgegevens maken een groot aantal conclusies mogelijk over het gebruiksgedrag en zijn problematisch in termen van gegevensbeveiliging.

Uw Avira-product detecteert adware. Wanneer de optie **Adware** is ingeschakeld met een vinkje in de configuratie onder [Dreigingscategorieën](#), ontvangt u een relevante waarschuwing zo gauw uw Avira-product adware detecteert.

Adware/Spyware

Software die reclame weergeeft of software die de persoonlijke gegevens van gebruikers, vaak zonder hun toestemming en buiten hun medeweten, naar derden verzendt, en om deze reden ongewenst kan zijn.

Uw Avira-product herkent "Adware/Spyware". Wanneer de optie **Adware/Spyware** is ingeschakeld met een vinkje in de configuratie onder [Dreigingscategorieën](#), ontvangt u een relevante waarschuwing zo gauw uw Avira-product adware of spyware detecteert.

Toepassing

De term APPL, respectievelijk applicatie, verwijst naar een toepassing die een risico kan inhouden bij gebruik of die van twijfelachtige oorsprong is.

Uw Avira-product herkent "Applicatie (APPL)". Wanneer de **Applicatie**-optie is ingeschakeld met een vinkje in de configuratie onder [Dreigingscategorieën](#), ontvangt u een relevante waarschuwing zo gauw uw Avira-product dergelijk gedrag detecteert.

Backdoor-clients

Om gegevens te stelen of om computers te manipuleren, wordt een backdoor-serverprogramma binnengesmokkeld dat onbekend is bij de gebruiker. Dit programma kan worden gecontroleerd door derden met behulp van backdoor-besturingssoftware (client) via het internet of een netwerk.

Uw Avira product herkent "Backdoor-besturingssoftware". Wanneer de optie **Backdoor-besturingssoftware** is ingeschakeld met een vinkje in de configuratie onder [Dreigingscategorieën](#), ontvangt u een relevante waarschuwing zo gauw uw Avira-product dergelijke software detecteert.

Dialer

Voor bepaalde services die beschikbaar zijn op het internet moet worden betaald. Deze worden gefactureerd in Duitsland via dialers met 0190/0900-nummers (of via 09x0-nummers in Oostenrijk en Zwitserland; in Duitsland wordt op de middellange termijn het nummer verandert in 09x0). Eenmaal geïnstalleerd op de computer garanderen deze programma's een verbinding via een voordelig premium-tariefnummer, waarvan de omvang van de kosten sterk kan variëren.

De marketing van online-inhoud via uw telefoonrekening is legaal en kan van voordeel zijn voor de gebruiker. Betrouwbare dialers laten geen ruimte over voor twijfel dat ze opzettelijk en bewust gebruikt worden door de gebruiker. Ze worden alleen op de computer van de gebruiker geïnstalleerd met toestemming van de gebruiker, die moet worden gegeven via een volledig eenduidig en duidelijk zichtbaar label of verzoek. Het dial-upproces van betrouwbare dialers wordt duidelijk weergegeven. Bovendien vertellen betrouwbare dialers u de gemaakte kosten exact en ondubbelzinnig.

Helaas zijn er ook dialers die zich ongemerkt installeren op computers met behulp van dubieuze middelen of zelfs met bedrieglijke bedoelingen. Zij vervangen bijvoorbeeld de standaard datacommunicatie-link van de internetgebruiker naar de ISP (Internet Service Provider) en bellen in via een kostenverhogend en vaak verschrikkelijk duur 0190/0900-nummer, elke keer als er een verbinding wordt gemaakt. De getroffen gebruiker merkt dit waarschijnlijk niet, totdat zijn volgende telefoonrekening laat zien dat een ongewenst 0190/0900-dialerprogramma bij elke verbinding op zijn computer heeft ingebeld via een premiumbetaalnummer, wat resulteert in dramatisch hogere kosten.

Wij raden u aan uw telefoonmaatschappij te vragen dit soort nummers direct te blokkeren voor onmiddellijke bescherming tegen ongewenste dialers (0190/0900-dialers).

Uw Avira-product kan standaard de bekende dialers detecteren.

