bitdefender

INTERNET SECURITY 2008

Gebruiksaanwijzing

BitDefender Internet Security 2008
Gebruiksaanwijzing

Uitgegeven 2007.12.05

Wettelijke verklaring


bitdefender

Inhoudsopgave

Licentie en garantie

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.

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 de wetten op auteursrecht en internationale verdragen inzake auteursrecht en andere wetten en verdragen inzake intellectuele eigendom. Voor BitDefender wordt een licentie verleend. Het programma wordt dus 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.

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 het adres 5, Fabrica de Glucoza str., 72322-Sector 2, Boekarest, Roemenië of op het telefoonnr.: 40-21-2330780 of Fax: 40-21-2330763, e-mailadres: office@bitdefender.com.

Voorwoord

Deze handleiding is bedoeld voor alle gebruikers die voor **BitDefender Internet Security 2008** hebben gekozen als een beveiligingsoplossing voor hun computers. De informatie die in dit boek wordt geleverd is niet alleen geschikt voor geavanceerde computergebruikers, maar is ook gemakkelijk te begrijpen door iedereen die met Windows kan werken.

Dit boek biedt u een beschrijving van **BitDefender Internet Security 2008**, 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 Internet Security 2008** 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. xii)	Dit is een interne koppeling naar een locatie in het document.
`filename`	Bestandsnamen en mappen worden afgedrukt met een `enkelspatielettertype`.

Weergave	Beschrijving
option	Alle productopties worden afgedrukt met **harde** tekens.
`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 Internet Security 2008**. 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 beveiligingsbeheer. Een gedetailleerde voorstelling van de beveiligingsmogelijkheden die door BitDefender worden geboden. De hoofdstukken

bieden een gedetailleerde verklaring van alle opties van de console met de geavanceerde instellingen. U wordt geleerd hoe u alle BitDefender-modules te configureren en gebruiken om uw computer op een efficiënte manier te beveiligen tegen elk type bedreiging (malware, spam, hackers, ongepaste inhoud, enz.).

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.

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

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. Installatie BitDefender Internet Security 2008

Het hoofdstuk **BitDefender Internet Security 2008 installeren** van deze handleiding bevat de volgende onderwerpen:

- Systeemvereisten
- Installatiestappen
- Initiële configuratiewizard
- Upgrade
- BitDefender repareren of verwijderen

1.1. Systeemvereisten

Voor een correcte werking van het product, moet u vóór de installatie ervoor zorgen dat een van de volgende besturingssystemen op uw computer is geïnstalleerd en aan de overeenkomende systeemvereisten wordt voldaan:

- Besturingsplatform: Windows 2000 SP4 / XP SP2 32b & 64b / Vista 32b & 64b; Internet Explorer 6.0 (of hoger)
- Ondersteunde e-mailclients: Microsoft Outlook 2000 / 2003 / 2007; Microsoft Outlook Express; Microsoft Windows Mail; Thunderbird 1.5 en 2.0

Windows 2000

- 800 MHz processor of hoger
- Minimum 256 MB RAM-geheugen (512 MB aanbevolen)
- Minimum 60 MB beschikbare harde schijfruimte

Windows XP

- 800 MHz processor of hoger
- Minimum 256 MB RAM-geheugen (1 GB aanbevolen)
- Minimum 60 MB beschikbare harde schijfruimte

Windows Vista

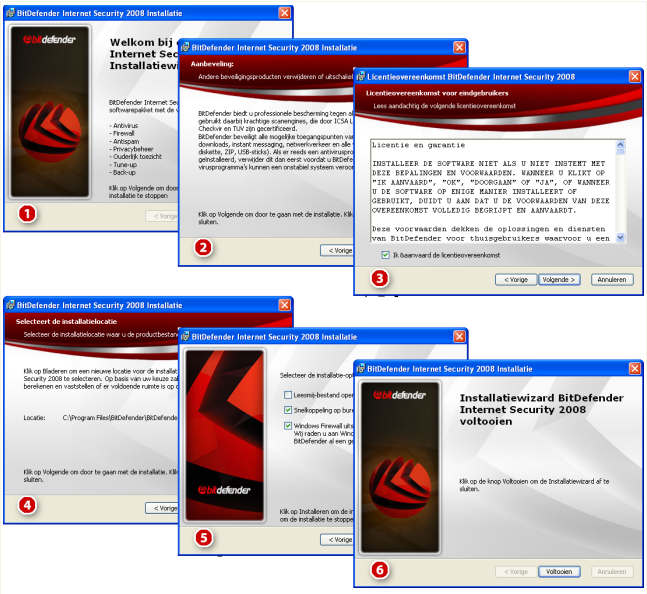
- 800 MHz processor of hoger
- Minimum 512 MB RAM-geheugen (1 GB aanbevolen)
- Minimum 60 MB beschikbare harde schijfruimte

BitDefender Internet Security 2008 kan voor een evaluatie worden gedownload van de BitDefender website: http://www.bitdefender.com.

1.2. Installatiestappen

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 op nieuwere versies van het installatiepakket. 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 Internet Security 2008 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 Internet Security 2008 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 de andere gedetecteerde 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, selecteer **Ik aanvaard de voorwaarden van de Licentieovereenkomst** en klik op **Volgende**. Als u niet instemt met deze voorwaarden, klik dan op **Annuleren**. Het installatieproces wordt afgebroken en u verlaat de installatie.
4. BitDefender Internet Security 2008 wordt standaard geïnstalleerd onder `C:\Program Files\BitDefender\BitDefender 2008`. Als u het installatiepad wilt wijzigen, klikt u op **Bladeren** en selecteert u de map waarin u BitDefender Internet Security 2008 wilt installeren.

   Klik op **Volgende**.
5. Selecteer de opties met betrekking tot het installatieproces. Sommige opties zullen standaard zijn geïnstalleerd.
   - **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 v10 Plus 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 Firewall uitschakelen** - hiermee schakelt u de Windows Firewall uit.

     Belangrijk
     Wij raden u aan Windows Firewall uit te schakelen omdat BitDefender Internet Security 2008 al een geavanceerde firewall bevat. Het uitvoeren van twee firewalls op dezelfde computer kan problemen veroorzaken.

   - **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.

Belangrijk

Tijdens het installatieproces verschijnt een wizard. De wizard helpt u bij het registreren van **BitDefender Internet Security 2008**, het maken van een BitDefender-account en het instellen van BitDefender voor het uitvoeren van belangrijke beveiligingstaken. Voltooi het door de wizard begeleide proces om naar de volgende stap te gaan.

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.

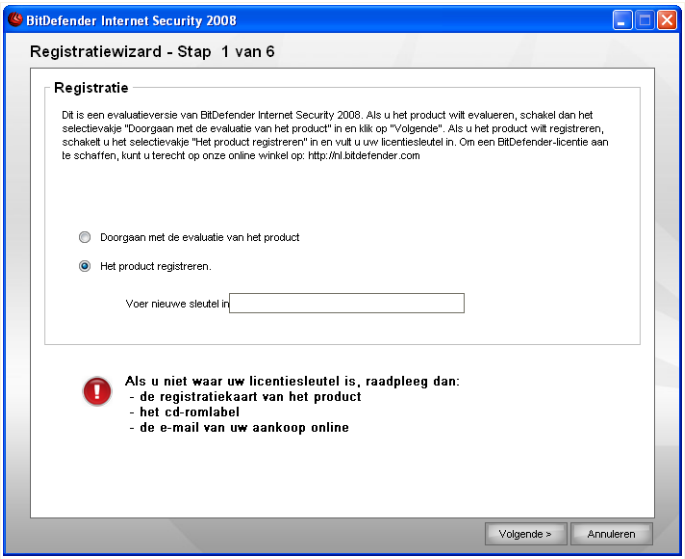
   Als u de standaardinstellingen voor het installatiepad hebt geaccepteerd, ziet u in `Program Files` een nieuwe map, genaamd `BitDefender`, met daarin de submap `BitDefender 2008`.

1.3. Initiële configuratiewizard

Tijdens het installatieproces verschijnt een wizard. De wizard helpt u bij het registreren van **BitDefender Internet Security 2008**, het maken van een BitDefender-account en het instellen van BitDefender voor het uitvoeren van belangrijke beveiligingstaken.

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 Internet Security 2008 is geïnstalleerd.

1.3.1. Stap 1/6 - BitDefender Internet Security 2008 registreren



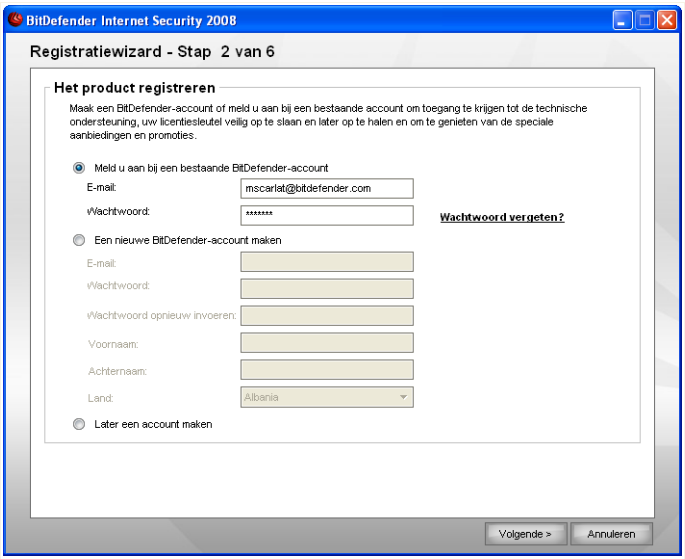
Registratie

Selecteer **Het product registreren** om **BitDefender Internet Security 2008** te registreren. Geef de licentiesleutel op in het veld **Voer nieuwe sleutel in**.

Selecteer **Doorgaan met de evaluatie van het product** om het product verder te testen.

Klik op **Volgende**.

1.3.2. Stap 2/6 - Een BitDefender-account maken



Account maken

Ik heb geen BitDefender-account

Om van de gratis technische ondersteuning en andere gratis diensten van BitDefender te kunnen genieten, moet u een account maken. Selecteer **Een nieuwe BitDefender-account maken** en geef de vereiste informatie op. De gegevens die u hier opgeeft blijven vertrouwelijk.

Opmerking
Als u later een account wilt maken, selecteert u de overeenkomende optie.

Voer een geldig e-mailadres in het veld **E-mail** in. Bedenk een wachtwoord en typ dit in het veld **Wachtwoord**. Bevestig het wachtwoord in het veld **Wachtwoord herhalen**. Gebruik het e-mailadres en het wachtwoord om aan te melden op uw account op http://myaccount.bitdefender.com.

Opmerking
Het wachtwoord moet minstens vier tekens bevatten.

Vul uw voornaam, achternaam en het land waarin u woont in.

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.

Klik op **Volgende** om door te gaan of op **Annuleren** om de wizard af te sluiten.

Ik heb al een BitDefender-account

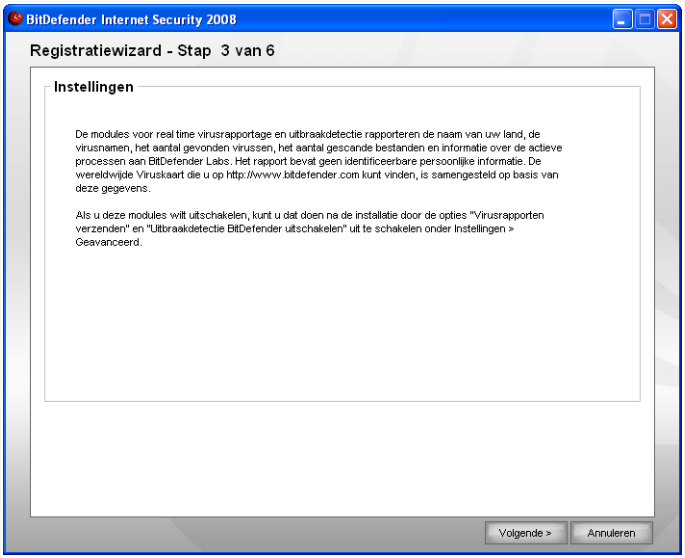
Als u al een actieve account hebt, selecteer dan **Inloggen op een bestaande BitDefender Account** en vul het e-mailadres en het wachtwoord van uw account in.

Opmerking
Als u een verkeerd wachtwoord hebt ingevuld, kunt u het opnieuw invullen nadat u hebt geklikt op **Next**. Klik op **Ok** om het wachtwoord opnieuw in te vullen of op **Annuleren** om het programma te verlaten.

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

Klik op **Volgende** om door te gaan of op **Annuleren** om de wizard af te sluiten.

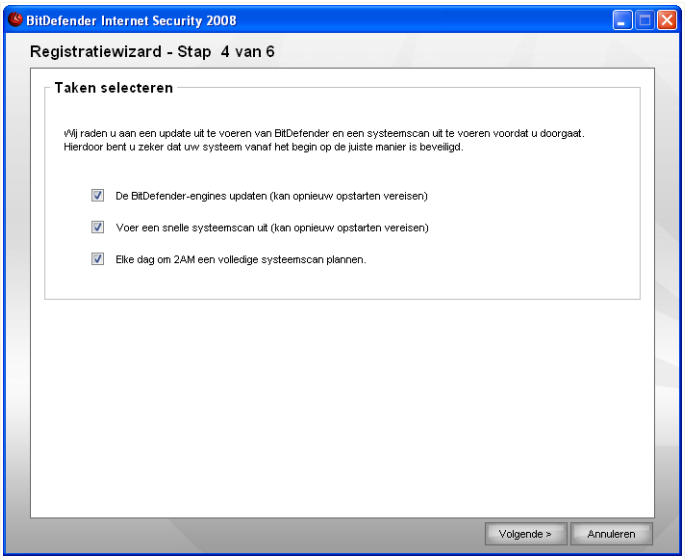
1.3.3. Stap 3/6 - Informatie over Real-Time Virusrapportage (RTVR)



RTVR-informatie

Klik op **Volgende** om door te gaan of op **Annuleren** om de wizard af te sluiten.

1.3.4. Stap 4/6 – De uit te voeren taken selecteren



Taakselectie

Stel BitDefender Antivirus v10 Plus in om belangrijke taken voor de beveiliging van uw systeem uit te voeren.

De volgende opties zijn beschikbaar:

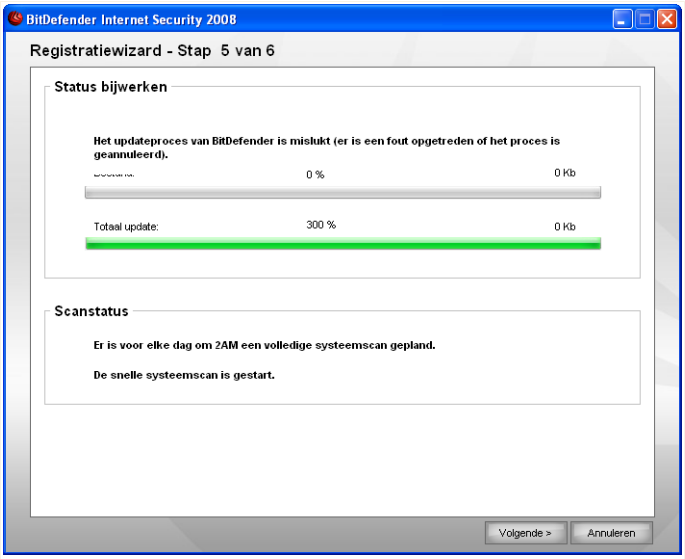
- **De BitDefender-engines updaten (kan opnieuw opstarten vereisen)** - bij de volgende stap wordt een update van de BitDefender-engines uitgevoerd om uw computer te beschermen tegen de meest recente bedreigingen.
- **Voer een snelle systeemscan uit (kan opnieuw opstarten vereisen)** - bij de volgende 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 of op **Annuleren** om de wizard af te sluiten.

1.3.5. Stap 5/6 - Wacht tot de taken zijn voltooid

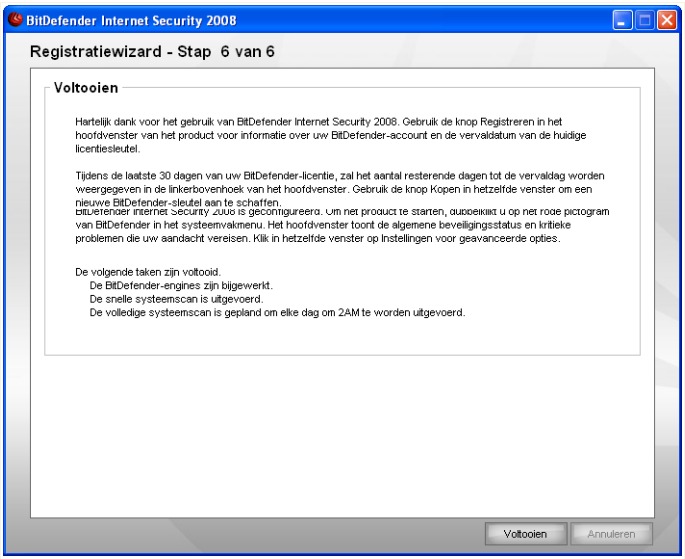


Taakstatus

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 of op **Annuleren** om de wizard af te sluiten.

1.3.6. Stap 6/6 – Overzicht weergeven



Voltooien

Dit is de laatste stap van de configuratiewizard.

Klik op **Installeren** om de installatie van het product te starten.

1.4. Upgrade

De upgradeprocedure kan op een van de volgende manieren worden uitgevoerd:

- **Installeren zonder de vorige versie te verwijderen - voor v8 of hoger, zonder Internet Security**

  Dubbelklik op het installatiebestand en volg de wizard die is beschreven in het gedeelte "*Installatiestappen*" (p. 3).

  Belangrijk
  Tijdens het installatieproces zal een foutbericht verschijnen dat wordt veroorzaakt door de `Filespy-service`. Klik op **OK** om door te gaan met de installatie.

- **Verwijder uw vorige versie en installeer de nieuwe - voor alle BitDefender-versies**

  U moet eerst uw vorige versie verwijderen, vervolgens uw computer opnieuw opstarten en daarna de nieuwe versie installeren zoals beschreven in het hoofdstuk "*Installatiestappen*" (p. 3).

Belangrijk
Als u een upgrade uitvoert vanaf BitDefender v8 of hoger, raden wij u aan de BitDefender-instellingen, de Vriendenlijst en de Spammerslijst op te slaan. Nadat de upgrade is voltooid, kunt u deze items laden.

1.5. BitDefender repareren of verwijderen

Als u **BitDefender Internet Security 2008** wilt repareren of verwijderen, volg dan dit pad vanaf het startmenu van Windows: **Start** → **Programma's** → **BitDefender 2008** → **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.

Belangrijk
Voordat u het product repareert, is het raadzaam de Vriendenlijst en de Spammerslijst op te slaan. U kunt ook de BitDefender-instellingen en de Bayes-database opslaan. Nadat de reparatie is voltooid, kunt u deze items opnieuw laden.

  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 Internet Security 2008 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

Door BitDefender te verwijderen, zult u niet langer beschermd zijn tegen virussen, spyware en hackers. Als u wilt dat Windows Firewall en Windows Defender (alleen op Windows Vista) worden ingeschakeld nadat u BitDefender hebt verwijderd, schakelt u de overeenkomende selectievakjes in.

Klik op **Verwijderen** om het verwijderen van BitDefender Internet Security 2008 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

2. Aan de slag

Uw computer is beveiligd zodra u BitDefender hebt geïnstalleerd. U kunt het Beveiligingscentrum van BitDefender openen om de status van de systeembeveiliging te controleren, voorzorgsmaatregelen te nemen of op elk ogenblik het product volledig te configureren.

Om toegang te krijgen tot het Beveiligingscentrum van BitDefender, gebruikt u het menu Start van Windows en volgt u het pad **Start → Programma's → BitDefender 2008 → BitDefender Internet Security 2008**. U kunt dit ook sneller doen door te dubbelklikken op het **BitDefender-pictogram** in het systeemvak.

BitDefender Beveiligingscentrum

Het Beveiligingscentrum van BitDefender bevat twee gebieden:

- Het gebied **Status**: bevat informatie over en helpt u met het oplossen van de zwakke punten in de beveiliging van uw computer. U kunt gemakkelijk zien hoeveel problemen uw computer kunnen beïnvloeden. Door op de overeenkomende rode knop **Alle probl. herst.** worden de zwakke punten van uw computer ter plaatse

opgelost of wordt u geholpen om ze gemakkelijk op te lossen. Tegelijkertijd zijn vier statusknoppen beschikbaar die overeenkomen met vier beveiligingscategorieën. Groene statusknoppen geven aan dat er geen risico is. Gele of rode knoppen geven gemiddelde of hoge beveiligingsrisico's aan. Om ze op te lossen klikt u op de gele/rode knop en klikt u achtereenvolgens op elke knop **Herstellen** of klikt u op de knop **Alles nu herst** button. Grijs geeft een niet-geconfigureerde component aan.

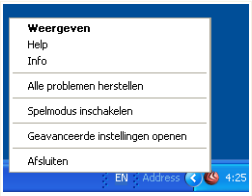
- Het gebied **Snelle taken**: helpt u uw systeem veilig te houden en uw gegevens te beveiligen.

Daarnaast bevat het Beveiligingscentrum van BitDefender meerdere nuttige snelkoppelingen.

Koppeling	*Beschrijving*
Kopen	Opent een pagina waar u het product kunt komen.
Mijn account	Opent de pagina van uw BitDefender-account.
Registreren	Opent de registratiewizard.
Help	Opent het Help-bestand.
Ondersteuning	Opent de webpagina van de BitDefender-ondersteuning.
Instellingen	Opent de console met de geavanceerde instellingen.
Geschiedenis	Opent een venster met de geschiedenis en gebeurtenissen van BitDefender.

2.1. BitDefender Icon in het Systeemvak

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



Contextmenu

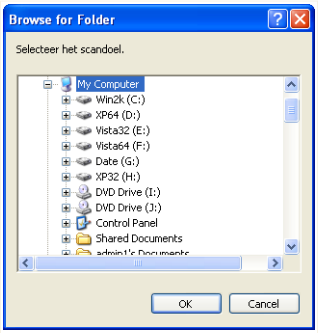
Als u dubbelklikt op dit pictogram, wordt het Beveiligingscentrum van BitDefender geopend. Door met de rechterknop op het pictogram te klikken, verschijnt een snelmenu waarmee u het BitDefender-product snel kunt beheren.

- **Weergeven** - opent het Beveiligingscentrum van BitDefender.
- **Help** - opent het Help-bestand.
- **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.
- **Geavanceerde instellingen openen** - biedt toegang tot de console met de geavanceerde instellingen.
- **Update nu** - start een directe update. Een nieuw venster verschijnt waarin u de updatestatus kan zien.
- **Afsluiten** - sluit de toepassing af.

2.2. 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 → Programma's → BitDefender 2008 → 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.

2.3. Spelmodus

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

- Alle BitDefender waarschuwingen en pop-ups zijn uitgeschakeld.
- Het BitDefender real-time beschermingsniveau is ingesteld op **Toegeeflijk**.
- De BitDefender Firewall is ingesteld op **Spelmodus**.

2.3.1. 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 `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.

2.3.2. Veranderen van de Spelmodus sneltoets

Volg deze stappen als u de sneltoets wilt veranderen:

1. Klik op **Instellingen** in het BitDefender Veiligheidscentrum om de instellingenconsole te openen.

Opmerking
U kan ook rechtsklikken op BitDefender pictogram in het systeemvak en **Open geavanceerde instellingen** selecteren.

2. Click **Geavanceerd**.
3. Stel de gewenste sneltoets in onder de **Sneltoets voor Spelmodus aan** 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 voor Spelmodus aan** te verwijderen, schakelt u de sneltoets uit.

3. Beveiligingsstatus

De beveiligingsstatus toont een systematisch georganiseerde en gemakkelijk beheerbare lijst van zwakke punten in de beveiliging van uw computer. BitDefender Internet Security 2008 zal u op de hoogte brengen wanneer een probleem de beveiliging van uw computer kan beïnvloeden.

Er zijn vier knoppen voor de beveiligingsstatus:

- **PC BEVEILIGING**
- **NETWERKBEVEILIGING**
- **IDENTITEITSCONTROLE**
- **OUDERLIJK TOEZICHT**

Aan de linkerzijde ziet u tegelijkertijd het aantal problemen dat de beveiliging van uw systeem beïnvloedt en een rode knop **Alle probl. herst.**.

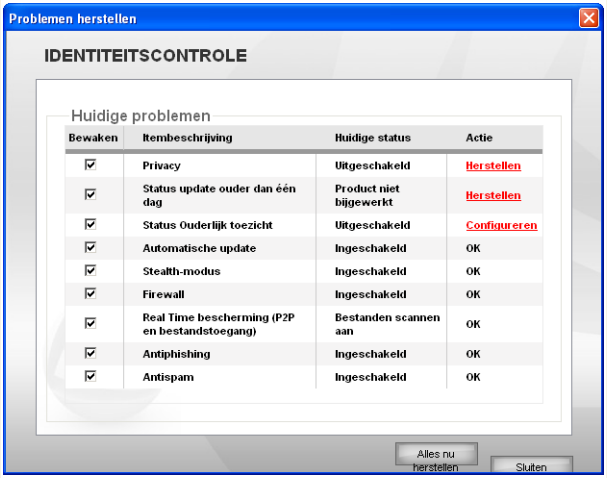
De vier statusknoppen kunnen, afhankelijk van het huidige beveiligingsniveau, in het groen, geel, rood of grijs worden weergegeven.

- **Groen** geeft een laag beveiligingsrisico voor uw computer aan.
- **Geel** geeft een gemiddeld beveiligingsrisico voor uw computer aan.
- **Rood** geeft een hoog beveiligingsrisico voor uw computer aan.
- **Grijs** geeft een niet-geconfigureerde component aan.

Het herstellen van beveiligingsproblemen vereist geen inspanningen en kan met één klik op de knop **Alle probl. herst.** worden uitgevoerd.

U zult een lijst van beveiligingsproblemen en een korte beschrijving van hun status zien.

Om een specifiek probleem te herstellen, klikt u op de overeenkomende knop **Herstellen**. Het probleem wordt onmiddellijk of nadat u de stappen van een wizard hebt gevolgd, opgelost. Als u beslist om ze allemaal op te lossen, klikt u op de knop **Alles nu herst** en volgt u de overeenkomende wizard.



Beveiligingsproblemen

Om de problemen op een later tijdstip te herstellen, klikt u op **Sluiten**.

Belangrijk
Voor elk probleem is er een selectievakje dat standaard is ingeschakeld. Als u wilt dat er geen rekening wordt gehouden met een specifiek probleem tijdens het berekenen van het beveiligingsrisico, moet u het overeenkomende selectievakje uitschakelen. Ga voorzichtig te werk wanneer u deze optie gebruikt. Het is namelijk heel gemakkelijk om het beveiligingsrisico waaraan uw computer is blootgesteld, te verhogen.

3.1. PC Beveiliging statusknop

Als de knop voor de beveiligingsstatus groen is, hoeft u zich geen zorgen te maken. Als de knop geel, rood of grijs is, betekent dit dat de computer is blootgesteld aan een gemiddeld of hoog beveiligingsrisico.

De kleur van de statusknoppen kan niet alleen wijzigen wanneer u de instellingen configureert die de beveiliging van uw computer kunnen beïnvloeden, maar ook wanneer u belangrijke taken vergeet uit te voeren. Als uw laatste systeemscan bijvoorbeeld oud is, zal de knop voor de beveiligingsstatus geel zijn. Als de scan zeer oud is, wordt de knop rood.

De onderstaande tabel biedt u informatie over de elementen waarmee rekening wordt gehouden bij het berekenen van het beveiligingsrisico.

Probleem	Kleur
De laatste systeemscan is oud	Geel
De laatste systeemscan is zeer oud	Rood
De real time-beveiliging is uitgeschakeld	Rood
Het antivirusbeveiligingsniveau is ingesteld op "Toegeeflijk"	Geel
Automatische update is uitgeschakeld	Rood
De laatste update is één dag oud	Rood
De antispam is uitgeschakeld.	Grijs

Volg deze stappen om de problemen op te lossen:

1. Klik op de knop voor de beveiligingsstatus.
2. Klik op de knoppen **Herstellen** om de problemen een voor een op te lossen of op de knop **Alles nu herst** om ze allemaal samen op te lossen.
3. Als een probleem niet er plaatse wordt opgelost, moet u de wizard volgen om het op te lossen.

3.2. Knop Netwerkbeveiligingsstatus

Als de knop voor de netwerkbeveiligingsstatus groen is, hoeft u zich geen zorgen te maken. Als de knop rood is, betekent dit dat de computer is blootgesteld aan een hoog beveiligingsrisico.

De onderstaande tabel biedt u informatie over de elementen waarmee rekening wordt gehouden bij het berekenen van het beveiligingsrisico.

Probleem	Kleur
De firewall is uitgeschakeld.	Rood
De stealth-modus is uitgeschakeld	Rood
De draadloze verbinding is niet beveiligd	Rood

Volg deze stappen om de problemen op te lossen:

1. Klik op de knop voor de netwerkbeveiligingsstatus.
2. Klik op de knoppen **Herstellen** om de problemen een voor een op te lossen of op de knop **Alles nu herst** om ze allemaal samen op te lossen.
3. Als een probleem niet er plaatse wordt opgelost, moet u de wizard volgen om het op te lossen.

3.3. Identiteitscontrole statusknop

Als de identiteitscontrole statusknop groen is, hoeft u zich nergens zorgen om te maken. Anderzijds, als de knop rood of grijs is, dan is er een hoog veiligheidsrisico op uw computer aanwezig.

De onderstaande tabel biedt u informatie over de elementen waarmee rekening wordt gehouden bij het berekenen van het beveiligingsrisico.

Probleem	*Kleur*
De privacybeveiliging is ingesteld op AAN	Groen
De privacybeveiliging is ingesteld op UIT	Rood
De privacybeveiliging is niet ingesteld	Grijs

Volg deze stappen om de problemen op te lossen:

1. Klik op de statusknop voor de privacy.
2. Klik op de knoppen **Herstellen** om de problemen een voor een op te lossen of op de knop **Alles nu herst** om ze allemaal samen op te lossen.
3. Als een probleem niet er plaatse wordt opgelost, moet u de wizard volgen om het op te lossen.

3.4. Knop Status Ouderlijk toezicht

Als de knop voor de beveiligingsstatus groen is, betekent dit dat Ouderlijk toezicht is ingeschakeld. Als de knop grijs is, is de optie uitgeschakeld.

