bitdefender

INTERNET SECURITY v10

Gebruiksaanwijzing

Antivirus

Firewall

Antispam

Antispyware

Ouderlijk toezicht

bitdefender
secure your every bit

BitDefender Internet Security v10

Gebruiksaanwijzing

BitDefender

Uitgegeven 2007.01.26
Version 10.2

Wettelijke verklaring


bitdefender
secure your every bit

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 SOFTWIN voor het gebruik van het hierboven geidentificeerde softwareproduct van SOFTWIN. 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. SOFTWIN 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 geinstalleerd 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.

UPGRADES. Als BitDefender wordt gelabeld als een upgrade, moet u over de geschikte licentie beschikken om een product te gebruiken dat door SOFTWIN 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 SOFTWIN 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 geintegreerd), de begeleidende gedrukte materialen en elke kopie van BitDefender zijn eigendom van SOFTWIN. 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. SOFTWIN 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 SOFTWIN, volgens eigen voorkeur, de defecte media vervangt na ontvangst van de beschadigde media, of het bedrag, dat u voor BitDefender hebt betaald, terugbetaalt. SOFTWIN biedt geen garantie dat BitDefender ongestoord of

vrij van fouten zal werken, of dat de fouten zullen worden gecorrigeerd. SOFTWIN garandeert niet dat BitDefender zal voldoen aan uw behoeften.

TENZIJ UITDRUKKELIJK UITEENGEZET IN DEZE OVEREENKOMST, WIJST SOFTWIN 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 SOFTWIN ZIJN GELEVERD. SOFTWIN 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. SOFTWIN 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 SOFTWIN 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 SOFTWIN 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 SOFTWIN. 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 SOFTWIN 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.

SOFTWIN 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 beinvloeden 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 SOFTWIN is uitgegeven, de voorrang krijgen.

Neem contact op met SOFTWIN 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 v10** 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 v10**, 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 v10** 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. xv)	Dit is een interne koppeling naar een locatie in het document.
`filename`	Bestandsnamen en mappen worden afgedrukt met een `enkelspatielettertype`.
option	All the product options are printed using **strong** characters.

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

1.2. Waarschuwingen

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 7 delen met de volgende hoofdonderwerpen: Over BitDefender, Productinstallatie, Beschrijving en functies, Beheerconsole, Beste praktische toepassingen, BitDefender reddingsschijf en Hulp vragen. Bovendien vindt u ook een woordenlijst die enkele technische termen toelicht.

Over BitDefender. Een korte introductie van BitDefender. Hier wordt uitgelegd wie of wat BitDefender en SOFTWIN zijn.

Productinstallatie. Stapsgewijze instructies voor het installeren van BitDefender op een werkstation. Dit is een uitgebreide les over het installeren van **BitDefender Internet Security v10**. 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.

Beschrijving en functies. BitDefender Internet Security v10, de functies en de productmodules worden u voorgesteld.

Beheersconsole. Beschrijving van het basisbeheer en –onderhoud van BitDefender. In de hoofdstukken vindt u een gedetailleerde beschrijving van alle opties van **BitDefender Internet Security v10** en wordt uitgelegd hoe u het product kunt registreren, uw computer kunt scannen en de updates kunt uitvoeren. U leert hoe u alle BitDefender-modules kunt configureren en gebruiken.

Beste praktische toepassingen. Volg deze instructies om optimaal gebruik te maken van de mogelijkheden van BitDefender.

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.

Over BitDefender

1. Wie is BitDefender?

BitDefender is a leading global provider of security solutions that satisfy the protection requirements of today's computing environment. The company offers one of the industry's fastest and most effective lines of security software, setting new standards for threat prevention, timely detection and mitigation. BitDefender delivers products and services to over 41 million home and corporate users in more than 180 countries. BitDefender has offices in the **United States**, the **United Kingdom**, **Germany**, **Spain** and **Romania**.

- Biedt antivirus, firewall, antispyware, antispam en ouderlijk toezicht voor zakelijke en thuisgebruikers;
- Het gamma producten van BitDefender is bedoeld om te worden geimplementeerd in complexe IT-structuren (werkstations, bestandsservers, e-mailservers en gateways), op Windows-, Linux- en FreeBSD-platforms;
- Wereldwijde distributie, producten beschikbaar in 18 talen;
- Gebruiksvriendelijk, met een installatiewizard die u begeleidt doorheen de installatieprocedure en slechts enkele vragen stelt;
- Internationaal gecertificeerde producten: Virus Bulletin, ICSA Labs, Checkmark, IST Prize, enz;
- 24/24 uur klantendienst: het team van de klantendienst staat 24 uur per dag en 7 dagen per week tot uw beschikking;
- Bliksemsnelle responstijd op nieuwe computeraanvallen;
- Beste detectiesnelheid;
- Elk uur internetupdates van virushandtekeningen - automatische of geplande acties bieden bescherming tegen de nieuwste virussen.

1.1. Waarom BitDefender?

Bewezen. De antivirusproducent met het hoogste reactievermogen. Het snelle reactievermogen van BitDefender in het geval van een computervirusepidemie werd nog maar eens bewezen tijdens de laatste uitbraken van CodeRed, Nimda en Sircam, evenals Badtrans.B of andere gevaarlijke, zich snel verspreidende kwaadaardige codes. BitDefender was de eerste die een remedie bood tegen deze codes en deze gratis beschikbaar maakte op het internet voor alle getroffen gebruikers. Met de voortdurende uitbreiding van het Klez-virus in verschillende versies is een onmiddellijke

virusbescherming nu nog maar eens een kritische behoefte geworden voor elk computersysteem.

Innovatief. Bekroond voor innovatie door de Europese Commissie en EuroCase. BitDefender werd uitgeroepen tot de winnaar van de Europese IST-prijs die door de Europese Commissie en vertegenwoordigers van 18 academies in Europa wordt uitgereikt. De Europese IST-prijs is al aan zijn achtste jaargang toe en is een bekroning voor baanbrekende producten die het beste van de Europese innovatie in de IT-sector vertegenwoordigen.

Uitgebreid. Dekt elk afzonderlijk punt in uw netwerk en biedt een complete beveiliging. De beveiligingsoplossingen van BitDefender voor de bedrijfsomgeving voldoen aan de beveiligingsvereisten van de hedendaagse zakelijke omgeving en maken het mogelijk het beheer te voeren van alle complexe bedreigingen die een netwerk in gevaar brengen, van kleine LAN's tot grote WAN's met meerdere servers en platforms.

Uw ultieme bescherming. De laatste grens voor elke mogelijke bedreiging van uw computersysteem. Omdat virusdetectie op basis van codeanalyse niet altijd goede resultaten heeft opgeleverd, heeft BitDefender bescherming op basis van gedrag geimplementeerd, zodat ook beveiliging tegen nieuwe malware wordt geboden.

These are **the costs** that organizations want to avoid and what the security products are designed to prevent:

- Wormaanvallen
- Communicatieverlies door geinfecteerde e-mails
- Uitval van e-mail
- Opruimen en herstellen van systemen
- Verloren productiviteit die door eindgebruikers worden ervaren omdat de systemen niet beschikbaar zijn.
- Hackers en onbevoegde toegang die schade veroorzaken

Some simultaneously **developments and benefits** can be accomplished by using the BitDefender security suite:

- Verhoogde netwerkbeschikbaarheid door de verspreiding te stoppen van aanvallen door kwaadaardige codes (bijv. Nimda, Trojaanse paarden, DDoS).
- Bescherming van externe gebruikers tegen aanvallen.
- Lagere administratieve kosten en snelle inzet met de BitDefender Enterprise-beheercapaciteiten.
- Stop de verspreiding van malware via e-mail door gebruik te maken van een e-mailbeveiliging van BitDefender bij de gateway van de onderneming. U kunt

onbevoegde, kwetsbare en dure toepassingsverbindingen tijdelijk of permanent blokkeren.

Meer informatie over BitDefender kunt u vinden op de site: http://www.bitdefender.com.

1.2. Over SOFTWIN

SOFTWIN, een bedrijf dat in 1990 werd opgericht en in 2002 werd bekroond met de IST-prijs, wordt nu beschouwd als de technologische leider van de Oost-Europese softwaresector met een jaarlijks groeipercentage van meer dan 50% gedurende de laatste 5 jaar en waarvan 70% van de jaarlijkse omzet uit de export komt.

Met een team van meer dan 800 geschoolde vakmensen en meer dan 10.000 projecten die tot nog toe werden beheerd, richt SOFTWIN zich op het leveren van complexe softwareoplossingen en diensten die snelgroeiende bedrijven de mogelijkheid bieden kritische zakelijke uitdagingen op te lossen en voordeel te halen uit nieuwe zakelijke kansen. Het SOFTWIN-ontwikkelingsproces heeft het ISO9001-certificaat.

As it is active on the most advanced IT markets of the US and European Union, SOFTWIN develops on 4 interlinked **business lines**:

- eContent Solutions
- BitDefender
- Business Information Solutions
- Customer Relationship Management

Productinstallatie

2. BitDefender Internet Security v10 installeren

Het hoofdstuk **BitDefender Internet Security v10 installeren** van deze handleiding bevat de volgende onderwerpen:

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

2.1. 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 geinstalleerd en aan de overeenkomende systeemvereisten wordt voldaan:

Microsoft Windows 2000 / XP 32-bits

- Pentium II 350 MHz processor of hoger
- Minimum 128 MB RAM-geheugen (256 MB aanbevolen)
- Minimum 60 MB beschikbare harde schijfruimte
- Internet Explorer 5.5 of hoger

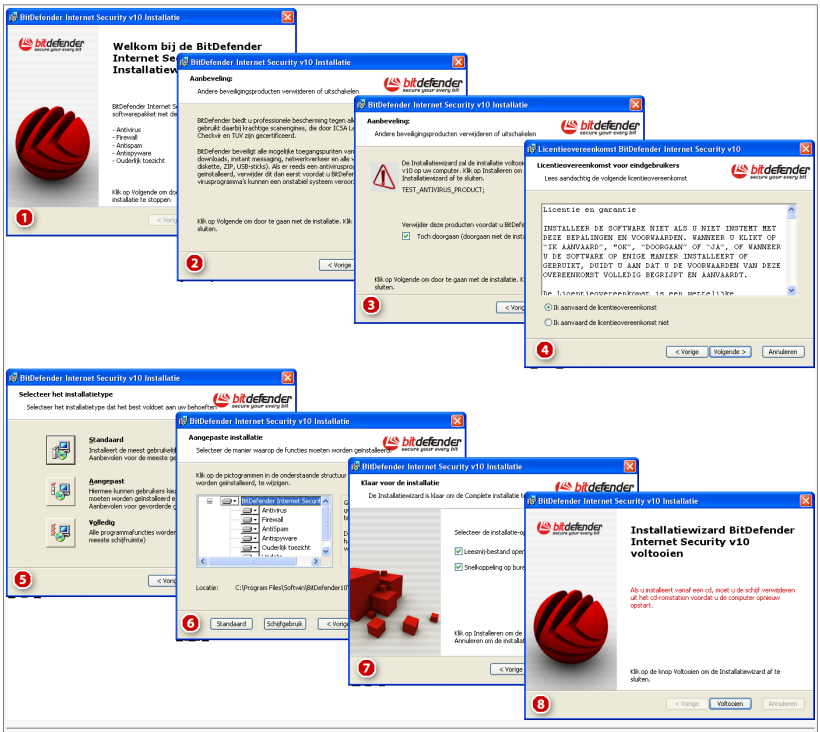
Microsoft Windows Vista 32-bits

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

BitDefender Internet Security v10 kan voor evaluatie worden gedownload van http://www.bitdefender.com, de bedrijfswebsite van SOFTWIN die aan gegevensbeveiliging is gewijd.

2.2. Installatiestappen

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



Installatiestappen

1. Klik op **Volgende** om door te gaan of klik op **Annuleren** als u de installatie wilt afbreken.
2. Klik op **Volgende** om door te gaan of klik op **Vorige** om terug te keren naar de eerste stap.
3. BitDefender Internet Security v10 waarschuwt u als er andere antivirusproducten op uw computer zijn geïnstalleerd.

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.

Klik op **Vorige** om terug te keren naar de vorige stap of op **Annuleren** om de installatie af te sluiten. Als u wilt doorgaan, klikt u op **Volgende**.

Opmerking

Als BitDefender Internet Security v10 geen andere antivirusproducten op uw computer detecteert, wordt deze stap overgeslagen.

4. 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.
5. U kunt zelf bepalen welk installatietype u wilt uitvoeren: standaard, aangepast of volledig.

   Typical
   Het programma wordt geinstalleerd met de meest gebruikelijke opties. Dit is de aanbevolen optie voor de meeste gebruikers.

   Custom
   U kunt zelf de componenten kiezen die u wilt installeren. Alleen aanbevolen voor geavanceerde gebruikers.

   Complete
   Voor een volledige installatie van het product. Alle modules van BitDefender worden geinstalleerd.

   Als u **Standaard** of **Volledig** selecteert, wordt stap 6 overgeslagen.
6. Als u **Aangepast** hebt geselecteerd, wordt een nieuw venster geopend met een lijst van alle componenten van BitDefender. Op die manier kunt u de componenten selecteren die u wilt installeren.

   Als u op een van de componentnamen klikt, wordt een korte beschrijving (inclusief de minimale vereiste schijfruimte op de harde schijf) weergegeven aan de rechterzijde. Als u klikt op een willekeurig componentpictogram, verschijnt een venster waarin u kunt bepalen of u de geselecteerde module al dan niet wilt installeren.

   U kunt de map selecteren waarin u het product wilt installeren. De standaardmap is `C:\Program Files\Softwin\BitDefender 10`.

   Als u een andere map wilt selecteren, klikt u op **Bladeren** en selecteert u in het venster dat wordt geopend, de map waarin u BitDefender Internet Security v10 wilt installeren. Klik op **Volgende**.
7. U hebt de keuze uit twee opties die standaard zijn geselecteerd:

- **Leesmij-bestand openen** - hiermee opent u het leesmij-bestand aan het einde van de installatie.
- **Een snelkoppeling op het bureaublad plaatsen** - hiermee plaatst u een snelkoppeling naar BitDefender Internet Security v10 op het bureaublad aan het einde van de installatie.

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 v10**, 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.

8. Klik op **Voltooien** om de installatie van het product te voltooien. Als u de standaardinstellingen voor het installatiepad hebt aanvaard, wordt een nieuwe map gemaakt met de naam `Softwin` onder `Program Files`. Deze map zal de submap `BitDefender 10` bevatten.

Opmerking

Het is mogelijk dat u wordt gevraagd uw systeem opnieuw op te starten zodat de configuratiewizard het installatieproces kan voltooien.

2.3. Initiële configuratiewizard

Tijdens het installatieproces verschijnt een wizard. De wizard helpt u bij het registreren van **BitDefender Internet Security v10**, 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 v10 is geinstalleerd.

2.3.1. Stap 1/8 - Initiële configuratiewizard BitDefender

Welkomstvenster

Klik op **Volgende**.

2.3.2. Stap 2/8 - BitDefender Internet Security v10 registreren

Registratie

Selecteer **Het product registreren** om **BitDefender Internet Security v10** 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**.

2.3.3. Stap 3/8 - Een BitDefender-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.

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 opnieuw invoeren**. 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.

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.

Belangrijk

Activeer uw account voordat u doorgaat naar de volgende stap.

Klik op **Deze stap overslaan** als u geen BitDefender-account wilt maken. Hiermee slaat u ook de volgende stap van de wizard over.

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

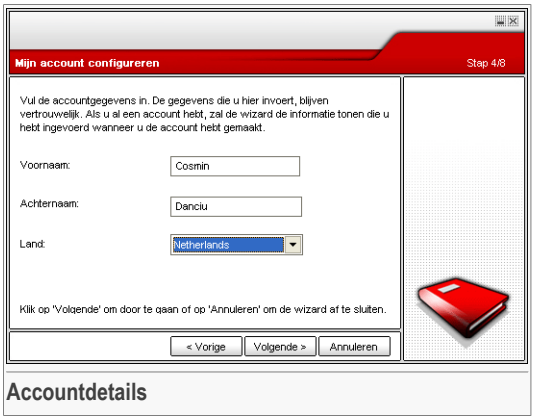
Ik heb al een BitDefender-account

Als u al een actieve account hebt, geef dan het e-mailadres en het wachtwoord van uw account op. Als u een onjuist wachtwoord opgeeft, wordt u gevraagd dit opnieuw in te voeren wanneer u op **Volgende** klikt. Klik op **OK** om het wachtwoord opnieuw in te voeren of op **Annuleren** om de wizard af te sluiten.

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.

2.3.4. Stap 4/8 - Accountdetails invoeren



Accountdetails

Opmerking

Als u **Deze stap overslaan** hebt geselecteerd in de derde stap, wordt deze stap niet weergegeven.

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

Als u al een account hebt, toont de wizard de informatie die u eerder hebt opgegeven, als die er is. Hier kunt u deze informatie desgewenst wijzigen.

Belangrijk

De gegevens die u hier opgeeft blijven vertrouwelijk.