Wanneer de **Dialers**-optie is ingeschakeld met een vinkje in de configuratie onder [Dreigingscategorieën](#), ontvangt u een relevante waarschuwing zo gauw er een dialer wordt gedetecteerd. U kunt nu gewoon de mogelijk ongewenste 0190/0900-dialer verwijderen. Echter, wanneer het een gewenst dial-upprogramma betreft, kunt u dit markeren als uitgezonderd bestand, dat dan voortaan niet meer wordt gescand.

Bestanden met dubbele extensie

Uitvoerbare bestanden die hun echte bestandsextensie op een verdachte manier verbergen. Deze camouflagemethode wordt vaak toegepast door malware.

Uw Avira-product herkent "Bestanden met dubbele extensie". Wanneer de optie **Bestanden met dubbele extensie** is ingeschakeld met een vinkje in de configuratie onder [Dreigingscategorieën](#), ontvangt u een relevante waarschuwing zo gauw uw Avira-product zulke bestanden detecteert.

Frauduleuze software

Ook bekend als "scareware" of "rogueware"; dit is frauduleuze software die pretendeert dat uw computer is geïnfecteerd door virussen of malware. Deze software lijkt bedrieglijk veel op professionele antivirussoftware, maar is bedoeld om de onzekerheid te verhogen of om de gebruiker bang te maken. De bedoeling is dat de slachtoffers zich bedreigd voelen door naderend (onwerkkelijk) gevaar en om ze te laten betalen voor het opheffen daarvan. Er zijn ook gevallen waarin men de slachtoffers laat geloven dat ze zijn aangevallen, en die vervolgens worden geïnstrueerd een actie uit te voeren, die in werkelijkheid de echte aanval is.

Uw Avira-product detecteert scareware. Wanneer de optie **Frauduleuze software** is ingeschakeld met een vinkje in de configuratie onder [Dreigingscategorieën](#), ontvangt u een relevante waarschuwing zo gauw uw Avira-product dergelijke bestanden detecteert.

Games

Er is ruimte voor computergames - maar dit is niet per se op het werk (behalve misschien in de lunchpauze). Maar met de overvloed aan games die te downloaden zijn van het internet, wordt er aanzienlijk aan mijnnevegen en patience gedaan door werknemers en ambtenaren. Je kunt een hele reeks aan spellen downloaden via het internet. E-mailgames zijn ook steeds populairder geworden: er is een groot aantal varianten in omloop, variërend van eenvoudig schaken tot "vlootoefeningen" (inclusief torpedogevechten): de bijbehorende zetten worden verzonden naar partners via e-mailprogramma's, die deze zetten dan beantwoorden.

Onderzoeken hebben aangetoond dat het aantal werkuren dat wordt besteed aan computergames al lange tijd economisch significante proporties heeft bereikt. Het is dan ook niet verwonderlijk dat steeds meer bedrijven manieren overwegen om computergames te verbannen van de werkplekcomputers.

Uw Avira-product herkent computergames. Wanneer de **Games**-optie is ingeschakeld met een vinkje in de configuratie onder [Dreigingscategorieën](#), ontvangt u een relevante waarschuwing zo gauw uw Avira-product een game detecteert. Het spel is nu uit in de ware zin van het woord, want u kunt het gewoon verwijderen.

Grappen

Grappen zijn alleen bedoeld om iemand te laten schrikken of algemeen amusement te bieden zonder schade te veroorzaken of die te reproduceren. Als er een grappenprogramma is geladen, begint de computer meestal op een gegeven moment met het spelen van een melodie of het weergeven van iets ongewoons op het scherm. Voorbeelden van grappen zijn de wasmachine in de diskdrive (DRAIN.COM) of de schermvreter (BUGSRES.COM).

Maar let op! Alle symptomen van grappenprogramma's kunnen ook afkomstig zijn van een virus of Trojaans paard. Op zijn minst schrikken gebruikers flink of worden ze zodanig in paniek gebracht dat ze zelf reële schade kunnen veroorzaken.