Klik op de overeenkomende statusknop om Ouderlijk toezicht in te schakelen en klik vervolgens op de knop **Configureren**.

4. Snelle taken

Onder de vier statusknoppen vindt u het gebied **Snelle taken**.

4.1. Beveiliging

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

Klik op het tabblad **Beveiliging** om de beveiligingsmodule te openen.

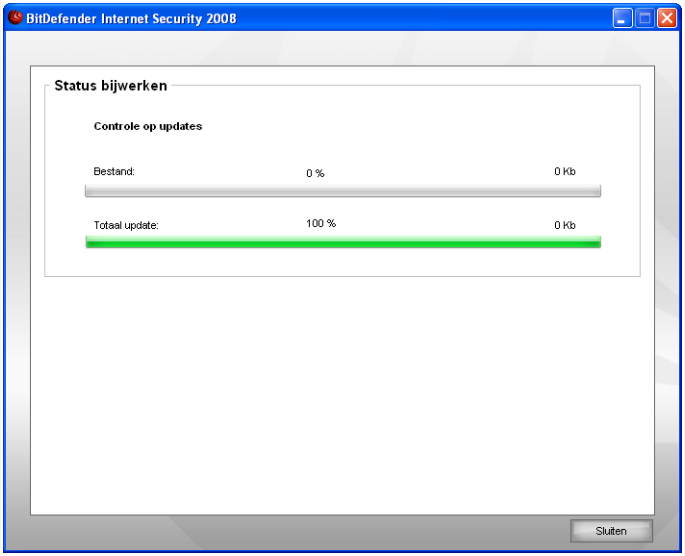
De volgende knoppen zijn beschikbaar:

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

4.1.1. 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 **Sluiten**. 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.

Computer opnieuw opstarten. Als het een belangrijke update betreft, wordt u gevraagd de computer opnieuw op te starten:

Als u niet telkens gevraagd wilt worden om na een update te herstarten, kruist u **Wacht met herstarten, in plaats van erom vragen**. Op deze manier blijft het product de

volgende keer dat na een update een herstart noodzakelijk is, doorwerken met de oude bestanden totdat u zelf het systeem opnieuw opstart.

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.

4.1.2. 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*
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.
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.

Opmerking

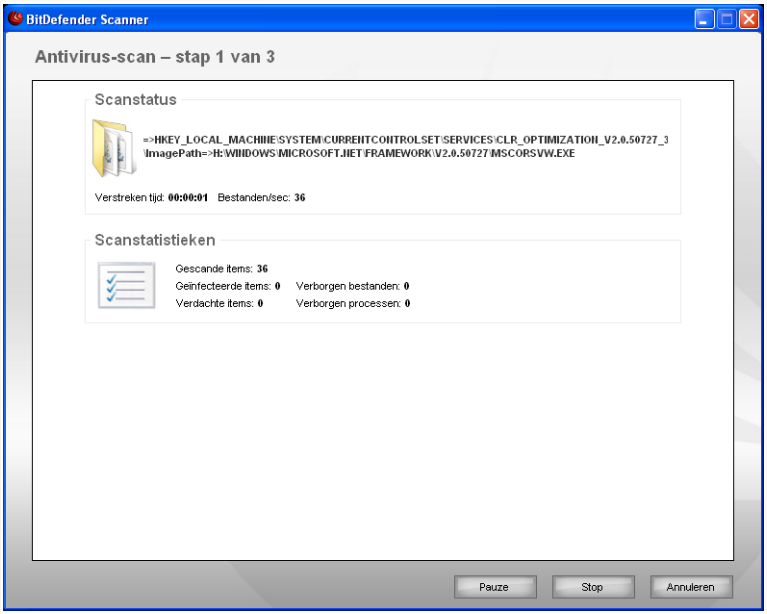
Omdat de taken **Diepe systeemscan** en **Volledige systeemscan** analyseren het volledige systeem. Het scannen kan enige tijd in beslag nemen. Wij raden u daarom aan deze taken uit te voeren met een lage prioriteit, of bij voorkeur wanneer uw systeem inactief is.

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.

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.

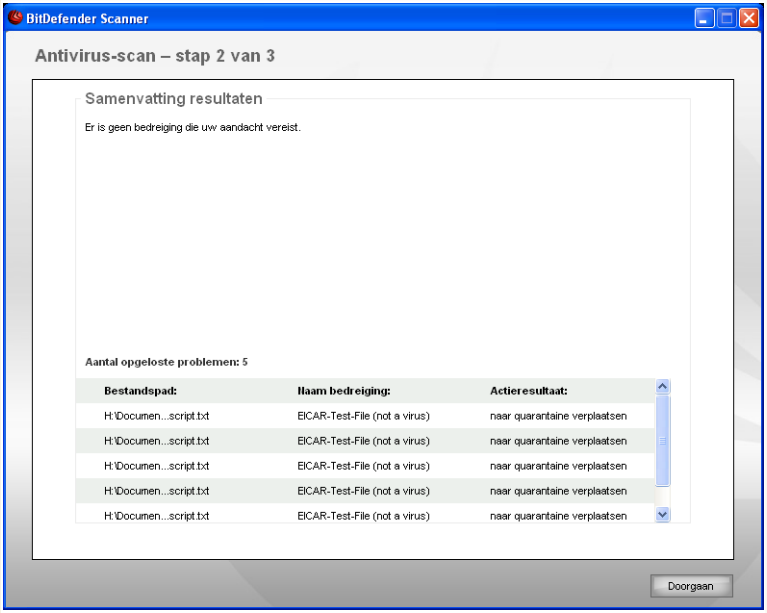
Klik op **Pauze** om het scanproces tijdelijk te stoppen. Om het scannen te hervatten, klikt u op **Hervatten**.

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 kunt 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 kunt een algemene actie selecteren die moet worden genomen voor elke groep problemen of u kunt afzonderlijke acties voor elk probleem selecteren.

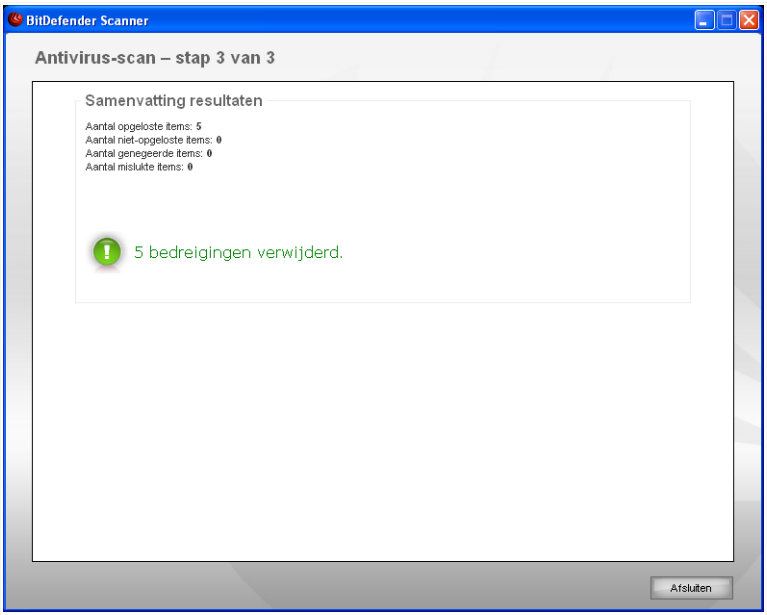
De volgende opties kunnen in het menu verschijnen.

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.



Overzicht

U kunt een samenvatting van de resultaten zien.

Als er tijdens het scannen verdachte bestanden zijn gedetecteerd, wordt u gevraagd ze naar het BitDefender Lab te sturen. Verdachte bestanden zijn bestanden die zijn gedetecteerd door de heuristische analyse en die mogelijk geïnfecteerd zijn met malware waarvan de signatuur nog niet bekend is.

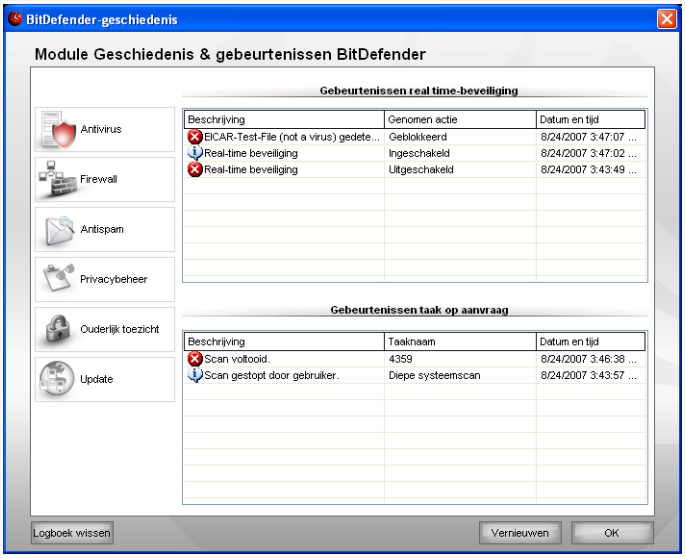
Het rapportbestand wordt automatisch opgeslagen in het gedeelte Logboeken in het venster **Eigenschappen** van de respectievelijke taak.

Waarschuwing

Als er niet-opgeloste problemen zijn, raden wij u aan contact op te nemen met het ondersteuningsteam van BitDefender op www.bitdefender.com.

5. Geschiedenis

De koppeling **Geschiedenis** onderaan in het venster van het Beveiligingscentrum van BitDefender opent een ander venster met de Geschiedenis en gebeurtenissen van BitDefender. Dit venster biedt u een overzicht van gebeurtenissen die betrekking hebben op de beveiliging. U kunt bijvoorbeeld gemakkelijk controleren of de update is gelukt, of er malware op uw computer is gevonden, of uw back-uptaken worden uitgevoerd zonder fouten, enz.



Gebeurtenissen

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

- **Antivirus**
- **Firewall**
- **Antispam**
- **Privacybeheer**
- **Ouderlijk toezicht**
- **Update**

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.

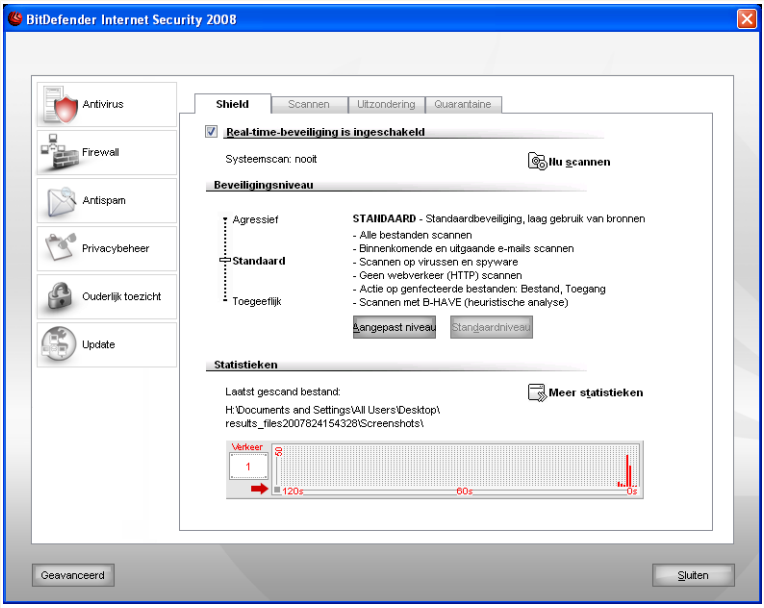
Klik op **Logboek wissen** als u de oude logboeken wilt verwijderen of klik op **Vernieuwen** om zeker te zijn dat de recentste logboeken worden weergegeven.

Geavanceerd beveiligingsbeheer

6. Aan de slag

BitDefender Internet Security 2008 wordt geleverd met een gecentraliseerde instellingsconsole waarmee geavanceerde configuratie en geavanceerd beheer van BitDefender mogelijk is.

Open de instellingsconsole en klik onderaan in het Beveiligingscentrum op de koppeling **Instellingen**.



Instellingsconsole

De instellingsconsole is onderverdeeld in modules: **Antivirus**, **Firewall**, **Antispam**, **Privacybeheer**, **Ouderlijk toezicht** en **Update**. Hiermee kunt u BitDefender gemakkelijk beheren op basis van het type beveiligingsprobleem dat wordt aangepakt.

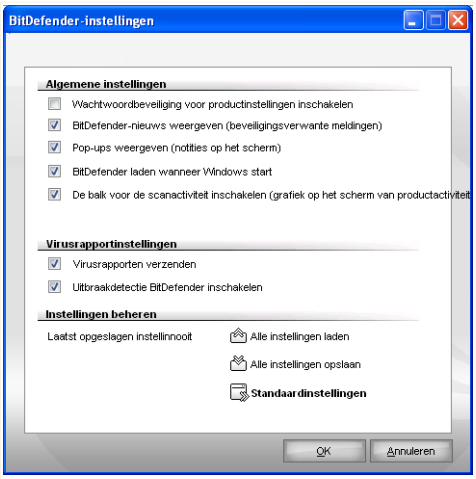
Aan de linkerzijde van de instellingsconsole ziet u de moduleselector:

- Antivirus - in deze sectie kunt u de **Antivirus**-module configureren.
- Firewall - in deze sectie kunt u de **Firewall**-module configureren.

- Antispam - in deze sectie kunt u de **Antispam**-module configureren.
- Identiteitscontrole - in deze sectie kunt u de module **Identiteitscontrole** configureren.
- Ouderlijk toezicht - in deze sectie kunt u de module **Ouderlijk toezicht** configureren.
- Update - in deze sectie kunt u de **Update**-module configureren.

6.1. Algemene instellingen configureren

Om de algemene instellingen te configureren voor BitDefender Internet Security 2008 en zijn instellingen te beheren, klikt u op **Geavanceerd**. Een nieuw venster wordt weergegeven.



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.

6.1.1. 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:

Wachtwoord invoeren

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.

Als u alleen om het wachtwoord gevraagd wilt worden voor het configureren van Ouderlijk Toezicht, moet u ook **Wachtwoord alleen vragen/toepassen voor de Ouderlijk Toezicht module**. Anderzijds, als er alleen een wachtwoord was ingesteld voor Ouderlijk Toezicht en u het kruisje voor deze optie verwijdert, zal het betreffende wachtwoord gevraagd worden voor het configureren van elke BitDefender optie.

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

- **Wachtwoord vragen voor inschakelen Ouderlijk Toezicht** - als deze optie is ingeschakeld en er is geen wachtwoord ingesteld, wordt u gevraagd een wachtwoord in te stellen bij het inschakelen van Ouderlijk Toezicht.
- **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.
- **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)** - schakelt de balk Scanactiviteit in/uit.

- **Sneltoets voor Spelmodus inschakelen** - staat het gebruik toe van een combinatie van toetsen (sneltoets) voor het aanzetten/uitzetten van de Spelmodus. De standaard sneltoets is `Alt+G`.

  U kan deze sneltoets op de volgende manier wijzigen:

  1. 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`).
  2. Typ in het invulveld de letter van de normale toets die u wilt gebruiken.

6.1.2. 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.

6.1.3. Instellingen beheren

Gebruik de knoppen **Alle instellingen opslaan** / **Alle instellingen laden** om de instellingen die u hebt gedefinieerd voor BitDefender op de gewenste locatie op te slaan / te laden. Op deze manier kunt u dezelfde instellingen gebruiken nadat u uw BitDefender-product opnieuw hebt geïnstalleerd of hebt gerepareerd.

Belangrijk
Alleen gebruikers met beheermachtigingen kunnen instellingen opslaan en laden.

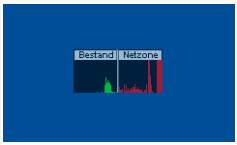
Om de standaardinstellingen te laden, klikt u op **Standaardinstellingen**.

6.2. De balk voor de scanactiviteit gebruiken

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

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

De rode balken die in de **Netzone** worden weergegeven, tonen het aantal overgedragen Kbytes (verzonden en ontvangen via het internet) per seconde op een schaal van 0 tot 100.



Activiteitenbalk

Opmerking
De balk voor de scanactiviteit zal aangeven wanneer de real time-beveiliging of de firewall is uitgeschakeld door een rood kruis over de overeenkomende zone (**Bestand** of **Netzone**) 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.

Opmerking
Meer informatie vindt u onder "*Scannen door slepen & neerzetten*" (p. 63).

Als u deze grafische voorstelling niet langer wilt zien, klik er dan op met de rechtermuisknop en selecteer **Verbergen**. Om dit venster volledig te verbergen, klikt u op **Geavanceerd** in de instellingsconsole en schakelt u het selectievakje naast **De balk voor de scanactiviteit inschakelen (grafiek op het scherm van productactiviteit)** uit.

7. Antivirus

BitDefender beveiligt uw computer tegen alle types malware (virussen, Trojanen, spyware, rootkits, enz.).

Naast het klassieke scannen op basis van malware-handtekeningen, zal BitDefender ook een heuristische analyse uitvoeren op de gescande bestanden. Heuristisch scannen heeft het doel nieuwe virussen te identificeren op basis van bepaalde patronen en algoritmen, voordat een virusdefinitie wordt gevonden. In dat geval zijn valse alarmberichten mogelijk. Wanneer een dergelijk bestand wordt gedetecteerd, wordt het beschouwd als verdacht. In deze gevallen raden wij u aan het bestand te verzenden naar het BitDefender lab voor analyse.

De BitDefender-bescherming is ingedeeld in twee categorieën:

- **Scannen bij toegang** - verhindert dat nieuwe malware-bedreigingen uw systeem binnenkomen. Dit wordt ook real time bescherming genoemd. De bestanden worden gescand op het ogenblik dat u ze gebruikt - bij toegang. BitDefender zal bijvoorbeeld een Worddocument scannen op bekende gevaren wanneer u het opent, en een e-mailbericht wanneer u het ontvangt.
- **Scannen op aanvraag** - hiermee kunt 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.

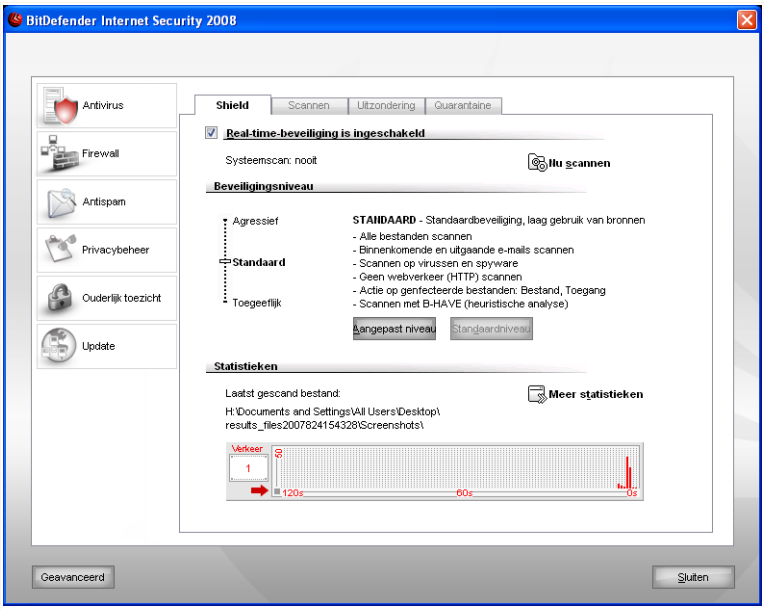
Het gedeelte **Antivirus** in deze gebruiksaanwijzing bevat de volgende onderwerpen:

- Scannen bij toegang
- Scannen op aanvraag
- Objecten die zijn uitgesloten van de scan
- Quarantaine

7.1. Scannen bij toegang

Scannen bij toegang, ook bekend als real time-beveiliging, houdt u computer beveiligd tegen alle types malware-bedreigingen door alle geopende bestanden, e-mailbestanden en communicatie via toepassingen voor instant messaging (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger) te scannen.

Om de real time-beveiliging te configureren en te controleren, klikt u in de instellingsconsole op **Antivirus>Shield**. Het volgende venster wordt geopend:



Real-time-beveiliging

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

In het onderste gedeelte van het venster kunt u de statistieken van de **Real-time-beveiliging** over de gescande bestanden en e-mailberichten bekijken. Klik op de knop **Meer statistieken** om een venster weer te geven met meer informatie over deze statistieken.

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

7.1.1. 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.

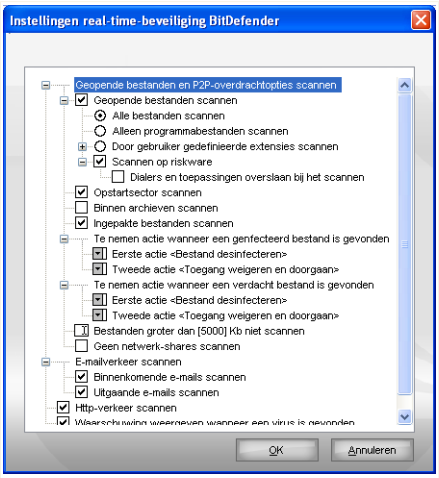
Om de standaard real time beveiligingsinstellingen toe te passen, klikt u op **Standaard**.

7.1.2. 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.
	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.

Optie		Beschrijving
	Toegang weigeren en doorgaan	Wanneer een geïnfecteerd bestand is gedetecteerd, zal de toegang tot dit bestand worden geweigerd.
	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.
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.

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

7.1.3. 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.

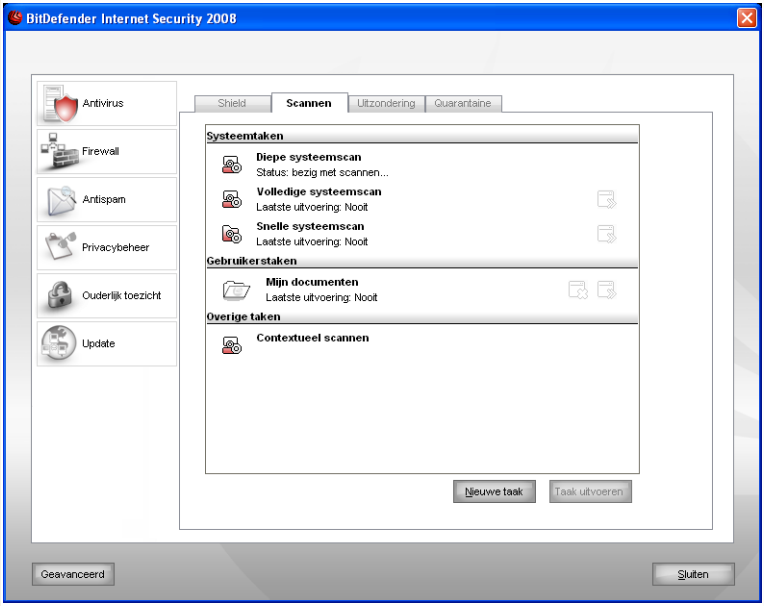
Waarschuwing
Dit is een kritiek beveiligingsprobleem. Wij raden u aan de real time-beveiliging zo kort mogelijk uit te schakelen. Als de real time-beveiliging is uitgeschakeld, wordt u niet beveiligd tegen malware-bedreigingen.

7.2. 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, klikt u in de instellingsconsole op **Antivirus>Scannen**. Het volgende venster wordt geopend:



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.

7.2.1. 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. 52).

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.

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.

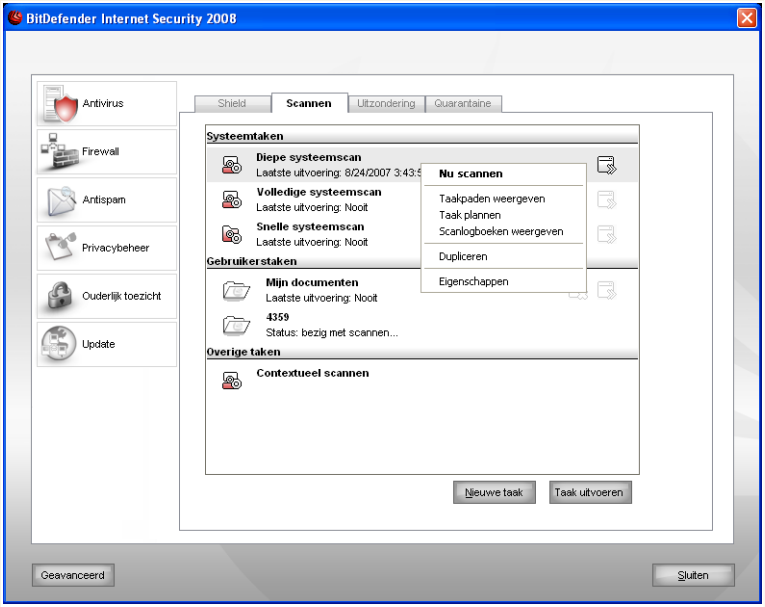
> ***Opmerking***
> Niet beschikbaar voor systeemtaken. U kunt geen systeemtaak verwijderen.

- **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.

7.2.2. Het snelmenu gebruiken

Voor elke taak is een



Snelmenu

snelmenu beschikbaar. Klik met de rechtermuisknop op de geselecteerde taak om deze te openen.

De volgende opdrachten zijn beschikbaar in het snelmenu:

- **Nu scannen** - voert de geselecteerde taak uit en start een onmiddellijke scan.
- **Scandoel wijzigen** - opent het venster **Eigenschappen**. Klik op het tabblad Scanpad 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.

- **Taak plannen** - opent het venster **Eigenschappen**. Klik op het tabblad Planner waar u de geselecteerde taak kunt plannen.
- **Log weergeven** - opent het venster **Eigenschappen**. Klik op het tabblad Scanlogboeken waar u de rapporten kunt bekijken die werden gegenereerd nadat de geselecteerde taak werd uitgevoerd.
- **Kopiëren** - dupliceert de geselecteerde taak.

Opmerking
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.

- **Eigenschappen** - 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 **Eigenschappen** en **Scanlogboeken weergeven** beschikbaar.

7.2.3. 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.

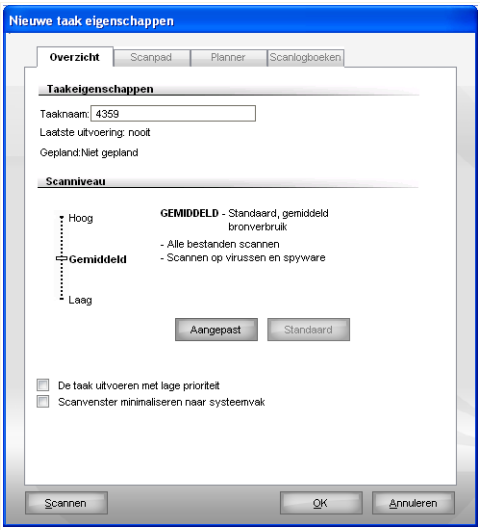
7.2.4. Scantaken configureren

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 "*Scanlogboeken weergeven*" (p. 68).

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. 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.

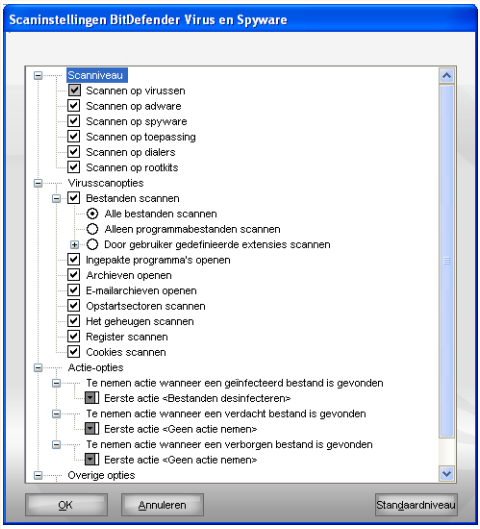
Optie	*Beschrijving*
De taak uitvoeren met lage prioriteit	Verlaagt de prioriteit van het scanproces. U zult andere programma's sneller kunnen uitvoeren en de tijd die nodig is om het scanproces te voltooien, verlengen.
Scanvenster naar systeemvak minimaliseren bij opstarten	Minimaliseert het scanvenster naar het systeemvak. Dubbelklik op het pictogram BitDefender om het programma te openen.

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 vijf categorieën:

- **Scanniveau**
- **Virusscanopties**
- **Actie-opties**
- **Overige opties**

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

  De volgende opties zijn beschikbaar:

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.
Scannen op spyware	Scant op bekende spyware-bedreigingen. Gedetecteerde bestanden zullen worden behandeld als geïnfecteerd.
Scannen op toepassing	Scant toepassingen (`.exe`- en `.dll`-bestanden).
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.

- Geef het type objecten op dat moet worden gescand (archieven, e-mailberichten, enz.) en definieer andere opties. Selecteer hiervoor bepaalde opties van de categorie **Virusscanopties**.

  De volgende opties zijn beschikbaar:

Optie		Beschrijving
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 ";".
Ingepakte programma's openen		Scant ingepakte bestanden.
Archieven openen		Scant binnen archieven.
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.

- Geef de acties op die moeten worden genomen voor de geïnfecteerde, verdachte of verborgen bestanden die in de categorie **Actie-opties** zijn gedetecteerd. U kunt een verschillende actie voor elke categorie opgeven.
  - 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	Desinfecteert geïnfecteerde bestanden.

Actie	Beschrijving
Bestanden verwijderen	Verwijdert onmiddellijk de geïnfecteerde bestanden, zonder enige waarschuwing.
Bestanden verplaatsen naar quarantaine	Verplaatst de geïnfecteerde bestanden naar de quarantaine.

- 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.

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.
Zichtbaar maken	Maakt verborgen bestanden zichtbaar.

Opmerking

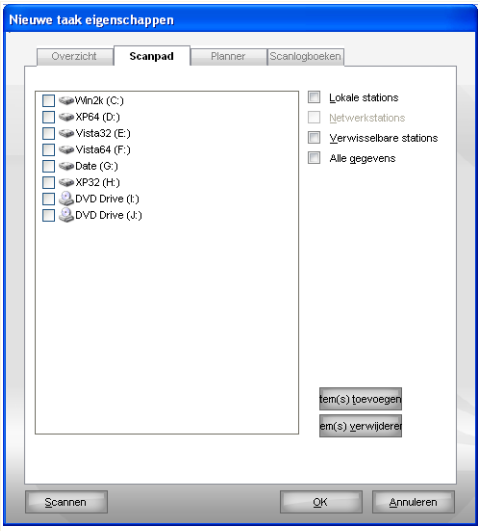
Als u de gedetecteerde bestanden wilt negeren of als de gekozen actie mislukt, moet u een actie selecteren in de scanwizard.

- Om te worden gevraagd alle verdachte bestanden naar het BitDefender lab te sturen nadat het scanproces is voltooid, schakelt u het selectievakje **Verdachte bestanden verzenden naar BitDefender Lab** in de categorie **Andere opties** in.