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

2.3.5. Stap 5/8 - Leren over RTVR

RTVR-informatie

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

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

Taakselectie

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

De volgende opties zijn beschikbaar:

- **De BitDefender Internet Security v10-engines updaten (kan opnieuw opstarten vereisen)** - bij de volgende stap wordt een update van de BitDefender Internet Security v10-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 Internet Security v10 kan controleren of uw bestanden in de mappen `Windows` en `Program Files` niet zijn geinfecteerd.
- **Elke dag om 2 uur een volledige systeemscan uitvoeren** - voert elke dag om 2 uur een volledige systeemscan uit.

Belangrijk

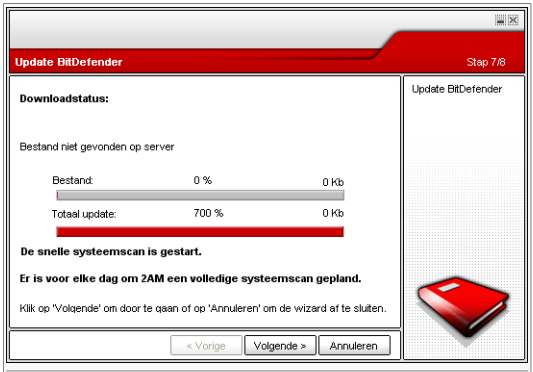
Wij raden u aan deze opties in te schakelen voordat u naar de volgende stap gaat, zodat de beveiliging van uw systeem gegarandeerd is.

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

U kunt eventuele wijzigingen aanbrengen door terug te keren naar de vorige stappen (klik op **Vorige**). Dit proces is niet omkeerbaar. Als u ervoor kiest om door te gaan, zult u niet kunnen terugkeren naar de vorige stappen.

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

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

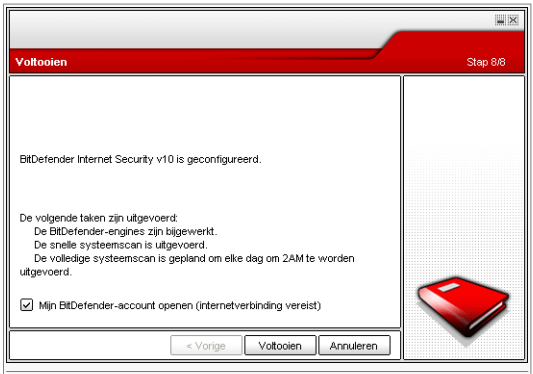


Taakstatus

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

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

2.3.8. Stap 8/8 – Overzicht weergeven



Voltooien

Dit is de laatste stap van de configuratiewizard.

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

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

2.4. Upgrade

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

- **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. 9).

Belangrijk

Als u een upgrade uitvoert van 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.

2.5. BitDefender verwijderen, repareren of wijzigen

Als u **BitDefender Internet Security v10** wilt wijzigen, repareren of verwijderen, volgt u het pad vanaf het menu Start van Windows: **Start → Programma's → BitDefender 10 → Wijzigen, 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:

- **Wijzigen** - om nieuwe programmacomponenten te selecteren die u wilt toevoegen of momenteel geinstalleerde componenten te selecteren die u wilt verwijderen.
- **Repareren** - om alle programmacomponenten die bij de vorige installatie werden geinstalleerd, opnieuw te installeren.

Belangrijk

Voordat u het product repareert, raden wij u aan 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.

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

Selecteer een van de bovenstaande opties om door te gaan met de installatie. Wij raden u aan de optie **Verwijderen** te selecteren zodat u zeker bent dat het opnieuw installeren probleemloos verloopt. Wij raden u aan de map `Softwin` te verwijderen uit `Program Files` nadat het verwijderingsproces is voltooid.

Beschrijving en functies

3. BitDefender Internet Security v10

Complete bescherming tegen internetbedreigingen.

BitDefender Internet Security v10 dekt alle behoeften van een met het internet verbonden familie op het vlak van beveiliging. Het programma biedt een uitgebreide bescherming tegen virussen, spyware, spam, scams, phishing-pogingen, indringers en ongewenste webinhoud.

BitDefender v10 is ontwikkeld om de gebruikers het hostsysteem zo weinig mogelijk te belasten, terwijl toch een optimale beveiliging wordt geboden tegen de huidige internetbedreigingen.

3.1. Antivirus

Het doel van de antivirusmodule bestaat eruit alle virussen in het wild te detecteren en te verwijderen. BitDefender Antivirus gebruikt krachtige scanengines, die werden gecertificeerd door ICSA Labs, Virus Bulletin, Checkmark, CheckVir en TÜV.

Proactieve detectie. B-HAVE (Behavioral Heuristic Analyzer in Virtual Environment) emuleert een virtuele computer in een computer, waarbij gedeelten van de software worden uitgevoerd om te controleren op potentiële gedragingen van kwaadaardige software. De eigen technologie van BitDefender vertegenwoordigt een nieuwe beveiligingslaag die het besturingssysteem beschermt tegen onbekende virussen door kwaadaardige codes te detecteren waarvoor nog geen handtekeningen werden uitgegeven.

Permanente antivirusbeveiliging. De nieuwe en verbeterde scanengines van BitDefender zullen bestanden bij de toegang scannen en desinfecteren, zodat het gegevensverlies tot een minimum wordt beperkt. Geinfecteerde documenten kunnen nu worden hersteld, in plaats van verwijderd.

De rootkit detecteren en verwijderen. Een nieuwe BitDefender-module zoekt rootkits (kwaadaardige programma's die zijn ontwikkeld om "slachtoffer"-computers te beheren terwijl ze verborgen blijven) en verwijdert ze wanneer ze worden gedetecteerd.

Webscannen. Het webverkeer wordt nu in real time gefilterd, zelfs voordat het uw browser bereikt, zodat u kunt rekenen op een veilige en aangename ervaring tijdens het surfen op het internet.

Beveiliging peer-to-peer- en IM-toepassingen. Filter tegen virussen die worden verspreid via instant messaging en softwaretoepassingen die bestanden delen.

Complete e-mailbeveiliging. BitDefender werkt op het POP3/SMTP-protocolniveau waarbij binnenkomende en uitgaande e-mailberichten worden gefilterd, ongeacht de e-mailclient (Outlook™, Outlook Express™ / Windows Mail™, The Bat!™, Netscape®, enz.) die wordt gebruikt, zonder dat hiervoor enige extra configuratie nodig is.

3.2. Firewall

De firewallmodule filtert netwerkverkeer en beheert de toegangsmachtigingen van toepassingen die een verbinding maken met internet. In de Stealthmodus wordt uw computer "verborgen" voor kwaadaardige software en hackers. De firewallmodule kan poortscans (pakketstromen die naar een machine worden verzonden om "toegangspunten" te vinden, vaak als voorbereiding voor een aanval) automatisch detecteren en uw computer beschermen tegen dit gevaar.

Beheer Internetverkeer. Definieert precies welke binnenkomende of uitgaande verbindingen u zult toestaan/weigeren. Definieert de regels inzake specifieke protocollen, poorten, toepassingen en/of externe adressen.

Internettoepassingsbeheer. BitDefender houdt een database bij van vertrouwde toepassingen en brengt gebruikers op de hoogte of de toepassingen die netwerktoegang vragen al dan niet betrouwbaar zijn, zodat ze gefundeerde beslissingen kunnen nemen. Daarnaast kan BitDefender automatisch toegang verleven voor vertrouwde toepassingen.

Verbindingsbeheer. BitDefender toont u in real time welke programma's welke verbindingen met het netwerk heeft geopend. U kunt ervoor kiezen om ze definitief of tijdelijk toe te staan of te blokkeren met één klik van de muis.

Stealth-modus. 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.

Poortscandetectie. De firewallmodule van BitDefender kan poortscans nu automatisch detecteren en blokkeren. Een poortscan is een eenvoudige manier om uit te zoeken of uw computer kwetsbaar is. Hierbij wordt een poging ondernomen om een verbinding te maken met de poorten om te zien of er enige reactie. Dit is te vergelijken met een inbreker die deuren probeert om te zien welke open is.

Firewall-wizard. De firewall-wizard helpt gebruikers bij het selecteren van het beveiligingsprofiel dat het best geschikt is voor hun omgeving - thuis, op kantoor of onderweg.

3.3. Antispam

De nieuwe en verbeterde antispamtechnologie van BitDefender maakt gebruik van opmerkelijke technologische innovaties waarmee het programma zich kan aanpassen aan de nieuwe spamtechnieken naarmate ze zich voordoen. Daarnaast leert het de voorkeuren van de gebruikers aan om spam te blokkeren terwijl een zeer laag percentage van rechtmatige e-mails als spam wordt gelabeld.

Aanpasbare filter. BitDefender maakt gebruik van cluster- en neurale netwerkanalysetechnieken om e-mail te classificeren op basis van de gebruikersvoorkeuren en patronen die zich voordoen in de lokale verzameling van e-mails. De antispam Bayes-filter kan worden aangeleerd door de gebruiker (door gewoon sommige e-mails als spam of rechtmatig te classificeren) en is ook zelflerend, zodat doorlopend nieuwe filtercriteria worden ontwikkeld op basis van eerdere beslissingen.

Anti-phishing. De nieuwe phishing-detectie van BitDefender houdt uw computer vrij van kwaadaardige e-mails die u proberen te misleiden en u vragen de gegevens van uw bankrekening of andere gevoelige gegevens te leveren.

Heuristische, URL-, Witte lijst/zwarte lijst-, tekenset- en afbeeldingsfilters. Vijf filtertypes helpen u het beheer van uw e-mail nog te verfijnen. De heuristische filter controleert de e-mail op kenmerken van spam. De filter Witte lijst/ Zwarte lijst weigert e-mail van bekende spammersadressen en laat de e-mail van uw vrienden door. De URL-filter blokkeert e-mail die kwaadaardige koppelingen bevat, terwijl de tekensetfilter e-mails blokkeert die in "vreemde" tekens zijn geschreven. De afbeeldingsfilter bepaalt of afbeeldingen die in e-mails zijn geintegreerd, specifiek zijn voor spam.

Compatibiliteit en OutlookTM-integratie. BitDefender antispam is compatibel met alle e-mailclients. Via de antispamwerkbalk van BitDefender in Microsoft Outlook™ en Outlook Express™ / Windows Mail™ kunnen gebruikers de Bayes-filter aanleren.

3.4. Antispyware

BitDefender controleert en voorkomt potentiële spyware-bedreigingen in real-time, voordat ze uw systeem kunnen beschadigen. Door gebruik te maken van een uitgebreide database van spyware-handtekeningen, blijft uw computer vrij van spyware.

Real-time antispyware. BitDefender controleert tientallen potentiële "hotspots" in uw systeem waar spyware kan optreden en controleert ook alle wijzigingen aan uw systeem en software. Bekende spyware-bedreigingen worden ook in real-time geblokkeerd.

Scannen op en opruimen van spyware. BitDefender kan het volledige systeem of een gedeelte ervan ook scannen op bekende spyware-bedreigingen. De scan maakt gebruik van een voortdurende bijgewerkte database van spyware-handtekeningen.

Privacybescherming. De privacybescherming controleert HTTP- (web) en SMTP-verkeer (e-mail) van uw computer op mogelijke persoonlijke informatie, zoals creditcardnummers, nummer van de sociale zekerheid en andere door de gebruiker gedefinieerde tekenreeksen (bijv. bits van wachtwoorden).

Anti-dialer. Een instelbare anti-dialer verhindert dat kwaadaardige toepassingen u opzadelen met een gigantische telefoonrekening.

3.5. Ouderlijk toezicht

De module voor ouderlijk toezicht van BitDefender kan de toegang blokkeren tot websites, e-mails waarvan u denkt dat ze ongepast zijn, of het internet (bepaalde perioden, zoals wanneer het "tijd is voor huiswerk"). Daarnaast kan deze module ook verhinderen dat toepassingen zoals games, chat, programma's voor het delen van bestanden of andere worden uitgevoerd.

Webbeheer. Met een URL-filter kunt u de toegang blokkeren tot ongepaste webinhoud. 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.

Heuristische webfilter. Heuristische filter classificeren webpagina's automatisch op basis van de inhoud en andere criteria. In plaats van alleen op trefwoorden te vertrouwen, past deze benadering tijdens het classificeren van de webpagina's principes toe voor antispamonderzoek. Het programma biedt vooraf gedefinieerde profielen op basis van de leeftijd van de gebruiker.

Webtrefwoordfilter. BitDefender-gebruikers kunnen nu alle webpagina's die specifieke woorden of uitdrukkingen bevatten, expliciet blokkeren.

E-mailtrefwoordfilter. Binnenkomende e-mail die ongepaste woorden of uitdrukkingen bevat, kan worden gefilterd voordat de berichten het Postvak IN bereiken.

Webtijdbeperking. Met de webtijdbeperking kunt u de webtoegang gedurende opgegeven tijdintervallen toestaan of blokkeren voor gebruikers of toepassingen.

Toepassingsbeheer. Elke toepassing kan worden geblokkeerd. Games, media en messaging software, maar ook andere categorieën van software en malware kunnen op deze manier worden geblokkeerd. Dit type blokkering beschermt toepassingen ook tegen wijzigingen, kopiëren of verplaatsen.

3.6. Andere functies

Implementatie en gebruik. Een installatiewizard wordt onmiddellijk na de installatie gestart en helpt gebruikers de meest geschikte update-instellingen te selecteren, een scanplanning te implementeren en biedt een snelle weg naar de registratie en activering van het product.

Gebruikerservaring. BitDefender heeft de gebruikerservaring volledig opnieuw ontwikkeld en de nadruk geplaatst op gebruiksvriendelijkheid en het vermijden van wanorde. Hierdoor vereisen talrijke modules van BitDefender v10 aanzienlijk minder interactie van de gebruiker dankzij het handige gebruik van automatisering en het aanleren van het systeem.

Updates per uur. Uw exemplaar van BitDefender wordt 24 maal per dag bijgewerkt via het Internet, direct of via een proxyserver. Het product is in staat zichzelf, indien nodig, te repareren door de beschadigde of ontbrekende bestanden van de BitDefender-servers te downloaden.

24/7 ondersteuning. Dit wordt u online geboden door gekwalificeerde medewerkers van de ondersteuningsdienst en via een online database met antwoorden op vaak gestelde vragen.

Reddingsschijf. **BitDefender Internet Security v10** wordt geleverd op een opstartbare cd. Deze cd kan worden gebruikt om een geinfecteerd systeem dat niet kan worden opgestart, te analyseren/repareren/desinfecteren.

4. BitDefender-modules

BitDefender Internet Security v10 contains the modules: **General**, **Antivirus**, **Firewall**, **Antispam**, **Antispyware**, **Parental Control** and **Update**.

4.1. Module Algemeen

BitDefender wordt volledig geconfigureerd geleverd voor een maximale beveiliging.

In de module Algemeen kunt u het beveiligingsniveau configureren en belangrijke beveiligingstaken uitvoeren. U kunt ook uw product registreren en de algemene gedragingen van BitDefender instellen.

4.2. Antivirusmodule

BitDefender beschermt u tegen virussen, spyware en andere malware die uw systeem binnendringen door uw bestanden, e-mailberichten, downloads en elke andere inhoud te scannen wanneer zij uw systeem binnenkomen.

De BitDefender-bescherming is ingedeeld in twee categorieën:

- Scannen bij toegang - verhindert dat nieuwe virussen, spyware en andere malware uw system binnendringt. Dit wordt ook real time bescherming genoemd. De bestanden worden gescand op het ogenblik dat de gebruiker ze opent. BitDefender zal bijvoorbeeld een Worddocument scannen op bekende gevaren wanneer u het opent, en een e-mailbericht wanneer u het ontvangt. BitDefender scant "terwijl u uw bestanden gebruikt" - bij toegang.
- Scannen op aanvraag - detecteert reeds aanwezige virussen, spyware of andere malware in uw systeem. Dit is de klassieke scan die door de gebruiker wordt geactiveerd. U selecteert welk station, welke map of welk bestand BitDefender moet scannen, en BitDefender doet dat - op aanvraag.

4.3. Module 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.

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.

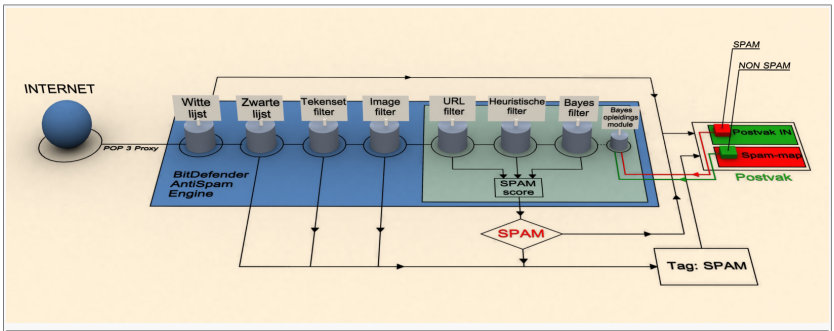
Een firewall is bijzonder belangrijk wanneer u een breedband- of DSL-verbinding hebt.

4.4. Module Antispam

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.

4.4.1. Werkschema

Het onderstaande schema toont u hoe BitDefender te werk gaat.



Antispamfilters

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.

4.4.2. 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 de sectie 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/Spammerslijst** kan worden beheerd vanaf de Beheerconsole of via de Antispam-werkbalk.

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

De meeste spamberichten zijn geschreven in Cyrillische en/of Aziatische tekensets. Configureer deze filter als u alle e-mailberichten wilt verwerpen die in deze tekensets zijn geschreven.