Dankzij de uitbreiding van de scan- en identificatieroutines kan uw Avira-product grappenprogramma's detecteren en indien gewenst elimineren als ongewenste programma's. Wanneer de optie **Grappen** is ingeschakeld met een vinkje in de configuratie onder [Dreigingscategorieën](#), ontvangt u een relevante waarschuwing zo gauw er een grappenprogramma wordt gedetecteerd.

Phishing

Phishing, ook wel bekend als "brand spoofing" is een slimme vorm van gegevensdiefstal die gericht is op klanten of potentiële klanten van internet-serviceproviders, banken, onlinebanking-services en registratie-autoriteiten.

Door het afgeven van uw e-mailadres op het internet, het invullen van onlineformulieren, toegang tot nieuwsgroepen of websites, kunnen uw gegevens worden gestolen door "Internet crawling spiders" en vervolgens zonder uw toestemming worden gebruikt om fraude of andere misdrijven te plegen.

Uw Avira-product herkent "Phishing". Wanneer de **Phishing**-optie is ingeschakeld met een vinkje in de configuratie onder [Dreigingscategorieën](#), ontvangt u een relevante waarschuwing zo gauw uw Avira-product dergelijk gedrag detecteert.

Programma's die het privédomein schenden

Software die in staat is om de beveiliging van uw systeem te schaden, ongewenste programma-activiteiten te starten, uw privacy te schenden of uw gebruikersgedrag te bespioneren en die daarom ongewenst kan zijn.

Uw Avira-product detecteert software met "Security Privacy Risk". Wanneer de optie **Programma's die het privédomein schenden** is ingeschakeld met een vinkje in de configuratie onder [Dreigingscategorieën](#), ontvangt u een relevante waarschuwing zo gauw uw Avira-product dergelijke software detecteert.

Ongebruikelijke runtime packers

Bestanden die zijn gecomprimeerd met een ongewone runtime packer en die daarom kunnen worden aangemerkt als mogelijk verdacht.

Uw Avira-product herkent "Ongebruikelijke runtime packers". Wanneer de optie **Ongebruikelijke runtime packers** is ingeschakeld met een vinkje in de configuratie onder [Dreigingscategorieën](#), ontvangt u een relevante waarschuwing zo gauw uw Avira-product dergelijke packers detecteert.

15.2 Virussen en andere malware

Adware

Adware is software die banner-advertenties in beeld brengt of deze in pop-upvensters door middel van een balk die op een computerscherm verschijnt, laat zien. Deze advertenties kunnen normaliter niet worden verwijderd en zijn dus altijd zichtbaar. De verbindingsgegevens staan een groot aantal conclusies over het gebruiksgedrag toe en zijn problematisch in termen van gegevensbeveiliging.

Backdoors

Een backdoor kan toegang tot een computer krijgen door het omzeilen van de toegangsbeveiligingsmechanismen van de computer.

Een programma dat op de achtergrond wordt uitgevoerd, verleent in het algemeen de aanvaller bijna onbeperkte rechten. Persoonlijke gegevens van de gebruiker kunnen worden bespioneerd door middel van de backdoor's help.. Maar worden voornamelijk gebruikt om andere computervirussen of wormen op het betreffende systeem te installeren.

Boot-virussen

De boot- of masterbootsector van de harde schijven wordt voornamelijk met bootsectorvirussen geïnfecteerd. Deze overschrijven belangrijke informatie die nodig is voor het uitvoeren van het systeem. Een van de pijnlijke gevolgen: het computersysteem kan niet meer worden opgestart...

Botnet

Een botnet wordt gedefinieerd als een extern netwerk van computers (op het internet) dat bestaat uit bots die met elkaar communiceren. Een botnet kan bestaan uit een verzameling van gekraakte computerprogramma's (meestal aangeduid als wormen, Trojaanse paarden) onder een gemeenschappelijke commando- en controle-infrastructuur. Botnets dienen voor verschillende doeleinden, waaronder denial-of-service-aanvallen enz., meestal zonder dat de betrokken pc-gebruiker hiervan kennis heeft. Een van de belangrijkste mogelijkheden van botnets is dat de netwerken een omvang kunnen bereiken van duizenden computers en dat hun totale bandbreedte de meeste conventionele internettoegangen overtreft.

