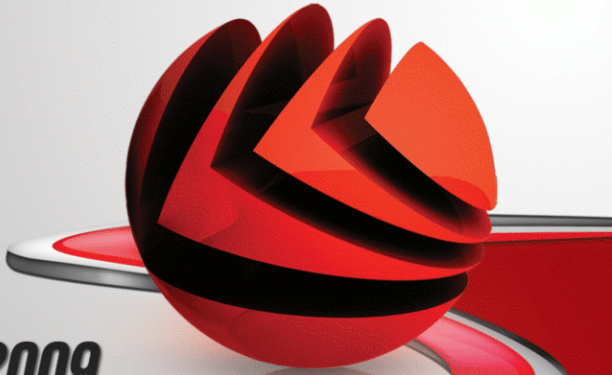
bitdefender



ANTIVIRUS 2009

Handleiding

bitdefender

BitDefender Antivirus 2009

Handleiding

Uitgegeven 2009.01.07

Wettelijke bepaling

bitdefender

Inhoudsopgave

Licentieovereenkomst voor eindgebruikers

INSTALLEER DE SOFTWARE NIET ALS U NIET INSTEMT MET DEZE BEPALINGEN EN VOORWAARDEN. WANNEER U KLIKT OP "IK AANVAARD", "OK", "DOORGAAN" OF "JA", OF WANNEER U DE SOFTWARE OP ENIGE MANIER INSTALLEERT OF GEBRUIKT, DUIDT U AAN DAT U DE VOORWAARDEN VAN DEZE OVEREENKOMST VOLLEDIG BEGRIJPT EN AANVAARDT.

PRODUCTREGISTRATIE. Door deze Overeenkomst te accepteren, gaat u akkoord om uw Software te registeren, via "Mijn account", als voorwaarde voor uw gebruik van de Software (ontvangst van updates) en uw recht op Onderhoud. Deze controle helpt u garanderen dat de Software alleen werkt op computers met een geldige licentie en dat alleen eindgebruikers met een geldige licentie gebruik kunnen maken van de onderhoudsdiensten. De registratie vereist een geldig serienummer voor het product en een geldig e-mailadres voor verlengingen en andere wettelijke mededelingen.

Deze voorwaarden dekken de oplossingen en diensten van BitDefender voor thuisgebruikers waarvoor u een licentie wordt verleend, inclusief verwante documentatie en elke update en upgrade van de toepassingen die u werden geleverd onder de aangekochte licentie of elke andere verwante serviceovereenkomst, zoals gedefinieerd in de documentatie en elke kopie van deze items.

De Licentieovereenkomst is een wettelijke overeenkomst tussen u (een natuurlijk persoon of een rechtspersoon) en BitDefender voor het gebruik van het hierboven geïdentificeerde softwareproduct van BitDefender. Dit omvat de computersoftware en diensten en kan verwante media, afgedrukte materialen, en "online" of elektronische documentatie (hierna aangegeven als "BitDefender") bevatten, die allemaal door de internationale wetten op auteursrecht en internationale verdragen worden beschermd. Door BitDefender te installeren, te kopiëren of te gebruiken, aanvaardt u dat u gebonden bent door de voorwaarden van deze overeenkomst.

Als u de voorwaarden van deze overeenkomst niet aanvaardt, mag u BitDefender niet installeren of gebruiken.

BitDefender-licentie. BitDefender is beschermd door copyright-wetten en internationale copyright verhandelingen, evenals door intellictueel bezit wetten en bverhandelingen. BitDefender is gedeponeerd, niet verkocht.

LICENTIEVERLENING. BitDefender verleent u, en u alleen, hierbij de volgende niet-exclusieve, beperkte, niet-overdraagbare licentie met royalty's voor het gebruik van BitDefender.

TOEPASSINGSSOFTWARE U mag BitDefender installeren en gebruiken op zoveel computers als nodig met de beperking die is opgelegd door het totaal aantal gelicentieerde gebruikers. U mag één extra kopie maken voor back-updoeleinden.

DESKTOPGEBRUIKERSLICENTIE Deze licentie is van toepassing op de BitDefender-software die kan worden geïnstalleerd op één computer die geen netwerkdiensten biedt. Elke primaire gebruiker mag deze software installeren op één computer en mag één extra kopie maken op een ander apparaat voor back-updoeleinden. Het toegelaten aantal primaire gebruikers is het aantal gebruikers van de licentie.

DUUR VAN DE LICENTIE. De hieronder verleende licentie zal beginnen op de aankoopdatum van BitDefender en zal vervallen aan het einde van de periode waarvoor de licentie is aangekocht.

VERVALDATUM. Het product zal zijn functies niet langer uitvoeren zodra de licentie is verlopen.

UPGRADES. Als BitDefender wordt gelabeld als een upgrade, moet u over de geschikte licentie beschikken om een product te gebruiken dat door BITDEFENDER is aangeduid als in aanmerking komend voor de upgrade, om BitDefender te gebruiken. Een versie van BitDefender die als upgrade is gelabeld, vervangt en/of vult het product aan dat werd gebruikt als basis om te bepalen of u in aanmerking kwam voor de upgrade. U mag het resulterende upgradeproduct uitsluitend gebruiken in overeenstemming met de voorwaarden van deze Licentieovereenkomst. Als BitDefender een upgrade is van een component van een pakket softwareprogramma's, dat u als alleenstaand product hebt gelicentieerd, dan kan BitDefender alleen worden gebruikt of overgedragen als onderdeel van dit alleenstaand productpakket en mag hij niet worden gescheiden voor gebruik door meer dan het totale aantal gelicentieerde gebruikers. De voorwaarden en bepalingen van deze licentie vervangen en krijgen de voorrang op alle voorafgaande overeenkomsten die mogelijk bestonden tussen u en BITDEFENDER met betrekking tot het originele product of het resulterende product na een upgrade.

AUTEURSRECHT. Alle rechten, aanspraken op en belangen in BitDefender en alle auteursrechten in en voor BitDefender (met inbegrip van, maar niet beperkt tot elke afbeelding, foto, logo, animatie, video, audio, muziek, tekst en "applet" die in BitDefender zijn geïntegreerd), de begeleidende gedrukte materialen en elke kopie van BitDefender zijn eigendom van BITDEFENDER. BitDefender is beschermd door wetten op auteursrecht en internationale verdragsvoorwaarden. U moet BitDefender daarom behandelen als elk ander materiaal dat auteursrechtelijk is beschermd. U mag geen kopieën maken van het gedrukte materiaal, dat bij BitDefender wordt geleverd. U moet alle auteursrechtelijke bepalingen produceren en overnemen in hun

oorspronkelijke vorm voor alle gemaakte kopieën, ongeacht de media of de vorm waarin BitDefender bestaat. U mag een licentie van BitDefender niet verhuren, verkopen, leasen of delen. U mag geen reverse engineering toepassen, niet opnieuw compileren, demonteren, afgeleide werken maken, vertalen, of enige poging ondernemen om de broncode van BitDefender te onthullen.

BEPERKTE GARANTIE. BITDEFENDER garandeert dat de media waarop BitDefender wordt verdeeld, vrij is van defecten gedurende een periode van dertig dagen vanaf de datum waarop BitDefender aan u werd geleverd. Uw enig verhaal bij een inbreuk op deze garantie, is dat BITDEFENDER, volgens eigen voorkeur, de defecte media vervangt na ontvangst van de beschadigde media, of het bedrag, dat u voor BitDefender hebt betaald, terugbetaalt. BITDEFENDER biedt geen garantie dat BitDefender ongestoord of vrij van fouten zal werken, of dat de fouten zullen worden gecorrigeerd. BITDEFENDER garandeert niet dat BitDefender zal voldoen aan uw behoeften.

TENZIJ UITDRUKKELIJK UITEENGEZET IN DEZE OVEREENKOMST, WIJST BITDEFENDER ALLE ANDERE GARANTIES, UITDRUKKELIJK OF IMPLICIET, AF MET BETREKKING TOT DE PRODUCTEN, VERBETERINGEN, ONDERHOUD OF ONDERSTEUNING DIE HIERMEE VERWANT IS OF ALLE ANDERE MATERIALEN (TASTBAAR OF NIET-TASTBAAR) DIE DOOR BITDEFENDER ZIJN GELEVERD. BITDEFENDER WIJST HIERBIJ UITDRUKKELIJK ALLE IMPLICIETE GARANTIES EN BEPALINGEN AF, MET INBEGRIP VAN, MAAR NIET BEPERKT TOT IMPLICIETE GARANTIES VAN VERKOOPBAARHEID, GESCHIKTHEID VOOR EEN BEPAALD DOEL, AANSPRAKEN, NIET-INTERFERENTIE, NAUWKEURIGHEID VAN GEGEVENS, NAUWKEURIGHEID VAN INFORMATIEVE INHOUD, SYSTEEMINTEGRATIE EN NIET-INBREUK VAN RECHTEN VAN DERDEN DOOR HET FILTEREN, UITSCHAKELEN OF VERWIJDEREN VAN DERGELIJKE SOFTWARE VAN DERDEN, SPYWARE, ADWARE, COOKIES, E-MAILS, DOCUMENTEN, ADVERTENTIES OF GELIJKSOORTIGE ZAKEN, ONGEACHT OF ZE VOORTVLOEIEN UIT STATUTEN, WETTEN, HANDELSWIJZEN, DOUANE EN PRAKTIJKEN, OF HANDELSGEBRUIK.

AFWIJZING VAN SCHADE. Iedereen die BitDefender gebruikt, test of evalueert draagt het volledige risico met betrekking tot de kwaliteit en prestatie van BitDefender. BITDEFENDER zal in geen geval aansprakelijk zijn voor elke willekeurige schade, met inbegrip van en zonder beperking op directe of indirecte schade, voortvloeiend uit het gebruik, de prestatie of de levering van BitDefender, zelfs indien BITDEFENDER op de hoogte werd gesteld van het bestaan of de mogelijkheid van dergelijke schade.

SOMMIGE LANDEN STAAN DE BEPERKING OF UITSLUITING VAN AANSPRAKELIJKHEID VOOR INCIDENTELE OF GEVOLGSCHADE NIET TOE. DE

BOVENSTAANDE BEPERKING OF UITSLUITING ZAL BIJGEVOLG MOGELIJK NIET VAN TOEPASSING ZIJN OP U.

IN GEEN GEVAL ZAL DE AANSPRAKELIJKHEID VAN BITDEFENDER DE AANKOOPPRIJS, DIE U VOOR BITDEFENDER HEBT BETAALD, OVERSCHRIJDEN. De afwijzingen en beperkingen, zoals hierboven beschreven, zullen steeds worden toegepast ongeacht of u BitDefender gebruikt, evalueert of test.

BELANGRIJKE MEDEDELING AAN GEBRUIKERS. DEZE SOFTWARE IS NIET FOUT-TOLERANT EN IS NIET ONTWIKKELD OF BEDOELD VOOR GEBRUIK IN EEN GEVAARLIJKE OMGEVING DIE EEN STORINGSVEILIGE PRESTATIE OF WERKING VEREIST. DEZE SOFTWARE IS NIET VOOR GEBRUIK BIJ DE BEDIENING VAN VLIEGTUIGNAVIGATIE, NUCLEAIRE FACILITEITEN OF COMMUNICATIESYSTEMEN, WAPENSYSTEMEN, DIRECTE OF INDIRECTE LIFE-SUPPORTSYSTEMEN, LUCHTVERKEERSLEIDING, OF ELKE TOEPASSING OF INSTALLATIE WAAR DEFECTEN DE DOOD, ERNSTIGE LICHAMELIJKE LETSELS OF MATERIËLE SCHADE KUNNEN VEROORZAKEN.

TOESTEMMING VOOR ELEKTRONISCHE COMMUNICATIE. BitDefender kan worden verplicht u wettelijke mededelingen en andere berichten te bezorgen over de abonnementsdiensten voor de Software en het Onderhoud of over ons gebruik van de informatie die u ons levert ("Mededelingen"). BitDefender zal u mededelingen sturen via vermeldingen in het product of via e-mail naar het geregistreerde e-mail adres van de hoofdgebruiker of zal deze mededelingen op haar sites plaatsen. Door deze Overeenkomst te accepteren, gaat u akkoord dat u alle mededelingen alleen via elektronische weg zult ontvangen. Hiermee erkent u en geeft u aan dat u toegang kunt krijgen tot de mededelingen op de sites.

ALGEMEEN. Deze overeenkomst zal worden beheerd door de Roemeense wetten en de internationale voorschriften en verdragen inzake auteursrecht. De exclusieve jurisdictie en rechtsgebied om elk geschil te beslechten dat voortvloeit uit deze licentievoorwaarden, ligt bij de rechtbanken van Roemenië.

Prijzen, kosten en vergoedingen voor het gebruik van BitDefender zijn onderhevig aan wijzigingen zonder dat u hiervan vooraf op de hoogte wordt gebracht.

In geval van ongeldigheid van een willekeurige voorwaarde van deze overeenkomst, zal de ongeldigheid geen invloed hebben op het resterende gedeelte van deze overeenkomst.

BitDefender en de logo's van BitDefender zijn handelsmerken van BITDEFENDER. Alle overige handelsmerken die in het product of in verwante materialen worden gebruikt, zijn eigendom van hun respectieve eigenaars.

De licentie wordt onmiddellijk beëindigd zonder kennisgeving als u een van deze voorwaarden en bepalingen overtreedt. U zult geen aanspraak kunnen maken op een terugbetaling van BITDEFENDER of enige andere wederverkopers van BitDefender na het beëindigen omwille van deze reden. De voorwaarden en bepalingen met betrekking tot de vertrouwelijkheid en beperkingen op het gebruik zullen van kracht blijven, zelfs na het beëindigen van de licentie.

BITDEFENDER kan deze voorwaarden op elk ogenblik herzien en de herziene voorwaarden zullen automatisch van toepassing zijn op de overeenkomende versies van de software die wordt verdeeld met de herziene voorwaarden. Als een van deze voorwaarden ongeldig is of niet kan worden afgedwongen, zal dit de geldigheid van de rest van de voorwaarden niet beïnvloeden die geldig en afdwingbaar blijven.

In geval van tegenstrijdigheid of inconsistentie tussen de vertalingen van deze voorwaarden in andere talen, zal de Engelse versie die door BITDEFENDER is uitgegeven, de voorrang krijgen.

Neem contact op met BITDEFENDER, op 24, Preciziei Boulevard, West Gate Building H2, ground floor, Sector 6, Boekarest, Roemenië, of via tel.nr.: 40-21-206.34.70 of fax: 40-21-264.17.99, e-mailadres: office@bitdefender.com.

Voorwoord

Deze handleiding is bedoeld voor alle gebruikers die voor **BitDefender Antivirus 2009** hebben gekozen als een beveiligingsoplossing voor hun computers. De informatie die in dit boek staat is niet alleen geschikt voor gevorderde computergebruikers, maar is ook gemakkelijk te begrijpen door iedereen die met Windows kan werken.

Dit boek biedt u een beschrijving van **BitDefender Antivirus 2009**, het bedrijf en het team dat het programma heeft samengesteld. Het zal u ook begeleiden doorheen de installatieprocedure en u leren hoe u het programma kunt configureren. U zult leren hoe u **BitDefender Antivirus 2009** kunt gebruiken, updaten, testen en aanpassen. Deze handleiding biedt u alle informatie die u nodig hebt om optimaal gebruik te maken van BitDefender.

Wij wensen u veel aangenaam en nuttig leesplezier.

1. Conventies die in dit boek worden gebruikt

1.1. Typografische conventies

In dit boek worden verschillende tekststijlen gebruikt, zodat de tekst leesbaarder is. De weergave en betekenis worden in de onderstaande tabel weergegeven.

Weergave	Beschrijving
`sample syntax`	Syntaxisvoorbeelden zijn gedrukt in `enkelspatietekens`.
http://www.bitdefender.com	De URL-koppeling wijst naar een externe locatie op http- of ftp-servers.
support@bitdefender.com	E-mailadressen worden in de tekst ingevoegd voor contactgegevens.
“Voorwoord” (p. xiv)	Dit is een interne koppeling naar een locatie in het document.
`filename`	Bestandsnamen en mappen worden afgedrukt met een `enkelspatielettertype`.
option	Alle productopties worden afgedrukt met **harde** tekens.

Weergave	Beschrijving
`sample code listing`	De codeweergave wordt gedrukt met `enkelspatietekens`.

1.2. Waarschuw.

De waarschuwingen zijn opmerkingen in de tekst die grafisch zijn gemarkeerd en uw aandacht wordt getrokken naar extra informatie met betrekking tot de huidige paragraaf.

Opmerking
De opmerking is slechts een kort commentaar. Hoewel u opmerkingen kunt weglaten, kunnen ze toch waardevolle informatie bieden zoals over een specifieke functie of een koppeling naar een verwant onderwerp.

Belangrijk
Dit vereist uw aandacht en het wordt niet aanbevolen dit te negeren. Doorgaans betreft het niet-kritische, maar belangrijke informatie.

Waarschuwing
Dit is kritische informatie die u aandachtig moet lezen. Er zullen geen ernstige problemen optreden als u de aanwijzingen volgt. U moet de informatie lezen en begrijpen omdat hier iets wordt beschreven dat hoge risico's inhoudt.

2. De boekstructuur

Het boek bestaat uit verschillende delen die de belangrijkste onderwerpen bevatten. Bovendien vindt u ook een woordenlijst die enkele technische termen toelicht.

Installatie. Stapsgewijze instructies voor het installeren van BitDefender op een werkstation. Dit is een uitgebreide les over het installeren van **BitDefender Antivirus 2009**. Er wordt gestart met de vereisten voor een geslaagde installatie. Daarna wordt u verder begeleid doorheen het volledige installatieproces. Tot slot wordt de verwijderingsprocedure beschreven voor het geval u BitDefender moet verwijderen.

Basisbeheer. Beschrijving van het basisbeheer en onderhoud van BitDefender.

Geavanceerd beheer. Een gedetailleerde voorstelling van de beveiligingsmogelijkheden die door BitDefender worden geboden. U wordt geleerd hoe u alle BitDefender-modules te configureren en gebruiken om uw computer op een efficiënte manier te beveiligen tegen elk type malwarebedreiging (virussen, spyware, rootkits, enz.).

Hulp vragen. Informatie over waar u om hulp kunt vragen indien er zich onverwachte problemen voordoen.

BitDefender reddingsschijf. Beschrijving van de BitDefender reddingsschijf. Dit zal u helpen de functies die door deze opstartbare cd worden geboden, te begrijpen en te gebruiken.

Woordenlijst. De woordenlijst biedt een verklaring voor enkele technische en ongebruikelijke termen die u in de pagina's van het document zult vinden.

3. Verzoek om commentaar

We willen u uitnodigen ons te helpen dit boek te verbeteren. Wij hebben alle informatie zo goed mogelijk getest en gecontroleerd. Laat ons weten of u enige tekortkomingen hebt ontdekt in dit boek of als u ideeën hebt om dit te verbeteren, zodat wij u de best mogelijke documentatie kunnen bieden.

U kunt contact met ons opnemen door een e-mail te sturen naar documentation@bitdefender.com.

Belangrijk
Wij verzoeken u al uw e-mails met betrekking tot de documentatie in het Engels te schrijven, zodat we uw opmerkingen op een efficiënte manier kunnen verwerken.

Installatie

1. Systeemvereisten

U kunt BitDefender Antivirus 2009 uitsluitend installeren op computers met de volgende besturingssystemen:

- Windows XP met Service Pack 2 (32/64-bits) of hoger
- Windows Vista (32/64-bits) of Windows Vista met Service Pack 1
- Windows Home Server

Controleer vóór de installatie of uw computer voldoet aan de minimum hardware en software vereisten.

Opmerking
Om het Windows besturingsssysteem en de hardware-informatie van uw computer te zien, rechtsklikt u op **Deze Computer** op het bureaublad en selecteert u **Eigenschappen** in het menu.

1.1. Hardwarevereisten

Voor Windows XP

- 800 MHz processor of hoger
- 256 MB RAM-geheugen (1 GB aanbevolen)
- 170 MB beschikbare harde schijfruimte (200 MB aanbevolen)

Voor Windows Vista

- 800 MHz processor of hoger
- 512 MB RAM-geheugen (1 GB aanbevolen)
- 170 MB beschikbare harde schijfruimte (200 MB aanbevolen)

Voor Windows Home Server

- 800 MHz processor of hoger
- 512 MB RAM-geheugen (1 GB aanbevolen)
- 170 MB beschikbare harde schijfruimte (200 MB aanbevolen)

1.2. Softwarevereisten

- Internet Explorer 6.0 (of hoger)
- .NET Framework 1.1 (ook aanwezig in het installatiepakket)

Antiphishing-beveiliging is alleen aanwezig voor:

- Internet Explorer 6.0 of hoger
- Mozilla Firefox 2.0
- Yahoo! Messenger 8.1
- Windows Live (MSN) Messenger 8.5

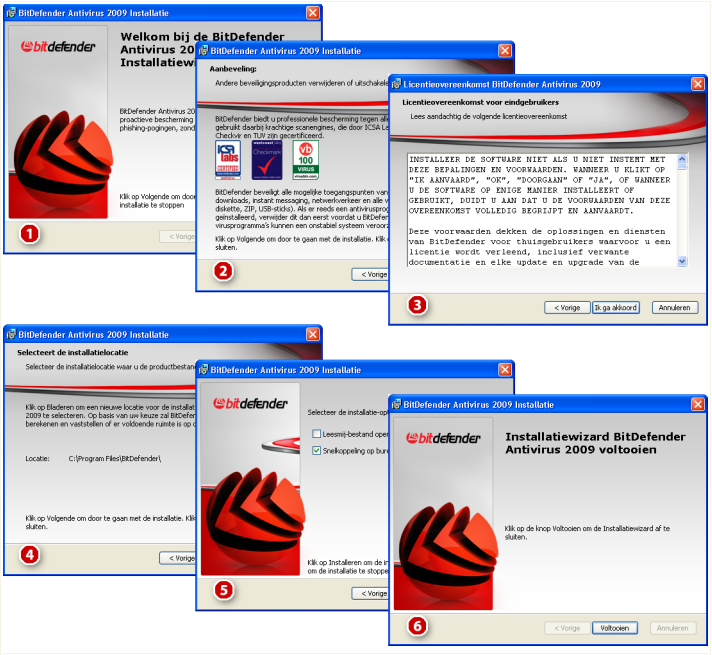
Instant Messaging (IM) encryptie is alleen aanwezig voor:

- Yahoo! Messenger 8.1
- Windows Live (MSN) Messenger 8.5

2. BitDefender installeren

Zoek het installatiebestand en dubbelklik op dit bestand. Hierdoor wordt de installatiewizard gestart, die u zal helpen tijdens het installatieproces.

Voordat u de installatiewizard uitvoert, zal BitDefender controleren of er nieuwere versies van het installatiepakket zijn. Als er een nieuwere versie beschikbaar is, zult u worden gevraagd deze versie te downloaden. Klik op **Ja** om de nieuwere versie te downloaden of klik op **Nee** om door te gaan met de installatie van de versie die beschikbaar is in het installatiebestand.



Installatiestappen

Volg deze stappen om BitDefender Antivirus 2009 te installeren:

1. Klik op **Volgende** om door te gaan of klik op **Annuleren** als u de installatie wilt afbreken.
2. Klik op **Volgende**.

   BitDefender Antivirus 2009 waarschuwt u als er andere antivirusproducten op uw computer zijn geïnstalleerd. Klik op **Verwijderen** om het overeenkomende product te verwijderen. Klik op **Volgende** als u wilt doorgaan zonder de gedetecteerde producten te verwijderen.

   Waarschuwing
   Het is sterk aanbevolen gedetecteerde andere antivirusproducten te verwijderen voordat u BitDefender installeert. Het uitvoeren van twee of meer antivirusproducten tegelijk op een computer, maakt het systeem doorgaans onbruikbaar.

3. Lees de Licentieovereenkomst en klik op **Akkoord**.

   Belangrijk
   Als u niet instemt met deze voorwaarden, klik dan op **Annuleren**. Het installatieproces wordt afgebroken en u verlaat het installatieprogramma.

4. BitDefender Antivirus 2009 wordt standaard geïnstalleerd in `C:\Program Files\BitDefender\BitDefender 2009`. Als u het installatiepad wilt wijzigen, klikt u op **Bladeren** en selecteert u de map waarin u BitDefender Antivirus 2009 wilt installeren.

   Klik op **Volgende**.

5. Selecteer de opties met betrekking tot het installatieproces. Sommige worden standaard geselecteerd:
   - **Leesmij-bestand openen** - hiermee opent u het leesmij-bestand aan het einde van de installatie.
   - **Een snelkoppeling op het bureaublad plaatsen** - hiermee plaatst u een snelkoppeling naar BitDefender Antivirus 2009 op het bureaublad aan het einde van de installatie.
   - **Cd uitwerpen nadat installatie is voltooid** - om de cd uit te werpen aan het einde van de installatie. Deze optie verschijnt wanneer u het product vanaf de cd installeert.

- **Windows Defender uitschakelen** - hiermee wordt Windows Defender uitgeschakeld. Deze optie verschijnt alleen in Windows Vista.

Klik op **Installeren** om de installatie van het product te starten. Als .NET Framework 1.1 nog niet is geïnstalleerd, zal BitDefender dit eerst installeren.

Wacht tot de installatie voltooid is.

6. Klik op **Voltooien**. U wordt gevraagd uw systeem opnieuw te starten zodat het installatieprogramma de installatie kan voltooien. Wij adviseren dit zo snel mogelijk te doen.

Belangrijk

Na de installatie en het opnieuw starten van de computer verschijnen een registratiewizard en een configuratiewizard. Voltooi deze wizards om BitDefender Antivirus 2009 te registreren en te configureren en een BitDefender-account te creëren.

Als u de standaardinstellingen voor het installatiepad hebt geaccepteerd, ziet u in `Program Files` een nieuwe map, genaamd `BitDefender`, met daarin de submap `BitDefender 2009`.

2.1. Registratiewizard

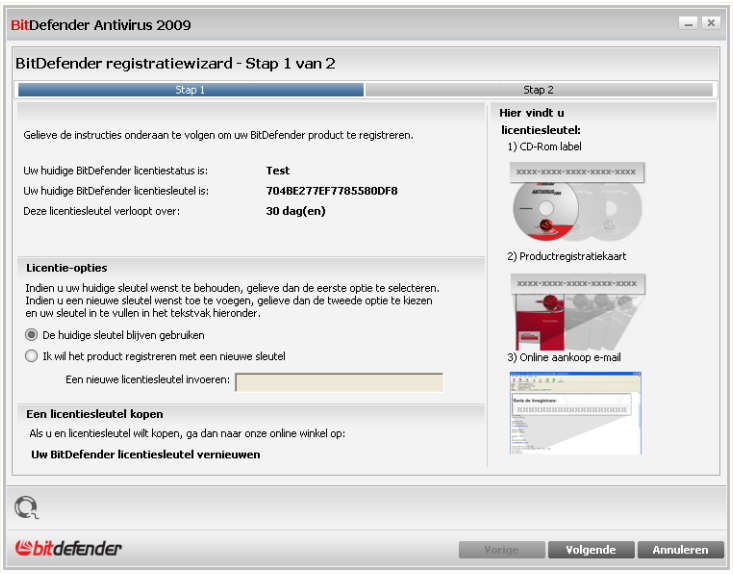
De eerste keer dat u de computer start na de installatie, verschijnt een registratiewizard. De wizard helpt u bij het registreren van BitDefender and het configureren van een BitDefender-account

U MOET een BitDefender-account maken om BitDefender-updates te ontvangen. De BitDefender-account biedt u ook toegang tot de gratis technische ondersteuning en speciale aanbiedingen en promoties. Als u uw licentiesleutel kwijt bent, kunt u inloggen op uw account op http://myaccount.bitdefender.com om hem op te halen.

Opmerking

Als u de wizard niet wilt volgen, klik dan op **Annuleren**. U kan u de registratiewizard op elk gewenst moment openen door te klikken op de link **Registreren** aan de onderkant van de gebruikersinterface.

2.1.1. Stap 1/2 - BitDefender Antivirus 2009 registreren



Registratie

U kan de BitDefender registratiestatus zien, evenals de huidige licentiesleutel en over hoeveel dagen de licentiesleutel verloopt.

Selecteer **Doorgaan met de huidige sleutel** om het product verder te evalueren.

Om BitDefender Antivirus 2009 te registreren:

1. Selecteer **Ik wil het product registreren met een nieuwe sleutel**.
2. Typ de licentiesleutel in het bewerkingsveld.

Opmerking

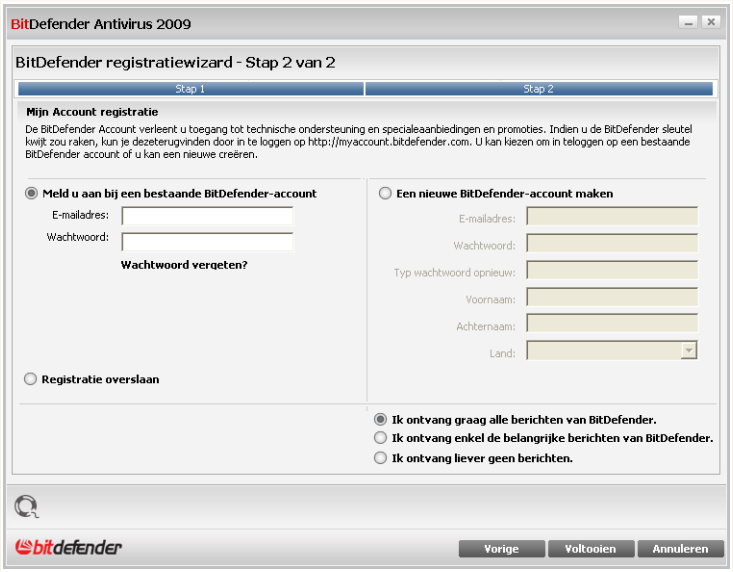
U kan uw licentiesleutel vinden:

- op het cd label.
- op de productregistratiekaart.
- in de online aankoop e-mail.

Als u geen BitDefender licentiesleutel hebt, klik dan op de aanwezige link om naar de BitDefender online winkel te gaan en een licentiesleutel te kopen.

Klik op **Volgende** om door te gaan.

2.1.2. Stap 2/2 - Een BitDefender-account creëren



Account creëren

Als u nu geen BitDefender-account wilt creëren, selecteer dan **Registratie overslaan** en klik op **Voltooien**. Ga anders te werk zoals past bij uw situatie:

- “Ik heb geen BitDefender-account” (p. 9)
- “Ik heb al een BitDefender-account” (p. 9)

Belangrijk

U moet een account maken binnen de 15 dagen na het installeren van BitDefender (als u het product registreert, wordt de deadline verlengd tot 30 dagen). Anders zullen er geen updates van BitDefender meer worden uitgevoerd.

Ik heb geen BitDefender-account

Om een BitDefender-account te creëren, selecteert u **Een nieuwe BitDefender-account maken** en geeft u de vereiste informatie op. De gegevens die u hier opgeeft blijven vertrouwelijk.

- **E-mailadres** - voer uw e-mailadres in.
- **Wachtwoord** - voer een wachtwoord voor uw BitDefender-account in. Het wachtwoord moet minstens zes tekens bevatten.
- **Wachtwoord opnieuw** - voer het zojuist gebruikte wachtwoord opnieuw in.
- **Voornaam** - voer uw voornaam in.
- **Achternaam** - voer uw achternaam in.
- **Land** - selecteer het land waar u woont.

Opmerking
Gebruik het door u ingevoerde e-mailadres en wachtwoord om in te loggen op uw account op http://myaccount.bitdefender.com.

Om een account te kunnen maken, moet u eerst uw e-mailadres activeren. Controleer uw e-mailadres en volg de instructies in de e-mail die u van de registratieservice van BitDefender hebt ontvangen.

Optioneel kan BitDefender u informeren over speciale aanbiedingen via het e-mailadres van uw account. Selecteer een van de beschikbare opties:

- **Stuur mij alle berichten van BitDefender**
- **Stuur mij alleen de belangrijkste berichten**
- **Stuur mij geen berichten**

Klik op **Voltooien**.

Ik heb al een BitDefender-account

BitDefender detecteert automatisch of u al een BitDefender-account hebt geregistreerd op uw computer. Geef in dit geval het wachtwoord van uw account op.

Als u al een actieve account hebt, maar BitDefender deze niet detecteert, selecteer dan **Aanmelden bij een bestaande BitDefender Account** en vul het e-mailadres en het wachtwoord van uw account in.

Als u uw wachtwoord bent vergeten, klikt u op **Wachtwoord vergeten?** en volgt u de instructies.

Optioneel kan BitDefender u informeren over speciale aanbiedingen via het e-mailadres van uw account. Selecteer een van de beschikbare opties:

- **Stuur mij alle berichten van BitDefender**
- **Stuur mij alleen de belangrijkste berichten**
- **Stuur mij geen berichten**

Klik op **Voltooien**.

2.2. Configuratiewizard

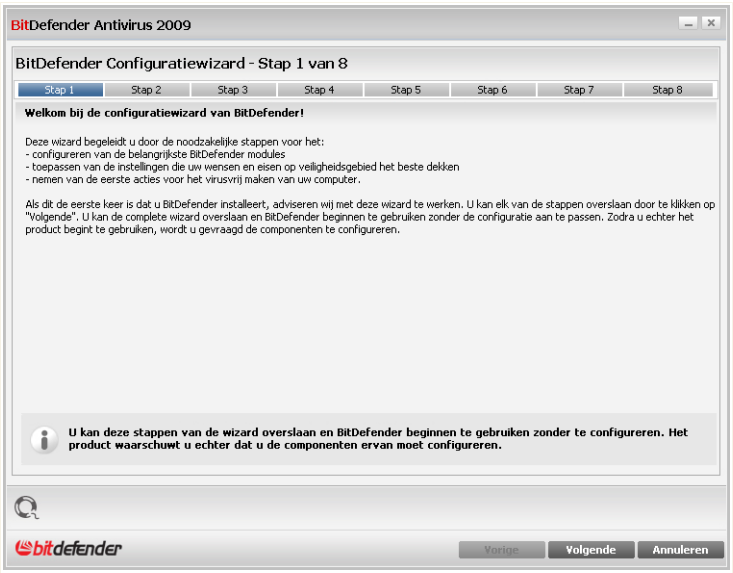
Na het voltooien van de registratiewizard verschijnt een configuratiewizard. De wizard helpt u bij het configureren van specifieke productmodules en het instellen van de beveiligingstaken van BitDefender.

U bent niet verplicht deze wizard te voltooien. Wij raden u echter aan dit toch te doen om tijd te besparen en zeker te zijn dat uw systeem veilig is, zelfs voordat BitDefender Antivirus 2009 is geïnstalleerd.

Opmerking

Als u de wizard niet wilt volgen, klik dan op **Annuleren**. Als u de gebruikersinterface opent, geeft BitDefender aan welke componenten u moet configureren.

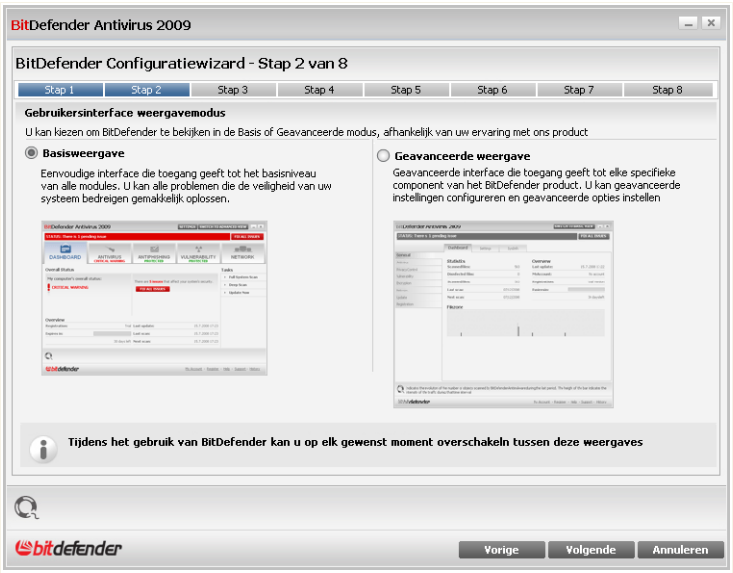
2.2.1. Stap 1/8 – Welkomstvenster



Welkomstvenster

Klik op **Volgende** om door te gaan.

2.2.2. Stap 2/8 - Weergave selecteren



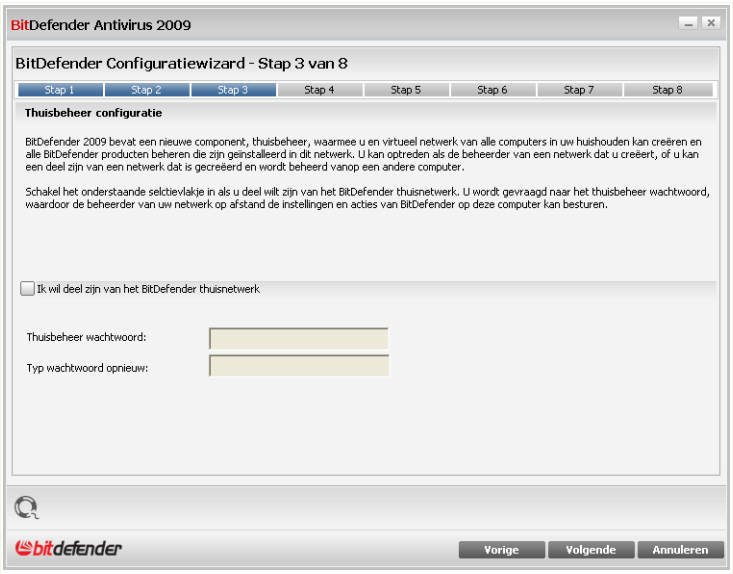
Weergaves

Kies een van de twee weergaves van de gebruikersinterface, afhankelijk van uw ervaring met BitDefender:

- **Basisweergave.** Eenvoudige interface voor beginners en gebruikers die basistaken willen uitvoeren en problemen eenvoudig oplossen. U hoeft alleen maar de BitDefender waarschuwingen te volgen en de aangegeven problemen oplossen.
- **Geavanceerde weergave.** Geavanceerde weergave voor meer technische gebruikers die het product volledig willen configureren. U kan elke productcomponent configureren en geadvanceerde taken uitvoeren.

Klik op **Volgende** om door te gaan.

2.2.3. Stap 3/8 - BitDefender netwerk configureren



BitDefender netwerkconfiguratie

Met BitDefender kan u een virtueel netwerk van de computers in uw huishouden creëren en de op dit netwerk geïnstalleerde BitDefender producten beheren.

Volg deze stappen als u deze computer wilt opnemen in een BitDefender thuisnetwerk:

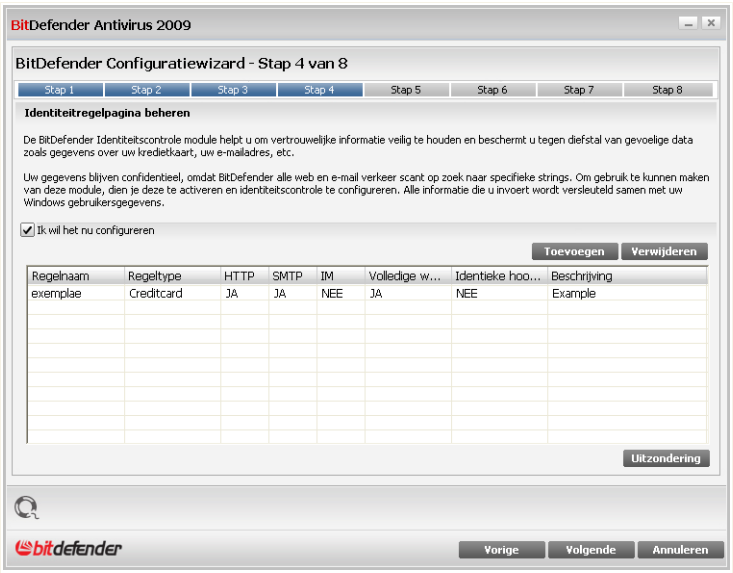
1. Selecteer **Ik wil deel zijn van het BitDefender thuisnetwerk**.
2. Voer hetzelfde administrator wachtwoord in elk van de bewerkingsvelden in.

Belangrijk

Met het wachtwoord kan een administrator dit BitDefender product beheren vanaf een andere computer.

Klik op **Volgende** om door te gaan.

2.2.4. Stap 4/8 - Identiteitscontrole configureren



Identiteitscontrole configuratie

Identiteitscontrole beschermt u tegen diefstal van gevoelige data als u online bent. Op basis van de door u gecreëerde regels scant Identiteitscontrole het web, e-mail en instant messaging verkeer dat uw computer verlaat op specifieke tekenreeksen (bijvoorbeeld uw creditcardnummer). Als er een overeenkomst is gevonden, wordt de betreffende webpagina, e-mail of instant message geblokkeerd.

Volg deze stappen als u Identiteitscontrole wilt gebruiken:

1. Selecteer **Ik wil dit nu configureren**.
2. Creëer regels om uw gevoelige data te beschermen. Meer informatie vindt u onder “Identiteitscontroleregels maken” (p. 15).
3. Definieer indien nodig specifieke uitzonderingen op de door u gecreëerde regels. Meer informatie vindt u onder “Identiteitscontrole uitzonderingen definiëren” (p. 16).

Klik op **Volgende** om door te gaan.

Identiteitscontroleregels maken

Om een Identiteitscontroleregel te creëren, klikt u op **Toevoegen**. Het configuratievenster wordt weergegeven.

Identiteitscontroleregel

U moet de volgende parameters instellen:

- **Regelnaam** - voer de naam van de regel in dit bewerkingsveld in.
- **Regeltype** - kies het type regel (adres, naam, creditcard, PIN, BSN, enz.).
- **Regeldata** - voer de te beveiligen data in dit bewerkingsveld in. Bijvoorbeeld, als u uw credicardnummer wilt beveiligen, voer het dan hier in zijn geheel of gedeeltelijk in

> ***Opmerking***
> Als u minder dan drie tekens invoert, wordt u gevraagd de gegevens te valideren. Wij raden u aan minstens drie tekens in te voeren om te vermijden dat berichten en webpagina's ten onrechte worden geblokkeerd.

U kunt ervoor kiezen de regels alleen toe te passen als de regeldata overeenkomen met volledige woorden of als de regeldata en de gedetecteerde tekenreeks overeenkomen.

Om snel te zien welke informatie de regel blokkeert, geeft u een gedetailleerde beschrijving in het bewerkingsveld.

Om het te scannen type verkeer aan te geven, configureert u deze opties:

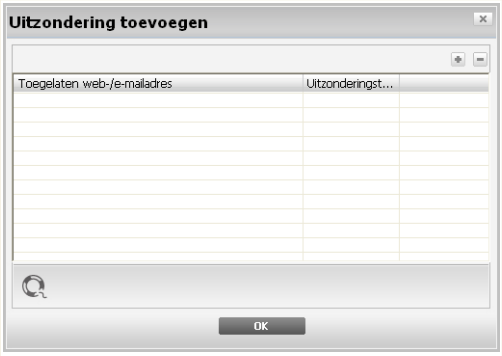
- **HTTP scannen** - scant het HTTP-verkeer (web) en blokkeert de uitgaande data die overeenkomt met de regeldata.
- **SMTP scannen** - scant het SMTP-verkeer (mail) en blokkeert de uitgaande e-mailberichten die de regeldata bevatten.
- **Instant Messaging scannen** - scant het Instant Messaging verkeer en blokkeert de uitgaande chatberichten die de regeldata bevatten.

Klik op **OK** om de regel toe te voegen.

Identiteitscontrole uitzonderingen definiëren

Er zijn situaties waarin u uitzonderingen op specifieke identiteitsregels moet definiëren. Laten we even een situatie bekijken waarbij u een regel hebt gemaakt die verhindert dat uw creditcardnummer via HTTP (het web) wordt verzonden. Telkens wanneer uw creditcardnummer vanaf uw gebruikersaccount naar een website wordt verzonden, wordt de desbetreffende pagina geblokkeerd. Als u bijvoorbeeld schoenen wilt kopen in een online winkel (waarvan u zeker bent dat deze veilig is), moet u een uitzondering op de desbetreffende regel opgeven.

Klik op **Uitzonderingen** om het venster te openen waarin u de uitzonderingen kunt beheren.