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 in te stellen van een scantaak van een specifieke gebruiker, klikt u rechts op de taak en selecteert u **Scandoel wijzigen**. 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.

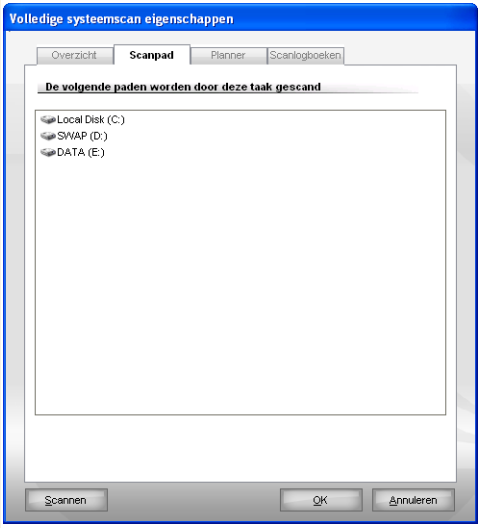
Opmerking
Activeer het selectievakje naast **Alle gegevens** als u uw volledige computer wilt scannen op virussen.

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

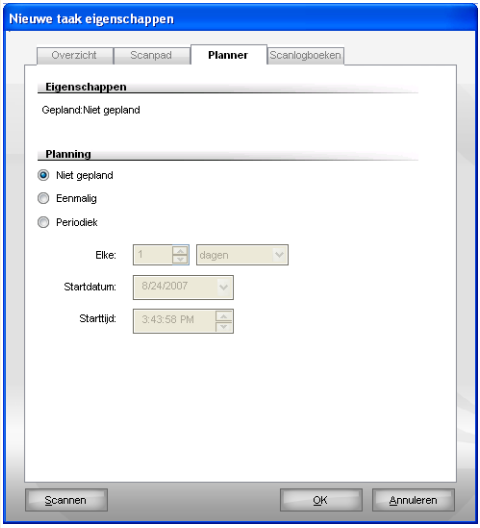
Volledige systeemscan en **Diepe systeemscan** scannen alle lokale schijven, terwijl **Snelle systeemscan** alleen de `Windows` en `Program Files` mappen scant.

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**.

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

7.2.5. 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 2008.
- 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.

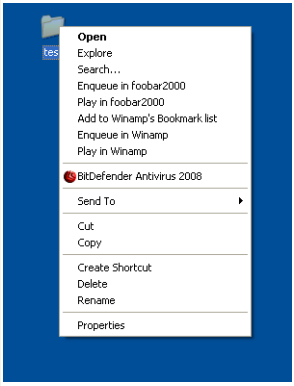
Gebruik een van de volgende methoden om een scantaak uit te voeren:

- 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. 64).

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

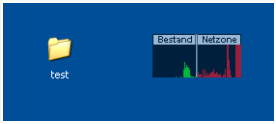
Klik met de rechtermuisknop op het bestand of de map die u wilt scannen en selecteer **BitDefender Antivirus 2008**.

BitDefender Scanner verschijnt en het scannen wordt gestart. Meer informatie vindt u onder "*BitDefender Scanner*" (p. 64).

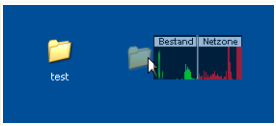
U kunt de scanopties wijzigen en de rapportbestanden weergeven door het venster **Eigenschappen** van de taak **Contextmenuscan** te openen.

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. 64).

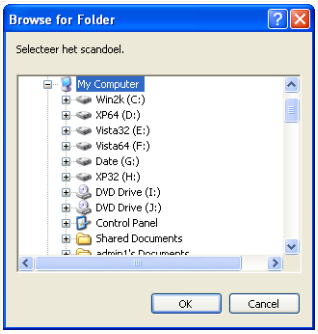
Handmatig scannen

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 2008 → BitDefender Handmatig scannen**.

Het volgende venster wordt geopend:



Handmatig scannen

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

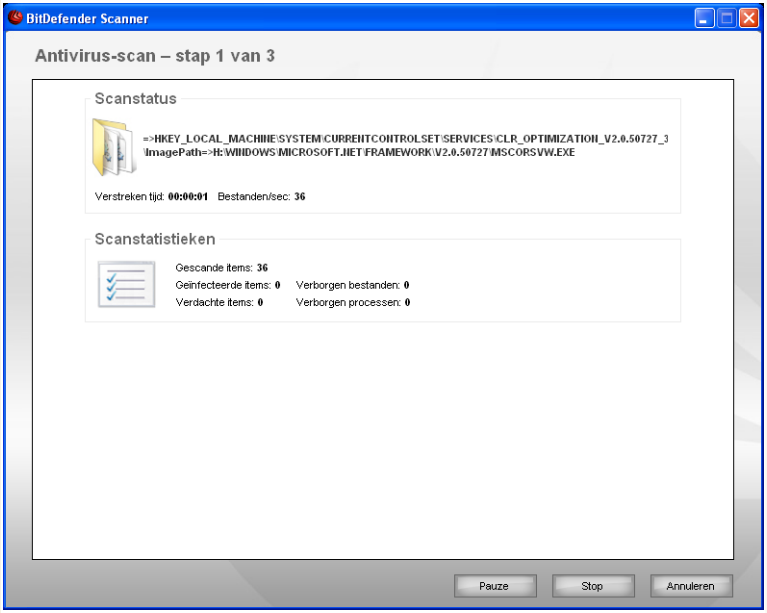
BitDefender Scanner verschijnt en het scannen wordt gestart. Meer informatie vindt u onder "*BitDefender Scanner*" (p. 64).

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.

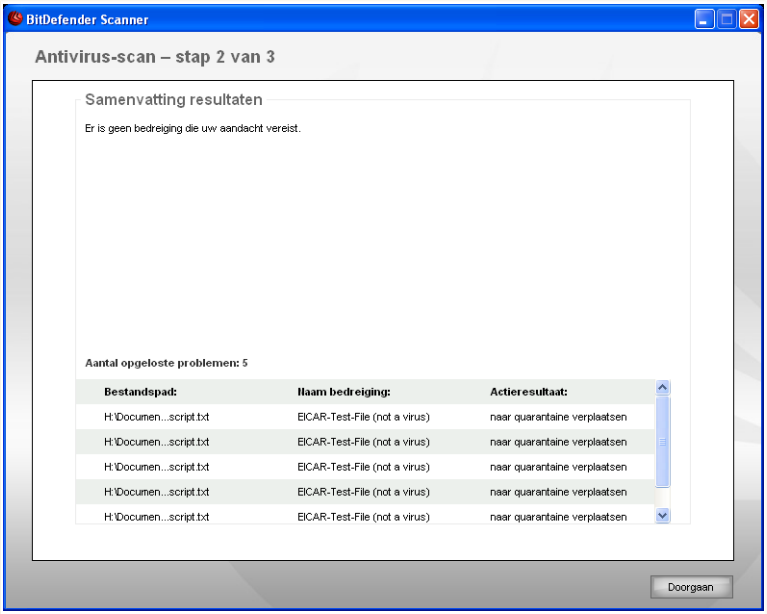
Klik op **Pauze** om het scanproces tijdelijk te stoppen. Om het scannen te hervatten, klikt u op **Hervatten**.

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 kunt 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 kunt een algemene actie selecteren die moet worden genomen voor elke groep problemen of u kunt afzonderlijke acties voor elk probleem selecteren.

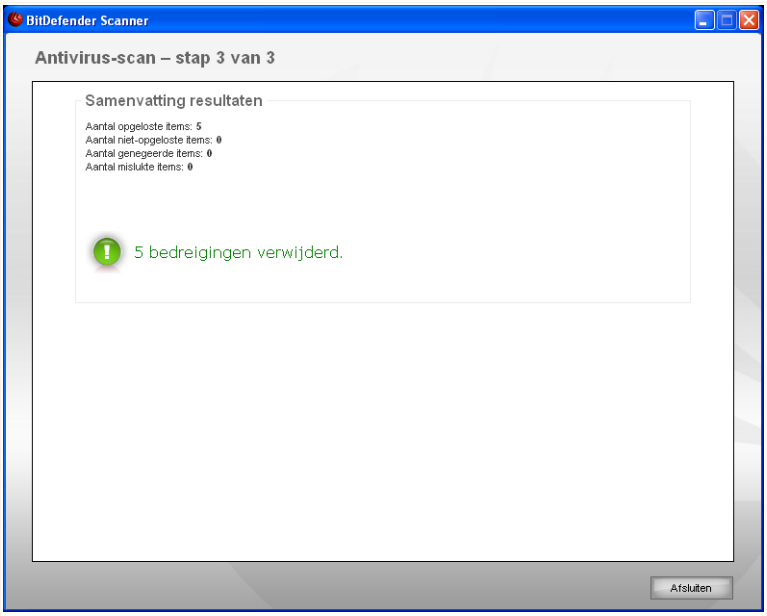
De volgende opties kunnen in het menu verschijnen.

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.



Overzicht

U kunt een samenvatting van de resultaten zien.

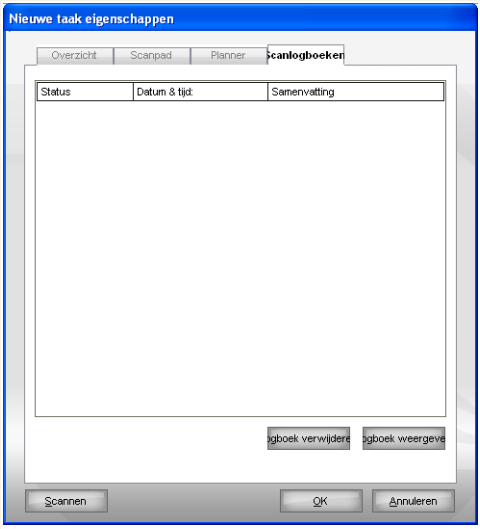
Als er tijdens het scannen verdachte bestanden zijn gedetecteerd, wordt u gevraagd ze naar het BitDefender Lab te sturen. Verdachte bestanden zijn bestanden die zijn gedetecteerd door de heuristische analyse en die mogelijk geïnfecteerd zijn met malware waarvan de signatuur nog niet bekend is.

Het rapportbestand wordt automatisch opgeslagen in het gedeelte Logboeken in het venster **Eigenschappen** van de respectievelijke taak.

Waarschuwing
Als er niet-opgeloste problemen zijn, raden wij u aan contact op te nemen met het ondersteuningsteam van BitDefender op www.bitdefender.com.

7.2.6. Scanlogboeken 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:

- **Log verwijderen** - om het geselecteerde scanlog rapportbestand te verwijderen.
- **Log weergeven** - om het geselecteerde scanlog rapportbestand weer te geven. Het scanlog rapportbestand wordt geopend in uw standaard webbrowser.

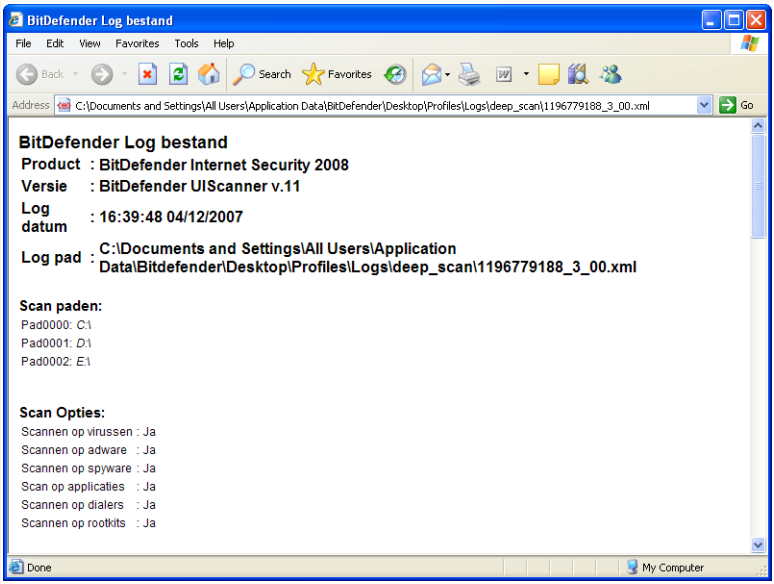
Opmerking

Om een bestand weer te geven of te verwijderen, kunt u ook met de rechtermuisknop op de overeenkomende optie klikken 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.

Scanlogs

De volgende afbeelding is een voorbeeld van een scanlog rapportbestand:



Scanlogs

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

7.3. Objecten die zijn uitgesloten van het scannen

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

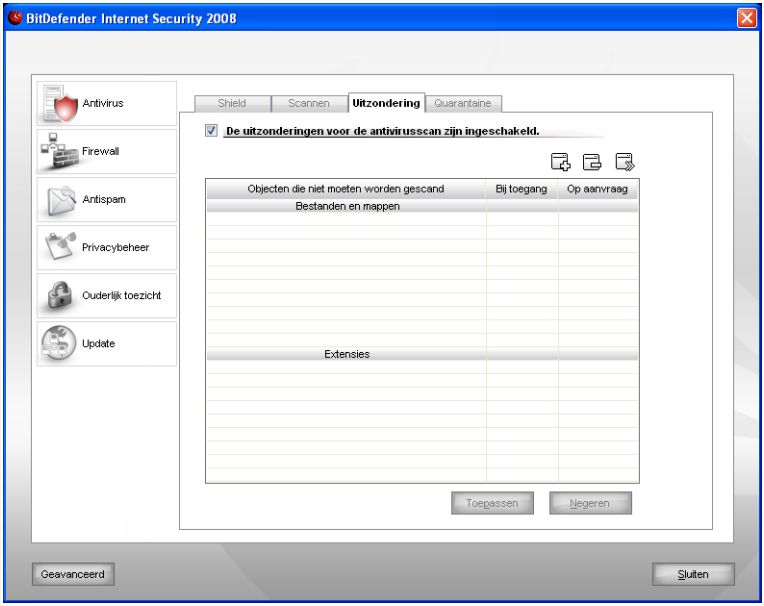
Met BitDefender kunt u objecten uitsluiten van een Scan bij toegang, een Scan op aanvraag, of beide. Deze functie is bedoeld om de scantijden te verkorten en onderbreking in uw werk te vermijden.

Er kunnen 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 zullen worden uitgesloten van de scan.

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

Om de objecten die zijn uitgesloten van het scannen, weer te geven en te beheren, klikt u op **Antivirus>Uitzonderingen** in de instellingsconsole. Het volgende venster wordt geopend:



Uitzonderingen

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

Opmerking
De uitzonderingen die hier zijn opgegeven, zullen NIET van toepassing zijn 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. Hier kunt 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 kunt ook met de rechtermuisknop op een object klikken en de opties in het snelmenu gebruiken om het object te bewerken of te verwijderen.

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

7.3.1. 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 doorheen het proces voor het uitsluiten van paden van de scan.

Stap 1/3 - Objecttype selecteren

Objecttype

Selecteer de optie om een pad uit te sluiten van de scan.

Klik op **Volgende**.

Stap 2/3 - Uitgesloten paden opgeven

Uitgesloten paden

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

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

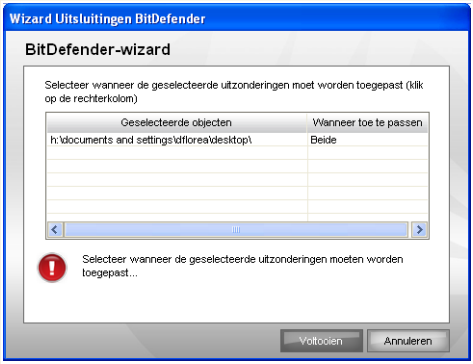
> ***Opmerking***
> Als het opgegeven pad niet bestaat, verschijnt een foutbericht. Klik op **OK** en controleer het pad op geldigheid.

De paden verschijnen in de tabel wanneer u ze toevoegt. U kunt 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 3/3 - Scantype selecteren



Scantype

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

De geselecteerde paden worden standaard uitgesloten van Scan bij toegang en van Scan bij 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 **Voltooien**.

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

7.3.2. Extensies uitsluiten van het scannen

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

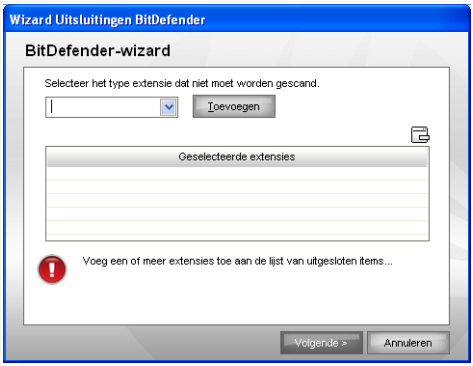
Stap 1/3 - Objecttype selecteren

Objecttype

Selecteer de optie om een extensie uit te sluiten van de scan.

Klik op **Volgende**.

Stap 2/3 - Uitgesloten extensies opgeven



Uitgesloten extensies

Om de extensies die moeten worden uitgesloten van de scan op te geven, gebruikt u een van de volgende methoden.

- Selecteer de extensie die u wilt uitsluiten van de scan 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, kunt u de beschrijving zien, indien deze beschikbaar is.

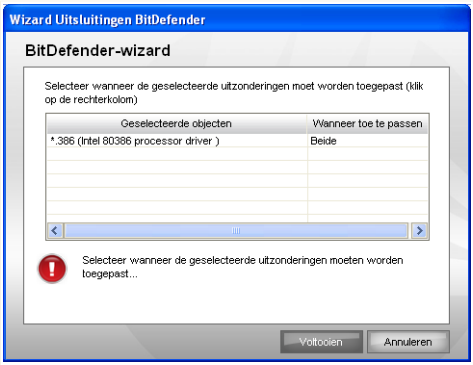
- Voer de extensie in die u wilt uitsluiten van de scan in het bewerkingsveld en klik op **Toevoegen**.

De extensies verschijnen in de tabel wanneer u ze toevoegt. U kunt 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 3/3 - Scantype selecteren



Scantype

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

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

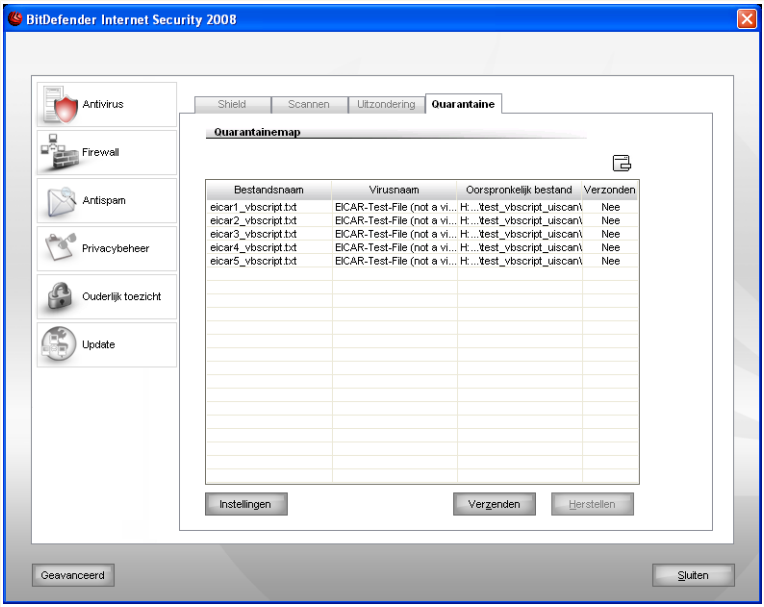
Klik op **Voltooien**.

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

7.4. 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 lab.

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



Quarantaine

7.4.1. Bestanden in quarantaine beheren

Zoals u wellicht zult merk, bevat het onderdeel **Quarantaine** een lijst van alle bestanden die tot nog toe werden geïsoleerd. Elk bestand bevat zijn naam, grootte, isolatiedatum en verzendingsdatum.

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

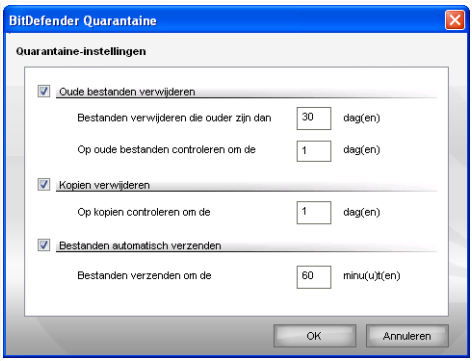
Om een geselecteerd bestand uit de quarantaine te verwijderen, klikt u op de knop **Verwijderen**. Als u een geselecteerd bestand wilt terugzetten op zijn oorspronkelijke locatie, klikt u op **Herstellen**.

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

Contextmenu. Er is een snelmenu beschikbaar waarmee u de bestanden in quarantaine gemakkelijk kunt beheren. Dezelfde opties zoals eerder vermeld, zijn beschikbaar. U kunt ook **Vernieuwen** selecteren om het gebied Quarantaine te vernieuwen.

7.4.2. Quarantaine-instellingen configureren

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



Quarantaine-instellingen

Met de quarantaine-instellingen, kunt 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 zou moeten controleren.

Opmerking
BitDefender zal standaard elke dag controleren op oude bestanden en bestanden die ouder zijn dan 10 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 kopieën opgeven.

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

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

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

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

8. Firewall

De Firewall beschermt uw computer tegen onbevoegde binnenkomende en uitgaande verbindingspogingen. Deze functie is te vergelijken met een schildwacht bij de poort. Hij houdt een waakzaam oog op uw internetverbinding en volgt op wie hij toegang kan verlenen tot het internet en wie hij moet blokkeren.

Opmerking
Een firewall is bijzonder belangrijk wanneer u een breedband- of DSL-verbinding hebt.

In de Stealth-modus wordt uw computer "verborgen" voor kwaadaardige software en hackers. De firewallmodule is in staat poortscans (pakketstromen die naar een machine worden verzonden om de "toegangspunten" te zoeken) automatisch te detecteren en het systeem tegen deze scans te beschermen.

Het gedeelte **Firewall** in deze gebruiksaanwijzing bevat de volgende onderwerpen:

- Firewall-begrippen
- Firewall-status
- Verkeerbeveiliging
- Geavanceerde instellingen
- Firewall-activiteit
- Netwerkzones

8.1. Firewall-begrippen

De firewall van BitDefender is ontwikkeld om u de beste beveiliging te bieden voor uw netwerk / internetverbindingen, zonder dat u deze hoeft te configureren. Het maakt niet uit of u rechtstreeks met het internet bent verbonden, met één netwerk of met meerdere netwerken (ethernet, draadloos, VPN of een ander netwerktype), vertrouwd of verdacht, de firewall zal zichzelf configureren om zich aan de overeenkomende situatie aan te passen.

BitDefender zal standaard de netwerkconfiguraties op uw computer detecteren en maakt een geschikt standaard firewallprofiel. Het programma voegt de gedetecteerde netwerken ook toe aan het profiel als vertrouwde of verdachte netwerkzones, afhankelijk van hun configuratie.

8.1.1. Wat zijn firewall-profielen?

Een firewall-profiel bestaat uit een reeks regels die de netwerk-/internettoegang van de toepassing beheert.

Afhankelijk van de netwerkconfiguratie op uw computer, maakt BitDefender automatisch een specifiek type profiel. Het gemaakte basisprofiel bevat regels voor de netwerktoegang of elementaire regels voor internettoegang die vereist zijn door systeemtoepassingen en BitDefender-componenten.

Opmerking
Er wordt één firewall-profiel gemaakt, ongeacht het aantal netwerken waarmee u verbonden bent.

Er zijn die types basisprofielen:

Profiel	*Beschrijving*
Directe verbinding	Bevat de elementaire internettoegangsregels die zijn aanbevolen voor een netwerkconfiguratie en directe toegang tot het internet toestaan. De regels staan niet toe dat netwerkgebruikers toegang krijgen tot uw computer of dat u op het netwerk kunt zoeken.
Verdacht	Bevat de netwerktoegangsregels die zijn aanbevolen voor een netwerkconfiguratie gekoppeld aan een verdacht netwerk. Deze regels staan u toe te zoeken op het netwerk, maar verhinderen de toegang tot uw computer door andere netwerkgebruikers.
Vertrouwd	Bevat de netwerktoegangsregels die zijn aanbevolen voor een netwerkconfiguratie gekoppeld aan een vertrouwd netwerk. Er zijn geen beperkingen opgelegd voor de netwerktoegang. Dit betekent dat u toegang hebt tot de netwerk-shares, netwerkprinters en andere netwerkbronnen. Netwerkleden kunnen tegelijkertijd een verbinding maken met uw computer en toegang krijgen tot uw shares.

Wanneer toepassingen een verbinding proberen te maken met het internet, worden geschikte regels toegevoegd aan het profiel. U kunt ervoor kiezen om de toegang tot het internet door toepassingen waarvoor geen regels werden geconfigureerd, toe te

laten of te weigeren. U kunt ook standaard alleen de toepassingen die in de witte lijst zijn opgenomen, toegang verlenen en andere toepassingen alleen toegang verlenen nadat ze toestemming hebben gevraagd.

Opmerking

Om het toegangsbeleid te bepalen voor toepassingen die de eerste keer een verbinding proberen te maken met het internet, gaat u naar het gedeelte Status en stelt u het beveiligingsniveau in. Om het bestaande profiel te bewerken, gaat u naar het gedeelte Verkeer en klikt u op **Profiel bewerken**.

8.1.2. Wat zijn netwerkzones?

Een netwerkzone staat voor een computer binnen een netwerk of een volledig netwerk dat volledig is geïsoleerd van uw computer of, omgekeerd, uw computer kan detecteren en een verbinding ermee kan maken. In de praktijk is een zone een IP-adres of een reeks IP-adressen waarvoor de toegang tot uw computer wordt geweigerd of toegestaan.

Standaard voegt BitDefender automatisch zones toe voor specifieke netwerkconfiguraties. Een zone wordt toegevoegd door een geschikte netwerktoegangsregel te maken die in het huidige profiel van toepassing is op een volledig netwerk.

Er zijn twee types zones:

Zonetype	Beschrijving
Vertrouwd	Computers van een vertrouwde zone kunnen een verbinding maken met uw computer en u kunt er een verbinding mee maken. Alle verbindingspogingen die van een dergelijke zone komen, evenals alle verbindingspogingen van uw computer met een dergelijke zone, zijn toegestaan. Als een netwerk wordt toegevoegd als een vertrouwde zone, hebt u onbeperkte toegang tot netwerkshares, netwerkprinters en andere netwerkbronnen. Daarnaast kunnen leden van het netwerk ook een verbinding maken met uw computer en toegang krijgen tot uw shares.

Zonetype	Beschrijving
Verdacht	Computers van een verdachte zone kunnen geen verbinding maken met uw computer en u kunt er geen verbinding mee maken. Alle verbindingspogingen die van een dergelijke zone komen, evenals alle verbindingspogingen van uw computer met een dergelijke zone, worden geblokkeerd. Wanneer het ICMP-verkeer is geweigerd en de Stealth-modus is ingeschakeld, zal uw computer nagenoeg onzichtbaar zijn voor computers in die zone.

Opmerking

Om een zone te bewerken, gaat u naar het gedeelte Zones. Om de regel die overeenkomt met een zone te bewerken, gaat u naar het gedeelte Verkeer en klikt u op **Profiel bewerken**.

8.1.3. Firewall-werking

Wanneer u het systeem opnieuw opstart na de installatie, zal BitDefender automatisch uw netwerkconfiguratie detecteren, een geschikt basisprofiel maken en een zone toevoegen op basis van het gedetecteerde netwerk.

Opmerking

Als u een rechtstreekse verbinding maakt met het internet, wordt er geen netwerkzone gemaakt voor de overeenkomende netwerkconfiguratie. Als u verbonden bent met meer dan één netwerk, worden zones toegevoegd afhankelijke van de respectievelijke netwerken.

Telkens wanneer de netwerkconfiguratie wijzigt, wordt een nieuw firewall-profiel gemaakt, ongeacht of u een verbinding met een ander netwerk maakt of een netwerkverbinding uitschakelt. De netwerkzones worden tegelijkertijd overeenkomstig gewijzigd.

Wanneer een nieuw firewall-profiel wordt gemaakt, wordt het oude profiel opgeslagen, zodat het opnieuw kan worden geladen wanneer u terugkeert naar de overeenkomende netwerkconfiguratie.

Afhankelijk van de netwerkconfiguratie, zal BitDefender zichzelf overeenkomstig configureren. De firewall van BitDefender wordt op deze manier standaard geconfigureerd:

- als u rechtstreeks een verbinding maakt met het internet, wordt een profiel Directe verbinding gemaakt, ongeacht of u ook met andere netwerken bent verbonden. Anders maakt BitDefender een verdacht firewall-profiel.

Opmerking

Omwille van beveiligingsmaatregelen, worden vertrouwde profielen niet standaard gemaakt. Om een vertrouwd profiel te maken, moet u het bestaande profiel opnieuw instellen. Meer informatie vindt u onder "*Profielen opnieuw instellen*" (p. 96).

- De zones worden toegevoegd afhankelijk van de netwerkconfiguratie.

Zonetype	*Netwerkconfiguratie*
Vertrouwd	**Persoonlijk IP zonder gateway** - De computer maakt deel uit van een lokaal netwerk (LAN) en maakt geen verbinding met het internet. Een voorbeeld van een dergelijke situatie is een thuisnetwerk dat is gemaakt om familieleden toe te staan bestanden, printers of andere bronnen te delen.
	Persoonlijk IP met gedetecteerde domeincontroller - De computer maakt deel uit van een LAN en is verbonden met een domein. Een voorbeeld van een dergelijke situatie is een kantoornetwerk dat gebruikers toestaat bestanden of andere bronnen binnen een domein te delen. Een domein impliceert het bestaan van een reeks beleidsregels waaraan de ledencomputers moeten voldoen.
Verdacht	**(Onbeveiligd) draadloos openen** - De computer maakt deel uit van een draadlos lokaal netwerk (WLAN). Een voorbeeld van een dergelijke situatie is wanneer u vanaf een openbare plaats een verbinding maakt met het internet door middel van een vrij toegangspunt.