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

De meeste spamberichten bevatten koppelingen naar verschillende weblocaties (die doorgaans meer reclame en shoppingmogelijkheden bevatten). BitDefender beschikt over een database die koppelingen naar dit type sites bevat.

Elke URL-koppeling in een e-mailbericht zal worden gecontroleerd volgens de URL-database. Wanneer een overeenkomstig gegeven wordt gevonden, wordt een spamscore toegevoegd aan de e-mail.

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.

De filter detecteert ook de e-mailberichten met het label SEXUALLY EXPLICIT in de onderwerpregel. Deze berichten worden beschouwd 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.

Belangrijk

BitDefender kan automatische updates uitvoeren om u te beschermen tegen spammers. Houd de optie **Automatische update** ingeschakeld.

4.5. Module Antispyware

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 geinstalleerd door hackers, die proberen uw privacy in gevaar te brengen en uw persoonlijke informatie, zoals kredietkaartnummers, verzenden van uw computer naar de hacker.

4.6. Module Ouderlijk toezicht

De BitDefender-module Ouderlijk Toezicht kan toegang tot websites blokkeren die u ongeschikt vindt, toegang tot internet blokkeren voor bepaalde perioden (zoals wanneer het tijd is voor school) en toepassingen blokkeren zoals spelletjes, chatprogramma's en programma's waarmee bestanden worden gedeeld of andere toepassingen.

4.7. Module Update

Elke dag wordt nieuwe malware gevonden en geidentificeerd. Het is dan ook heel belangrijk dat u BitDefender up-to-date houdt met de meest recente malware handtekeningen. BitDefender is standaard ingesteld om elk uur te controleren op updates.

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**.

Daarnaast kunnen we vanuit het standpunt van de gebruiker ook rekening houden met de volgende types:

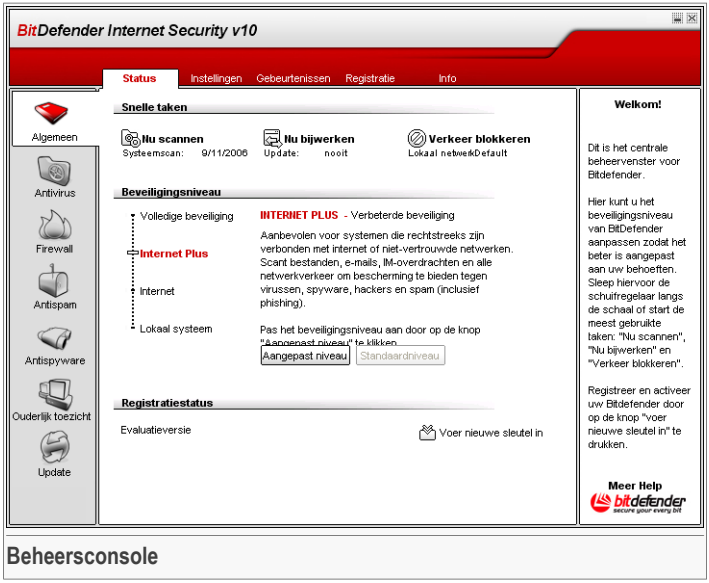
- Automatische update - BitDefender neemt automatisch contact op met de updateserver om te controleren of een nieuwe update werd uitgegeven. Als dat zo is, wordt er automatisch een update van BitDefender uitgevoerd. De automatische update kan ook op elk ogenblik worden uitgevoerd door op **Nu bijwerken** te klikken in de Update-module.
- Handmatige update - u moet de meest recente handtekeningen van gevaren handmatig downloaden en installeren.

Beheersconsole

5. Overzicht

BitDefender Internet Security v10 is ontwikkeld met een gecentraliseerde beheerconsole die de configuratie van de beveiligingsopties voor alle BitDefender-modules mogelijk maakt. Het volstaat met andere woorden de beheerconsole te openen om toegang te krijgen tot alle modules: **Antivirus**, **Firewall**, **Antispam**, **Antispyware**, **Ouderlijk toezicht** and **Update**.

Om toegang te krijgen tot de beheerconsole, kiest u in het Start-menu van Windows voor **Start → Programma's → BitDefender 10 → BitDefender Internet Security v10**. U kunt dit ook sneller doen door te dubbelklikken op het **BitDefender-pictogram** in het systeemvak.



Beheersconsole

Aan de linkerzijde van de beheersconsole ziet u de moduleselector:

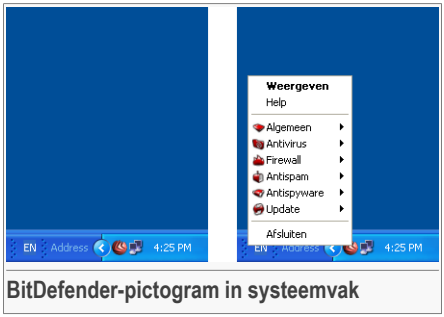
- Algemeen - in deze sectie kunt u het algemene beveiligingsniveau instellen en essentiële beveiligingstaken uitvoeren. Hier kunt u ook het product registreren en een overzicht weergeven van alle hoofdinstellingen, productdetails en contactgegevens van BitDefender.

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

Aan de rechterkant van de beheerconsole ziet u informatie over het gedeelte waarin u aan het werk bent. De optie **Meer Help** die rechts onderaan is geplaatst, opent het **Help**-bestand.

5.1. Systeemvak

Wanneer u de console minimaliseert, verschijnt een pictogram in het systeemvak.



BitDefender-pictogram in systeemvak

Wanneer u dubbelklikt op dit pictogram, wordt de beheerconsole geopend. Als u rechts klikt op het pictogram verschijnt een contextmenu. Dit biedt een snel beheer van BitDefender:

- **Weergeven / Sluiten** - opent de beheerconsole of minimaliseert de console naar het systeemvak.
- **Help** - opent het Help-bestand.
- **Algemeen** - beheer van de module Algemeen.
  - **Voer nieuwe sleutel in** - start de registratiewizard die u zal begeleiden doorheen het registratieproces.
  - **Account bewerken** - start een wizard die u zal helpen een BitDefender-account te maken.
- **Antivirus** - beheer van de Antivirus-module.

- **Real-time-beveiliging is ingeschakeld/uitgeschakeld** - toont de status van de real-time-beveiliging (ingeschakeld/uitgeschakeld). Klik op deze optie om de real-time-beveiliging in of uit te schakelen.
- **Scannen** - opent een submenu waarin u kunt kiezen om een van de taken uit te voeren die beschikbaar zijn in de sectie Scannen.

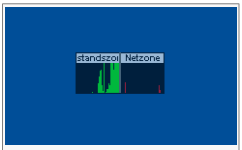
- **Firewall** - beheer van de module Firewall-module.
  - **Firewall is ingeschakeld / uitgeschakeld** - toont de status van de Firewallbeveiliging (ingeschakeld / uitgeschakeld). Klik op deze optie om de firewallbeveiliging in of uit te schakelen.
  - **Alle verkeer blokkeren** - blokkeert alle netwerk-/internetverkeer.
- **Antispam**-beheer van de Antispam-module.
  - **Antispamfilter is ingeschakeld / uitgeschakeld** - toont de status van de antispambeveiliging (ingeschakeld / uitgeschakeld). Klik op deze optie om de antispambeveiliging in of uit te schakelen.
  - **Vriendenlijst** - opent de Vriendenlijst.
  - **Spammerslijst** - opent de Spammerslijst.
- **Antispyware** - beheer van de Antispyware-module.
  - **Gedrags-antispyware is ingeschakeld / uitgeschakeld** - toont de status van de Gedrags-antispywarebeveiliging (ingeschakeld / uitgeschakeld). Klik op deze optie om de gedrags-antispywarebeveiliging in of uit te schakelen.
  - **Geavanceerde instellingen** - hiermee kunt u de antispyware-besturingselementen configureren.
- **Update** - beheer van de module Update-module.
  - **Nu bijwerken** - voert een onmiddellijke update uit.
  - **Automatische update is ingeschakeld / uitgeschakeld** - toont de status van de automatische update (ingeschakeld / uitgeschakeld). Klik op deze optie om de automatisch update in of uit te schakelen.
- **Afsluiten** - sluit de toepassing af. Wanneer u deze optie selecteert, verdwijnt het pictogram uit het systeemvak. Als u de beheersconsole opnieuw wilt openen, moet u hem opnieuw starten vanaf het menu Start van Windows.

Opmerking

Als u een of meer BitDefender-modules uitschakelt, wordt het pictogram zwart. Hierdoor weet u of bepaalde modules zijn uitgeschakeld, zonder dat u hiervoor de beheerconsole hoeft te openen.
Het pictogram zal knipperen wanneer een update beschikbaar is.

5.2. Balk scanactiviteit

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



Activiteitenbalk

De groene balken (de **Bestandszone**) 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.

Opmerking

Wanneer de Virus Shield of de Firewall is uitgeschakeld zal de **balk Scanactiviteit** dit aangeven met een rood kruis over het overeenkomende gebied (**Bestandszone** of **Netzone**). Hierdoor weet u of u beschermd bent, zonder dat u hiervoor de beheerconsole hoeft te openen.

Als u deze grafische voorstelling niet langer wilt zien, klik er dan op met de rechtermuisknop en selecteer **Verbergen**.

Opmerking

Om dit venster volledig te verbergen, schakelt u de optie **De balk voor scanactiviteit inschakelen (grafiek op het scherm van productactiviteit)** uit (in de module **Algemeen** onder de sectie Instellingen).

6. Module Algemeen

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

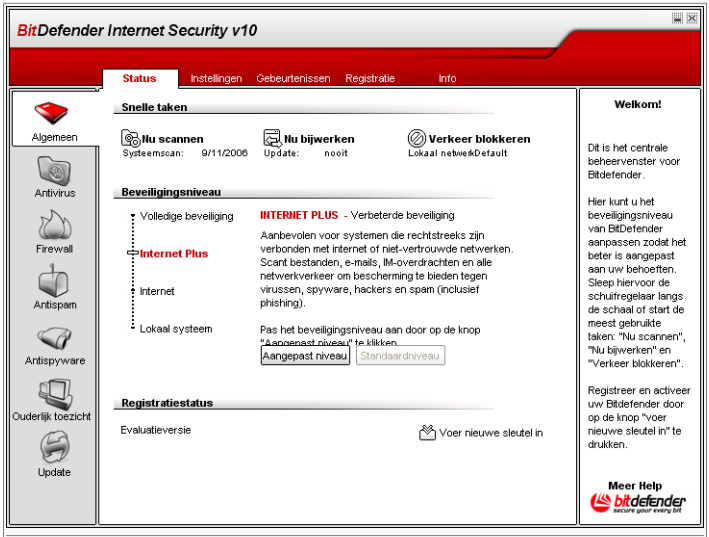
- Centraal beheer
- Instellingen beheerconsole
- Gebeurtenissen
- Productregistratie
- Info

Opmerking

Meer details over de module **Algemeen** kunt u vinden in de beschrijving van "*Module Algemeen*" (p. 29).

6.1. Centraal beheer

Om dit gedeelte te openen, klikt u op het tabblad **Status** in de module **Algemeen**.



Centraal beheer

In dit gedeelte kunt u het algemene beveiligingsniveau configureren en belangrijke BitDefender-taken uitvoeren. U kunt ook het product registreren en de vervaldatum bekijken.

6.1.1. Snelle taken

BitDefender biedt u snel toegang tot de belangrijkste beveiligingstaken. Met deze taken kunt u BitDefender up-to-date houden, uw systeem scannen en verkeer blokkeren.

Om het volledige systeem te scannen, hoeft u alleen op **Nu scannen** te klikken. Het scanvenster wordt geopend en een volledige systeemscan wordt gestart.

Belangrijk

We raden u sterk aan minstens eenmaal per week een volledige systeemscan uit te voeren. Raadpleeg het gedeelte Scannen op aanvraag van deze gebruiksaanwijzing voor meer details over de scantaken en het scanproces.

Wij raden u aan een update uit te voeren van BitDefender voordat u het systeem scant, zodat de meest recente bedreigingen kunnen worden gedetecteerd. Om een update uit te voeren van BitDefender, hoeft u alleen op **Nu bijwerken** te klikken. Wacht enkele seconden tot het updateproces is voltooid. Het zelfs nog beter om de updatestatus te controleren in het gedeelte Update.

Opmerking

Raadpleeg het gedeelte Automatische update van deze gebruiksaanwijzing voor meer details over het updateproces.

Om alle netwerk-/internetverkeer te blokkeren, hoeft u alleen op **Verkeer blokkeren** te klikken. Hiermee wordt uw computer geisoleerd tegen andere computer op het netwerk.

Opmerking

Raadpleeg het hoofdstuk de Firewall-modulevan deze handleiding om te leren hoe u uw computer op een efficiënte manier kunt beveiligen binnen het netwerk waarvan de pc deel uitmaakt.

6.1.2. Beveiligingsniveau

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 4 beveiligingsniveaus:

Beveiligingsniveau	Beschrijving
Lokaal systeem	Vooral aanbevolen voor computer zonder netwerk- of internettoegang. Het verbruiksniveau van de bron is laag. Geopende bestanden worden gescand op virussen en spyware.
Internet	Biedt standaard bescherming voor computers die rechtstreeks verbonden zijn met het internet of niet-vertrouwde netwerken. Het verbruiksniveau van de bron is gemiddeld. Geopende bestanden, e-mail, IM-overdrachten en al het netwerkverkeer worden gescand om bescherming te bieden tegen virussen, spyware en hackers.
Internet Plus	Biedt geavanceerde bescherming voor computers die rechtstreeks verbonden zijn met het internet of niet-vertrouwde netwerken. Het verbruiksniveau van de bron is gemiddeld. Geopende bestanden, e-mail, IM-overdrachten en al het netwerkverkeer worden gescand om bescherming te bieden tegen virussen, spyware, hackers en spam (phishing inbegrepen).
Volledige beveiliging	Biedt een volledige bescherming van uw systeem. Het verbruiksniveau van de bron is hoog. Scant geopende bestanden, e-mail, IM-overdrachten en al het netwerkverkeer om bescherming te bieden tegen virussen, spyware, hackers, spam (phishing inbegrepen) en ongepaste inhoud.

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

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

6.1.3. Registratiestatus

U kunt informatie over de status van uw BitDefender-licentie weergeven. Hier kunt u het product registreren en de vervaldatum bekijken.

Om een nieuwe sleutel in te voeren, hoeft u alleen op **Voer nieuwe sleutel in** te klikken. Voltooi de registratiewizard om BitDefender te registreren.

Opmerking

Raadpleeg het gedeelte Productregistratie van deze gebruiksaanwijzing voor meer details over het registratieproces.

6.2. Instellingen beheerconsole

Om dit gedeelte te openen, klikt u op het tabblad **Instellingen** in de module **Algemeen**.

Instellingen beheerconsole

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.

Er zijn 4 optiecategorieën: **Algemene instellingen**, **Virusrapportinstellingen**, **Skin-instellingen** en **Instellingen beheren**.

6.2.1. Algemene instellingen

- **Wachtwoordbeveiliging voor productinstellingen inschakelen** - hiermee kan een wachtwoord worden ingesteld om de configuratie van de BitDefender-beheerconsole te beveiligen.

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, wordt het volgende venster geopend:

Wachtwoord invoeren

Geef het wachtwoord op in het veld **Wachtwoord** en typ het opnieuw in het veld **Wachtwoord opnieuw invoeren**. Klik daarna op **OK**.

Wanneer u voortaan de opties van de BitDefender-configuratie wilt wijzigen, zult u worden gevraagd het wachtwoord in te voeren.

Belangrijk

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

- **BitDefender-nieuws weergeven (berichten i.v.m. beveiliging)** - toont af en toe beveiligingsberichten die door de BitDefender-server zijn verzonden met betrekking tot de uitbraak van virussen.
- **Pop-ups weergeven (notities op het scherm)** - toont pop-upvensters die betrekking hebben op de productstatus.
- **BitDefender laden wanneer Windows start** - start BitDefender automatisch wanneer het systeem wordt opgestart.

Opmerking

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.
- **Console minimaliseren bij opstarten** - minimaliseert de BitDefender-beheerconsole nadat deze is geladen bij het opstarten van het systeem. Alleen het BitDefender-pictogram verschijnt in het systeemvak.

6.2.2. Virusrapportinstellingen

- **Virusrapporten verzenden** - verzendt rapporten met betrekking tot virussen die op uw computer werden geidentificeerd 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.

6.2.3. Skin-instellingen

Hiermee kunt u de kleur van de beheerconsole selecteren. De skin vertegenwoordigt de achtergrondafbeelding op de interface. Om een andere skin te selecteren, klikt u op de overeenkomstige kleur.

6.2.4. 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 geinstalleerd of hebt gerepareerd.

Belangrijk

Alleen gebruikers met beheermachtigingen kunnen instellingen opslaan en laden.

Klik op **Toepassen** om de wijzigingen op te slaan. Als u op **Standaard** klikt, worden de standaardinstellingen geladen.

6.3. Gebeurtenissen

Om dit gedeelte te openen, klikt u op het tabblad **Gebeurtenissen** in de module **Algemeen**.

Gebeurtenissen

In dit gedeelte worden alle gebeurtenissen weergegeven die door BitDefender zijn gegenereerd.

Er zijn 3 types gebeurtenissen: **Informatie**, **Waarschuwing** en **Kritiek**.