Identiteitscontrole uitzonderingen

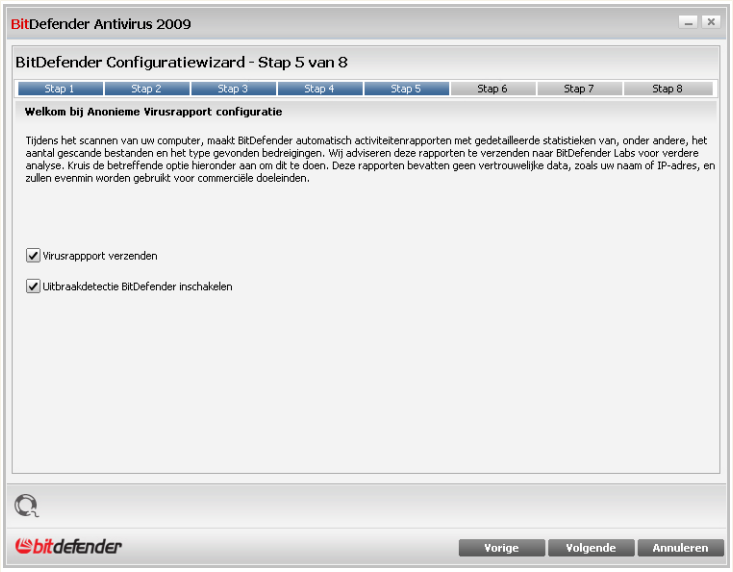
Volg deze stappen om een uitzondering toe te voegen:

1. Klik op de knop **Toevoegen** om een nieuwe invoer in de tabel toe te voegen.
2. Dubbelklik op **Toegelaten adres opgeven** en geef het webadres of het e-mailadres op dat u wilt toevoegen als uitzondering.
3. Dubbelklik op **Type kiezen** en selecteer de optie die overeenkomt met het eerder opgegeven adrestype in het menu.
   - Selecteer **HTTP** als u een webadres hebt opgegeven.
   - Selecteer **SMTP** als u een e-mailadres hebt opgegeven.

Om een uitzondering te verwijderen, selecteert u deze en klikt u op de knop **Verwijderen**.

Klik op **OK** om het venster te sluiten.

2.2.5. Stap 5/8 - Virusrapportage configureren



Virusrapport opties

BitDefender kan rapporten met betrekking tot virussen die op uw computer werden geïdentificeerd naar de BitDefender Labs verzenden om virusuitbraken te volgen.

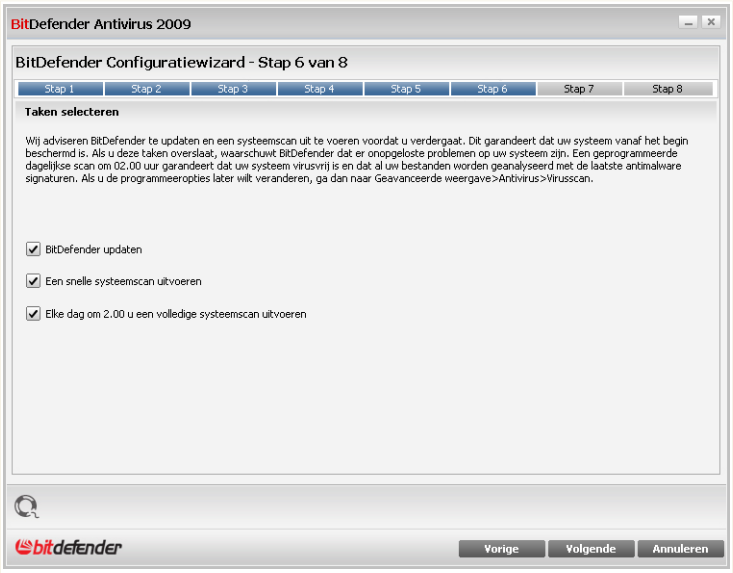
U kan de volgende opties configureren:

- **Virusrapporten verzenden** - verzendt rapporten met betrekking tot virussen die op uw computer werden geïdentificeerd naar de BitDefender Labs.
- **BitDefender Uitbraakdetectie inschakelen** - verzendt rapporten met betrekking tot potentiële virusuitbraken naar de BitDefender Labs.

Opmerking
De rapporten bevatten geen vertrouwelijke gegevens, zoals uw naam of IP-adres en zullen niet worden gebruikt voor commerciële doeleinden.

Klik op **Volgende** om door te gaan.

2.2.6. Stap 6/8 – De uit te voeren taken selecteren



Taakselectie

Stel BitDefender Antivirus 2009 in om belangrijke taken voor de beveiliging van uw systeem uit te voeren. De volgende opties zijn beschikbaar:

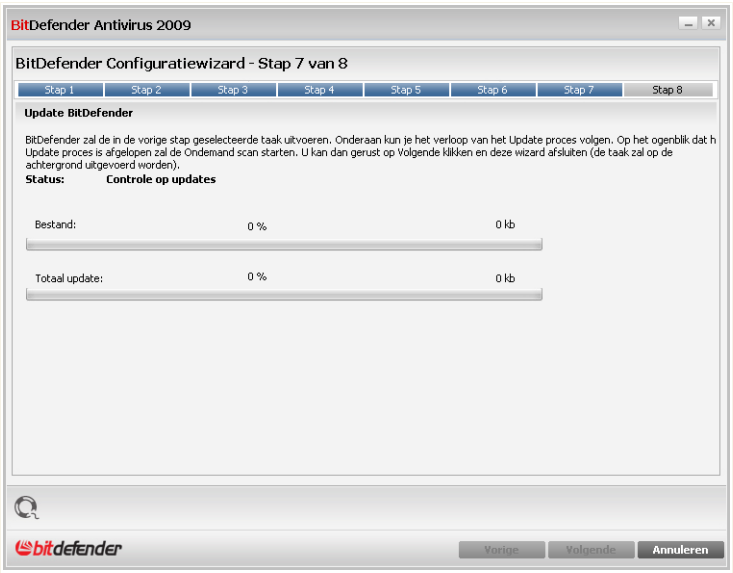
- **De BitDefender-engines updaten (kan opnieuw opstarten vereisen)** - bij de volgende stap wordt een update van de BitDefender-engines uitgevoerd om uw computer te beschermen tegen de meest recente bedreigingen.
- **Voer een snelle systeemscan uit (kan opnieuw opstarten vereisen)** - bij de volgende stap wordt een snelle systeemscan uitgevoerd zodat BitDefender kan controleren of uw bestanden in de mappen `Windows` en `Program Files` niet zijn geïnfecteerd.
- **Elke dag om 2 uur een volledige systeemscan uitvoeren** - voert elke dag om 2 uur een volledige systeemscan uit.

Belangrijk
Wij raden u aan deze opties in te schakelen voordat u naar de volgende stap gaat, zodat de beveiliging van uw systeem gegarandeerd is.

Als u alleen de laatste optie of geen enkele optie selecteert, wordt de volgende stap overgeslagen.

Klik op **Volgende** om door te gaan.

2.2.7. Stap 7/8 - Wacht tot de taken zijn voltooid

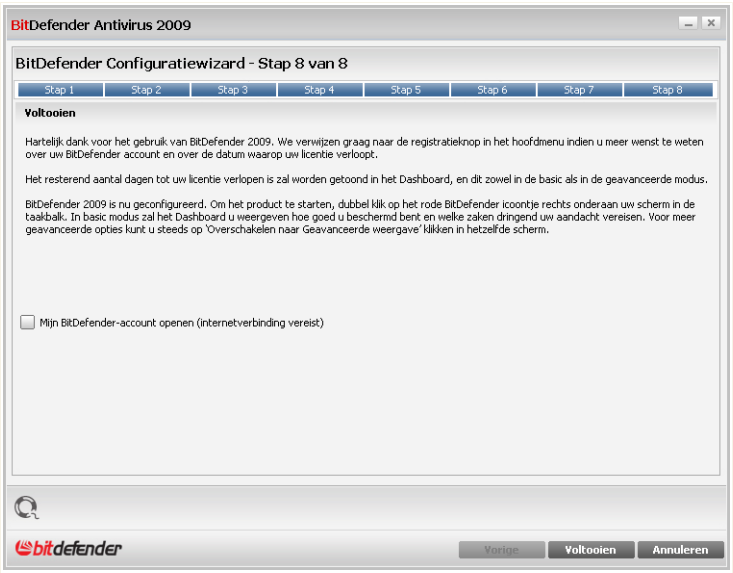


Taakstatus

Wacht tot de taak of taken zijn voltooid. U kunt de status bekijken van de taak of taken die in de vorige stap zijn geselecteerd.

Klik op **Volgende** om door te gaan.

2.2.8. Stap 8/8 – Voltooien



Voltooien

Selecteer **Mijn BitDefender-account openen** om naar uw BitDefender-account te gaan. Internetverbinding vereist.

Klik op **Voltooien**.

3. Upgrade

Volg deze stappen om een oudere versie van BitDefender te upgraden naar BitDefender Antivirus 2009:

1. Verwijder de oudere versie van BitDefender van uw computer. Raadpleeg het Help-bestand of de handleiding van het product voor meer informatie.
2. Start de computer opnieuw.
3. Installeer BitDefender Antivirus 2009 zoals beschreven in het hoofdstuk "*BitDefender installeren*" (p. 4) van deze handleiding.

4. BitDefender repareren of verwijderen

Als u **BitDefender Antivirus 2009** wilt repareren of verwijderen, volg dan dit pad vanaf het startmenu van Windows: **Start** → **Programma's** → **BitDefender 2009** → **Repareren of verwijderen**.

U wordt gevraagd uw keuze te bevestigen door te klikken op **Volgende**. Een nieuw venster wordt geopend, waarin u het volgende kunt selecteren:

- **Repareren** - om alle programmacomponenten die bij de vorige installatie werden geïnstalleerd, opnieuw te installeren.

  Als u ervoor kiest BitDefender te repareren, verschijnt een nieuw venster. Klik op **Repareren** om het reparatieproces te starten.

  Start de computer opnieuw op nadat u dit wordt gevraagd en klik daarna op **Installeren** om BitDefender Antivirus 2009 opnieuw te installeren.

  Nadat het installatieproces is voltooid, verschijnt een nieuw venster. Klik op **Voltooien**.

- **Verwijderen** - om alle geïnstalleerde componenten te verwijderen.

  Opmerking
  Wij raden u aan de optie **Verwijderen** te selecteren voor een zuivere nieuwe installatie.

  Als u ervoor kiest BitDefender te verwijderen, verschijnt een nieuw venster.

  Belangrijk
  Windows Vista alleen! Wanneer u BitDefender verwijdert, bent u niet langer beveiligd tegen malwarebedreigingen, zoals virussen en spyware. Als u wilt dat Windows Defender wordt ingeschakeld nadat u BitDefender hebt verwijderd, schakelt u het overeenkomende selectievakje in.

  Klik op **Verwijderen** om het verwijderen van BitDefender Antivirus 2009 van uw computer te starten.

  Tijdens het verwijderen wordt u gevraagd ons uw feedback te geven. Klik op **OK** om deel te nemen aan een online onderzoek van niet meer dan vijf korte vragen. Als u niet wilt deelnemen aan het onderzoek, klikt u op **Annuleren**.

  Nadat het verwijderen is voltooid, verschijnt een nieuw venster. Klik op **Voltooien**.

Opmerking

Nadat het verwijderen is voltooid, raden wij u aan de map `BitDefender` te verwijderen uit de map `Program Files`.

Er is een fout opgetreden tijdens het verwijderen van BitDefender

Als er een fout is opgetreden tijdens het verwijderen van BitDefender, wordt het verwijderen afgebroken en verschijnt een nieuw venster. Klik op **Hulpprogramma Verwijderen uitvoeren** om zeker te zijn dat BitDefender volledig is verwijderd. Met het hulpprogramma voor het verwijderen worden alle bestanden en registersleutels verwijderd die niet tijdens het automatisch verwijderen werden verwijderd.

Basisbeheer

5. Aan de slag

Zodra u BitDefender hebt geïnstalleerd is uw computer beschermd.

5.1. Start BitDefender Antivirus 2009

De eerste stap om het beste uit BitDefender te halen, is het starten van de applicatie.

Om toegang te krijgen tot het hoofdscherm van BitDefender 2009, gebruikt u het menu Start van Windows en volgt u het pad **Start → Programma's → BitDefender 2009 → BitDefender Antivirus 2009**. U kunt dit ook sneller doen door te dubbelklikken op het **BitDefender-pictogram** in het systeemvak.

5.2. Gebruikersinterface weergavemodus

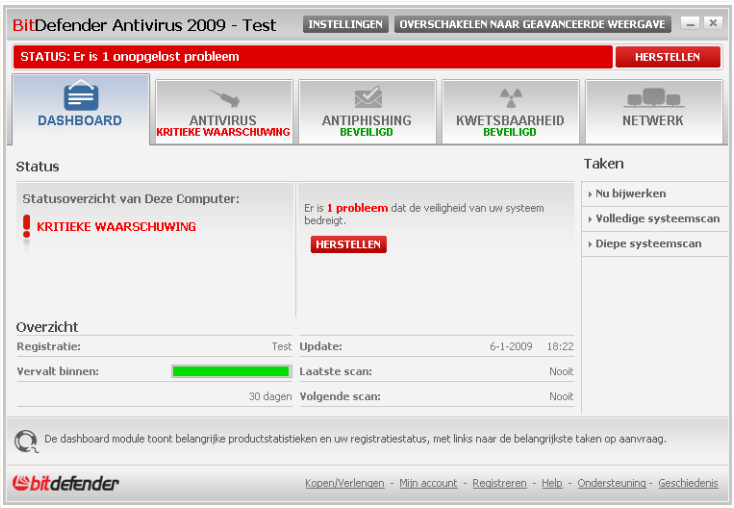
BitDefender Antivirus 2009 is bestemd voor zowel technici of beginners op computergebied. De grafische gebruikersinterface is ontworpen voor elke categorie van gebruikers.

U kan kiezen om BitDefender te bekijken in de Basis of Geavanceerde modus, afhankelijk van uw ervaring met ons product.

Opmerking
U kan gemakkelijk een van deze vensters selecteren door te klikken op respectievelijk de knop **Basisweergave** of de knop **Geavanceerde weergave**.

5.2.1. Basisweergave

Basisweergave is een eenvoudige interface die toegang geeft tot het basisniveau van alle modules. U moet de waarschuwingen en kritieke waarschuwingen en ongewenste problemen oplossen.



Basisweergave

- Zoals u ziet, zijn er aan de bovenkant van het venster twee knoppen en een statusbalk.

Item	Beschrijving
Instellingen	Opent een venster waarin u gemakkelijk belangrijke veiligheidsmodules kan aan- en uitzetten.
Geavanceerde instellingen	Opent het Geavanceerde weergavevenster. Hier ziet u de volledige lijst van modules en kan u de details configureren van de component. BitDefender onthoudt deze optie de volgende keer dat u de gebruikersinterface opent.
Status	Bevat informatie over en helpt u bij het herstellen van de veiligheidskwetsbaarheden van uw computer.

- In het midden van het venster zijn er vijf tabs.

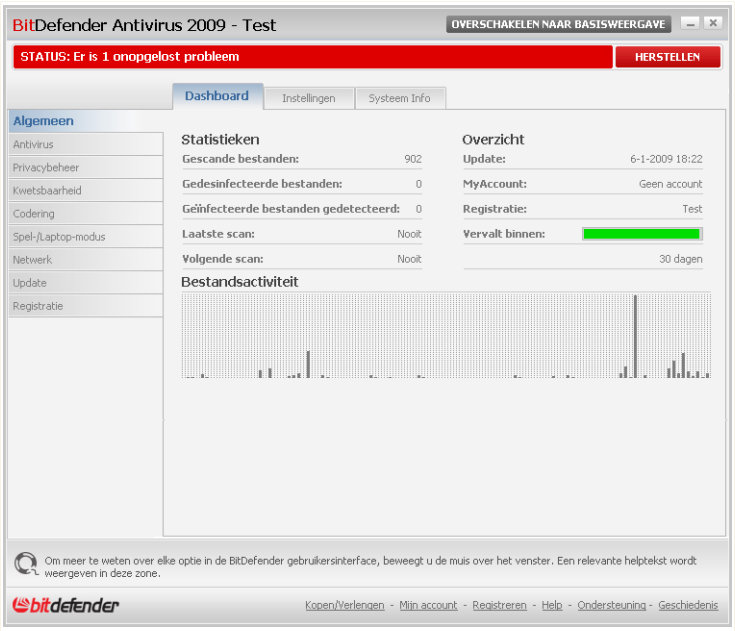
Tab	Beschrijving
Dashboard	Toont belangrijke productstatistieken en uw registratiestatus, met links naar de belangrijkste taken op aanvraag.
Antivirus	Toont de status van de antivirusmodule die u helpt BitDefender up-to-date en uw computer virusvrij te houden.
Antiphishing	Toont de status van de antiphishingmodule die garandeert dat alle webpagina's, die u via Internet Explorer of Firefox opent, veilig zijn.
Kwetsbaarheid	Toont de status van de kwetsbaarheidsmodule die helpt de cruciale software op uw PC up-to-date te houden.
Netwerk	Toont de structuur van het BitDefender thuisnetwerk.

- Daarnaast bevat het Basisweergavevenster van BitDefender meerdere nuttige snelkoppelingen.

Koppeling	Beschrijving
Mijn account	Hiermee kan u uw BitDefender account creëren of erop inloggen. BitDefender Account geeft u gratis toegang tot technische ondersteuning
Registreren	Hier kan u een nieuwe licentiesleutel invoeren of de huidige licentiesleutel en de registratiestatus zien.
Help	Opent een help bestand dat u leert hoe u BitDefender gebruikt.
Ondersteuning	Hiermee kan u contact maken met het BitDefender-ondersteuningsteam.
Geschiedenis	Hier ziet u een gedetailleerde geschiedenis van alle door BitDefender op uw systeem uitgevoerde taken.

5.2.2. Geavanceerde weergave

Geavanceerde weergave geeft toegang tot elke specifieke component van het BitDefender product. U kan geavanceerde instellingen configureren en geavanceerde opties instellen.



Geavanceerde weergave

- Zoals u ziet, zijn er aan de bovenkant van het venster een knop en een statusbalk.

Item	*Beschrijving*
Geavanceerde weergave	Opent het Basisweergavevenster. Hier ziet u de basisinterface van BitDefender met de belangrijkste modules (Beveiliging, Tune-up, Bestandsbeheer, Netwerk) en een dashboard. BitDefender onthoudt deze optie de volgende keer dat u de gebruikersinterface opent.
Status	Bevat informatie over en helpt u bij het herstellen van de veiligheidskwetsbaarheden van uw computer.

- Aan de linkerzijde van het venster ziet u een menu met alle beveiligingsmodules.

Module	Beschrijving
Algemeen	Hiermee gaat u naar de algemene instellingen of ziet u het dashboard en gedetailleerde systeeminformatie.
Antivirus	Hiermee kan u uw virusschild en de scanning operaties in detail configureren, de uitzonderingen instellen en de quarantaine module configureren.
Privacybeheer	Hiermee voorkomt u diefstal van data van uw computer en beschermt u uw privacy als u online bent.
Encryptie	Hiermee encrypteert u Yahoo en Windows Live (MSN) Messenger verbindingen.
Kwetsbaarheid	Hiermee kan u de cruciale software op uw PC up-to-date houden.
Spel-/Laptop-modus	Hiermee kan u de geprogrammeerde BitDefender taken uitstellen als uw laptop op de accu werkt en verschijnen er geen waarschuwingen en pop-ups tijdens het spelen.
Netwerk	Hiermee kan u de computers in uw huishouden configureren en beheren.
Update	Hiermee kan u informatie krijgen over de laatste updates, voor het updaten van het product en voor het configureren van de details van het updateproces.
Registratie	Hiermee kan u BitDefender Antivirus 2009 registreren, de licentiesleutel veranderen, of een BitDefender-account creëren.

- Daarnaast bevat het Geavanceerde weergavevenster van BitDefender meerdere nuttige snelkoppelingen.

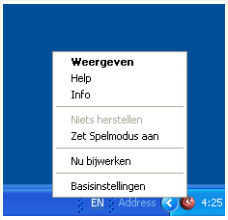
Koppeling	Beschrijving
Mijn account	Hiermee kan u uw BitDefender account creëren of erop inloggen. BitDefender Account geeft u gratis toegang tot technische ondersteuning
Registreren	Hier kan u een nieuwe licentiesleutel invoeren of de huidige licentiesleutel en de registratiestatus zien.

Koppeling	Beschrijving
Help	Opent een help bestand dat u leert hoe u BitDefender gebruikt.
Ondersteuning	Hiermee kan u contact maken met het BitDefender-ondersteuningsteam.
Geschiedenis	Hier ziet u een gedetailleerde geschiedenis van alle door BitDefender op uw systeem uitgevoerde taken.

5.3. BitDefender Icon in het Systeemvak

Om het volledige product sneller te beheren, kunt u ook het BitDefender-pictogram in het systeemvak gebruiken.

Als u dubbelklikt op dit pictogram, wordt BitDefender geopend. Als u rechtsklikt op het pictogram, verschijnt een contextafhankelijk menu waarmee u het BitDefender-product snel kan beheren.



BitDefender-pictogram

- **Weergeven** - opent BitDefender.
- **Help** - opent het help-bestand waarin BitDefender Antivirus 2009 in details wordt uitgelegd.
- **Info** - opent de webpagina van BitDefender.
- **Alle probl. herst.** - helpt u de zwakke punten in de beveiliging te verwijderen.
- **Spelmodus aan/uit** - zet de Spelmodus aan/uit.
- **Update nu** - start een directe update. Een nieuw venster verschijnt waarin u de updatestatus kan zien.
- **Basisinstellingen** - hiermee kan u belangrijke veiligheidsmodules gemakkelijk aan- of uitzetten. Een nieuw venster verschijnt waarin u deze met een enkele klik kan inschakelen/uitschakelen.

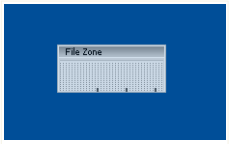
Als de Spelmodus is ingeschakeld, ziet u de letter G boven het BitDefender-pictogram.

Als kritieke problemen de veiligheid van uw systeem bedreigen, staat er een uitroepteken boven het BitDefender-pictogram. U kunt het aantal problemen dat uw systeem beïnvloedt, zien door de muis op het pictogram te plaatsen.

5.4. Scan activiteitenbalk

De **balk Scanactiviteit** is een grafische voorstelling van de scanactiviteit op uw systeem.

De grijze balken (de **Bestandzone**) toont het aantal gescande bestanden per seconde op een schaal van 0 tot 50.



Activiteitenbalk

Opmerking
De balk voor de scanactiviteit zal aangeven wanneer de real time-beveiliging is uitgeschakeld door een rood kruis over de **Bestand** weer te geven

U kunt de **balk Scanactiviteit** gebruiken om objecten te scannen. Sleep de objecten die u wilt scannen en zet ze neer op de balk. Meer informatie vindt u onder "*Scannen door slepen & neerzetten*" (p. 120).

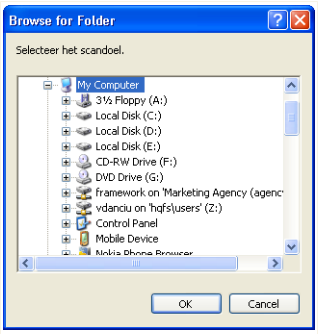
Als u deze grafische voorstelling niet langer wilt zien, klik er dan op met de rechtermuisknop en selecteer **Verbergen**. Volg deze stappen om dit venster geheel te verbergen:

1. Klik op **Geavanceerde weergave** (als u in de **Basisweergave** bent).
2. Klik op de module **Algemeen** in het linkermenu
3. Klik op het tabblad **Instellingen**.
4. Maak het vakje **De scanactiviteitbalk inschakelen (grafiek op het scherm van productactiviteit)** leeg.

5.5. BitDefender Handmatig scannen

Als u een bepaalde map snel wilt scannen, kunt u BitDefender Handmatig scannen gebruiken.

Om toegang te krijgen tot BitDefender Handmatig scannen, gebruikt u het menu Start van Windows via het pad **Start → Programmas → BitDefender 2009 → BitDefender Handmatig scannen** Het volgende venster wordt geopend:



BitDefender Handmatig scannen

U hoeft alleen maar door de mappen te bladeren, de map die u gescand wilt hebben te selecteren en te klikken op **OK**. De BitDefender Scanner verschijnt en begeleidt u door het scanproces.

5.6. Spelmodus

De nieuwe Spelmodus verandert tijdelijk de beveiligingsinstellingen om de snelheid van het systeem zo weinig mogelijk te beïnvloeden. Als u in de Spelmodus bent, worden de volgende instellingen toegepast:

- Minimale processortijd & geheugenverbruik
- Automatische updates & scans uitstellen
- Alle waarschuwingen en pop-ups tegenhouden
- Alleen de belangrijkste bestanden scannen

Als de Spelmodus is ingeschakeld, ziet u de letter `G` boven het BitDefender-pictogram.

5.6.1. Gebruik van de Spelmodus

Gebruik één van de volgende methodes om de Spelmodus aan te zetten:

- Rechtsklik op het BitDefender pictogram in het systeemvak en selecteer **Spelmodus aanzetten**.
- Druk op `Ctrl+Shift+Alt+G` (de standaard sneltoets).

Belangrijk
Vergeet niet de Spelmodus uit te zetten als u klaar bent. Doe dit op dezelfde manier als bij het aanzetten.

5.6.2. Veranderen van de Spelmodus sneltoets

Volg deze stappen als u de sneltoets wilt veranderen:

1. Klik op **Geavanceerde weergave** (als u in de **Basisweergave** bent).
2. Klik op **Spel-/Laptopmodus** in het menu aan de linkerzijde.
3. Klik op het tabblad **Spelmodus**.
4. Klik op de knop **Geavanceerde instellingen**.
5. Stel de gewenste sneltoets in onder de **Sneltoets gebruiken** optie:
   - Kies de gewijzigde toetsen die u wilt gebruiken door één van de volgende aan te kruisen: Control toets (`Ctrl`), Shift toets (`Shift`) of Alternate toets (`Alt`).
   - Typ in het invulveld de letter van de normale toets die u wilt gebruiken.

   Bijvoorbeeld, als u de `Ctrl+Alt+D` sneltoets wilt gebruiken, kruist u `Ctrl` en `Alt` aan en typt u `D`.

Opmerking
Door het kruisje naast **Sneltoets gebruiken** te verwijderen, schakelt u de sneltoets uit.

5.7. Integratie in webbrowsers

BitDefender beveiligt u tegen phishing-pogingen terwijl u op het internet surft. Het programma scant de bezochte websites en waarschuwt u als er phishing-bedreigingen zijn. U kunt een Witte lijst configureren van websites die niet door BitDefender moeten worden gescand.

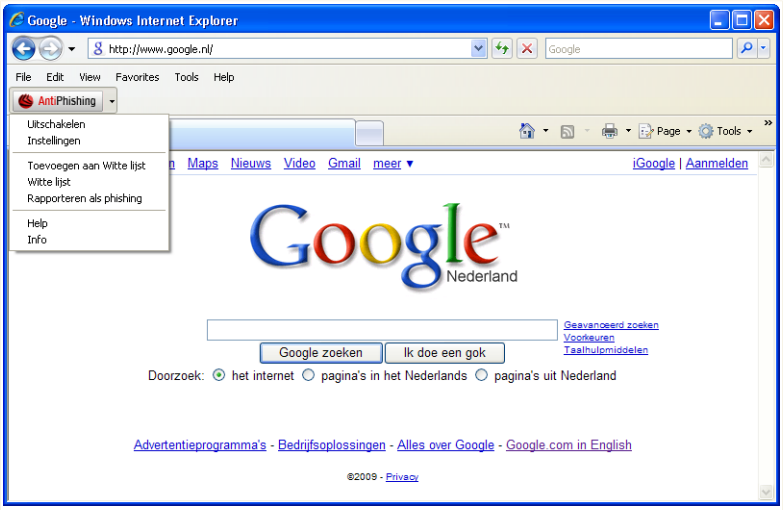
BitDefender wordt rechtstreeks in de volgende webbrowsers geïntegreerd door middel van een intuïtieve en gemakkelijk te gebruiken werkbalk:

- Internet Explorer
- Mozilla Firefox

U kan de antiphishing-beveiliging en de Witte lijst gemakkelijk en efficiënt beheren met de werkbalk van BitDefender Antiphishing die in de bovenstaande webbrowsers is geïntegreerd.

De antiphishing-werkbalk die wordt voorgesteld door het **BitDefender-pictogram**, bevindt zich bovenaan in de browser. Klik op dit pictogram om het werkbalkmenu te openen.

Opmerking
Als u de werkbalk niet kunt zien, opent u het menu **Weergave**, wijst u **Werkbalken** aan en selecteert u **Werkbalk BitDefender**.



Antiphishing-werkbalk

De volgende opdrachten zijn beschikbaar in het werkbalkmenu:

- Met **Inschakelen / Uitschakelen** - wordt de Antiphishing-werkbalk van BitDefender in- of uitgeschakeld.

Opmerking
Als u ervoor kiest de antiphishing-werkbalk uit te schakelen, bent u niet langer beveiligd tegen phishing-pogingen.

- **Instellingen** - opent een venster waarin u de instellingen voor de antiphishing-werkbalk kunt opgeven.

  De volgende opties zijn beschikbaar:
  - **Scannen inschakelen** - schakelt het scannen van antiphishing in.
  - **Vragen vóór toevoegen aan witte lijst** - vraagt uw bevestiging voordat een website aan de witte lijst wordt toegevoegd.
- **Toevoegen aan Witte lijst** - voegt de huidige website toe aan de Witte lijst.

  Opmerking
  Wanneer een site wordt toegevoegd aan de Witte lijst, betekent dit dat BitDefender de site niet langer zal scannen op phishing-pogingen. Wij raden u aan alleen sites die u volledig vertrouwt toe te voegen aan de Witte lijst.

- **Witte lijst tonen** - opent de Witte lijst.

  U kunt de lijst weergeven van alle websites die niet door de antiphishing-engines van BitDefender worden gecontroleerd.

  Als u een site uit de Witte lijst wilt verwijderen, zodat u op de hoogte wordt gebracht van eventuele phishing-bedreigingen op die pagina, klikt u op de knop **Verwijderen** naast de naam van de site.

  U kunt de sites die u volledig vertrouwt toevoegen aan de Witte lijst, zodat ze niet langer worden gescand door de antiphishing-engines. Om een site toe te voegen aan de Witte lijst, geeft u het adres van de site op in het overeenkomende veld en kikt u op **Toevoegen**.
- **Help** - opent het Help-bestand.
- **Info** - opent een venster waar u informatie over BitDefender kunt bekijken en waar u hulp kunt zoeken wanneer er zich een onverwachte gebeurtenis voordoet.

5.8. Integratie in Messenger

BitDefender heeft de encryptiemogelijkheden voor het beschermen van uw vertrouwelijke documenten en uw instant messaging gesprekken via Yahoo Messenger en MSN Messenger.

Standaard crypteert BitDefender al uw instant messaging chatsessies, op voorwaarde dat:

- uw chatpartner een BitDefender-versie heeft geïnstalleerd die IM Encryptie ondersteunt en IM Encryption is ingeschakeld voor de instant messaging applicatie die bij het chatten wordt gebruikt.

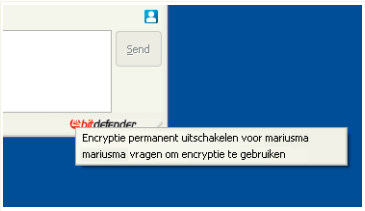
- U en uw chatpartner gebruiken ofwel Yahoo Messenger of Windows Live (MSN) Messenger.

Belangrijk
BitDefender crypteert een gesprek niet als een chatpartner een webgebaseerde chatapplicatie gebruikt, zoals Meebo, of en andere chatapplicatie die Yahoo Messenger of MSN ondersteunt.

U kan instant messaging encryptie gemakkelijk configureren met de BitDefender werkbalk in het chatvenster.

Als u rechtklikt op de BitDefender werkbalk krijgt u de volgende opties:

- Encryptie permanent aan/uit voor een bepaalde chatpartner
- Een bepaalde chatpartner vragen encryptie te gebruiken
- Een bepaalde chatpartner verwijderen uit de Zwarte lijst van Ouderlijk Toezicht

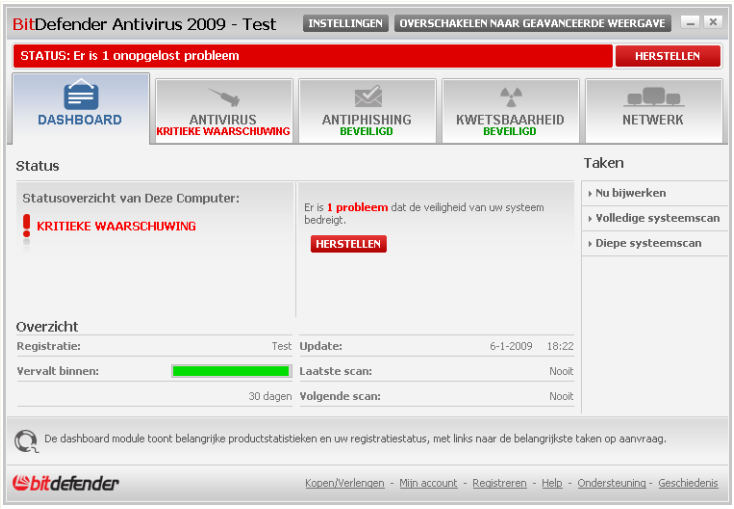


Instant Messaging (IM) encryptie opties:

Klik op een van bovengenoemde opties om die te gebruiken.

6. Dashboard

Als u klikt op de Dashboard-tab krijgt u belangrijke productstatistieken en uw registratiestatus te zien, met links naar de belangrijkste taken op aanvraag.



Dashboard

6.1. Overzicht

Hier ziet u een overzicht van statistieken over de updatestatus, uw accountstatus, registratie en licentie-informatie.

Item	Beschrijving
Laatste update	Geeft de datum waarop uw BitDefender product voor het laatst is geüpdatet. Voer regelmatig updates uit om uw systeem volledig te beschermen.
Mijn account	Geeft het e-mailadres dat u kan gebruiken om uw online account te openen en uw verloren BitDefender licentiesleutel op te halen,

Item	Beschrijving
	of te profiteren van BitDefender ondersteuning en andere aangepaste diensten.
Registratie	Geeft het type en de status van uw licentiesleutel. Om uw systeem veilig te houden moet u BitDefender vernieuwen of upgraden als uw sleutel is verlopen.
Verloopt over	Geeft het aantal dagen tot het verlopen van uw licentiesleutel.

Om BitDefender te updaten, klikt u op de knop **Update nu** in de taaksectie.

Volg deze stappen om uw BitDefender-account te creëren of erop in te loggen:

1. Klik op de link **Mijn Account** aan de onderkant van het venster. Een webpagina verschijnt.
2. Voer uw gebruikersnaam en wachtwoord in en klik op de knop **Login**.
3. Om een BitDefender-account te creëren, selecteert u **U hebt geen BitDefender-account?** en geeft u de vereiste informatie op.

Opmerking
De gegevens die u hier opgeeft blijven vertrouwelijk.

Volg deze stappen om BitDefender Antivirus 2009 te registreren:

1. Klik op de link **Mijn Account** aan de onderkant van het venster. Een stap-voor-stap registratiewizard verschijnt.
2. Klik op de ronde knop **Ik wil het product registreren met een nieuwe sleutel**.
3. Typ de mieuwe licentiesleutel in het bijbehorende tekstveld.
4. Klik op **Voltooien**.

Volg deze stappen om een nieuwe licenteiesleutel te kopen:

1. Klik op de link **Mijn Account** aan de onderkant van het venster. Een stap-voor-stap registratiewizard verschijnt.
2. Klik op de link **Uw BitDefender licentiesleutel vernieuwen**. Een webpagina verschijnt.
3. Klik op de knop **Nu kopen**.

6.2. Taken

Hier vindt u links naar de belangrijkste beveiligingstaken: volledige systeemscan, diepe scan, update nu.

De volgende knoppen zijn beschikbaar:

- **Volledige systeemscan** - start een complete scan van uw computer (exclusief archiefbestanden).
- **Diepe systeemscan** - start een complete scan van uw computer (inclusief archiefbestanden).
- **Update nu** - start een directe update.

6.2.1. Scannen met BitDefender

Om uw computer te scannen op malware, voert u een speciale scantaak uit door te klikken op de overeenkomende knop. In de volgende tabel staan de beschikbare scantaken met hun beschrijving:

Taak	Beschrijving
Volledige systeemscan	Scant het volledige systeem, behalve archieven. In de standaardconfiguratie wordt er gescand op alle types malware die de beveiliging van uw systeem bedreigen, zoals virussen, spyware, adware, rootkits en andere.
Diepe scan	Scant het volledige systeem. In de standaardconfiguratie wordt er gescand op alle types malware die de beveiliging van uw systeem bedreigen, zoals virussen, spyware, adware, rootkits en andere.

Opmerking
Omdat de taken **Diepe systeemscan** en **Volledige systeemscan** analyseren het volledige systeem. Het scannen kan enige tijd in beslag nemen. Wij raden u daarom aan deze taken uit te voeren met een lage prioriteit, of bij voorkeur wanneer uw systeem inactief is.

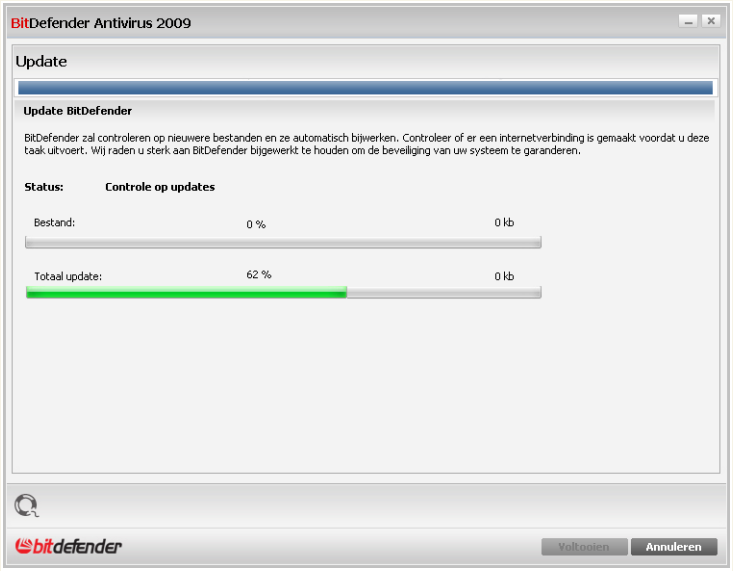
Wanneer u een proces Scannen op aanvraag start, verschijnt BitDefender Scanner, ongeacht of het om een snelle of volledige scan gaat.

Volg de begeleide procedure van drie stappen om het scanproces te voltooien.

6.2.2. Updaten BitDefender

Elke dag wordt nieuwe malware gevonden en geïdentificeerd. Het is dan ook heel belangrijk dat u BitDefender up-to-date houdt met de meest recente malware handtekeningen.

Standaard controleert BitDefender of er updates zijn als u uw computer aanzet en **ieder uur** daarna. Als u echter BitDefender wilt updaten, klik dan op **Update nu**. Het updateproces wordt gestart en het volgende venster verschijnt direct:



Updaten BitDefender

In dit venster kan u de status van het updateproces zien.

Het updateproces wordt geleidelijk uitgevoerd, wat betekent dat de te updaten bestanden een voor een worden vervangen. Op deze manier vormt het updateproces geen belemmering voor de werking van het product, en is tegelijk elke kwetsbaarheid uitgesloten.

Als u dit venster wilt sluiten, klik dan op **Annuleren**. Hierdoor stopt het updateproces echter niet.

Opmerking
Als u met het internet bent verbonden via een inbelverbinding, dan adviseren wij BitDefender regelmatig handmatig te updaten.

Start de computer indien nodig opnieuw op. Als het een belangrijke update betreft, wordt u gevraagd de computer opnieuw op te starten:

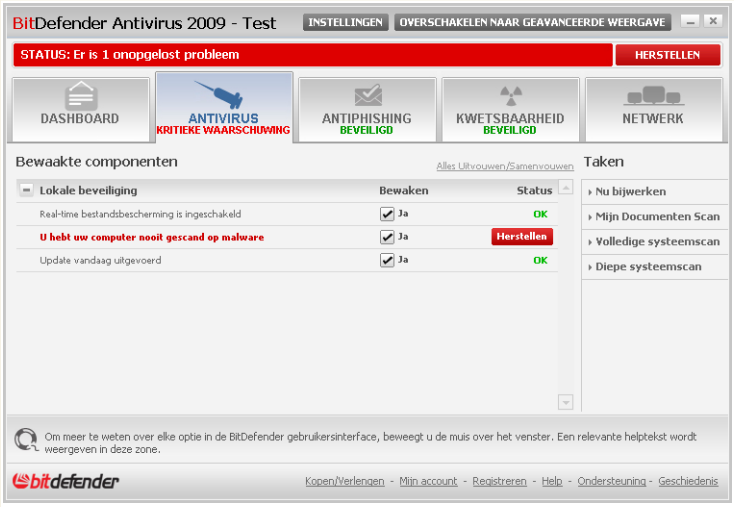
Klik op **Herstarten** om uw systeem direct opnieuw op te starten.

Als u uw systeem op een later tijdstip wilt herstarten, klik dan op **OK**. Wij adviseren dat u uw systeem zo snel mogelijk opnieuw opstart.

7. Antivirus

BitDefender wordt geleverd met een Antivirusmodule waarmee u uw BitDefender up-to-date en uw computer virusvrij houdt.

Klik op het tabblad **Antivirus** om de Antivirusmodule te openen.



Antivirus

De Anitivirusmodule bestaat uit twee delen:

- **Bewaakte componenten** - Toont u de complete lijst van bewaakte componenten voor elke veiligheidsmodule. U kan kiezen welke van de modules moet worden bewaakt. Wij adviseren het bewaken van alle componenten in te schakelen.
- **Taken** - Hier vindt u links naar de belangrijke beveiligingstaken: volledige systeemscan, diepe scan, update nu.

7.1. Bewaakte componenten

De volgende component wordt bewaakt:

Categorie	Beschrijving
Lokale beveiliging	Hier kan u de status controleren van elke beveiligingsmodule die op uw computer opgeslagen objecten (bestanden, register, geheugen, enz.) beschermt.

Klik op het vakje met het teken "+" om een categorie te openen of klik op het vakje met het teken "-" om een categorie te sluiten.

7.1.1. Lokale beveiliging

Wij weten dat het belangrijk is om gewaarschuwd te worden als een probleem de veiligheid van uw computer bedreigt. Door het bewaken van elke beveiligingsmodule laat BitDefende 2009 u niet alleen weten wanneer u de instellingen configureert die de veiligheid van uw computer kunnen beïnvloeden, maar ook wanneer u belangrijke taken vergeet uit te voeren.

De problemen voor de lokale veiligheid worden in duidelijke zinnen beschreven. In lijn met elke zin ziet u, als er iets de veiligheid van uw computer bedreigt, een rode statusknop **Herstellen**. Anders ziet u een goene statusknop **OK**.

Probleem	Beschrijving
Real-time bestandsbescherming is ingeschakeld	Garandeert dat alle bestanden worden gescand, ongeacht of ze door u of door een toepassing op uw systeem zijn geopend.
U hebt uw computer vandaag gescand op malware	Wij adviseren met kracht om zo spoedig mogelijk een op aanvraag scan uit te voeren, om te controleren of de op uw computer opgeslagen bestanden geen malware bevatten.
Automatische update is ingeschakeld	Houd automatische update ingeschakeld om te garanderen dat de malware signaturen van uw BitDefender product regelmatig geüpdatet worden.
Update nu bezig	Update van product en malware signaturen wordt uitgevoerd.

Als de statusknoppen groen zijn, is het veiligheidsrisico van uw systeem minimaal. Volg deze stappen op de knoppen groen te maken:

1. Klik op de knop **Herstellen** om de zwakke punten in de beveiliging een voor een te herstellen.

2. Als een probleem niet er plaatse wordt opgelost, moet u de wizard volgen om het op te lossen.

Als u iets niet wilt controleren, verwijder dan het kruisje uit het vakje **Ja, deze component bewaken**.

7.2. Taken

Hier vindt u links naar de belangrijkste beveiligingstaken: volledige systeemscan, diepe scan, update nu.

De volgende knoppen zijn beschikbaar:

- **Volledige systeemscan** - start een complete scan van uw computer (exclusief archiefbestanden).
- **Diepe systeemscan** - start een complete scan van uw computer (inclusief archiefbestanden).
- **Mijn documenten scannen** - start een snelscan van uw documenten en instellingen.
- **Update nu** - start een directe update.

7.2.1. Scannen met BitDefender

Om uw computer te scannen op malware, voert u een speciale scantaak uit door te klikken op de overeenkomende knop. In de volgende tabel staan de beschikbare scantaken met hun beschrijving:

Taak	Beschrijving
Volledige systeemscan	Scant het volledige systeem, behalve archieven. In de standaardconfiguratie wordt er gescand op alle types malware die de beveiliging van uw systeem bedreigen, zoals virussen, spyware, adware, rootkits en andere.
Diepe scan	Scant het volledige systeem. In de standaardconfiguratie wordt er gescand op alle types malware die de beveiliging van uw systeem bedreigen, zoals virussen, spyware, adware, rootkits en andere.
Scan Mijn documenten	Gebruik deze taak om belangrijke gangbare gebruikersmappen te scannen: `Mijn documenten`, `Bureaublad` en `Opstarten`. Dit garandeert de

Taak	Beschrijving
	veiligheid van uw documenten, een veilige werkruimte en schone applicaties bij het opstarten.