Exploit

Een exploit (gat in de beveiliging) is een computerprogramma of script dat gebruik maakt van een bug, glitch of beveiligingslek, en leidt tot escalatie van bevoegdheden of denial-of-service op een computersysteem. Een vorm van exploitatie is bijvoorbeeld een aanval via het internet met behulp van gemanipuleerde gegevenspakketten. Programma's kunnen worden geïnfiltrerd om meer toegangsmogelijkheden te verkrijgen.

Frauduleuze software

Ook bekend als "scareware" of "rogueware"; dit is frauduleuze software die pretendeert dat uw computer is geïnfecteerd door virussen of malware. Deze software lijkt bedrieglijk veel op professionele antivirussoftware, maar is bedoeld om de onzekerheid te verhogen of om de gebruiker bang te maken. De bedoeling is dat de slachtoffers zich bedreigd voelen door naderend (onwerkelijk) gevaar en om ze te laten betalen voor het opheffen daarvan. Er zijn ook gevallen waarin men de slachtoffers laat geloven dat ze zijn aangevallen, en die vervolgens worden geïnstrueerd een actie uit te voeren, die in werkelijkheid de echte aanval is.

Hoaxes

Sinds enkele jaren hebben internet- en andere netwerkgebruikers waarschuwingen ontvangen over virussen die ogenschijnlijk worden verspreid via e-mail. Deze waarschuwingen worden verspreid via e-mail met het verzoek om ze te verzenden naar het hoogst mogelijke aantal collega's en aan andere gebruikers, om iedereen tegen het "gevaar" te waarschuwen.

Honeypot

Een honeypot is een service (programma of server) die geïnstalleerd is op een netwerk. Zijn functie is om toezicht te houden over een netwerk en om aanvallen te registreren. Deze service is bij de legitieme gebruiker niet bekend - dat is de reden waarom hij niet aangesproken wordt. Als een aanvaller een netwerk onderzoekt op zwakke punten en gebruik maakt van de service die wordt aangeboden door een honeypot, wordt deze geregistreerd en er wordt een waarschuwing gegenereerd.

Macrovirussen

Macrovirussen zijn kleine programma's die zijn geschreven in de macrotaal van een toepassing (bijvoorbeeld WordBasic onder WinWord 6.0) en die normaal gesproken alleen verspreid kunnen worden door de documenten van deze toepassing. Om deze reden worden ze ook wel documentvirussen genoemd. Om actief te zijn, moeten de bijbehorende toepassingen worden geactiveerd en moet één van de geïnfecteerde macro's worden uitgevoerd. In tegenstelling tot "normale" virussen, vallen macrovirussen dus geen uitvoerbare bestanden aan, maar ze vallen de documenten van de bijbehorende host-applicatie aan.

Pharming

Pharming is een manipulatie van het hostbestand van webbrowsers, door verschillende aanvragen naar vervalste websites te leiden. Dit is een verdere ontwikkeling van het klassieke phishing. Pharmingfraudeurs exploiteren een eigen grote serverfarm waarop nepwebsites zijn opgeslagen. Pharming heeft zich gevestigd als een overkoepelende term voor verschillende soorten DNS-aanvallen. In het geval van een manipulatie van het hostbestand wordt een specifieke manipulatie van een systeem uitgevoerd met behulp van een Trojaans paard of virus. Het resultaat is dat het systeem nu alleen toegang tot nepwebsites heeft, zelfs als het juiste webadres wordt ingevoerd.

Phishing

Phishing betekent vissen naar persoonlijke gegevens van de internetgebruiker. Phishers sturen hun slachtoffers meestal ogenschijnlijk officiële brieven zoals e-mails die bedoeld zijn om hen te goeder trouw ertoe te brengen vertrouwelijke informatie te onthullen, in het bijzonder gebruikersnamen en wachtwoorden of PIN- en TAN-codes van onlinebankrekeningen. Met de gestolen toegangsgegevens kunnen de phishers de identiteit van de slachtoffers simuleren en transacties in hun naam uitvoeren. Voor de duidelijkheid: banken en verzekeraars vragen nooit naar creditcardnummers, PIN-, TAN-codes of andere toegangsgegevens per e-mail, SMS of telefoon.