Voorbeelden van gebeurtenissen:

- **Informatie** - wanneer een e-mail is gescand;
- **Waarschuwing** - wanneer een verdacht bestand is gevonden;
- **Kritiek** - wanneer een geinfecteerd bestand is gevonden;

Voor elke gebeurtenis wordt de volgende informatie weergegeven: de datum en het tijdstip waarop de gebeurtenis zich heeft voorgedaan, een korte beschrijving en de bron (**Antivirus**, **Firewall**, **Antispyware** of **Update**). Dubbelklik op een gebeurtenis om de eigenschappen weer te geven.

U kunt deze gebeurtenissen op twee manieren filteren (op type of op bron):

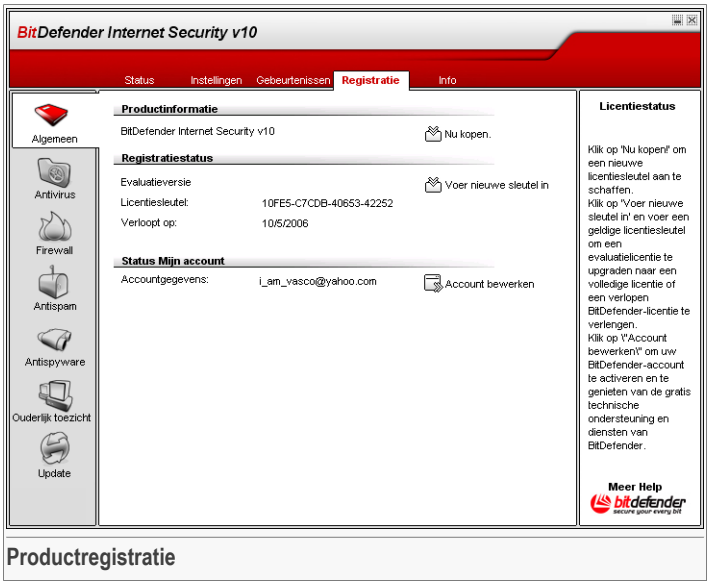
- Klik op **Filter** om het type weer te geven gebeurtenissen te selecteren.
- Selecteer de bron van de gebeurtenis in het vervolgkeuzemenu.

Als de beheerconsole is geopend op het gedeelte **Gebeurtenissen** en er zich op hetzelfde ogenblik een gebeurtenis voordoet, moet u op **Vernieuwen** klikken om die gebeurtenis weer te geven.

Klik op **Logboek wissen** om alle gebeurtenissen uit de lijst te verwijderen.

6.4. Productregistratie

Om dit gedeelte te openen, klikt u op het tabblad **Registreren** in de module **Algemeen**.



Productregistratie

Dit gedeelte bevat informatie over het BitDefender-product (registratiestatus, product-ID, vervaldatum) en de BitDefender-account. Hier kunt u het product registreren en uw BitDefender-account configureren.

Klik op de knop **Nu kopen** om een nieuwe licentiesleutel aan te schaffen in de online winkel van BitDefender.

Wanneer u op de knop **Nu kopen** klikt, kunt u het product registreren en de registratiesleutel of de accountdetails wijzigen. Om uw BitDefender-account te configureren, klikt u op **Account bewerken**. In beide gevallen verschijnt de registratiewizard.

6.4.1. Registratiewizard

De registratiewizard is een procedure die uit 5 stappen bestaat.

Stap 1/5 - Welkom bij de registratiewizard van BitDefender

Welkomstvenster

Klik op **Volgende**.

Stap 2/5 - BitDefender registreren

Registratie

Selecteer **Het product registreren** om **BitDefender Internet Security v10** 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**.

Stap 3/5 - Een BitDefender-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.

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 opnieuw invoeren**. 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.

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.

Belangrijk

Activeer uw account voordat u doorgaat naar de volgende stap.

Klik op **Deze stap overslaan** als u geen BitDefender-account wilt maken. Hiermee slaat u ook de volgende stap van de wizard over.

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

Ik heb al een BitDefender-account

Als u al een actieve account hebt, geef dan het e-mailadres en het wachtwoord van uw account op. Als u een onjuist wachtwoord opgeeft, wordt u gevraagd dit opnieuw in te voeren wanneer u op **Volgende** klikt. Klik op **OK** om het wachtwoord opnieuw in te voeren of op **Annuleren** om de wizard af te sluiten.

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

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

Stap 4/5 - Accountdetails invoeren

Accountdetails

Opmerking

Als u **Deze stap overslaan** hebt geselecteerd in de derde stap, wordt deze stap niet weergegeven.

Vul eerst uw voornaam, achternaam en uw land in.

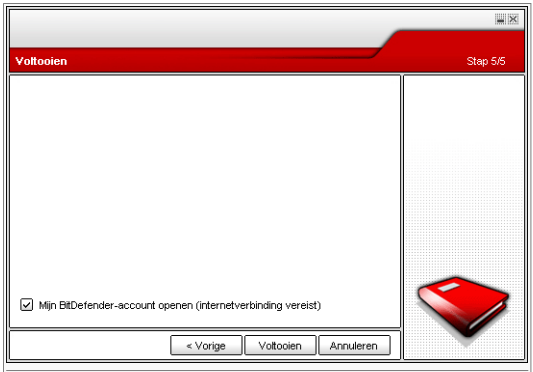
Als u al een account hebt, toont de wizard de informatie die u eerder hebt opgegeven, als die er is. Hier kunt u deze informatie ook desgewenst wijzigen.

Belangrijk

De gegevens die u hier opgeeft blijven vertrouwelijk.

Klik op **Volgende**.

Stap 5/5 – Overzicht weergeven



Voltooien

Dit is de laatste stap van de configuratiewizard. 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.

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

6.5. Info

Om dit gedeelte te openen, klikt u op het tabblad **Info** in de module **Algemeen**.

Algemene informatie

In dit onderdeel vindt u de contactinformatie en productdetails.

BitDefender™ is een toonaangevende wereldwijde leverancier van beveiligingsoplossingen die voldoen aan de beschermingsvereisten van de hedendaagse computeromgeving. Het bedrijf biedt een van de snelste en meest effectieve lijnen van beveiligingssoftware in de sector en legt nieuwe maatstaven vast voor de preventie, tijdige detectie en beperking van bedreigingen. BitDefender levert producten en diensten aan meer dan 41 miljoen thuis- en zakelijke gebruikers in meer dan 180 landen.

BitDefenderTM is gecertificeerd door alle belangrijke, onafhankelijke controle-instellingen - **ICSA Labs**, **CheckMark** en **Virus Bulletin**, en is het enige beveiligingsproduct dat met een **IST-prijs** werd bekroond.

Meer informatie over BitDefender kunt u vinden op de site: http://www.bitdefender.com.

7. Antivirusmodule

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

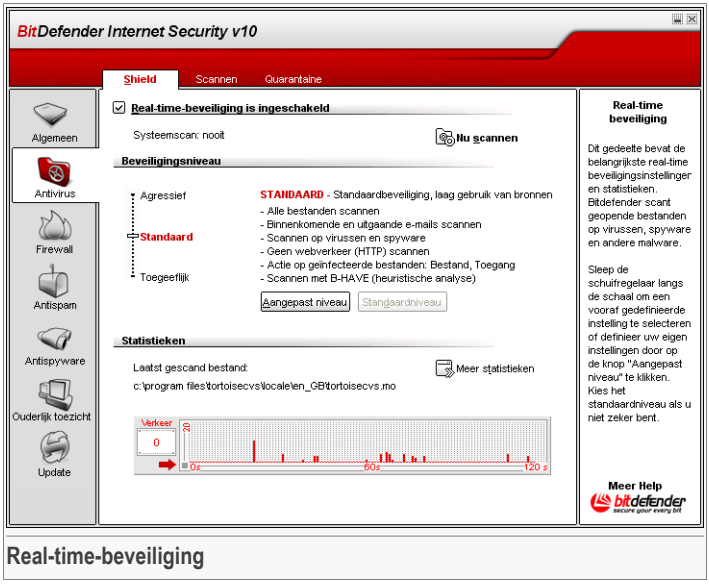
- Scannen bij toegang
- Scannen op aanvraag
- Quarantaine

Opmerking

Meer details over de module **Antivirus** kunt u vinden in de beschrijving van "*Antivirusmodule*" (p. 29).

7.1. Scannen bij toegang

Om dit gedeelte te openen, klikt u op het tabblad **Shield** in de module **Antivirus**.



Real-time-beveiliging

In dit gedeelte kunt u de **Real-time-beveiliging** configureren en informatie over de activiteiten van deze optie bekijken. De **Real-time-beveiliging** houdt uw computer veilig door e-mailberichten, downloads en alle geopende bestanden te scannen.

Belangrijk

Om te verhinderen dat uw computer door virussen wordt geinfecteerd, 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.

7.1.1. Beveiligingsniveau

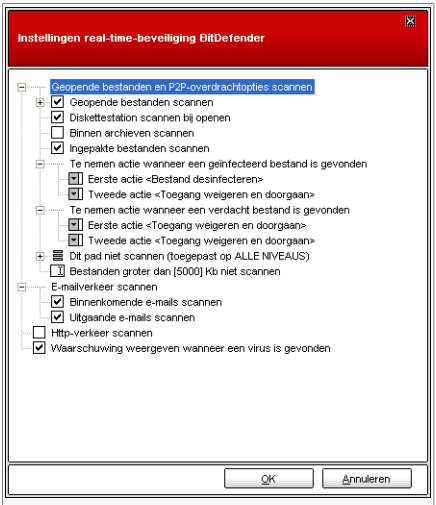
U kunt het beveiligingsniveau kiezen dat beter voldoet aan uw beveiligingsbehoeften. Sleep de schuifregelaar langs de schaal om het geschikte beveiligingsniveau in te stellen.

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 geinfecteerde 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 geinfecteerde 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 geinfecteerde bestanden: bestand opruimen/toegang weigeren.

Gevorderde gebruikers willen wellicht voordeel halen uit de scaninstellingen die door BitDefender worden aangeboden. U kunt de scanner instellen om extensies, mappen of archieven over te slaan, waarvan u weet dat ze onschadelijk zijn. 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 niveau** te klikken. Het volgende venster wordt geopend:



Shield-instellingen

De scanopties zijn in een uitvouwbaar menu geordend op een gelijkaardige wijze als in de Verkenner van Windows.

Klik op het vakje met een "+" om een optie te openen of op het vakje met een "-" om een optie te sluiten.

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`;

Optie		Beschrijving
		.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 ";".
	Extensies uitsluiten van scan: [ ]	De bestanden met de extensies die door de gebruiker zijn gedefinieerd, worden NIET gescand. Deze extensies moeten worden gescheiden door ";".
	Scannen op riskware	Scannen op riskware. Deze bestanden zullen worden behandeld als geinfecteerde bestanden. 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.
Diskettestation scannen bij openen		Scant het diskettestation wanneer het wordt gebruikt.
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 geinfecteerde en verdachte bestanden in het vervolgkeuzemenu.
	Toegang weigeren en doorgaan	Wanneer een geinfecteerd bestand is gedetecteerd, zal de toegang tot dit bestand worden geweigerd.
	Bestand opruimen	Desinfecteert het geinfecteerde bestand.

Optie		Beschrijving
	Bestand verwijderen	Verwijdert onmiddellijk de geinfecteerde bestanden, zonder enige waarschuwing.
	Bestand verplaatsen naar quarantaine	De geinfecteerde bestanden worden naar de quarantaine verplaatst.
Tweede actie		Selecteer in het vervolgkeuzemenu de tweede actie die moet worden genomen op geinfecteerde bestanden in het geval de eerste actie mislukt.
	Toegang weigeren en doorgaan	Wanneer een geinfecteerd bestand is gedetecteerd, zal de toegang tot dit bestand worden geweigerd.
	Bestand verwijderen	Verwijdert onmiddellijk de geinfecteerde bestanden, zonder enige waarschuwing.
	Bestand verplaatsen naar quarantaine	De geinfecteerde bestanden worden naar de quarantaine verplaatst.
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.
Dit pad niet scannen (toegepast op ALLE NIVEAUS)		Klik op "+" naast DEZE OPTIE om een map te definiëren die niet moet worden gescand. Hierdoor zal de optie uitbreiden en wordt de nieuwe optie `Nieuw item` weergegeven. Klik op het overeenkomende selectievakje van het nieuwe item en selecteer in het verkennervenster de map die u wilt uitsluiten van de scan. De objecten die hier zijn geselecteerd, zullen van het scannen worden uitgesloten, ongeacht het gekozen beveiligingsniveau (niet uitsluitend voor **Aangepast niveau**).

- **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 geinfecteerd 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 geinfecteerde e-mail zal het waarschuwingsvenster ook informatie over de afzender en de ontvanger bevatten.

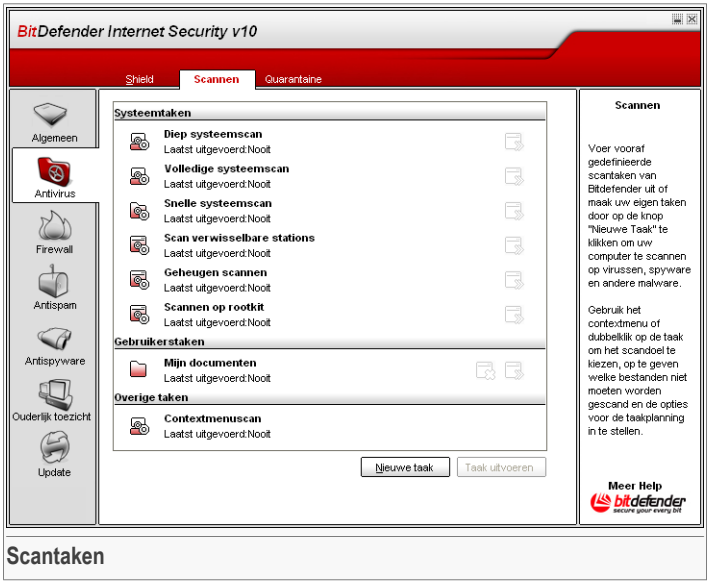
  Als een verdacht bestand is gedetecteerd, kunt u een wizard starten vanaf het waarschuwingsvenster. Deze wizard zal u helpen bij het verzenden van dat bestand naar BitDefender Labs voor verdere analyse. U kunt uw e-mailadres invoeren om informatie te ontvangen over dit rapport.

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

Klik op **Standaardniveau** als u wilt terugkeren naar het standaardniveau.

7.2. Scannen op aanvraag

Om dit gedeelte te openen, klikt u op het tabblad **Scannen** in de module **Antivirus**.



Scantaken

In dit onderdeel kunt u BitDefender configureren om uw computer te scannen.

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 geinstalleerd. En het is zeker ook een goed idee om uw computer frequent te scannen op virussen.

7.2.1. Scantaken

Scannen op aanvraag is gebaseerd op scantaken. De gebruiker kan de computer scannen met de standaardtaken of met zijn eigen scantaken (door gebruiker gedefinieerde taken).

Er zijn drie categorieën scantaken:

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

Standaardtaak	Beschrijving
Diep systeemscan	Scant het volledige systeem, inclusief archieven, op virussen en spyware.
Volledige systeemscan	Scant het volledige systeem, behalve archieven, op virussen en spyware.
Snelle systeemscan	Scant alle programma's op virussen en spyware.
Scan verwisselbare stations	Scant verwisselbare stations op virussen en spyware.
Scan Geheugen	Scan het geheugen op bekende spyware-bedreigingen.
Scannen op rootkits	Scant het geheugen op stealth-malware.

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

  Er is een taak voorzien met de naam `Mijn documenten`. Gebruik deze taak om uw documenten in de map `Mijn documenten` te scannen.
- **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:

- **Taak plannen** - geeft aan dat de geselecteerde taak voor later is gepland. Klik op deze knop om naar het gedeelte Planner in het venster **Eigenschappen** te gaan waar u deze instelling kunt wijzigen.
- **Verwijderen** - verwijdert de geselecteerde taak.

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

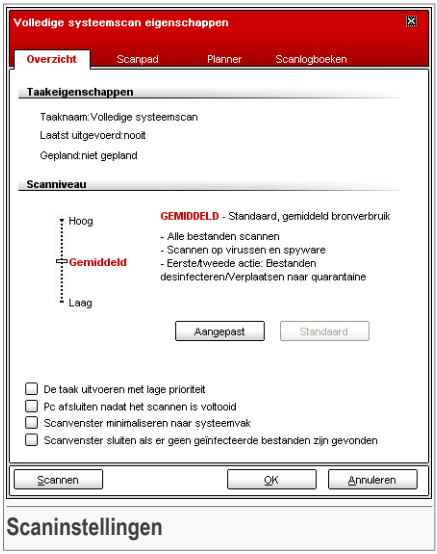
- **Nu scannen** - voert de geselecteerde taak uit en start de optie Onmiddellijk scannen.

7.2.2. Eigenschappen scantaak

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. Dubbelklik op de taak om dit venster te openen. Het volgende venster wordt geopend:

Scaninstellingen



Scaninstellingen

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

Scanniveau

U moet eerst het scanniveau 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. De volgende acties worden

Beveiligingsniveau	Beschrijving
	ondernomen op geinfecteerde bestanden: bestand opruimen/verplaatsen naar quarantaine.
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. De volgende acties worden ondernomen op geinfecteerde bestanden: bestand opruimen/verplaatsen naar quarantaine.
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. De volgende acties worden ondernomen op geinfecteerde bestanden: bestand opruimen/verplaatsen naar quarantaine.