Opmerking
Omdat de taken **Diepe systeemscan** en **Volledige systeemscan** analyseren het volledige systeem. Het scannen kan enige tijd in beslag nemen. Wij raden u daarom aan deze taken uit te voeren met een lage prioriteit, of bij voorkeur wanneer uw systeem inactief is.

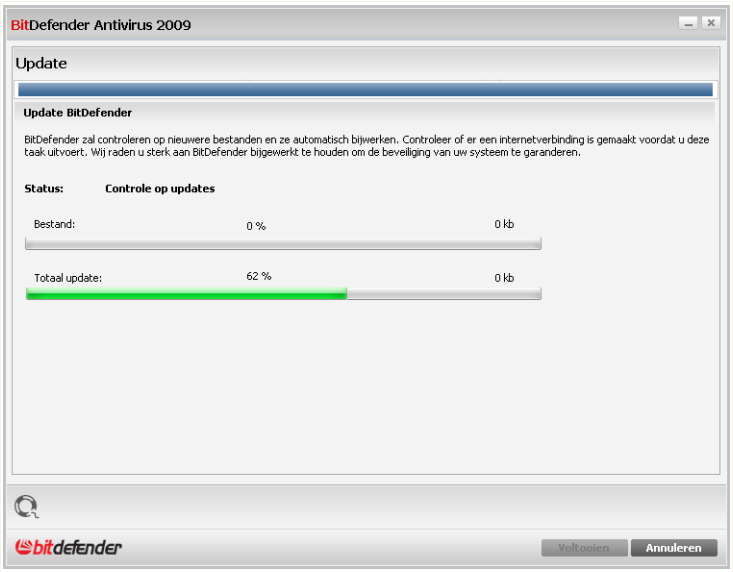
Wanneer u een proces Scannen op aanvraag start, verschijnt BitDefender Scanner, ongeacht of het om een snelle of volledige scan gaat.

Volg de begeleide procedure van drie stappen om het scanproces te voltooien.

7.2.2. Updaten BitDefender

Elke dag wordt nieuwe malware gevonden en geïdentificeerd. Het is dan ook heel belangrijk dat u BitDefender up-to-date houdt met de meest recente malware handtekeningen.

Standaard controleert BitDefender of er updates zijn als u uw computer aanzet en **ieder uur** daarna. Als u echter BitDefender wilt updaten, klik dan op **Update nu**. Het updateproces wordt gestart en het volgende venster verschijnt direct:



Updaten BitDefender

In dit venster kan u de status van het updateproces zien.

Het updateproces wordt geleidelijk uitgevoerd, wat betekent dat de te updaten bestanden een voor een worden vervangen. Op deze manier vormt het updateproces geen belemmering voor de werking van het product, en is tegelijk elke kwetsbaarheid uitgesloten.

Als u dit venster wilt sluiten, klik dan op **Annuleren**. Hierdoor stopt het updateproces echter niet.

Opmerking
Als u met het internet bent verbonden via een inbelverbinding, dan adviseren wij BitDefender regelmatig handmatig te updaten.

Start de computer indien nodig opnieuw op. Als het een belangrijke update betreft, wordt u gevraagd de computer opnieuw op te starten:

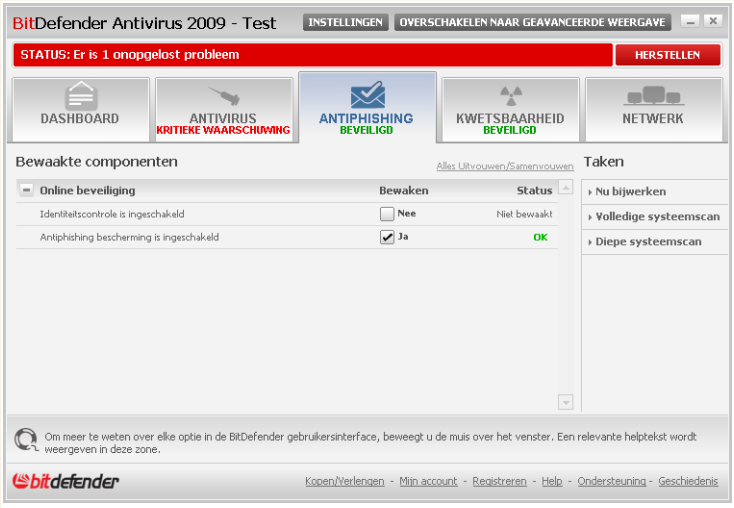
Klik op **Herstarten** om uw systeem direct opnieuw op te starten.

Als u uw systeem op een later tijdstip wilt herstarten, klik dan op **OK**. Wij adviseren dat u uw systeem zo snel mogelijk opnieuw opstart.

8. Antiphishing

BitDefender heeft een antiphishingmodule die garandeert dat alle webpagina's, die u via Internet Explorer of Firefox opent, veilig zijn.

Klik op het tabblad **Antiphishing** om de antiphishingmodule te openen.



Antiphishing

De antiphishingmodule bestaat uit twee delen:

- **Bewaakte componenten** - Toont u de complete lijst van bewaakte componenten voor elke veiligheidsmodule. U kan kiezen welke van de modules moet worden bewaakt. Wij adviseren het bewaken van alle componenten in te schakelen.
- **Taken** - Hier vindt u links naar de belangrijke beveiligingstaken: volledige systeemscan, diepe scan, update nu.

8.1. Bewaakte componenten

De volgende component wordt bewaakt:

Categorie	Beschrijving
Online beveiliging	Hier kan u de status controleren van elke beveiligingsmodule die uw online transacties en uw computer beschermt tijdens de verbinding met het internet.

Klik op het vakje met het teken "+" om een categorie te openen of klik op het vakje met het teken "-" om een categorie te sluiten.

8.1.1. Online beveiliging

De problemen voor de online beveiliging worden in duidelijke zinnen beschreven. In lijn met elke zin ziet u, als er iets de veiligheid van uw computer bedreigt, een rode statusknop **Herstellen**. Anders ziet u een goene statusknop **OK**.

Probleem	Beschrijving
Gespreksencryptie voor IM is ingeschakeld	Als uw IM contacten BitDefender 2009 hebben geïnstalleerd, worden alle IM gesprekken via Yahoo! Messenger en Windows Live Messenger gecrypteerd. Wij adviseren om gespreksencryptie voor IM ingeschakeld te hebben om te garanderen dat uw IM gesprekken privé blijven.
Firefox antiphishing bescherming is ingeschakeld	BitDefender beveiligt u tegen phishing-pogingen terwijl u op het internet surft.
Internet Explorer antiphishing bescherming is ingeschakeld	BitDefender beveiligt u tegen phishing-pogingen terwijl u op het internet surft.

Als de statusknoppen groen zijn, is het veiligheidsrisico van uw systeem minimaal. Volg deze stappen op de knoppen groen te maken:

1. Klik op de knop **Herstellen** om de zwakke punten in de beveiliging een voor een te herstellen.
2. Als een probleem niet er plaatse wordt opgelost, moet u de wizard volgen om het op te lossen.

Als u iets niet wilt controleren, verwijder dan het kruisje uit het vakje **Ja, deze component bewaken**.

8.2. Taken

Hier vindt u links naar de belangrijkste beveiligingstaken: volledige systeemscan, diepe scan, update nu.

De volgende knoppen zijn beschikbaar:

- **Volledige systeemscan** - start een complete scan van uw computer (exclusief archiefbestanden).
- **Diepe systeemscan** - start een complete scan van uw computer (inclusief archiefbestanden).
- **Mijn documenten scannen** - start een snelscan van uw documenten en instellingen.
- **Update nu** - start een directe update.

8.2.1. Scannen met BitDefender

Om uw computer te scannen op malware, voert u een speciale scantaak uit door te klikken op de overeenkomende knop. In de volgende tabel staan de beschikbare scantaken met hun beschrijving:

Taak	Beschrijving
Volledige systeemscan	Scant het volledige systeem, behalve archieven. In de standaardconfiguratie wordt er gescand op alle types malware die de beveiliging van uw systeem bedreigen, zoals virussen, spyware, adware, rootkits en andere.
Diepe scan	Scant het volledige systeem. In de standaardconfiguratie wordt er gescand op alle types malware die de beveiliging van uw systeem bedreigen, zoals virussen, spyware, adware, rootkits en andere.
Scan Mijn documenten	Gebruik deze taak om belangrijke gangbare gebruikersmappen te scannen: `Mijn documenten`, `Bureaublad` en `Opstarten`. Dit garandeert de veiligheid van uw documenten, een veilige werkruimte en schone applicaties bij het opstarten.

Opmerking
Omdat de taken **Diepe systeemscan** en **Volledige systeemscan** analyseren het volledige systeem. Het scannen kan enige tijd in beslag nemen. Wij raden u daarom aan deze taken uit te voeren met een lage prioriteit, of bij voorkeur wanneer uw systeem inactief is.

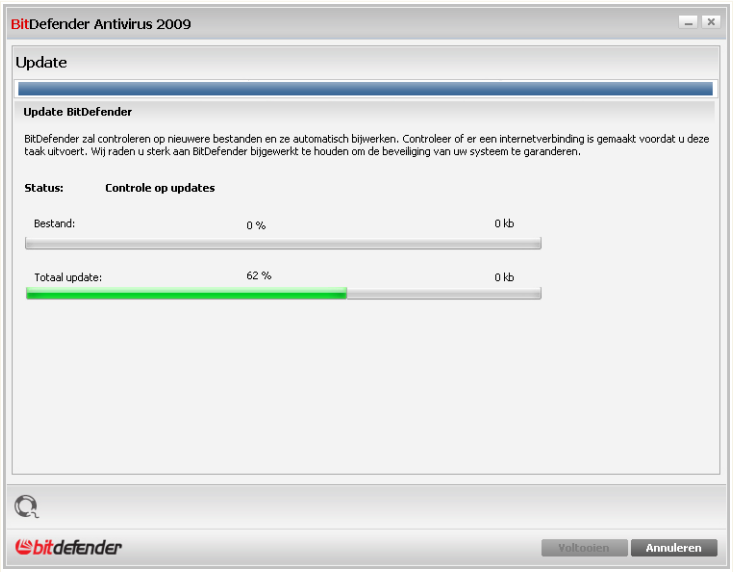
Wanneer u een proces Scannen op aanvraag start, verschijnt BitDefender Scanner, ongeacht of het om een snelle of volledige scan gaat.

Volg de begeleide procedure van drie stappen om het scanproces te voltooien.

8.2.2. Updaten BitDefender

Elke dag wordt nieuwe malware gevonden en geïdentificeerd. Het is dan ook heel belangrijk dat u BitDefender up-to-date houdt met de meest recente malware handtekeningen.

Standaard controleert BitDefender of er updates zijn als u uw computer aanzet en **ieder uur** daarna. Als u echter BitDefender wilt updaten, klik dan op **Update nu**. Het updateproces wordt gestart en het volgende venster verschijnt direct:



Updaten BitDefender

In dit venster kan u de status van het updateproces zien.

Het updateproces wordt geleidelijk uitgevoerd, wat betekent dat de te updaten bestanden een voor een worden vervangen. Op deze manier vormt het updateproces geen belemmering voor de werking van het product, en is tegelijk elke kwetsbaarheid uitgesloten.

Als u dit venster wilt sluiten, klik dan op **Annuleren**. Hierdoor stopt het updateproces echter niet.

Opmerking
Als u met het internet bent verbonden via een inbelverbinding, dan adviseren wij BitDefender regelmatig handmatig te updaten.

Start de computer indien nodig opnieuw op. Als het een belangrijke update betreft, wordt u gevraagd de computer opnieuw op te starten:

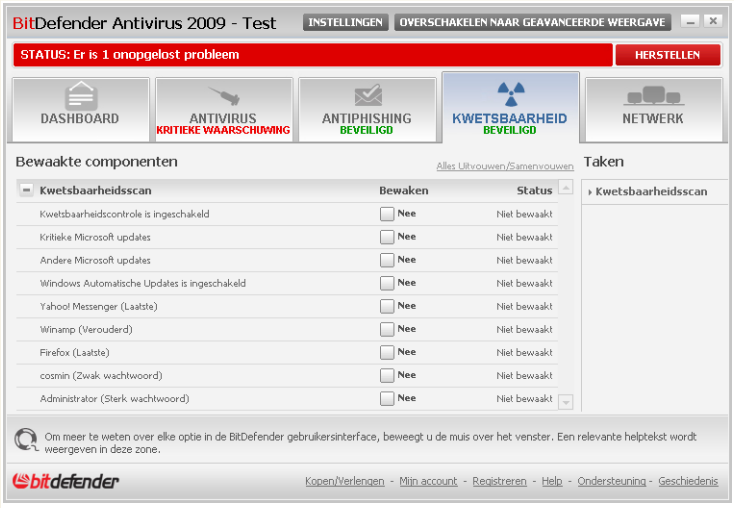
Klik op **Herstarten** om uw systeem direct opnieuw op te starten.

Als u uw systeem op een later tijdstip wilt herstarten, klik dan op **OK**. Wij adviseren dat u uw systeem zo snel mogelijk opnieuw opstart.

9. Kwetsbaarheid

BitDefender heeft een kwetsbaarheidsmodule die helpt de cruciale software op uw PC up-to-date te houden.

Klik op het tabblad **Kwetsbaarheid** om de kwetsbaarheidsmodule te openen.



Kwetsbaarheid

De Kwetsbaarheidsmodule betaat uit twee delen:

- **Bewaakte componenten** - Toont u de complete lijst van bewaakte componenten voor elke veiligheidsmodule. U kan kiezen welke van de modules moet worden bewaakt. Wij adviseren het bewaken van alle componenten in te schakelen.
- **Taken** - Hier vindt u links naar de belangrijke beveiligingstaken.

9.1. Bewaakte componenten

De volgende component wordt bewaakt:

Categorie	Beschrijving
Kwetsbaarheidsscan	Hier kan u controleren of cruciale software op uw PC up-to-date is. Wachtwoorden van Windows accounts worden gecontroleerd volgens de veiligheidsregels.

Klik op het vakje met het teken "+" om een categorie te openen of klik op het vakje met het teken "-" om een categorie te sluiten.

9.1.1. Kwetsbaarheidsscan

De problemen voor de kwetsbaarheid worden in duidelijke zinnen beschreven. In lijn met elke zin ziet u, als er iets de veiligheid van uw computer bedreigt, een rode statusknop **Herstellen**. Anders ziet u een goene statusknop **OK**.

Probleem	Beschrijving
Kwetsbaarheidsscan is ingeschakeld is ingeschakeld.	Bewaakt Microsoft Windows Updates, Microsoft Windows Office Updates en Microsoft Windows accounts wachtwoorden om te garanderen dat uw besturingssysteem up-to-date is en niet kwetsbaar is voor wachtwoord ontwijking.
Kritieke Microsoft updates	Beschikbare kritieke Microsoft updates installeren.
Andere Microsoft updates	Beschikbare niet-kritieke Microsoft updates installeren.
Windows Automatische Updates is ingeschakeld	Nieuwe Windows beveiligingsupdates installeren zodra deze beschikbaar zijn.
Admin (Sterk wachtwoord)	Geeft de sterkte van het wachtwoord voor specifieke gebruikers.

Als de statusknoppen groen zijn, is het veiligheidsrisico van uw systeem minimaal. Volg deze stappen op de knoppen groen te maken:

1. Klik op de knop **Herstellen** om de zwakke punten in de beveiliging een voor een te herstellen.
2. Als een probleem niet er plaatse wordt opgelost, moet u de wizard volgen om het op te lossen.

Als u iets niet wilt controleren, verwijder dan het kruisje uit het vakje **Ja, deze component bewaken**.

9.2. Taken

Hier vindt u links naar de belangrijkste beveiligingstaken.

De volgende knop is beschikbaar:

- **Kwetsbaarheidsscan**

9.2.1. Bezig met zoeken van kwetsbaarheden

Een kwetsbaarheidsscan controleert Microsoft Windows Updates, Microsoft Windows Office Updates en wachtwoorden van Microsoft Windows accounts om te garanderen dat uw besturingssysteem up to date is en dat het niet kwetsbaar is voor wachtwoord ontwijking.

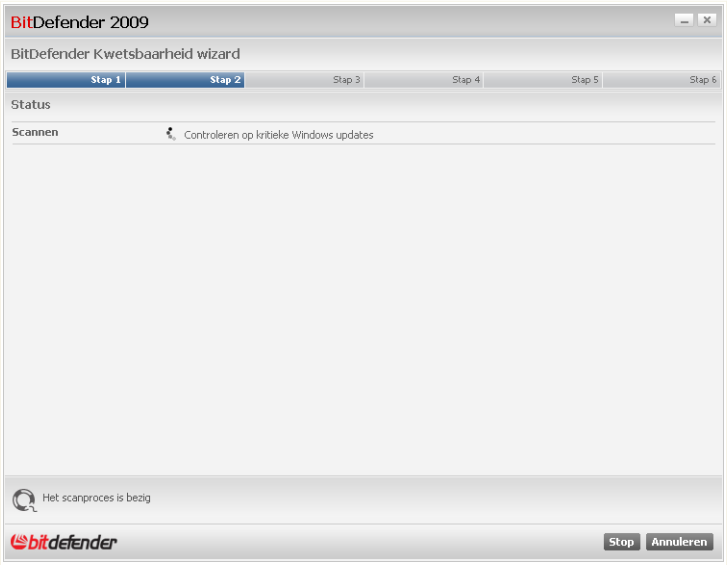
Om uw computer te controleren op kwetsbaarheden, klikt u op **Kwetsbaarheidsscan** en volgt u de wizard.

Stap 1/6 - Te controleren kwetsbaarheden selecteren

Kwetsbaarheden

Klik op **Volgende** om het systeem op de geselecteerde kwetsbaarheden te controleren.

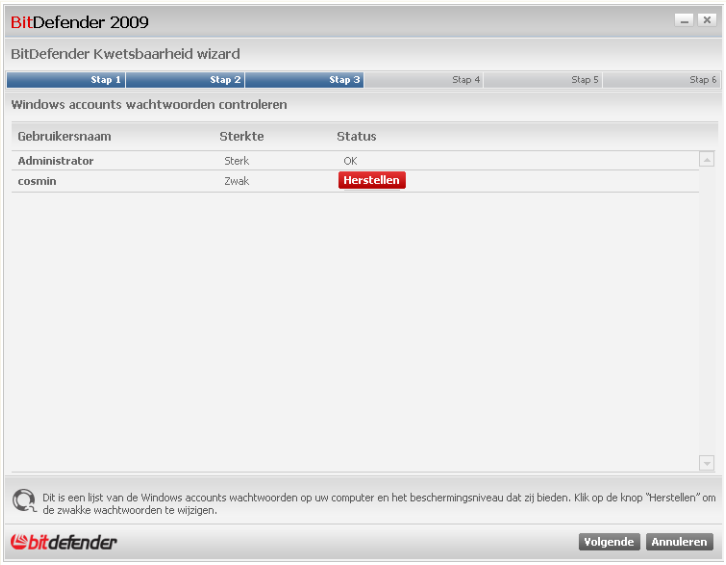
Stap 2/6 - Op kwetsbaarheden controleren



Kwetsbaarheidscontrole

Wacht tot BitDefender de kwetsbaarheidscontrole heeft voltooid.

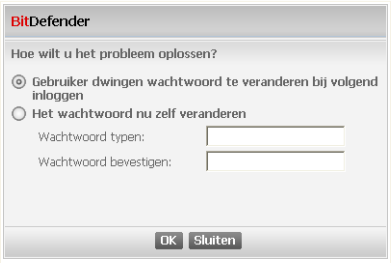
Stap 3/6 - Zwakke wachtwoorden veranderen



Gebruikers wachtwoord

U ziet de lijst van Windows gebruikersaccounts die zijn geconfigureerd op uw computer en de beschermingsniveaus van de wachtwoorden.

Klik op **Herstellen** om de zwakke wachtwoorden te wijzigen. Een nieuw venster wordt weergegeven.



Wachtwoord veranderen

Selecteer de methode voor het herstellen van dit probleem:

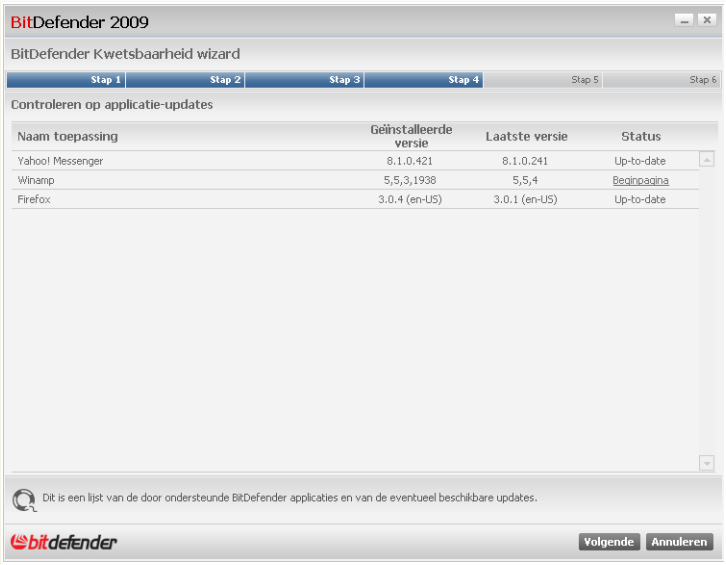
- **Gebruiker dwingen wachtwoord te veranderen bij volgend inloggen.** BitDefender vraagt de gebruiker het wachtwoord te veranderen als hij zich de volgende keer aanmeldt bij Windows.
- **Gebruikerswachtwoord veranderen.** U moet het nieuwe wachtwoord in de overeenkomende velden invoeren.

Opmerking
Voor een sterk wachtwoord gebruikt u een combinatie van hoofdletters en kleine letters, getallen en speciale tekens (zoals #, $ of @).

Klik op **OK** om het wachtwoord op te slaan.

Klik op **Volgende**.

Stap 4/6 - Applicaties updaten

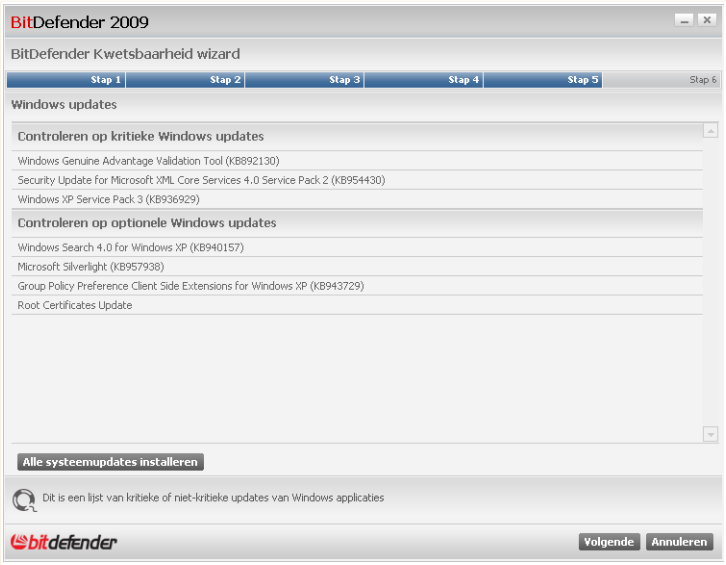


Applicaties

U kan de lijst zien van de applicaties die door BitDefender worden gecontroleerd en of zij up-to-date zijn. Als een applicatie niet up-to-date is, klik dan op de getoonde link om de laatste versie te downloaden.

Klik op **Volgende**.

Stap 5/6 – Windows updaten



Windows updates

U ziet de lijst van kritieke en niet-kritieke Windows updates die niet zijn geïnstalleerd op uw computer. Klik op **Alle systeemupdates installeren** om alle beschikbare producten te installeren.

Klik op **Volgende**.

Stap 6/6 - Resultaten weergeven

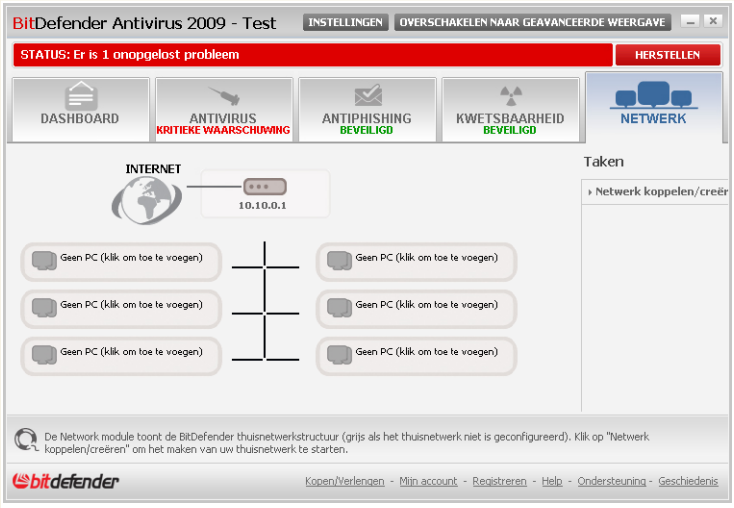
Resultaten

Klik op **Sluiten**.

10. Netwerk

Met de Netwerkmodule kan u de BitDefender producten die zijn geïnstalleerd op uw thuiscomputers beheren vanaf één enkele computer.

Klik op het tabblad **Bestandsbeheer** om de Netwerkmodule te openen.



Netwerk

Volg deze stappen om de BitDefender producten die zijn geïnstalleerd op uw computer te beheren:

1. Het BitDefender thuisnetwerk koppelen aan uw computer. Het koppelen van het netwerk bestaat uit het configureren van een administratief wachtwoord voor het thuisnetwerkbeheer.
2. Naar elke computer gaan die u wilt beheren en koppelen aan het netwerk (wachtwoord instellen)
3. Naar uw computer teruggaan en de computers toevoegen die u wilt beheren.

10.1. Taken

Aan het begin is er maar één knop beschikbaar.

- **Koppelen/Creëren** - hiermee kan u het netwerkwachtwoord instellen en dus naar het netwerk gaan.

Na het koppelen van het netwerk verschijnen meer knoppen.

- **Netwerk verlaten** - hiermee kan u het netwerk verlaten.
- **Netwerk beheren** - hiermee kan u de computer toevoegen aan uw netwerk.
- **Alles scannen** - hiermee kan u alle beheerde computers tegelijk scannen.
- **Alles updaten** - hiermee kan u alle beheerde computers tegelijk updaten.
- **Alles registreren** - hiermee kan u alle beheerde computers tegelijk registreren.

10.1.1. Het BitDefender netwerk koppelen

Volg deze stappen om het BitDefender thuisnetwerk te koppelen:

1. Klik op **Koppelen/Creëren**. U wordt gevraagd het thuisbeheer wachtwoord te configureren.

Wachtwoord configureren

2. Voer hetzelfde wachtwoord in elk van de bewerkingsvelden in.
3. Klik op **OK**.

U ziet de naam van de computer in de netwerkmap.

10.1.2. Bezig met toevoegen van computers aan het BitDefender netwerk

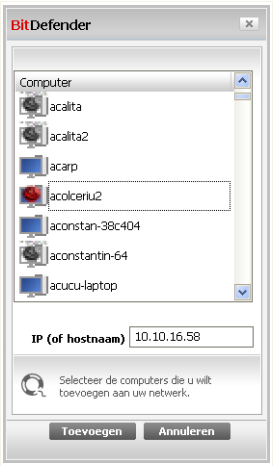
Voordat u een computer kan toevoegen aan het BitDefender thuisnetwerk, moet u het BitDefender thuisbeheer wachtwoord configureren op de betreffende computer.

Volg deze stappen als u een computer wilt toevoegen aan het BitDefender thuisnetwerk:

1. Klik op **Netwerk beheren**. U wordt gevraagd het lokale thuisbeheer wachtwoord in te voeren.

Wachtwoord invoeren

2. Voer het thuisbeheer wachtwoord in en klik op **OK**. Een nieuw venster wordt weergegeven.



Computer toevoegen

U ziet de lijst van computers in het netwerk. Het pictogram betekent:

- Een online computer zonder BitDefender producten.
- Een online computer met BitDefender producten.
- Een offline computer met BitDefender producten.

3. U kunt een van de volgende methoden gebruiken:
   - In de lijst de naam van de toe te voegen computer selecteren.
   - Het IP-adres of de naam van de comuter in het overeenkomende veld invoeren.
4. Klik op **Toevoegen**. U wordt gevraagd het thuismanagement wachtwoord van de betreffende computer in te voeren.

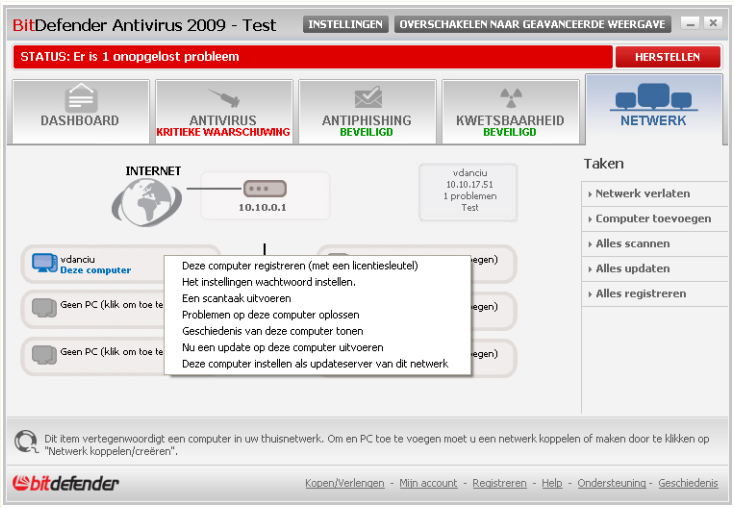
Identificeren

5. Het thuismanagement wachtwoord dat is geconfigureerd op de betreffende computer invoeren.
6. Klik op **OK**. Als het correcte wachtwoord is ingevoerd, verschijnt de naam van de geselecteerde computer in de netwerkmap.

Opmerking
U kan maximaal vijf comuters toevoegen aan de netwerkmap.

10.1.3. Het BitDefender netwerk beheren

Als met succes een BitDefender thuisnetwerk is gecreëerd, kan u alle BitDefender producten beheren vanaf één enkele computer.



Netwerk map

Als u de muiscursor boven een computer in de netwerkmap plaatst, ziet u korte informatie ervan (naam, IP-adres, aantal problemen die de systeemveiligheid bedreigen, BitDefender registratiestatus).

Als u rechtsklikt op een computernaam in de netwerkmap, kan u alle administratieve taken zien die u op verre computer kan uitvoeren.

- **Deze computer registreren**
- **Wachtwoordinstellingen instellen**
- **Een scantaak uitvoeren**
- **Problemen op deze computer herstellen**
- **Geschiedenis van deze computer weergeven**
- **Nu een update op deze computer uitvoeren**
- **Profiel toepassen**
- **Een Tune-up taak op deze computer uitvoeren**
- **Deze computer instellen als updateserver van dit netwerk**

Voordat u een taak op een specifieke computer kan uitvoeren, moet u het lokale thuisbeheer wachtwoord invoeren.

Wachtwoord invoeren

Voer het thuisbeheer wachtwoord in en klik op **OK**.

Opmerking

Als u verschillende taken wilt uitvoeren, kan u het selectievakje **Dit bericht niet weergeven tijdens deze sessie** inschakelen. Als u deze optie selecteert, wordt u tijdens de huidige sessie niet opnieuw naar het wachtwoord gevraagd.

10.1.4. Alle computers scannen

Volg deze stappen om alle beheerde computers te scannen:

1. Klik op **Alles scannen**. U wordt gevraagd het lokale thuisbeheer wachtwoord in te voeren.

Wachtwoord invoeren

2. Selecteer een scantype.
   - **Volledige systeemscan** - start een complete scan van uw computer (exclusief archiefbestanden).
   - **Diepe systeemscan** - start een complete scan van uw computer (inclusief archiefbestanden).
   - **Mijn documenten scannen** - start een snelscan van uw documenten en instellingen.

Scantype selecteren

3. Klik op **OK**.

10.1.5. Alle computers updaten

Volg deze stappen om alle beheerde comupter te updaten:

1. Klik op **Alles updaten**. U wordt gevraagd het lokale thuisbeheer wachtwoord in te voeren.

Wachtwoord invoeren

2. Klik op **OK**.

10.1.6. Alle computers registreren

Volg deze stappen om alle beheerde computers te registreren:

1. Klik op **Alles registreren**. U wordt gevraagd het lokale thuisbeheer wachtwoord in te voeren.

Wachtwoord invoeren

2. Voer de sleutel in waarmee u wilt registreren.

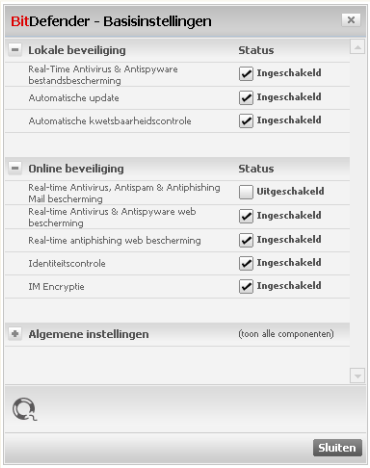
Alles registreren

3. Klik op **OK**.

11. Basisinstellingen

In de Basisinstellingen module kan u gemakkelijk belangrijke veiligheidsmodules aan- en uitzetten.

Om de Basisinstellingen module te openen, klikt u op de knop **Instellingen** aan de bovenkant van de Basisweergave.



Basisinstellingen

De beschikbare veiligheidsmodules zijn gegroepeerd in verschillende categorieën.

Categorie	Beschrijving
Lokale beveiliging	Hier kan kan u real time bestandsbescherming of de automatische update inschakelen/uitschakelen.
Online beveiliging	Hier kan kan u real time mail- en webbescherming inschakelen/uitschakelen.
Algemene instellingen	Hier kan kan u spelmodus, laptop-modus, wachtwoorden, scanactiviteitbalk en andwere inschakelen/uitschakelen.

Klik op het vakje met het teken "+" om een categorie te openen of klik op het vakje met het teken "-" om een categorie te sluiten.

11.1. Lokale beveiliging

U kan veiligheidsmodules met een klik inschakelen/uitschakelen.

Veiligheidmodule	Beschrijving
Real time antivirus & antispyware bestandsbescherming	Real-time bestandsbescherming garandeert dat alle bestanden worden gescand als zij worden benaderd door u of door een toepassing op dit systeem.
Automatische update	Automatische update garandeert dat de nieuwste BitDefender product- en signatuurbestanden regelmatig automatisch worden gedownload en geïnstalleerd.
Automatische kwetsbaarheidscontrole	Automatische kwetsbaarheidscontrole garandeert dat de cruciale software op uw PC up-to-date is.

11.2. Online beveiliging

U kan veiligheidsmodules met een klik inschakelen/uitschakelen.

Veiligheidmodule	Beschrijving
Real time antiphishing web bescherming	Real time web antiphishing bescherming garandeert dat alle via HTTP gedownloade bestanden zijn gescand op phishing pogingen.
Identiteitscontrole	Identiteitscontrole helpt uw vertrouwelijke data veilig te houden door het scannen van alle web en mail verkeer op specifieke woorden.
IM encryptie	Als uw IM contacten BitDefender 2009 hebben geïnstalleerd, worden alle IM gesprekken via Yahoo! Messenger en Windows Live Messenger gecrypteerd.

11.3. Algemene instellingen

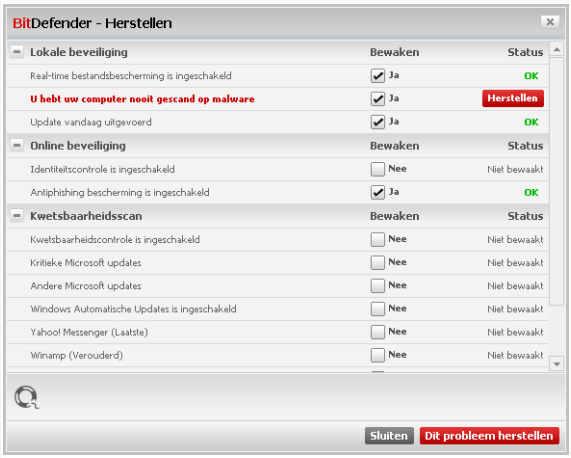
U kan veiligheidsgerelateerde items met een klik inschakelen/uitschakelen.

Item	Beschrijving
Spelmodus	Spelmodus wijzigt tijdelijk de beveiligingsinstellingen om de snelheid van uw systeem zo weinig mogelijk te beïnvloeden.
Laptop-modus	Laptop-modus wijzigt tijdelijk de beveiligingsinstellingen om de accu van uw laptop zo weinig mogelijk te belasten.
Instellingen wachtwoord	Dit garandeert dat de BitDefender instellingen alleen kunnen worden veranderd door degene die dit wachtwoord kent.
BitDefender News	Als u deze optie inschakelt, ontvangt u belangrijk nieuws over bedrijf, product updates of nieuwe bedreigingen van de veiligheid.
Productmededelingen	Als u deze optie inschakelt, ontvangt u waarschuwingsinformatie.
Scanactiviteitenbalk	De scanactiviteitenbalk is een klein, transparant balkje dat de voortgang van de BitDefender scanactiviteit laat zien. De groene bewegende lijn geeft de scanactiviteit op uw lokale systeem weer. De rode bewegende lijn geeft de scanactiviteit op uw internet verbinding weer.
BitDefender laden bij het opstarten	Als u deze optie inschakelt, wordt de BitDefender gebruikersinterface geladen bij het opstarten. Deze optie heeft geen invloed op het beveiligingsniveau.
Virusrapporten verzenden	Als u deze optie inschakelt, worden virusscanrapporten verzonden naar BitDefender labs voor analyse. Merk op dat deze rapporten geen vertrouwelijke data bevatten, zoals uw naam of IP-adres, en evenmin worden gebruikt voor commerciële doeleinden.
Uitbraakdetectie	Als u deze optie inschakelt, worden rapporten over potentiële virusuitbraken verzonden naar BitDefender labs voor analyse. Merk op dat deze rapporten geen vertrouwelijke data bevatten, zoals uw naam of IP-adres, en evenmin worden gebruikt voor commerciële doeleinden.

12. Statusbalk

Aan de bovenkant van het BitDefender Antivirus 2009 venster ziet u een statusbalk met het aantal onopgeloste problemen. Klik op de knop **Herstellen** op bedreigingen van de veiligheid van uw computer te verwijderen. Een veiligheidsstatusvenster verschijnt.

De beveiligingsstatus toont een systematisch georganiseerde en gemakkelijk beheerbare lijst van zwakke punten in de beveiliging van uw computer. BitDefender Antivirus 2009 zal u op de hoogte brengen wanneer een probleem de beveiliging van uw computer kan beïnvloeden.



Statusbalk

12.1. Lokale beveiliging

Wij weten dat het belangrijk is om gewaarschuwd te worden als een probleem de veiligheid van uw computer bedreigt. Door het bewaken van elke beveiligingsmodule laat BitDefende 2009 u niet alleen weten wanneer u de instellingen configureert die de veiligheid van uw computer kunnen beïnvloeden, maar ook wanneer u belangrijke taken vergeet uit te voeren.

De problemen voor de lokale veiligheid worden in duidelijke zinnen beschreven. In lijn met elke zin ziet u, als er iets de veiligheid van uw computer bedreigt, een rode statusknop **Herstellen**. Anders ziet u een goene statusknop **OK**.

Probleem	*Beschrijving*
Real-time bestandsbescherming is ingeschakeld	Garandeert dat alle bestanden worden gescand, ongeacht of ze door u of door een toepassing op uw systeem zijn geopend.
U hebt uw computer vandaag gescand op malware	Wij adviseren met kracht om zo spoedig mogelijk een op aanvraag scan uit te voeren, om te controleren of de op uw computer opgeslagen bestanden geen malware bevatten.
Automatische update is ingeschakeld	Houd automatische update ingeschakeld om te garanderen dat de malware signaturen van uw BitDefender product regelmatig geüpdatet worden.
Update nu bezig	Update van product en malware signaturen wordt uitgevoerd.

Als de statusknoppen groen zijn, is het veiligheidsrisico van uw systeem minimaal. Volg deze stappen op de knoppen groen te maken:

1. Klik op de knop **Herstellen** om de zwakke punten in de beveiliging een voor een te herstellen.
2. Als een probleem niet er plaatse wordt opgelost, moet u de wizard volgen om het op te lossen.

Als u iets niet wilt controleren, verwijder dan het kruisje uit het vakje **Ja, deze component bewaken**.

12.2. Online beveiliging

De problemen voor de online beveiliging worden in duidelijke zinnen beschreven. In lijn met elke zin ziet u, als er iets de veiligheid van uw computer bedreigt, een rode statusknop **Herstellen**. Anders ziet u een goene statusknop **OK**.

Probleem	Beschrijving
Gespreksencryptie voor IM is ingeschakeld	Als uw IM contacten BitDefender 2009 hebben geïnstalleerd, worden alle IM gesprekken via Yahoo! Messenger en Windows Live Messenger gecrypteerd. Wij adviseren om gespreksencryptie voor IM ingeschakeld te hebben om te garanderen dat uw IM gesprekken privé blijven.
Firefox antiphishing bescherming is ingeschakeld	BitDefender beveiligt u tegen phishing-pogingen terwijl u op het internet surft.
Internet Explorer antiphishing bescherming is ingeschakeld	BitDefender beveiligt u tegen phishing-pogingen terwijl u op het internet surft.

Als de statusknoppen groen zijn, is het veiligheidsrisico van uw systeem minimaal. Volg deze stappen op de knoppen groen te maken:

1. Klik op de knop **Herstellen** om de zwakke punten in de beveiliging een voor een te herstellen.
2. Als een probleem niet er plaatse wordt opgelost, moet u de wizard volgen om het op te lossen.

Als u iets niet wilt controleren, verwijder dan het kruisje uit het vakje **Ja, deze component bewaken**.

12.3. Kwetsbaarheidsscan

De problemen voor de kwetsbaarheid worden in duidelijke zinnen beschreven. In lijn met elke zin ziet u, als er iets de veiligheid van uw computer bedreigt, een rode statusknop **Herstellen**. Anders ziet u een goene statusknop **OK**.

Probleem	Beschrijving
Kwetsbaarheidsscan is ingeschakeld is ingeschakeld.	Bewaakt Microsoft Windows Updates, Microsoft Windows Office Updates en Microsoft Windows accounts wachtwoorden om te garanderen dat uw besturingssysteem up-to-date is en niet kwetsbaar is voor wachtwoord ontwijking.

Probleem	Beschrijving
Kritieke Microsoft updates	Beschikbare kritieke Microsoft updates installeren.
Andere Microsoft updates	Beschikbare niet-kritieke Microsoft updates installeren.
Windows Automatische Updates is ingeschakeld	Nieuwe Windows beveiligingsupdates installeren zodra deze beschikbaar zijn.
Admin (Sterk wachtwoord)	Geeft de sterkte van het wachtwoord voor specifieke gebruikers.

Als de statusknoppen groen zijn, is het veiligheidsrisico van uw systeem minimaal. Volg deze stappen op de knoppen groen te maken:

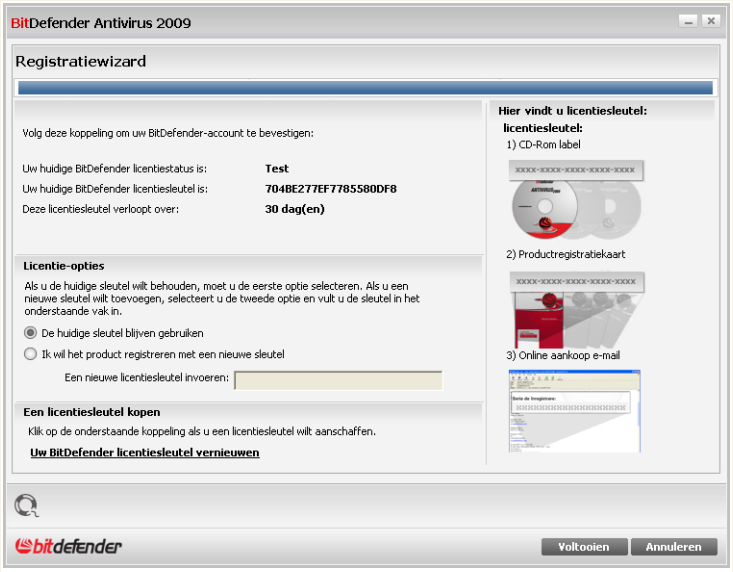
1. Klik op de knop **Herstellen** om de zwakke punten in de beveiliging een voor een te herstellen.
2. Als een probleem niet er plaatse wordt opgelost, moet u de wizard volgen om het op te lossen.

Als u iets niet wilt controleren, verwijder dan het kruisje uit het vakje **Ja, deze component bewaken**.