Polymorfe virussen

Polymorfe virussen zijn de echte meesters van vermomming. Ze veranderen hun eigen programmeringscodes - en zijn daarom zeer moeilijk te detecteren.

Programmavirussen

Een computervirus is een programma dat in staat is zich te hechten aan andere programma's, nadat deze zijn uitgevoerd, en een infectie te veroorzaken. Virussen vermenigvuldigen zich, in tegenstelling tot logische bommen en Trojaanse paarden. In tegenstelling tot een worm, vereist een virus altijd een programma als host, waarin het virus zijn kwaadaardige code achterlaat. De programma-uitvoering van de host zelf wordt in de regel niet veranderd.

Rootkits

Een rootkit is een verzameling softwaretools die is geïnstalleerd nadat een computersysteem is geïnfiltrerd, om inloggegevens van de infiltrant te verbergen, processen te verbergen en gegevens op te slaan - in het algemeen gesproken: om zichzelf onzichtbaar te maken. Ze proberen al geïnstalleerde spionageprogramma's bij te werken en verwijderde spyware opnieuw te installeren.

Scriptvirussen en wormen

Dergelijke virussen zijn zeer eenvoudig te programmeren en ze kunnen zich - als de nodig technologieën ter beschikking staan - binnen een paar uur via e-mail verspreiden over de wereld.

Scriptvirussen en wormen gebruiken een van de scripttalen, zoals Javascript, VBScript etc., om zich te voegen in andere, nieuwe scripts of om zichzelf te verspreiden door functies van het besturingssysteem op te vragen. Dit gebeurt vaak via e-mail of via het uitwisselen van bestanden (documenten).

Een worm is een programma dat zichzelf vermenigvuldigt, maar niet de host infecteert. Wormen kunnen dus geen deel uitmaken van andere programmadelen. Wormen zijn vaak de enige mogelijkheid om iedere willekeurige vorm van schadelijke programma's te infiltreren op systemen met beperkte veiligheidsmaatregelen.

Spyware

Spyware zijn zogenaamde spionageprogramma's die de gedeeltelijke controle over de werking van een computer hebben of deze onderscheppen, zonder toestemming van de gebruiker. Spyware is ontworpen om geïnfecteerde computers voor commercieel voordeel te exploiteren.

Trojaanse paarden (afgekort Trojans)

Trojaanse paarden zijn tegenwoordig vrij gebruikelijk. Trojaanse paarden zijn programma's die pretenderen een bepaalde functie te hebben, maar die hun echte functie na uitvoering laten zien; in de meeste gevallen een destructieve. Trojaanse paarden kunnen zichzelf niet vermenigvuldigen, dat onderscheidt hen van virussen en wormen. De meeste van hen hebben een interessante naam (SEX.EXE of STARTME.EXE) met de bedoeling de gebruiker te verleiden om het Trojaanse paard te starten. Onmiddellijk na uitvoering worden ze actief en kunnen bijvoorbeeld de harde schijf formatteren. Een dropper is een speciale vorm van Trojaans paard die virussen 'dropt', d.w.z. virussen op het computersysteem installeert.

Zombie

Een zombie-pc is een computer die is geïnfecteerd met malwareprogramma's en die hackers in staat stelt om computers via afstandsbediening voor criminele doeleinden te misbruiken. Op basis van een opdracht worden op de getroffen pc bijv. denial-of-service-aanvallen (DoS) gestart of worden spam- en phishing-e-mails verstuurd.

16. Informatie en Service

Dit hoofdstuk bevat informatie over Info en services van Avira.

- [Contactadres](#)
- [Technische ondersteuning](#)
- [Verdacht bestand](#)
- [Valse positieven rapporteren](#)
- [Uw feedback voor meer veiligheid](#)

16.1 Contactadres

Mocht u vragen of verzoeken met betrekking tot het productassortiment van Avira hebben, dan zijn wij u graag van dienst. Raadpleeg Control Center onder **Help > Over Avira Internet Security Suite** voor onze contactadressen.