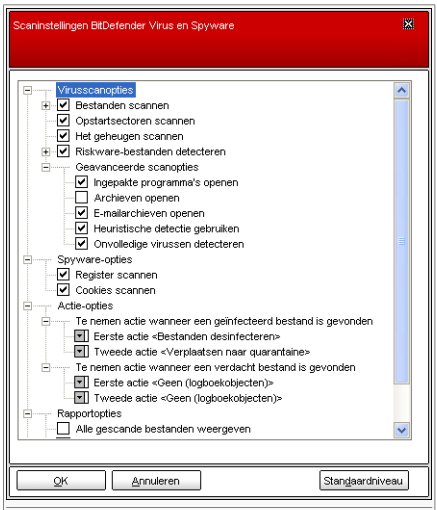
Belangrijk

De taak **Scannen op rootkits** heeft dezelfde scanniveaus. De opties zijn echter verschillend:

- **Laag** - Alleen de processen worden gescand. Er wordt geen actie ondernomen voor de gedetecteerde objecten.
- **Gemiddeld** - Bestanden en processen worden gescand bij het zoeken van verborgen objecten. Er wordt geen actie ondernomen voor de gedetecteerde objecten.
- **Hoog** - Bestanden en processen worden gescand bij het zoeken van verborgen objecten. De naam van de gedetecteerde objecten wordt gewijzigd.

Gevorderde gebruikers willen wellicht voordeel halen uit de scaninstellingen die door BitDefender worden aangeboden. U kunt de scanner instellen om extensies, mappen of archieven over te slaan, waarvan u weet dat ze onschadelijk zijn. 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. Het volgende venster wordt geopend:



Scaninstellingen

De scanopties zijn in een uitvouwbaar menu geordend op een gelijkaardige wijze als in de Verkenner van Windows.

De scanopties zijn gegroepeerd in vijf categorieën:

- **Virusscanopties**
- **Spyware-opties**
- **Actie-opties**
- **Rapportopties**
- **Overige opties**

Klik op het vakje met een "+" om een optie te openen of op het vakje met een "-" om een optie te sluiten.

Belangrijk

Voor de taak **Scannen op rootkits** zijn er slechts drie categorieën beschikbaar: **Scanopties rootkit**, **Rapportopties** en **Overige opties**. In de eerste categorie kunt u kiezen wat u wilt scannen (bestanden, geheugen of beide) en kunt u de actie instellen die moet worden ondernomen voor de gedetecteerde objecten (**Geen (logboekobjecten)/Naam bestanden wijzigen**). De laatste twee categorieën zijn identiek aan de hieronder beschreven categorieën.

- 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**.

Optie		Beschrijving
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 ";".
	Door gebruiker gedefinieerde extensies uitsluiten	De bestanden met de extensies die door de gebruiker zijn gedefinieerd, worden NIET gescand. Deze extensies moeten worden gescheiden door ";".
Opstartsectoren scannen		Scant de opstartsector van het systeem.
Geheugen scannen		Scant het geheugen op virussen en andere malware.
Riskware-bestanden detecteren		Scannen op andere bedreigingen dan virussen, zoals dialers en adware. Deze bestanden zullen worden behandeld als geinfecteerde bestanden. Software die adware-componenten bevat, zal mogelijk niet meer werken als deze optie is ingeschakeld. Selecteer **Behalve toepassingen en dialers** als u dit type bestanden wilt uitsluiten van het scannen.
Geavanceerde scanopties	**Ingepakte programma's openen**	Scant ingepakte bestanden.
	Archieven openen	Scant binnen archieven.

Optie	Beschrijving
E-mailarchieven openen	Scant binnen e-mailarchieven.
Heuristische detectie gebruiken	Om heuristisch scannen van de bestanden te gebruiken. 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.
Onvolledige virussen detecteren	Detecteert onvolledige virussen.

- Geef het spyware-scandoel op (register, cookies). Selecteer hiervoor bepaalde opties van de categorie **Spyware-scanopties**.

Optie	Beschrijving
Register scannen	Scant registergegevens.
Cookies scannen	Scant cookiebestanden.

- Geef de actie op die moet worden uitgevoerd op geinfecteerd of verdachte bestanden. Open de categorie **Actie-opties** om alle mogelijke acties op deze bestanden weer te geven.

  Selecteer de acties die moeten worden ondernomen wanneer een geinfecteerd of verdacht bestand is gevonden. U kunt verschillende acties instellen voor geinfecteerde en verdachte bestanden. U kunt ook een tweede actie selecteren indien de eerste mislukt.

Actie	Beschrijving
Geen (logboekobjecten)	Er wordt geen actie ondernomen voor geinfecteerde bestanden. Deze bestanden zullen verschijnen in het rapportbestand.

Actie	Beschrijving
Gebruiker vragen naar actie	Wanneer een geinfecteerd bestand wordt gedetecteerd, verschijnt een venster waarin de gebruiker wordt gevraagd de actie voor dat bestand te selecteren. Afhankelijk van het belang van dat bestand, kunt u kiezen om het te desinfecteren, te isoleren naar het quarantainegebied of te verwijderen.
Bestanden desinfecteren	Desinfecteert het geinfecteerde bestand.
Bestanden verwijderen	Verwijdert onmiddellijk de geinfecteerde bestanden, zonder enige waarschuwing.
Bestanden verplaatsen naar quarantaine	Verplaatst de geinfecteerde bestanden naar de quarantaine.
Naam bestanden wijzigen	Wijzigt de extensie van de geinfecteerde bestanden. De nieuwe extensie van de geinfecteerde bestanden zal `.vir` zijn. Door de naam van de geinfecteerde bestanden te wijzigen, wordt de mogelijkheid ze uit te voeren uitgesloten, zodat de infectie zich niet kan verspreiden. Ze kunnen bovendien ook tegelijkertijd worden opgeslagen voor verder onderzoek en analyse.

Belangrijk

Naam bestanden wijzigen heeft een gelijksoortig effect op de verborgen bestanden (rootkits). De nieuwe extensie van de gedetecteerde bestanden zal `.bd.ren` zijn. Door de naam van de gedetecteerde bestanden te wijzigen, wordt de mogelijkheid ze uit te voeren uitgesloten, zodat de potentiële infectie zich niet kan verspreiden. Ze kunnen bovendien ook tegelijkertijd worden opgeslagen voor verder onderzoek en analyse.

- Geef de opties op voor de rapportbestanden. Open de categorie **Rapportopties** om alle mogelijke opties weer te geven.

Optie	Beschrijving
Alle gescande bestanden weergeven	Geeft een lijst weer van alle gescande bestanden en hun status (geinfecteerd of niet) in een rapportbestand. Wanneer u deze optie inschakelt, zal de computer langzamer werken.

Optie	Beschrijving
Logboeken ouder dan [x] dagen verwijderen	Dit is een bewerkingsveld waarin u kunt opgeven hoelang een rapport moet worden bewaard in het gedeelte Scanlogboeken. Selecteer deze optie en voer een nieuw tijdinterval in. Het standaard tijdinterval is 180 dagen.

Opmerking

De rapportbestanden kunnen worden weergegeven in het gedeelte Scanlogboeken in het venster **Eigenschappen**.

- Geef de overige opties op. Open de categorie **Overige opties** waar u de volgende optie kunt selecteren:

Optie	Beschrijving
Verdachte bestanden verzenden naar BitDefender Lab	U wordt gevraagd alle verdachte bestanden naar BitDefender Lab te verzenden nadat het scanproces is voltooid.

Als u op **Standaard** klikt, worden de standaardinstellingen geladen.

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

Overige instellingen

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

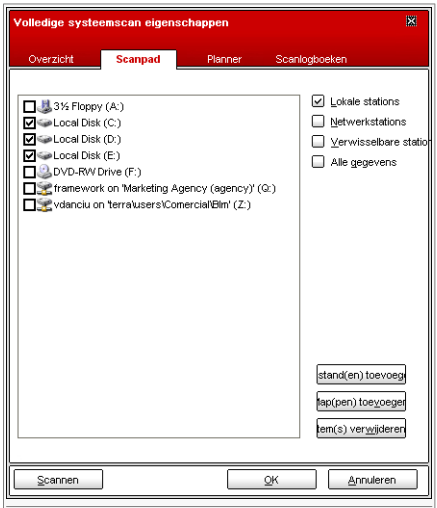
Optie	Beschrijving
De taak uitvoeren met lage prioriteit	Verlaagt de prioriteit van het scanproces. U zult andere programma's sneller kunnen uitvoeren en de tijd die nodig is om het scanproces te voltooien, verlengen.
Pc afsluiten nadat het scannen is voltooid	Met deze optie wordt de computer uitgeschakeld nadat het scanproces is voltooid.
Verdachte bestanden verzenden naar BitDefender Lab	U wordt gevraagd alle verdachte bestanden naar BitDefender Lab te verzenden nadat het scanproces is voltooid.

Optie	Beschrijving
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.

Scandoel

Dubbelklik op een geselecteerde taak en klik vervolgens op het tabblad **Scanpad** om dit onderdeel te openen.



Scandoel

Hier kunt u het scandoel instellen.

Dit onderdeel bevat de volgende knoppen:

- **Bestand(en) toevoegen** - opent een zoekvenster waarin u de bestanden die u wilt scannen, kunt selecteren.
- **Map(pen) toevoegen** - idem als hierboven, maar hier selecteert u in plaats van de bestanden, de mappen door BitDefender moeten worden gescand.

Opmerking

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

- **Item(s) verwijderen** - verwijdert bestanden/mappen die vooraf werden geselecteerd uit de lijst 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.

Planner

Dubbelklik op een geselecteerde taak en klik vervolgens op het tabblad **Planner** om dit onderdeel te openen.

Planner

Hier kunt u zien of de taak al dan niet is gepland en kunt u deze eigenschap wijzigen.

Belangrijk

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.

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

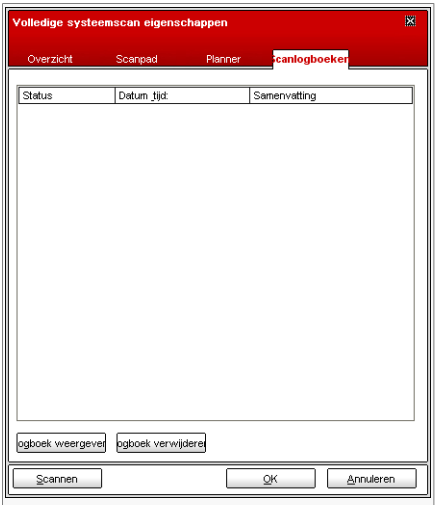
- **Niet gepland** - start de taak alleen wanneer de gebruiker dit vraagt.
- **Eenmalig** - start het scannen eenmalig op een bepaald ogenblik. Geef de startdatum en het starttijdstip op in de velden **Startdatum/Starttijd**.
- **Periodiek** - start de scan periodiek, met bepaalde tijdintervallen (uren,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

Scanlogboeken

Dubbelklik op een geselecteerde taak en klik vervolgens op het tabblad **Scanlogboeken** om dit onderdeel te openen.



Scanlogboeken

Hier kunt u de rapportbestanden weergeven die telkens worden gegenereerd wanneer de taak wordt uitgevoerd. Elke bestand bevat ingesloten informatie in zijn status (opgeruimd/geinfecteerd), de datum en het tijdstip waarop de scan werd uitgevoerd en een overzicht (scan voltooid).

Er zijn twee knoppen beschikbaar:

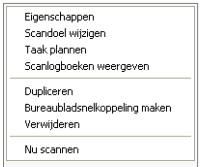
- **Logboek weergeven** - om het geselecteerde rapportbestand weer te geven;
- **Logboek verwijderen** - om het geselecteerde rapportbestand te verwijderen.

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.

7.2.3. Snelmenu

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



Snelmenu

De volgende opdrachten zijn beschikbaar in het snelmenu:

- **Eigenschappen** - opent het venster **Eigenschappen**, het tabblad **Overzicht** waar u de instellingen van de geselecteerde taak kunt wijzigen;
- **Scandoel wijzigen** - opent het venster **Eigenschappen**, het tabblad **Scanpad** waar u het scandoel voor de geselecteerde taak kunt wijzigen;
- **Taak plannen** - opent het venster **Eigenschappen**, het tabblad **Planner** waar u de geselecteerde taak kunt plannen;
- **Scanlogboeken weergeven** - opent het venster **Eigenschappen**, het tabblad **Scanlogboeken** waar u de rapporten kunt weergeven die zijn gegenereerd nadat de geselecteerde taak is uitgevoerd;
- **Dupliceren** - 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.

- **Bureaubladsnelkoppeling maken** - maakt een bureaubladsnelkoppeling naar de geselecteerde taak;
- **Verwijderen** - verwijdert de geselecteerde taak;

Opmerking

Niet beschikbaar voor systeemtaken. U kunt geen systeemtaak verwijderen.

- **Nu scannen** - voert de geselecteerde taak uit en start een onmiddellijke scan.

Belangrijk

Door hun specifieke aard, zijn alleen de opties **Eigenschappen** en **Scanlogboeken weergeven** beschikbaar voor de taken in de categorie **Diverse taken**.

7.2.4. Types Scannen op aanvraag

BitDefender biedt u drie 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 v10;
- Scannen door slepen & neerzetten - sleep een bestand of map naar de balk Scanactiviteit;

Onmiddellijk scannen

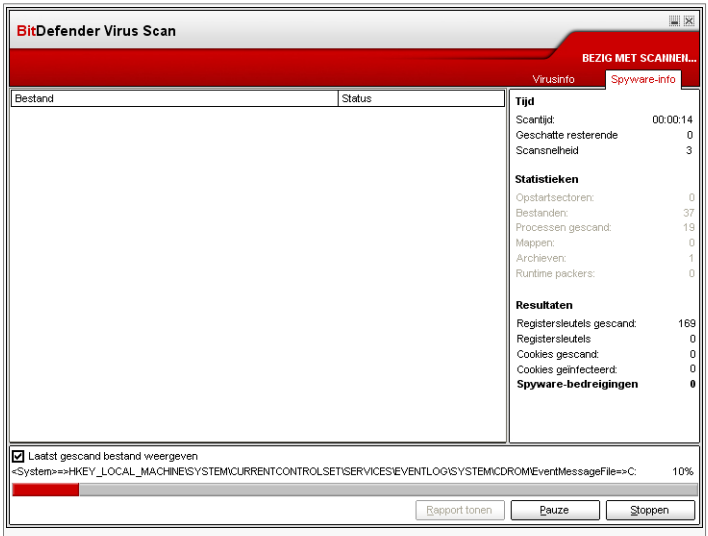
Om uw computer volledig of gedeeltelijk te scannen, kunt u de standaard scantaken gebruiken of uw eigen scantaken maken. Er zijn twee methoden om scantaken te maken:

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

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).

Voordat u BitDefender uw computer laat scannen, moet u ervoor zorgen dat de virushandtekeningen van BitDefender up-to-date zijn omdat er dagelijks nieuwe virussen worden gevonden en geidentificeerd. In het bovenste gedeelte van de Update-module kunt u controleren wanneer de laatste update is uitgevoerd.

Om het scannen te starten, selecteert u de gewenste scantaak in de lijst en klikt u op de knop **Nu scannen** aan de rechterzijde. U kunt ook klikken op **Taak uitvoeren**. Het scanvenster wordt geopend:



Scanvenster

Wanneer een scanproces wordt uitgevoerd, verschijnt een pictogram in het systeemvak.

Tijdens het scannen toont BitDefender de voortgang van het proces en waarschuwt het programma u wanneer bedreigingen worden gevonden. Aan de rechterkant ziet u de statistieken van het scanproces. Afhankelijk van het scandoel zal informatie over spyware en/of virussen beschikbaar zijn. Als beide beschikbaar zijn, kunt u op het overeenkomende tabblad klikken voor meer informatie over het spyware- of virusscanproces.

Schakel het selectievakje naast **Laatst gescand bestand weergeven** in om alleen de informatie over het laatst gescande bestand weer te geven.

Opmerking

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

Er zijn drie knoppen beschikbaar:

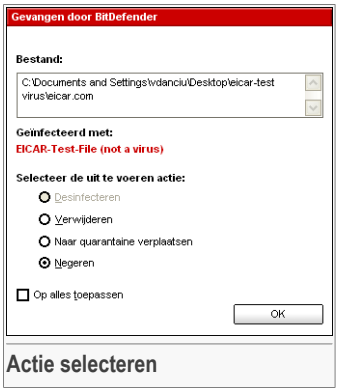
- **Stoppen** - opent een nieuw venster waarin u het scanproces kunt beëindigen. Klik op **Ja**&**Sluiten** om het scanvenster af te sluiten.
- **Pauze** - stopt het scanproces tijdelijk. U kunt doorgaan door te klikken op **Hervatten**.

- **Rapport tonen** - opent het scanrapport.

Opmerking

Als u met de rechtermuisknop klikt op een taak die wordt uitgevoerd, kunt u via een snelmenu (contextueel) het scanvenster beheren dat wordt geopend. De opties (**Pauze / Hervatten**, **Stoppen** en **Stoppen & sluiten**) zijn dezelfde als deze van de knoppen in het scanvenster.