13. Registratie

BitDefender Antivirus 2009 begint met een 30-dagen proefperiode. Voor het registreren van BitDefender Antivirus 2009, het veranderen van de licentiesleutel of het maken van een BitDefender-account, klikt u op de link **Registreren**, aan de onderkant van het BitDefender venster. De registratiewizard verschijnt.

13.1. Stap 1/1 - BitDefender Antivirus 2009 registreren



Registratie

U kan de BitDefender registratiestatus zien, evenals de huidige licentiesleutel en over hoeveel dagen de licentiesleutel verloopt.

Om BitDefender Antivirus 2009 te registreren:

1. Selecteer **Ik wil het product registreren met een nieuwe sleutel**.

2. Typ de licentiesleutel in het bewerkingsveld.

Opmerking

U kan uw licentiesleutel vinden:

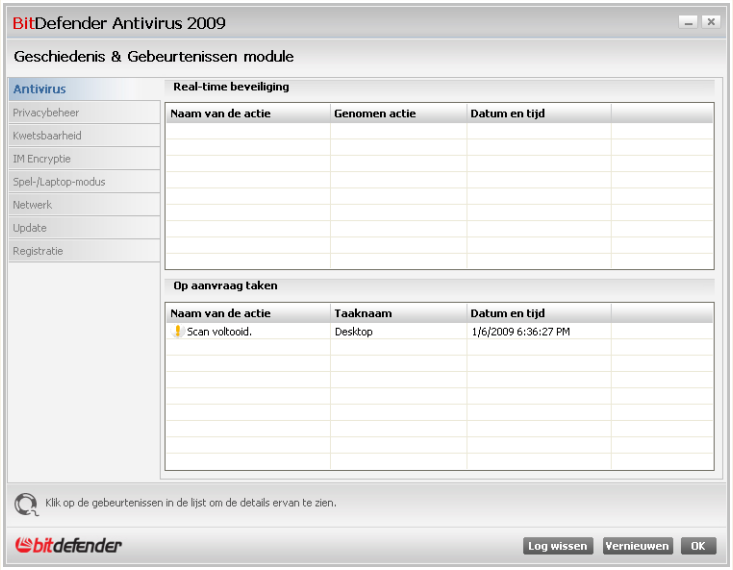
- op het cd label.
- op de productregistratiekaart.
- in de online aankoop e-mail.

Als u geen BitDefender licentiesleutel hebt, klik dan op de aanwezige link om naar de BitDefender online winkel te gaan en een licentiesleutel te kopen.

Klik op **Voltooien**.

14. Geschiedenis

De link **Geschiedenis** onderaan in het venster van het Beveiligingscentrum van BitDefender opent een ander venster met de Geschiedenis en gebeurtenissen. Dit venster geeft u een overzicht van gebeurtenissen die betrekking hebben op de beveiliging. U kan bijvoorbeeld gemakkelijk controleren of de update is gelukt, of er malware op uw computer is gevonden, enz.



Gebeurtenissen

Om u te helpen de geschiedenis en gebeurtenissen van BitDefender te filteren, worden de volgende categorieën aan de linkerzijde weergegeven:

- **Antivirus**
- **Privacybeheer**
- **Update**
- **Netwerk**

Voor elke categorie is een lijst gebeurtenissen beschikbaar. Elke gebeurtenis biedt de volgende informatie: een korte beschrijving, de actie die BitDefender heeft genomen wanneer de gebeurtenis is opgetreden en de datum en het tijdstip van de gebeurtenis. Als u meer informatie over een specifieke gebeurtenis in de lijst wilt krijgen, dubbelklikt u op die gebeurtenis.

Klik op **Logboek wissen** als u de oude logboeken wilt verwijderen of klik op **Vernieuwen** om zeker te zijn dat de recentste logboeken worden weergegeven.

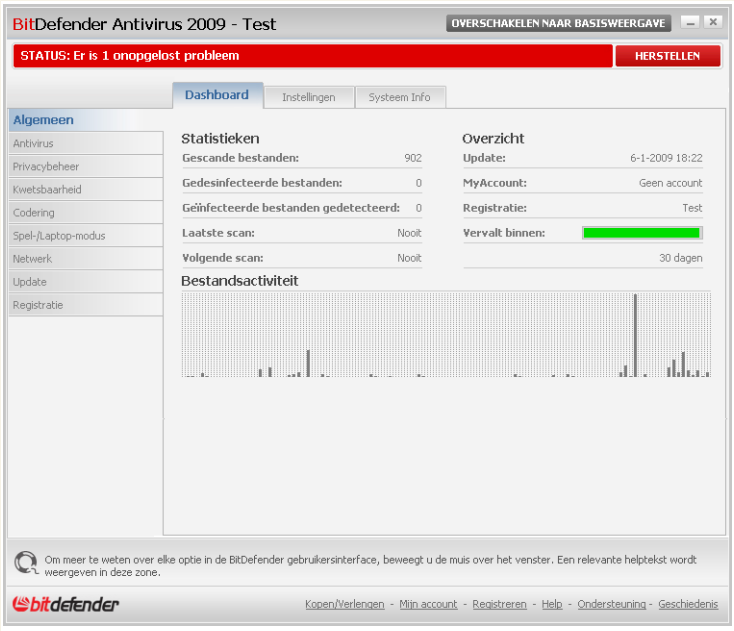
Geavanceerd beheer

15. Algemeen

De Algemeen module geeft informatie over de BitDefender activiteit en het systeam. Hier kan u ook de grote lijnen van het gedrag van BitDefender veranderen.

15.1. Dashboard

Om de productactiviteitstatistieken en uw registratiestatus te zien, gaat u naar **Algemeen>Dashboard** in de Geavanceerde weergave.



Dashboard

Het dashboard bestaat uit verschillende delen:

- **Statistieken** - Toont belangrijke informatie over de BitDefender activiteit.

- **Overzicht** - Toont de updatestatus, uw accountstatus, registratie en licentie-informatie.
- **Bestandszone** - Geeft de ontwikkeling van het aantal door BitDefender Antimalware gescande objecten. De hoogte van de balk geeft de intensiteit van het verkeer gedurende dat tijdsinterval.

15.1.1. Statistieken

Als u zicht wil hebben op de BitDefender activiteit, begin dan met de Statistieken. U kan de volgende items zien:

Item	Beschrijving
Gescande bestanden	Geeft het aantal op malware gecontroleerde bestanden tijdens de laatste scan.
Gedesinfecteerde bestanden	Geeft het aantal gedesinfecteerde bestanden tijdens de laatste scan.
Gedetecteerde virussen	Geeft het aantal op uw systeem gevonden virussen tijdens de laatste scan.

15.1.2. Overzicht

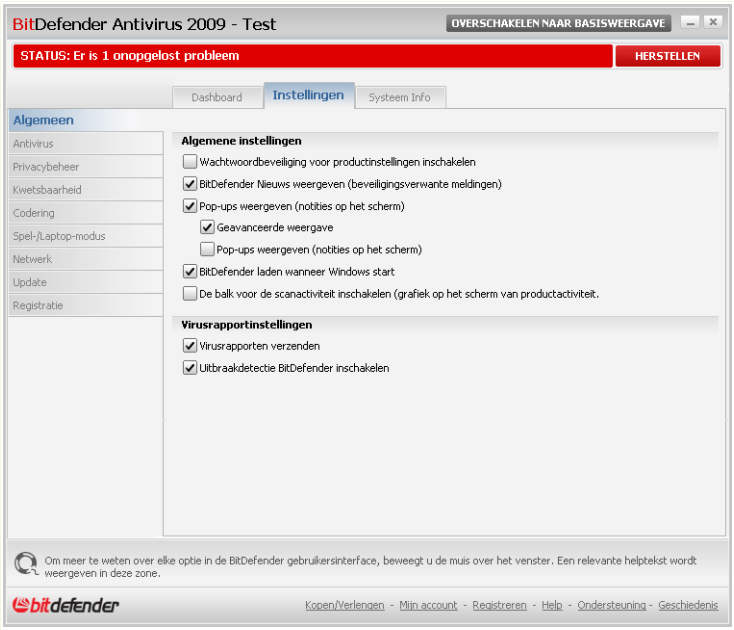
Hier ziet u een overzicht van statistieken over de updatestatus, uw accountstatus, registratie en licentie-informatie.

Item	Beschrijving
Laatste update	Geeft de datum waarop uw BitDefender product voor het laatst is geüpdatet. Voer regelmatig updates uit om uw systeem volledig te beschermen.
Mijn account	Geeft het e-mailadres dat u kan gebruiken om uw online account te openen en uw verloren BitDefender licentiesleutel op te halen, of te profiteren van BitDefender ondersteuning en andere aangepaste diensten.
Registratie	Geeft het type en de status van uw licentiesleutel. Om uw systeem veilig te houden moet u BitDefender vernieuwen of upgraden als uw sleutel is verlopen.

Item	Beschrijving
Verloopt over	Geeft het aantal dagen tot het verlopen van uw licentiesleutel.

15.2. Instellingen

Om de algemene instellingen te configureren voor BitDefender en zijn instellingen te beheren, klikt u op **General>Settings** in de Geavanceerde weergave.



Algemene instellingen

Hier kunt u de algemene gedragingen van BitDefender instellen. BitDefender wordt standaard geladen bij het opstarten van Windows en wordt vervolgens geminimaliseerd uitgevoerd in de taakbalk.

15.2.1. Algemene instellingen

- **Wachtwoord voor productinstellingen aan** - maakt het gebruik van een wachtwoord mogelijk om de BitDefender configuratie te beschermen.

  Opmerking
  Als u niet de enige persoon met beheermachtigingen bent die deze computer gebruikt, raden wij u aan uw BitDefender-instellingen te beveiligen met een wachtwoord.

  Als u deze optie selecteert, verschijnt het volgende venster:

Voer wachtwoord in

Typ het wachtwoord in het **Wachtwoord** veld, typ het nogmaals in het **Wachtwoord herhalen** veld en klik op **OK**.

Zodra u het wachtwoord hebt ingesteld, zal er elke keer om gevraagd worden als u de instellingen van BitDefender wilt veranderen. De andere systeembeheerders (als die er zijn) moeten dit wachtwoord ook invullen om de instellingen van BitDefender te kunnen veranderen.

Belangrijk
Als u uw wachtwoord vergeten bent, zult u het product moeten repareren om de BitDefender-configuratie te wijzigen.

- **BitDefender-nieuws weergeven (berichten i.v.m. beveiliging)** - toont af en toe beveiligingsberichten die door de BitDefender-server zijn verzonden met betrekking tot de uitbraak van virussen.
- **Pop-ups weergeven (notities op het scherm)** - toont pop-upvensters die betrekking hebben op de productstatus. U kunt BitDefender configureren om alleen pop-ups weer te geven wanneer u de Basisweergave of Geavanceerde gebruikt.
- **BitDefender laden wanneer Windows start** - start BitDefender automatisch wanneer het systeem wordt opgestart. Wij raden u aan deze optie ingeschakeld te houden.
- **De balk voor de scanactiviteit inschakelen (grafiek op het scherm van productactiviteit)** - toont de Scanactiviteit balk als u inlogt op Windows. Maak dit vakje leeg als u de Scanactiviteit balk niet langer wilt zien.

Opmerking
Deze optie kan alleen worden geconfigureerd voor de huidige Windows gebruiker.

15.2.2. Virusrapportinstellingen

- **Virusrapporten verzenden** - verzendt rapporten met betrekking tot virussen die op uw computer werden geïdentificeerd naar de BitDefender Labs. Hierbij helpt u ons virusuitbraken op te volgen.

  De rapporten zullen geen vertrouwelijke gegevens, zoals uw naam, IP-adres of andere bevatten, en zullen niet worden gebruikt voor commerciële doeleinden. De geleverde informatie zal alleen de naam van het virus bevatten en zal uitsluitend worden gebruikt voor het maken van statistische rapporten.

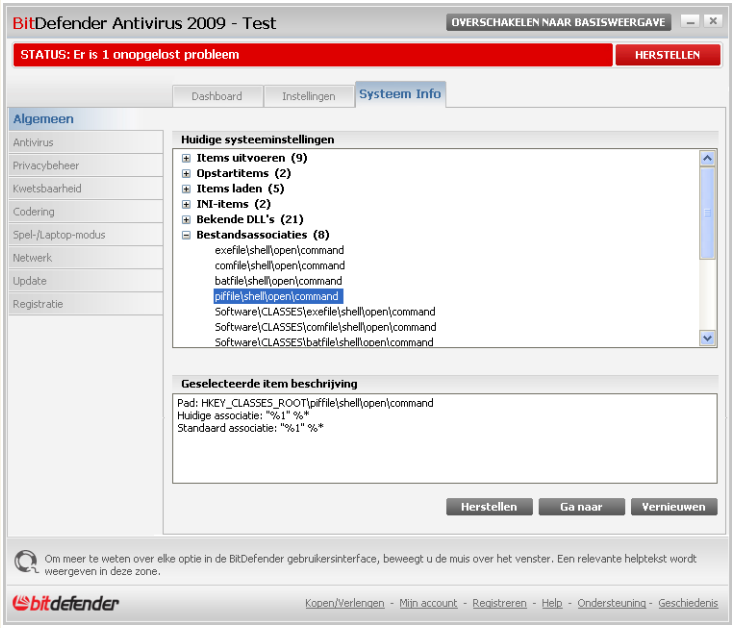
- **Uitbraakdetectie BitDefender inschakelen** - verzendt rapporten met betrekking tot potentiële virusuitbraken naar de BitDefender Labs.

  De rapporten zullen geen vertrouwelijke gegevens, zoals uw naam, IP-adres of andere bevatten, en zullen niet worden gebruikt voor commerciële doeleinden. De geleverde informatie zal alleen de naam van het potentiële virus bevatten en zal uitsluitend worden gebruikt om nieuwe virussen te detecteren.

15.3. Systeem- informatie

Met BitDefender kunt u vanaf één locatie alle systeeminstellingen bekijken, samen met de toepassingen die zijn geregistreerd om te worden uitgevoerd bij het opstarten. Hierdoor kunt u de activiteit controleren van het systeem en de toepassingen die op het systeem zijn geïnstalleerd en kunt u mogelijke systeeminfecties identificeren.

Om systeeminformatie te verkrijgen, gaat u naar **Algemeen>Systeeminformatie** in de Geavanceerde weergave.



Systeem- informatie

De lijst bevat alle items die zijn geladen bij het opstarten van het systeem, maar ook de items die door de verschillende toepassingen zijn geladen.

Er zijn drie knoppen beschikbaar:

- **Herstellen** - zet de huidige bestandsassociatie terug naar de standaardinstelling. Alleen beschikbaar voor de **Bestandsassociaties**!
- **Ga naar** - opent een venster waar het geselecteerde item is geplaatst (bijvoorbeeld **Register**).

> ***Opmerking***
> Afhankelijk van het geselecteerde item, kan de knop **Ga naar** misschien niet verschijnen.

- **Vernieuwen** - opent het gedeelte **Systeeminfo** opnieuw.

16. Antivirus

BitDefender beveiligt uw computer tegen alle types malware (virussen, Trojanen, spyware, rootkits, enz.). De BitDefender-bescherming is ingedeeld in twee categorieën:

- Real-time bescherming - voorkomt dat nieuwe malware bedreigingen uw systeem binnendringen. BitDefender zal bijvoorbeeld een Worddocument scannen op bekende gevaren wanneer u het opent, en een e-mailbericht wanneer u het ontvangt.

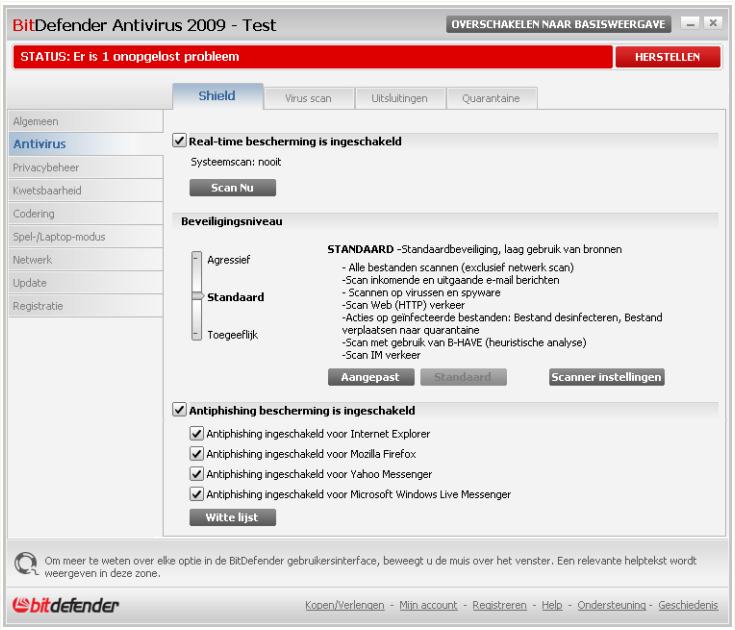
  Opmerking
  Real-time bescherming wordt ook wel on-access scannen geneomd - bestanden worden gescand als de gebruikers deze openen.

- Scannen op aanvraag - hiermee kan u malware die al op uw systeem aanwezig is, detecteren en verwijderen. Dit is de klassieke scan die door de gebruiker wordt geactiveerd. U selecteert het station, de map of het bestand dat BitDefender moet scannen, en BitDefender doet dat - op aanvraag. Met de scantaken kunt u aangepaste scanroutines maken en ze kunnen op regelmatige basis worden uitgevoerd.

16.1. Real-time beveiliging

BitDefender geeft continu, real-time bescherming tegen een groot aantal types malware-bedreigingen door alle geopende bestanden, e-mailbestanden en communicatie via toepassingen voor instant messaging (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger) te scannen. BitDefender Antiphishing dat persoonlijke informatie over u wordt onthuld, als u over het Internet surft, door u te waarschuwen voor potentiële phishing webpagina's.

Om de real-time bescherming en BitDefender Antiphishing te configureren, gaat u naar **Antivirus>Schild** in de Geavanceerde weergave.



Real-time beveiliging

De real-time bescherming is uitgeschakeld. Als u de status van de real-time bescherming wilt veranderen, schakelt u het overeenkomende selectievakje in of uit.

Belangrijk
Om te verhinderen dat uw computer door virussen wordt geïnfecteerd, moet u de **Real-time-beveiliging** ingeschakeld houden.

Om een snelle systeemscan te starten, klikt u op **Nu scannen**.

16.1.1. Het beveiligingsniveau configureren

U kunt het beveiligingsniveau kiezen dat beter voldoet aan uw beveiligingsbehoeften. Sleep de schuifregelaar langs de schaal om het geschikte beveiligingsniveau in te stellen.

Er zijn 3 beveiligingsniveaus:

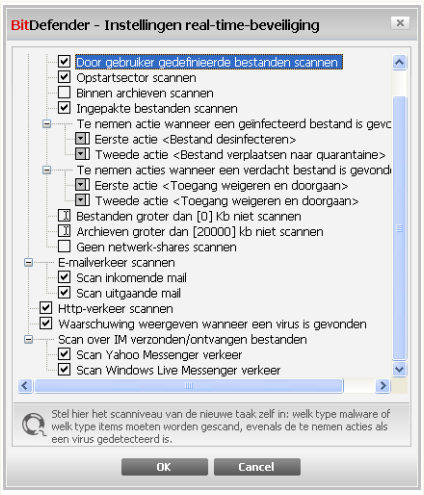
Beveiligingsniveau	Beschrijving
Toegeeflijk	Dekt de basisbehoeften aan beveiliging. Het verbruiksniveau van de bron is zeer laag. Programma's en binnenkomende e-mailberichten worden alleen op virussen gescand. Naast de klassieke op handtekeningen gebaseerde scan, wordt ook de heuristische analyse gebruikt. De volgende acties worden ondernomen op geïnfecteerde bestanden: bestand opruimen/toegang weigeren.
Standaard	Biedt standaardbeveiliging. Het verbruiksniveau van de bron is laag. Alle bestanden en binnenkomende/uitgaande e-mailberichten worden gescand op virussen en spyware. Naast de klassieke op handtekeningen gebaseerde scan, wordt ook de heuristische analyse gebruikt. De volgende acties worden ondernomen op geïnfecteerde bestanden: bestand opruimen/toegang weigeren.
Agressief	Biedt een hoge beveiliging. Het verbruiksniveau van de bron is gemiddeld. Alle bestanden, binnenkomende/uitgaande e-mailberichten en webverkeer worden gescand op virussen en spyware. Naast de klassieke op handtekeningen gebaseerde scan, wordt ook de heuristische analyse gebruikt. De volgende acties worden ondernomen op geïnfecteerde bestanden: bestand opruimen/toegang weigeren.

Om de standaard real time beveiligingsinstellingen toe te passen, klikt u op **Standaard**.

16.1.2. Het beveiligingsniveau aanpassen

Gevorderde gebruikers willen wellicht voordeel halen uit de scaninstellingen die door BitDefender worden aangeboden. De scanner kan worden ingesteld om alleen specifieke bestandsextensies te scannen, specifieke malware-bedreigingen te zoeken of archieven over te slaan. Dat kan de duur van het scannen aanzienlijk verkorten en de reactie van uw computer tijdens het scannen verbeteren.

U kunt de **Real-time-beveiliging** inschakelen door op **Aangepast** te klikken. Het volgende venster wordt geopend:



Shield-instellingen

De scanopties zijn georganiseerd als een uitbereidbaar menu, vergelijkbaar met de menu's die in Windows gebruikt worden. Klik op het vakje met een "+" om een optie te openen of op het vakje met een "-" om een optie te sluiten.

Opmerking
U zult merken dat sommige scanopties toch niet kunnen worden geopend, zelfs indien het teken "+" wordt weergegeven. De reden hiervoor is dat deze optie nog niet werd geselecteerd. Wanneer u deze selecteert, zult u merken dat ze nu wel kunnen worden geopend.

- **Geopende bestanden en P2P-overdrachten scannen** - scant de geopende bestanden en de communicatie via Instant Messaging-software (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Selecteer vervolgens het type bestanden dat u wilt scannen.

Optie		Beschrijving
Geopende bestanden scannen	**Alle bestanden scannen**	Alle geopende bestanden worden gescand, ongeacht hun type.

Optie		Beschrijving
	Alleen programmabestanden scannen	Alleen de programmabestanden worden gescand. Dit betekent alleen bestanden met de volgende extensies: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml en .nws.
	Door gebruiker gedefinieerde extensies scannen	Alleen de bestanden met de extensies die door de gebruiker zijn gedefinieerd, worden gescand. Deze extensies moeten worden gescheiden door ";".
	Scannen op riskware	Scannen op riskware. Gedetecteerde bestanden zullen worden behandeld als geïnfecteerd. Software die adware-componenten bevat, zal mogelijk niet meer werken als deze optie is ingeschakeld. Selecteer **Dialers en toepassingen overslaan bij scan** als u dit type bestanden wilt uitsluiten van het scannen.
Opstartsector scannen		Scant de opstartsector van het systeem.
Binnen archieven scannen		De geopende archieven worden gescand. Wanneer u deze optie inschakelt, zal de computer langzamer werken.
Ingepakte bestanden scannen		Alle ingepakte bestanden worden gescand.
Eerste actie		Selecteer de eerste actie die moet worden genomen op geïnfecteerde en verdachte bestanden in het vervolgkeuzemenu.
	Toegang weigeren en doorgaan	Wanneer een geïnfecteerd bestand is gedetecteerd, zal de toegang tot dit bestand worden geweigerd.

Optie		Beschrijving
	Bestand opruimen	Desinfecteert geïnfecteerde bestanden.
	Bestand verwijderen	Verwijdert onmiddellijk de geïnfecteerde bestanden, zonder enige waarschuwing.
	Bestand verplaatsen naar quarantaine	Verplaatst de geïnfecteerde bestanden naar de quarantaine.
Tweede actie		Selecteer in het vervolgkeuzemenu de tweede actie die moet worden genomen op geïnfecteerde bestanden in het geval de eerste actie mislukt.
	Toegang weigeren en doorgaan	Wanneer een geïnfecteerd bestand is gedetecteerd, zal de toegang tot dit bestand worden geweigerd.
	Bestand verwijderen	Verwijdert onmiddellijk de geïnfecteerde bestanden, zonder enige waarschuwing.
	Bestand verplaatsen naar quarantaine	Verplaatst de geïnfecteerde bestanden naar de quarantaine.
Bestanden groter dan [x] Kb niet scannen		Voer de maximale grootte in van de bestanden die moeten worden gescand. Als u de grootte instelt op 0 Kb, worden alle bestanden gescand, ongeacht hun grootte.
Archieven groter dan [20000] Kb niet scannen		Typ de maximumgrootte in kilobytes (KB) van de te scannen archieven. Typ 0 als u alle archieven, ongeacht hun grootte, wilt scannen.
Geen netwerk-shares scannen		Als deze optie is ingeschakeld, zal BitDefender de netwerk-shares niet scannen, zodat u sneller toegang krijgt tot het netwerk. Wij raden u aan deze optie alleen in te schakelen als het netwerk waarvan u deel uitmaakt, door een antivirusoplossing is beveiligd.

- **E-mailverkeer scannen** - scant het e-mailverkeer.

De volgende opties zijn beschikbaar:

Optie	Beschrijving
Binnenkomende e-mails scannen	Scant alle binnenkomende e-mailberichten.
Uitgaande e-mails scannen	Scant alle uitgaande e-mailberichten.

- **Http-verkeer scannen** - scant het http-verkeer.
- **Waarschuwing weergeven wanneer een virus is gevonden** - opent een waarschuwingsvenster wanneer een virus wordt gevonden in een bestand of in een e-mailbericht.

  Voor een geïnfecteerd bestand zal het waarschuwingsvenster de naam van het virus bevatten, het pad naar het virus, de actie die door BitDefender wordt ondernomen en een koppeling naar de BitDefender-site waar u meer informatie over het virus kunt vinden. Voor een geïnfecteerde e-mail zal het waarschuwingsvenster ook informatie over de afzender en de ontvanger bevatten.

  Als een verdacht bestand is gedetecteerd, kunt u een wizard starten vanaf het waarschuwingsvenster. Deze wizard zal u helpen bij het verzenden van dat bestand naar BitDefender Labs voor verdere analyse. U kunt uw e-mailadres invoeren om informatie te ontvangen over dit rapport.
- **Via IM ontvangen/verzonden bestanden scannen.** Selecteer de overeenkomende vakjes om bestanden te scannen die u ontvangt of verzendt via Yahoo Messenger of Windows Live Messenger.

Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

16.1.3. Gedragscanner configureren

De Gedragscanner biedt bescherming tegen nieuwe bedreigingen waarvan nog geen signaturen bekend zijn. Hij bewaakt en analyseert voortdurend het gedrag van de aplicaties op uw computer en waarschuwt als een applicatie zicht verdacht gedraagt.

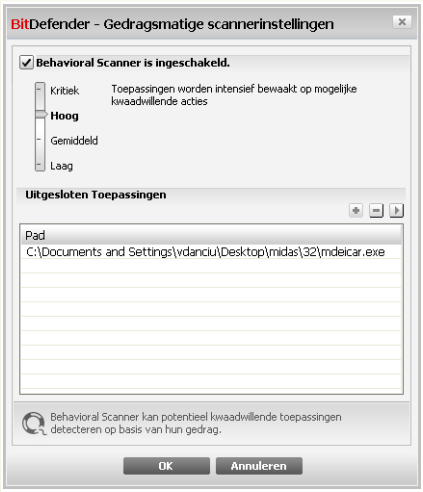
De Gedragscanner waarschuwt u als een applicatie probeert een mogelijk kwaadwillende actie uit te voeren en vraagt u om in te grijpen.

Gedragscanner waarschuwing

Klik op **Toestaan** als u de gedetecteerde applicatie vertrouwt. De Gedragscanner zal de applicatie niet langer scanner op kwaadwillend gedrag.

Klik op **OK** als u de applicatie onmiddellijk wilt sluiten.

Klik op **Scanner instellingen** om de Gedragscanner te configureren.



Behavioral Scanner Instellingen

Als u de Gedragscanner wilt uitschakelen, maak dan het selectievakje **Behavioral Scanner is ingeschakeld** leeg.

Belangrijk
Houd de Gedragscanner ingeschakeld om beschermd te zijn tegen onbekende virussen.

Het beschermingsniveau configureren

Het beschermingsniveau van de Gedragscanner verandert automatisch als u u een nieuw real-time beschermingsniveau instelt Als u niet tevreden bent met de standaardinstelling, kan u het beschermingsniveau handmatig configureren.

Opmerking
Bedenk dat als u het huidige real-time beschermingsniveau verandert, het beschermingsniveau van de Gedragscanner overeenkomstig verandert.

Sleep de schuifregelaar langs de schaal om het beschermingsniveau in te stellen dat het beste bij u past ij uw behoefte.

Beveiligingsniveau	*Beschrijving*
Kritiek	Applicaties worden streng bewaakt tegen mogelijke kwaadwillende acties.
Hoog	Applicaties worden intensief bewaakt tegen mogelijke kwaadwillende acties.
Gemiddeld	Applicaties worden gemiddeld bewaakt tegen mogelijke kwaadwillende acties.
Laag	Applicaties worden bewaakt tegen mogelijke kwaadwillende acties.

Uitgesloten applicaties beheren

U kan de Gedragscanner configureren om specifieke applicaties niet te scannen. De applicaties die niet worden gecontroleerd door Gedragscanner staan in de **Uitgesloten Applicaties** tabel.

Om de uitgesloten applicaties te beheren, kan u de knoppen aan de bovenkant van de tabel gebruiken:

- **Add** - exclude a new application from scanning.
- **Remove** - remove an application from the list.
- **Edit** - edit an application path.

16.1.4. Real time-beveiliging uitschakelen

Als u de real time-beveiliging wilt uitschakelen, verschijnt een waarschuwingsvenster.

Real time-beveiliging uitschakelen

U moet uw keuze bevestigen door in het menu te selecteren hoelang u de real time-beveiliging wilt uitschakelen. U kunt de real time-beveiliging uitschakelen gedurende 5, 15 of 30 minuten, 1 uur, definitief of tot het systeem opnieuw wordt opgestart.

Waarschuwing
Dit is een kritiek beveiligingsprobleem. Wij raden u aan de real time-beveiliging zo kort mogelijk uit te schakelen. Als de real time-beveiliging is uitgeschakeld, wordt u niet beveiligd tegen malware-bedreigingen.

16.1.5. Antiphishing bescherming configureren

BitDefender biedt real-time antiphishing beschermingvoor:

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger
- Windows Live (MSN) Messenger

U kan kiezen de antiphishing bescherming compleet of alleen voor specifieke applicaties uit te schakelen.

U kan klikken op **Witte lijst** om een lijst van websites te configureren en te beheren die BitDefender Antiphishing niet zal scannen.

Antiphishing Witte lijst

U ziet de websites die niet door BitDefender worden gecontroleerd op phishing inhoud.

Om een nieuwe website toe te voegen aan de witte lijst, typt u het url-adres van de site in het veld **Nieuw adres** en kikt u op **Toevoegen**. In de witte lijst mogen alleen websites staan die u volledig vertrouwt. Voeg bijvoorbeeld de websites toe waar u regelmatig online winkelt.

Opmerking

Met behulp van de werkbalk van BitDefender Antiphishing, die in uw webbrowser is geïntegreerd, kan u gemakkelijk websites toevoegen aan de witte lijst.

Om een website uit de witte lijst te verwijderen, klikt u op overeenkomende knop **Verwijderen**.

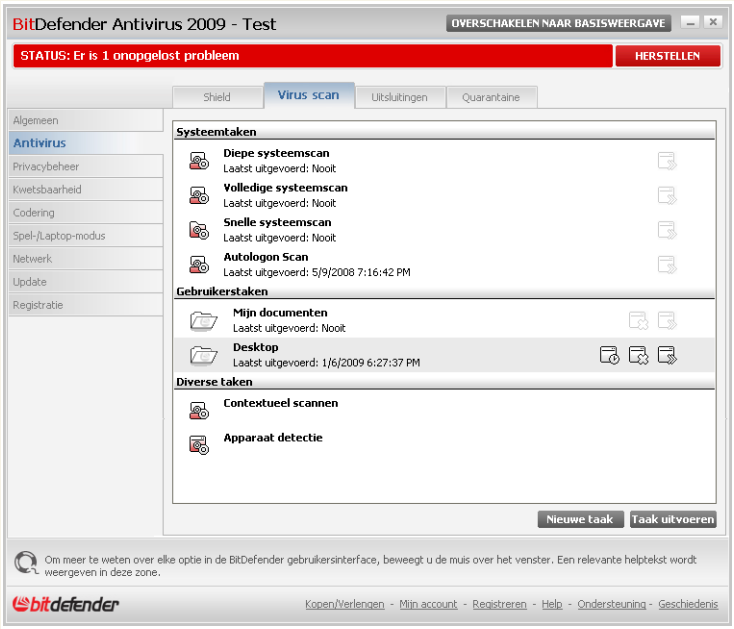
Klik op **Sluiten** om de wijzigingen op te slaan en het venster te sluiten.

16.2. Scannen op aanvraag

BitDefender heeft als hoofddoel uw computer vrij te houden van virussen. Dit wordt in de eerste plaats gedaan door nieuwe virussen uit uw computer weg te houden en door uw e-mailberichten en alle nieuwe bestanden, die u downloadt of kopieert naar uw systeem, te scannen.

Het risico bestaat dat een virus zich reeds in uw systeem heeft genesteld voordat u BitDefender installeert. Het is dan ook een bijzonder goed idee uw computer meteen te scannen op aanwezige virussen nadat u BitDefender hebt geïnstalleerd. En het is zeker ook een goed idee om uw computer frequent te scannen op virussen.

Om scannen op aanvraag te configureren en te starten, gaat u naar **Antivirus>Scannen** in de Geavanceerde weergave.



Scantaken

Scannen op aanvraag is gebaseerd op scantaken. Scantaken bepalen de scanopties en de objecten die moeten worden gescand. U kunt de computer scannen wanneer u dat wilt door de standaardtaken of uw eigen scantaken (door gebruiker gedefinieerde taken) uit te voeren. U kunt ook een planning instellen om taken regelmatig uit te voeren of wanneer het systeem inactief is zodat uw niet wordt gehinderd in uw werk.

16.2.1. Scantaken

BitDefender wordt geleverd met meerdere taken die standaard zijn gemaakt en de gebruikelijke beveiligingsproblemen dekken. U kunt ook uw eigen aangepaste scantaken maken.

Elke taak heeft een venster **Eigenschappen** waarmee u de taak kunt configureren en de scanresultaten kunt weergeven. Meer informatie vindt u onder "*Scantaken configureren*" (p. 106).

Er zijn drie categorieën scantaken:

- **Systeemtaken** - bevat de lijst van standaard systeemtaken. De volgende taken zijn beschikbaar:

Standaardtaak	*Beschrijving*
Diepe systeemscan	Scant het volledige systeem. In de standaardconfiguratie wordt er gescand op alle types malware die de beveiliging van uw systeem bedreigen, zoals virussen, spyware, adware, rootkits en andere.
Volledige systeemscan	Scant het volledige systeem, behalve archieven. In de standaardconfiguratie wordt er gescand op alle types malware die de beveiliging van uw systeem bedreigen, zoals virussen, spyware, adware, rootkits en andere.
Snelle systeemscan	Scant de mappen `Windows`, `Program Files` en `All Users`. In de standaardconfiguratie wordt gescand op alle types malware, behalve rootkits, maar het geheugen, het register en de cookies worden niet gescand.
Autologon Scan	Scant de items die worden uitgevoerd als een gebruiker zich aanmeldt bij Windows. Standaard is het automatisch scannen bij het aanmelden uitgeschakeld. Als u deze taak wilt gebruiken, klikt u met de rechtermuisknop op de taak, selecteert u **Planning** en stelt u de taak in die moet worden uitgevoerd **bij het opstarten van het systeem**. U kunt opgeven hoe

Standaardtaak	Beschrijving
	lang na het opstarten de taak moet worden gestart (in minuten).

Opmerking
Omdat de taken **Diepe systeemscan** en **Volledige systeemscan** analyseren het volledige systeem. Het scannen kan enige tijd in beslag nemen. Wij raden u daarom aan deze taken uit te voeren met een lage prioriteit, of bij voorkeur wanneer uw systeem inactief is.

- **Gebruikerstaken** - bevat de door de gebruiker gedefinieerde taken.

  Er wordt een taak geleverd met de naam `Mijn documenten`. Gebruik deze taak om belangrijke mappen van de huidige gebruiker te scannen. `Mijn documenten`, `Bureaublad` en `Opstarten`. Dit zal de veiligheid van uw documenten, een veilige werkruimte en opgeruimde toepassingen bij het opstarten garanderen.
- **Diverse taken** - bevat een lijst van diverse scantaken. Deze scantaken verwijzen naar alternatieve scantypes die vanaf dit venster kunnen worden uitgevoerd. U kunt alleen hun instellingen wijzigen of de scanrapporten weergeven.

Rechts van elke taak zijn drie knoppen beschikbaar:

- **Planning** - geeft aan dat de geselecteerde taak voor later is gepland. Klik op deze knop om het venster **Eigenschappen** te openen. Klik op het tabblad Planner waar u de taakplanning kunt bekijken en wijzigen.
- **Verwijderen** - verwijdert de geselecteerde taak.

Opmerking
Niet beschikbaar voor systeemtaken. U kunt geen systeemtaak verwijderen.

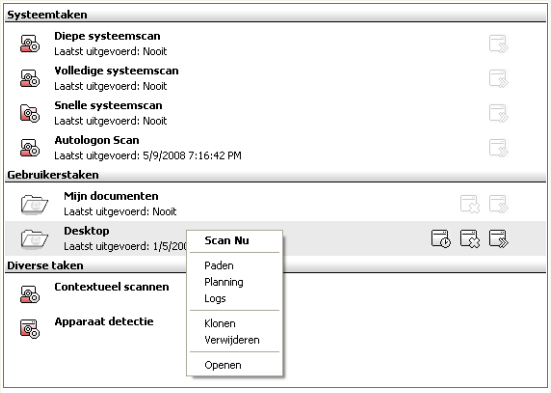
- **Nu scannen** - voert de geselecteerde taak uit en start de optie Onmiddellijk scannen.

Links naast elke taak ziet u de knop **Eigenschappen** waarmee u de taak kunt configureren en de scanlogs kunt weergeven.

16.2.2. Het snelmenu gebruiken

Voor elke taak is een snelmenu beschikbaar. Klik met de rechtermuisknop op de geselecteerde taak om deze te openen.

De volgende opdrachten zijn beschikbaar in het snelmenu:



Snelmenu

- **Nu scannen** - voert de geselecteerde taak uit en start een onmiddellijke scan.
- **Paden** - opent het venster **Eigenschappen**. Klik op het tabblad Paden waar u het scandoel van de geselecteerde taak kunt wijzigen.

Opmerking
In het geval van systeemtaken wordt deze optie vervangen door **Taakpaden weergeven** omdat u alleen hun scandoel kunt zien.

- **Planning** - opent het venster **Eigenschappen**. Klik op het tabblad Planner waar u de geselecteerde taak kunt plannen.
- **Logboeken** - opent het venster **Eigenschappen**. Klik op het tabblad Logboeken waar u de rapporten kunt bekijken die werden gegenereerd nadat de geselecteerde taak werd uitgevoerd.
- **Klonen** - dupliceert de geselecteerde taak. Dit is nuttig wanneer u nieuwe taken maakt omdat u de instellingen van een duplicaat van de taak kunt wijzigen.
- **Verwijderen** - verwijdert de geselecteerde taak.

Opmerking
Niet beschikbaar voor systeemtaken. U kunt geen systeemtaak verwijderen.

- **Openen** - opent het venster **Eigenschappen**. Klik op het tabblad Overzicht waar u de instellingen van de geselecteerde taak kunt wijzigen.

Opmerking
Door de specifieke aard van de categorie **Overige taken**, zijn in dit geval alleen de opties **Logboeken** and **Openen** beschikbaar.

16.2.3. Scantaken maken

Gebruik een van de volgende methoden om een scantaak te maken:

- Kopieer een bestaande taak, wijzig de naam van de taak en breng de nodige wijzigingen aan in het venster Eigenschappen.
- Klik op **Nieuwe taak** om een nieuwe taak te maken en te configureren.

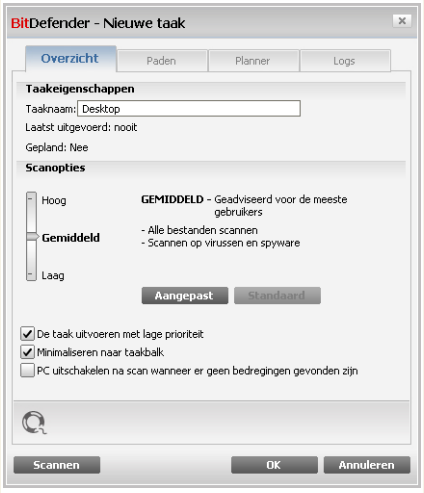
16.2.4. Scantaken configureren

Elke scantaak heeft zijn eigen venster **Eigenschappen** waarin u de scanopties kunt configureren, het scandoel kunt instellen, de taak kunt plannen of rapporten kunt weergeven. Om dit venster te openen, klikt u op de knop **Openen** die zich rechts van de taak bevindt (of klik met de rechtermuisknop op de taak en klik daarna op **Openen**).

Opmerking
Meer informatie over het weergeven van logboeken en het tabblad **Logboeken**, vindt u onder “*Scanlogs weergeven*” (p. 125).

Scaninstellingen configureren

Om de scanopties van een specifieke scantaak te configureren, klikt u met de rechtermuisknop en selecteert u **Openen**. Het volgende venster wordt geopend:



Overzicht

Hier ziet u informatie over de taak (naam, laatste uitvoering en status van de planning) en de scaninstellingen definiëren.

Het scanniveau selecteren

U kunt de scaninstellingen gemakkelijk configureren door het scanniveau te kiezen. Sleep de schuifregelaar langs de schaal om het geschikte scanniveau in te stellen.

Er zijn 3 scanniveaus:

Beveiligingsniveau	*Beschrijving*
Laag	Biedt een redelijke detectie-efficiëntie. Het verbruiksniveau van de bron is laag. Alleen programma's worden gescand op virussen. Naast de klassieke op handtekeningen gebaseerde scan, wordt ook de heuristische analyse gebruikt.
Gemiddeld	Biedt een goede detectie-efficiëntie. Het verbruiksniveau van de bron is gemiddeld.

Beveiligingsniveau	Beschrijving
	Alle bestanden worden gescand op virussen en spyware. Naast de klassieke op handtekeningen gebaseerde scan, wordt ook de heuristische analyse gebruikt.
Hoog	Biedt een hoge detectie-efficiëntie. Het verbruiksniveau van de bron is hoog. Alle bestanden en archieven worden gescand op virussen en spyware. Naast de klassieke op handtekeningen gebaseerde scan, wordt ook de heuristische analyse gebruikt.

Er is ook een reeks algemene opties beschikbaar voor het scanproces.

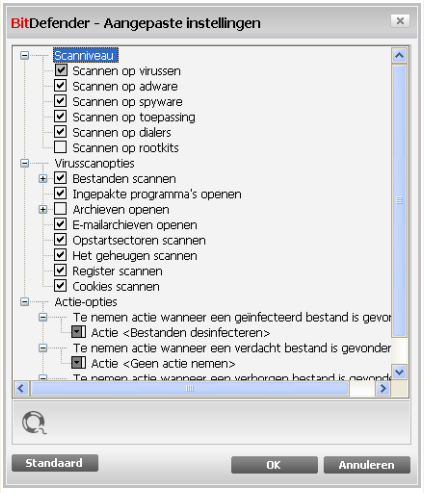
- **De taak uitvoeren met lage prioriteit.** Verlaagt de prioriteit van het scanproces. U zult andere programma's sneller kunnen uitvoeren en de tijd die nodig is om het scanproces te voltooien, verlengen.
- **Scanvenster naar systeemvak minimaliseren bij opstarten.** Minimaliseert het scanvenster naar het systeemvak. Dubbelklik op het pictogram BitDefender om het programma te openen.
- **Computer afsluiten nadat het scannen is voltooid als geen bedreigingen zijn gevonden**

Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten. Klik op **Scannen** om de taak uit te voeren.

Het scanniveau aanpassen

Gevorderde gebruikers willen wellicht voordeel halen uit de scaninstellingen die door BitDefender worden aangeboden. De scanner kan worden ingesteld om alleen specifieke bestandsextensies te scannen, specifieke malware-bedreigingen te zoeken of archieven over te slaan. Dat kan de duur van het scannen aanzienlijk verkorten en de reactie van uw computer tijdens het scannen verbeteren.

Klik op **Aangepast** om uw eigen scanopties in te stellen. Een nieuw venster wordt weergegeven.



Scaninstellingen

De scanopties zijn georganiseerd als een uitbereidbaar menu, vergelijkbaar met de menu's die in Windows gebruikt worden. Klik op het vakje met een "+" om een optie te openen of op het vakje met een "-" om een optie te sluiten.

De scanopties zijn gegroepeerd in drie categorieën:

- **Scanniveau.** Geef het type malware op waarop BitDefender moet scannen door de geschikte opties te selecteren in de categorie **Scanniveau**.