16.2 Technische ondersteuning

Avira support biedt betrouwbare hulp bij het beantwoorden van uw vragen of het oplossen van een technisch probleem.

Alle benodigde informatie over onze uitgebreide ondersteuningservice kan worden verkregen van onze website:

<http://www.avira.nl/support>

Om u te kunnen voorzien van snelle, betrouwbare hulp, dient u de volgende informatie bij de hand te hebben:

- **Licentie-informatie.** U vindt deze informatie in de programma-interface onder het menu-item **Help > Over Avira Internet Security Suite > Licentie-informatie**. Zie [Licentie-informatie](#).
- **Versie-informatie.** U vindt deze informatie in de programma-interface onder het menu-item **Help > Over Avira Internet Security Suite > Versie-informatie**. Zie [Versie-informatie](#).
- **Besturingssysteem-versie** en geïnstalleerde Service Packs.
- **Geïnstalleerde softwarepakketten**, bijvoorbeeld antivirussoftware van andere aanbieders.
- **Nauwkeurige berichten** van het programma of van het rapportbestand.

16.3 Verdacht bestand

Verdachte bestanden of virussen die nog niet zijn gedetecteerd of verwijderd door onze producten kunnen naar ons worden gestuurd. We stellen hiervoor verschillende manieren beschikbaar.

- Identificeer het bestand in de quarantaine manager van het Control Center van de Avira Server Security Console en selecteer het item **Verstuur bestand** via het contextmenu of de desbetreffende knop.
- Stuur het gewenste bestand ingepakt (WinZIP, PKZip, Arj, etc.) als bijlage van een email naar het volgende adres:
virus@avira.nl
. Omdat sommige e-mailgateways werken met antivirussoftware, dient u het bestand(en) ook te voorzien van een wachtwoord (vergeet niet ons het wachtwoord mee te delen).
- U kunt ons het verdachte bestand ook via onze website sturen:
<http://www.avira.nl/sample-upload>

16.4 Valse positieven rapporteren

Wanneer u denkt dat uw Avira Internet Security Suite een detectie rapporteert in een bestand dat hoogstwaarschijnlijk "schoon" is, stuurt u het betreffende bestand dan gezippt (WinZIP, PKZip, Arj, etc.) als e-mailbijlage naar het volgende adres:

virus@avira.nl

Aangezien sommige e-mailgateways met anti-virussoftware werken, moet u de bestanden ook van een wachtwoord voorzien (vergeet niet ons het wachtwoord mee te delen).

16.5 Uw feedback voor meer veiligheid

Bij Avira staat de veiligheid van onze klanten voorop. Vandaar dat we niet alleen een team van experts ter beschikking hebben dat de kwaliteit en de veiligheid van elke Avira-oplossing test voordat het product wordt vrijgegeven. We hechten ook veel belang aan de signalen met betrekking tot veiligheidsgerelateerde lacunes die kunnen ontstaan en behandelen deze serieus.

Wanneer u denkt dat u een lacune in de beveiliging heeft ontdekt in een van onze producten, stuur dan een email naar het volgende adres:

vulnerabilities@avira.nl



Avira

Deze handleiding is met veel zorg gemaakt. Fouten in ontwerp en inhoud zijn echter niet uit te sluiten.
Het vermenigvuldigen van deze publicatie in welke vorm dan ook is verboden zonder voorafgaande
schriftelijke toestemming van Avira Operations GmbH & Co. KG.

Merk- en productnamen zijn handelsmerken of gedeponeerde handelsmerken van hun respectieve eigenaars.
Beschermd handelsmerken worden niet als zodanig aangegeven in deze handleiding.
Dit betekent echter niet dat deze vrijelijk mogen worden gebruikt.

Gepubliceerd 4e kwartaal 2013.

© 2013 Avira Operations GmbH & Co. Alle rechten voorbehouden.
Behoudens vergissingen, weglatingen en technische wijzigingen.

Avira | Kaplaneiweg 1 | 88069 Tettnang | Duitsland | Tel.nr.: +49 7542-500 0
www.avira.com