Als de optie **Gebruiker vragen naar actie** is ingesteld in het venster Eigenschappen, verschijnt bij de detectie van een geinfecteerd bestand, een waarschuwingsvenster waarin u wordt gevraagd de actie te selecteren die moet worden ondernomen op de geinfecteerde bestanden.



Actie selecteren

U kunt de naam van het bestand en de naam van het virus bekijken.

Selecteer een van de volgende acties die moet worden ondernomen op het geinfecteerde bestand:

- **Desinfecteren** - desinfecteert het geinfecteerde bestand.
- **Verwijderen** - verwijdert het geinfecteerde bestand;
- **Naar quarantaine verplaatsen** - verplaatst het geinfecteerde bestand naar de quarantaine;
- **Negeren** - negeert de infectie. Er wordt geen actie ondernomen voor het geinfecteerde bestand.

Als u een map scant en wilt dat de actie voor de geinfecteerde bestanden dezelfde is voor alle bestanden, schakelt u het selectievakje in naast **Op alles toepassen**.

Opmerking

Als de optie **Desinfecteren** niet is ingeschakeld, betekent dit dat het bestand niet kan worden gedesinfecteerd. De beste keuze is het bestand te isoleren in het quarantainegebied en het ons te zenden voor analyse of het te verwijderen.

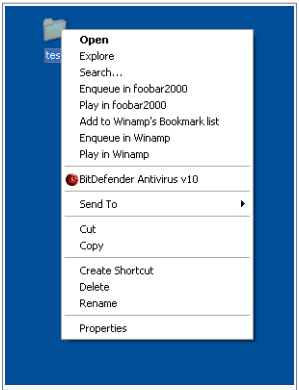
Klik op **OK**.

Opmerking

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

Contextueel scannen

Klik met de rechtermuisknop op het bestand of de map die u wilt scannen en selecteer **BitDefender Antivirus v10**.

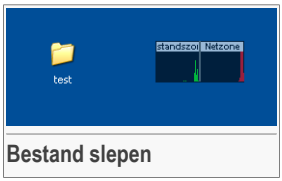


Contextueel scannen

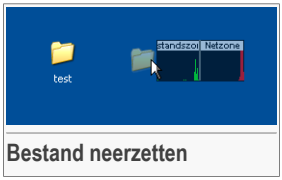
U kunt de scanopties wijzigen en de rapportbestanden weergeven door het venster Eigenschappen van de taak **Contextmenuscan** te openen.

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

Wanneer een geinfecteerd bestand is gedetecteerd, verschijnt een waarschuwingsvenster waarin u wordt gevraagd de actie te selecteren die u voor het geinfecteerde bestand wilt ondernemen.

Bij beide alternatieve scanmethodes (Contextueel scannen en Scannen via slepen & neerzetten), verschijnt het scanvenster.

7.2.5. Rootkit scannen

BitDefender is ontwikkeld om de nieuwste beveiligingsgevaren op te lossen door samen met zijn efficiënte antivirus/antispyware-motors een rootkit-detector te introduceren. BitDefender is nu in staat rootkits te detecteren door te zoeken naar verborgen bestanden, mappen of processen. Bovendien kan dit uw systeem beschermen door de malware die gebruik maakt van rootkits te hernoemen.

Voer de taak **Scannen op rootkits** uit om uw computer te scannen op rootkits. Een scanvenster wordt geopend.

Belangrijk

Wij raden u sterk aan bij het controleren op rootkits, BitDefender zo in te stellen dat er geen acties worden ondernomen voor verborgen bestanden.

Wanneer de scan is voltooid, kunt u de resultaten bekijken. Als er verborgen bestanden zijn gedetecteerd, moet u ze nauwkeurig controleren. De aanwezigheid van verborgen bestanden kan wijzen op mogelijke indringers.

Als u zeker bent dat de gedetecteerde bestanden tot malware behoren, raden wij u aan de actie **Naam bestanden wijzigen** in te stellen en de taak **Scannen op rootkits** uit te voeren. Op deze manier worden de verborgen bestanden geblokkeerd.

Waarschuwing

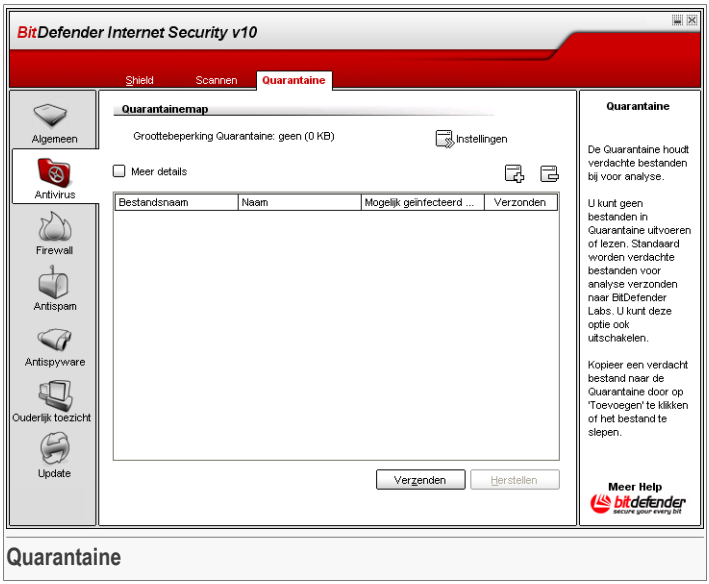
NIET ALLE VERBORGEN ITEMS ZIJN MALWARE! Voordat u de naam van de verborgen bestanden wijzigt, moet u controleren of ze niet tot een geldige toepassing of tot het systeem behoren. Het wijzigen van de naam van dergelijke bestanden, kan uw systeem onbruikbaar maken.

Belangrijk

Als er een hacker op uw systeem is binnengedrongen, is er slechts één veilige manier om deze indringer te verwijderen: het systeem opnieuw installeren.

7.3. Quarantaine

Om dit gedeelte te openen, klikt u op het tabblad **Quarantaine** in de module **Antivirus**.



Quarantaine

BitDefender biedt u de mogelijkheid geinfecteerde 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.

Het onderdeel dat zorgt voor het beheer van de geisoleerde bestanden, is de **Quarantaine**. Deze module werd ontwikkeld met een functie waarmee u geinfecteerde bestanden automatisch naar het BitDefender lab kunt verzenden.

Zoals u wellicht zult merk, bevat het onderdeel **Quarantaine** een lijst van alle bestanden die tot nog toe werden geisoleerd. Elk bestand bevat zijn naam, grootte, isolatiedatum en verzendingsdatum. Klik op **Meer details** als u meer informatie wilt weergeven over de bestanden in quarantaine.

Opmerking

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

Klik op de knop **Toevoegen** om een bestand waarvan u vermoedt dat het geinfecteerd is, toe te voegen aan de quarantaine. In het venster dat wordt geopend kunt u het bestand selecteren op zijn locatie op de schijf. Op deze manier wordt het bestand gekopieerd naar de quarantaine. Als u het bestand wilt verplaatsen naar het quarantainegebied, schakelt u het selectievakje in naast **Verwijderen van originele locatie**. U kunt verdachte bestanden ook sneller toevoegen aan de quarantaine door ze te slepen naar de quarantainelijst.

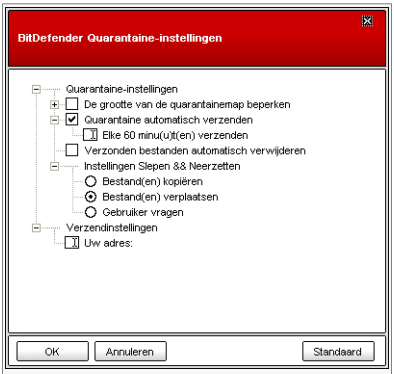
Om een geselecteerd bestand uit de quarantaine te verwijderen, klikt u op de knop **Verwijderen**. Als u een geselecteerd bestand wilt terugzetten op zijn oorspronkelijke locatie, klikt u op **Herstellen**.

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

Belangrijk

Voordat u deze bestanden verzendt, moet u enkele gegevens definiëren. Klik hiervoor op **Instellingen** en vul de velden in het onderdeel **Verzendinstellingen** in zoals hieronder beschreven.

Klik op **Instellingen** om de geavanceerde opties voor het quarantainegebied te openen. Het volgende venster wordt geopend:



Quarantaine-instellingen

De quarantaine-opties zijn gegroepeerd in twee categorieën:

- **Quarantaine-instellingen**
- **Verzendinstellingen**

Opmerking

Klik op het vakje met een "+" om een optie te openen of op het vakje met een "-" om een optie te sluiten.

Quarantaine-instellingen

- **De grootte van de quarantainemap beperken** - houdt de grootte van de quarantaine onder controle. Deze optie is standaard ingeschakeld. De grootte bedraagt 12000 kB. Als u deze waarde wilt wijzigen, geeft u een nieuwe waarde op in het overeenkomende veld. Wanneer u het selectievakje naast **Oude bestanden automatisch verwijderen** selecteert, de quarantaine vol is en u een nieuw bestand toevoegt, worden de oudste bestanden in de quarantaine automatisch verwijderd om ruimte vrij te maken voor het nieuwe bestand.
- **Quarantaine automatisch verzenden** - verzendt de bestanden in quarantaine automatisch naar de BitDefender Labs voor verdere analyse. In het veld **Elke x minuten verzenden**, kunt u de periode tussen twee opeenvolgende verzendingen in minuten instellen.
- **Verzonden bestanden automatisch verwijderen** - verwijdert automatisch de bestanden in quarantaine nadat u ze voor verdere analyse naar de BitDefender labs hebt verzonden.

- **Instellingen slepen & neerzetten** - als u de methode Slepen en neerzetten gebruikt om bestanden toe te voegen aan de quarantaine, kunt u hier de actie opgeven: kopiëren, verplaatsen of gebruiker vragen.

Verzendinstellingen

- **Uw adres** - voer uw e-mailadres als u e-mails wilt ontvangen van onze experts met betrekking tot de verdachte bestanden die u voor analyse hebt verzonden.

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

8. Module Firewall

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

- Firewall-wizard
- Firewall-status
- Verkeerbeveiliging
- Geavanceerde instellingen
- Firewall-activiteit

Opmerking

Meer details over de module **Firewall** kunt u vinden in de beschrijving van "*Module Firewall*" (p. 29).

8.1. Firewall-wizard

Telkens wanneer u zich aanmeldt op een nieuw netwerk, verschijnt een wizard die u zal helpen bij het maken van een nieuw netwerkprofiel voor BitDefender Firewall voor het huidige netwerk. De wizard helpt u ook bij het maken van een reeks standaard firewall-regels die nodig zijn voor uw meest gebruikte toepassingen. Het eindresultaat is een beveiligd systeem met een werkende e-mailclient en webbrowser.

Opmerking

De wizard kan ook op elk ogenblik worden gestart door te klikken op de knop **Profiel opnieuw configureren** in het onderdeel Verkeer.

Belangrijk

Als de wizard niet wordt voltooid, wordt de Firewall uitgeschakeld. De wizard wordt automatisch weergegeven wanneer u probeert de Firewall in te schakelen.

8.1.1. Stap 1/7 – Welkomstvenster

Welkomstvenster

Geef de naam op van het nieuwe netwerkprofiel in het veld **Profielnaam**.

Selecteer **Nieuw profiel maken** om de wizard te volgen en een reeks standaard firewallregels te maken.

Als u **Regels van eerder gemaakt profiel importeren** selecteert, moet u een netwerkprofiel in de lijst kiezen. Het nieuwe profiel importeert alle regels van het geselecteerde profiel. U gaat meteen naar de laatste stap van de wizard, zonder verdere configuratie.

Selecteer **Maak dit een algemeen profiel en pas het op alle nieuwe netwerken toe** om een algemeen profiel te maken of om de bestaande te overschrijven. Het algemene profiel wordt elke keer uitgevoerd zodra BitDefender een nieuw netwerk vindt zonder de firewall wizard te moeten uitvoeren.

Opmerking

Om dit onderdeel uit te schakelen, ga naar Advanced onderdeel en vink de **Gebruik hetzelfde (algemene) profiel voor alle nieuwe netwerken** optie uit.

Klik op **Volgende**.

8.1.2. Stap 2/7 - Geavanceerde firewall-instellingen

Geavanceerde firewall-instellingen

Configureer de geavanceerde firewall-instellingen van het huidige netwerkprofiel.

De volgende opties zijn beschikbaar:

Optie	Beschrijving
Witte lijst toestaan	Laat automatisch uitgaande verbindingspogingen toe van programma's die door BitDefender als rechtmatig zijn gekend. Op basis van deze optie worden, zonder enige tussenkomst van u, in het gedeelte Verkeer regels gemaakt die uitgaande verbindingspogingen van dergelijke programma's toestaan. Wanneer een dergelijke regel wordt gemaakt, verschijnt een pop-upvenster met de melding hiervan. 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.
ICS (Internet Connection Sharing) toestaan op deze computer	Biedt uw computer de mogelijkheid ICS (Internet Connection Sharing) te ondersteunen. Met deze optie wordt ICS niet automatisch ingeschakeld op uw systeem,

Optie	Beschrijving
	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.

8.1.3. Stap 3/7 – Opties voor internetbrowser

Opties voor internetbrowser

BitDefender zal uw standaardbrowser detecteren. Selecteer of het netwerk-/internetverkeer dat door de standaardbrowser wordt gegenereerd, standaard moet worden toegestaan of selecteer een andere browser.

Belangrijk

Als u deze stap overslaat, zullen er geen regels worden gemaakt die van deze keuze afhankelijk zijn. U zult uw eigen regelset moeten maken. Sla deze stap niet over als u niet zeker weet of u zelf de juiste regels wilt maken.

Klik op **Volgende**.

8.1.4. Stap 4/7 – Opties voor e-mailclient

Opties voor e-mailclient

BitDefender zal uw standaard e-mailclient detecteren. Selecteer of het netwerk-/internetverkeer dat door de standaard e-mailclient wordt gegenereerd, standaard moet worden toegestaan of selecteer een andere e-mailclient.

Belangrijk

Als u deze stap overslaat, zullen er geen regels worden gemaakt die van deze keuze afhankelijk zijn. U zult uw eigen regelset moeten maken. Sla deze stap niet over als u niet zeker weet of u zelf de juiste regels wilt maken.

Klik op **Volgende**.

8.1.5. Stap 5/7 – Opties voor proxyserver

Opties voor proxyserver

Als u een proxyserver gebruikt om verbinding met het internet te maken, zal BitDefender deze detecteren. Selecteer of het netwerk-/internetverkeer naar een proxyserver standaard moet worden toegestaan of klik op . . . naast **Ik gebruik een andere server** en voer het IP-adres en de poort van de proxyserver in.

Belangrijk

Als u deze stap overslaat, zullen er geen regels worden gemaakt die van deze keuze afhankelijk zijn. U zult uw eigen regelset moeten maken. Sla deze stap niet over als u niet zeker weet of u zelf de juiste regels wilt maken.

Klik op **Volgende**.

8.1.6. Stap 6/7 – Selectie netwerktype

Selectie netwerktype

U moet het type van uw netwerk-/internetverbinding selecteren. De volgende opties zijn beschikbaar:

Optie	Beschrijving
Een vertrouwd lokaal netwerk	U mag alleen netwerken vertrouwen die worden beveiligd met een firewall en een antivirusprogramma. Raadpleeg uw netwerkbeheerder om dit te controleren. Als u niet weet welk verbindingstype u gebruikt, moet u deze instelling niet kiezen.
Een niet-vertrouwd lokaal netwerk	Selecteer deze instelling als u een gast bent op het netwerk dat niet behoort tot uw thuis- of kantoornetwerk. Als u niet weet welk verbindingstype u gebruikt, moet u deze instelling niet kiezen.
Directe verbinding	Kies deze instelling als u rechtstreeks verbinding maakt met het internet of als u niet weet welk type verbinding u gebruikt. Alle binnenkomende verbindingen zullen worden geweigerd. Hoewel de verbinding van sommige toepassing hierdoor kan worden verbroken, zal de beveiliging worden verscherpt. U kunt regels handmatig toevoegen voor de toepassingen die niet meer werken.

Belangrijk

Als u deze stap overslaat, zullen er geen regels worden gemaakt die van deze keuze afhankelijk zijn. U zult uw eigen regelset moeten maken. Sla deze stap niet over als u niet zeker weet of u zelf de juiste regels wilt maken.

Klik op **Volgende**.

8.1.7. Stap 7/7 – Overzicht

Overzicht

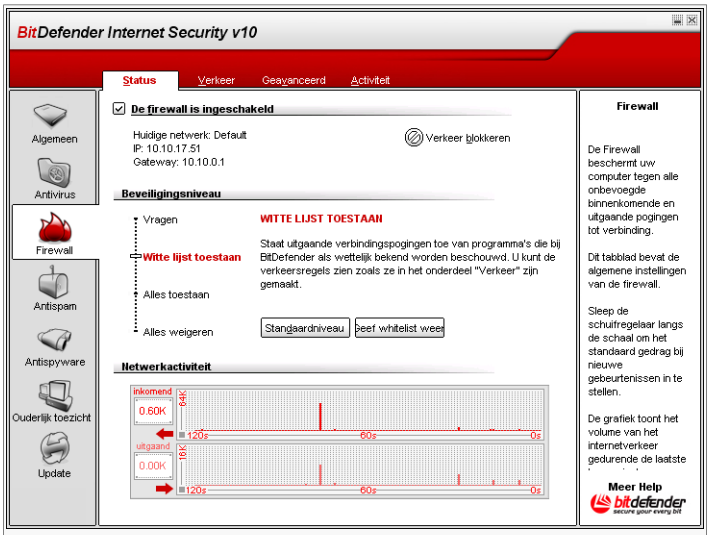
Dit is de laatste stap van de configuratiewizard. U kunt eventuele wijzigingen aanbrengen door terug te keren naar de vorige stappen (klik op **Vorige**).