Optie	*Beschrijving*
Scannen op virussen	Scant op bekende virussen. BitDefender detecteert ook onvolledige virussen waardoor elke mogelijke bedreiging die de beveiliging van uw systeem kan beïnvloeden, wordt verwijderd.
Scannen op adware	Scant op adware-bedreigingen. Gedetecteerde bestanden zullen worden behandeld als geïnfecteerd. Software die adware-componenten bevat, zal mogelijk niet meer werken als deze optie is ingeschakeld.

Optie	Beschrijving
Scannen op spyware	Scant op bekende spyware-bedreigingen. Gedetecteerde bestanden zullen worden behandeld als geïnfecteerd.
Scannen op toepassing	Scannen op legitieme applicaties die kunnen worden gebruikt voor spionage, voor het verbergen van kwaadwillende applicaties of voor andere kwaadwillende bedoelingen.
Scannen op dialers	Scant op toepassingen die dure nummers belt. Gedetecteerde bestanden zullen worden behandeld als geïnfecteerd. Software die dialer-componenten bevat, zal mogelijk niet meer werken als deze optie is ingeschakeld.
Scannen op rootkits	Scant op verborgen objecten (bestanden en processen), algemeen bekend als rootkits.

- **Virusscanopties.** Geef het type objecten op dat moet worden gescand (bestandstypes, e-mailberichten, enz.) door het selecteren van de overeenkomende opties van de categorie **Virusscanopties**.

Optie		Beschrijving
Bestanden scannen	**Alle bestanden scannen**	Alle bestanden worden gescand, ongeacht hun type.
	Alleen programmabestanden scannen	Alleen de programmabestanden worden gescand. Dit betekent alleen bestanden met de volgende extensies: exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml en nws.
	Door gebruiker gedefinieerde extensies scannen	Alleen de bestanden met de extensies die door de gebruiker zijn gedefinieerd, worden gescand. Deze extensies moeten worden gescheiden door ";".

Optie	Beschrijving
Ingepakte programma's openen	Scant ingepakte bestanden.
Archieven openen	Scant binnen archieven. Scannen van gearchiveerde bestanden verlengt de scantijd en vereist meer systeembronnen. U kan klikken op het veld **Max. archiefgrootte** en de maximumgrootte in kilobytes (KB) van de te scannen archieven intypen.
E-mailarchieven openen	Scant binnen e-mailarchieven.
Opstartsectoren scannen	Scant de opstartsector van het systeem.
Geheugen scannen	Scant het geheugen op virussen en andere malware.
Register scannen	Scant registergegevens.
Cookies scannen	Scant cookiebestanden.

- **Actie-opties.** Geef met behulp van de opties in de categorie **Actie-opties** de actie op die moet worden uitgevoerd op elke categorie van gedetecteerde bestanden.

  Opmerking
  Om een nieuwe actie in te stellen, klikt u op de huidige actie en selecteert u de gewenste optie in het menu.

  - Selecteer de actie die moet worden genomen voor de geïnfecteerde bestanden. De volgende opties zijn beschikbaar:

Actie	Beschrijving
Geen (logboekobjecten)	Er wordt geen actie ondernomen voor geïnfecteerde bestanden. Deze bestanden zullen verschijnen in het rapportbestand.
Bestanden desinfecteren	De malware code van de geïnfecteerde bestanden verwijderen.
Bestanden verwijderen	Verwijdert onmiddellijk de geïnfecteerde bestanden, zonder enige waarschuwing.

Actie	Beschrijving
Bestanden verplaatsen naar quarantaine	Verplaatst de geïnfecteerde bestanden naar de quarantaine. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer.

- Selecteer de actie die moet worden genomen voor de verdachte bestanden die zijn gedetecteerd. De volgende opties zijn beschikbaar:

Actie	Beschrijving
Geen (logboekobjecten)	Er wordt geen actie ondernomen voor verdachte bestanden. Deze bestanden zullen verschijnen in het rapportbestand.
Bestanden verwijderen	Verwijdert onmiddellijk de verdachte bestanden, zonder enige waarschuwing.
Bestanden verplaatsen naar quarantaine	Verplaatst de verdachte bestanden naar de quarantaine. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer.

Opmerking
De bestanden worden gedetecteerd als verdacht door de heuristische analyse. Wij raden u aan deze bestanden naar het BitDefender Lab te sturen.

- Selecteer de actie die moet worden genomen voor de verborgen objecten (rootkits) die zijn gedetecteerd. De volgende opties zijn beschikbaar:

Actie	Beschrijving
Geen (logboekobjecten)	Er wordt geen actie ondernomen voor verborgen bestanden. Deze bestanden zullen verschijnen in het rapportbestand.
Bestanden verplaatsen naar quarantaine	Verplaatst de verborgen bestanden naar de quarantaine. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer.

Actie	Beschrijving
Zichtbaar maken	Maakt verborgen bestanden zichtbaar.

- **Actieopties voor archiefbestanden.** Voor het scannen en behandelen van bestanden in archieven gelden er beperkingen. Met een wachtwoord beveiligde archieven kunnen niet worden gescand, tenzij u het wachtwoord opgeeft. Afhankelijk van het archiefformaat (type), kan BitDefender gearchiveerde bestanden misschien niet desinfecteren, isoleren of verwijderen. Configureer met behulp van de geschikte opties van de categorie **Gearchiveerde bestanden actie-opties** de op de gedetecteerde gearchiveerde bestanden uit te voeren acties.
  - Selecteer de actie die moet worden genomen voor de geïnfecteerde bestanden. De volgende opties zijn beschikbaar:

Actie	Beschrijving
Geen actie nemen	Geïnfecteerde gearchiveerde bestanden alleen in het scan logboek opnemen. Als de scan is voltooid, kan u het scanlogbestand openen om informatie over deze bestanden te zien.
Bestanden desinfecteren	De malware code van de geïnfecteerde bestanden verwijderen. In sommige gevallen kan desinfectie mislukken, bijvoorbeeld als het geïnfecteerde bestand zich in specifieke mailarchieven bevindt.
Bestanden verwijderen	Verwijder onmiddellijk de geïnfecteerde bestanden van de schijf, zonder enige waarschuwing.
Bestanden verplaatsen naar quarantaine	Verplaats geïnfecteerde bestanden van hun oorspronkelijke locatie naar de quarantainemap In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer.

  - Selecteer de actie die moet worden genomen voor de verdachte bestanden die zijn gedetecteerd. De volgende opties zijn beschikbaar:

Actie	Beschrijving
Geen actie nemen	Verdachte gearchiveerde bestanden alleen in het scan logboek opnemen. Als de scan is voltooid, kan u het scanlogbestand openen om informatie over deze bestanden te zien.
Bestanden verwijderen	Verwijdert onmiddellijk de verdachte bestanden, zonder enige waarschuwing.
Bestanden verplaatsen naar quarantaine	Verplaatst de verdachte bestanden naar de quarantaine. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer.

- Selecteer de actie die moet worden genomen voor de met een wachtwoord beschermde bestanden. De volgende opties zijn beschikbaar:

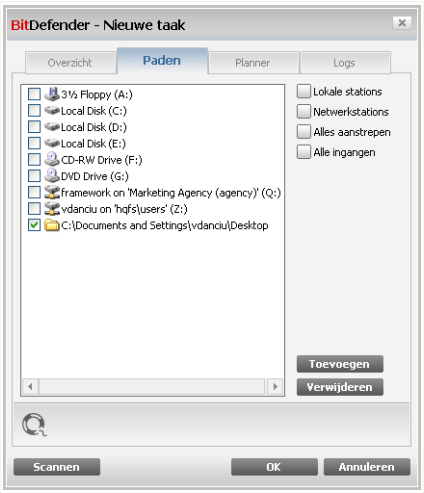
Actie	Beschrijving
Log als niet gescand	Met een wachtwoord beschermde bestanden alleen in het scan logboek opnemen. Als de scan is voltooid, kan u het scanlogbestand openen om informatie over deze bestanden te zien.
Vragen om wachtwoord	Als een met een wachtwoord beschermd bestand is gedetecteerd, de gebruiker vragen om het wachtwoord te geven voor het scannen van het bestand.

Opmerking
Als u de gedetecteerde bestanden wilt negeren of als de gekozen actie mislukt, moet u een actie selecteren in de scanwizard.

Als u op **Standaard** klikt, worden de standaardinstellingen geladen. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

Het scandoel instellen

Om het scandoel van een specifieke scantaak van de gebruiker in te stellen, klikt u met de rechtermuisknop op de taak en selecteert u **Paden**. Het volgende venster wordt geopend:



Scandoel

U kunt de lijst van lokale, netwerk en verwisselbare stations evenals de bestanden of mappen die eventueel eerder werden toegevoegd, weergeven. Alle ingeschakelde items zullen worden gescand tijdens het uitvoeren van de taak.

Dit onderdeel bevat de volgende knoppen:

- **Item toevoegen** - opent een zoekvenster waarin u de bestanden/mappen die u wilt scannen, kunt selecteren.

  Opmerking
  U kunt ook slepen & neerzetten gebruiken om bestanden/mappen toe te voegen aan de lijst.

- **Item verwijderen** - verwijdert bestanden/mappen die vooraf werden geselecteerd in de lijst van objecten die moeten worden gescand.

Opmerking
Alleen de bestanden/mappen die achteraf werden toegevoegd, kunnen worden verwijderd. Dat is niet mogelijk met de bestanden/mappen die automatisch door BitDefender werden "gezien".

Naast de knoppen die hierboven zijn toegelicht, zijn er ook enkele opties waarmee u de scanlocaties snel kunt selecteren.

- **Lokale stations** - om de lokale stations te scannen.
- **Netwerkstations** - om alle netwerkstations te scannen.
- **Verwisselbare stations** - om de verwisselbare stations (cd-rom, diskettestation) te scannen.
- **Alle gegevens** - om alle stations te scannen, ongeacht of ze lokaal, in het netwerk of verwisselbaar zijn.

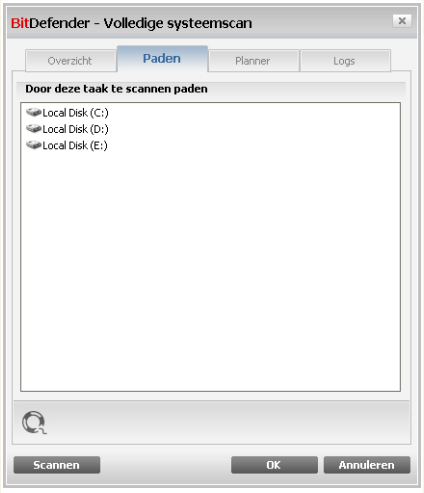
Opmerking
Activeer het selectievakje naast **Alle gegevens** als u uw volledige computer wilt scannen op virussen.

Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten. Klik op **Scannen** om de taak uit te voeren.

Scandoel van systeemtaken bekijken

U kunt het scandoel van de scantaken niet wijzigen via de categorie **Systeemtaken**. U kan alleen het scandoel ervan zien.

Om het scandoel te tonen van een scantaak van een specifieke systeem, klikt u rechts op de taak en selecteert u **Taakpaden weergeven**. Voor een **Volledige systeemscan**, bijvoorbeeld, verschijnt het volgende venster:



Scandoel van Volledige systeemscan

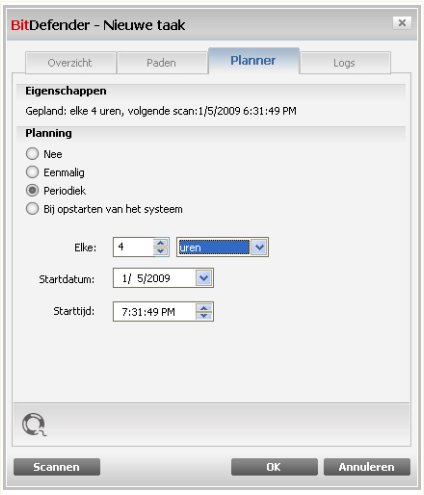
Volledige systeemscan en **Diepe systeemscan** scannen alle lokale schijven, terwijl **Snelle systeemscan** alleen de `Windows` en `Program Files` mappen scant.

Klik op **OK** om het venster te sluiten. Om deze taak uit te voeren, klikt u op **Scan**.

Scantaken plannen

Bij complexe taken zal het scanproces enige tijd in beslag nemen en zal het proces het beste werken als u alle andere programma's afsluit. Daarom is het aan te raden dergelijke taken te plannen op tijdstippen waarop u de computer niet gebruikt en naar de inactieve stand is overgeschakeld.

Om de planning van een specifieke taak weer te geven of te wijzigen, klikt u met de rechtermuisknop op de taak en selecteert u **Planning**. Het volgende venster wordt geopend:



Planner

Als er een taakplanning is, kunt u deze bekijken.

Wanneer u een taak plant, moet u een van de volgende opties kiezen:

- **Niet gepland** - start de taak alleen wanneer de gebruiker dit vraagt.
- **Eenmalig** - start het scannen eenmalig op een bepaald ogenblik. Geef de startdatum en het starttijdstip op in de velden **Startdatum/Starttijd**.
- **Periodiek** - start de scan periodiek, met bepaalde tijdintervallen (uren, dagen, weken, maanden, jaren) vanaf een opgegeven datum en tijdstip.

  Selecteer **Periodiek** als u wilt dat het scannen met bepaalde intervallen wordt herhaald en geef het aantal minuten/uren/dagen/weken/maanden/jaren op in het bewerkingsvak **Elke** om de frequentie van dit proces aan te geven. U moet ook de startdatum en het starttijdstip opgeven in de velden **Startdatum/Starttijd**.
- **Bij opstarten van het systeem** - start de scan na het aangegeven aantal minuten nadat de gebruiker zich heeft aangemeld bij Windows.

Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten. Klik op **Scannen** om de taak uit te voeren.

16.2.5. Objecten scannen

Voordat u het scanproces start, moet u controleren of de malware-handtekeningen up-to-date zijn in BitDefender. Het scannen van uw computer met een oude handtekeningendatabase kan verhinderen dat BitDefender nieuwe malware die sinds de laatste update is gevonden, detecteert. Om te controleren wanneer de laatste update is uitgevoerd, klikt u in de instellingsconsole op **Update>Update** .

Opmerking
Als u wilt dat BitDefender een volledige scan uitvoert, moet u alle geopende programma's afsluiten. Het is vooral belangrijk dat u uw e-mail-client afsluit (Outlook, Outlook Express of Eudora).

Scanmethoden

BitDefender biedt u vier types voor het scannen op aanvraag:

- Onmiddellijk scannen - voer een scantaak uit van de systeem-/gebruikerstaken.
- Contextueel scannen - klik met de rechtermuisknop op een bestand of een map en selecteer BitDefender Antivirus 2009.
- Scannen door slepen & neerzetten - sleep een bestand of map naar de balk Scanactiviteit.
- Handmatig scannen - gebruik BitDefender Handmatig scannen om de bestanden of mappen die moeten worden gescand, rechtstreeks te selecteren.

Onmiddellijk scannen

Om uw computer volledig of gedeeltelijk te scannen, kunt u de standaard scantaken of uw eigen scantaken uitvoeren. Dit wordt Onmiddellijk scannen genoemd.

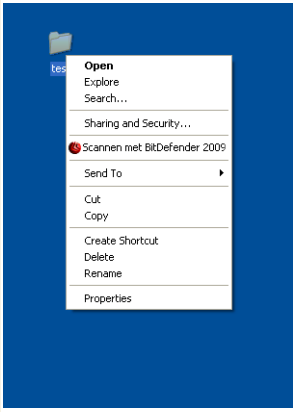
Gebruik een van de volgende methoden om een scantaak uit te voeren:

- dubbelklik op de gewenste scantaak in de lijst.
- klik op de knop **Nu scannen** die overeenkomt met de taak.
- selecteer de taak en klik vervolgens op **Taak uitvoeren**.

BitDefender Scanner verschijnt en het scannen wordt gestart. Meer informatie vindt u onder "*BitDefender Scanner*" (p. 121).

Contextueel scannen

Om een bestand of een map te scannen zonder een nieuwe scantaak te configureren, kunt u het contextmenu gebruiken. Dit wordt Contextueel scannen genoemd.



Contextueel scannen

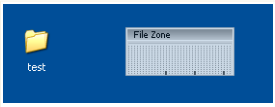
Klik met de rechtermuisknop op het bestand of de map die u wilt scannen en selecteer **BitDefender Antivirus 2009**.

BitDefender Scanner verschijnt en het scannen wordt gestart. Meer informatie vindt u onder "*BitDefender Scanner*" (p. 121).

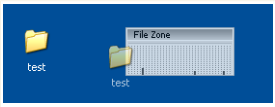
U kunt de scanopties wijzigen en de rapportbestanden weergeven door het venster **Eigenschappen** van de taak **Contextmenuscan** te openen.

Scannen door slepen & neerzetten

Sleep het bestand of de map die u wilt scannen naar de **balk Scanactiviteit** zoals hieronder weergegeven.



Bestand slepen



Bestand neerzetten

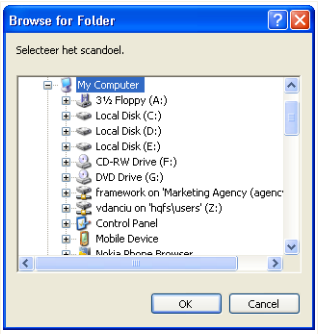
BitDefender Scanner verschijnt en het scannen wordt gestart. Meer informatie vindt u onder "*BitDefender Scanner*" (p. 121).

Handmatig scannen

Handmatig scannen bestaat uit het rechtstreeks selecteren van het object dat moet worden gescand door middel van de optie Handmatig scannen van BitDefender in de programmagroep BitDefender in het menu Start.

Opmerking
Het handmatig scannen is zeer nuttig omdat het ook kan worden uitgevoerd wanneer Windows in de veilige modus werkt.

Om het object dat door BitDefender moet worden gescand te selecteren, gebruikt u het menu Start van Windows en volgt u het pad **Start → Programma's → BitDefender 2009 → BitDefender Handmatig scannen**. Het volgende venster wordt geopend:



Handmatig scannen

Selecteer het object dat u wilt scannen en klik op **OK**.

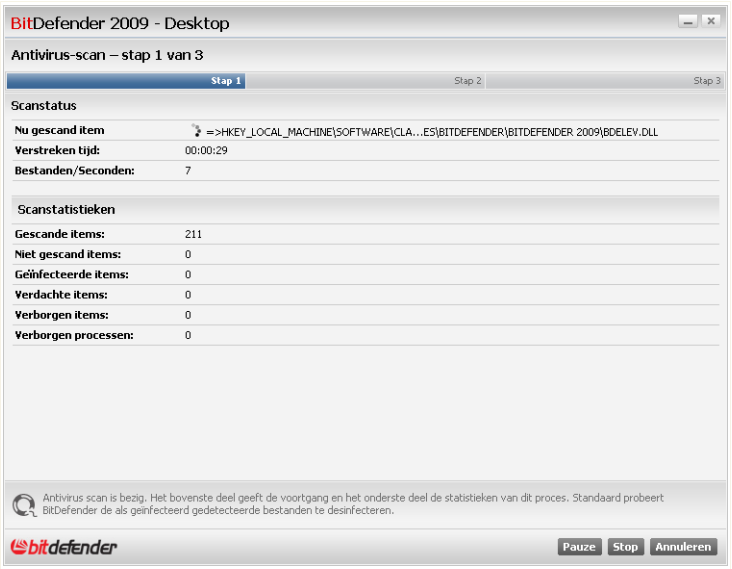
BitDefender Scanner verschijnt en het scannen wordt gestart. Meer informatie vindt u onder "*BitDefender Scanner*" (p. 121).

BitDefender Scanner

Wanneer u een proces Scannen op aanvraag start, verschijnt BitDefender Scanner. Volg de begeleide procedure van drie stappen om het scanproces te voltooien.

Stap 1/3 - Scannen

BitDefender start het scannen van de geselecteerde objecten.



Scannen

U kunt de scanstatus en de statistieken zien (scansnelheid, verstreken tijd, aantal gescande/geïnfecteerde/verdachte/verborgen objecten en andere).

Opmerking
Afhankelijk van de complexiteit van de scan, kan het scanproces enige tijd in beslag nemen.

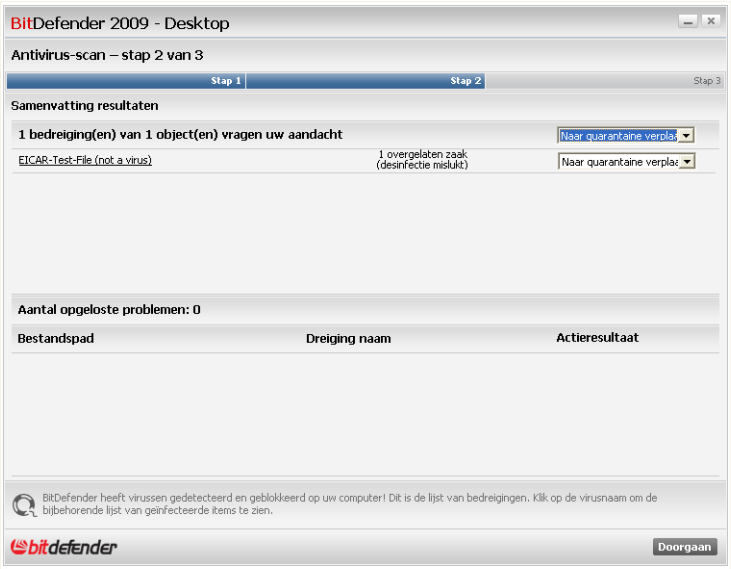
Klik op **Pauze** om het scanproces tijdelijk te stoppen. Om het scannen te hervatten, klikt u op **Hervatten**.

U kunt het scannen op elkogenblik stoppen door op **Stop&Ja** te klikken. U gaat dan rechtstreeks naar de laatste stap van de wizard.

Wacht tot BitDefender het scannen beëindigt.

Stap 2/3 - Acties selecteren

Wanneer het scannen is voltooid, verschijnt een nieuw venster waarin u de scanresultaten kunt zien.



Acties

U kan het aantal problemen dat uw systeem beïnvloedt, zien.

De geïnfecteerde objecten worden weergegeven in groepen, die zijn gebaseerd op de malware waarmee ze zijn geïnfecteerd. Klik op de link van de bedreiging voor meer informatie over de geïnfecteerde objecten.

U kan een algemene actie selecteren die moet worden genomen voor alle groepen problemen of u kan afzonderlijke acties voor elke groep problemen selecteren.

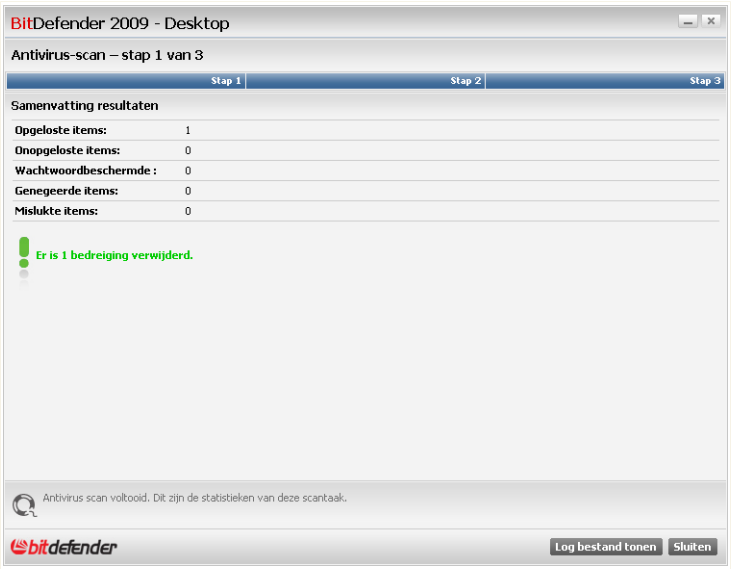
De volgende opties kunnen in het menu verschijnen:

Actie	*Beschrijving*
Geen actie nemen	Er wordt geen actie ondernomen voor de geïnfecteerde bestanden.
Desinfecteren	Desinfecteert geïnfecteerde bestanden.
Verwijderen	Verwijdert gedetecteerde bestanden.
Zichtbaar maken	Maakt verborgen objecten zichtbaar.

Klik op **Doorgaan** om de aangegeven acties toe te passen.

Stap 3/3 - Resultaten weergeven

Wanneer BitDefender het oplossen van de problemen heeft voltooid, verschijnen de scanresultaten in een nieuw venster.



Samenvatting

U kan een samenvatting van de resultaten zien. **Log weergeven** - om het geselecteerde scanlogbestand weer te geven.

Belangrijk
Start indien nodig uw systeem opnieuw, zodat het installatieprogramma de installatie kan voltooien.

Klik op **Sluiten** om het venster te sluiten.

BitDefender kon bepaalde problemen niet oplossen

In de meeste gevallen desinfecteert BitDefender met succes de geïnfecteerde bestanden die het detecteert of isoleert het de infectie. Echter niet alle problemen kunnen worden opgelost.

In deze gevallen, raden wij u aan contact op te nemen met het ondersteuningsteam van BitDefender op www.bitdefender.com. Onze experts helpen u de problemen op te lossen.

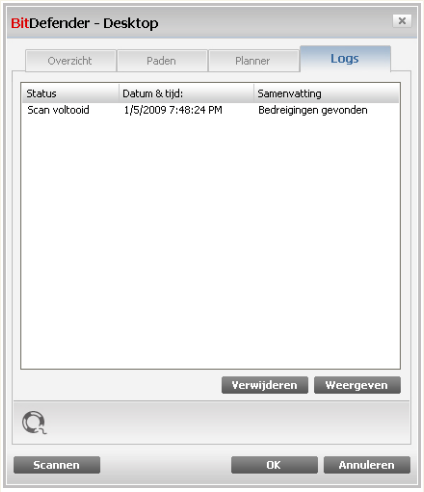
BitDefender detecteerde verdachte bestanden

Verdachte bestanden zijn bestanden die zijn gedetecteerd door de heuristische analyse als potentieel geïnfecteerd met malware waarvan de signatuur nog niet bekend is.

Als er tijdens het scannen verdachte bestanden zijn gedetecteerd, wordt u gevraagd ze naar het BitDefender Lab te sturen. Klik op **OK** om deze bestanden naar het BitDefender laboratorium te verzenden voor verdere analyse.

16.2.6. Scanlogs weergeven

Om de scanresultaten te zien nadat een taak is uitgevoerd, klikt u met de rechtermuisknop op de taak en selecteert u **Logboeken**. Het volgende venster wordt geopend:



Scanlogs

Hier ziet u de rapportbestanden die zijn gegenereerd bij het uitvoeren van de taak. Van elk bestand krijgt u informatie over de status van het gevolgde scanproces, de datum en tijd waarop de scan is uitgevoerd en een samenvatting van de scanresultaten.

Er zijn twee knoppen beschikbaar:

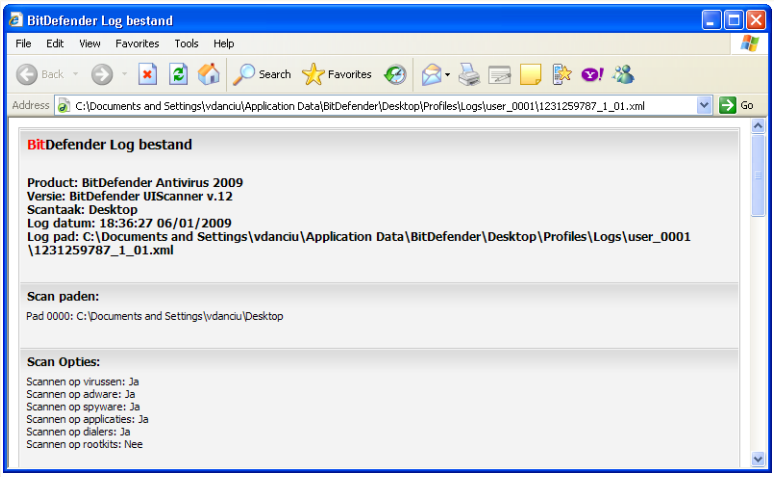
- **Verwijderen** - om het geselecteerde scanlogbestand te verwijderen.
- **Weergeven** - om het geselecteerde scanlogbestand weer te geven. Het scanlog wordt geopend in uw standaard webbrowser.

Opmerking
Om een bestand weer te geven of te verwijderen, klikt u met de rechtermuisknop op het bestand wn selecteert u de overeenkomende optie in het snelmenu.

Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten. Klik op **Scannen** om de taak uit te voeren.

Scanlog voorbeeld

De volgende afbeelding is een voorbeeld van een scanlog:



Scanlog voorbeeld

Het scanlog bevat gedetailleerde informatie over het gevolgde scanproces, zoals de scanopties, het scandoel, de gevonden bedreigingen en de hierop uitgevoerde acties.

16.3. Uitgesloten objecten van het scannen

Er zijn situaties waarbij u bepaalde bestanden wilt uitsluiten van het scannen. U wilt bijvoorbeeld een EICAR-testbestand uitsluiten van een Scan bij toegang of `.avi`-bestanden uitsluiten van een Scan op aanvraag.

Met BitDefender kan u objecten uitsluiten van een Scan bij toegang, een Scan op aanvraag, of beide. Deze functie is bedoeld om de scantijden te verkorten en onderbreking in uw werk te vermijden.

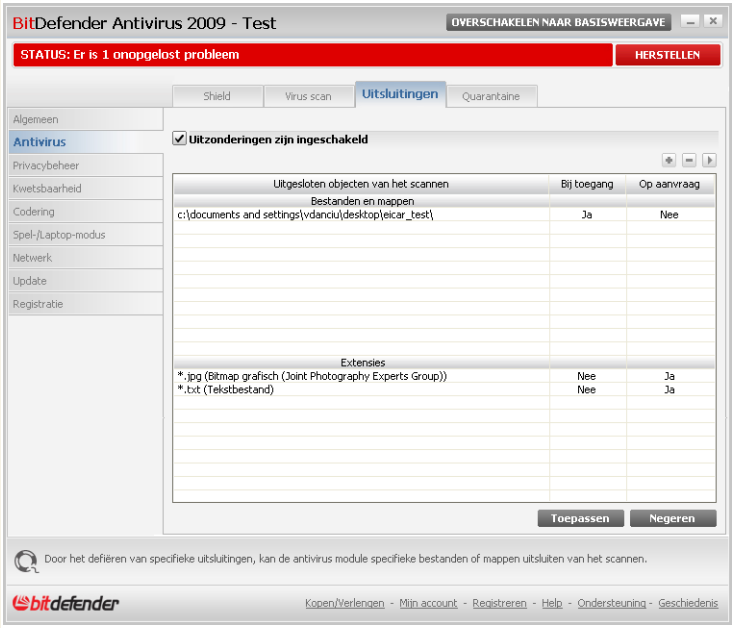
Er kunnen twee types objecten worden uitgesloten van het scannen:

- **Paden** - het bestand of de map (inclusief alle objecten die erin zijn opgenomen) die is aangegeven door een opgegeven pad, wordt uitgesloten van het scannen.
- **Extensies** - alle bestanden met een specifieke extensie worden uitgesloten van het scannen.

Opmerking

De objecten die zijn uitgesloten van scannen bij toegang, worden niet gescand, ongeacht of ze door u of door een toepassing worden geopend.

Om de objecten die zijn uitgesloten van het scannen, weer te geven en te beheren, klikt u op **Antivirus>Uitzonderingen** in de Geavanceerde weergave.



Uitzonderingen

U kan de objecten (bestanden, mappen, extensies) zien die van het scannen zijn uitgesloten. Voor elk object kan u zien of het is uitgesloten van scannen bij toegang, scannen op aanvraag of beide.

Opmerking
De uitzonderingen die hier zijn opgegeven, zijn NIET van toepassing voor contextueel scannen.

Om een gegeven uit de tabel te verwijderen, selecteert u het gegeven en klikt u op de knop **Verwijderen**.

Om een gegeven in de tabel te bewerken, selecteert u het gegeven en klikt u op de knop **Bewerken**. Er verschijnt een nieuw venster. Hierin kan u de extensie of het pad dat moet worden uitgesloten en het type scan waarvoor u ze wilt uitsluiten, wijzigen volgens uw voorkeur. Breng de nodige wijzigingen aan en klik op **OK**.

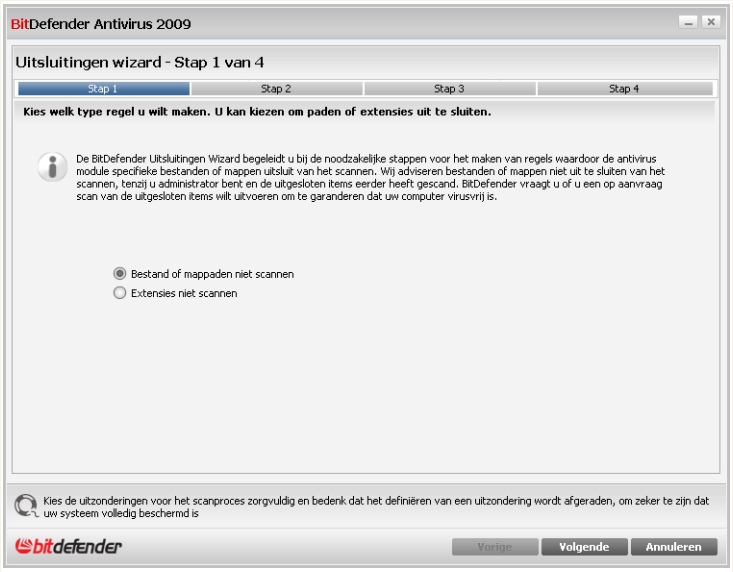
Opmerking
U kan ook met de rechtermuisknop op een object klikken en de opties in het snelmenu gebruiken om het object te bewerken of te verwijderen.

U kan klikken op **Negeren** om de wijzigingen aan de regeltabel ongedaan te maken, op voorwaarde dat u ze niet hebt opgeslagen door te klikken op **Toepassen**.

16.3.1. Paden uitsluiten van het scannen

Om paden uit te sluiten van het scannen, klikt u op de knop **Toevoegen**. De configuratiewizard die verschijnt, zal u begeleiden door het proces voor het uitsluiten van het scannen van paden.

Stap 1/4 - Objecttype selecteren

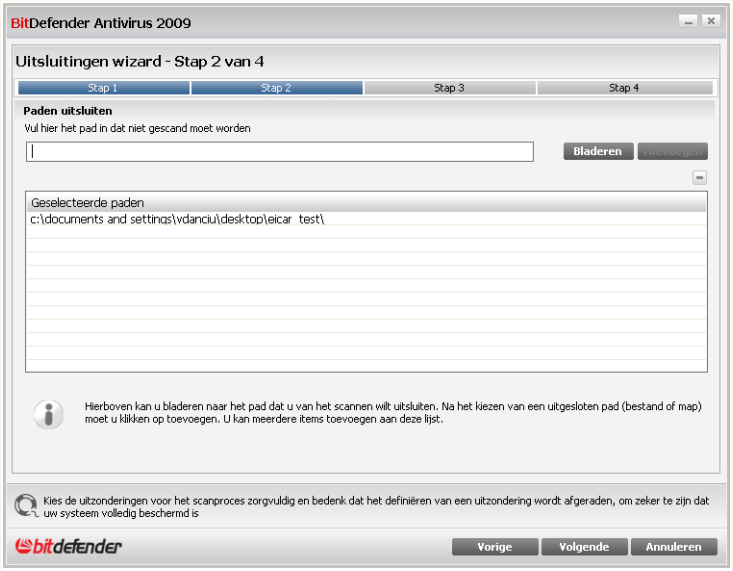


Objecttype

Selecteer de optie om een pad van het scannen uit te sluiten.

Klik op **Volgende**.

Stap 2/4 - Uitgesloten paden opgeven



Uitgesloten paden

Om de paden die moeten worden uitgesloten van het scannen op te geven, gebruikt u een van de volgende methoden.

- Klik op **Bladeren**, selecteer het bestand of de map die u van het scannen wilt uitsluiten en klik vervolgens op **Toevoegen**.
- Voer het pad dat u van het scannen wilt uitsluiten in het bewerkingsveld in en klik op **Toevoegen**.

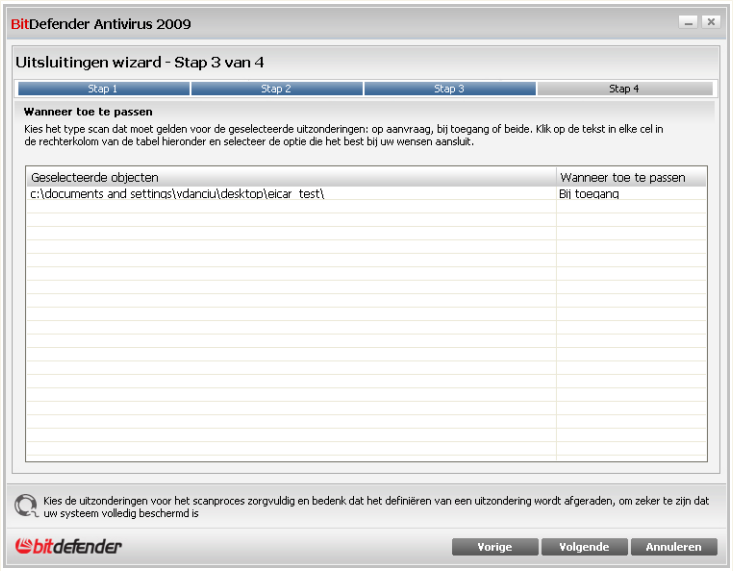
> ***Opmerking***
> Als het opgegeven pad niet bestaat, verschijnt een foutbericht. Klik op **OK** en controleer het pad.

De paden verschijnen in de tabel wanneer u ze toevoegt. U kan zoveel paden toevoegen als u wilt.

Om een gegeven uit de tabel te verwijderen, selecteert u het gegeven en klikt u op de knop **Verwijderen**.

Klik op **Volgende**.

Stap 3/4 - Scantype selecteren



Scantype

U ziet een tabel met de paden die zijn uitgesloten van het scannen en het type scan waarvan ze zijn uitgesloten.

De geselecteerde paden worden standaard uitgesloten van Scan bij toegang en van Scan op aanvraag. Om te wijzigen wanneer de uitzondering moet worden toegepast, klikt u op de rechterkolom en selecteert u de gewenste optie in de lijst.

Klik op **Volgende**.

Stap 4/4 - Uitgesloten bestanden scannen

Uitgesloten bestanden scannen

Wij adviseren met kracht de bestanden in de aangegeven paden te scannen, om er zeker van te zijn dat zij niet geïnfecteerd zijn. Kruis het vakje aan om deze bestanden te scannen voordat zij worden uitgesloten van het scannen.

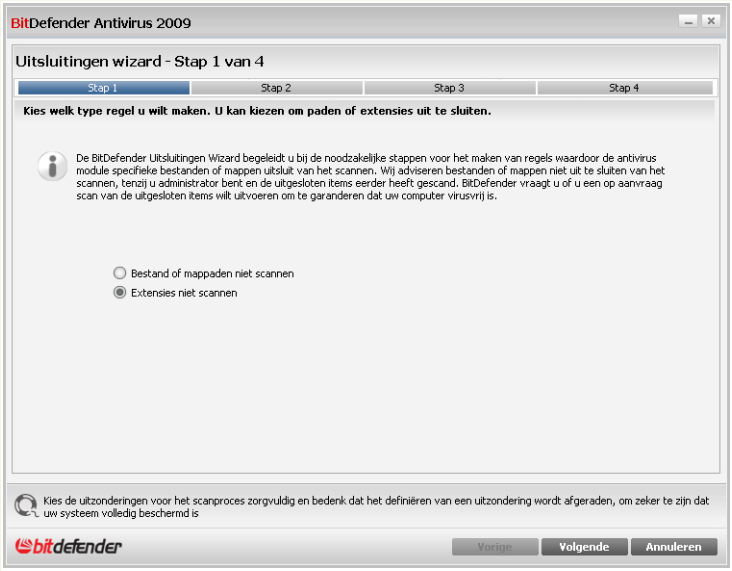
Klik op **Voltooien**.

Klik op **Toepassen** om de wijzigingen op te slaan.

16.3.2. Extensies uitsluiten van het scannen

Om extensies van het scannen uit te sluiten, klikt u op de knop **Toevoegen**. De configuratiewizard die verschijnt, zal u begeleiden door het proces voor het uitsluiten van het scannen van extensies.

Stap 1/4 - Objecttype selecteren

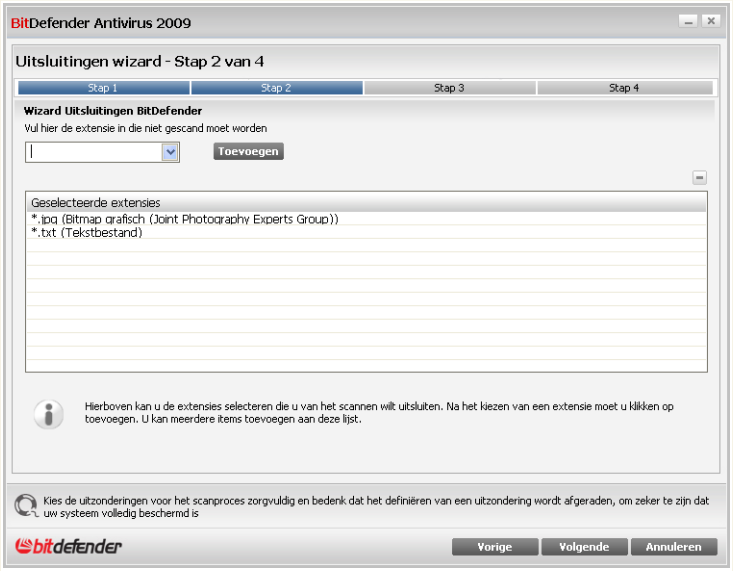


Objecttype

Selecteer de optie om een extensie van het scannen uit te sluiten.

Klik op **Volgende**.

Stap 2/4 - Uitgesloten extensies opgeven



Uitgesloten extensies

Om de extensies die van het scannen moeten worden uitgesloten op te geven, gebruikt u een van de volgende methoden:

- Selecteer de extensie die u van het scannen wilt uitsluiten in het menu en klik vervolgens op **Toevoegen**.

> ***Opmerking***
> Het menu bevat een lijst met alle extensies die op uw systeem zijn geregistreerd. Wanneer u een extensie selecteert, kan u de beschrijving zien, indien deze beschikbaar is.

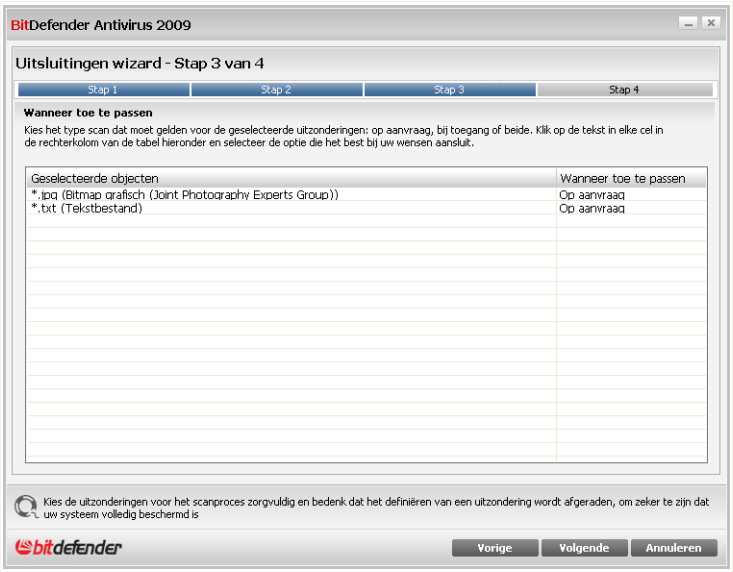
- Voer de extensie die u van het scannen wilt uitsluiten in het bewerkingsveld in en klik op **Toevoegen**.

De extensies verschijnen in de tabel wanneer u ze toevoegt. U kan zoveel extensies toevoegen als u wilt.

Om een gegeven uit de tabel te verwijderen, selecteert u het gegeven en klikt u op de knop **Verwijderen**.

Klik op **Volgende**.

Stap 3/4 - Scantype selecteren



Scantype

U ziet een tabel met de extensies die van het scannen zijn uitgesloten en het type scan waarvan ze zijn uitgesloten.

De geselecteerde extensies worden standaard uitgesloten van Scan bij toegang en van Scan op aanvraag. Om te wijzigen wanneer de uitzondering moet worden toegepast, klikt u op de rechterkolom en selecteert u de gewenste optie in de lijst.

Klik op **Volgende**.

Stap 4/4 - Scantype selecteren

Scantype

Wij adviseren met kracht de bestanden die de opgegeven extensies hebben te scannen, om er zeker van te zijn dat zij niet zijn geïnfecteerd.