Opmerking

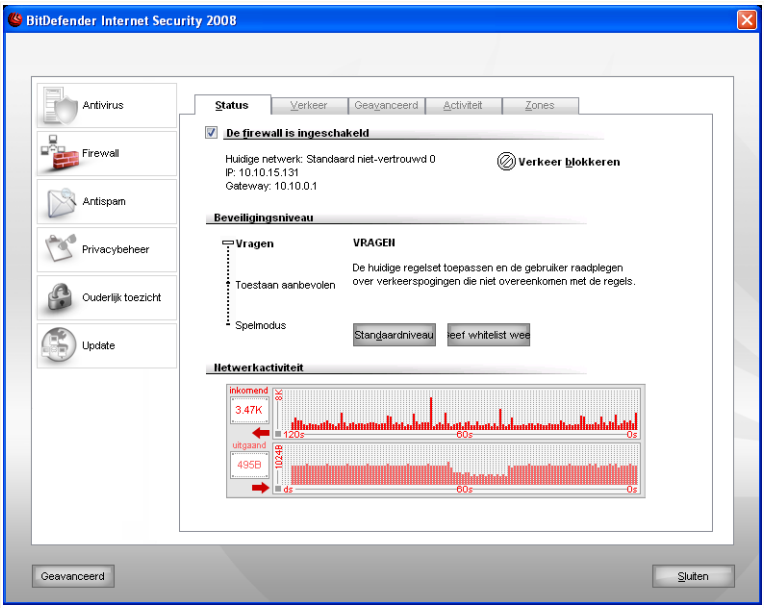
Voor sommige netwerkconfiguraties worden geen zones gemaakt, zoals:

- **Openbaar (routeerbaar) IP** - De computer is rechtstreeks verbonden met het internet.
- **Persoonlijk IP met gateway, maar geen domeincontroller gedetecteerd** - De computer maakt deel uit van een LAN, zonder ook deel uit te maken van een domein en maakt een verbinding met het internet via een gateway. Een voorbeeld van een dergelijke situatie is een netwerk op een schoolcampus dat gebruikers toestaat bestanden of andere bronnen te delen.

- De stealth-modus is ingeschakeld.
- VPN en Externe verbinding zijn toegestaan.
- Internet Connection Sharing is niet toegelaten voor verdachte zones.
- Toepassingen in de witte lijst krijgen automatisch toegang, terwijl u voor andere toepassingen zult worden gevraagd toestemming te geven wanneer ze voor de eerste keer proberen te verbinden.

8.2. Firewall-status

Om de firewall-beveiliging te configureren, klikt u in de instellingsconsole op **Firewall>Status**. Het volgende venster wordt geopend:



Firewall-status

In dit onderdeel kunt u de **Firewall** inschakelen/uitschakelen, alle netwerk-/internetverkeer blokkeren en het standaard gedrag bij nieuwe gebeurtenissen instellen.

Belangrijk
Houd **Firewall** ingeschakeld om tegen internetaanvallen te worden beschermd.

Om alle netwerk-/internetverkeer te blokkeren, klikt u op de knop **Verkeer blokkeren** en vervolgens op **Ja** om uw keuze te bevestigen. Hiermee wordt uw computer geïsoleerd tegen andere computers op het netwerk.

Om de blokkering van het verkeer later op te heffen, klikt u gewoon op **Blokkering verkeer opheffen**.

In het onderste gedeelte van het venster kunt u de statistieken van BitDefender over het binnenkomende en uitgaande verkeer bekijken. De grafiek toont het volume van het internetverkeer gedurende de laatste twee minuten.

Opmerking
De grafiek verschijnt ook als de **Firewall** is uitgeschakeld.

8.2.1. 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:

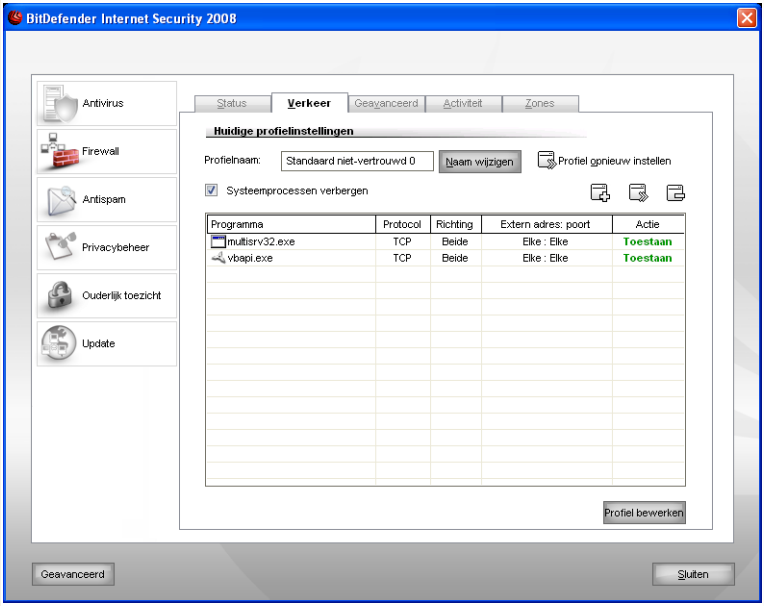
Beveiligingsniveau	*Beschrijving*
Spelmodus	Past de huidige regels toe en staat alle verkeerspogingen toe die niet overeenkomen met een van de huidige regels, zonder u te waarschuwen. Dit beleid wordt sterk afgeraden, maar kan handig zijn voor netwerkbeheerders en gamers.
Toestaan aanbevolen	Past de huidige regels toe en laat alle uitgaande verbindingspogingen van programma's die door BitDefender gekend zijn als rechtmatig (in witte lijst), zonder u te waarschuwen. Voor de rest van de verbindingspogingen, zal BitDefender u vragen om uw toestemming. U kunt de verkeersregels weergeven zoals ze in het onderdeel Verkeer zijn gemaakt.

Beveiligingsniveau	Beschrijving
	Programma's op de witte lijst zijn de meest gebruikte toepassingen in de hele wereld. Zij omvatten de meeste bekende webbrowsers, audio- en videospelers, chatprogramma's en programma's voor het delen van bestanden, evenals serverclients en besturingssystemen. Als u de programma's van de witte lijst wilt zijn, klikt u op **Witte lijst tonen**.
Vragen	Past de huidige regels toe en raadpleegt u bij alle verkeerspogingen die niet overeenkomen met een van de huidige regels.

Klik op **Standaard** om het standaardbeleid in te stellen (**Toestaan aanbevolen**).

8.3. Verkeerbeheer

Om de firewallregels van het huidige profiel te beheren, klikt u in de instellingsconsole op **Firewall>Verkeer**. Het volgende venster wordt geopend:



Verkeerbeheer

In dit onderdeel kunt u opgeven welke binnenkomende en uitgaande verbindingen moeten worden toegestaan/geweigerd door regels te maken met specifieke protocollen, poorten, toepassingen en/of externe adressen.

De regels kunnen automatisch worden ingevoerd (via het waarschuwingsvenster) of handmatig (Klik op **Toevoegen** en kies de parameters voor de regel).

8.3.1. Regels automatisch toevoegen

Wanneer **Firewall** is ingeschakeld, zal BitDefender uw toestemming vragen wanneer een verbinding met het internet wordt gemaakt:

Firewall-waarschuwing

U kunt de volgende zaken weergeven: de toepassing die probeert toegang te krijgen tot het internet, het pad naar het toepassingsbestand, de bestemming, het protocol dat wordt gebruikt en de poort waarop de toepassing een verbinding probeert te maken.

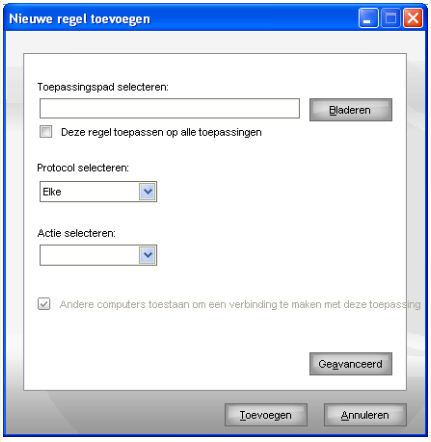
Klik op **Toestaan** om alle verkeer (binnenkomend en uitgaand) toe te staan die door deze toepassing vanaf de lokale host naar elke bestemming wordt gegenereerd via het respectieve IP-protocol en op alle poorten. Als u op **Blokkeren** klikt, wordt de toegang tot het internet via het respectieve IP-protocol volledig geweigerd voor de toepassing.

Op basis van uw antwoord wordt een regel gemaakt, toegepast en weergegeven in de tabel. Wanneer de toepassing de volgende keer probeert een verbinding te maken, wordt deze regels standaard toegepast.

Belangrijk
laat alleen binnenkomende verbindingspogingen toe van IP's of domeinen die u zeker vertrouwt.

8.3.2. Regels handmatig toevoegen

Klik op de knop **Regel toevoegen** en kies de parameters voor de regel. Het volgende venster wordt geopend:



Regel toevoegen

Volg deze stappen om een nieuwe firewallregel toe te voegen:

1. Selecteer de toepassing waarvoor de nieuwe firewallregel zal worden gemaakt.

   Om een toepassing te selecteren, klikt u op **Bladeren**, zoekt u de toepassing en klikt u op **OK**.

   Als u een regel voor alle toepassingen wilt maken, schakelt u het selectievakje **Deze regel toepassen voor alle toepassingen** in.
2. Selecteer het protocol waarvoor de regel van toepassing zal zijn.

   U hebt de beschikking over een lijst met de meest gebruikelijke protocollen zodat u alleen een specifiek protocol hoeft te selecteren. Selecteer het gewenste protocol (waarop de regel van toepassing is) in het overeenkomende vervolgkeuzemenu of selecteer **Alle** om alle protocollen te selecteren.

   De volgende tabel toont de protocollen die u kunt selecteren, samen met een korte beschrijving van elk protocol.

Protocol	*Beschrijving*
ICMP	Internet Control Message Protocol - is een extensie van het Internet Protocol (IP). ICMP ondersteunt pakketten met fout-, beheer- en informatieve berichten. De opdracht PING gebruikt bijvoorbeeld ICMP om een internetverbinding te testen.

Protocol	Beschrijving
TCP	Transmission Control Protocol - TCP activeert twee hosts om een verbinding tot stand te brengen en gegevensstromen uit te wisselen. TCP garandeert het afleveren van gegevens en verzekert eveneens dat de pakketten worden afgeleverd in dezelfde volgorde waarin ze worden verzonden.
UDP	User Datagram Protocol - UDP is een transport gebaseerd op IP en ontwikkeld voor hoge prestaties. Games en andere op video gebaseerde toepassingen gebruiken vaak UDP.

3. Selecteer de regelactie in het overeenkomende menu.

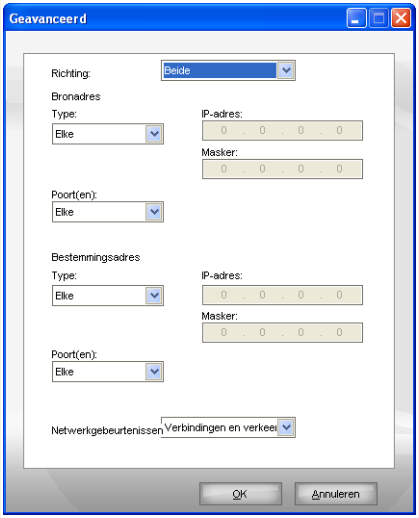
Actie	Beschrijving
Toestaan	De opgegeven toepassing zal netwerk-/internettoegang krijgen onder de opgegeven omstandigheden.
Weigeren	De opgegeven toepassing zal geen netwerk-/internettoegang krijgen onder de opgegeven omstandigheden.

4. Als het eerder geselecteerde protocol TCP of UDP is, kunt u niet bepalen of de regel van toepassing zal zijn voor de toepassing wanneer deze al dan niet optreedt als een server.

   Schakel het selectievakje **Andere computers toestaan een verbinding te maken met deze toepassing** om de actie toe te passen op alle netwerkgebeurtenissen. U zult het recht van deze toepassing om poorten te openen impliciet toestaan of weigeren.

   Als u de actie alleen wilt toepassen voor verkeer voor UDP- en verkeer & verbindingen voor TCP respectievelijk, schakelt u het overeenkomende selectievakje uit.

Klik op **Geavanceerd** als u meer geavanceerde instellingen voor de regel wilt configureren. Een nieuw venster wordt weergegeven:



Geavanceerde regelinstellingen

U kunt het volgende configureren:

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

Type	*Beschrijving*
Uitgaand	De regel zal alleen voor uitgaand verkeer worden toegepast.
Inkomend	De regel zal alleen voor inkomend verkeer worden toegepast.
Beide	De regel zal in beide richtingen worden toegepast.

- **Bronadres** - geef het bronadres op.

  Om het bronadres op te geven, selecteert u het adrestype in het menu en geeft u de vereiste gegevens op. De volgende opties zijn beschikbaar:

Type	*Beschrijving*
Alle	De regel is van toepassing op alle bronadressen.

Type	Beschrijving
Host	De regel is alleen van toepassing als de bron een specifieke host is. U moet het IP-adres van de host invoeren.
Netwerk	De regel is alleen van toepassing als de bron een specifiek netwerk is. U moet het IP-adres en het masker van de host invoeren.
Lokale host	De regel is alleen van toepassing als de bron een lokale host is. Als u meer dan een netwerkinterface gebruikt, selecteert u in het menu de netwerkinterface waarop de regel van toepassing is. Als u wilt dat de regel wordt toegepast op alle lokale hosts, selecteert u **Alle**.
Lokaal netwerk	De regel is alleen van toepassing als de bron het lokale netwerk is. Als u met meer dan een netwerk bent verbonden, selecteert u in het menu het netwerk waarop de regel van toepassing is. Als u wilt dat de regel wordt toegepast op alle lokale netwerken, selecteert u **Alle**.

Als u TCP of UDP hebt geselecteerd als protocol, kunt u een specifieke poort of een bereik tussen 0 en 65535 instellen. Als u wilt dat de regel van toepassing is op alle poorten, selecteert u **Alle**.

- **Doeladres** - geef het doeladres op.

Om het doeladres op te geven, selecteert u het adrestype in het menu en geeft u de vereiste gegevens op. De volgende opties zijn beschikbaar:

Type	Beschrijving
Alle	De regel is van toepassing op alle doeladressen.
Host	De regel is alleen van toepassing als de bestemming een specifieke host is. U moet het IP-adres van de host invoeren.
Netwerk	De regel is alleen van toepassing als de bestemming een specifiek netwerk is. U moet het IP-adres en het masker van de host invoeren.
Lokale host	De regel is alleen van toepassing als de bestemming een lokale host is. Als u meer dan een netwerkinterface gebruikt, selecteert u in het menu de netwerkinterface waarop de regel van toepassing is. Als u wilt dat de regel wordt toegepast op alle lokale hosts, selecteert u **Alle**.

Type	Beschrijving
Lokaal netwerk	De regel is alleen van toepassing als de bestemming een lokaal netwerk is. Als u met meer dan een netwerk bent verbonden, selecteert u in het menu het netwerk waarop de regel van toepassing is. Als u wilt dat de regel wordt toegepast op alle lokale netwerken, selecteert u **Alle**.

Als u TCP of UDP hebt geselecteerd als protocol, kunt u een specifieke poort of een bereik tussen 0 en 65535 instellen. Als u wilt dat de regel van toepassing is op alle poorten, selecteert u **Alle**.

- **Netwerkgebeurtenissen** - als u TCP of UDP hebt geselecteerd als het protocol, selecteert u de netwerkgebeurtenissen waarop de regel van toepassing is.

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

Klik op **Toevoegen** om een firewallregel toe te voegen.

8.3.3. Regels beheren

De regels die tot nog toe zijn gemaakt voor het huidige profiel, worden weergegeven in de tabel.

Schakel het selectievakje in naast **Systeemprocessen verbergen** als u de regels met betrekking tot de systeemprocessen wilt verbergen.

De regels worden weergegeven in aflopende volgorde van prioriteit waarbij de eerste regel staat voor de hoogste prioriteit. Klik op **Profiel bewerken** om de **Gedetailleerde weergave** te openen waarin u de prioriteit van de regels kunt weigeren door ze omhoog of omlaag te verplaatsen.

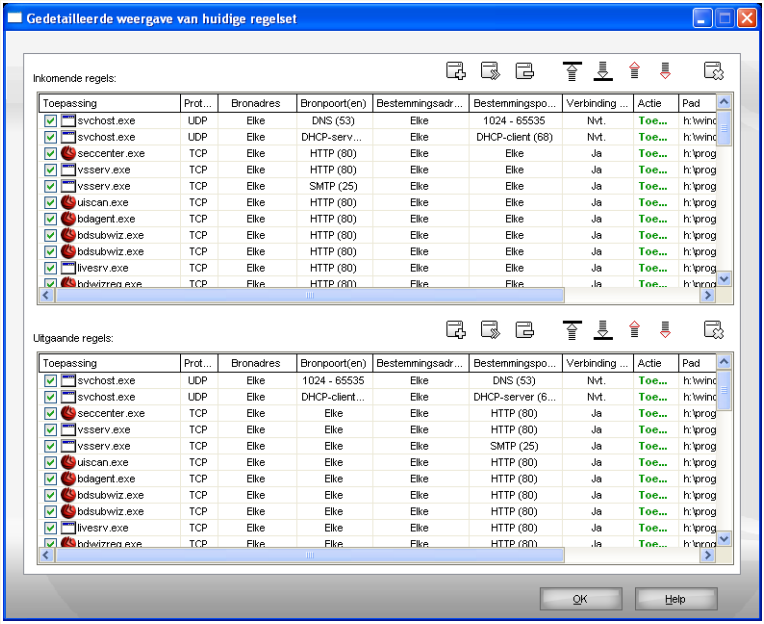
Om een regel te verwijderen, selecteert u de regel en klikt u op de knop **Regel verwijderen**.

Om een regel te wijzigen, selecteert u de regel en klikt u op de knop **Regel bewerken** of dubbelklikt u op de regel.

Opmerking
Een contextmenu is ook beschikbaar en bevat de volgende opties: **Regel toevoegen**, **Regel verwijderen** en **Regel bewerken**.

8.3.4. Profielen wijzigen

U kunt een profiel wijzigen door te klikken op **Profiel bewerken**. Het volgende venster wordt geopend:



Gedetailleerde weergave

De regels zijn opgesplitst in 2 secties: inkomende regels en uitgaande regels. U kunt de toepassing en de regelparameters van elke regel weergeven (bronadres, bestemmingsadres, bronpoorten, bestemmingspoorten, actie, enz.).

Om een regel te verwijderen, selecteert u de regel en klikt u op de knop **Regel verwijderen**. Om alle regels te verwijderen, klikt u op de knop **Lijst wissen**. Om een regel te wijzigen, selecteert u de regel en klikt u op de knop **Regel bewerken** of dubbelklikt u op de regel. Als u een regel tijdelijk wilt uitschakelen zonder deze te verwijderen, moet u het overeenkomende selectievakje uitschakelen.

U kunt de prioriteit van een regel verhogen of verlagen. Klik op de knop **Naar boven in lijst** om de prioriteit van de geselecteerde regel met één niveau te verhogen of klik

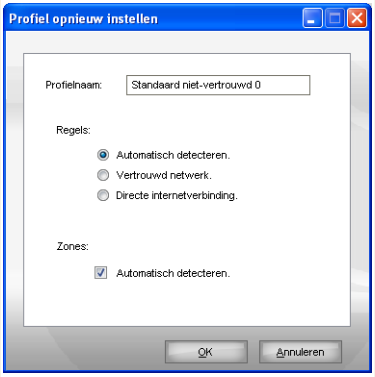
op de knop **Naar beneden in lijst** om de prioriteit van de geselecteerde regel met één niveau te verlagen. Om de hoogste prioriteit aan een regel toe te wijzen, klikt u op de knop **Eerst verplaatsen**. Om de laagste prioriteit aan een regel toe te wijzen, klikt u op de knop **Laatst verplaatsen**.

Opmerking
Er is ook een contextmenu beschikbaar dat de volgende opties bevat: **Regel toevoegen**, **Regel bewerken**, **Regel verwijderen**, **Omhoog verplaatsen**, **Omlaag verplaatsen**, **Eerst verplaatsen**, **Laatst verplaatsen** en **Lijst wissen**.

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

8.3.5. Profielen opnieuw instellen

Geavanceerde gebruikers kunnen ervoor kiezen het firewallprofiel opnieuw te configureren om de firewallbeveiliging te optimaliseren of om deze aan te passen op basis van hun behoeften. Om het firewallprofiel opnieuw in te stellen, klikt u op **Profiel opnieuw instellen**. Het volgende venster wordt geopend:



Profiel opnieuw instellen

U kunt het volgende configureren:

- **Profielnaam** - voer een nieuwe naam in het bewerkingsveld in.
- **Regels** - bepaal welk type regels moet worden gemaakt voor de systeemtoepassingen.

  De volgende opties zijn beschikbaar:

Optie	Beschrijving
Autodetectie	Hiermee detecteert BitDefender de netwerkconfiguratie en wordt een geschikte reeks van elementaire regels gemaakt.
Vertrouwd netwerk	Maakt een reeks elementaire regels die geschikt zijn voor een vertrouwd netwerk.
Directe internetverbinding	Maakt een reeks elementaire regels die geschikt zijn voor een directe verbinding met het internet.

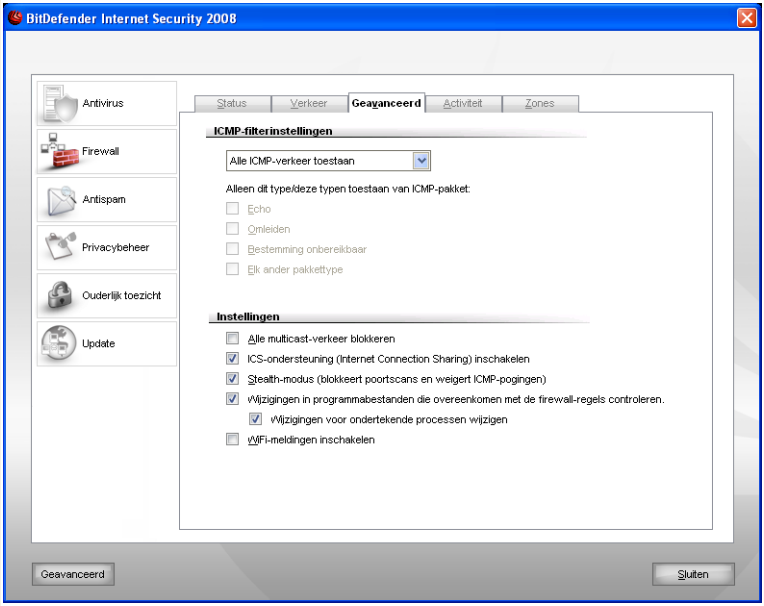
- **Zones** - schakel **Autodetectie** in om BitDefender de geschikte zones voor de gedetecteerde netwerken te laten maken.

Klik op **OK** om het venster te sluiten en het profiel opnieuw in te stellen.

Belangrijk
Alle regels die u in dit onderdeel hebt toegevoegd gaan verloren als u ervoor kiest het firewallprofiel opnieuw te configureren.

8.4. Geavanceerde instellingen

Om de geavanceerde instellingen van de BitDefender-firewall te configureren, klikt u in de instellingsconsole op **Firewall>Geavanceerd**. Het volgende venster wordt geopend:



Geavanceerde instellingen

In dit onderdeel kunt u de geavanceerde instellingen van de BitDefender-firewall configureren. Met de geavanceerde instellingen kunt u de filterregels opgeven voor het ICMP-verkeer (ICMP-filterinstellingen) en multicast-verkeer blokkeren om uw internetverbinding te delen of uw computer onzichtbaar te maken voor kwaadaardige software en hackers (Settings).

8.4.1. De ICMP-filterinstellingen configureren

In het menu kunt u een van de volgende beleidsregels selecteren om het ICMP-verkeer te filteren:

- **Alle ICMP-verkeer toegestaan** - staat al het ICMP-verkeer toe.
- **Alle ICMP-verkeer geblokkeerd** - blokkeert al het ICMP-verkeer.
- **Aangepaste ICMP-filtering** - past de manier aan waarop ICMP-verkeer wordt gefilterd. U zult kunnen kiezen welke types ICMP-pakketten moeten worden toegestaan.

De volgende opties zijn beschikbaar:

Optie	Beschrijving
Echo	Deze optie schakelt berichten voor Echo Reply en Echo Request in. De Echo Request is een ICMP-bericht dat een gegevenspakket verzendt naar de host en verwacht dat gegevens worden teruggestuurd in een Echo Reply. De host moet op alle Echo Requests reageren met een Echo Reply met daarin de exacte gegevens die in het verzoekbericht zijn ontvangen. De Echo Reply is een ICMP-bericht dat wordt gegenereerd in antwoord op een ICMP Echo Request-bericht en is verplicht voor alle hosts en routers.
Omleiden	Dit is een ICMP-bericht dat de host informeert om de routinginformatie om te leiden (pakketten via een alternatieve route verzenden). Als de host probeert gegevens te verzenden via een router (R1) en daarna via een andere router (R2) om de host te bereiken, en er een rechtstreeks pad van de host naar R2 beschikbaar is, zal de host hierover worden geïnformeerd. De router zal nog steeds het oorspronkelijke datagram naar de bedoelde bestemming verzenden. Als het datagram echter routinginformatie bevat, zal dit bericht niet worden verzonden, zelfs niet als er een betere route beschikbaar is.
Bestemming onbereikbaar	Dit is een ICMP-bericht dat wordt gegenereerd door de router om de client te informeren dat de doelhost onbereikbaar is, tenzij het datagram een multicast-adres heeft. Redenen voor dit bericht kunnen onder andere de volgende zijn: de fysieke verbinding met de host bestaat niet (afstand is oneindig), het aangegeven protocol of de poort is niet actief of de gegevens moeten worden gefragmenteerd, maar de vlag 'niet fragmenteren' is ingeschakeld.

Optie	Beschrijving
Elk ander pakkettype	Wanneer deze optie is ingeschakeld, zal elk pakket behalve **Echo**, **Bestemming onbereikbaar** of **Omleiden** worden doorgelaten.

8.4.2. Geavanceerde firewall-instellingen configureren

De volgende geavanceerde firewall-instellingen zijn beschikbaar:

- **Alle multicast-verkeer blokkeren** - weigert elk ontvangen multicast-pakket.

  Multicast-verkeer is het type verkeer dat is gericht op een speciale groep in een netwerk. De pakketten worden naar een speciaal adres verzonden, van waarde multicast-client ze kan ontvangen als deze hiermee instemt.

  Een lid van een netwerk dat een tv-tuner heeft, mag bijvoorbeeld de videostroom uitzenden (verzenden naar elk netwerklid) of multicasten (verzenden naar een speciaal adres). De computer die luisteren naar het multicast-adres kunnen het pakket accepteren of weigeren. Als ze accepteren kan de videostroom worden bekeken door de multicast-clients.

  Te hoge hoeveelheden multicast-verkeer verbruiken bandbreedte en bronnen. Met deze optie ingeschakeld zal elk ontvangen multicast-pakket worden geweigerd. Het is echter niet aanbevolen deze optie te selecteren.
- **ICS-ondersteuning (Internet Connection Sharing) inschakelen** - schakelt de ondersteuning in voor ICS (Internet Connection Sharing).

  Opmerking
  Met deze optie wordt ICS niet automatisch ingeschakeld op uw systeem, maar wordt dit type verbinding alleen toegestaan wanneer u het inschakelt via uw besturingssysteem.

  Met ICS (Internet Connection Sharing) kunnen leden van lokale netwerken via uw computer een verbinding maken met het internet. Dit is nuttig wanneer u gebruik maakt van een speciale/particuliere internetverbinding (bijv. draadloze verbinding) en u deze wilt delen met andere leden van uw netwerk.

  Het delen van uw internetverbinding met leden van lokale netwerken leidt tot een hoger verbruiksniveau van de bronnen en kan een zeker risico inhouden. Het neemt ook enkele van uw poorten in beslag (de poorten die zijn geopend door leden die uw internetverbinding gebruiken).

- **Stealth-modus** - maakt uw computer onzichtbaar voor kwaadaardige software en hackers.

  U kunt op een eenvoudige manier uitvinden of uw computer mogelijk kwetsbaar is. U hoeft alleen een verbinding te maken met de poorten om te zien of er enige reactie is. Dit wordt een poortscan genoemd.

  Kwaadaardige individuen of softwareprogramma's mogen zelfs niet ontdekken dat uw computer bestaat, om nog niet te spreken van het leveren van services aan het netwerk. De optie **Stealth-modus** houdt de reactie tegen van uw computer op pogingen om uit te zoeken welke poorten open zijn of waar de computer precies is.
- **Wijzigingen in programmabestanden die overeenkomen met de firewall-regels controleren** - controleert elke toepassing die probeert een verbinding te maken met het internet om te zien of er wijzigingen werden aangebracht sinds de regels die zijn toegang beheert, werd toegevoegd. Als de toepassing werd gewijzigd, wordt een waarschuwing weergegeven met de vraag of u de toegang tot het internet wilt toestaan of blokkeren voor de toepassing.

  Toepassing worden doorgaans gewijzigd door updates; Er bestaat echter een risico dat ze worden gewijzigd door malware-toepassingen met het doel uw computer en andere computers op het netwerk te infecteren.

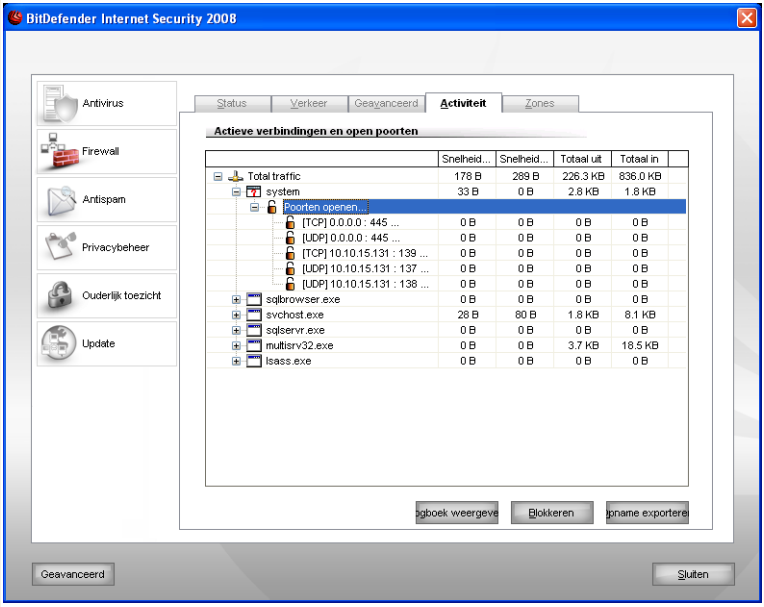
  Opmerking

  Wij raden u aan deze optie geselecteerd te houden en de toegang alleen toe te staan voor de toepassingen waarvan u verwacht dat ze zijn gewijzigd, nadat de regel die hun toegang beheert, werd gemaakt.