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

De Firewall-installatiewizard kan ook op elk ogenblik worden gestart door te klikken op de knop **Profiel opnieuw configureren** in het onderdeel Verkeer.

8.2. Firewall-status

Om dit gedeelte te openen, klikt u op het tabblad **Status** in de module **Firewall**.



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**.

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. Beveiligingsniveau

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 4 beveiligingsniveaus:

Beveiligingsniveau	Beschrijving
Alles weigeren	Weigert verkeerpogingen die niet overeenkomen met de huidige regels zonder dit te vragen. Gebruik dit beleid als u al regels hebt ingesteld voor alle programma's en verbindingen die u nodig hebt.
Alles toestaan	Staat verkeerpogingen toe die niet overeenkomen met de huidige regels zonder dit te vragen. Dit beleid wordt sterk afgeraden, maar kan handig zijn voor netwerkbeheerders.
Witte lijst toestaan	Laat alle uitgaande verbindingspogingen toe van programma's die door BitDefender als rechtmatig zijn gekend. U kunt de verkeersregels weergeven zoals ze in het onderdeel Verkeer zijn gemaakt. 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.
Vragen	Vragen of verkeerpogingen die niet overeenkomen met de huidige regels moeten worden toegestaan.

Belangrijk

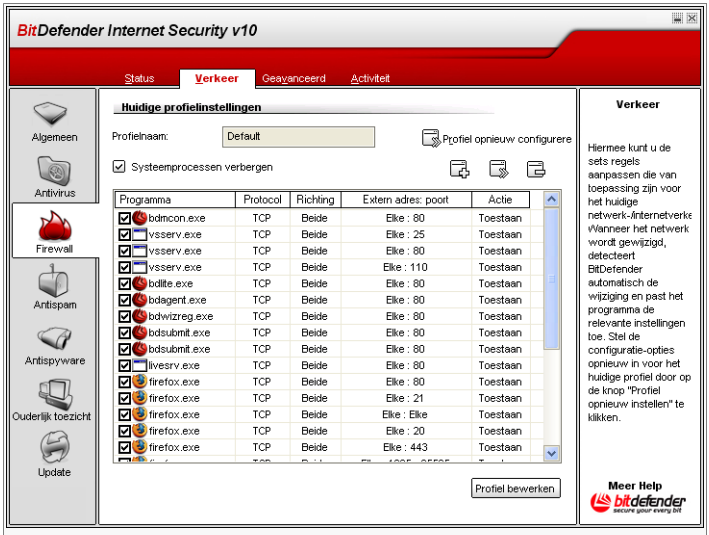
Als de beheerconsole is gesloten en er geen overeenkomst is gevonden in de regelset voor de nieuwe gebeurtenis, is de actie **Weigeren**.

Klik op **Standaardniveau** om het standaardbeleid in te stellen (**Witte lijst toestaan**).

Als u de programma's van de witte lijst wilt zijn, klikt u op **Witte lijst weergeven**.

8.3. Verkeerbeheer

Om dit gedeelte te openen, klikt u op het tabblad **Verkeer** in de module **Firewall**.



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.

Schakel het selectievakje in naast **Systeemprocessen verbergen** als u de regels met betrekking tot het systeem of BitDefender processen wilt verbergen.

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

8.3.1. Regels automatisch toevoegen

De regels worden toegevoegd aan de lijst wanneer u een antwoord geeft op de vragen van BitDefender over een nieuw programma dat probeert toegang te krijgen tot het internet.

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 een verbinding te maken met het internet, het protocol, het IP-adres en de poort die de toepassing probeert te gebruiken voor het maken van de verbinding.

Schakel de optie **Optie onthouden** in, selecteer de gewenste actie in het vervolgkeuzemenu **Actie** en klik op **OK**. Er wordt een regel gemaakt, toegepast en weergegeven in de regeltabel. Op deze manier wordt u niet langer op de hoogte gebracht wanneer het proces wordt herhaald.

U kunt een van de volgende acties selecteren:

Actie	Beschrijving
Toestaan	Alle verkeer van deze toepassing toestaan via het opgegeven protocol.
Weigeren	Alle verkeer van deze toepassing weigeren via het opgegeven protocol.
Alle verkeer van deze toepassing toestaan	Alle verkeer van deze toepassing toestaan via alle IP-protocollen.
Alle verkeer van deze toepassing weigeren	Alle verkeer van deze toepassing blokkeren via alle IP-protocollen.
Alleen deze externe host toestaan	Alle verkeer van deze toepassing toestaan via het opgegeven protocol met de opgegeven externe host.
Alleen deze poort toestaan	Alle verkeer van deze toepassing toestaan via het opgegeven protocol op de opgegeven poort voor elke bestemming.
Alleen deze externe host weigeren	Alle verkeer van deze toepassing blokkeren via het opgegeven protocol met de opgegeven externe host.

Actie	Beschrijving
Alleen deze poort weigeren	Alle verkeer van deze toepassing blokkeren via het opgegeven protocol op de opgegeven poort voor elke bestemming.

Belangrijk

Laat alleen binnenkomende verbindingspogingen toe van IP's of domeinen die u specifiek vertrouwt.

U kunt elke regel die werd onthouden, openen in het onderdeel **Verkeer** om deze fijner in te stellen.

Belangrijk

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.

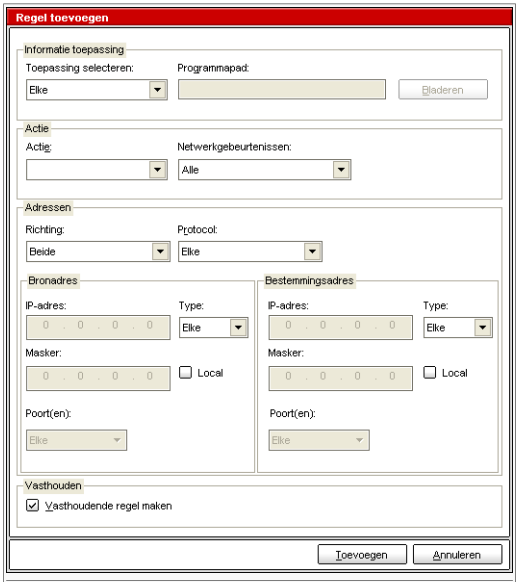
Om een regel te verwijderen, selecteert u de regel en klikt u op de knop **Regel verwijderen** button. Om een regel te wijzigen, selecteert u de regel en klikt u op de knop **Regel bewerken** of dubbelklikt u op de regel. Als u een regel tijdelijk wilt uitschakelen zonder deze te verwijderen, moet u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

Opmerking

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

8.3.2. Regels handmatig toevoegen

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



Parameters selecteren

U kunt de volgende parameters instellen:

- **Toepassing** - selecteer de toepassing voor de regel. U kunt slechts één toepassing kiezen (selecteer **Pad/bestandsnaam** in de vervolgkeuzelijst **Toepassing selecteren**, klik op **Bladeren** en selecteer de toepassingen) of u kunt alle toepassingen kiezen (Selecteer **Alle** in de vervolgkeuzelijst **Toepassing selecteren**).
- **Actie** - selecteer de actie voor de regel en de overeenkomende gebeurtenis(sen).

Actie	Beschrijving
Toestaan	De actie wordt toegestaan.
Weigeren	De actie wordt geweigerd.

- **Adressen** - selecteer de richting van het verkeer en het protocol voor de regel.

  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.

Protocoltype - selecteer een van de volgende protocollen: ICMP, TCP, UDP of een ander protocol.

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.

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.
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.

- **Bronadres** - voer het IP-adres en het masker in of schakel **Lokaal** in als de regel van toepassing is op de lokale computer. 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**.
- **Bestemmingsadres** - voer het IP-adres en het masker in of schakel **Lokaal** in als de bestemming van de regel van toepassing is op de lokale computer. 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**.
- **Vasthouden** - schakel het selectievakje naast **Vathoudende regel maken** in om de regel te bewaren voor toekomstige "sessies". Als deze opties niet zijn

geselecteerd, wordt de regel verwijderd aan het einde van deze sessie (opnieuw opstarten van de computer of update van BitDefender).

Klik op **Toevoegen**.

Belangrijk

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** button. 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 overeenkomstige selectievakje uitschakelen.

Opmerking

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

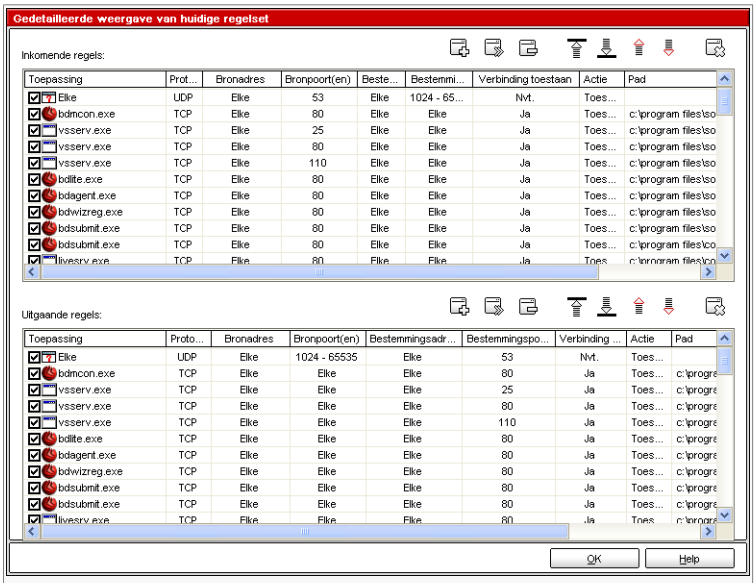
8.3.3. Profielen wijzigen

Voordat u de Firewall-module inschakelt, wordt u gevraagd de wizard te voltooien om een nieuw netwerkprofiel te maken. De wizard helpt u bij het maken van een reeks standaard firewall-regels die nodig zijn voor uw meest gebruikte toepassingen. Klik op **Profiel opnieuw configureren** om de wizard opnieuw uit te voeren en het profiel opnieuw te configureren.

Belangrijk

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

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** button. 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.

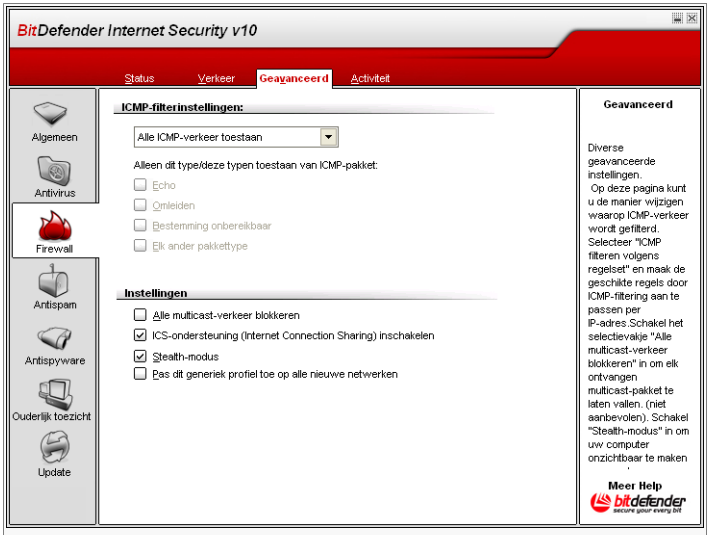
Opmerking

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

Klik op **OK** om terug te keren naar de beheerconsole.

8.4. Geavanceerde instellingen

Om dit gedeelte te openen, klikt u op het tabblad **Geavanceerd** in de module **Firewall**.



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. ICMP-filterinstellingen

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 kunt de volgende opties configureren.

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

- **Huidige regelset toepassen voor ICMP** - is van toepassing op het ICMP-verkeer met de huidige instellingen die zijn opgegeven in het onderdeel Status van de **Firewall**-module.

8.4.2. Instellingen

De volgende geavanceerde firewall-instellingen zijn beschikbaar:

Optie	Beschrijving
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). 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.

Optie	Beschrijving
	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. 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. 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. BitDefender detecteert automatisch poortscans en blokkeert ze.
Gebruik hetzelfde (algemene) profiel voor alle nieuwe netwerken	Voert het algemene profiel uit, indien aanwezig, op alle nieuwe netwerken gevonden door BitDefender. Het heeft geen enkel effect op de netwerken waarvoor u al een netwerk profiel heeft gemaakt. Vink deze optie uit om de firewall wizard te krijgen wanneer BitDefender een nieuw netwerk detecteerd. Het algemene profiel is gemaakt wanneer u de firewall wizard heeft uitgevoerd, met de **Maak dit een algemeen profiel en pas het toe op alle nieuwe netwerken** optie geselecteerd in de eerste stap van deze wizard.

8.5. Verbindingsbeheer

Om dit gedeelte te openen, klikt u op het tabblad **Activiteit** in de module **Firewall**.

Verbindingsbeheer

In dit gedeelte kunt u de huidige netwerk-/internetactiviteit zien (via TCP en UDP), gesorteerd op toepassing. Hier kunt u ook het logboek van BitDefender Firewall openen.

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.

Gebruik de knop **Vernieuwen** om het gedeelte **Activiteit** opnieuw te openen (om de laatste activiteiten van de **Firewall**-module weer te geven).

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 **Logboek weergeven**. Het bestand bevindt zich in de map Common Files van de huidige Windows-gebruiker, onder het pad: `...Softwin\BitDefender Firewall\bdfirewall.txt`.

9. Module Antispam

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

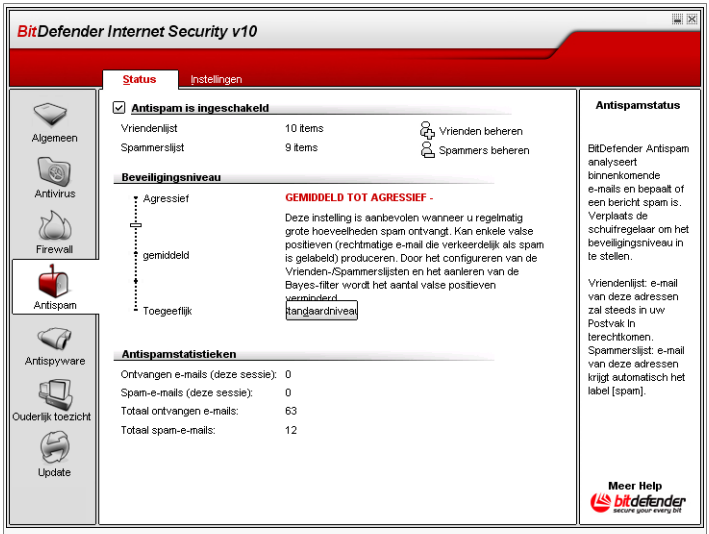
- Antispamstatus
- Antispaminstellingen
- Integratie met Microsoft Outlook / Outlook Express / Windows Mail

Opmerking

Meer details over de module **Antispam** kunt u vinden in de beschrijving van "*Module Antispam*" (p. 30).

9.1. Antispamstatus

Om dit gedeelte te openen, klikt u op het tabblad **Status** in de module **Antispam**.



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:

9.1.1. De lijst met adressen invullen

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

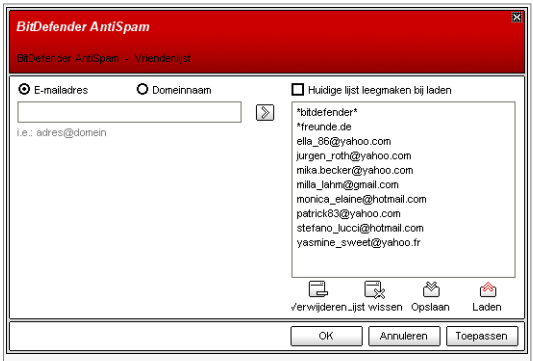
Vriendenlijst

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.

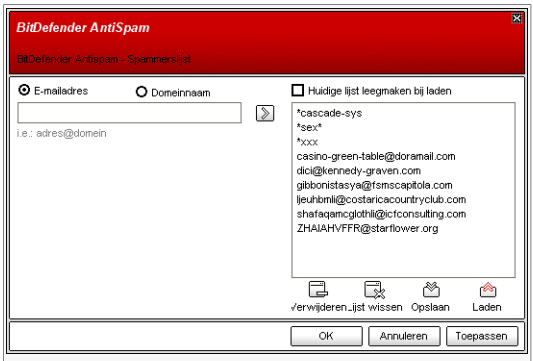
Spammerslijst

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.

9.1.2. 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.