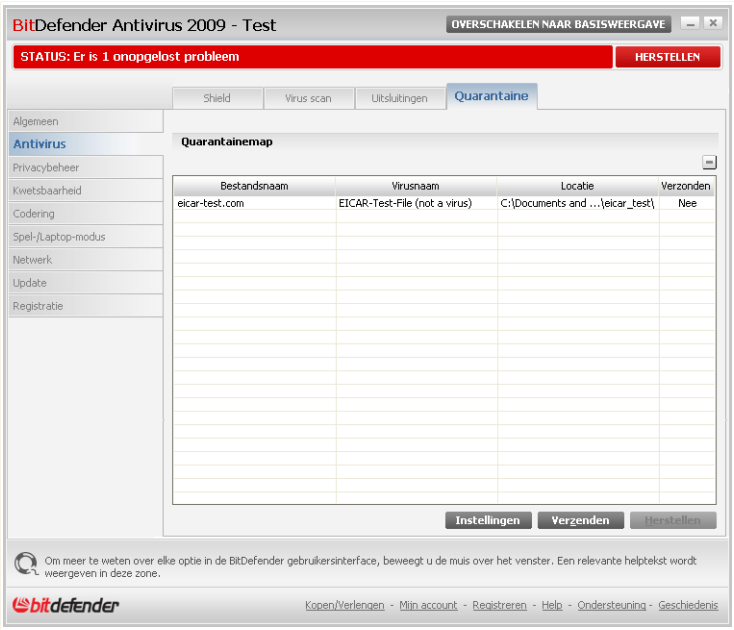
Klik op **Voltooien**.

Klik op **Toepassen** om de wijzigingen op te slaan.

16.4. Quarantainegebied

BitDefender biedt u de mogelijkheid geïnfecteerde of verdachte bestanden te isoleren in een beveiligd gebied, de quarantaine. Door deze bestanden te isoleren in de quarantaine verdwijnt het risico op infecties, maar hebt u tegelijk ook de mogelijkheid deze bestanden voor verdere analyse te verzenden naar het BitDefender laboratorium.

Om de bestanden in quarantaine te zien en te beheren en om de quarantaine-instellingen te configureren, klikt u op **Antivirus>Quarantaine** in de Geavanceerde weergave.



Quarantaine

In de quarantainesectie ziet u alle bestanden die op dit moment zijn geïsoleerd in de quarantainemap. Voor elk bestand in quarantaine, ziet de naam, de naam van het gedetecteerde virus, het pad naar de oorspronkelijke locatie en de verzendingsdatum.

Opmerking
Wanneer het virus in quarantaine is, kan het geen schade berokkenen, aangezien het niet kan worden uitgevoerd of gelezen.

16.4.1. Bestanden in quarantaine beheren

Om een geselecteerd bestand uit de quarantaine te verwijderen, klikt u op de knop **Verwijderen**. Als u een geselecteerd bestand wilt terugzetten op zijn oorspronkelijke locatie, klikt u op **Herstellen**.

U kan elk geselecteerd bestand van de quarantaine verzenden naar het BitDefender Lab door te klikken op **Verzenden**.

Contextafhankelijk menu. Er is een contextafhankelijk menu beschikbaar waarmee u de bestanden in quarantaine gemakkelijk kan beheren. Dezelfde opties zoals eerder vermeld, zijn beschikbaar. U kan ook **Vernieuwen** selecteren om de quarantainesectie te vernieuwen.

16.4.2. Quarantaine-instellingen configureren

Klik op **Instellingen** om de quarantaine-instellingen te configureren. Een nieuw venster wordt weergegeven.

Quarantaine-instellingen

Met de quarantaine-instellingen, kan u BitDefender instellen om de volgende acties automatisch uit te voeren:

Oude bestanden verwijderen. Om oude bestanden in quarantaine automatisch te verwijderen, schakelt u de overeenkomende optie in. U moet opgeven na hoeveel dagen de bestanden in quarantaine moeten worden verwijderd en de frequentie instellen waarmee BitDefender oude bestanden moet controleren.

Opmerking
BitDefender zal standaard elke dag controleren op oude bestanden en bestanden die ouder zijn dan 30 dagen verwijderen.

Kopieën verwijderen. Om dubbele bestanden in quarantaine automatisch te verwijderen, schakelt u de overeenkomende optie in. U moet het aantal dagen tussen twee opeenvolgende controles op dubbele bestanden opgeven.

Opmerking
Standaar zal BitDefender dagelijks controleren op dubbele bestanden in quarantaine.

Bestanden automatisch verzenden. Om bestanden in quarantaine automatisch te verzenden, schakelt u de overeenkomende optie in. U moet de frequentie waarmee de bestanden worden verzonden, opgeven.

Opmerking
Standaard verzendt BitDefender de bestanden in quarantaine automatisch elke 60 minuten.

Bestanden in quarantaine scannen na update. Om bestanden in quarantaine automatisch te scannen na elke update, schakelt u de overeenkomende optie in. U kan de opgeruimde bestanden automatisch naar hun oorspronkelijke locatie terugplaatsen door het selecteren van **Opgeruimde bestanden herstellen**.

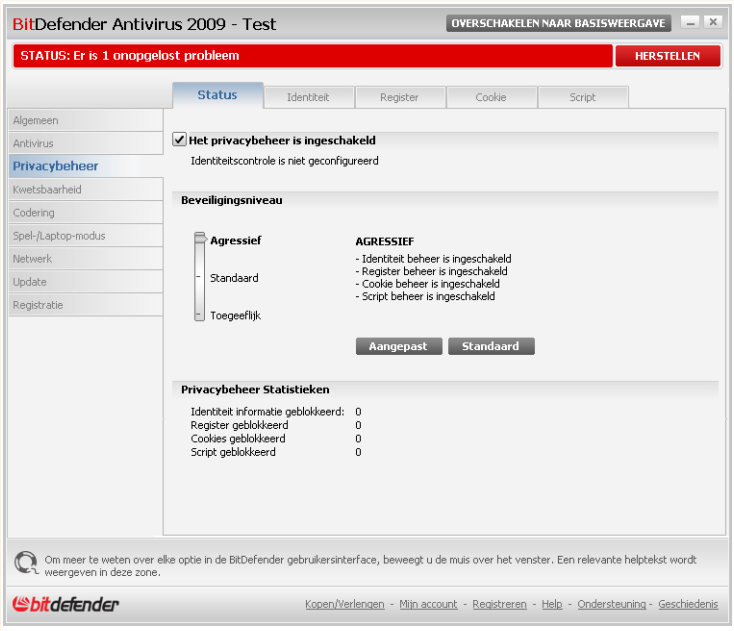
Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

17. Privacybeheer

BitDefender controleert tientallen potentiële "hotspots" in uw systeem waar spyware kan optreden en controleert ook alle wijzigingen van uw systeem en software. Het is bijzonder efficiënt bij het blokkeren van Trojaanse paarden en andere programma's die worden geïnstalleerd door hackers, die proberen uw privacy in gevaar te brengen en uw persoonlijke informatie, zoals kredietkaartnummers, verzenden van uw computer naar de hacker.

17.1. Privacybeheer Statistieken

Om het Privacybeheer te configureren en informatie met betrekking tot zijn activiteit te bekijken, gaat u naar **Privacybeheer>Status** in de Geavanceerde weergave.



Privacybeheer Statistieken

U kan zien of Privacybeheer is ingeschakeld of uitgeschakeld. Als u de status van Privacybeheer wilt veranderen, schakelt u het overeenkomende selectievakje in of uit.

Belangrijk
Om diefstal van data te voorkomen en om uw privacy te beschermen, moet u **Privacybeheer** ingeschakeld houden.

Het Privacybeheer beveiligt uw computer met 5 belangrijke beveiligingselementen:

- Identiteitscontrole - beschermt uw vertrouwelijke gegevens door al het uitgaande webverkeer (HTTP) en e-mailverkeer (SMTP) te filteren volgens de regels die u in de sectie Identiteit hebt gemaakt.
- Registerbeheer - vraagt uw toestemming wanneer een programma probeert een registergegeven te wijzigen om te worden uitgevoerd bij het opstarten van Windows.
- Cookiebeheer - vraagt uw toestemming wanneer een nieuwe website een cookie probeert te plaatsen.
- Scriptbeheer - vraagt uw toestemming wanneer een website een script of andere actieve inhoud probeert te activeren.

Onderaan in de sectie ziet u de **Privacybeheer Statistieken**.

17.1.1. Het beveiligingsniveau configureren

U kunt het beveiligingsniveau kiezen dat beter voldoet aan uw beveiligingsbehoeften. Sleep de schuifregelaar langs de schaal om het geschikte beveiligingsniveau in te stellen.

Er zijn 3 beveiligingsniveaus:

Beveiligingsniveau	Beschrijving
Toegeeflijk	Alleen **Registerbeheer** is ingeschakeld.
Standaard	**Registerbeheer** en **Identiteitcontrole** zijn ingeschakeld.
Agressief	**Registerbeheer**, **Identiteitscontrole** en **Scriptbeheer** zijn ingeschakeld.

U kan het beveiligingsniveau aanpassen door te klikken op **Aangepast niveau**. In het venster dat verschijnt, selecteert u de beveiligingen die u wilt inschakelen en klikt u op **OK**.

Klik op **Standaard** om de schuifregelaar op het standaardniveau in te stellen.

17.2. Identiteitscontrole

Het veilig houden van vertrouwelijke gegevens is een belangrijke kwestie die iedereen aangaat. Gegevensdiefstal is de ontwikkeling van internetcommunicatie gevolgd en maakt gebruik van nieuwe methoden om mensen te misleiden zodat ze persoonlijke gegevens vrijgeven.

Of het nu uw e-mail is of uw creditcardnummer, als deze gegevens in verkeerde handen terechtkomen, kunnen ze u schade berokkenen. U kan worden overspoeld door spamberichten of u kan plotseling voor een onaangename verrassing komen te staan als u ziet dat uw rekening is leeggeplunderd.

Identiteitscontrole beschermt u tegen diefstal van gevoelige data als u online bent. Op basis van de door u gecreëerde regels scant Identiteitscontrole het web, e-mail en instant messaging verkeer dat uw computer verlaat op specifieke tekenreeksen (bijvoorbeeld uw creditcardnummer). Als er een overeenkomst is gevonden, wordt de betreffende webpagina, e-mail of instant message geblokkeerd.

U kan regels creëren voor het beveiligen van elke persoonlijke of vertrouwelijke informatie, van uw telefoonnummer of e-mailadres tot uw bankrekeninginformatie. Er is ondersteuning voorzien voor meerdere gebruikers, zodat andere gebruikers die zich aanmelden bij hun Windowa account hun eigen regels voor de beveiliging kunnen configureren en gebruiken. De regels die u creëert worden alleen toegepast en kunnen alleen worden geopend als u bent aangemeld bij uw Windows account.

Waarom Identiteitscontrole gebruiken?

- Identiteitscontrole blokkeert toetsenbord spyware bijzonder effectief. Dit type van kwaadwillende applicaties noteert uw toetsaanslagen en zendt deze via het Internet naar een kwaadwillend persoon (hacker). De hacker kan gevoelige informatie uit de gestolen data halen, zoals bankrekeningnummers en wachtwoorden, en deze voor zijn eigen doeleinden gebruiken.

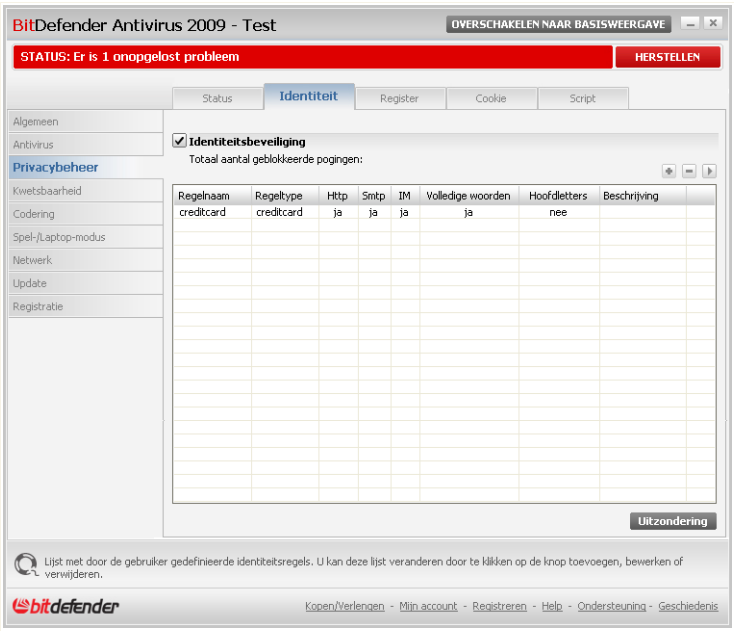
  In he geval dat zo'n applicatie erin slaagt om door de antivirusdetectie te glippen, kan het de gestolen data niet verzenden via e-mail, web of instant messages als u de juiste identiteitscontroleregels hebt gecreëerd.

- Identiteitscontrole kan u beschermen tegen phishing pogingen (pogingen tot diefstal van persoonlijke informatie). De meeste phishing pogingen maken gebruik van een misleidende e-mail om u te verleiden uw persoonlijke informatie in te vullen op een nep webpagina.

Bijvoorbeeld, u ontvangt een e-mail die zegt afkomstig te zijn van uw bank en waarin wordt gevraagd om zo snel mogelijk u bankrekeninginformatie te vernieuwen. In de e-mail staat een link naar de webpagina waar u uw persoonlijke informatie moet invullen. Hoewel de e-mail en de webpagina waar de misleidende link u naartoe brengt er echt uitzien, zijn zij dat niet. Als u klikt op de link in de e-mail en uw persoonlijke informatie invult op de nep webpagina, geeft u deze informatie aan de kwaadwillende personen die achter de phishing poging zitten.

Als de juiste regels voor de identiteitsbescherming zijn ingesteld, kan u geen persoonlijke informatie (zoals uw creditcardnummer) op een webpagina verzenden, tenzij u nadrukkelijk een uitzondering hebt gemaakt voor de betreffende webpagina.

Om Identiteitscontrole te configureren, gaat u naar **Privacybeheer>Identiteit** in de Geavanceerde weergave.



Identiteitscontrole

Volg deze stappen als u Identiteitscontrole wilt gebruiken:

1. Selecteer het vakje **Identiteitscontrole** .
2. Creëer regels om uw gevoelige data te beschermen. Meer informatie vindt u onder "*Privacyregels maken*" (p. 144).
3. Definieer indien nodig specifieke uitzonderingen op de door u gecreëerde regels. Meer informatie vindt u onder "*Uitzonderingen definiëren*" (p. 147).

17.2.1. Privacyregels maken

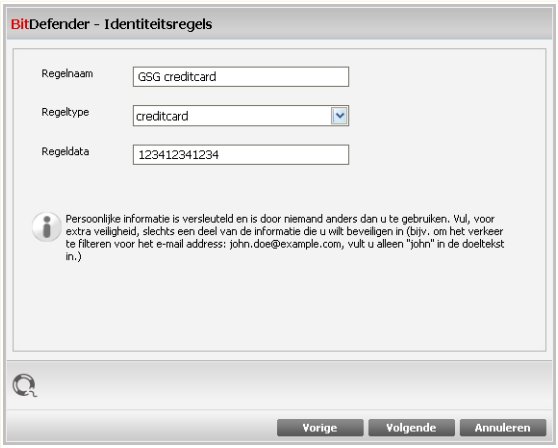
Om een identiteitcontroleregel te maken, klikt u op de knop **Toevoegen** en volgt u de configuratiewizard.

Stap 1/4 - Welkomstvenster

Welkomstvenster

Klik op **Volgende**.

Stap 2/4 - Type en gegevens van de regel instellen



Type en gegevens van de regel instellen

U moet de volgende parameters instellen:

- **Regelnaam** - voer de naam van de regel in dit bewerkingsveld in.
- **Regeltype** - kies het type regel (adres, naam, creditcard, PIN, BSN, enz.).
- **Regeldata** - voer de te beveiligen data in dit bewerkingsveld in. Bijvoorbeeld, als u uw credicardnummer wilt beveiligen, voer het dan hier in zijn geheel of gedeeltelijk in

> ***Opmerking***
> Als u minder dan drie tekens invoert, wordt u gevraagd de gegevens te valideren. Wij raden u aan minstens drie tekens in te voeren om te vermijden dat berichten en webpagina's ten onrechte worden geblokkeerd.

Alle gegevens die u invoert, worden gecrypteerd. Voor extra veiligheid adviseren wij van de gegevens die u wilt beschermen niet alles in tevoeren.

Klik op **Volgende**.

Stap 3/4 - Verkeer selecteren

Verkeer selecteren

Selecteer het type verkeer dat u door BitDefender wilt laten scannen. De volgende opties zijn beschikbaar:

- **HTTP scannen** - scant het HTTP-verkeer (web) en blokkeert de uitgaande data die overeenkomt met de regeldata.
- **SMTP scannen** - scant het SMTP-verkeer (mail) en blokkeert de uitgaande e-mailberichten die de regeldata bevatten.
- **Instant Messaging scannen** - scant het Instant Messaging verkeer en blokkeert de uitgaande chatberichten die de regeldata bevatten.

U kunt ervoor kiezen de regels alleen toe te passen als de regeldata overeenkomen met volledige woorden of als de regeldata en de gedetecteerde tekenreeks overeenkomen.

Klik op **Volgende**.

Stap 4/4 - Regel beschrijven

Regel beschrijven

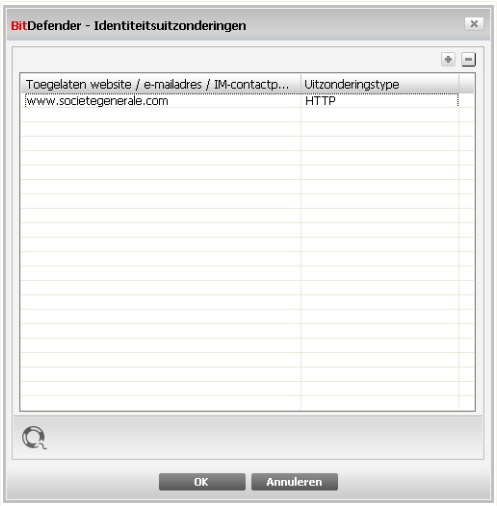
Voer een korte beschrijving in van de regel in het bewerkingsveld. Omdat de geblokkeerde data (tekenreeks) niet in normale tekst zichtbaar is als u de regel opent, kan u deze met de beschrijving beter herkennen.

Klik op **Voltooien**. De regels worden weergegeven in de tabel.

17.2.2. Uitzonderingen definiëren

Er zijn situaties waarin u uitzonderingen op specifieke identiteitsregels moet definiëren. Laten we even een situatie bekijken waarbij u een regel hebt gemaakt die verhindert dat uw creditcardnummer via HTTP (het web) wordt verzonden. Telkens wanneer uw creditcardnummer vanaf uw gebruikersaccount naar een website wordt verzonden, wordt de desbetreffende pagina geblokkeerd. Als u bijvoorbeeld schoenen wilt kopen in een online winkel (waarvan u zeker bent dat deze veilig is), moet u een uitzondering op de desbetreffende regel opgeven.

Klik op **Uitzonderingen** om het venster te openen waarin u de uitzonderingen kunt beheren.



Uitzonderingen

Volg deze stappen om een uitzondering toe te voegen:

1. Klik op **Toevoegen** om een nieuw gegeven in de tabel toe te voegen.
2. Dubbelklik op **Toegelaten adres opgeven** en geef het webadres, het e-mailadres of het IM contact op dat u wilt toevoegen als uitzondering.
3. Dubbelklik op **Type kiezen** en selecteer de optie die overeenkomt met het eerder opgegeven adrestype in het menu.
   - Selecteer **HTTP** als u een webadres hebt opgegeven.
   - Selecteer **SMTP** als u een e-mailadres hebt opgegeven.
   - Selecteer **IM** als u een Im contact hebt opgegeven.

Om een uitzondering uit de lijst te verwijderen, selecteert u deze en klikt u op **Verwijderen**.

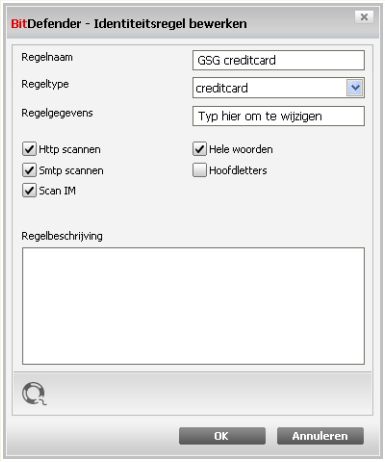
Klik op **OK** om de wijzigingen op te slaan.

17.2.3. Regels beheren

De regels die tot nu toe zijn gemaakt, worden weergegeven in de tabel.

Om een regel te verwijderen, selecteert u deze en klikt u op de knop **Verwijderen**.

Om een regel te bewerken, selecteert u deze en klikt u op de knop **Bewerken** of dubbelklikt u erop. Een nieuw venster verschijnt.



Regel bewerken

Hier kan u de naam, de beschrijving en de parameters (type, gegevens en verkeer) van de regel wijzigen. Klik op **OK** om de wijzigingen op te slaan.

17.3. Registerbeheer

Een bijzonder belangrijk onderdeel van het Windows-besturingssysteem wordt het **Register** genoemd. Dit is de plaats waar Windows zijn instellingen, geïnstalleerde programma's, gebruikersinformatie enzovoort bijhoudt.

Het **Register** wordt ook gebruikt om te definiëren welke programma's automatisch moeten worden gestart wanneer Windows wordt gestart. Virussen maken er dan ook vaak gebruik van om automatisch te worden geactiveerd, zodra de gebruiker zijn computer opnieuw opstart.

Het **Registerbeheer** houdt de gebeurtenissen in het Windows register in het oog. Hierdoor is het ook een nuttig middel om Trojaanse paarden te detecteren. U wordt gewaarschuwd zodra een programma probeert een registergegeven te wijzigen, zodat het wordt uitgevoerd bij het opstarten van Windows.

Registerwaarschuwing

U ziet het programma dat probeert het Windows register te wijzigen.

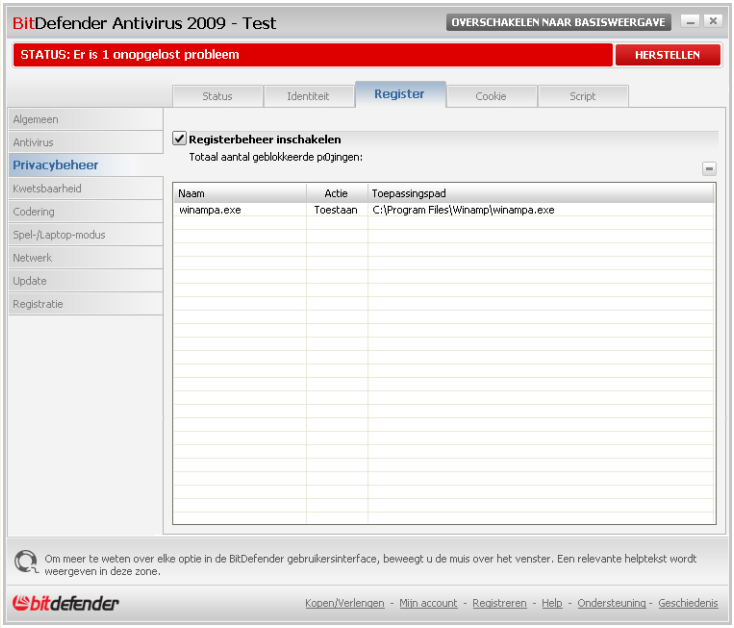
Ale u het programma niet herkent en het verdacht lijkt, klik dan op **Blokkeren** om te voorkomen dat het Windows register wijzigt. Klik anders op **Toestaan** om de wijziging toe te laten.

Afhankelijk van uw antwoord, wordt een regels gemaakt en weergegeven in de tabel met regels. Dezelfde actie wordt telkens toegepast wanneer dit programma een registergegeven probeert te wijzigen.

Opmerking

BitDefender zal u doorgaans waarschuwen wanneer u nieuwe programma's installeert die moeten worden uitgevoerd nadat u de computer de volgende keer opstart. In de meeste gevallen zijn deze programma's rechtmatig en kunnen ze worden vertrouwd.

Om het Registerbeheer te configureren, gaat u naar **Privacy Control>Registry** in de Geavanceerde weergave.



Registerbeheer

De regels die tot nu toe zijn gemaakt, worden weergegeven in de tabel.

Om een regel te verwijderen, selecteert u deze en klikt u op de knop **Verwijderen**.

17.4. Cookiebeheer

Cookies zijn een bijzonder gangbaar fenomeen op het Internet. Het zijn kleine bestanden die op uw computer worden opgeslagen. Websites maken deze cookies om specifieke informatie over u bij te houden.

Cookies zijn meestal ontwikkeld om u het leven te vergemakkelijken. Ze kunnen de website bijvoorbeeld helpen uw naam en voorkeuren te onthouden, zodat u ze niet telkens opnieuw moet invoeren wanneer u de site bezoekt.

Cookies kunnen echter ook worden gebruikt om uw privacy in gevaar te brengen door de patronen van uw surfgedrag op te sporen.

Dit is waar het **Cookiebeheer** ingrijpt. Wanneer u het **Cookiebeheer** inschakelt, zal het telkens uw toestemming vragen wanneer een nieuwe website een cookie probeert te plaatsen:

Cookie waarschuwing

U ziet de naam van de toepassing die u probeert het cookiebestand te zenden.

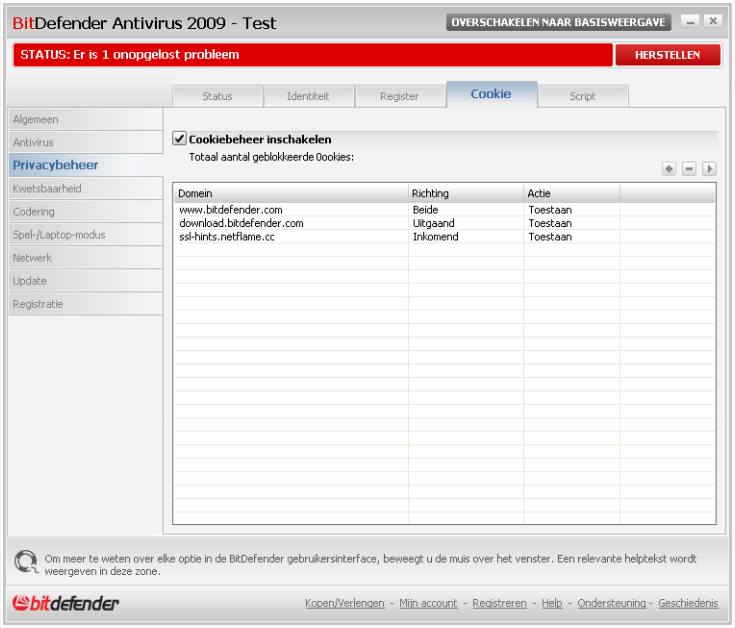
Schakel de optie **Dit antwoord onthouden** in en klik op **Ja** of **Nee**. Een regel wordt gemaakt, toegepast en weergegeven in de tabel met regels. U zult niet langer op de hoogte worden gebracht wanneer u de volgende keer een verbinding maakt met dezelfde site.

Dit helpt bij het kiezen van de websites die u wel of niet vertrouwt.

Opmerking

Gezien het grote aantal cookies dat tegenwoordig op het Internet wordt gebruikt, kan het **Cookiebeheer** aanvankelijk nogal hinderlijk zijn. Het zal u eerst veel vragen stellen over sites die proberen cookies te plaatsen op uw computer. Zodra u uw gebruikelijke sites toevoegt aan de regellijst, zult u opnieuw even gemakkelijk kunnen surfen als voorheen.

Om het Cookiebeheer te configureren, gat u naar **Privacybeheer>Cookie** in de Geavanceerde weergave.



Cookiebeheer

De regels die tot nu toe zijn gemaakt, worden weergegeven in de tabel.

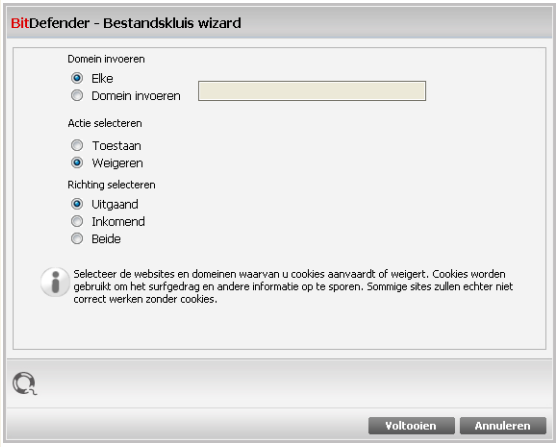
Belangrijk
De regels worden vanaf boven weergegeven in volgorde van prioriteit, wat betekent dat de eerste regel de hoogste prioriteit heeft. U kunt de regels slepen & neerzetten om hun prioriteit te wijzigen.

Om een regel te verwijderen, selecteert u deze en klikt u op de knop **Verwijderen**. Om de parameters van de regel te wijzigen, dubbelklikt u op de regel en maakt u de veranderingen in het configuratievenster.

Om handmatig een regel toe te voegen, klikt u op de knop **Toevoegen** en configureert u de parameters van de regel in het configuratievenster.

17.4.1. Configuratievenster

Als u handmatig een regel bewerkt of toevoegt, verschijnt het configuratievenster.



Adres, actie en richting selecteren

U kunt de volgende parameters instellen:

- **Domeinadres** - voer het domein in waarop de regel moet worden toegepast.
- **Actie** - selecteer de actie van de regel.

Actie	*Beschrijving*
Toestaan	De cookies op dat domein zullen worden uitgevoerd.
Weigeren	De cookies op dat domein zullen niet worden uitgevoerd.

- **Richting** - selecteer de richting voor het verkeer.

Type	*Beschrijving*
Uitgaand	De regel zal alleen worden toegepast op cookies die worden teruggezonden naar de verbonden site.
Binnenkomend	De regel zal alleen worden toegepast op cookies die worden ontvangen van de verbonden site.
Beide	De regel zal in beide richtingen worden toegepast.

Opmerking
U kunt cookies aanvaarden, maar ze nooit terugsturen. Stel hiervoor de actie in op **Weigeren** en de richting op **Uitgaand**.

Klik op **Voltooien**.

17.5. Scriptbeheer

Scripts en andere codes, zoals ActiveX-besturingselementen en Java-applets, die worden gebruikt om interactieve webpagina's te maken, kunnen worden geprogrammeerd om schadelijke effecten te veroorzaken. ActiveX-elementen kunnen bijvoorbeeld de volledige toegang verkrijgen tot uw gegevens en kunnen gegevens lezen van uw computer, informatie verwijderen, wachtwoorden overnemen en berichten onderscheppen terwijl u on line bent. Wij raden u dan ook aan alleen actieve inhoud te aanvaarden van sites die u volledig kent en vertrouwt.

Met BitDefender kunt u beslissen of u deze elementen wilt uitvoeren of als u het uitvoeren wilt blokkeren.

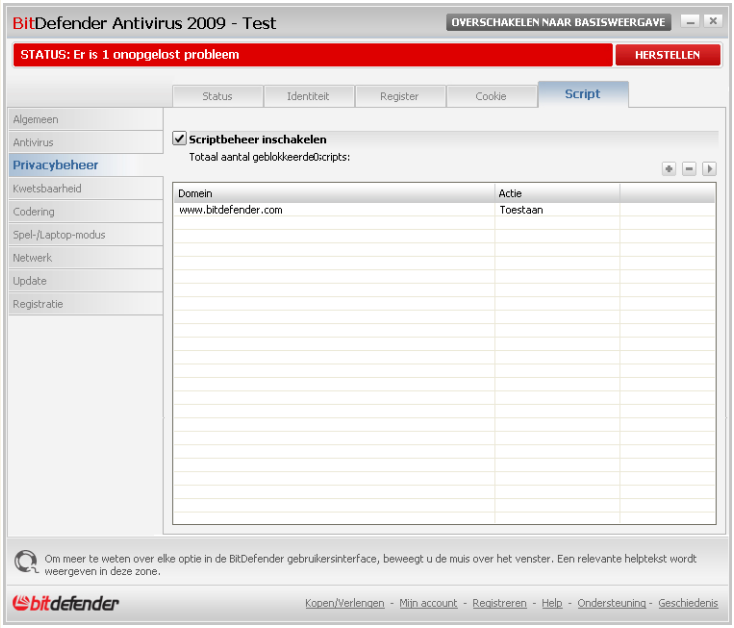
Met het **Scriptbeheer** bepaalt u zelf welke websites u vertrouwt en welke niet. BitDefender zal telkens uw toestemming vragen wanneer een website een script of andere actieve inhoud probeert te activeren.

Script waarschuwing

De naam van de bron wordt weergegeven.

Schakel de optie **Dit antwoord onthouden** in en klik op **Ja** of **Nee**. Een regel wordt gemaakt, toegepast en weergegeven in de tabel met regels. U wordt niet langer op de hoogte gebracht wanneer dezelfde site probeert u actieve inhoud te zenden.

Om Scriptbeheer te configureren, gaat u naar **Privacy Control>Script** in de Geavanceerde weergave.



Scriptbeheer

De regels die tot nu toe zijn gemaakt, worden weergegeven in de tabel.

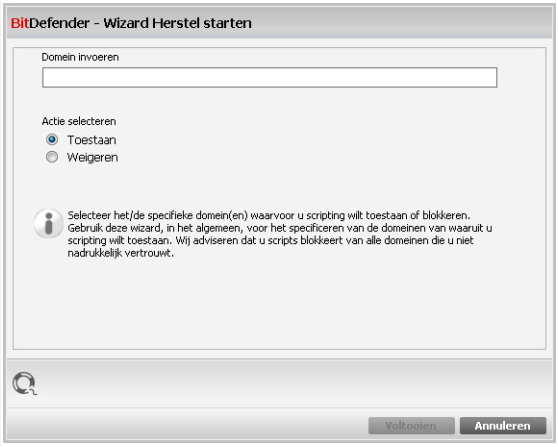
Belangrijk
De regels worden vanaf boven weergegeven in volgorde van prioriteit, wat betekent dat de eerste regel de hoogste prioriteit heeft. U kunt de regels slepen & neerzetten om hun prioriteit te wijzigen.

Om een regel te verwijderen, selecteert u deze en klikt u op de knop **Verwijderen**. Om de parameters van de regel te wijzigen, dubbelklikt u op de regel en maakt u de veranderingen in het configuratievenster.

Om handmatig een regel te creëren, klikt u op de knop **Toevoegen** en configureert u de parameters van de regel in het configuratievenster.

17.5.1. Configuratievenster

Als u handmatig een regel bewerkt of toevoegt, verschijnt het configuratievenster.



Adres en actie selecteren

U kunt de volgende parameters instellen:

- **Domeinadres** - voer het domein in waarop de regel moet worden toegepast.
- **Actie** - selecteer de actie van de regel.

Actie	*Beschrijving*
Toestaan	De scripts op dat domein zullen worden uitgevoerd.
Weigeren	De scripts op dat domein zullen niet worden uitgevoerd.

Klik op **Voltooien**.

18. Instant Messaging (IM) encryptie

Standaard crypteert BitDefender al uw instant messaging chatsessies, op voorwaarde dat:

- uw chatpartner een BitDefender-versie heeft geïnstalleerd die IM Encryptie ondersteunt en IM Encryption is ingeschakeld voor de instant messaging applicatie die bij het chatten wordt gebruikt.
- U en uw chatpartner gebruiken ofwel Yahoo Messenger of Windows Live (MSN) Messenger.

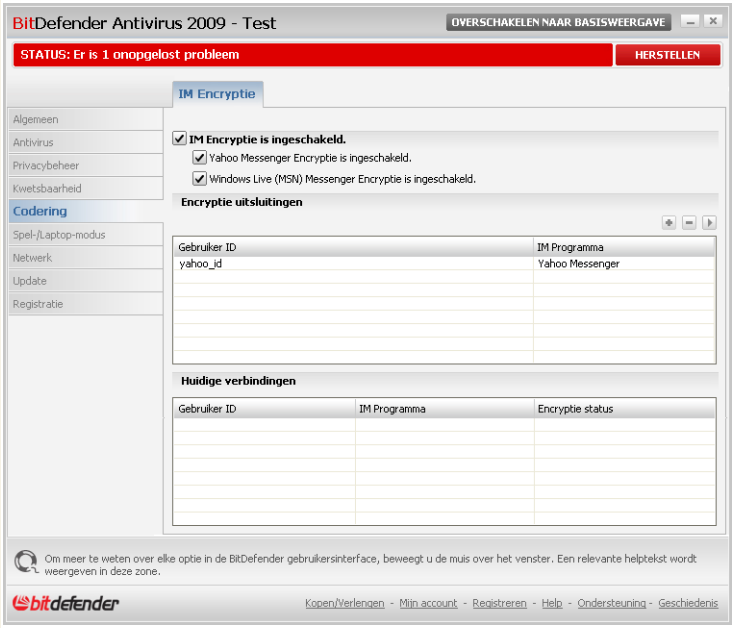
Belangrijk

BitDefender crypteert een gesprek niet als een chatpartner een webgebaseerde chatapplicatie gebruikt, zoals Meebo, of en andere chatapplicatie die Yahoo Messenger of MSN ondersteunt.

Om instant messaging encryptie te configureren, gaat u naar **Encryption>IM Encryption** in de Geavanceerde weergave.

Opmerking

U kan instant messaging encryptie gemakkelijk configureren met de BitDefender werkbalk in het chatvenster. Meer informatie vindt u onder "*Integratie in Messenger*" (p. 36).



Instant Messaging beheer

Standaard is IM encryptie ingeschakleld voor zowel Yahoo Messenger en Windows Live (MSN) Messenger. U kan kiezen IM encryptie compleet of alleen voor een specifieke chat-applicatie uit te schakelen.

Er worden twee tabellen weergegeven:

- **Encryptie uitzonderingen** - geeft de lijst van gebruiker-ID's en het bijbehorende IM programma waarvoor encryptie is uitgeschakeld. Om een contact uit de lijst te verwijderen, selecteert u deze en klikt u op de knop **Verwijderen**.
- **Huidige verbindingen** - geeft de lijst van huidige instant messaging verbindingen (gebruiker-ID en bijbehorend IM programma) en of deze gecrypteerd zijn of niet. Een verbinding kan niet gecrypteerd zijn om deze redenen:
  - U hebt encryption voor het betreffende contact uitgeschakeld.
  - Uw contact heeft geen BitDefender versie geïnstalleerd die IM encryptie ondersteunt.

18.1. Encryptie uitschakelen voor specifieke gebruikers

Volg deze stappen om encryptie voor een specifieke gebruiker uit te schakelen:

1. Klik op de knop **Toevoegen** om het configuratievenster te openen.

Contacten toevoegen

2. Typ het gebruiker-ID van uw contact in het bewerkingsveld.
3. Selecteer de instant messaging applicatie die behoort bij het contact.
4. Klik op **OK**.

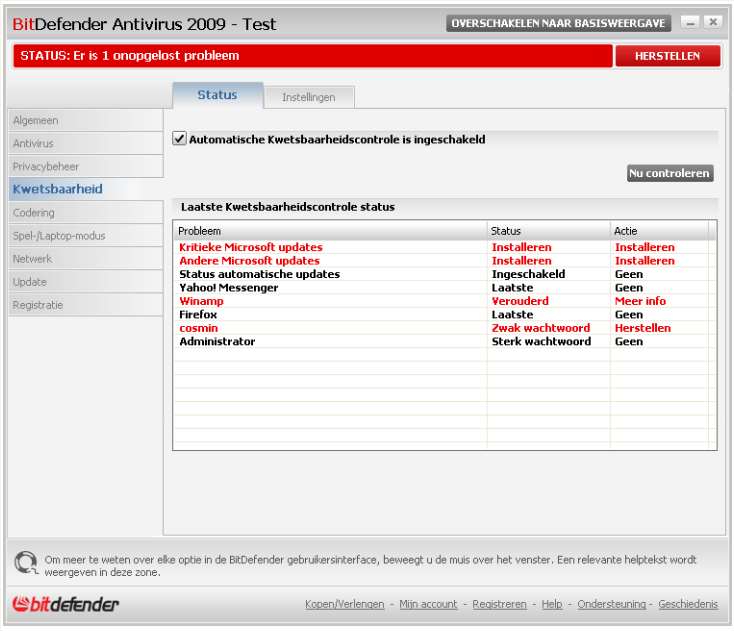
19. Kwetsbaarheid

Een belangrijke stap bij het beschermen van uw computer tegen kwaadwillende personen en applicaties is het up-to-date houden van het besturingssysteem en van de applicaties die u regelmatig gebruikt. Bovendien moeten, om onbevoegden de toegang tot uw computer te ontzeggen, sterke wachtwoorden (wachtwoorden die moeilijk te raden zijn) voor elke Windows gebruikersaccount zijn geconfigureerd.

BitDefender controleert uw systeem regelmatig op kwetsbaarheden en waarschuwt u voor de bestaande problemen.

19.1. Status

Om de automatische kwetsbaarheidcontrole te configureren of om een kwetsbaarheidscontrole uit te voeren, gaat u naar **Vulnerability>Status** in de Geavanceerde weergave.



Kwetsbaarheidsscan

De tabel toont de problemen die werden aangepakt bij de laatste controle op kwetsbaarheden en hun status; U kunt zien welke actie u moet ondernemen om elk zwak punt, als dat er al is, uit te schakelen. Als de actie **Geen** is, staat het respectieve probleem niet voor een zwak punt.

Belangrijk
Houd **Automatische kwetsbaarheidscontrole** ingeschakeld om automatisch te worden gewaarschuwd voor kwetsbaarheden in het systeem of in applicaties.

19.1.1. Zwakke punten verwijderen

Om een specifiek zwak punt te herstellen, dubbelklikt u erop en gaat u, afhankelijk van het probleem, als volgt te werk:

- Als er Windows-updates beschikbaar zijn, klikt u op **Alle systeemupdates installeren** om ze te installeren.
- Als een toepassing verouderd is, kunt u de koppeling **Startpagina** gebruiken om de nieuwste versie van die toepassing te downloaden en te installeren.
- Als een Windows-gebruikersaccount een zwak wachtwoord heeft, wordt de gebruiker geforceerd het wachtwoord te wijzigen bij de volgende aanmelding of moet u het wachtwoord zelf wijzigen.

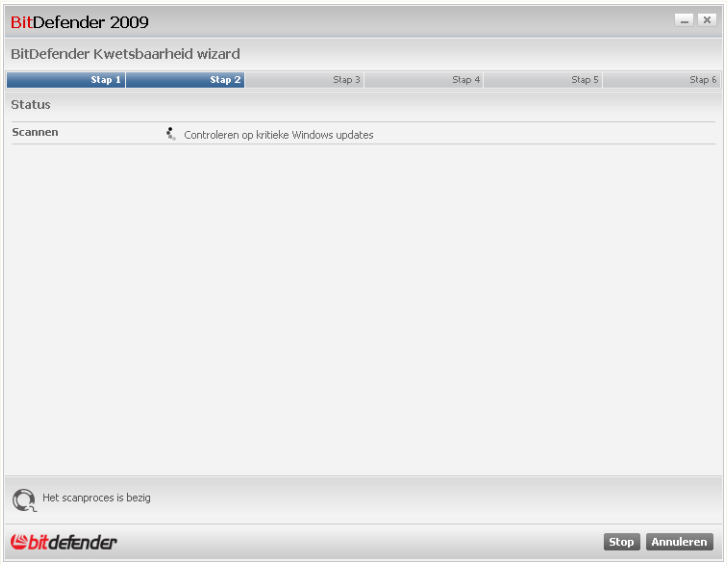
U kunt op **Nu controleren** klikken en de wizard volgen om de zwakke punten stapsgewijs uit te schakelen.

Stap 1/6 - Te controleren kwetsbaarheden selecteren

Kwetsbaarheden

Klik op **Volgende** om het systeem op de geselecteerde kwetsbaarheden te controleren.

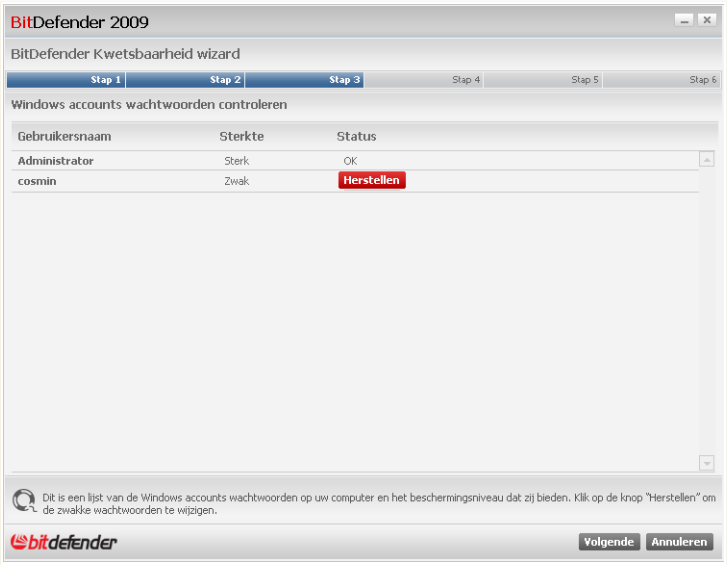
Stap 2/6 - Op kwetsbaarheden controleren



Kwetsbaarheidscontrole

Wacht tot BitDefender de kwetsbaarheidscontrole heeft voltooid.