  Getekende toepassingen worden verondersteld vertrouwd te zijn en hebben een hogere beveiligingsgraad. U kunt **Wijzigingen voor ondertekende processen negeren** inschakelen om gewijzigde getekende toepassingen toe te staan een verbinding te maken met het internet zonder dat u een waarschuwing over deze gebeurtenis ontvangt.
- **WiFi-meldingen inschakelen** - schakelt de WiFi-meldingen in.

8.5. Verbindingsbeheer

Om de huidige netwerk-/internetactiviteit (via TCP en UDP) te bewaken, gesorteerd op toepassing en het BitDefender Firewall-logboek te openen, klikt u in de instellingsconsole op **Firewall>Activiteit**. Het volgende venster wordt geopend:



Verbindingsbeheer

U kunt alle verkeer, gesorteerd op toepassing, zien. Voor elke toepassing ziet u de verbindingen en open poorten, evenals de statistieken met betrekking tot de snelheid van het uitgaande & binnenkomende verkeer en de totale hoeveelheid verzonden/ontvangen gegevens.

Het venster toont de huidige netwerk-/internetactiviteit in real time. Wanneer de verbinding of poorten worden gesloten, ziet u dat de overeenkomende statistieken worden gedimd en, na verloop van tijd, verdwijnen. Hetzelfde gebeurt met alle statistieken die overeenkomen met een toepassing die verkeer genereert of open poorten heeft en die u sluit.

Klik op **Blokkeren** om regels te maken die verkeer beperken van de geselecteerde toepassing, poort of verbinding. U wordt gevraagd uw keuze te bevestigen. De regels zijn toegankelijk via het gedeelte Verkeer waar u ze verder kunt verfijnen.

Opmerking

Om een applicatie, poort of verbinding te blokkeren, kan u er ook op rechtsklikken en **Blokkeren** selecteren.

Klik op **Direct stoppen** om alle onderdelen van een geselecteerd proces te stoppen. U wordt gevraagd om uw keuze te bevestigen.

Opmerking
Om een proces direct te stoppen, kan er ook op rechtsklikken en **Direct stoppen** selecteren.

Klik op **Momentopname exporteren** om de lijst te exporteren naar een `.txt`-bestand.

Voor een uitgebreide lijst van gebeurtenissen met betrekking tot het gebruik van de Firewall-module (firewall starten/stoppen, verkeer blokkeren, Stealth-modus inschakelen, instellingen wijzigen, een profiel toepassen) of gebeurtenissen die werden gegenereerd door de activiteiten die erdoor zijn gedetecteerd (scannen van poorten, blokkeren van verbindingspogingen of verkeer volgens de regels), kunt u het logboekbestand van de BitDefender-firewall raadplegen door te klikken op **Log weergeven**. Het bestand bevindt zich in de map Common Files van de huidige Windows-gebruiker, onder het pad: `...BitDefender\BitDefender Firewall\bdfirewall.txt`.

8.6. Netwerkzones

Een zone is een IP-adres of een reeks IP-adressen waarvoor een speciale regel binnen een profiel wordt gemaakt. De regel kan netwerkleden onbeperkte toegang tot uw computer (vertrouwde zones) verlenen, of uw computer volledig isoleren van de netwerkcomputers (verdachte zone).

Standaard detecteert BitDefender automatisch het netwerk waarmee u verbonden bent en voegt een zone toe op basis van de netwerkconfiguratie.

Opmerking
Als u met meerdere netwerken bent verbonden, kan meer dan één zone worden toegevoegd afhankelijk van de configuratie van deze netwerken.

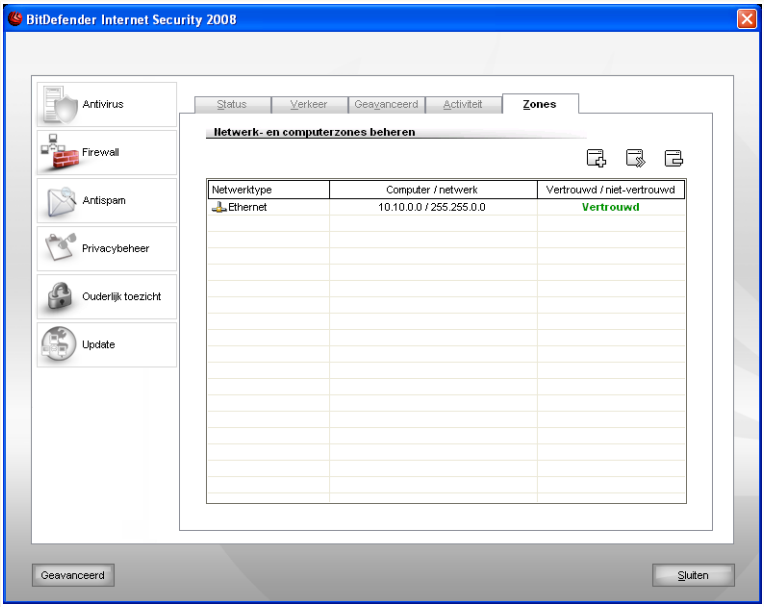
Vertrouwde zones worden standaard toegevoegd voor de volgende netwerkconfiguraties:

- **Persoonlijk IP zonder gateway** - De computer maakt deel uit van een lokaal netwerk (LAN) en maakt geen verbinding met het internet.
- **Persoonlijk IP met gedetecteerde domeincontroller** - De computer maakt deel uit van een LAN en is verbonden met een domein.

Verdachte zones worden standaard toegevoegd voor de volgende netwerkconfiguraties:

- **(Onbeveiligd) draadloos openen** - De computer maakt deel uit van een draadlos lokaal netwerk (WLAN).

Om de netwerkzones te beheren, klikt u in de instellingsconsole op **Firewall>Zones**. Het volgende venster wordt geopend:



Netwerkzones

U kunt de netwerkzones zien die overeenkomen met het huidige profiel dat in de tabel wordt weergegeven. Voor elke zone ziet u het netwerktype (Ethernet, draadloos, PPP, enz.), de computer of het netwerk dat aan die zone is gekoppeld en of de zone vertrouwd of verdacht is.

Om een zone te wijzigen, selecteert u de zone en klikt u op de knop **Zone bewerken** of dubbelklikt u op de regel.

Opmerking

Standaard voegt BitDefender open draadloze netwerken toe als verdachte zones. Als u verbonden bent met een open draadloos ad hoc-netwerk met vertrouwde computers

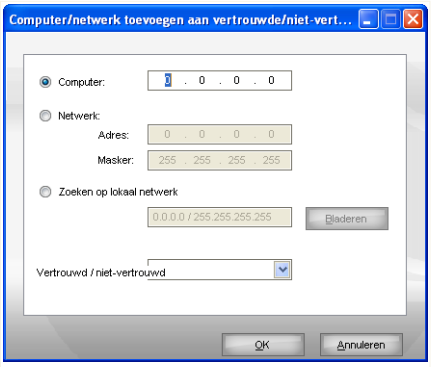
(thuis of met enkele vrienden), zult u mogelijk de gekoppelde zone willen bewerken. Om bronnen met de andere netwerkleden te kunnen delen, moet u het netwerk instellen als een vertrouwde zone.

Om een zone te verwijderen, selecteert u de zone en klikt u op de knop **Zone verwijderen**.

8.6.1. Zones toevoegen

U kunt zones handmatig toevoegen. Hierdoor kunt u bijvoorbeeld bestanden alleen met uw vrienden binnen een open draadloos netwerk delen (door hun computers toe te voegen als vertrouwde zones) of kunt u een computer van een vertrouwd netwerk blokkeren (door het toe te voegen als een verdachte zone).

Om een nieuwe zone toe te voegen, klikt u op de knop **Zone toevoegen**. Het volgende venster wordt geopend:



Zone toevoegen

Volg deze stappen om een zone toe te voegen:

1. Geef een computer van een lokaal netwerk of een volledig lokaalnetwerk op dat u wilt toevoegen als een zone. U kunt een van de volgende methoden gebruiken:
   - Om een specifieke computer toe te voegen, selecteert u **Computer** en geeft u het IP-adres op.
   - Om een specifiek netwerk toe te voegen, selecteert u **Netwerk** en geeft u het IP-adres en het masker op.

- Blader naar de lokale netwerken om een computer of netwerk te zoeken en toe te voegen.

  Om lokale netwerken te zoeken, selecteert u **Lokaal netwerk zoeken** en klikt u vervolgens op **Bladeren**. Een nieuw venster wordt geopend waarin u alle netwerken waarmee u verbonden bent en alle leden van elk netwerk kunt zien.

  Selecteer de computer of het netwerk in de lijst dat u wilt toevoegen als een zone en klik op **OK**

2. Selecteer in het menu het type zone dat u wilt maken (vertrouwd of verdacht).
3. Klik op **OK** om de zone toe te voegen.

9. Antispam

BitDefender Antispam gebruikt opmerkelijke technologische innovaties en industriestandaard antispamfilters om spam op te sporen voordat deze het Postvak IN van de gebruiker bereikt.

Het gedeelte **Antispam** in deze gebruiksaanwijzing bevat de volgende onderwerpen:

- Antispam-begrippen
- Antispamstatus
- Antispaminstellingen
- Integratie in e-mailclients

9.1. Antispam-begrippen

Spam betekent zowel voor individuele gebruikers als voor bedrijven een steeds groter probleem. Het is niet mooi, u wilt niet dat uw kinderen het zien, u kunt erdoor ontslagen worden (omdat u teveel tijd verspilt of omdat u porno ontvangt in uw zakelijke e-mail) en u kunt niet verhinderen dat men u deze berichten blijft zenden. De op één na beste oplossing ligt dus voor de hand: de ontvangst van dergelijke berichten blokkeren. Jammer genoeg komen spamberichten voor in allerlei vormen en formaten en op zeer grote schaal.

9.1.1. Antispamfilters

De BitDefender Antispam-engine bevat zeven verschillende filters die garanderen dat uw Postvak IN vrij blijft van SPAM: Witte lijst, Zwarte lijst, Tekensetfilter, Afbeeldingsfilter, URL-filter, NeuNet (Heuristische) filter en Bayes-filter.

Opmerking
U kunt elk van deze filters inschakelen/uitschakelen in het gedeelte Instellingen van de **Antispam**-module.

Witte lijst / Zwarte lijst

De meeste mensen communiceren regelmatig met een groep mensen of ontvangen zelfs berichten van bedrijven of organisaties in hetzelfde domein. Wanneer u gebruik maakt van **vrienden- of spammerslijsten**, kunt u gemakkelijk een classificatie maken van de mensen van wie u e-mails wilt ontvangen, ongeacht de inhoud (vrienden), of van de mensen van wie u nooit meer wilt horen (spammers).

Opmerking
De **Witte lijst / Zwarte lijst** zijn ook bekend als respectievelijk de **Vriendenlijst/Spammerslijst**.

De **Vrienden-/Spammerslijsten** kunnen worden beheerd via de Instellingsconsole of via de Antispam-werkbalk die in enkele van de meest gebruikte e-mailclients wordt geïntegreerd.

Opmerking
Wij raden u aan de namen en e-mailadressen van uw vrienden toe te voegen aan de **Vriendenlijst**. BitDefender blokkeert geen berichten van de namen in de lijst. Door het toevoegen van vrienden bent u zeker dat rechtmatige berichten worden doorgelaten.

Tekensetfilter

Heel wat spamberichten zijn geschreven in Cyrillische en/of Aziatische tekensets. De tekensetfilter detecteert dit type berichten en labelt ze als SPAM.

Afbeeldingsfilter

Omdat het vermijden van de heuristische filterdetectie een ware uitdaging is geworden, wordt het Postvak IN tegenwoordig steeds meer overstelpt met berichten die een afbeelding met ongewenste inhoud bevatten. Om dit toenemende probleem aan te pakken, heeft BitDefender de **Afbeeldingsfilter** ingevoerd. deze filter vergelijkt de afbeeldingshandtekening van de e-mail met deze in de BitDefender-database. In geval de handtekening overeenkomst, wordt de e-mail als SPAM gelabeld.

URL-filter

Bijna alle spamberichten bevatten koppelingen naar verschillende weblocaties. Deze locaties bevatten doorgaans meer reclame en de mogelijkheid om zaken te kopen. Bovendien worden ze soms ook gebruikt voor phishing.

BitDefender houdt een database bij van dergelijke koppelingen. De URL-filter controleert elke URL-koppeling in een bericht ten opzichte van zijn database. Als een treffer is gevonden, wordt het bericht gelabeld als SPAM.

NeuNet (Heuristische) filter

De **NeuNet (Heuristische) filter** voert een aantal tests uit op alle componenten van het bericht (dus niet alleen op de koptekst, maar ook op het hoofdbericht in HTML- of tekstindeling). Hierbij wordt gezocht naar woorden, zinnen, koppelingen of andere

kenmerken van SPAM. Op basis van de resultaten van de analyse, voegt het programma een SPAM-score aan het bericht toe.

De filter detecteert ook berichten die in de onderwerpregel zijn gemarkeerd als `SEXUALLY-EXPLICIT:` en labelt ze als SPAM.

Opmerking
Sinds 19 mei 2004 moet spam met seksueel gericht materiaal de waarschuwing `SEXUALLY-EXPLICIT:` bevatten in de onderwerpregel anders kunnen boeten worden opgelegd voor het overtreden van de nationale wetgeving.

Bayes-filter

De **Bayes-filter**-module classificeert berichten volgens de statistische informatie met betrekking tot de snelheid waaraan specifieke woorden verschijnen in berichten die als SPAM zijn geclassificeerd, in vergelijking met de berichten die als NIET-SPAM werden bestempeld (door u of door de heuristische filter).

Wanneer een bepaald vierletterwoord bijvoorbeeld vaker voorkomt in een SPAM-bericht, ligt het voor de hand dat we veronderstellen dat er een grotere kans bestaat dat het volgende binnenkomende bericht met dit woord inderdaad SPAM IS. Alle relevante woorden in een bericht worden bij de controle in aanmerking genomen. Door een synthese te maken van de statistische informatie, wordt de algemene waarschijnlijkheid dat het volledige bericht SPAM is, berekend.

Bovendien beschikt deze module over een andere interessante eigenschap: hij kan worden opgeleid. Hij past zich snel aan het type berichten aan die door een bepaalde gebruiker worden ontvangen, en slaat alle informatie op. Voor een efficiënte werking, moet de filter worden opgeleid. Dit betekent dat hij voorbeelden van SPAM en van rechtmatige berichten moet krijgen, net zoals een hond wordt opgeleid om het spoor van een bepaalde geur te volgen. U moet de filter soms ook corrigeren en deze vragen zich aan te passen wanneer een verkeerde beslissing is genomen.

Belangrijk
U kunt de Bayes-module corrigeren door gebruik te maken van de knoppen **Is Spam** en **Geen Spam** in de Antispam-werkbalk.

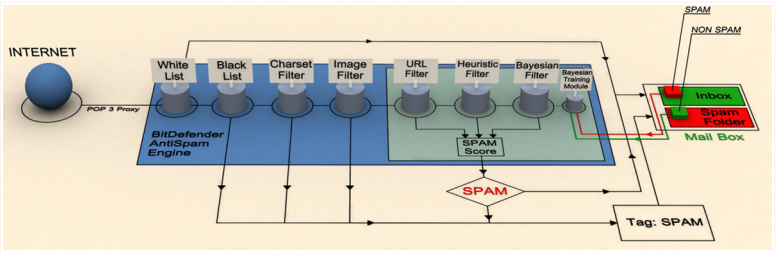
Opmerking
Telkens wanneer u een update uitvoert:

- worden nieuwe afbeeldingshandtekeningen toegevoegd aan de **Afbeeldingsfilter**.
- worden nieuwe koppelingen toegevoegd aan de **URL-filter**.
- Er worden nieuwe regels toegevoegd aan de **NeuNet (heuristische) filter**.

Dit zal de doeltreffendheid van uw Antispam-engine verbeteren.
BitDefender kan automatische updates uitvoeren om u te beschermen tegen spammers. Houd de optie **Automatische update** ingeschakeld.

9.1.2. Antispamgebruik

Het onderstaande schema toont u hoe BitDefender te werk gaat.



Antispamgebruik

De antispamfilters van het bovenstaande schema (Witte lijst, Zwarte lijst, Tekensetfilter, Afbeeldingsfilter, URL-filter, NeuNet (Heuristische) filter en Bayes-filter) worden in combinatie gebruikt door BitDefender om te bepalen of een bepaalde e-mail uw **Postvak IN** mag bereiken of niet.

Elke e-mail die van het internet komt, wordt eerst gecontroleerd volgens de filter Witte lijst/Zwarte lijst. Als het adres van de afzender in de Witte lijst wordt gevonden, wordt de e-mail rechtstreeks naar uw **Postvak IN** verplaatst.

Anders zal de filter Zwarte lijst de e-mail overnemen om te controleren of het adres van de afzender in zijn lijst voorkomt. De e-mail zal worden gelabeld als SPAM en naar de map **Spam** worden verplaatst (bevindt zich in Microsoft Outlook) als een overeenkomst is gevonden.

Anders zal de Tekensetfilter controleren of de e-mail in Cyrillische of Aziatische tekens is geschreven. Als dat het geval is, wordt de e-mail gelabeld als SPAM en verplaatst naar de map **Spam**.

Als de e-mail niet in Aziatische of Cyrillische tekens is geschreven, wordt hij doorgegeven naar de Afbeeldingsfilter. De **Afbeeldingsfilter** zal alle e-mailberichten detecteren die afbeeldingen met spaminhoud bevatten in de bijlage.

De URL-filter zal koppelingen zoeken en de gevonden koppelingen vergelijken met de koppelingen in de BitDefender-database. Wanneer een overeenkomstig gegeven wordt gevonden, wordt een SPAM-score toegevoegd aan de e-mail.

The NeuNet (Heuristische) filter zal de e-mail overnemen en een aantal tests uitvoeren op alle componenten van het bericht, waarbij wordt gezocht naar woorden, zinnen, koppelingen of andere kenmerken van Spam. Hierdoor zal eveneens een Spamscore aan de e-mail worden toegevoegd.

Opmerking
Als de e-mail het label SEXUALLY EXPLICIT vermeldt in de onderwerpregel, zal BitDefender dit bericht als SPAM beschouwen.

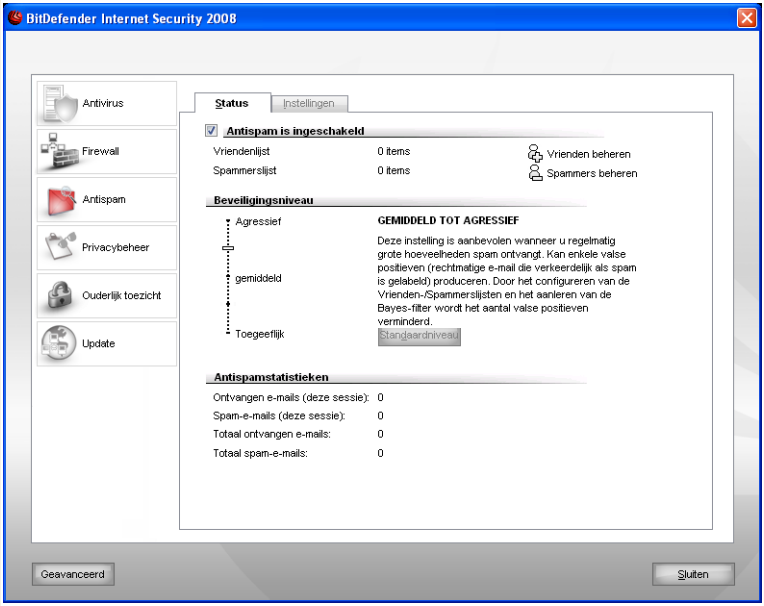
De module Bayes-filter zal het bericht verder analyseren volgens de statistische informatie met betrekking tot de snelheid waaraan specifieke woorden verschijnen in berichten die als SPAM zijn geclassificeerd, in vergelijking met de berichten die als NIET-SPAM werden bestempeld (door u of door de heuristische filter). Een Spamscore wordt aan de e-mail toegevoegd.

Als de samengevoegde score (URL-score + heuristische score + Bayes-score) de SPAM-score voor een bericht overschrijdt (ingesteld door de gebruiker in de sectie Status als een tolerantieniveau), dan wordt het bericht als SPAM beschouwd.

Belangrijk
Als u een andere e-mailclient dan Microsoft Outlook of Microsoft Outlook Exprees gebruikt, moet u een regel gebruiken om de e-mailberichten die door BitDefender als SPAM zijn gelabeld, te verplaatsen naar een aangepaste quarantainemap. BitDefender voegt het voorvoegsel `[SPAM]` toe aan het onderwerp van berichten die als SPAM worden beschouwd.

9.2. Antispamstatus

Om de antispambeveiliging te configureren, klikt u in de instellingsconsole op **Antispam>Status**. Het volgende venster wordt geopend:



Antispamstatus

In dit gedeelte kunt u de **Antispam**-module configureren en informatie over de activiteiten bekijken.

Belangrijk
Om te verhinderen dat spam uw **Postvak IN** binnendringt, moet u de **Antispamfilter** ingeschakeld houden.

In het gedeelte **Statistieken** kunt u de resultaten weergeven van de antispamactiviteit, voorgesteld per sessie (sinds u uw computer hebt opgestart) of met een overzicht (sinds de installatie van BitDefender).

Om de **Antispam**-module te configureren, moet u als volgt te werk gaan:

9.2.1. Stap 1 / 2 - Het tolerantieniveau instellen

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 5 tolerantieniveaus:

Tolerantieniveau	Beschrijving
Toegeeflijk	Biedt beveiliging voor accounts die veel rechtmatige commerciële e-mails ontvangen. De filter zal de meeste e-mail doorlaten, maar kan valse negatieven produceren (spam die als rechtmatige e-mail is geclassificeerd).
Toegeeflijk tot Gemiddeld	Biedt beveiliging voor accounts die enkele rechtmatige commerciële e-mails ontvangen. De filter zal de meeste e-mail doorlaten, maar kan valse negatieven produceren (spam die als rechtmatige e-mail is geclassificeerd).
Gemiddeld	Biedt beveiliging voor gewone accounts. De filter zal de meeste spam blokkeren, terwijl valse positieven worden vermeden.
Gemiddeld tot agressief	Biedt beveiliging voor accounts die regelmatige grote volumes spam ontvangen. De filter zal zeer weinig spam doorlaten, maar kan valse positieven produceren (rechtmatige e-mail die verkeerdelijk als spam is gelabeld). Configureer de **Vrienden-/Spammerslijsten** en leer de **Leerengine (Bayes)** aan om het aantal valse positieven te verminderen.
Agressief	Biedt beveiliging voor accounts die regelmatige zeer grote volumes spam ontvangen. De filter zal zeer weinig spam doorlaten, maar kan valse positieven produceren (rechtmatige e-mail die verkeerdelijk als spam is gelabeld).

Tolerantieniveau	Beschrijving
	Voeg uw contactpersonen toe aan de **Vriendenlijst** om het aantal valse positieven te verminderen.

Om het standaard beveiligingsniveau in te stellen (**Gemiddeld tot agressief**), klikt u op **Stand.niveau**.

9.2.2. Stap 2 / 2 - De lijst met adressen invullen

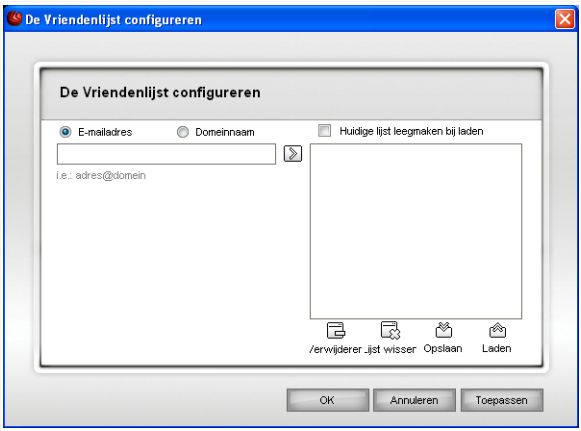
De lijsten met adressen bevatten informatie over e-mailadressen die u rechtmatige e-mails of spam zenden.

Vriendenlijst

De **Vriendenlijst** is een lijst van alle e-mailadressen waarvan u altijd berichten wilt ontvangen, ongeacht hun inhoud. Berichten van uw vrienden zijn niet als spam gelabeld, zelfs wanneer de inhoud op spam lijkt.

Opmerking
Elke e-mail die afkomstig is van een adres in de **Vriendenlijst**, wordt automatisch en zonder verdere verwerking in uw Postvak IN geleverd.

Om de **Vriendenlijst** te beheren, klikt u op  (in overeenstemming met de **Vriendenlijst**) of klikt u op de knop  **Vrienden** in de Antispam-werkbalk.



Vriendenlijst

Hier kunt u gegevens toevoegen aan of verwijderen uit de **Vriendenlijst**.

Als u een e-mailadres wilt toevoegen, schakelt u de optie **E-mailadres** in, typt u het adres en klikt u op ⊠. Het adres wordt weergegeven in de **Vriendenlijst**.

Belangrijk
Syntaxis: naam@domein.com.

Als u een domein wilt toevoegen, schakelt u de optie **Domeinnaam** in, typt u het domein en klikt u op ⊠. Het domein wordt weergegeven in de **Vriendenlijst**.

Belangrijk
Syntaxis:

- @domein.com, *domein.com en domein.com - alle ontvangen e-mailberichten van domein.com zullen uw **Postvak IN** bereiken, ongeacht hun inhoud;
- *domein* - alle ontvangen e-mailberichten van domein (ongeacht de domeinachtervoegsels) zullen uw **Postvak IN** bereiken, ongeacht hun inhoud;
- *com* - alle ontvangen e-mailberichten die het domeinachtervoegsel com hebben, zullen uw **Postvak IN** bereiken, ongeacht hun inhoud;

Om een item uit de lijst verwijderen, selecteert u het item en klikt u op de knop **Verwijderen**. Als u op de knop **Lijst wissen** klikt, zult u alle gegevens uit de lijst verwijderen. Maar let op: u kunt ze niet meer herstellen.

Gebruik de knoppen **Opslaan**/ **Laden** om de **Vriendenlijst** op te slaan / te laden op de gewenste locatie. Het bestand zal de extensie `.bwl` hebben.

Om de inhoud van de huidige lijst opnieuw in te stellen wanneer u een eerder opgeslagen lijst laadt, selecteert u **Huidige lijst leegmaken bij laden**.

Opmerking
Wij raden u aan de namen en e-mailadressen van uw vrienden toe te voegen aan de **Vriendenlijst**. BitDefender blokkeert geen berichten van de namen in de lijst. Door het toevoegen van vrienden bent u zeker dat rechtmatige berichten worden doorgelaten.

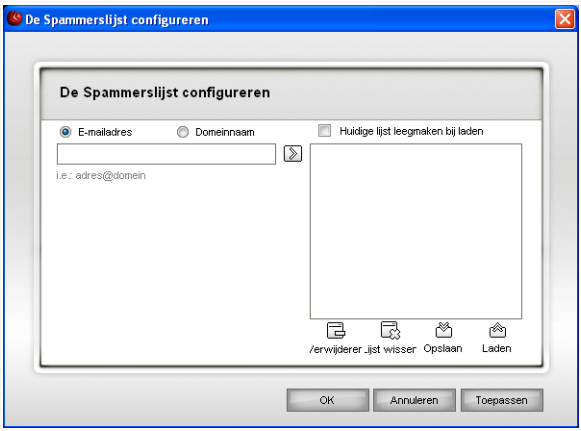
Klik op **Toepassen** en **OK** om de **Vriendenlijst** op te slaan en te sluiten.

Spammerslijst

De **Spammerslijst** is een lijst van alle e-mailadressen waarvan u geen berichten wilt ontvangen, ongeacht hun inhoud.

Opmerking
Alle e-mailberichten die worden ontvangen van een adres van de **Spammerslijst**, worden automatisch en zonder verdere verwerking als SPAM gelabeld.

Om de **Spammerslijst** te beheren, klikt u op (in overeenstemming met de **Spammerslijst**) of klikt u op de knop **Spammers** in de Antispam-werkbalk.



Spammerslijst

Hier kunt u gegevens toevoegen aan of verwijderen uit de **Spammerslijst**.

Als u een e-mailadres wilt toevoegen, schakelt u de optie **E-mailadres** in, typt u het adres en klikt u op ⊠. Het adres wordt weergegeven in de **Spammerslijst**.

Belangrijk
Syntaxis: naam@domein.com.

Als u een domein wilt toevoegen, schakelt u de optie **Domeinnaam** in, typt u het domein en klikt u op ⊠. Het domein wordt weergegeven in de **Spammerslijst**.

Belangrijk
Syntaxis:

- @domein.com, *domein.com en domein.com - alle ontvangen e-mailberichten van domein.com worden als SPAM gelabeld;
- *domein* - alle ontvangen e-mailberichten van domein (ongeacht de domeinachtervoegsels), worden als SPAM gelabeld;
- *com* - alle ontvangen e-mailberichten met het domeinachtervoegsel com als SPAM gelabeld;

Om een item uit de lijst verwijderen, selecteert u het item en klikt u op de knop **Verwijderen**. Als u op de knop **Lijst wissen** klikt, zult u alle gegevens uit de lijst verwijderen. Maar let op: u kunt ze niet meer herstellen.

Gebruik de knoppen **Opslaan**/ **Laden** om de **Spammerlijst** op te slaan / te laden op de gewenste locatie. Het bestand zal de extensie `.bwl` hebben.

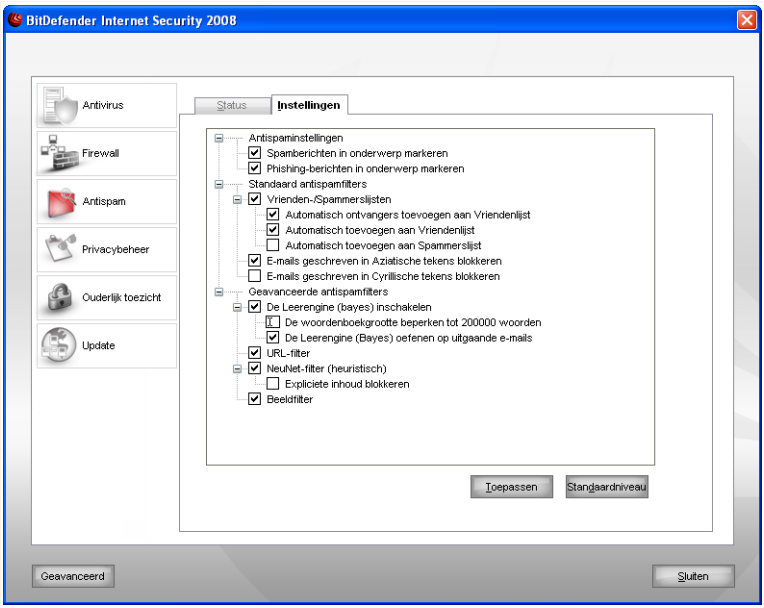
Om de inhoud van de huidige lijst opnieuw in te stellen wanneer u een eerder opgeslagen lijst laadt, selecteert u **Huidige lijst leegmaken bij laden**.