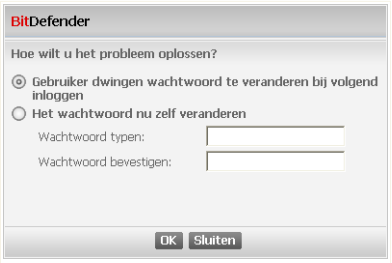
Stap 3/6 - Zwakke wachtwoorden veranderen



Gebruikers wachtwoord

U ziet de lijst van Windows gebruikersaccounts die zijn geconfigureerd op uw computer en de beschermingsniveaus van de wachtwoorden.

Klik op **Herstellen** om de zwakke wachtwoorden te wijzigen. Een nieuw venster wordt weergegeven.



Wachtwoord veranderen

Selecteer de methode voor het herstellen van dit probleem:

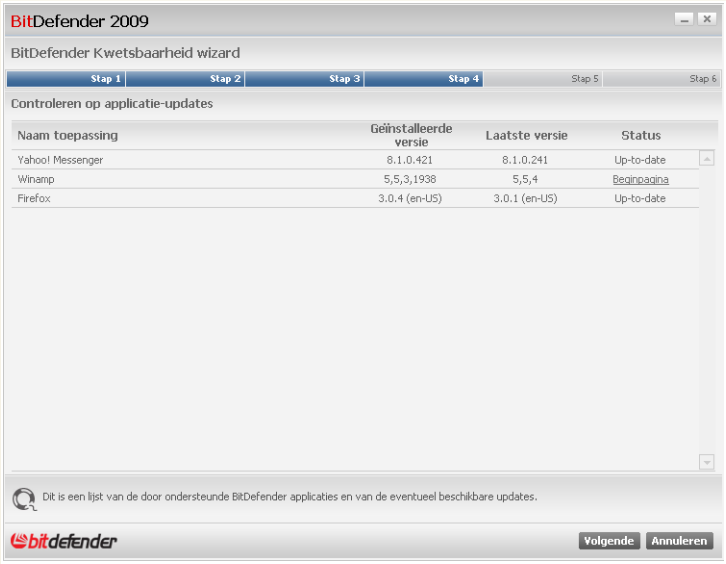
- **Gebruiker dwingen wachtwoord te veranderen bij volgend inloggen.** BitDefender vraagt de gebruiker het wachtwoord te veranderen als hij zich de volgende keer aanmeldt bij Windows.
- **Gebruikerswachtwoord veranderen.** U moet het nieuwe wachtwoord in de overeenkomende velden invoeren.

> ***Opmerking***
> Voor een sterk wachtwoord gebruikt u een combinatie van hoofdletters en kleine letters, getallen en speciale tekens (zoals #, $ of @).

Klik op **OK** om het wachtwoord op te slaan.

Klik op **Volgende**.

Stap 4/6 - Applicaties updaten

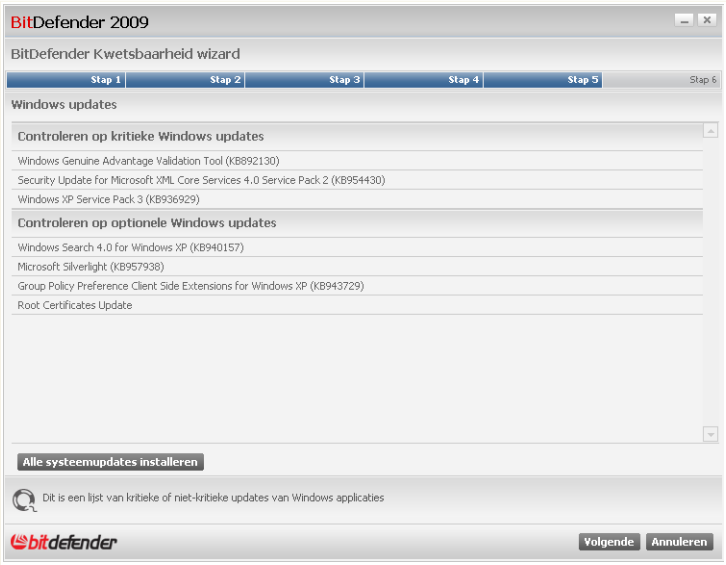


Applicaties

U kan de lijst zien van de applicaties die door BitDefender worden gecontroleerd en of zij up-to-date zijn. Als een applicatie niet up-to-date is, klik dan op de getoonde link om de laatste versie te downloaden.

Klik op **Volgende**.

Stap 5/6 – Windows updaten



Windows updates

U ziet de lijst van kritieke en niet-kritieke Windows updates die niet zijn geïnstalleerd op uw computer. Klik op **Alle systeemupdates installeren** om alle beschikbare producten te installeren.

Klik op **Volgende**.

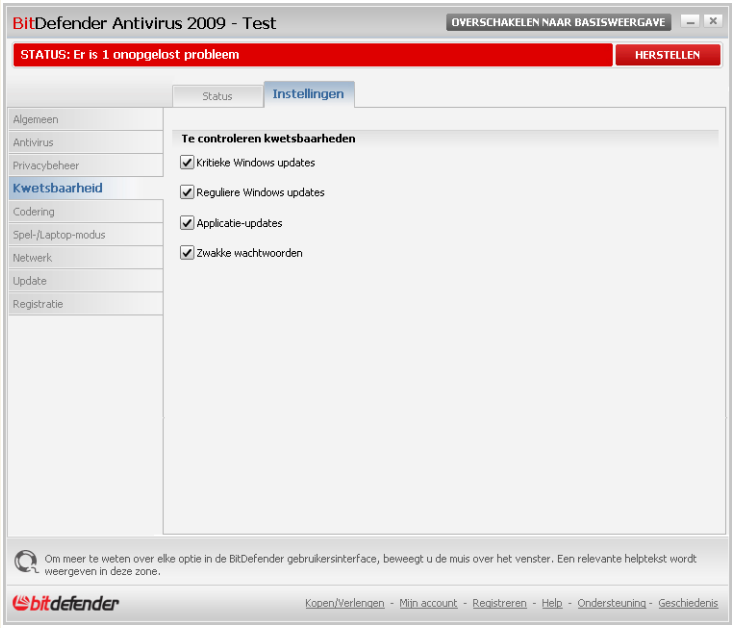
Stap 6/6 - Resultaten weergeven

Resultaten

Klik op **Sluiten**.

19.2. Instellingen

Om de instellingen van de automatische kwetsbaarheidscontrole te configureren, gaat u naar **Kwetsbaarheid>Instellingen** in de Geavanceerde weergave.



Automatische kwetsbaarheidscontrole instellingen

Selecteer de vakjes voor de kwetsbaarheden van het systeem die u regelmatig wilt laten controleren.

- **Kritieke Microsoft updates**
- **Normale Microsoft updates**
- **Zwakke wachtwoorden**
- **Toepassing-updates**

Opmerking
Als u het vakje voor een specifieke kwetsbaarheid leeg maakt, waarschuwt BitDefender niet langer voor de betreffende problemen.

20. Spel- / Laptop-modus

Met de Spel- / Laptop-modus module kan u de speciale werkingsmodi van BitDefender configureren:

- Spelmodus verandert tijdelijk de beveiligingsinstellingen om de snelheid van het systeem zo weinig mogelijk te beïnvloeden.
- Laptop-modus voorkomt dat geprogrammeerde taken worden uitgevoerd als de laptop op de accu werkt om het stroomverbruik te sparen.

20.1. Spelmodus

De Spelmodus verandert tijdelijk de beveiligingsinstellingen om de snelheid van het systeem zo weinig mogelijk te beïnvloeden. Als u in de Spelmodus bent, worden de volgende instellingen toegepast:

- Alle BitDefender waarschuwingen en pop-ups zijn uitgeschakeld.
- Het BitDefender real-time beschermingsniveau is ingesteld op **Toegeeflijk**.
- Updates worden niet standaard uitgevoerd.

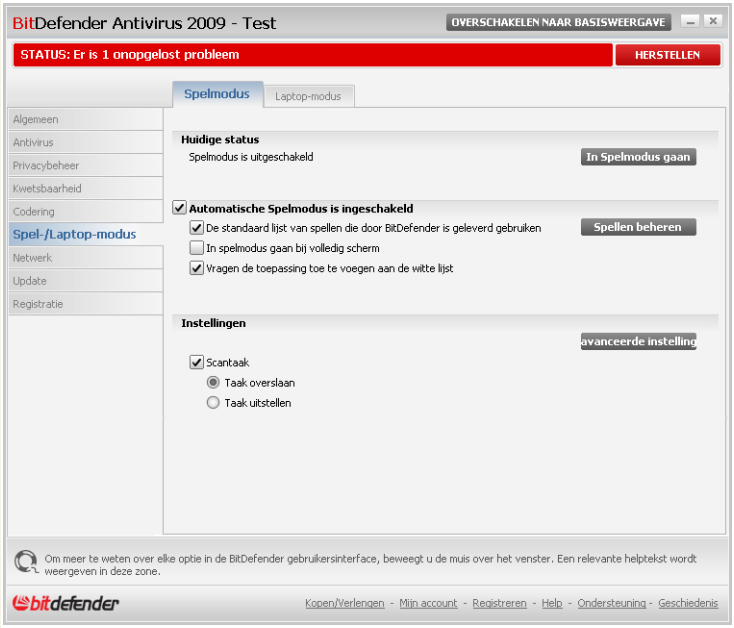
> ***Opmerking***
> Om deze instelling te veranderen, gaat u naar Update>Instellingen en maakt u het vakje **Geen update uitvoeren wanneer de Spelmodus is ingeschakeld** leeg.

- Geprogrammeerde scantaken zijn standaard uitgeschakeld.

Standaard gaat BitDefender automatisch in de Spelmodus als u een spel start uit de lijst van BitDefender's bekende spelen of als een applicatie overgaat op volledig scherm. U kan de Spelmodus handmatig inschakelen met de standaard sneltoets `Ctrl+Alt+Shift+G`. Wij adviseren krachtig de Spelmodus uit te schakelen als u bent uitgespeeld (gerbuik dezelfde standaard sneltoets `Ctrl+Alt+Shift+G`).

> ***Opmerking***
> Als de Spelmodus is ingeschakeld, ziet u de letter `G` boven het BitDefender-pictogram.

Om de Spelmodus te configureren, gaat u naar **Spel-/laptopmodus>Spelmodus** in de Geavanceerde weergave.



Spelmodus

Aan de bovenkant van de sectie kan u de status van de Spelmodus zien. Klik op **In spelmodus gaan** of **Spelmodus afsluiten** om de huidige status te veranderen.

20.1.1. Automatische Spelmodus configureren

Met Automatische Spelmodus kan BitDefender automatisch in de Spelmodus gaan wanneer een spel is gedetecteerd. U kan de volgende opties configureren:

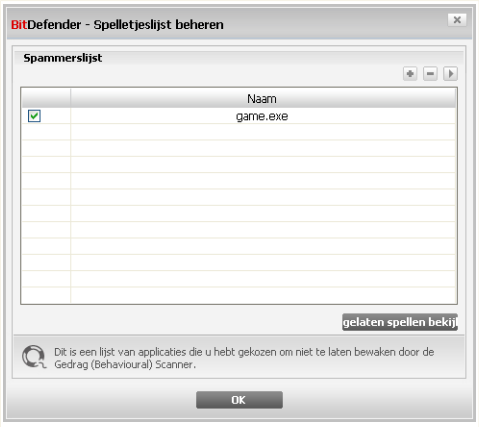
- **De standaard lijst van spellen die door BitDefender is geleverd gebruiken** - Spelmodus wordt automatisch ingeschakeld als u een spel start dat voorkomt in de lijst van BitDefender's bekende spelen. Om deze lijst te zien, klikt u op **Spellen beheren** en dan op **Toegelaten spellen bekijken**.
- **Spelmodus inschakelen bij volledig scherm** - Spelmodus wordt automatisch ingeschakeld als een applicatie overgaat op volledig scherm.

- **Applicatie toevoegen aan de spellenlijst?** - om gevraagd te worden een nieuwe applicatie toe te voegen aan de spellenlijst als u het volledige schem verlaat. Door een nieuwe applicatie toe te voegen an de spellenlijst, gaat BitDefender automatisch in de Spelmodus als u de applicatie de volgende keer start.

Opmerking
Als u niet wilt dat BitDefender automatisch in de Spelmodus gaat, maak dan het selectievakje **Automatische Spelmodus** leeg.

20.1.2. De spellenlijst beheren

BitDefender gaat automatisch in de Spelmodus als u een applicatie uit de spellenlijst start. Om de spellenlijst te bekijken en te beheren, klikt u op **Spellen beheren**. Een nieuw venster wordt weergegeven.



Spellenlijst

Nieuwe applicaties worden automatisch toegevoegd aan de lijst als:

- U een spel start uit de BitDefender's lijst van bekende spellen. Om deze lijst te zien, klikt u op **Toegelaten spellen bekijken**.
- Na het verlaten van het volledige scherm, voegt u de applicatie toe aan de spellenlijst vanuit het vraagvenster.

Als u de Automatische Spelmodus wilt uitschakelen voor een specifieke applicatie uit de lijst, schakelt u het overeenkomende selectievakje uit. Schakel de Automatische Spelmodus uit voor applicatie die normaal in volledig scherm werken, zoals webbrowsers en filmspelers.

Om de spellenlijst te beheren, kan u de knoppen aan de bovenkant van de tabel gebruiken:

- **Toevoegen** - hiermee voegt u een nieuwe toepassing toe aan de lijst met spelletjes.
- **Verwijderen** - hiermee verwijdert u een toepassing uit de lijst met spelletjes.
- **Bewerken** - hiermee bewerkt u een bestaand gegeven in de lijst met spelletjes.

Spellen toevoegen of bewerken

Als u een spel in de spellenlijst toevoegt of bewerkt, verschijnt het volgende venster:

Spel toevoegen

Klik op **Bladeren** om de applicatie te selecteren of typ het complete pad naar de applicatie in het bewerkingsveld.

Als u niet automatisch in de Spelmodus wilt gaan als de geselecteerde applicatie wordt gestart, selecteert u **Uitschakelen**.

Klik op **OK** om de invoer toe te voegen aan de spellenlijst.

20.1.3. Spelmodus instellingen configureren

Gebruik deze opties om het gedrag voor geprogrammeerde taken te configureren:

- **Scantaken** - om te voorkomen dat een scantaak wordt uitgevoerd in de Spelmodus. U kan een van de volgende opties kiezen:

Optie	Beschrijving
Taak overslaan	De geprogrammeerde taak wordt helemaal niet uitgevoerd.
Taak uitstellen	De taak wordt uitgevoerd zodra u de Spelmodus verlaat.

20.1.4. Veranderen van de Spelmodus sneltoets

U kan de Spelmodus handmatig inschakelen met de standaard sneltoets `Ctrl+Alt+Shift+G`. Volg deze stappen als u de sneltoets wilt veranderen:

1. Klik op **Geavanceerde instellingen**. Een nieuw venster wordt weergegeven.

Geavanceerde instellingen

2. Stel de gewenste sneltoets in onder de **Sneltoets gebruiken** optie:
   - Kies de gewijzigde toetsen die u wilt gebruiken door één van de volgende aan te kruisen: Control toets (`Ctrl`), Shift toets (`Shift`) of Alternate toets (`Alt`).
   - Typ in het invulveld de letter van de normale toets die u wilt gebruiken.

   Bijvoorbeeld, als u de `Ctrl+Alt+D` sneltoets wilt gebruiken, kruist u `Ctrl` en `Alt` aan en typt u `D`.
3. Klik op **OK** om de wijzigingen op te slaan.

Opmerking
Door het kruisje naast **Sneltoets gebruiken** te verwijderen, schakelt u de sneltoets uit.

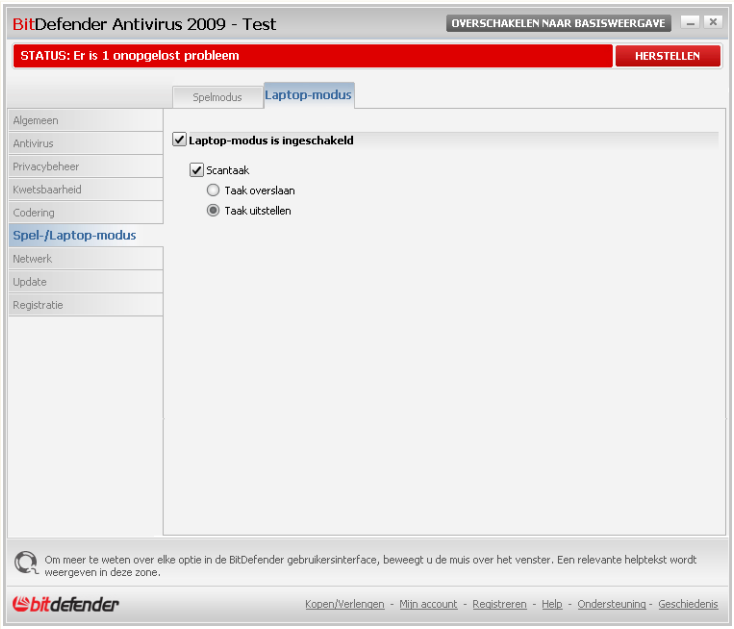
20.2. Laptop-modus

De Laptop-modus is speciaal bestemd voor laptop en notebook gebruikers. Het doel is dat BitDefender een zo klein mogelijke invloed op het stroomverbruik heeft als deze apparaten op de accu werken.

In de Laptop-modus worden geprogrammeerde taken standaard niet uitgevoerd.

BitDefender detecteert wanneer uw laptop overschakelt op accuvoeding en gaat automatisch in de Laptop-modus. Op dezelfde manier verlaat BitDefender automatisch de Laptop-modus, als de laptop niet langer op de accu werkt.

Om de Laptopmodus te configureren, gaat u naar **Spel/laptopmodus>Laptopmodus** in de Geavanceerde weergave.



Laptop-modus

U kan zien of de Laptop-modus is ingeschakeld of niet. Als de Laptop-modus is ingeschakeld, past BitDefender de configureerde instellingen toe als de laptop op de accu werkt.

20.2.1. Laptop-modus instellingen configureren

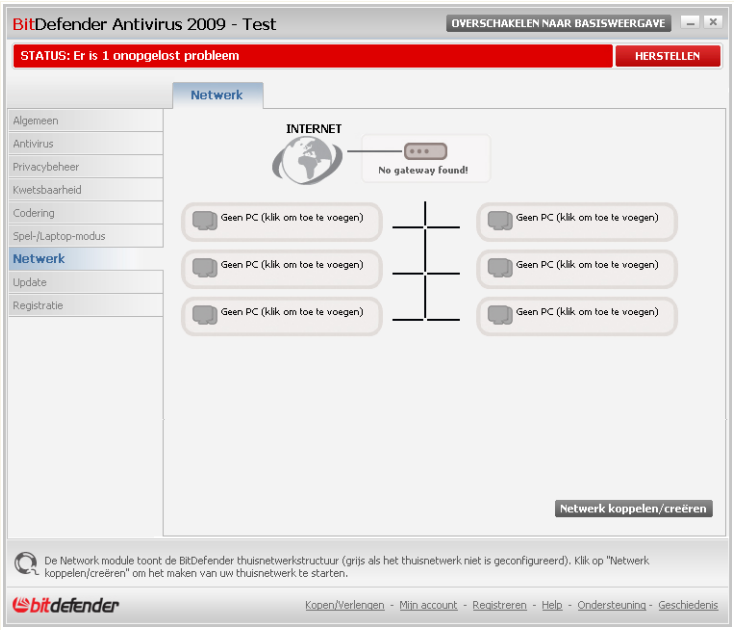
Gebruik deze opties om het gedrag voor geprogrammeerde taken te configureren:

- **Scan taken** - voorkomt dat geprgrammeerde taken worden uitgevoerd in de Laptop-modus. U kan een van de volgende opties kiezen:

Optie	Beschrijving
Taak overslaan	De geprogrammeerde taak wordt helemaal niet uitgevoerd.
Taak uitstellen	De geprogrammeerde taak uitvoeren zodra u de Laptop-modus verlaat.

21. Netwerk

Met de Netwerkmodule kan u de BitDefender producten die zijn geïnstalleerd op uw thuiscomputers beheren vanaf één enkele computer.



Netwerk map

Volg deze stappen om de BitDefender producten die zijn geïnstalleerd op uw computer te beheren:

1. Het BitDefender thuisnetwerk koppelen aan uw computer. Het koppelen van het netwerk bestaat uit het configureren van een administratief wachtwoord voor het thuisnetwerkbeheer.
2. Naar elke computer gaan die u wilt beheren en koppelen aan het netwerk (wachtwoord instellen)
3. Naar uw computer teruggaan en de computers toevoegen die u wilt beheren.

21.1. Het BitDefender netwerk koppelen

Volg deze stappen om het BitDefender thuisnetwerk te koppelen:

1. Klik op **Koppelen/Creëren**. U wordt gevraagd het thuisbeheer wachtwoord te configureren.

Wachtwoord configureren

2. Voer hetzelfde wachtwoord in elk van de bewerkingsvelden in.
3. Klik op **OK**.

U ziet de naam van de computer in de netwerkmap.

21.2. Bezig met toevoegen van computers aan het BitDefender netwerk

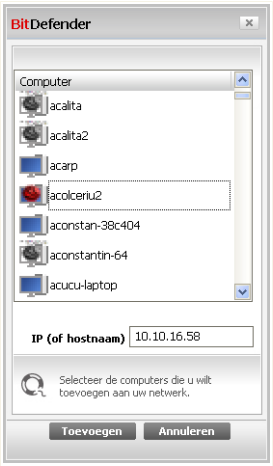
Voordat u een computer kan toevoegen aan het BitDefender thuisnetwerk, moet u het BitDefender thuisbeheer wachtwoord configureren op de betreffende computer.

Volg deze stappen als u een computer wilt toevoegen aan het BitDefender thuisnetwerk:

1. Klik op **Netwerk beheren**. U wordt gevraagd het lokale thuisbeheer wachtwoord in te voeren.

Wachtwoord invoeren

2. Voer het thuisbeheer wachtwoord in en klik op **OK**. Een nieuw venster wordt weergegeven.



Computer toevoegen

U ziet de lijst van computers in het netwerk. Het pictogram betekent:

- Een online computer zonder BitDefender producten.
- Een online computer met BitDefender producten.
- Een offline computer met BitDefender producten.

3. U kunt een van de volgende methoden gebruiken:
   - In de lijst de naam van de toe te voegen computer selecteren.
   - Het IP-adres of de naam van de comuter in het overeenkomende veld invoeren.
4. Klik op **Toevoegen**. U wordt gevraagd het thuismanagement wachtwoord van de betreffende computer in te voeren.

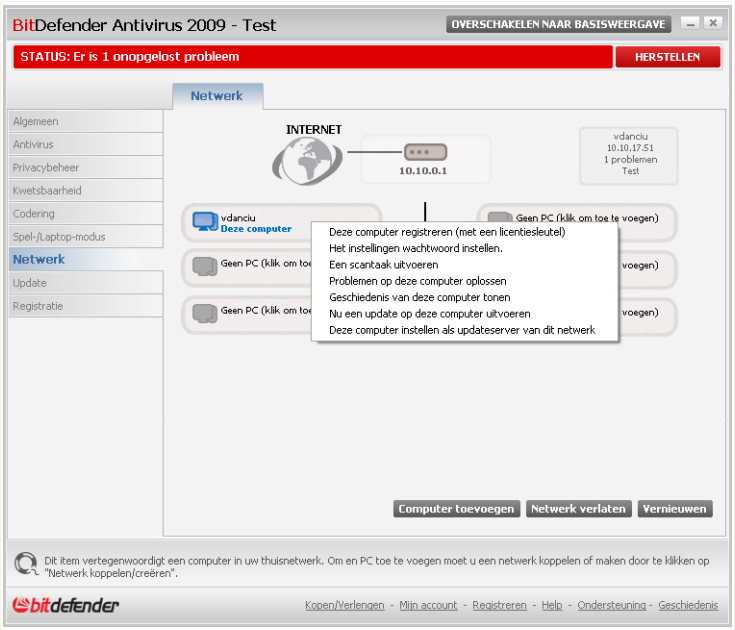
Identificeren

5. Het thuismanagement wachtwoord dat is geconfigureerd op de betreffende computer invoeren.
6. Klik op **OK**. Als het correcte wachtwoord is ingevoerd, verschijnt de naam van de geselecteerde computer in de netwerkmap.

Opmerking
U kan maximaal vijf comuters toevoegen aan de netwerkmap.

21.3. Het BitDefender netwerk beheren

Als met succes een BitDefender thuisnetwerk is gecreëerd, kan u alle BitDefender producten beheren vanaf één enkele computer.



Netwerk map

Als u de muiscursor boven een computer in de netwerkmap plaatst, ziet u korte informatie ervan (naam, IP-adres, aantal problemen die de systeemveiligheid bedreigen, BitDefender registratiestatus).

Als u rechtsklikt op een computernaam in de netwerkmap, kan u alle administratieve taken zien die u op verre computer kan uitvoeren.

- **Deze computer registreren**
- **Wachtwoordinstellingen instellen**
- **Een scantaak uitvoeren**
- **Problemen op deze computer herstellen**
- **Geschiedenis van deze computer weergeven**
- **Nu een update op deze computer uitvoeren**
- **Profiel toepassen**

- **Een Tune-up taak op deze computer uitvoeren**
- **Deze computer instellen als updateserver van dit netwerk**

Voordat u een taak op een specifieke computer kan uitvoeren, moet u het lokale thuisbeheer wachtwoord invoeren.

Wachtwoord invoeren

Voer het thuisbeheer wachtwoord in en klik op **OK**.

Opmerking

Als u verschillende taken wilt uitvoeren, kan u het selectievakje **Dit bericht niet weergeven tijdens deze sessie** inschakelen. Als u deze optie selecteert, wordt u tijdens de huidige sessie niet opnieuw naar het wachtwoord gevraagd.

22. Update

Elke dag wordt nieuwe malware gevonden en geïdentificeerd. Het is dan ook heel belangrijk dat u BitDefender up-to-date houdt met de meest recente malware handtekeningen.

Als u via breedband of DSL verbonden bent met het Internet, zal BitDefender deze taak op zich nemen. Het programma controleert standaard op updates wanneer u uw computer inschakelt en daarna ieder **uur**.

Als een update is gedetecteerd, kan u gevraagd worden het updaten te bevestigen, ofwel het updaten wordt automatisch uitgevoerd, afhankelijk van de automatische update instellingen.

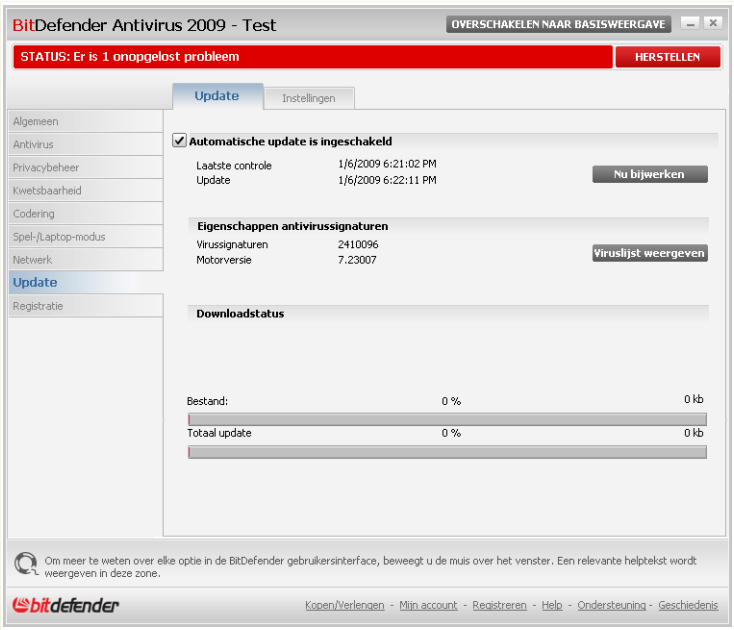
Het updateproces wordt “on the fly” uitgevoerd. Dit betekent dat de bestanden die moeten worden bijgewerkt, progressief worden vervangen. Hierdoor zal het updateproces de productwerking niet beïnvloeden wordt tegelijkertijd elk zwak punt uitgeschakeld.

Updates worden op de volgende manieren beschikbaar gesteld:

- **Updates voor antivirus-engines** - aangezien er steeds nieuwe virussen dreigen, moeten de bestanden met de virushandtekeningen voortdurend worden bijgewerkt om een permanente up-to-date beveiliging te garanderen. Dit type update is ook bekend als **Update virusdefinities**.
- **Updates voor de antispyware-engines** - er worden nieuwe spyware-handtekeningen toegevoegd aan de database. Dit type update is ook bekend als **Antispyware -update**.
- **Product upgrades** - Bij de lancering van een nieuwe productversie worden nieuwe functies en scantechnieken ingevoerd met het oog op een betere prestatie van het product. Dit type update is ook bekend als **Product-update**.

22.1. Automatische update

Om informatie met betrekking tot de update weer te geven en automatische updates uit te voeren, klikt u op **Update>Update** in de Geavanceerde weergave.



Automatische update

Hier kunt u zien wanneer de laatste controle op updates en de laatste update werd uitgevoerd. Daarnaast vindt u hier ook informatie over de laatst uitgevoerde update (indien gelukt of als er fouten zijn opgetreden). Ook informatie over de huidige engine-versie en het aantal handtekeningen wordt weergegeven.

Als u deze sectie opent tijdens een update, kunt u de downloadstatus zien.

Belangrijk
Houd **Automatische update** ingeschakeld om tegen de meest recente gevaren te worden beschermd.

U kan de malware signaturen van BitDefender ophalen door te klikken op **Virus Lijst Tonen**. Er wordt een HTML-bestand gemaakt dat alle beschikbare signaturen bevat. Dit bestand wordt geopend in een webbrowser. U kan in de database zoeken naar een specifieke malware signatuur of klikken op **BitDefender Viruslijst** om naar de online signaturen database van BitDefender te gaan.

22.1.1. Een update aanvragen

De automatische update kan ook op elk gewenst ogenblik worden uitgevoerd door te klikken op **Nu Updaten**. Dit type update is ook bekend als de **Update op aanvraag van de gebruiker**.

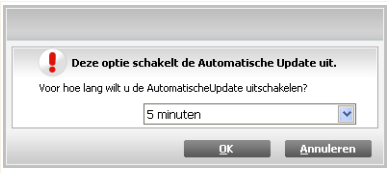
De module **Update** zal een verbinding maken met de updateserver van BitDefender en controleren of er een update beschikbaar is. Als een update is gedetecteerd, wordt u, afhankelijk van de opties die zijn ingesteld in het gedeelte Handmatige update-instellingen, gevraagd de update te bevestigen of wordt de update automatisch uitgevoerd.

Belangrijk
Het kan noodzakelijk zijn de computer opnieuw op te starten wanneer de update is voltooid. Wij adviseren dit zo snel mogelijk te doen.

Opmerking
Als u met het internet bent verbonden via een inbelverbinding, dan adviseren wij BitDefender regelmatig handmatig te updaten.

22.1.2. Automatische update uitschakelen

Als u de automatische update wilt uitschakelen, verschijnt een waarschuwingsvenster.



Automatische update uitschakelen

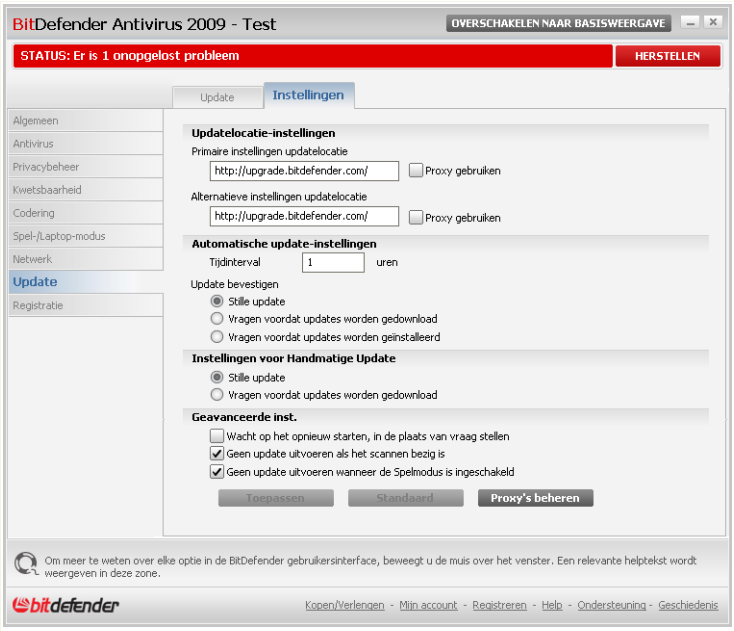
U moet uw keuze bevestigen door in het menu te selecteren hoelang u de automatische update wilt uitschakelen. U kan de automatische update uitschakelen gedurende 5, 15 of 30 minuten, 1 uur, permanent of tot het systeem opnieuw wordt opgestart.

Waarschuwing
Dit is een kritiek beveiligingsprobleem. Wij adviseren de automatische update zo kort mogelijk uit te schakelen. Als BitDefender niet regelmatig wordt geüpdatet, zal het programma niet in staat zijn u te beschermen tegen de nieuwste bedreigingen.

22.2. Update- instellingen

De updates kunnen worden uitgevoerd vanaf het lokale netwerk, via het Internet, rechtstreeks of via een proxyserver. BitDefender zal standaard elk uur via het internet controleren op updates en de beschikbare updates zonder enige waarschuwing installeren.

Om de update-instellingen te configureren en de proxy's te beheren, gaat u naar **Update>Instellingen** in de Geavanceerde weergave.



Update- instellingen

De update-instellingen zijn gegroepeerde in 4 categorieën (**Updatelocatie-instellingen**, **Automatische update-instellingen**, **Handmatige update-instellingen** en **Geavanceerde instellingen**). Elke categorie wordt afzonderlijk beschreven.

22.2.1. Updatelocaties instellen

Gebruik de opties in de categorie **Updatelocatie-instellingen** om de updatelocaties in te stellen.

Opmerking
Configureer deze instellingen alleen als u verbonden bent met een lokaal netwerk dat de malware signaturen van BitDefender lokaal opslaat of als u via een proxyserver met het internet bent verbonden.

Voor betrouwbaardere en snellere updates kunt u twee updatelocaties configureren: een **Primaire updatelocatie** en een **Alternatieve updatelocatie**. Deze locaties zijn standaard dezelfde: `http://upgrade.bitdefender.com`.

Om een van de updatelocaties te wijzigen, geeft u de URL van de lokale spiegel op in het **URL**-veld dat overeenkomt met de locatie die u wilt wijzigen.

Opmerking
Wij adviseren de lokale spiegel in te stellen als de primaire updatelocatie en de alternatieve updatelocatie ongewijzigd te laten als een alternatieve mogelijkheid in het geval de lokale spiegel niet bereikbaar is.

Als het bedrijf een proxyserver gebruikt om een verbinding te maken met het internet, schakelt u het selectievakje **Proxy gebruiken** in en klikt u vervolgens op **Proxy's beheren** om de proxy-instellingen te configureren. Meer informatie vindt u onder "*Proxy's beheren*" (p. 189).

22.2.2. Automatische update configureren

U kan het automatisch uitvoeren van de update door BitDefender instellen met de opties in de categorie **Automatische update-instellingen**.

In het veld **Tijdinterval** kan u het aantal uren tussen twee opeenvolgende controles op updates opgeven. Het tijdinterval voor de update is standaard ingesteld op 1 uur.

Selecteer een van de volgende opties om op te geven hoe de automatische update moet worden uitgevoerd:

- **Stille update** - BitDefender downloadt en installeert de update automatisch.
- **Vragen voordat updates worden gedownload** - telkens wanneer een update beschikbaar is, wordt uw bevestiging gevraagd voordat de update wordt gedownload.
- **Vragen voordat updates worden geïnstalleerd** - telkens wanneer een update is gedownload, wordt uw bevestiging gevraagd voordat de update wordt geïnstalleerd.

22.2.3. Handmatige update configureren

Selecteer een van de volgende opties in de categorie **Handmatige update-instellingen** om op te geven hoe de handmatige update (update op aanvraag van gebruiker) moet worden uitgevoerd:

- **Stille update** - de handmatige update wordt automatisch uitgevoerd op de achtergrond, zonder enige tussenkomst van de gebruiker.
- **Vragen voordat updates worden gedownload** - telkens wanneer een update beschikbaar is, wordt uw bevestiging gevraagd voordat de update wordt gedownload.

22.2.4. Geavanceerde instellingen configureren

Om ervoor te zorgen dat het updateproces van BitDefender uw werk niet hindert, congigureert u de opties in de categorie **Geavanceerde instellingen**:

- **Wacht op het opnieuw starten, in de plaats van vraag te stellen** - Als een update het opnieuw opstarten vereist, zal het product blijven werken met de oude bestanden tot het systeem opnieuw is opgestart. De gebruiker wordt niet gevraagd om opnieuw op te starten. Daarom zal het updateproces van BitDefender geen invloed hebben op het werk van de gebruiker.
- **Geen update uitvoeren als het scannen bezig is** - BitDefender zal geen update uitvoeren als een scanproces wordt uitgevoerd. Hierdoor zal het updateproces van BitDefender de scantaken niet hinderen.

  Opmerking
  Als de update van BitDefender wordt uitgevoerd terwijl het scannen bezig is, wordt het scanproces afgebroken.

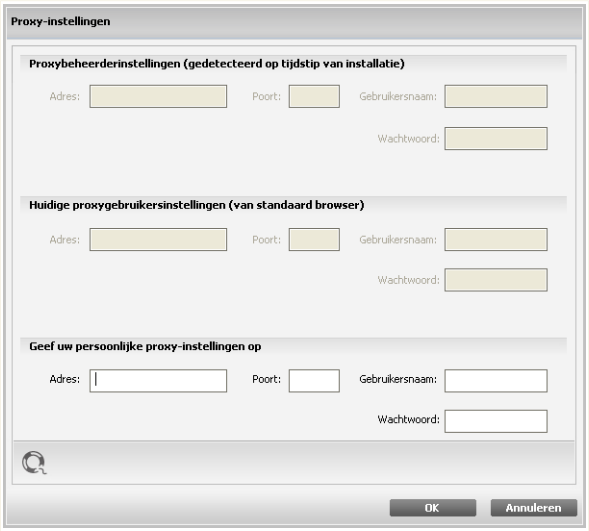
- **Geen update uitvoeren wanneer de spelmodus is ingeschakeld** - BitDefender zal geen update uitvoeren wanneer de spelmodus is ingeschakeld. Hierdoor kan u de invloed van het product op de systeemprestaties beperken tijdens het spelen van spelletjes.

22.2.5. Proxy's beheren

Als uw bedrijf een proxyserver gebruikt om een verbinding te maken met het internet, moet u de proxy-instellingen opgeven zodat BitDefender zichzelf kan updaten. Anders zal het programma gebruik maken van de proxy-instellingen van de beheerder die het product heeft geïnstalleerd of van de eventuele standaardbrowser van de huidige gebruiker.

Opmerking
De proxy-instellingen kunnen alleen worden geconfigureerd door gebruikers met beheerdersrechten op de computer of door hoofdgebruikers (gebruikers die het wachtwoord voor de productinstellingen kennen).

Klik op **Proxy's beheren** om de proxy-instellingen te beheren. Het venster **Proxybeheer** verschijnt.



Proxybeheer

Er zijn drie reeksen proxy-instellingen:

- **Proxybeheerderinstellingen (gedetecteerd op tijdstip van installatie)** - proxy-instellingen die tijdens de installatie op de beheerdersaccount zijn gedetecteerd en die alleen kunnen worden geconfigureerd wanneer u bij die account bent aangemeld. Als de proxyserver een gebruikersnaam en wachtwoord vereist, moet u deze gegevens opgeven in de overeenkomende velden.
- **Huidige proxygebruikersinstellingen (van standaard browser)** - proxy-instellingen van de huidige gebruiker, opgehaald van de standaard browser. Als de proxyserver een gebruikersnaam en wachtwoord vereist, moet u deze gegevens opgeven in de overeenkomende velden.

Opmerking
De ondersteunde webbrowsers zijn Internet Explorer, Mozilla Firefox en Opera. Als u standaard een andere browser gebruikt, zal BitDefender de proxy-instellingen van de huidige gebruiker niet kunnen ophalen.

- **Uw persoonlijke reeks proxy-instellingen** - proxy-instellingen die u kan configureren als u bent aangemeld als beheerder.

  U moet de volgende instellingen definiëren:
  - **Adres** - voer het IP-adres van de proxyserver in.
  - **Poort** - voer de poort in die BitDefender gebruikt om een verbinding te maken met de proxyserver.
  - **Gebruikersnaam** - voer een gebruikersnaam in die wordt herkend door de proxy.
  - **Wachtwoord** - voer het geldige wachtwoord voor de eerder opgegeven gebruiker in.

Wanneer u een verbinding probeert te maken met het internet, wordt elke reeks proxy-instellingen achtereenvolgens geprobeerd, tot BitDefender erin slaagt een verbinding te maken.

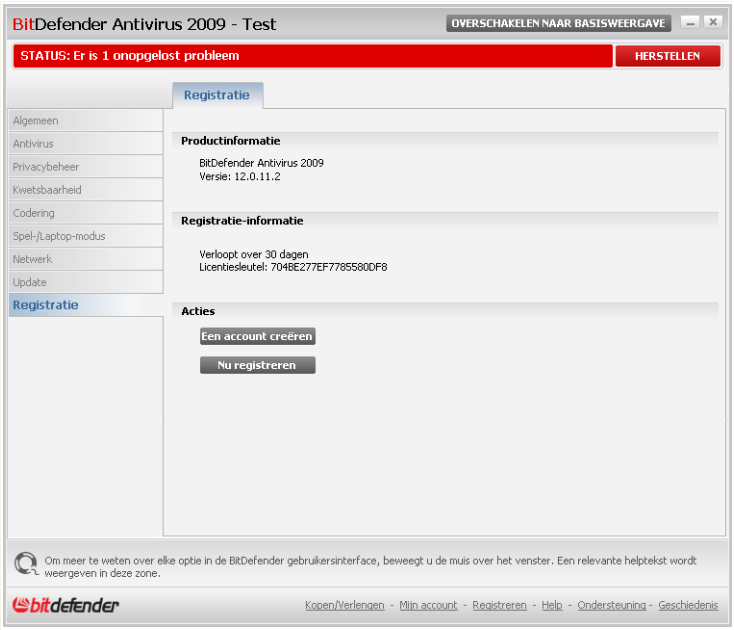
Eerst wordt de reeks met uw persoonlijke proxy-instellingen gebruikt om een verbinding te maken met het internet. Als dat niet werkt, worden daarna de proxy-instellingen die op het tijdstip van de installatie zijn gedetecteerd, geprobeerd. Als dat evenmin werkt, worden tot slot de proxy-instellingen van de huidige gebruiker overgenomen van de standaard browser en gebruikt om een verbinding te maken met het internet.

Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

Klik op **Toepassen** om de wijzigingen op te slaan of klik op **Standaard** om de standaardinstellingen te laden.

23. Registratie

Om alle informatie over uw BitDefender product en de registratiestatus te zien, gaat u naar **Registratie** in de Geavanceerde weergave.



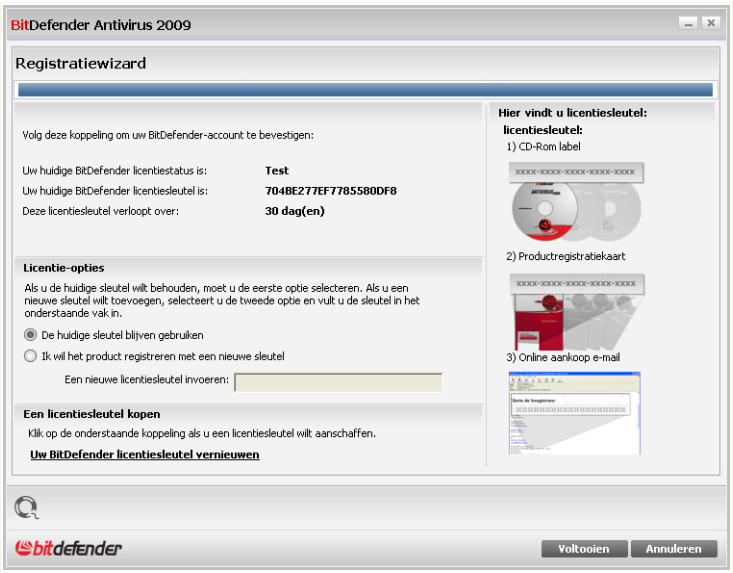
Registratie

In deze sectie ziet u:

- **Productinformatie**: het BitDefender product en de versie.
- **Registratie-informatie**: het e-mailadres waarmee u inlogt op uw BitDefender-account (indien geconfigureerd), de huidige licentiesleutel en over hoeveel dagen de licentiesleutel verloopt.

23.1. BitDefender Antivirus 2009 registreren

Klik op **Nu registreren** om de registratie van het product te starten.



Registratie

U kan de BitDefender registratiestatus zien, evenals de huidige licentiesleutel en over hoeveel dagen de licentiesleutel verloopt.

Om BitDefender Antivirus 2009 te registreren:

1. Selecteer **Ik wil het product registreren met een nieuwe sleutel**.
2. Typ de licentiesleutel in het bewerkingsveld.

Opmerking

U kan uw licentiesleutel vinden:

- op het cd label.
- op de productregistratiekaart.
- in de online aankoop e-mail.

Als u geen BitDefender licentiesleutel hebt, klik dan op de aanwezige link om naar de BitDefender online winkel te gaan en een licentiesleutel te kopen.

Klik op **Voltooien**.

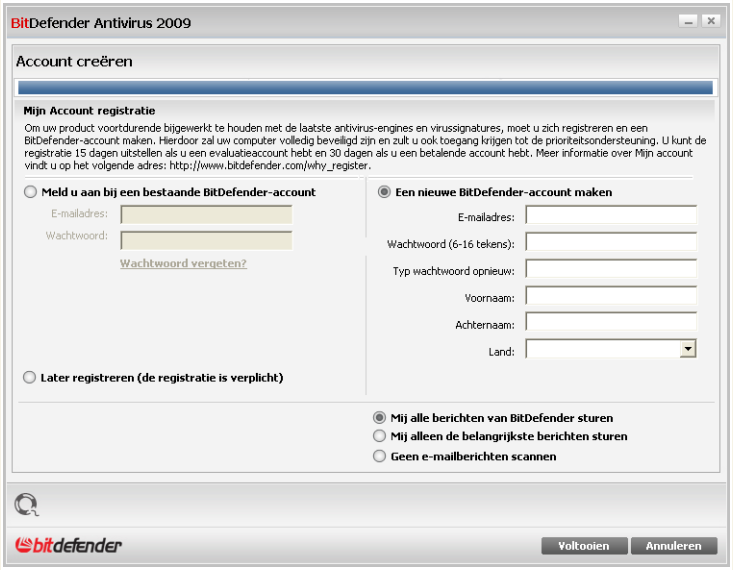
23.2. Een BitDefender-account creëren

Als onderdeel van het registratieproces MOET u een BitDefender-account maken. De BitDefender-account biedt u toegang tot de BitDefender-updates, gratis technische ondersteuning en speciale aanbiedingen en promoties. Als u uw licentiesleutel kwijt bent, kunt u inloggen op uw account op http://myaccount.bitdefender.com om hem op te halen.

Belangrijk

U moet een account maken binnen de 15 dagen na het installeren van BitDefender (als u het product registreert, wordt de deadline verlengd tot 30 dagen). Anders zullen er geen updates van BitDefender meer worden uitgevoerd.

Als nog geen BitDefender-account is gecreëerd, klikt u op **Een account creëren** om het accountregistratievenster te openen.



Account creëren

Als u nu geen BitDefender-account wilt creëren, selecteer dan **Registratie overslaan** en klik op **Voltooien**. Ga anders te werk zoals past bij uw situatie:

- “Ik heb geen BitDefender-account” (p. 195)
- “Ik heb al een BitDefender-account” (p. 196)

Ik heb geen BitDefender-account

Om een BitDefender-account te creëren, selecteert u **Een nieuwe BitDefender-account maken** en geeft u de vereiste informatie op. De gegevens die u hier opgeeft blijven vertrouwelijk.

- **E-mailadres** - voer uw e-mailadres in.
- **Wachtwoord** - voer een wachtwoord voor uw BitDefender-account in. Het wachtwoord moet minstens zes tekens bevatten.
- **Wachtwoord opnieuw** - voer het zojuist gebruikte wachtwoord opnieuw in.

- **Voornaam** - voer uw voornaam in.
- **Achternaam** - voer uw achternaam in.
- **Land** - selecteer het land waar u woont.

Opmerking
Gebruik het door u ingevoerde e-mailadres en wachtwoord om in te loggen op uw account op http://myaccount.bitdefender.com.

Om een account te kunnen maken, moet u eerst uw e-mailadres activeren. Controleer uw e-mailadres en volg de instructies in de e-mail die u van de registratieservice van BitDefender hebt ontvangen.

Optioneel kan BitDefender u informeren over speciale aanbiedingen via het e-mailadres van uw account. Selecteer een van de beschikbare opties:

- **Stuur mij alle berichten van BitDefender**
- **Stuur mij alleen de belangrijkste berichten**
- **Stuur mij geen berichten**

Klik op **Voltooien**.

Ik heb al een BitDefender-account

BitDefender detecteert automatisch of u al een BitDefender-account hebt geregistreerd op uw computer. Geef in dit geval het wachtwoord van uw account op.

Als u al een actieve account hebt, maar BitDefender deze niet detecteert, selecteer dan **Aanmelden bij een bestaande BitDefender Account** en vul het e-mailadres en het wachtwoord van uw account in.

Als u uw wachtwoord bent vergeten, klikt u op **Wachtwoord vergeten?** en volgt u de instructies.

Optioneel kan BitDefender u informeren over speciale aanbiedingen via het e-mailadres van uw account. Selecteer een van de beschikbare opties:

- **Stuur mij alle berichten van BitDefender**
- **Stuur mij alleen de belangrijkste berichten**
- **Stuur mij geen berichten**

Klik op **Voltooien**.

Hulp vragen

24. Ondersteuning

Als gewaardeerd provider streeft BitDefender ernaar zijn klanten een ongeëvenaard niveau van snelle en nauwkeurige ondersteuning te bieden. Het Ondersteuningscentrum (dat u kan bereiken op het onderstaande adres) houdt voortdurend de laatste bedreigingen bij. Hier worden al uw vragen zo snel mogelijk beantwoord.

Bij BitDefender is het onze absolute prioriteit onze klant te helpen tijd en geld te besparen, door hem de meest geavanceerde producten te bieden voor de eerlijkste prijs. Bovendien zijn wij ervan overtuigd dat een succesvol bedrijf gebaseerd is op goede communicatie en zich inzet voor uitmuntendheid in klantenondersteuning.

U kunt op elk ogenblik hulp vragen op support@bitdefender.com. Voor een snel antwoord vragen wij u zoveel mogelijk details over uw BitDefender product en uw systeem te vermelden in uw e-mail en het probleem waarmee u te kampen hebt zo nauwkeurig mogelijk te omschrijven.

24.1. BitDefender Knowledge Base

De BitDefender Knowledge Base is een online opslagplaats van informatie over BitDefender-producten. Hier worden rapporten bijgehouden in een gemakkelijk toegankelijk formaat over de doorlopende technische ondersteuning en activiteiten voor foutoplossingen van de ondersteunings- en ontwikkelingsteams van BitDefender. Daarnaast vindt u hier ook meer algemene artikels over viruspreventie, het beheer van BitDefender-oplossingen met gedetailleerde uitleg en talrijke andere artikels.

De BitDefender Knowledge Base is toegankelijk voor het publiek en kan vrij worden doorzocht. De uitgebreide informatie die de database bevat is nog een middel om BitDefender-klanten de technische kennis en het inzicht te bieden die ze nodig hebben. Alle geldige aanvragen voor informatie of foutrapporten die van BitDefender-klanten komen, vinden uiteindelijk hun weg naar de BitDefender Knowledge Base als rapporten over het oplossen van problemen, tips om een probleem te omzeilen of informatieve artikels om de helpbestanden van het product aan te vullen.

De BitDefender Knowledge Base is altijd beschikbaar op http://kb.bitdefender.com.

24.2. Hulp vragen

24.2.1. Ga naar Web-zelfbediening

Hebt u een vraag? Onze beveiligingsexperts staan 24/7 gratis tot uw dienst via telefoon, e-mail of chat.

Gebruik de onderstaande links:

Engels

http://www.bitdefender.com/site/KnowledgeBase/

Duits

http://www.bitdefender.com/de/KnowledgeBase/

Frans

http://www.bitdefender.com/fr/KnowledgeBase/

Roemeens

http://www.bitdefender.com/ro/KnowledgeBase/

Spaans

http://www.bitdefender.com/es/KnowledgeBase/

24.2.2. Een ondersteuningsticket openen

Als u een ondersteuningsticket wilt openen en hulp via e-mail wilt ontvangen, volgt u een van deze links:

Engels: http://www.bitdefender.com/site/Main/contact/1/
Duits: http://www.bitdefender.de/site/Main/contact/1/
Frans: http://www.bitdefender.fr/site/Main/contact/1/
Roemeens: http://www.bitdefender.ro/site/Main/contact/1/
Spaans: http://www.bitdefender.es/site/Main/contact/1/

24.3. Contactinformatie

Efficiënte communicatie is de sleutel naar het succes. Gedurende de laatste 10 jaar heeft BITDEFENDER een onberispelijke reputatie opgebouwd door voortdurend te streven naar een betere communicatie om de verwachtingen van onze klanten en partners steeds opnieuw te overtreffen. Aarzel niet contact op te nemen met ons als u vragen hebt.

24.3.1. Nederland

Telefoon: +40-21-233.07.80; +40-21-408.56.00
Fax: +40-21-233.07.63
E-mail: sales@editions-profil.com
Verkoop: http://www.bitdefender.com/links/nl/2009/buy/antivirus.html
Technische ondersteuning:
http://www.bitdefender.com/P2216--en--Browse-by-BitDefender-Antivirus-2009.html
Website: http://www.bitdefender.com/links/nl/homepage.html

BitDefender reddingsschijf

25. Overzicht

BitDefender Antivirus 2009 wordt geleverd met een opstartbare CD (BitDefender reddingsschijf) die in staat is alle bestaande harde schijven te scannen en te desinfecteren voordat uw besturingssysteem opstart.

Gebruik telkens de BitDefender reddingsschijf wanneer uw besturingssysteem niet correct werkt door virusinfecties. Dit gebeurt doorgaans wanneer u geen antivirusproduct gebruikt.

Telkens wanneer u de BitDefender reddingsschijf opstart, wordt de update van de virussignaturen automatisch uitgevoerd, zonder tussenkomst van de gebruiker.

De BitDefender reddingsschijf is een geremasterde Knoppix-distributie van BitDefender, die de nieuwste BitDefender voor Linux-beveiligingsoplossing integreert in de GNU/Linux Knoppix Live CD en een desktopantivirus biedt die bestaande harde schijven kan scannen en desinfecteren (inclusief Windows NTFS-partities). Op hetzelfde ogenblik kan u de BitDefender reddingsschijf gebruiken om uw waardevolle data te herstellen wanneer u Windows niet kan opstarten.

Opmerking
De BitDefender reddingsschijf kan worden gedownload van deze locatie: http://download.bitdefender.com/rescue_cd/

25.1. Systeemvereisten

Voordat u de BitDefender reddingsschijf opstart, moet u eerst controleren of uw systeem voldoet aan de volgende vereisten.

Processortype
x86-compatibel, minimum 166 MHz, maar verwacht geen hoge prestaties in dit geval. Een processor van de i686-generatie met 800 MHz is een betere keuze.

Geheugen
Minimum 512 MB RAM-geheugen (1 GB aanbevolen)

Cd-rom
De BitDefender reddingsschijf wordt uitgevoerd vanaf een cd-rom. Daarom is een cd-rom en een BIOS waarmee ervan kan worden opgestart vereist.

Internetverbinding
Hoewel de BitDefender reddingsschijf kan werken zonder internetverbinding, is er toch een actieve http-verbinding vereist voor de updateprocedure, zelfs via

een proxyserver. Voor een up-to-date beveiliging is een internetverbinding dus een absolute vereiste.

Grafische resolutie
Standaard SVGA-compatibele grafische kaart.

25.2. Bijgeleverde software

De BitDefender reddingsschijf bevat de volgende softwarepakketten.

Xedit
Dit is een tekstbestandseditor.

Vim
Dit is een krachtige tekstbestandseditor die syntaxmarkering, een GUI en veel meer bevat. Meer informatie vindt u op de Vim-startpagina.

Xcalc
Dit is een rekenmachine.

RoxFiler
RoxFiler is een snel en krachtig grafisch bestandsbeheer.

Meer informatie vindt u op de RoxFiler-startpagina.

MidnightCommander
GNU Midnight Commander (mc) is een beheerprogramma voor tekstmodusbestanden.

Meer informatie vindt u op de MC-startpagina.

Pstree
Pstree toont de actieve processen.

Top
Top toont Linux-taken.

Xkill
Xkill vernietigt een client door middel van zijn X-bronnen.

Partition Image
Met Partition Image kunt u partities in de bestandssysteemformaten EXT2, Reiserfs, NTFS, HPFS, FAT16 en FAT32 opslaan naar een imagebestand. Dit programma kan nuttig zijn voor back-updoeleinden.

Meer informatie vindt u op de Partimage-startpagina.

GtkRecover

GtkRecover is een GTK-versie van het consoleprogrammaherstel. Het helpt u een bestand te herstellen.

Meer informatie vindt u op de GtkRecover-startpagina.

ChkRootKit

ChkRootKit is een hulpprogramma dat u helpt uw computer te scannen op rootkits.

Meer informatie vindt u op de ChkRootKit-startpagina.

Nessus Network Scanner

Nessus is een externe beveiligingsscanner voor Linux, Solaris, FreeBSD en Mac OS X.

Meer informatie vindt u op de Nessus-startpagina.

Iptraf

Iptraf is een programma voor IP-netwerkbewaking.

Meer informatie vindt u op de Iptraf-startpagina.

Iftop

Iftop toont het bandbreedtegebruik op een interface.

Meer informatie vindt u op de Iftop-startpagina.

MTR

MTR is een netwerkdiagnosehulpprogramma.

Meer informatie vindt u op de MTR-startpagina.

PPPStatus

PPPStatus toont statistieken over het binnenkomende en uitgaande TCP/IP-verkeer.

Meer informatie vindt u op de PPPStatus-startpagina.

Wavemon

Wavemon is een bewakingstoepassing voor draadloze netwerkapparaten.

Meer informatie vindt u op de Wavemon-startpagina.

USBView

USBView toont informatie over apparaten die zijn aangesloten op de USB-bus.

Meer informatie vindt u op de USBView-startpagina.

Pppconfig

Pppconfig helpt bij het automatisch tot stand brengen van een ppp-inbelverbinding.

DSL/PPPoe

DSL/PPPoe configureert PPPoE-verbinding (ADSL).

I810rotate

I810rotate schakelt de video-uitvoer op i810-hardware door middel van de i810switch(1).

Meer informatie vindt u op de I810rotate-startpagina.

Mutt

Mutt is een krachtige, op tekst gebaseerde MIME-mailclient.

Meer informatie vindt u op de Mutt-startpagina.

Mozilla Firefox

Mozilla Firefox is een bekende webbrowser.

Meer informatie vindt u op de Mozilla Firefox-startpagina.

Elinks

Elinks is een webbrowser in tekstmodus.

Meer informatie vindt u op de Elinks-startpagina.

26. De BitDefender reddingsschijf gebruiken

Dit hoofdstuk bevat informatie over het starten en stoppen van de BitDefender reddingsschijf, het scannen van uw computer op malware en het opslaan van gegevens vanaf uw aangetaste Windows-pc naar een verwisselbaar apparaat. Wanneer u de softwaretoepassingen die op de cd zijn geleverd gebruikt, kan u echter veel meer taken uitvoeren dan binnen het bereik van deze handleiding kunnen worden beschreven.

26.1. BitDefender reddingsschijf starten

Om de cd te starten, stelt u de BIOS van uw computer in om te starten vanaf de cd, plaatst u de cd in het cd-romstation en start u de computer opnieuw op. Controleer of uw computer kan opstarten vanaf een cd.

Wacht tot het volgende scherm wordt getoond en volg de instructies op het scherm om de BitDefender reddingsschijf te starten.

Opmerking
Selecteer in de lijst de taal die u wilt gebruiken voor de reddingsschijf.

Splash-scherm opstarten

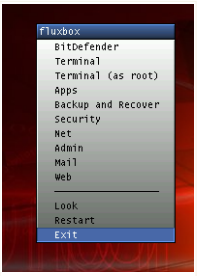
Bij het opstarten wordt de update van de virussignaturen automatisch uitgevoerd. Dit kan even duren.

Wanneer het opstartproces is voltooid, ziet u het volgende bureaublad. U kan nu starten met het gebruik van de BitDefender reddingsschijf.

Het bureaublad

26.2. BitDefender reddingsschijf stoppen

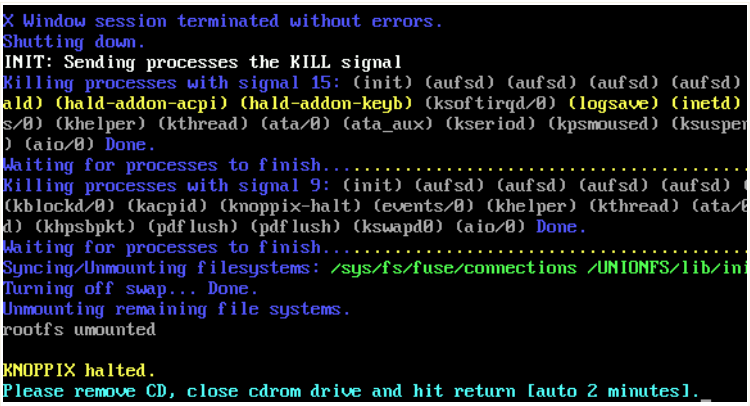
Daarna kan u de computer veilig afsluiten door **Afsluiten** te selecteren in het contextafhankelijke menu van de BitDefender reddingsschijf (rechtsklikken om het te openen) of door de opdracht **stoppen** te selecteren op een werkstation.



Kies "AFSLUITEN"

Wanneer de BitDefender reddingsschijf alle programma's met succes heeft afgesloten, ziet u het in de volgende afbeelding weergegeven scherm. U kan de cd verwijderen

om opnieuw op te starten vanaf uw harde schijf. U kan nu uw computer veilig uitschakelen of opnieuw opstarten.



Wacht op dit bericht wanneer u afsluit.

26.3. Hoe kan ik een antivirusscan uitvoeren?

Nadat het opstartproces is voltooid, verschijnt een wizard waarmee u een volledige scan van uw computer kunt uitvoeren. Hiervoor hoeft u alleen te klikken op de knop **Start** .

Opmerking
Als uw schermresolutie niet hoog genoeg is, wordt u gevraagd het scannen te starten in de tekstmodus.

Volg de begeleide procedure van drie stappen om het scanproces te voltooien.

1. U kunt de scanstatus en de statistieken zien (scansnelheid, verstreken tijd, aantal gescande/geïnfecteerde/verdachte/verborgen objecten en andere).

   Opmerking
   Afhankelijk van de complexiteit van de scan, kan het scanproces enige tijd in beslag nemen.

2. U kan het aantal problemen dat uw systeem beïnvloedt, zien.

De problemen worden weergegeven in groepen. Klik op het vakje "+" om een groep te openen of op het vakje "-" om een groep te sluiten.

U kan een algemene actie selecteren die moet worden genomen voor elke groep problemen of u kan afzonderlijke acties voor elk probleem selecteren.

3. U kan een samenvatting van de resultaten zien.

Als u slechts één bepaalde map wilt scannen, gaat u als volgt te werk:

Blader door uw mappen, klik met de rechtermuisknop op een bestand of map en selecteer **Verzenden naar**. Kies vervolgens **BitDefender Scanner**.

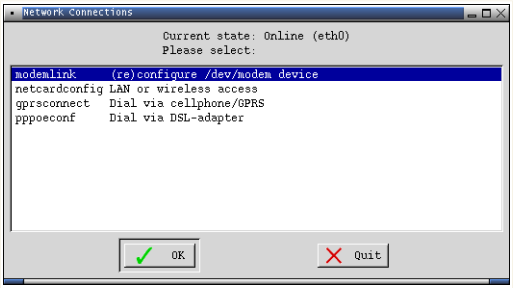
U kunt ook de volgende opdracht als hoofdmap opgeven vanaf een terminal. De **BitDefender Antivirusscanner** zal starten met het geselecteerde bestand of de map als de standaardlocatie voor het scannen.

```
# bdscan /path/to/scan/
```

26.4. Hoe configureer ik de internetverbinding?

Als u in een DHCP-netwerk bent en een ethernet-netwerkkaart hebt, moet de internetverbinding al gedetecteerd en geconfigureerd zijn. Volg de onderstaande stappen voor een handmatige configuratie.

1. Dubbelklik op de snelkoppeling Netwerkverbindingen op het bureaublad. Het volgende venster verschijnt.



Netwerkverbindingen

2. Selecteer het type verbinding dat u gebruikt en klik op OK.

Verbinding	Beschrijving
modemlink	Selecteer dit type verbinding als u een modem en een telefoonlijn gebruikt om naar het internet te gaan.
netcardconfig	Selecteer dit type verbinding als u een lokaal netwerk (LAN) gebruikt om naar het internet te gaan. Dit is ook geschikt voor draadloze verbindingen.
gprsconnect	Selecteer dit type verbinding als u naar het internet gaat via een mobiele telefoon met GPRS (General Packet Radio Service) protocol. Natuurlijk kan u ook een RPRS modem gebruiken in plaats van een mobiele telefoon.
pppoeconf	Selecteer dit type verbinding als u een DSL (Digital Subscriber Line) modem gebruikt om naar het internet te gaan.

3. Volg de instructies op het scherm. Als u niet zeker bent wat u moet schrijven, neem dan contact op met uw systeem- of netwerkbeheerder voor details.

Belangrijk
Bedenk dat u alleen het modem activeert door het selecteren van bovengenoemde opties. Volg deze stappen om de netwerkverbinding te configureren.

1. Rechtsklik op het Bureaublad. Het contextafhankelijke menu van de BitDefender reddingsschijf verschijnt.
2. Selecteer **Werkstation (als hoofdmap)**.
3. Typ de volgende commando's:

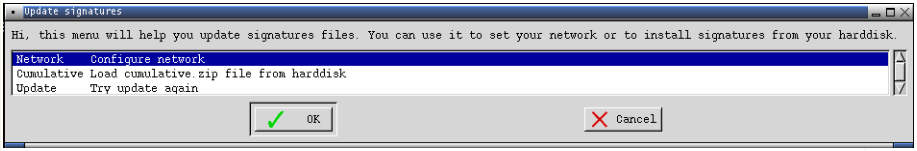
```
# pppconfig
```

4. Volg de instructies op het scherm. Als u niet zeker bent wat u moet schrijven, neem dan contact op met uw systeem- of netwerkbeheerder voor details.

26.5. Hoe kan ik BitDefender updaten?

Bij het opstarten wordt de update van de virussignaturen automatisch uitgevoerd. Maar als u deze stap hebt overgeslagen, ziet u hier hoe u BitDefender updatet.

1. Dubbelklik op de snelkoppeling Update signaturen op het bureaublad. Het volgende venster verschijnt.



Update signaturen

2. U kunt een van de volgende methoden gebruiken:
   - Selecteer **Cumulatief** voor het installeren van reeds op uw harde schijf opgeslagen signaturen door te bladeren in uw computer en het laden van het `cumulative.zip` bestand.
   - Selecteer **Update** om direct verbinding met het internet te maken en de laatste virus signaturen te downloaden.
3. Klik op **OK**.

26.5.1. Hoe kan ik BitDefender updaten over een proxy?

Als er een proxy server is tussen uw computer en het Internet, moeten een paar configuraties worden uitgevoerd om de virussignaturen te kunnen updaten.

Volg deze stappen om BitDefender te updaten over een proxy:

1. Rechtsklik op het Bureaublad. Het contextafhankelijke menu van de BitDefender reddingsschijf verschijnt.
2. Selecteer **Werkstation (als hoofdmap)**.
3. Typ het commando: **cd /ramdisk/BitDefender-scanner/etc**.
4. Typ het commando: **mcedit bdscan.conf** om dit bestand te bewerken met behulp van GNU Midnight Commander (mc).
5. Verwijder de toelichting van de volgende regel: `#HttpProxy =` (verwijder alleen het `#` teken) en geef het domein, gebruikersnaam, wachtwoord en serverpoort van de proxy server aan. De betreffende regel kan er, bijvoorbeeld, als volgt uitzien:

   ```
   HttpProxy = myuser:mypassword@proxy.company.com:8080
   ```
6. Druk op **F2** om het actuele bestand op te slaan, bevestig het opslaan, en druk dan op **F10** om het te sluiten.
7. Typ het commando: **bdscan update**.

26.6. Hoe kan ik mijn gegevens opslaan?

Laten we veronderstellen dat u uw Windows-pc door enkele onbekende problemen niet meer kan opstarten. U moet echter tegelijkertijd absoluut toegang krijgen tot enkele belangrijke gegevens op uw computer. Dit is het ogenblik waarop de BitDefender reddingsschijf in actie komt.

Volg deze stappen om gegevens van de computer op te slaan naar een verwisselbaar apparaat, zoals een usb-geheugenstick:

1. Plaats de BitDefender reddingsschijf in het cd-romstation. Steek de geheugenstick in de usb-aansluiting en start de computer opnieuw op.

   Opmerking
   Als u de geheugenstick op een later moment inplugt, moet u de hardware op de volgende manier verbinden:
   a. Dubbelklik op de snelkoppeling Terminal emulator op het bureaublad.
   b. Typ het volgende commando:

   ```
   # mount  /media/sdb1
   ```

   Afhankelijk van uw computer configuratie kan dit `sda1` zijn, in plaats van `sdb1`.

2. Wacht tot de BitDefender reddingsschijf volledig is opgestart. Het volgende venster verschijnt.

Bureaubladscherm

3. Dubbelklik op de partitie die de gegevens die u wilt opslaan, bevat (bijv. `[sda3]`).

Opmerking

Wanneer u met de BitDefender reddingsschijf werkt, krijgt u te maken met partitienamen van het Linux-type. Zo zal `[sda1]` waarschijnlijk overeenkomen met de `(C:)`-partitie van het Windows-type, `[sda3]` met `(F:)` en `[sdb1]` met de geheugenstick.

Belangrijk

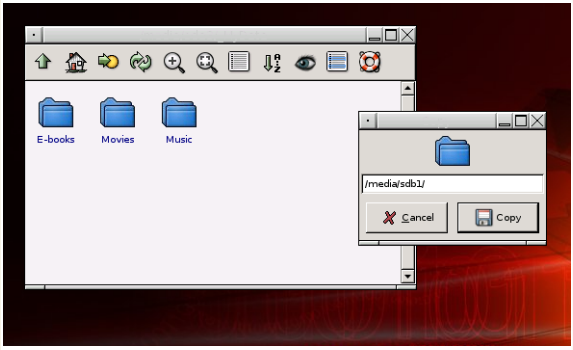
Als de computer niet correct was afgesloten, is het mogelijk dat sommige partities niet automatisch zijn geopend. Volg deze stappen om een partitie te openen.

a. Dubbelklik op de snelkoppeling Terminal emulator op het bureaublad.

b. Typ het volgende commando:

```
# mount  /media/partition_name
```

4. Blader door uw mappen en open de gewenste map. Bijvoorbeeld: `Mijn gegevens` dat de submappen `Films`, `Muziek` en `E-boeken` bevat.
5. Klik met de rechtermuisknop op de gewenste map en selecteer **Kopiëren**. Het volgende venster verschijnt.



Gegevens opslaan

6. Typ `/media/sdb1/` in het overeenkomende tekstvak en klik op **Kopiëren**.

   Afhankelijk van uw computer configuratie kan dit `sda1` zijn, in plaats van `sdb1`.

Woordenlijst

ActiveX

ActiveX is een model voor het schrijven van programma's zodat andere programma's en het besturingssysteem ze kunnen oproepen. De ActiveX-technologie wordt gebruikt bij Microsoft Internet Explorer om interactieve Webpagina's te maken die eruitzien en zich gedragen als computerprogramma's in plaats van statische pagina's. Met ActiveX kunnen gebruikers vragen stellen of beantwoorden, drukknoppen gebruiken en op andere manieren interactief omgaan met de Webpagina. ActiveX-besturingselementen zijn vaak geschreven met de hulp van Visual Basic.

ActiveX is berucht door een compleet gebrek aan beveiligingscontroles; computerbeveiligingsexperts raden het gebruik ervan via het Internet sterk af.

Adware

Adware wordt vaak gecombineerd met een hosttoepassing die gratis wordt aangeboden op voorwaarde dat de gebruiker akkoord gaat met het uitvoeren van de adware. Omdat adware-toepassingen doorgaans worden geïnstalleerd nadat de gebruiker een licentieovereenkomst die het doel van de toepassing vermeldt heeft geaccepteerd, wordt er geen inbreuk gepleegd.

Pop-upadvertenties kunnen echter irritant worden en in sommige gevallen de systeemprestaties negatief beïnvloeden. De gegevens die door sommige van deze toepassingen worden verzameld, kunnen bovendien privacy-problemen veroorzaken voor gebruikers die niet volledig op de hoogte waren van de voorwaarden van de licentieovereenkomst.

Archief

Een schijf, tape, of map die bestanden bevat waarvan een back-up werd gemaakt.

Een bestand dat één of meer bestanden bevat in een gecomprimeerd formaat.

Achterdeur

Een gat in de beveiliging van een systeem, dat opzettelijk werd achtergelaten door ontwikkelaars of beheerders. De motivatie voor dergelijke gaten is niet altijd boosaardig. Sommige besturingssystemen worden bijvoorbeeld geleverd met bevoegde accounts die bedoeld zijn voor gebruik door technici voor service ter plaatse of onderhoudsprogrammeurs van de leverancier.

Opstartsector

Een sector aan het begin van elke schijf die de architectuur van de schijf identificeert (sectorgrootte, clustergrootte, enz.) Bij opstartschijven bevat de opstartsector ook een programma dat het besturingssysteem laadt.

Opstartsectorvirus

Een virus dat de opstartsector van een vaste schijf of een diskette infecteert. Wanneer u probeert op te starten vanaf een diskette die geïnfecteerd is met een opstartsectorvirus, zal het virus actief worden in het geheugen. Wanneer u daarna uw systeem opstart, zal het virus telkens in het geheugen actief zijn.

Browser

De korte naam voor Webbrowser, een softwaretoepassing die wordt gebruikt op Webpagina's te zoeken en weer te geven. De twee populairste browsers zijn Netscape Navigator en Microsoft Internet Explorer. Beide zijn grafische browsers. Dit betekent dat ze zowel grafische beelden als tekst kunnen weergeven. Bovendien kunnen de meeste moderne browsers ook multimedia-informatie weergeven met geluid en video, hoewel voor sommige formaten plug-ins vereist zijn.

Opdrachtregel

In een opdrachtregelinterface typt de gebruiker opdrachten in opdrachttaal rechtstreeks op het scherm in de ruimte die hiervoor wordt geboden.

Cookie

Binnen de Internetindustrie worden cookies beschreven als kleine programma's die informatie bevatten over individuele computers, die door adverteerders wordt geanalyseerd en gebruikt om uw on line interesse en smaak te volgen. De cookietechnologie wordt in dit kader nog steeds verder ontwikkeld met het doel reclameberichten rechtstreeks te richten op de interesses die u hebt meegedeeld. Dit is voor veel mensen een mes dat aan twee kanten snijdt. Aan de ene kant is het efficiënt en relevant aangezien u alleen reclames ontvangt voor zaken waarvoor u interesse hebt. Aan de andere kant betekent het ook dat elke plaats die u bezoekt en alles wat u aanklikt wordt "opgespoord" en "gevolgd". Het is dan ook te begrijpen dat er heel wat wordt gedebatteerd over privacy. Bovendien zijn veel mensen verontwaardigd omdat ze het gevoel hebben dat ze als een "SKU-nummer" worden beschouwd (u weet wel, de barcode op de verpakkingen die bij de kassa van het warenhuis wordt gescand). Hoewel dit standpunt misschien nogal extreem is, is het in sommige gevallen wel juist.

Schijfstation

Dit is een apparaat dat gegevens leest van en schrijft naar een schijf.

Een harde-schijfstation leest en schrijft harde schijven.

Een diskettestation opent diskettes.

Schijfstations kunnen intern (binnen de behuizing van een computer) of extern zijn (in een afzonderlijke behuizing die op de computer wordt aangesloten).

Downloaden

Om gegevens (meestal een volledig bestand) te kopiëren van een hoofdbron naar een randapparaat. De term wordt vaak gebruikt om het proces te beschrijven waarbij een bestand van een on line-service wordt gekopieerd naar de eigen computer. Downloaden kan ook verwijzen naar het kopiëren van een bestand van een netwerkbestandsserver naar een computer in het netwerk.

E-mail

Elektronische post. Een dienst die berichten naar computers verzendt via lokale of globale netwerken.

Gebeurtenissen

Een actie of gebeurtenis die door een programma wordt gedetecteerd. Gebeurtenissen kunnen gebruikersacties zijn, zoals het klikken met de muis of het indrukken van een toets, of systeemgebeurtenissen, zoals een tekort aan geheugen.

Vals positief

Doet zich voor wanneer een scanner een bestand ten onrechte beschouwt als geïnfecteerd.

Bestandsnaamextensie

Het gedeelte van een bestandsnaam achter de punt, waarmee het gegevenstype dat in het bestand is opgeslagen wordt aangeduid.

Heel wat besturingssystemen, zoals Unix, VMS en MS-DOS, maken gebruik van bestandsnaamextensies. Ze gebruiken doorgaans één tot drie letters (sommige oude besturingssystemen ondersteunen niet meer dan drie letters). Voorbeelden hiervan zijn "c" voor C-broncode, "ps" voor PostScript, "txt" voor tekst zonder opmaak.

Heuristisch

Een methode voor het identificeren van nieuwe virussen op basis van regels. Deze scanmethode steunt niet op specifieke virussignatures. Het voordeel van de heuristische scan is dat hij zich niet laat misleiden door een nieuwe variant van een bestaand virus. Dit type kan echter af en toe een verdachte code rapporteren in normale programma's, zodat de zogenoemde "valse positieve" rapporten worden gegenereerd.

IP

Internet Protocol - Een routeerbaar protocol in de TCP/OP-protocolreeks die verantwoordelijk is voor de IP-adressering, routing en de fragmentatie en defragmentatie van IP-pakketten.

Java-applet

Een Java-programma dat is ontwikkeld om alleen op een webpagina te worden uitgevoerd. Om een applet op een webpagina te gebruiken, geeft u de naam van het applet op en de grootte (lengte en breedte in pixels) die het applet kan gebruiken. Wanneer de webpagina wordt geopend, downloadt de browser het applet van een server en voert hij het uit op de computer van de gebruiker (de client). Applets onderscheiden zich van toepassingen omdat ze worden beheerd door een streng beveiligingsprotocol.

Zelfs wanneer applets op de client worden uitgevoerd kunnen ze, bijvoorbeeld, geen gegevens lezen van of schrijven naar de computer van de client. Bovendien worden applets verder beperkt zodat ze alleen gegevens kunnen lezen van en schrijven naar hetzelfde domein waarvan ze worden bediend.

Macrovirus

Een type computervirus dat is gecodeerd als een macro die in een document is ingesloten. Talrijke toepassingen, zoals Microsoft Word en Excel, ondersteunen krachtige macrotalen.

Met deze toepassingen kan u een macro in een document insluiten, en die macro telkens laten uitvoeren wanneer het document wordt geopend.

Mailclient

Een e-mailclient is een toepassing waarmee u e-mail kan verzenden en ontvangen.

Geheugen

Interne opslaggebieden in de computer. De term geheugen staat voor gegevensopslag die in de vorm van chips wordt geleverd. Het woord opslag wordt gebruikt voor geheugen dat aanwezig is op tapes of schijven. Elke computer wordt geleverd met een bepaalde hoeveelheid fysiek geheugen, dat meestal het hoofdgeheugen of RAM wordt genoemd.

Niet-heuristisch

Deze scanmethode steunt op specifieke virussignaturen. Het voordeel van de niet-heuristische scan is dat hij zich niet laat misleiden door iets dat kan lijken op een virus en dat hij geen vals alarm genereert.

Ingepakte programma's

Een bestand in een gecomprimeerd formaat. Talrijke besturingssystemen en toepassingen beschikken over opdrachten waarmee u bestanden kunt inpakken,

zodat ze minder geheugen in beslag nemen. Veronderstel bijvoorbeeld dat u een tekstbestand hebt dat tien opeenvolgende spatietekens bevat. Normaal zou dit tien bytes opslagruimte vereisen.

Een programma dat bestanden inpakt kan echter de spatietekens vervangen door een speciaal spatiereeks-teken, gevolgd door het aantal spaties dat wordt vervangen. In dit geval hebben de tien spaties slechts twee bytes nodig. Dit is slechts één inpaktechniek, maar er zijn er veel meer.

Pad

De exacte weg naar een bestand op een computer. Deze weg wordt doorgaans beschreven door middel van het hiërarchische bestandssysteem van boven naar beneden.

De route tussen twee willekeurige punten, zoals het communicatiekanaal tussen twee computers.

Phishing

Het onder valse voorwendselen verzenden van een e-mail aan een gebruiker, waarbij de indruk wordt gewekt dat het bericht afkomstig is van een bestaande onderneming, in een poging de gebruiker persoonlijke gegevens te ontfutselen die zullen worden gebruikt voor identiteitsroof. In het e-mailbericht wordt de gebruiker doorverwezen naar een website voor het updaten van persoonlijke gegevens, zoals wachtwoorden en creditcard-, BSN- en bankrekeningnummers, die reeds in het bezit zijn van de rechtmatige organisatie. De website is echter nep en alleen opgezet om de gebruikersgegevens te stelen.

Polymorf virus

Een virus dat zijn vorm wijzigt bij elk bestand dat het infecteert. Aangezien zij geen consequent binair patroon hebben, zijn dergelijke virussen moeilijk te identificeren.

Poort

Een interface op een computer waarop u een apparaat kan aansluiten. PC's hebben verschillende types poorten. Intern zijn er verschillende poorten voor het aansluiten van schijfstations, beeldschermen en toetsenborden. Extern beschikken PC's over poorten voor het aansluiten van modems, printers, muizen en andere randapparatuur.

Bij TCP/IP- en UDP-netwerken, zijn ze een eindpunt voor een logische verbinding. Het poortnummer duidt aan over welk type poort het gaat. Poort 80 wordt bijvoorbeeld gebruikt voor HTTP-verkeer.

Rapportbestand

Een bestand dat de acties weergeeft die zich hebben voorgedaan. BitDefender houdt een rapportbestand bij met het gescande pad, het aantal gescande mappen, archieven en bestanden, en het aantal gevonden geïnfecteerde en verdachte bestanden.

Rootkit

Een rootkit is een set softwarehulpprogramma's die toegang biedt tot een systeem op beheerniveau. Deze term werd voor het eerst gebruikt voor UNIX-besturingssystemen en verwees naar opnieuw gecompileerde hulpprogramma's die indringers beheerrechten verleende, zodat ze hun aanwezigheid konden verbergen zodat ze onzichtbaar bleven voor systeembeheerders.

De belangrijkste rol van rootkits is het verbergen van processen, bestanden, aanmeldingen en logboeken. Ze kunnen ook gegevens onderscheppen van terminals, netwerkverbindingen of randapparaten als ze de geschikte software bevatten.

Rootkits zijn in wezen niet kwaadaardig. Systemen en zelfs sommige toepassingen verbergen kritieke bestanden met de hulp van rootkits. Ze worden echter het vaakst gebruikt om malware of de aanwezigheid van een indringer op het systeem te verbergen. In combinatie met malware, vormen rootkits een ernstige bedreiging voor de integriteit en beveiliging van een systeem. Ze kunnen het verkeer controleren, achterpoortjes in het systeem maken, bestanden en logboeken wijzigen en detectie vermijden.

Script

Script, een andere term voor een macro of batchbestand, is een lijst opdrachten die kunnen worden uitgevoerd zonder tussenkomst van de gebruiker.

Spam

Elektronische junkmail of berichten van junknieuwsgroepen. Algemeen bekend als ongewenste e-mail.

Spyware

Elke software die heimelijk gebruikersgegevens verzamelt via de internetverbinding van de gebruikers zonder dat hij/zij zich hiervan bewust is, doorgaans voor reclamedoeleinden. Spywaretoepassingen worden doorgaans gebundeld als een verborgen onderdeel van freeware- of sharewareprogramma's die kunnen worden gedownload van het internet. We moeten echter wel vermelden dat de meeste shareware- en freewaretoepassingen geen spyware bevatten. Zodra de spyware is geïnstalleerd, worden de activiteiten van de gebruiker op het Internet gevolgd en wordt deze informatie op de achtergrond naar iemand anders doorgestuurd.

Spyware kan ook informatie verzamelen over e-mailadressen en zelfs wachtwoorden en creditcardnummers.

Spyware is vergelijkbaar met een Trojaans paard omdat gebruikers ook in dit geval het product onbewust installeren wanneer ze een ander programma installeren. Een veel voorkomende manier om slachtoffer te worden van spyware is bepaalde P2P-bestandsuitwisselingsprogramma's te downloaden.

Naast het feit dat deze methode onethisch is en een inbreuk op de privacy van de gebruiker betekent, steelt spyware van de gebruiker door de geheugenbronnen van de computer te gebruiken en bandbreedte te verbruiken wanneer de informatie naar de thuisbasis van de spyware wordt verzonden via de internetverbinding van de gebruiker. Aangezien spyware geheugen- en systeembronnen gebruikt, kunnen de toepassingen die op de achtergrond worden uitgevoerd leiden tot systeemfouten of een algemene systeeminstabiliteit.

Opstartitems

Elk bestand in deze map wordt geopend wanneer de computer wordt gestart. Een opstartitem kan bijvoorbeeld een opstartscherm zijn, een geluidsbestand dat moet worden afgespeeld wanneer de computer voor de eerste maal opstart, een herinneringsagenda of een toepassingsprogramma. In normale omstandigheden wordt een alias van een bestand in deze map geplaatst, en niet het bestand zelf.

Systeemvak

Het systeemvak, dat met Windows 95 werd ingevoerd, bevindt zich in de taakbalk van Windows (doorgaans onderaan naast de klok) en bevat miniatuurpictogrammen die systeemfuncties zoals fax, printer, modem, volume en meer, gemakkelijk toegankelijk maken. Dubbelklik of klik met de rechtermuisknop op een pictogram om de details en de besturingselementen te bekijken en te openen.

TCP/IP

Transmission Control Protocol/Internet Protocol - Een reeks netwerkprotocollen, wijdverspreid gebruikt op het Internet, die communicatie bieden tussen onderling verbonden computernetwerken met verschillende hardware-architecturen en diverse besturingssystemen. TCP/IP bevat standaarden voor de manier waarop computers communiceren en regels voor het aansluiten van netwerken en het routeren van het verkeer.

Trojaans paard

Een destructief programma dat zich voordoet als een goedaardige toepassing. In tegenstelling tot virussen, maken ze geen kopie van zichzelf, maar ze kunnen wel even vernietigend zijn. Een van de meest verraderlijke types van de Trojaanse

paarden is een programma dat beweert dat het uw computer kan bevrijden van virussen, maar dat in werkelijkheid virussen op uw computer installeert.

De term komt uit een verhaal uit de Illias van Homerus, dat vertelt over de Grieken die hun vijanden, de Trojanen een reusachtig houten paard schonken, zogenaamd als een vredesgebaar. Maar nadat de Trojanen het paard binnen de stadsmuren hadden gesleept, kwamen de Griekse soldaten, die in de holle romp van het paard verborgen zaten te voorschijn en openden ze de poorten van de stad, zodat hun landgenoten Troje konden binnendringen en veroveren.

Update

Een nieuwe versie van een software- of hardwareproduct, dat werd ontwikkeld om een oudere versie van hetzelfde product te vervangen. Daarnaast zullen de installatieroutines voor updates vaak controleren of er reeds een oudere versie van het product op uw computer is geïnstalleerd. Is dat niet het geval, dan kunt u de update niet installeren.

BitDefender heeft zijn eigen updatemodule waarmee u handmatig kunt controleren op updates of die het product automatisch kan updaten.

Virus

Een programma of een deel van een code die op uw computer wordt geladen zonder uw medeweten en tegen uw wil wordt uitgevoerd. De meeste virussen kunnen zichzelf ook dupliceren. Alle computervirussen zijn door de mens gemaakt. Een eenvoudig virus dat zichzelf steeds opnieuw kan dupliceren is relatief eenvoudig te maken. Zelfs een dergelijke eenvoudig virus is gevaarlijk aangezien het snel al het beschikbare geheugen zal opgebruiken en het systeem zal blokkeren; Een nog gevaarlijker type is een virus dat in staat is zichzelf te verzenden via netwerken en beveiligingssystemen te omzeilen.

Virusdefinitie

Het binaire patroon van een virus, dat wordt gebruikt door het antivirusprogramma om het virus te detecteren en uit te schakelen.

Worm

Een programma dat zich verspreidt via een netwerk en zichzelf ondertussen reproduceert. Dit type kan zich niet vasthechten aan andere programma's.