Klik op **Toepassen** en **OK** om de **Spammerslijst** op te slaan en te sluiten.

Belangrijk
Als u BitDefender opnieuw wilt installeren, is het aanbevolen de **Vrienden-** / **Spammerslijsten** vooraf op te slaan. Nadat het programma opnieuw is geïnstalleerd kunt u deze lijsten opnieuw laden.

9.3. Antispam-instellingen

Om de antispaminstellingen te configureren, klikt u in de instellingsconsole op **Antispam>Instellingen**. Het volgende venster wordt geopend:



Antispam-instellingen

Hier kunt u elke Antispam-filter in-/uitschakelen en kunt u enkele andere instellingen met betrekking tot de Antispam-module opgeven.

Er zijn drie categorieën opties beschikbaar (**Antispam-instellingen**, **Standaard antispamfilters** en **Geavanceerde antispamfilters**) die zijn geordend als een uitvouwbaar menu zoals de menu's van Windows.

Opmerking
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.

9.3.1. Antispam-instellingen

- **Spamberichten in onderwerp markeren** - alle e-mailberichten die als spam worden beschouwd, zullen in het onderwerp worden gelabeld met SPAM.

- **Phishing-berichten in onderwerp markeren** - alle e-mailberichten die als phishing-berichten worden beschouwd, zullen in het onderwerp worden gelabeld met SPAM.

9.3.2. Standaard antispamfilters

- **Vrienden-/Spammerslijst** - activeert/deactiveert de Vrienden-/Spammerslijsten.
  - **Geadresseerden automatisch toevoegen aan Vriendenlijst** - voeg automatisch geadresseerden van verzonden e-mail toe aan de Vriendenlijst.
  - **Automatisch toevoegen aan Vriendenlijst** - wanneer u de volgende keer klikt op de knop **Geen spam** in de Antispam-werkbalk, wordt de afzender automatisch toegevoegd aan de **Vriendenlijst**.
  - **Automatisch toevoegen aan Spammerslijst** - wanneer u de volgende keer klikt op de knop **Geen spam** in de Antispam-werkbalk, wordt de afzender automatisch toegevoegd aan de **Spammerslijst**.

Opmerking
De knoppen **Geen spam** en **Is spam** worden gebruikt om de Bayes-filter aan te leren.

- **E-mails geschreven in Aziatische tekens blokkeren** - blokkeert berichten die in Aziatische tekensets zijn geschreven.
- **E-mails geschreven in Cyrillische tekens blokkeren** - blokkeert berichten die in Cyrillische tekensets zijn geschreven.

9.3.3. Geavanceerde antispamfilters

- **De Leerengine (bayes) inschakelen** - activeert/deactiveert de Leerengine (bayes).
  - **De woordenboekgrootte beperken tot 200000 woorden** - met deze optie kunt u de grootte van het Bayes-woordenboek instellen. Kleiner is sneller, groter is nauwkeuriger.

Opmerking
De aanbevolen grootte is: 200.000 woorden.

  - **De Leerengine (Bayes) oefenen op uitgaande e-mails** - oefent de Leerengine (bayes) op uitgaande e-mails.
- **URL-filter** - activeert/deactiveert de URL-filter.
- **NeuNet (Heuristische) filter** - activeert/deactiveert de NeuNet (Heuristische) filter.

- **Expliciete inhoud blokkeren** - activeert/deactiveert de detectie van berichten met de melding SEXUALLY EXPLICIT in de onderwerpregel.

■ **Afbeeldingsfilter** - activeert/deactiveert de Afbeeldingsfilter.

Opmerking
Schakel het selectievakje naast een optie in/uit om de optie in/uit te schakelen.

Klik op **Toepassen** om de wijzigingen op te slaan of klik op **Stand.niveau** om de standaardinstellingen te laden.

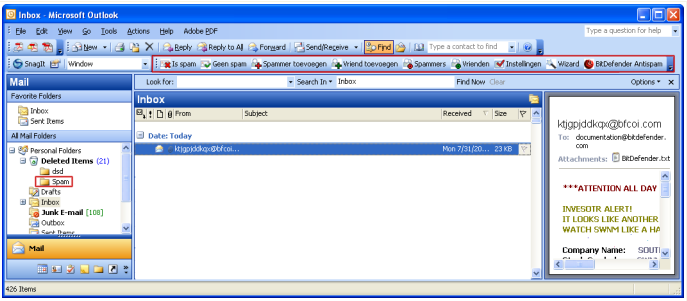
9.4. Integratie in e-mailclients

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

- Microsoft Outlook
- Outlook Express
- Windows Mail
- Mozilla Thunderbird

9.4.1. Antispam-werkbalk

Bovenaan in uw e-mailclient ziet u de antispamwerkbalk.



Antispam-werkbalk

Belangrijk
Het verschil tussen BitDefender AntiSpam voor Microsoft Outlook of Outlook Express / Windows Mail is dat de SPAM-berichten voor Microsoft Outlook naar de map **Spam**

worden verplaatst en bij Outlook Express / Windows Mail naar de map **Verwijderde items**. In beide gevallen worden de berichten in de onderwerpregel gelabeld als SPAM.

De map **Spam** wordt automatisch door BitDefender gemaakt in Microsoft Outlook en wordt weergegeven op hetzelfde niveau van de items van de **Mappenlijst**(Agenda, Contactpersonen, enz.).

Elke knop van de BitDefender-werkbalk wordt hieronder uitgelegd.

- **Is spam** - verzendt een bericht naar de Bayes-module met de melding dat de geselecteerde e-mail spam is. De e-mail wordt gelabeld als SPAM en naar de map **Spam** verplaatst.

  De toekomstige e-mailberichten die aan dezelfde patronen voldoen, zullen als SPAM worden gelabeld.

  Opmerking
  U kunt één e-mail of zoveel e-mails als u zelf wilt selecteren.

- **Geen spam** - verzendt een bericht naar de Bayes-module met de melding dat de geselecteerde e-mail geen spam is en dat BitDefender dit niet als spam mocht aangeven. De e-mail wordt verplaatst van de map **Spam** naar de map **Postvak IN**.

  De toekomstige e-mailberichten die aan dezelfde patronen voldoen, zullen niet langer als SPAM worden gelabeld.

  Opmerking
  U kunt één e-mail of zoveel e-mails als u zelf wilt selecteren.

  Belangrijk
  De knop **Geen spam** wordt actief wanneer u een bericht selecteert dat door BitDefender als SPAM is gemarkeerd (normaal bevinden deze berichten zich in de map **Spam**).

- **Spammer toevoegen** - voegt de afzender van de geselecteerde e-mail toe aan de **Spammerslijst**.

Spammer toevoegen

Selecteer **Dit bericht niet meer weergeven** als u niet om bevestiging wilt worden gevraagd wanneer u een adres van een spammer toevoegt aan de lijst.

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

De toekomstige e-mailberichten van dat adres zullen als SPAM worden gelabeld.

Opmerking
U kunt één afzender of zoveel afzenders als u zelf wilt selecteren.

- **Vriend toevoegen** - voegt de afzender van de geselecteerde e-mail toe aan de **Vriendenlijst**.

Vriend toevoegen

Selecteer **Dit bericht niet meer weergeven** als u niet om bevestiging wilt worden gevraagd wanneer u een adres van een vriend toevoegt aan de lijst.

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

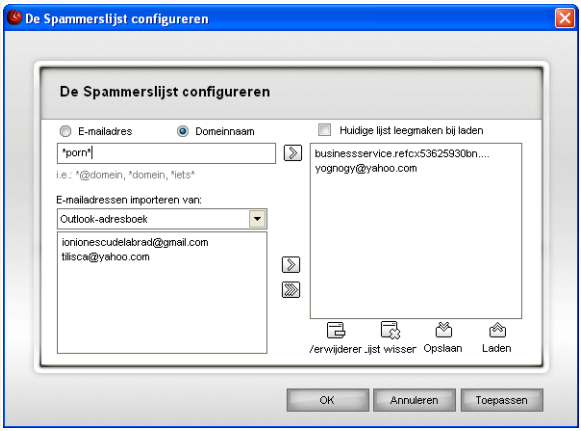
U zult e-mailberichten van dit adres altijd ontvangen, ongeacht de inhoud.

Opmerking
U kunt één afzender of zoveel afzenders als u zelf wilt selecteren.

- **Spammers** - opent de **Spammerslijst** die alle e-mailadressen bevatten waarvan u geen berichten wilt ontvangen, ongeacht hun inhoud.

Opmerking

Alle e-mailberichten die worden ontvangen van een adres van de **Spammerslijst**, worden automatisch en zonder verdere verwerking als SPAM gelabeld.



Spammerslijst

Hier kunt u gegevens toevoegen aan of verwijderen uit de **Spammerslijst**.

Als u een e-mailadres wilt toevoegen, schakelt u de optie **E-mailadres** in, typt u het adres en klikt u op de knop ⊠. Het adres wordt weergegeven in de **Spammerslijst**.

Belangrijk

Syntaxis: naam@domein.com.

Als u een domein wilt toevoegen, schakelt u de optie **Domeinnaam** in, typt u het domein en klikt u op de knop ⊠. Het domein wordt weergegeven in de **Spammerslijst**.

Belangrijk

Syntaxis:

- @domein.com, *domein.com en domein.com - alle ontvangen e-mailberichten van domein.com worden als SPAM gelabeld;
- *domein* - alle ontvangen e-mailberichten van domein (ongeacht de domeinachtervoegsels), worden als SPAM gelabeld;

- *com* - alle ontvangen e-mailberichten met het domeinachtervoegsel com als SPAM gelabeld;

Om e-mailadressen te importeren uit het **adresboek van Windows** / **de mappen van Outlook Express** in **Microsoft Outlook** / **Outlook Express** / **Windows Mail**, selecteert u de geschikte optie in het vervolgkeuzemenu **E-mailadressen importeren van**.

Voor **Microsoft Outlook Express / Windows Mail** wordt een nieuw venster geopend waarin u de map kunt selecteren met de e-mailadressen die u aan de **Spammerslijst** wilt toevoegen. Kies de adressen en klik op **Selecteren**.

In beide gevallen zullen de e-mailadressen in de importlijst verschijnen. Selecteer de gewenste adressen en klik op om ze toe te voegen aan de **Spammerslijst**. Als u op klikt, worden alle e-mailadressen toegevoegd aan de lijst.

Om een item uit de lijst verwijderen, selecteert u het item en klikt u op de knop **Verwijderen**. Als u op de knop **Lijst wissen** klikt, zult u alle gegevens uit de lijst verwijderen. Maar let op: u kunt ze niet meer herstellen.

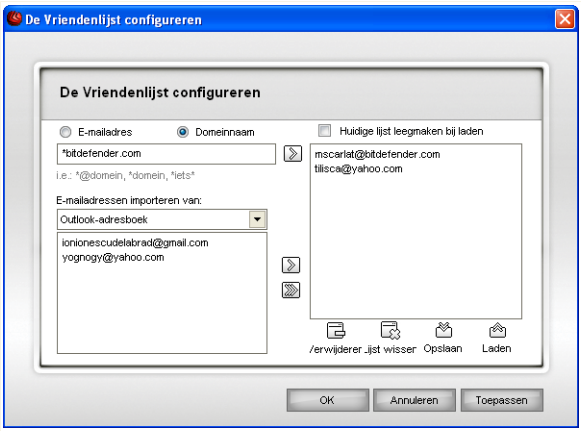
Gebruik de knoppen **Opslaan**/ **Laden** om de **Spammerlijst** op te slaan / te laden op de gewenste locatie. Het bestand zal de extensie `.bwl` hebben.

Om de inhoud van de huidige lijst opnieuw in te stellen wanneer u een eerder opgeslagen lijst laadt, selecteert u **Huidige lijst leegmaken bij laden**.

Klik op **Toepassen** en **OK** om de **Spammerslijst** op te slaan en te sluiten.

- **Vrienden** - opent de **Vriendenlijst** die alle e-mailadressen bevatten waarvan u altijd e-mailberichten wilt ontvangen, ongeacht hun inhoud.

Opmerking
Elke e-mail die afkomstig is van een adres in de **Vriendenlijst**, wordt automatisch en zonder verdere verwerking in uw Postvak IN geleverd.



Vriendenlijst

Hier kunt u gegevens toevoegen aan of verwijderen uit de **Vriendenlijst**.

Als u een e-mailadres wilt toevoegen, schakelt u de optie **E-mailadres** in, typt u het adres en klikt u op de knop . Het adres wordt weergegeven in de **Spammerslijst**.

Belangrijk
Syntaxis: naam@domein.com.

Als u een domein wilt toevoegen, schakelt u de optie **Domeinnaam** in, typt u het domein en klikt u op de knop . Het domein wordt weergegeven in de **Vriendenlijst**.

Belangrijk
Syntaxis:

- @domein.com, *domein.com en domein.com - alle ontvangen e-mailberichten van domein.com zullen uw **Postvak IN** bereiken, ongeacht hun inhoud;
- *domein* - alle ontvangen e-mailberichten van domein (ongeacht de domeinachtervoegsels) zullen uw **Postvak IN** bereiken, ongeacht hun inhoud;
- *com* - alle ontvangen e-mailberichten die het domeinachtervoegsel com hebben, zullen uw **Postvak IN** bereiken, ongeacht hun inhoud;

Om e-mailadressen te importeren uit het **adresboek van Windows** / **de mappen van Outlook Express** in **Microsoft Outlook** / **Outlook Express** / **Windows Mail**,

selecteert u de geschikte optie in het vervolgkeuzemenu **E-mailadressen importeren van**.

Voor **Microsoft Outlook Express / Windows Mail** wordt een nieuw venster geopend waarin u de map kunt selecteren met de e-mailadressen die u aan de **Vriendenlijst** wilt toevoegen. Kies de adressen en klik op **Selecteren**.

In beide gevallen zullen de e-mailadressen in de importlijst verschijnen. Selecteer de gewenste adressen en klik op om ze toe te voegen aan de **Vriendenlijst**. Als u op klikt, worden alle e-mailadressen toegevoegd aan de lijst.

Om een item uit de lijst verwijderen, selecteert u het item en klikt u op de knop **Verwijderen**. Als u op de knop **Lijst wissen** klikt, zult u alle gegevens uit de lijst verwijderen. Maar let op: u kunt ze niet meer herstellen.

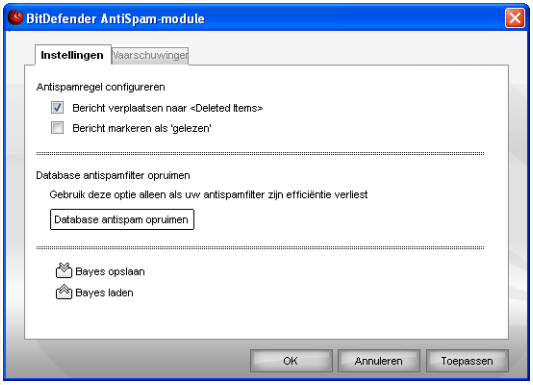
Gebruik de knoppen **Opslaan**/ **Laden** om de **Vriendenlijst** op te slaan / te laden op de gewenste locatie. Het bestand zal de extensie `.bwl` hebben.

Om de inhoud van de huidige lijst opnieuw in te stellen wanneer u een eerder opgeslagen lijst laadt, selecteert u **Huidige lijst leegmaken bij laden**.

Opmerking
Wij raden u aan de namen en e-mailadressen van uw vrienden toe te voegen aan de **Vriendenlijst**. BitDefender blokkeert geen berichten van de namen in de lijst. Door het toevoegen van vrienden bent u zeker dat rechtmatige berichten worden doorgelaten.

Klik op **Toepassen** en **OK** om de **Vriendenlijst** op te slaan en te sluiten.

- **Instellingen** - opent het venster **Instellingen** waarin u sommige opties kunt opgeven voor de **Antispam**-module.



Instellingen

De volgende opties zijn beschikbaar:

- **Bericht verplaatsen naar Verwijderde items** - verplaatst de spamberichten naar de map **Verwijderde items** (alleen voor Microsoft Outlook Express/ Windows Mail);
- **Bericht markeren als 'gelezen'** - markeert alle spamberichten als gelezen, zodat ze geen hinder vormen als nieuwe spamberichten binnenkomen.

Als uw antispamfilter zeer onnauwkeurig is, zult u mogelijk de filterdatabase moeten opruimen en de Bayes-filter opnieuw moeten aanleren. Klik op **Database antispam opruimen** om de Bayes-database opnieuw in te stellen.

Gebruik de knoppen **Opslaan**/ **Laden** om de lijst van de Bayes-database op te slaan / te laden op de gewenste locatie. Het bestand zal de extensie `.dat` hebben.

Klik op het tabblad **Waarschuw.** als u toegang wilt tot het gedeelte waar u de weergave van bevestigingsvensters kunt uitschakelen voor de knoppen **Spammer toevoegen** en **Vriend toevoegen**.

Opmerking
In het venster **Waarschuw.** kunt u ook de weergave van de waarschuwing **Selecteer een e-mailbericht** in- of uitschakelen. De waarschuwing verschijnt wanneer u een groep selecteert in plaats van een e-mailbericht.

- **Wizard** - opent de wizard die u zal begeleiden bij het aanleren van de Bayes-filter zodat de efficiëntie van BitDefender Antispam nog wordt verbeterd. U kunt ook adressen van uw **Adresboek** toevoegen aan uw **Vriendenlijst** / **Spammerslijst**.

- **BitDefender Antispam** - opent de Beheerconsole.

9.4.2. Configuratiewizard voor Antispam

Als u uw e-mailclient voor de eerste keer uitvoert nadat u BitDefender hebt geïnstalleerd, verschijnt een wizard die u zal helpen bij het configureren van de Vriendenlijst en de Spammerslijst en bij het aanleren van de Bayes-filter om de efficiëntie van de antispamfilter te vergroten.

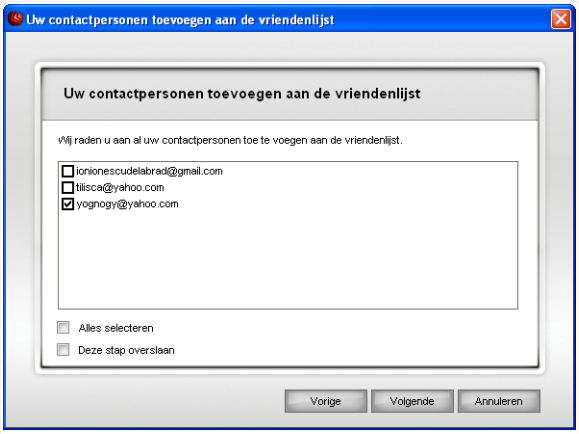
Opmerking
De wizard kan ook op elk ander ogenblik worden gestart door op de knop **Wizard** in de Antispam-werkbalk te klikken.

Stap 1/6 – Welkomstvenster

Welkomstvenster

Klik op **Volgende**.

Stap 2/6 – De Vriendenlijst opstellen



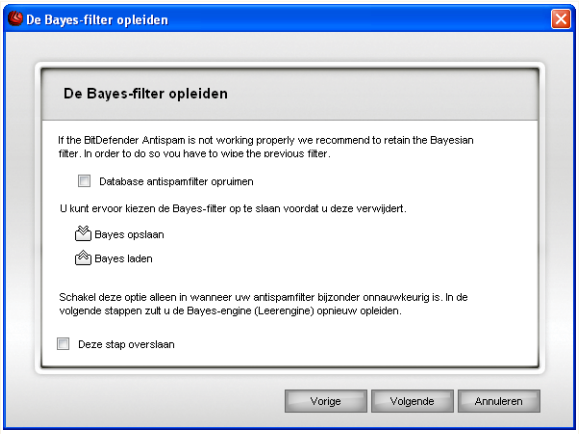
De Vriendenlijst opstellen

Hier kunt u alle adressen van uw **Adresboek** bekijken. Selecteer de adressen die u wilt toevoegen aan uw **Vriendenlijst** (wij raden u aan ze allemaal te selecteren). U zult alle e-mails ontvangen die van deze adressen komen, ongeacht hun inhoud.

Schakel het selectievakje **Alles selecteren** in om al uw contactpersonen toe te voegen aan de Vriendenlijst.

Selecteer **Deze stap overslaan** als u meteen naar de volgende stap wilt gaan. Klik op **Vorige** om terug te keren naar de vorige stap of klik op **Volgende** om door te gaan met de wizard.

Stap 3/6 – De Bayes-database verwijderen



De Bayes-database verwijderen

U kunt mogelijk merken dat het efficiënte gebruik van de antispamfilter afneemt. Dit kan te wijten zijn aan een onjuiste opleiding. (d.w.z dat u per ongeluk een aantal geldige berichten als spam hebt gelabeld, of omgekeerd). Als uw filter bijzonder onnauwkeurig is, zult u wellicht de filterdatabase moeten opruimen en de filter opnieuw opleiden door de volgende stappen van deze wizard te volgen.

Selecteer **Database antispamfilter opruimen** als u de Bayes-database opnieuw wilt instellen.

Gebruik de knoppen **Opslaan**/ **Laden** om de lijst van de Bayes-database op te slaan / te laden op de gewenste locatie. Het bestand zal de extensie `.dat` hebben.

Selecteer **Deze stap overslaan** als u meteen naar de volgende stap wilt gaan. Klik op **Vorige** om terug te keren naar de vorige stap of klik op **Volgende** om door te gaan met de wizard.

Stap 4/6 - De Bayes-filter opleiden met rechtmatige e-mail

De Bayes-filter opleiden met rechtmatige e-mail

Selecteer een map die rechtmatige e-mails bevat. Deze berichten zullen worden gebruikt om de antispamfilter op te leiden.

Onder de maplijst zijn er twee geavanceerde opties:

- **Inclusief submappen** - om de submappen op te nemen in uw selectie.
- **Automatisch toevoegen aan vriendenlijst** - om de afzenders toe te voegen aan de **Vriendenlijst**.

Selecteer **Deze stap overslaan** als u meteen naar de volgende stap wilt gaan. Klik op **Vorige** om terug te keren naar de vorige stap of klik op **Volgende** om door te gaan met de wizard.

Stap 5/6 - De Bayes-filter opleiden met spam

De Bayes-filter opleiden met spam

Selecteer een map die spam e-mails bevat. Deze berichten zullen worden gebruikt om de antispamfilter op te leiden.

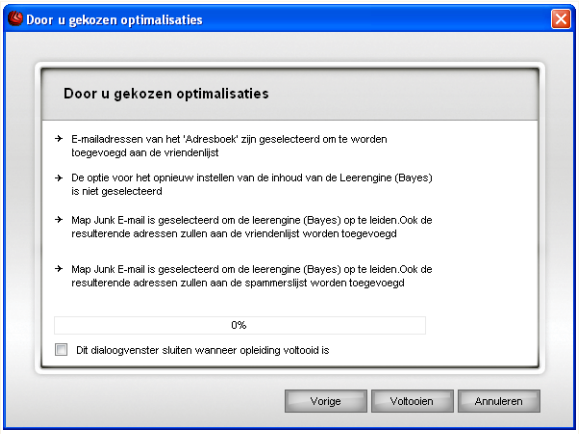
Belangrijk
Zorg ervoor dat de map die u selecteert geen enkele rechtmatige e-mail bevat, anders zal de prestatie van de antispam aanzienlijk verminderen.

Onder de maplijst zijn er twee geavanceerde opties:

- **Inclusief submappen** - om de submappen op te nemen in uw selectie.
- **Automatisch toevoegen aan spammerslijst** - om de afzenders toe te voegen aan de **Spammerslijst**.

Selecteer **Deze stap overslaan** als u meteen naar de volgende stap wilt gaan. Klik op **Vorige** om terug te keren naar de vorige stap of klik op **Volgende** om door te gaan met de wizard.

Stap 6/6 – Overzicht



Overzicht

Hier kunt u alle instellingen voor de configuratiewizard bekijken. U kunt eventuele wijzigingen aanbrengen door terug te keren naar de vorige stappen (klik op **Vorige**).

Als u geen wijzigingen wilt aanbrengen, klikt u op **Voltooien** om de wizard af te sluiten.

10. Privacybeheer

BitDefender controleert tientallen potentiële "hotspots" in uw systeem waar spyware kan optreden en controleert ook alle wijzigingen aan uw systeem en software. Hij 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.

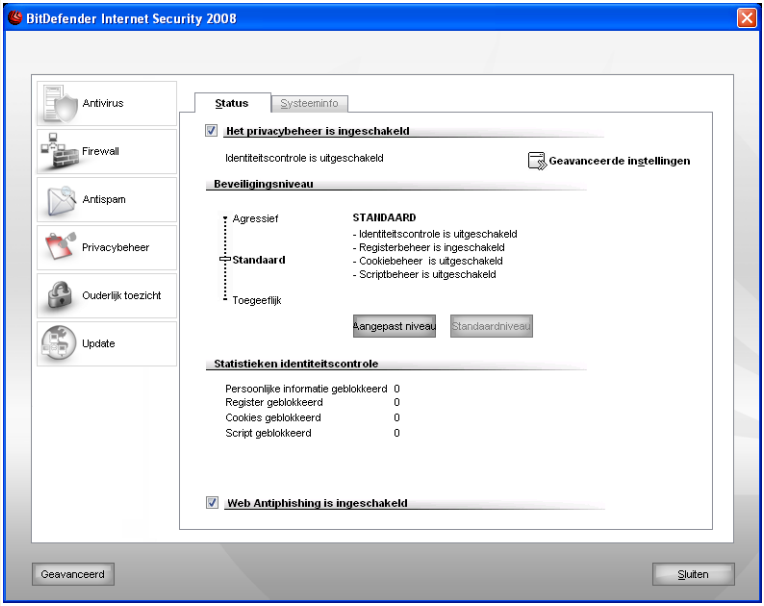
BitDefender scant ook de websites die u bezoekt en waarschuwt u als er een phishing-bedreiging is gedetecteerd.

Het gedeelte **Privacybeheer** in deze gebruiksaanwijzing bevat de volgende onderwerpen:

- Status Privacybeheer
- Geavanceerde instellingen - Identiteitscontrole
- Geavanceerde instellingen - Registerbeheer
- Geavanceerde instellingen - Cookiebeheer
- Geavanceerde instellingen - Scriptbeheer
- Systeeminformatie
- Antiphishing-werkbalk

10.1. Status Privacybeheer

Om het Privacybeheer te configureren en informatie met betrekking tot zijn activiteit te bekijken, klikt u op **Privacybeheer>Status** in de instellingsconsole. Het volgende venster wordt geopend:



Status Privacybeheer

10.1.1. Privacybeheer

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

Het Privacybeheer beveiligt uw computer met 5 belangrijke beveiligingselementen:

- Identiteitscontrole - beschermt uw vertrouwelijke gegevens door al het uitgaande HTTP- en SMTP-verkeer te filteren volgens de regels die u in de sectie Identiteit hebt gemaakt.

Opmerking
Aan het eind van de sectie ziet u de **Identiteitscontrole statistieken**.

- 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.

Om de instellingen voor deze beheeropties te configureren, klikt u op Geavanceerde instellingen.

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 **Stand.niveau** om de schuifregelaar op het standaardniveau in te stellen.

10.1.2. Antiphishing-beveiliging

Phishing is een criminele activiteit op het internet dat sociale technieken gebruikt om mensen door een list te overhalen persoonlijke informatie te geven.

In de meeste gevallen bestaan phishing-pogingen uit het verzenden van grote hoeveelheden e-mailberichten die valselijk beweren dat ze van een gevestigde, wettelijke onderneming afkomstig zijn. Deze valse berichten worden verzonden in de hoop dat er minstens enkele ontvangers die overeenkomen met het profiel van het phishing-doel, zullen worden overgehaald om persoonlijke informatie vrij te geven.

Een phishing-bericht vermeldt doorgaans een probleem met betrekking tot uw online rekening. Het probeert u te overtuigen om op een koppeling in het bericht te klikken om toegang te krijgen tot een zogenaamde wettelijke website (die in feite een vervalste site is) waar persoonlijke gegevens vereist zijn. U kunt bijvoorbeeld worden gevraagd de gegevens van uw rekening, zoals de gebruikersnaam en het wachtwoord, te bevestigen en het nummer van uw bankrekening of uw nummer bij de sociale zekerheid op te geven. Om nog overtuigender over te komen, kan het bericht soms doen alsof uw rekening al werd of mogelijk zal worden opgeschort als u de bijgeleverde koppeling niet gebruikt.

Phishing maakt ook gebruik van spyware, zoals Trojaanse paarden met toetsenregistratie, om de rekeninginformatie rechtstreeks van uw computer te stelen.

De belangrijkste doelwitten van phishing-pogingen zijn klanten van online betalingsdiensten, zoals eBay en Paypal, evenals banken die online diensten aanbieden. Onlangs werden ook gebruikers van websites van sociale netwerken belaagd door phishing om persoonlijke identificatiegegevens te verkrijgen die worden gebruikt voor identiteitsdiefstal.

Om u tegen phishing-pogingen te beveiligen, moet u **Antiphishing** ingeschakeld houden. Op deze manier zal BitDefender elke website scannen voordat u deze kunt bezoeken en wordt u op de hoogte gebracht van het bestaan van elke phishing-bedreiging. U kunt een Witte lijst configureren van websites die niet door BitDefender moeten worden gescand.

Om de antiphishing-beveiliging en de Witte lijst gemakkelijk te beheren, kunt u de werkbalk van BitDefender Antiphishing gebruiken die in Internet Explorer is geïntegreerd. Meer informatie vindt u onder “*Antiphishing-werkbalk*” (p. 154).

10.2. Geavanceerde instellingen - Identiteitscontrole

Het veilig houden van vertrouwelijke gegevens is een belangrijke kwestie die ons allen aanbelangt. 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 de verkeerde handen terechtkomen, kunnen ze u schade berokkenen. U kunt worden overspoeld door spamberichten of u kunt plotseling voor een onaangename verrassing komen te staan als u ziet dat uw rekening is leeggeplunderd.

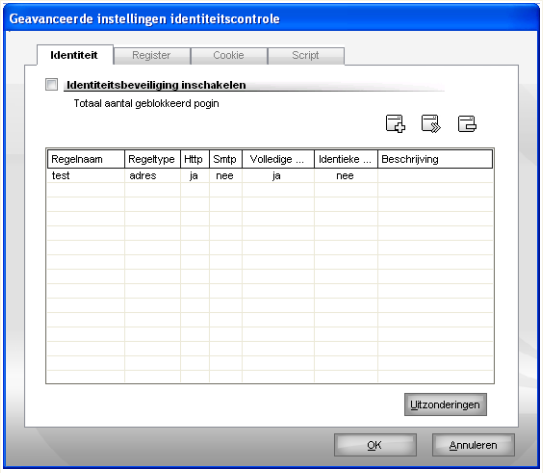
Identiteitscontrole helpt u vertrouwelijke gegevens veilig te houden. Hiermee wordt HTTP-, SMTP-verkeer, of beide gescand op bepaalde tekenreeksen die u hebt

gedefinieerd. Als een overeenkomst is gevonden, wordt de desbetreffende webpagina of e-mail geblokkeerd.

Er is ondersteuning voorzien voor meerdere gebruikers, zodat geen enkele andere gebruiker van het systeem de regels die u hebt geconfigureerd, kan zien.

De privacyregels kunnen worden geconfigureerd in de sectie **Identiteit**. Om toegang te krijgen tot deze sectie, opent u het venster **Geavanceerde instellingen Privacybeheer** en klikt u op het tabblad **Identiteit**.

Opmerking
Om het venster **Geavanceerde instellingen Privacybeheer** te openen, klikt u op **Privacybeheer>Status** in de instellingsconsole en klikt u op **Geavanceerde instellingen**.



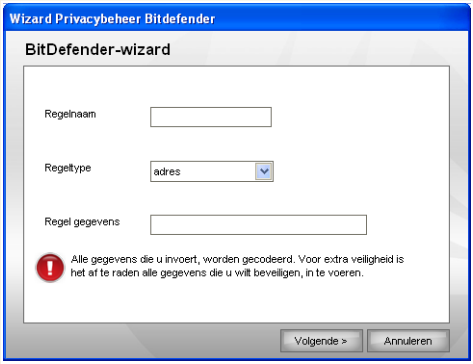
Identiteitscontrole

10.2.1. Privacyregels maken

De regels moeten handmatig worden ingevoerd (klik op de knop **Toevoegen** en kies de parameters voor de regel). De configuratiewizard wordt geopend.

De configuratiewizard is een procedure die uit 3 stappen bestaat.

Stap 1/3 - Type en gegevens van de regel instellen



Type en gegevens van de regel instellen

Voer de naam in van de regel in het bewerkingsveld.

U moet de volgende parameters instellen:

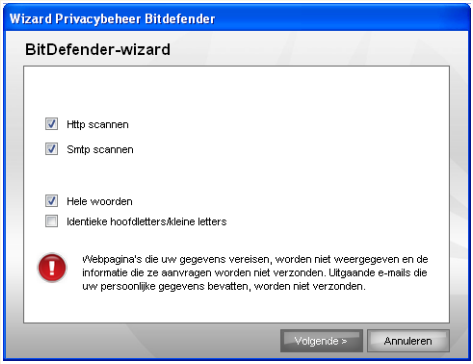
- **Regeltype** - kies het type regel (adres, naam, creditcard, PIN, SSN, enz.).
- **Regelgegevens** - voer de gegevens voor de regel in.

> ***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 verkeerdelijk worden geblokkeerd.

Alle gegevens die u invoert, worden gecodeerd. Voor extra veiligheid mag u niet alle gegevens invoeren die u wilt beschermen.

Klik op **Volgende**.

Stap 2/3 - Verkeer selecteren



Verkeer selecteren

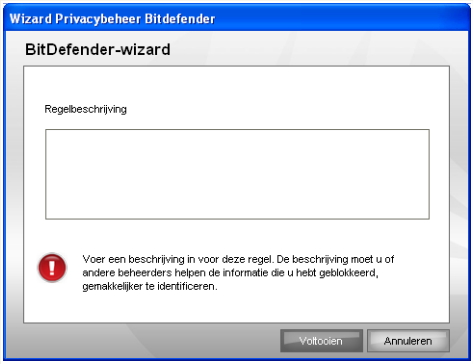
Selecteer het verkeer dat u door BitDefender wilt laten scannen. De volgende opties zijn beschikbaar:

- **HTTP scannen** - scant het HTTP-verkeer (web) en blokkeert uitgaande gegevens die overeenkomen met de regelgegevens.
- **SMTP scannen** - scant het SMTP-verkeer (e-mail) en blokkeert uitgaande e-mailberichten die de regelgegevens bevatten.

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

Klik op **Volgende**.

Stap 3/3 - Regel beschrijven



Regel beschrijven

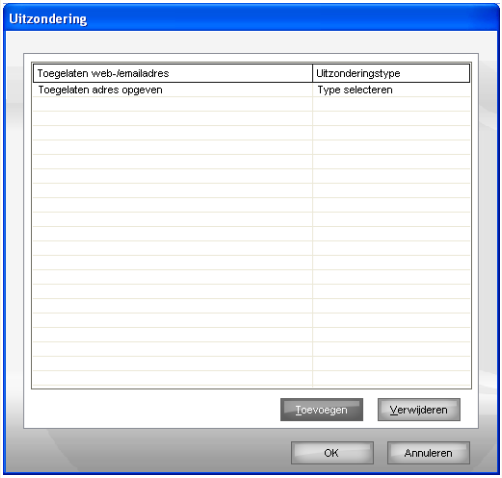
Voer een korte beschrijving in van de regel in het bewerkingsveld.

Klik op **Voltooien**.

10.2.2. 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 respectievelijke 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 of het e-mailadres op dat u wilt toevoegen als uitzondering.
3. Dubbelklik op **Type selecteren** 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 uit de lijst te verwijderen, selecteert u deze en klikt u op **Verwijderen**.

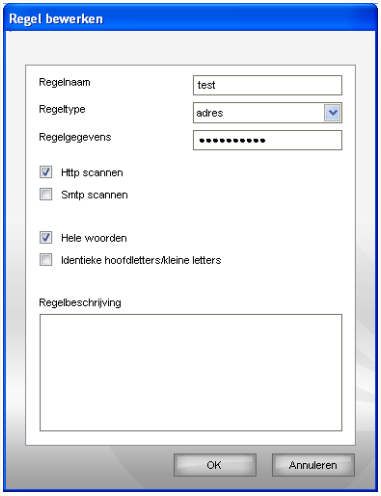
Klik op **OK** om de wijzigingen op te slaan.

10.2.3. Regels beheren

De regels worden weergegeven in de tabel.

Om een regel te verwijderen, selecteert u de regel en klikt u op de knop **Verwijderen**. Als u een regel tijdelijk wilt uitschakelen zonder deze te verwijderen, moet u het overeenkomende selectievakje uitschakelen.

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



Regel bewerken

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

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

10.3. Geavanceerde instellingen - 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 en heel wat andere gegevens 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 Register van Windows 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 kunt deze wijziging weigeren door op **Nee** te klikken of toestaan door op **Ja** te klikken.

Als u wilt dat BitDefender uw antwoord onthoudt, schakelt u de optie **Deze actie altijd toepassen voor dit programma** in. Hierdoor wordt een regel gemaakt en zal dezelfde actie telkens worden toegepast wanneer dit programma een registergegeven probeert te wijzigen zodat het moet worden uitgevoerd bij het opstarten van Windows.

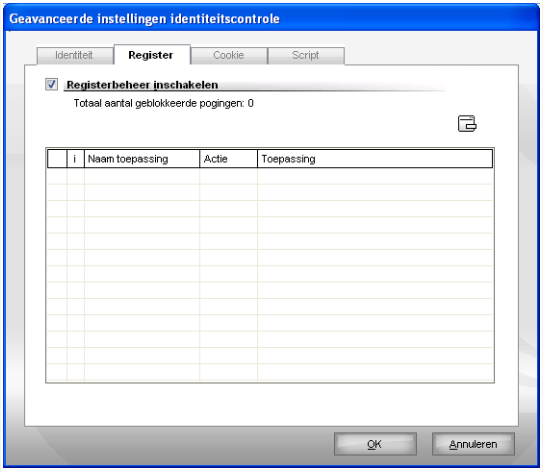
Opmerking

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.

U kunt elke regel die werd onthouden in het gedeelte **Register** openen om deze verder fijn af te stemmen. Om toegang te krijgen tot deze sectie, opent u het venster **Geavanceerde instellingen Privacybeheer** en klikt u op het tabblad **Register**.

Opmerking

Om het venster **Geavanceerde instellingen Privacybeheer** te openen, klikt u op **Privacybeheer>Status** in de instellingsconsole en klikt u op **Geavanceerde instellingen**.



Registerbeheer

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

Om een regel te verwijderen, selecteert u de regel en klikt u op de knop **Verwijderen**. Als u een regel tijdelijk wilt uitschakelen zonder deze te verwijderen, moet u het overeenkomende selectievakje uitschakelen.

Om de actie van een regel te wijzigen, dubbelklikt u op het actieveld en selecteert u de geschikte optie in het menu.

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

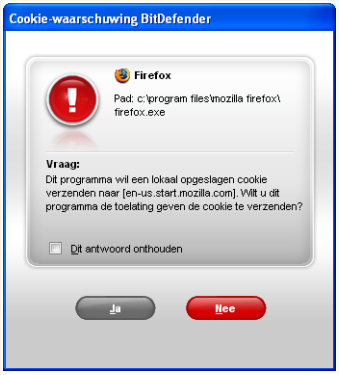
10.4. Geavanceerde instellingen - Cookiebeheer

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 het punt waarop 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 zal u helpen een keuze te maken van de websites die u wel of niet vertrouwt.

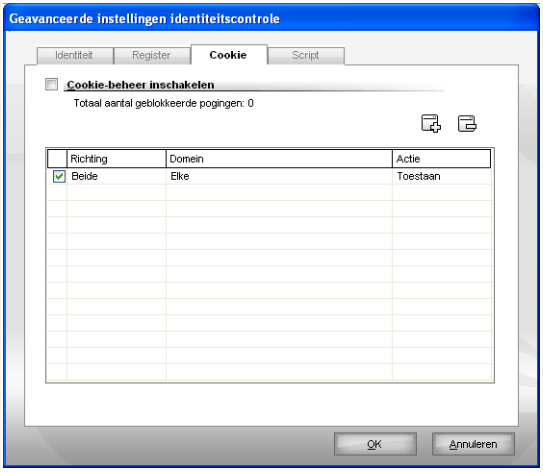
Opmerking

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.

U kunt elke regel die werd onthouden, openen in het onderdeel **Cookie** om deze fijner in te stellen. Om toegang te krijgen tot deze sectie, opent u het venster **Geavanceerde instellingen Privacybeheer** en klikt u op het tabblad **Cookie**.

Opmerking

Om het venster **Geavanceerde instellingen Privacybeheer** te openen, klikt u op **Privacybeheer>Status** in de instellingsconsole en klikt u op **Geavanceerde instellingen**.



Cookiebeheer

De regels die tot nog 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.

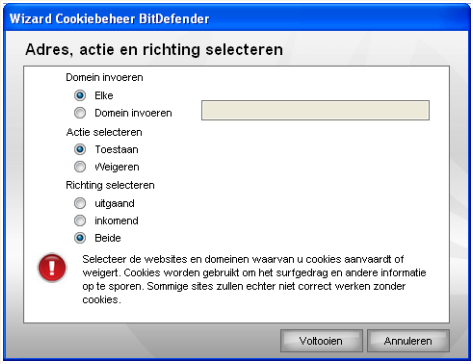
Om een regel te verwijderen, selecteert u de regel en klikt u op de knop **Verwijderen** Om een parameter van een regel te wijzigen, dubbelklikt u op zijn veld en brengt u de gewenste wijziging aan. Als u een regel tijdelijk wilt uitschakelen zonder deze te verwijderen, moet u het overeenkomende selectievakje uitschakelen.

De regels kunnen automatisch worden ingevoerd (via het waarschuwingsvenster) of handmatig (klik op de knop **Toevoegen** en kies de parameters voor de regel). De configuratiewizard wordt geopend.

10.4.1. Configuratiewizard

De configuratiewizard is een procedure die uit 1 stap bestaat.

Stap 1/1 - Adres, actie en richting selecteren



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.

Klik op **Voltooien**.

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

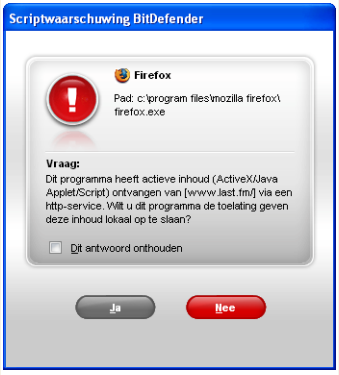
Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

10.5. Geavanceerde instellingen - 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.



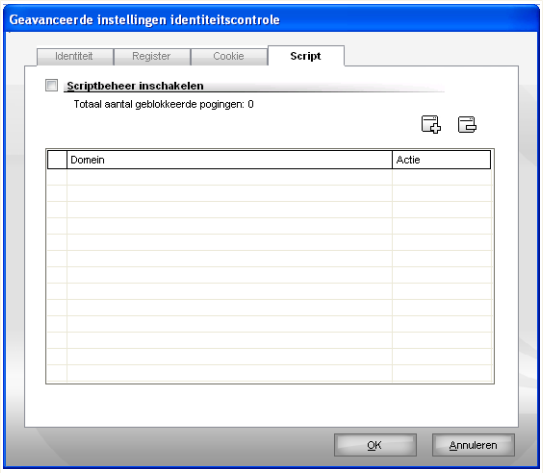
Script-waarschuwing

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.

U kunt elke regel die werd onthouden, openen in het onderdeel **Script** om deze fijner in te stellen. Om toegang te krijgen tot deze sectie, opent u het venster **Geavanceerde instellingen Privacybeheer** en klikt u op het tabblad **Script**.

Opmerking
Om het venster **Geavanceerde instellingen Privacybeheer** te openen, klikt u op **Privacybeheer>Status** in de instellingsconsole en klikt u op **Geavanceerde instellingen**.



Scriptbeheer

De regels die tot nog 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 de regel en klikt u op de knop **Verwijderen** Om een parameter van een regel te wijzigen, dubbelklikt u op zijn veld en brengt u de gewenste wijziging aan. Als u een regel tijdelijk wilt uitschakelen zonder deze te verwijderen, moet u het overeenkomende selectievakje uitschakelen.

De regels kunnen automatisch worden ingevoerd (via het waarschuwingsvenster) of handmatig (klik op de knop **Toevoegen** en kies de parameters voor de regel). De configuratiewizard wordt geopend.

10.5.1. Configuratiewizard

De configuratiewizard is een procedure die uit 1 stap bestaat.

Stap 1/1 - Adres en actie selecteren

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**.

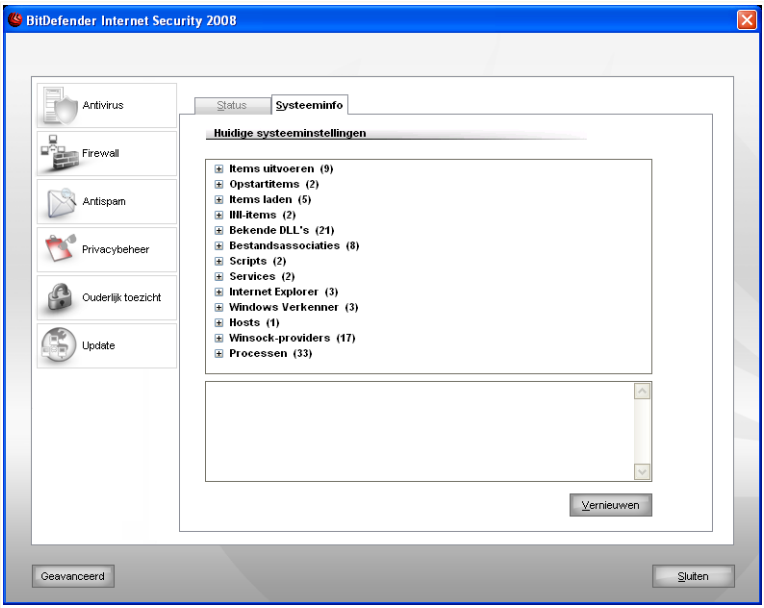
Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

10.6. Systeeminformatie

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, klikt u op **Privacybeheer>Systeeminfo** in de instellingsconsole. Het volgende venster wordt geopend:



Systeeminformatie

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:

- **Verwijderen** - verwijdert het geselecteerde item. U moet op **Ja** klikken om uw keuze te bevestigen.

> ***Opmerking***
> Als u tijdens de huidige sessie niet opnieuw wilt worden gevraagd uw keuze te bevestigen, moet u het selectievakje **Mij niet meer vragen tijdens deze sessie** inschakelen.

- **Ga naar** - opent een venster waar het geselecteerde item is geplaatst (bijvoorbeeld **Register**).
- **Vernieuwen** - opent het gedeelte **Systeeminfo** opnieuw.

Opmerking
Afhankelijk van het geselecteerde item, kan één of beide knoppen **Verwijderen** of **Ga naar** misschien niet verschijnen.

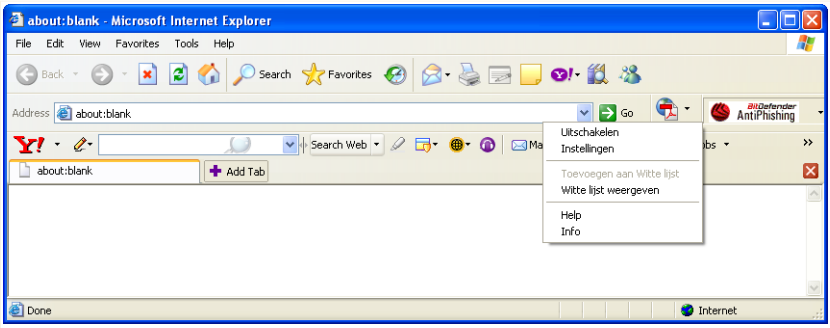
10.7. Antiphishing-werkbalk

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.

U kunt de antiphishing-beveiliging en de Witte lijst gemakkelijk en efficiënt beheren met de werkbalk van BitDefender Antiphishing die in Internet Explorer is geïntegreerd.

De antiphishing-werkbalk die wordt voorgesteld door het **BitDefender-pictogram**, bevindt zich bovenaan in Internet Explorer. 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.

11. Ouderlijk toezicht

Het Ouderlijk Toezicht kan de toegang blokkeren tot:

- ongeschikte webpagina's.
- het Internet, gedurende een bepaalde periode (bijvoorbeeld als het tijd is om huiswerk te maken).
- webpagina's en e-mail berichten die bepaalde sleutelwoorden bevatten.
- applicaties zoals spelletjes, chatten, programma's die bestanden uitwisselen en dergelijke.

Belangrijk
Deze module kan alleen worden geopend en geconfigureerd door gebruikers met beheerdersrechten (systeembeheerders). Als de instellingen door een wachtwoord zijn beveiligd, kunnen ze alleen worden gewijzigd als het wachtwoord wordt opgegeven. Een beheerder kan geen reeks regels opleggen aan een gebruiker voor wie eerder regels werden gedefinieerd door een andere beheerder.

Het gedeelte **Ouderlijk toezicht** in deze gebruiksaanwijzing bevat de volgende onderwerpen:

- Instellingen Ouderlijk Toezicht Beveiligen
- Status Ouderlijk toezicht
- Webbeheer
- Toepassingsbeheer
- Trefwoordfiltering
- Webtijdbeperking

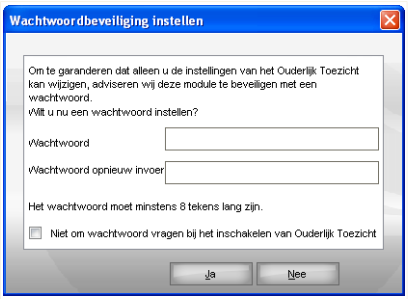
11.1. Instellingen Ouderlijk Toezicht Beveiligen

Als er meer personen met beheerdersrechten zijn die deze computer gebruiken, is het raadzaam dat u uw instellingen van Ouderlijk Toezicht beveiligt met een wachtwoord. Door het instellen van een wachtwoord, voorkomt u dat andere gebruikers met beheerdersrechten de instellingen van Ouderlijk Toezicht, die u voor een bepaalde gebruiker hebt geconfigureerd, kunnen wijzigen.

BitDefender vraagt standaard om een wachtwoord in te stellen bij het inschakelen van Ouderlijk Toezicht.

Stel de wachtwoordbeveiliging op de volgende manier in:

1. Typ het wachtwoord in het **Wachtwoord** veld.
2. Typ het wachtwoord nogmaals in het **Wachtwoord herhalen** veld om het te bevestigen.
3. Klik op **OK** om het wachtwoord op te slaan en het venster te sluiten.



Wachtwoordbeveiliging instellen

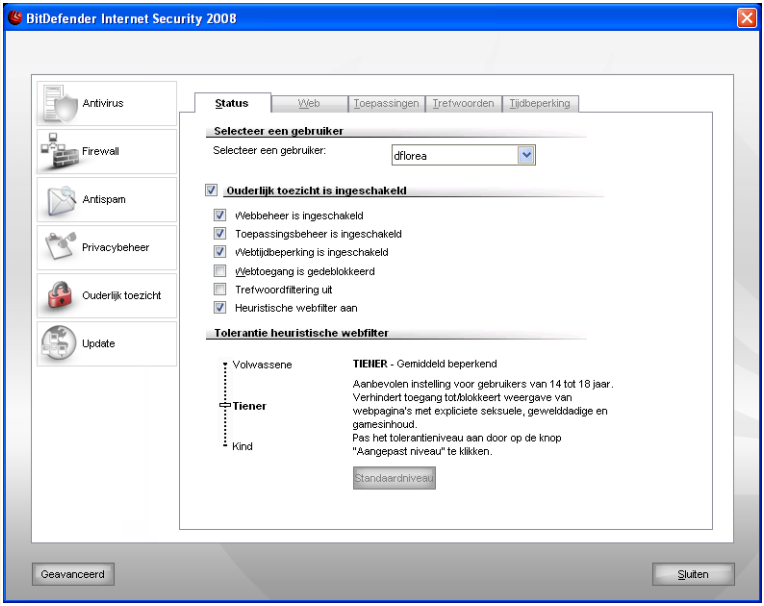
Zodra u het wachtwoord hebt ingesteld, zal erom gevraagd worden als u de instellingen van Ouderlijk Toezicht wilt veranderen. De andere systeembeheerders (als die er zijn) moeten dit wachtwoord ook invullen om de instellingen van Ouderlijk Toezicht te kunnen veranderen.

Opmerking
Dit wachtwoord beveiligt geen andere instellingen van BitDefender.

Als u geen wachtwoord wilt instellen en niet wilt dat dit venster opnieuw verschijnt, kruist u **Wachtwoord niet vragen bij inschakelen van Ouderlijk Toezicht** aan.

11.2. Status Ouderlijk toezicht

Om Ouderlijk toezicht voor een geselecteerde gebruiker te configureren, klikt u in de instellingsconsole op **Ouderlijk toezicht>Status**. Het volgende venster wordt geopend:



Status Ouderlijk toezicht

Belangrijk
Houd **Ouderlijk toezicht** ingeschakeld om uw kinderen te beschermen tegen ongepaste inhoud door uw aangepaste computertoegangsregels te gebruiken.

11.2.1. Beveiligingsbeheeropties selecteren

Om het beveiligingsniveau te configureren, moet u eerst de gebruiker selecteren waarop u deze instellingen wilt toepassen. Configureer vervolgens het beveiligingsniveau met de volgende beheeropties:

- **Webbeheer** - schakel **Webbeheer** in om de webnavigatie te filteren volgens de regels die u hebt ingesteld in het gedeelte Web.
- **Toepassingsbeheer** - schakel **Toepassingbeheer** in om de toegang tot toepassingen op uw computer te blokkeren volgens de regels die u hebt ingesteld in het gedeelte Toepassingen.
- **Webtijdbeperking** - schakel **Webtijdbeperking** om de webtoegang toe te staan volgens het tijdschema dat u hebt ingesteld in het gedeelte Tijdbeperking.

- **Webtoegang** - schakel deze optie in om de toegang tot alle websites te blokkeren (niet alleen de sites in het gedeelte Web).
- **Trefwoordfilter** - schakel **Trefwoordfilter** in om de web- en e-mailtoegang te filteren volgens de regels die u hebt ingesteld in het gedeelte Trefwoorden.
- **Heuristische webfilter** - schakel deze optie in om de webtoegang te filteren volgens de vooraf vastgestelde regels op basis van leeftijdcategorieën.

Opmerking

Om optimaal te genieten van de functies die u door Ouderlijk toezicht worden geboden, moet u de geselecteerde bedieningselementen configureren. Raadpleeg voor informatie over het configureren ervan, de volgende onderwerpen in dit hoofdstuk.

11.2.2. De heuristische webfilter configureren

De heuristische webfilter analyseert webpagina's en blokkeert de pagina's die overeenkomen met de patronen van potentieel ongeschikte inhoud.

Om webtoegang te filteren met een leeftijdgebonden filter, moet u een bepaald tolerantieniveau instellen. Versleep de schuiver over de schaal om het juiste tolerantieniveau voor de geselecteerde gebruiker in te stellen.

Er zijn 3 tolerantieniveaus:

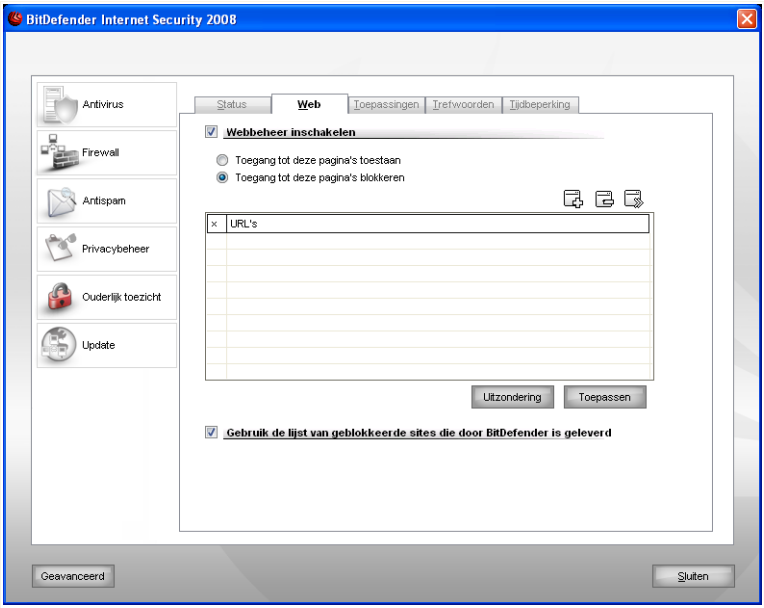
Tolerantieniveau	Beschrijving
Kind	Biedt beperkte webtoegang volgens de aanbevolen instellingen voor gebruikers die jonger zijn dan 14 jaar. Webpagina's met potentiële schadelijke inhoud voor kinderen (porno, seks, drugs, hacking, enz.) worden geblokkeerd.
Tiener	Biedt beperkte webtoegang volgens de aanbevolen instellingen voor gebruikers van 14 tot 18 jaar. Webpagina's met seksuele, pornografische of expliciete inhoud worden geblokkeerd.
Volwassene	Biedt onbeperkte toegang tot alle webpagina's, ongeacht hun inhoud.

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

11.3. Webbeheer

Met **Webbeheer** kunt u de toegang blokkeren tot websites met ongepaste inhoud. Een lijst van kandidaten voor het blokkeren van beide sites en onderdelen daarvan wordt geleverd en bijgewerkt door BitDefender als onderdeel van het regelmatige updateproces.

Om het webbeheer te configureren, klikt u in de instellingsconsole op **Ouderlijk toezicht>Web**. Het volgende venster wordt geopend:



Webbeheer

Om deze beveiliging in te schakelen, selecteert u het selectievakje naast **Webbeheer inschakelen**.

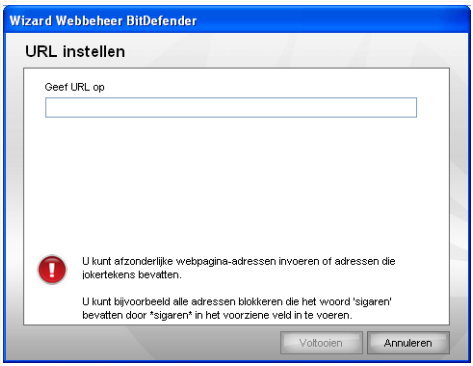
Selecteer **Toegang tot deze pagina's toestaan/Toegang tot deze pagina's blokkeren** om een lijst van toegelaten/geblokkeerde sites weer te geven. Klik op **Uitzonderingen...** om een venster te openen waarin u de aanvullende lijst kunt bekijken.

De regels moeten handmatig worden ingevoerd. Selecteer eerst **Toegang tot deze pagina's toestaan/Toegang tot deze pagina's blokkeren** om de toegang toe te staan/te weigeren tot de websites die u in de wizard zult opgeven. Klik vervolgens op de knop **Toevoegen…** om de configuratiewizard te starten.

11.3.1. Configuratiewizard

De configuratiewizard is een procedure die uit 1 stap bestaat.

Stap 1/1 – Websites opgeven



Websites opgeven

Voer de website in waarop de regel moet worden toegepast en klik op **Voltooien**.

Belangrijk
Syntaxis:

- `*.xxx.com` - de actie van de regel zal van toepassing zijn op alle websites die eindigen op `.xxx.com`;
- `*porn*` - de actie van de regel zal van toepassing zijn op alle websites die `porn` bevatten in het website-adres;
- `www.*.com` - de actie van de regel zal van toepassing zijn op alle websites met het domeinachtervoegsel `com`;
- `www.xxx.*` - de actie van de regel zal van toepassing zijn op alle websites die beginnen met `www.xxx.`, ongeacht het domeinachtervoegsel;

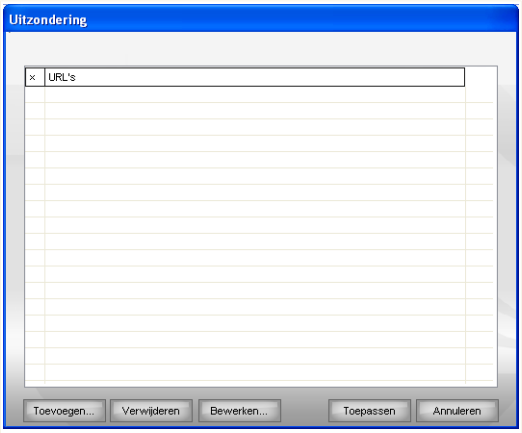
Klik op **Toepassen** om de wijzigingen op te slaan.

Om een regel te verwijderen, selecteert u de regel en klikt u op de knop **Verwijderen** Om een regel te wijzigen, selecteert u de regel en klikt u op de knop **Bewerken…** of dubbelklikt u op de regel. Als u een regel tijdelijk wilt uitschakelen zonder deze te verwijderen, moet u het overeenkomende selectievakje uitschakelen.

11.3.2. Uitzonderingen opgeven

In sommige gevallen zult u uitzonderingen op een bepaalde regel moeten opgeven. Als u bijvoorbeeld een regel opmaakt die sites blokkeert die het woord "killer" bevatten in het adres (syntaxis: `*killer*`). wordt ook een site geblokkeerd met de naam `killer-music` waar bezoekers muziek online kunnen beluisteren. Om een uitzondering in te stellen op de eerder gemaakte regel, opent u het venster **Uitzonderingen** en definieert u de uitzondering op de regel.

Klik op **Uitzonderingen…**. Het volgende venster wordt geopend:



Uitzonderingen opgeven

Klik op **Toevoegen…** om uitzonderingen op te geven. De configuratiewizard wordt weergegeven. Voltooi de wizard om de uitzondering in te stellen.

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

Om een regel te verwijderen, selecteert u de regel en klikt u op **Verwijderen**. Om een regel te wijzigen, selecteert u de regel en klikt u op **Bewerken...** of dubbelklikt u op

de regel. Als u een regel tijdelijk wilt uitschakelen zonder deze te verwijderen, moet u het overeenkomende selectievakje uitschakelen.

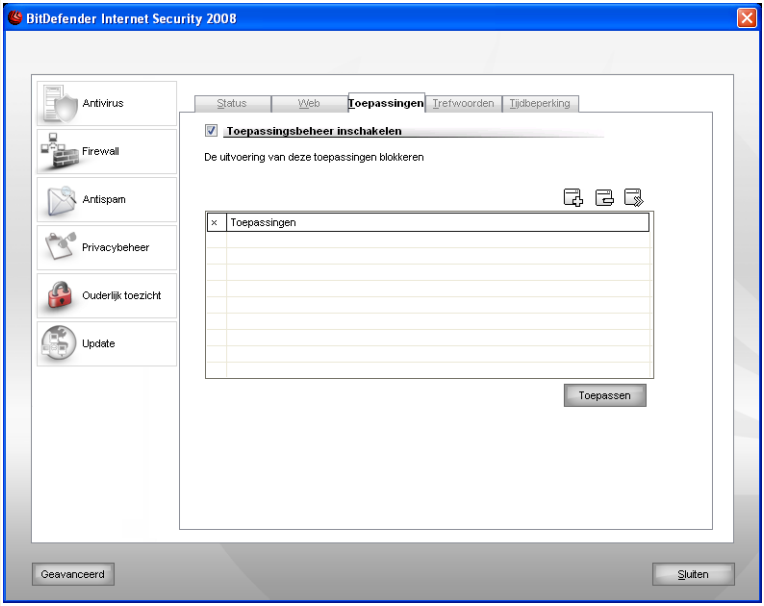
11.3.3. Zwarte lijst web BitDefender

Om u te helpen uw kinderen te beschermen, biedt BitDefender een zwarte lijst van websites met ongepaste of mogelijk gevaarlijke inhoud. Selecteer **Gebruik de lijst van geblokkeerde sites die door BitDefender is geleverd** om de sites die in deze lijst zijn weergegeven, te blokkeren.

11.4. Toepassingsbeheer

Het **Toepassingsbeheer** helpt u het uitvoeren van toepassingen te blokkeren. Games, media en messaging software, maar ook andere categorieën van software en malware kunnen op deze manier worden geblokkeerd. Toepassingen die op deze manier worden geblokkeerd, worden ook beschermd tegen wijzigingen en kunnen niet worden gekopieerd of verplaatst.

Om het toepassingsbeheer te configureren, klikt u in de instellingsconsole op **Ouderlijk toezicht>Toepassingen**. Het volgende venster wordt geopend:



Toepassingsbeheer

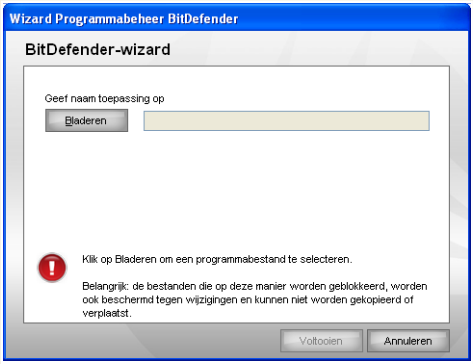
Om deze beveiliging in te schakelen, selecteert u het selectievakje naast **Toepassingsbeheer inschakelen**.

De regels moeten handmatig worden ingevoerd. Klik op de knop **Toevoegen…** om de configuratiewizard te starten.

11.4.1. Configuratiewizard

De configuratiewizard is een procedure die uit 1 stap bestaat.

Stap 1/1 - Te blokkeren toepassing selecteren



Te blokkeren toepassing selecteren

Klik op **Bladeren**, selecteer de toepassing die moet worden geblokkeerd en klik op **Voltooien**.

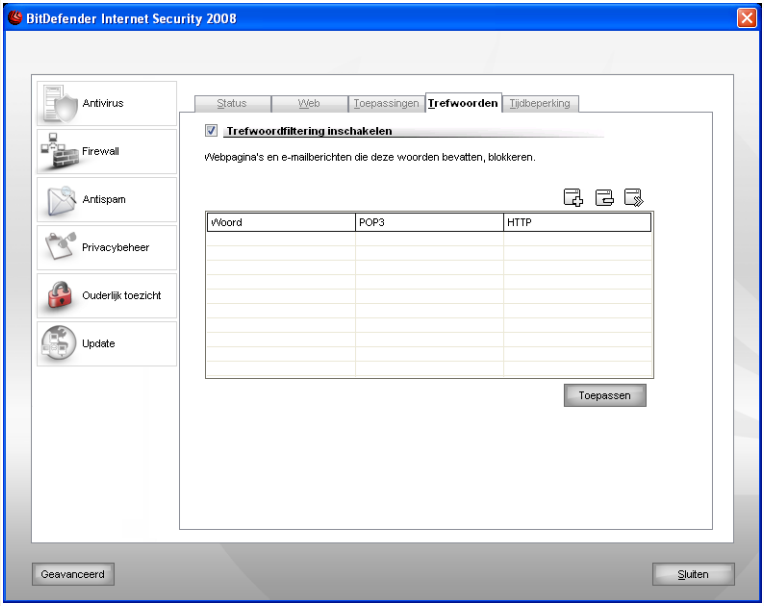
Klik op **Toepassen** om de wijzigingen op te slaan.

Om een regel te verwijderen, selecteert u de regel en klikt u op de knop **Verwijderen** Om een regel te wijzigen, selecteert u de regel en klikt u op de knop **Bewerken…** of dubbelklikt u op de regel. Als u een regel tijdelijk wilt uitschakelen zonder deze te verwijderen, moet u het overeenkomende selectievakje uitschakelen.

11.5. Trefwoordfilter

De **Trefwoordfilter** helpt u de toegang te blokkeren tot e-mailberichten of webpagina's die een specifiek woord bevatten. Op deze manier kunt u verhinderen dat gebruikers ongepaste woorden of uitdrukkingen kunnen zien.

Om de trefwoordfilter te configureren, klikt u in de instellingsconsole op **Ouderlijk toezicht>Trefwoorden**. Het volgende venster wordt geopend:



Trefwoordfilter

Om deze beveiliging in te schakelen, selecteert u het selectievakje naast **Trefwoordfilter**.

De regels moeten handmatig worden ingevoerd. Klik op de knop **Toevoegen…** om de configuratiewizard te starten.

11.5.1. Configuratiewizard

De configuratiewizard is een procedure die uit 1 stap bestaat.

Stap 1/1 - Trefwoord invoeren

Trefwoord invoeren

U moet de volgende parameters instellen:

- **Trefwoord** - typ het woord of de uitdrukking die u wilt blokkeren in het bewerkingsveld.
- **Protocol** - kies het protocol waarin BitDefender het opgegeven woord moet zoeken.

  De volgende opties zijn beschikbaar:

Optie	Beschrijving
POP3	E-mailberichten die het trefwoord bevatten, worden geblokkeerd.
HTTP	Webpagina's die het trefwoord bevatten, worden geblokkeerd.
Beide	E-mailberichten en webpagina's die het trefwoord bevatten, worden geblokkeerd.

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

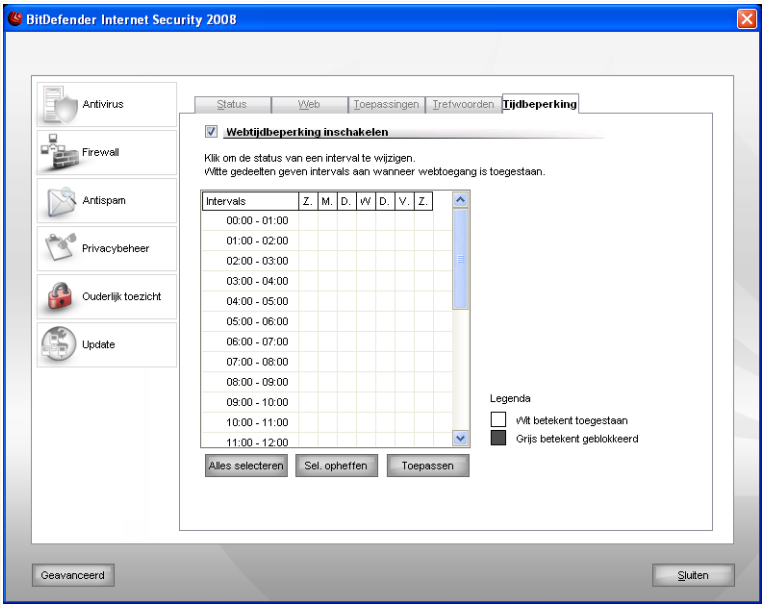
Om een regel te verwijderen, selecteert u de regel en klikt u op de knop **Verwijderen** Om een regel te wijzigen, selecteert u de regel en klikt u op de knop **Bewerken…** of dubbelklikt u op de regel. Als u een regel tijdelijk wilt uitschakelen zonder deze te verwijderen, moet u het overeenkomende selectievakje uitschakelen.

11.6. Webtijdbeperking

De **Webtijdbeperking** helpt u tijdens opgegeven tijdintervallen de webtoegang toe te staan of te blokkeren voor gebruikers of toepassingen.

Opmerking
BitDefender zal elk uur updates uitvoeren, ongeacht de instellingen van de **Webtijdbeperking**.

Om de webtijdbeperking te configureren, klikt u in de instellingsconsole op **Ouderlijk toezicht>Tijdbeperking**. Het volgende venster wordt geopend:



Webtijdbeperking

Om deze beveiliging in te schakelen, selecteert u het selectievakje naast **Webtijdbeperking inschakelen**.

Selecteer de tijdintervals voor het blokkeren van alle internetverbindingen. U kunt op individuele cellen klikken of klikken en slepen om langere perioden te dekken. U kunt

ook op **Alles selecteren** klikken om alle cellen te selecteren en alle webtoegang onvoorwaardelijk blokkeren. Als u op **Alle selecties opheffen** klikt, worden de internetverbindingen altijd toegelaten.

Belangrijk
De grijze vakken geven de tijdsintervallen weer wanneer alle internetverbindingen worden geblokkeerd.

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

12. 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 om het **uur**.

Als een update wordt gevonden, wordt u, afhankelijk van de opties die zijn ingesteld in het gedeelte Automatische update-instellingen, gevraagd de update te bevestigen of wordt de update automatisch uitgevoerd.

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:

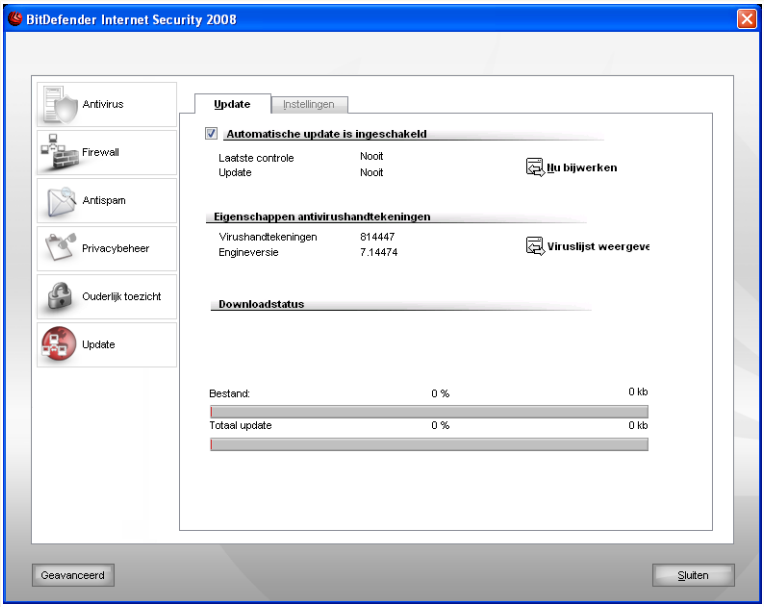
- **Updates voor antivirus-engines** - aangezien er steeds nieuwe virussen dreigen, moeten de bestanden met de virushandtekeningen voortdurend worden bijgewerkt om een permanente up-to-date beveiliging te garanderen. Dit type update is ook bekend als **Update virusdefinities**.
- **Updates voor antispam-engines** - er worden nieuwe regels toegevoegd aan de heuristische en URL-filters. Daarnaast worden nieuwe afbeeldingen toegevoegd aan de Afbeeldingsfilter. Dit zal de doeltreffendheid van uw Antispam-engine verbeteren. Dit type update is ook bekend als **Antispam-update**.
- **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**.

Het gedeelte **Update** in deze gebruiksaanwijzing bevat de volgende onderwerpen:

- Automatische update
- Update-instellingen

12.1. 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 instellingsconsole. Het volgende venster wordt geopend:



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.

U kunt de malware-handtekeningen van BitDefender ophalen door te klikken op **Viruslijst weergeven**. Er wordt een HTML-bestand gemaakt dat alle beschikbare handtekeningen bevat. Dit bestand wordt geopend in een webbrowser. U kunt in de database zoeken naar een specifieke malware-handtekening of op **Viruslijst BitDefender** klikken om naar de online handtekeningendatabase van BitDefender te gaan.

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.

12.1.1. Een update aanvragen

De automatische update kan ook op elk gewenst ogenblik worden uitgevoerd door te klikken op **Nu bijwerken**. Dit type update is ook bekend als de **Update op aanvraag van de gebruiker**.

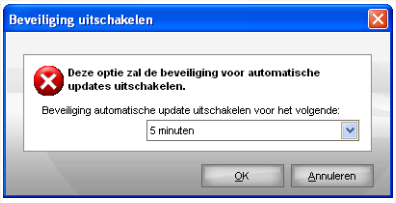
De module **Update** zal een verbinding maken met de updateserver van BitDefender en controleren of er een update beschikbaar is. Als een update wordt gevonden, wordt u, afhankelijk van de opties die zijn ingesteld in het gedeelte Handmatige update-instellingen, gevraagd de update te bevestigen of wordt de update automatisch uitgevoerd.

Belangrijk
Het kan noodzakelijk zijn de computer opnieuw op te starten wanneer de update is voltooid. We bevelen aan 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.

12.1.2. Automatisch update uitschakelen

Als u de automatische update wilt uitschakelen, verschijnt een waarschuwingsvenster.



Automatische update uitschakelen

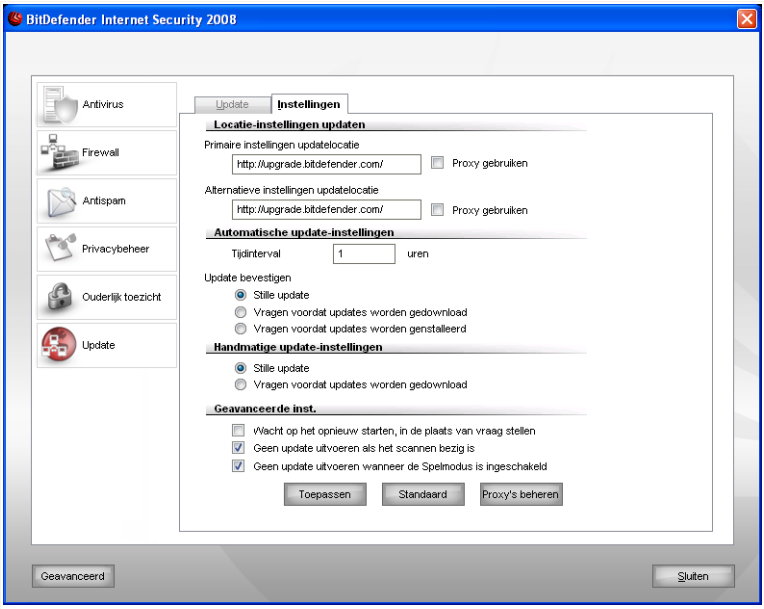
U moet uw keuze bevestigen door in het menu te selecteren hoelang u de automatische update wilt uitschakelen. U kunt de automatische update uitschakelen gedurende 5, 15 of 30 minuten, 1 uur, definitief of tot het systeem opnieuw wordt opgestart.

Waarschuwing
Dit is een kritiek beveiligingsprobleem. Wij raden u aan de automatische update zo kort mogelijk uit te schakelen. Als BitDefender niet regelmatig wordt bijgewerkt, zal het programma niet in staat zijn u te beschermen tegen de nieuwste bedreigingen.

12.2. Update-instellingen

De updates kunnen worden uitgevoerd vanaf het 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, klikt u in de instellingsconsole op **Update>Instellingen**. Het volgende venster wordt geopend:



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.

12.2.1. De 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-handtekeningen 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 raden u aan de lokale spiegel in te stellen als een primaire updatelocatie en de alternatieve updatelocatie ongewijzigd te laten als een back-upplan in het geval de lokale spiegel onbeschikbaar wordt.

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.

Opmerking
Meer informatie vindt u onder "*Proxy's beheren*" (p. 176)

12.2.2. Automatische update configureren

U kunt het automatisch uitvoeren van de update door BitDefender instellen met de opties in de categorie **Automatische update-instellingen**.

In het veld **Tijdinterval** kunt 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 implementeert automatisch de update.
- **Vragen voordat updates worden gedownload** - telkens wanneer een update beschikbaar is, wordt uw bevestiging gevraagd voordat de update wordt gedownload.

Opmerking
U wordt de vraag gesteld voordat de updates worden gedownload, zelfs als u het Beveiligingscentrum afsluit.

- **Vragen voordat updates worden geïnstalleerd** - telkens wanneer een update is gedownload, wordt uw bevestiging gevraagd voordat de update wordt geïnstalleerd.

Opmerking
U wordt de vraag gesteld voordat de updates worden geïnstalleerd, zelfs als u het Beveiligingscentrum afsluit.

12.2.3. 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 gebruikt:

- **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.

Opmerking
U wordt de vraag gesteld voordat de updates worden gedownload, zelfs als u het Beveiligingscentrum afsluit.

12.2.4. Geavanceerde instellingen configureren

Om te verhinderen dat het updateproces van BitDefender uw werk hindert, moet u de opties in de categorie **Geavanceerde instellingen** configureren:

- **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 wordt 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.

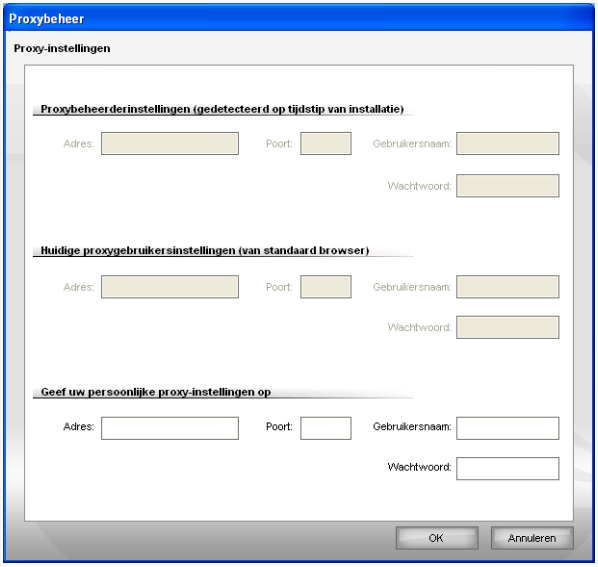
- **Geen update uitvoeren wanneer de spelmodus is ingeschakeld** - BitDefender zal geen update uitvoeren wanneer de spelmodus is ingeschakeld. Hierdoor kunt u de invloed van het product op de systeemprestaties beperken tijdens het spelen van spelletjes.

12.2.5. 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** wordt weergegeven.



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 gebruikers, 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 kunt 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.

BitDefender reddingsschijf

13. Overzicht

BitDefender Internet Security 2008 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 de virusinfecties. Dit gebeurt doorgaans wanneer u geen antivirusproduct gebruikt.

Telkens wanneer u de BitDefender reddingsschijf opstart, wordt de update van de virushandtekeningen 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 kunt u de BitDefender reddingsschijf gebruiken om uw waardevolle gegevens te herstellen wanneer u Windows niet kunt opstarten.

13.1. 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 waarvan 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 MUST.

Grafische resolutie
Standaard SVGA-compatibele grafische kaart.

13.2. 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-e-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.

14. 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, kunt u echter heel wat meer taken uitvoeren dan binnen het bereik van deze handleiding kunnen worden beschreven.

14.1. 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.

Splash-opstartscherm

Bij het opstarten wordt de update van de virushandtekeningen automatisch uitgevoerd. Dit kan even duren.

Wanneer het opstartproces is voltooid, ziet u het volgende bureaublad. U kunt nu starten met het gebruik van de BitDefender reddingsschijf.

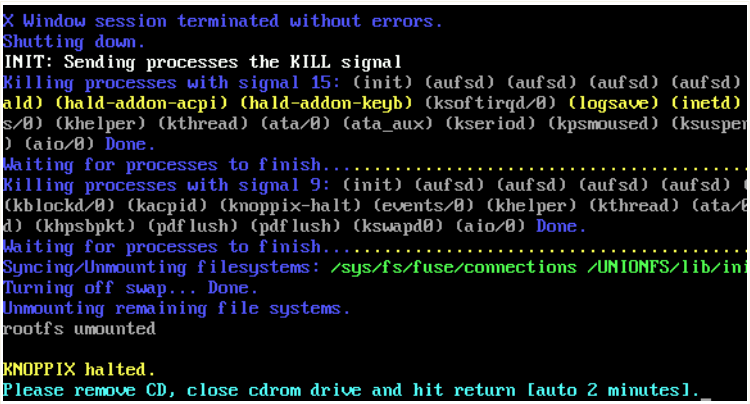
Het bureaublad

14.2. BitDefender reddingsschijf stoppen

Daarna kunt u de computer veilig afsluiten door **Afsluiten** te selecteren in het snelmenu van de BitDefender reddingsschijf (klikken met de rechtermuisknop 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, wordt een scherm weergegeven zoals in de volgende afbeelding. U kunt de cd verwijderen om opnieuw op te starten vanaf uw harde schijf. U kunt nu uw computer veilig uitschakelen of opnieuw opstarten.



Wacht op dit bericht wanneer u afsluit.

14.3. 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 op de knop **Start** te klikken.

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 kunt 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 kunt een algemene actie selecteren die moet worden genomen voor elke groep problemen of u kunt afzonderlijke acties voor elk probleem selecteren.
3. U kunt 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/
```

14.4. 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.

Doe het volgende BitDefender om te updaten over een proxy:

1. Rechtsklik op het Bureaublad. Het BitDefender reddingsschijf contextmenu verschijnt.
2. Selecteer **Werkstation (als root)**.
3. Typ het commando: **cd /ramdisk/BitDefender-scanner/etc**.
4. Typ het commando: **mcedit bdscan.conf** om dit bestand te wijzigen 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**.

14.5. Hoe kan ik mijn gegevens opslaan?

Laten we veronderstellen dat u uw Windows-pc door enkele onbekende problemen niet meer kunt 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. Stop de geheugenstick in het USB-station en start de computer opnieuw op.
2. Wacht tot de BitDefender reddingsschijf volledig is opgestart. Het volgende venster wordt geopend.

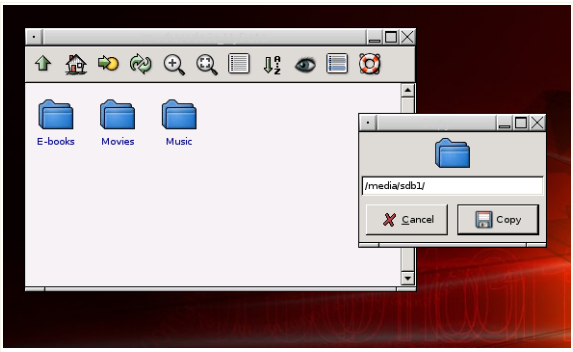
Bureaubladscherm

3. Dubbelklik op de partitie die de gegevens die u wilt opslaan, bevat (bijv. `[sda3]`).

> ***Opmerking***
> Wanneer u met de BitDefender reddingsschijf werkt, zult u te maken hebben 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.

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 wordt geopend.



Gegevens opslaan

6. Voer `/media/sdb1/` in het overeenkomende tekstvak in en klik op **Kopiëren**.

Hulp vragen

15. Ondersteuning

Als gewaardeerd provider streeft BitDefender ernaar zijn klanten een ongeëvenaard niveau van snelle en nauwkeurige ondersteuning te bieden. Het Ondersteuningscentrum (dat u kunt bereiken op de onderstaande adressen) houdt voortdurend de laatste bedreigingen bij. Hier worden al uw vragen zo snel mogelijk beantwoord.

Bij BitDefender is het onze absolute prioriteit wij 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 om goede communicatie en een inzet voor uitmuntendheid in klantenondersteuning.

U kunt op elk ogenblik hulp vragen op support@bitdefender.com. Voor een snel antwoord raden wij u aan zoveel mogelijk details over BitDefender en uw systeem te vermelden in uw e-mail en het probleem waarmee u te kampen hebt zo nauwkeurig mogelijk te omschrijven.

15.1. 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, "spiekbriefjes" 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.

15.2. Hulp vragen

15.2.1. Ga naar Web-selfservice

Hebt u vragen? Onze beveiligingsexperts staan 24/7 gratis tot uw dienst via telefoon, e-mail of chat.

Volg de onderstaande koppelingen:

Engels

http://www.bitdefender.com/site/KnowledgeBase/browseProducts/2195/

Duits

http://www.bitdefender.com/de/KnowledgeBase/browseProducts/2195/

Frans

http://www.bitdefender.com/fr/KnowledgeBase/browseProducts/2195/

Roemeens

http://www.bitdefender.com/ro/KnowledgeBase/browseProducts/2195/

Spaans

http://www.bitdefender.com/es/KnowledgeBase/browseProducts/2195/

15.2.2. Een ondersteuningsticket openen

Als u een ondersteuningsticket wilt openen en hulp via e-mail wilt ontvangen, volgt u een van deze koppelingen:

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/

15.3. 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 eventuele vragen hebt.

15.3.1. Webadressen

Verkoopsafdeling: sales@bitdefender.com
Technische ondersteuning support@bitdefender.com
Documentatie: documentation@bitdefender.com
Partnerprogramma: partners@bitdefender.com
Marketing: marketing@bitdefender.com
Perscontact: pr@bitdefender.com
Carrièremogelijkheden: jobs@bitdefender.com
Virusverzendingen: virus_submission@bitdefender.com
Spamverzendingen: spam_submission@bitdefender.com
Misbruikmeldingen: abuse@bitdefender.com
Website product: http://www.bitdefender.com
FTP-archieven product: ftp://ftp.bitdefender.com/pub
Lokale verdelers: http://www.bitdefender.com/partner_list
BitDefender Knowledge Base: http://kb.bitdefender.com

15.3.2. Bijkantoren

De BitDefender-kantoren zijn altijd paraat om te reageren op aanvragen met betrekking tot hun bedrijfsgebied, zowel op commercieel als algemeen vlak. Hun respectievelijke adressen en contactpersonen worden hieronder weergegeven:

Technische ondersteuning: support@abcsoft.be
Verkoop: sales@editions-profil.com
Telefoon: +40-21-233.07.80
Fax: +40-21-233.07.63
http://nl.bitdefender.com
http://www.bitdefender.com

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 bekend voor een compleet tekort aan beveiligingscontroles; experts op het vlak van computerbeveiliging 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 verkopers.

Opstartsector

Een sector aan het begin van elke schijf die de architectuur van de schijf identificeert (sectorgrootte, clustergrootte, enz.) Bij opstartdiskettes 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 vanaf dat ogenblik uw systeem opstart, zal het virus telkens in het geheugen geactiveerd 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 voorstellen 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 op 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 vaak een bijzonder nauwkeurige omschrijving.

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.

False positive

Doet zich voor wanneer een scanner een bestand ten onrechte beschouwt als geïnfecteerd.

Bestandsextensie

Het gedeelte van een bestandsnaam na het eindpunt, waarmee het gegevenstype dat in het bestand is opgeslagen wordt aangeduid.

Heel wat besturingssystemen, zoals Unix, VMS en MS-DOS, maken gebruik van bestandsextensies. Ze gebruiken doorgaans één tot drie letters (sommige betreurenswaardige 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, zou u de naam van het applet opgeven 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 bijvoorbeeld op de client worden uitgevoerd, kunnen ze 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 kunt u een macro in een document insluiten, en die macro telkens laten uitvoeren wanneer het document wordt geopend.

E-mailclient

Een e-mailclient is een toepassing waarmee u e-mail kunt 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 virussignatures. 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 zou echter de spatietekens vervangen door een speciaal spatiereeks-teken, gevolgd door het aantal spaties dat wordt vervangen. In dit geval zouden de tien spaties slechts twee bytes nodig hebben. 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 archiveringssysteem vanaf het begin.

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 waar persoonlijke gegevens kunnen worden bijgewerkt, zoals wachtwoorden en creditcard-, sofi- 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 hij infecteert. Aangezien ze geen consequent binair patroon hebben, zijn dergelijke virussen moeilijk te identificeren.

Poort

Een interface op een computer waarop u een apparaat kunt aansluiten. PC's hebben verschillende types poorten. Intern zijn er verschillende poorten voorzien 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.