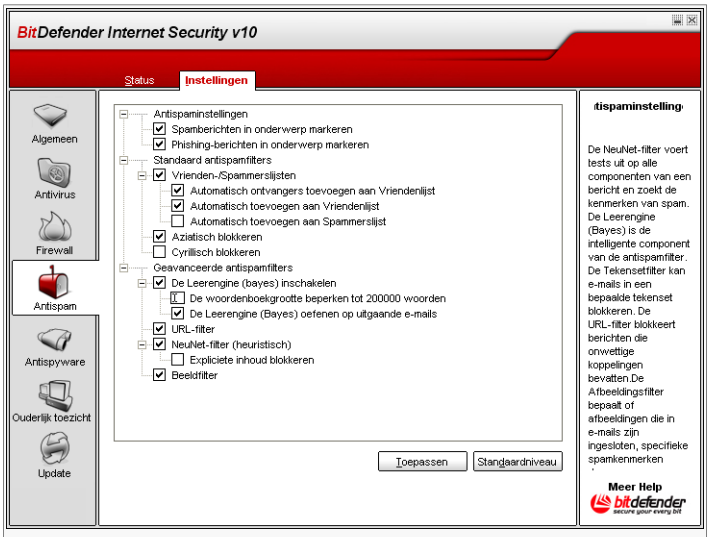
Er zijn 5 tolerantieniveaus:

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.

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

9.2. Antispam-instellingen

Om dit gedeelte te openen, klikt u op het tabblad **Instellingen** in de module **Antispam**.



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.

9.2.1. 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.

9.2.2. 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.

- **Aziatisch blokkeren** - blokkeert berichten die in Aziatische tekensets zijn geschreven.
- **Cyrillisch blokkeren** - blokkeert berichten die in Cyrillische tekensets zijn geschreven.

9.2.3. 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.

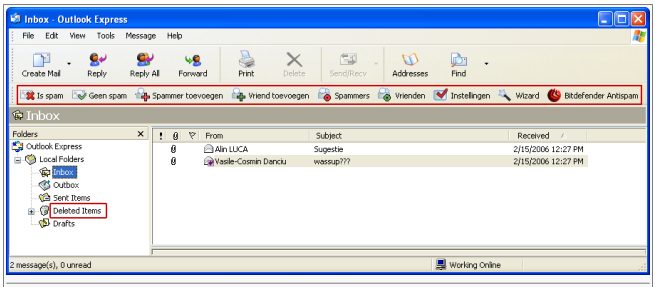
Klik op **Toepassen** om de wijzigingen op te slaan of klik op **Standaardniveau** om de standaardinstellingen te laden.

9.3. Integratie met Microsoft Outlook / Outlook Express / Windows Mail

BitDefender wordt rechtstreeks geintegreerd in Microsoft Outlook / Outlook Express / Windows Mail via een gebruiksvriendelijke en gemakkelijk te gebruiken werkbalk.

9.3.1. Antispam-werkbalk

Bovenaan in het venster van Microsoft Outlook / Outlook Express / Windows Mail kunt u de Antispam-werkbalk zien.



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.

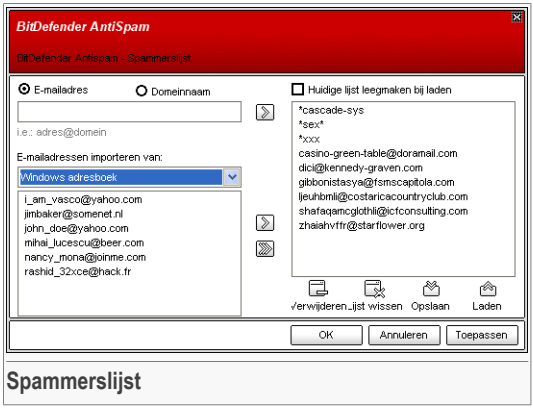
Opmerking

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.

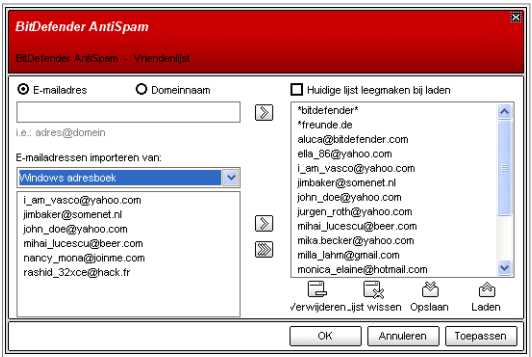
Om de inhoud van de huidige lijst opnieuw in te stellen wanneer u een eerder opgeslagen lijst laadt, selecteert u **Huidige lijst leegmaken bij laden**.

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.

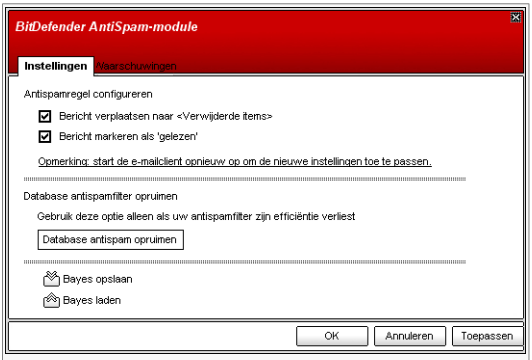
Om de inhoud van de huidige lijst opnieuw in te stellen wanneer u een eerder opgeslagen lijst laadt, selecteert u **Huidige lijst leegmaken bij laden**.

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 **Waarschuwingen** 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 **Waarschuwingen** 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.

9.3.2. Configuratiewizard voor Antispam

Als u Microsoft Outlook / Outlook Express / Windows Mail voor de eerste keer uitvoert wanneer BitDefender is geinstalleerd, 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 antispamfilters te vergroten.

Opmerking

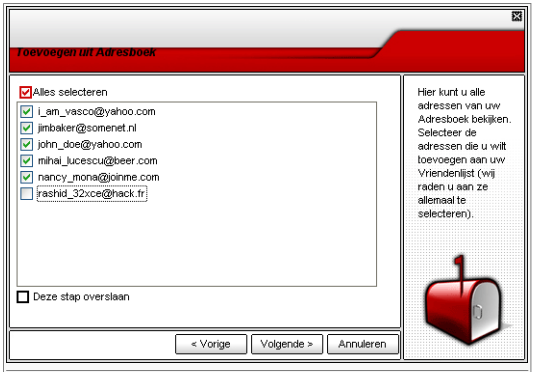
De wizard kan ook op elk ander ogenblik worden gestart door op de knop **Wizard** in de Antispam-werkbalk te klikken.

Stap 1/6 – Welkomstvenster

Welkomstvenster

Klik op **Volgende**.

Stap 2/6 – De Vriendenlijst opstellen

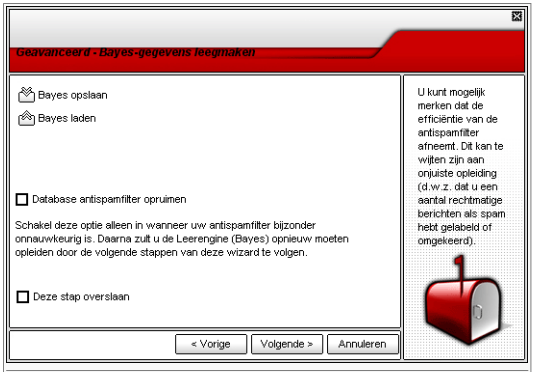


De Vriendenlijst opstellen

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.

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.

Bovenaan in het venster hebt u de keuze uit 2 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

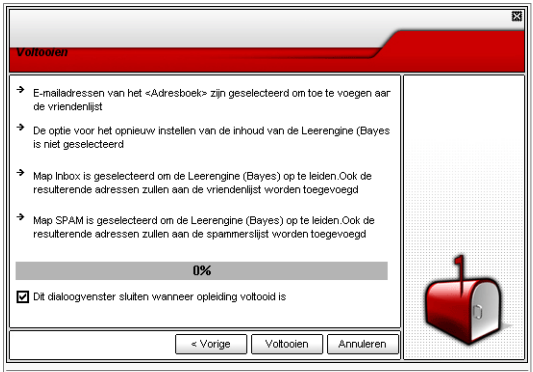
Zorg ervoor dat de map die u selecteert geen enkele rechtmatige e-mail bevat, anders zal de prestatie van de antispam aanzienlijk verminderen.

Bovenaan in het venster hebt u de keuze uit 2 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. Module Antispyware

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

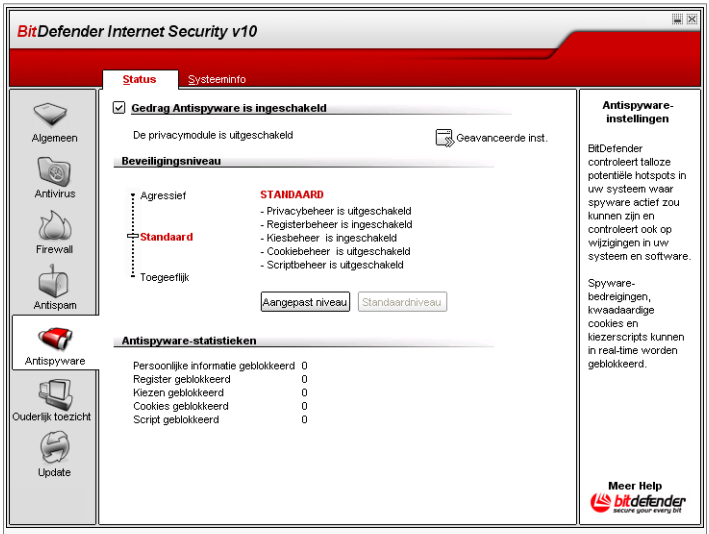
- Antispyware-status
- Geavanceerde instellingen - Privacybeheer
- Geavanceerde instellingen - Registerbeheer
- Geavanceerde instellingen - Kiesbeheer
- Geavanceerde instellingen - Cookiebeheer
- Geavanceerde instellingen - Scriptbeheer
- Systeeminformatie

Opmerking

Meer details over de module **Antispyware** kunt u vinden in de beschrijving van "*Module Antispyware*" (p. 34).

10.1. Antispyware-status

Om dit gedeelte te openen, klikt u op het tabblad **Status** in de module **Antispyware**.



Antispyware-status

In dit gedeelte kunt u het **Gedrag antispyware** configureren en informatie over de activiteiten bekijken.

Belangrijk

Om te verhinderen dat uw computer door spyware wordt geinfecteerd, moet u **Gedrag antispyware** ingeschakeld houden.

Onderaan in de sectie ziet u de **Antispyware-statistieken**.

De **Antispyware**-module beveiligt uw computer tegen spyware via 5 belangrijke beveiligingsbeheeropties:

- Privacybeheer - beschermt uw vertrouwelijke gegevens door al het uitgaande HTTP- en SMTP-verkeer te filteren volgens de regels die u in de sectie Privacy hebt gemaakt.
- Registerbeheer - vraagt uw toestemming wanneer een programma probeert een registergegeven te wijzigen om te worden uitgevoerd bij het opstarten van Windows.
- Kiesbeheer - vraagt uw toestemming wanneer een dialer probeert toegang te krijgen tot een computermodem.

- 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.

10.1.1. Beveiligingsniveau

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:

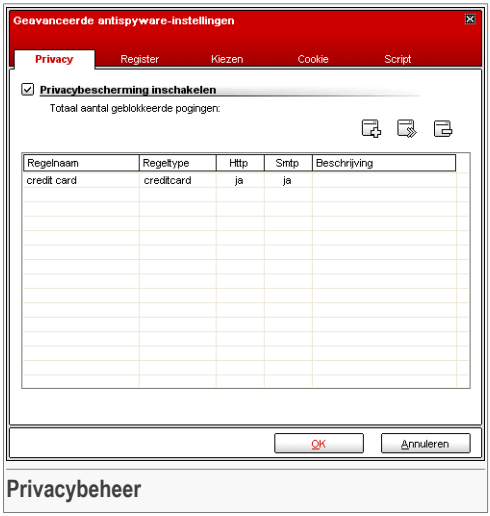
Beveiligingsniveau	Beschrijving
Toegeeflijk	Alleen **Registerbeheer** is ingeschakeld.
Standaard	**Registerbeheer** en **Kiesbeheer** zijn ingeschakeld.
Agressief	**Registerbeheer**, **Kiesbeheer** en **Privacybeheer** zijn ingeschakeld.

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

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

10.2. Geavanceerde instellingen - Privacybeheer

Om dit gedeelte te openen, klikt u op de knop **Geavanceerde instellingen** van de module **Antispyware** in het gedeelte Status.



Privacybeheer

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.

Privacybeheer 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.

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

10.2.1. Configuratiewizard

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.

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.

Klik op **Volgende**.

Stap 3/3 - Regel beschrijven

Regel beschrijven

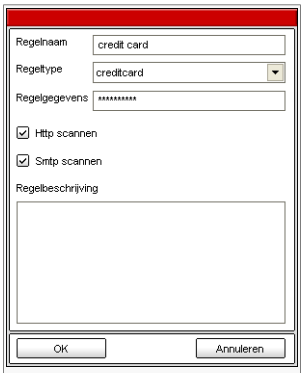
Voer een korte beschrijving in van de regel in het bewerkingsveld.

Klik op **Voltooien**.

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. Het volgende venster wordt geopend:



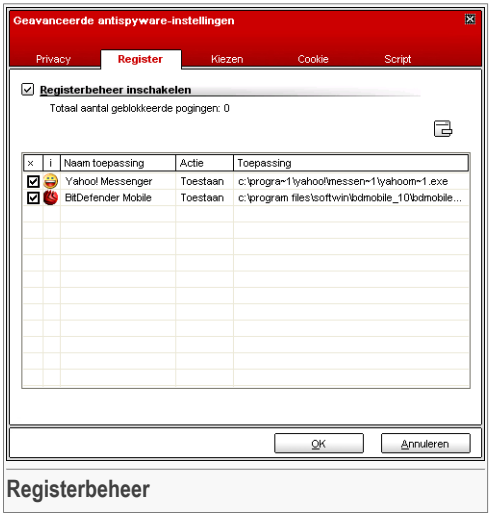
Regel bewerken

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

Om toegang te krijgen tot dit gedeelte, opent u het venster **Geavanceerde Antispyware-instellingen** (ga naar de **Antispyware**-module, het gedeelte Status en klik op **Geavanceerde instellingen**) en klik op het tabblad **Register**.



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, activeer dan het selectievakje: **Dit antwoord onthouden**

Opmerking

Uw antwoorden zullen de basis vormen voor de lijst met regels.

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

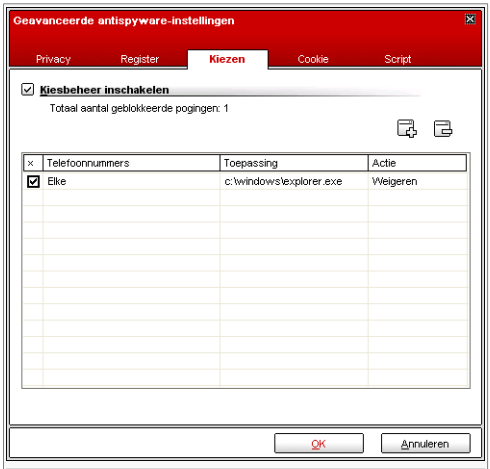
Opmerking

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.

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

10.4. Geavanceerde instellingen - Kiesbeheer

Om toegang te krijgen tot dit gedeelte, opent u het venster **Geavanceerde Antispyware-instellingen** (ga naar de **Antispyware**-module, het gedeelte Status en klik op **Geavanceerde instellingen**) en klik op het tabblad **Kiezen**.



Kiesbeheer

Dialers zijn toepassingen die modems van computers gebruiken om verschillende telefoonnummers te bellen. Deze dialers worden doorgaans gebruikt om toegang te krijgen tot verschillende locaties door dure telefonische betaalnummers te bellen.

Met het **Kiesbeheer** bepaalt u welke verbindingen naar verschillende telefoonnummers u toelaat of blokkeert. Deze functie controleert alle dialers die proberen toegang te krijgen tot een computermodem, waarschuwt de gebruiker onmiddellijk en vraagt hem te beslissen of dergelijke bewerkingen moeten worden geblokkeerd of toegestaan:

Kies-waarschuwing

U ziet de naam van de toepassing en het telefoonnummer.

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 de toepassing hetzelfde telefoonnummer probeert te bellen.

U kunt elke regel die werd onthouden, openen in het onderdeel **Kiezen** om deze fijner in te stellen.

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 2 stappen bestaat.

Stap 1 / 2 - Toepassing en actie selecteren

Toepassing en actie selecteren

U kunt de volgende parameters instellen:

- **Toepassing** - selecteer de toepassing voor de regel. U kunt slechts één toepassing kiezen (klik op **Toepassing selecteren**, daarna op **Bladeren** en selecteer de toepassing) of alle toepassingen (klik op **Elke**).

- **Actie** - selecteer de actie van de regel.

Actie	Beschrijving
Toestaan	De actie wordt toegestaan.
Weigeren	De actie wordt geweigerd.

Klik op **Volgende**.

Stap 2/2 - Telefoonnummers selecteren

Telefoonnummers selecteren

Klik op **Telefoonnummer opgeven**, typ het telefoonnummer waarvoor de regel zal worden toegepast en klik op **Toevoegen**.

Opmerking

U kunt jokertekens gebruiken in uw lijst met uitgesloten telefoonnummers; bijvoorbeeld: nummers die beginnen met 1900* zullen worden geblokkeerd.

Schakel **Elke** in als u wilt dat deze regel op alle telefoonnummers wordt toegepast. Om een telefoonnummer te verwijderen, selecteert u het nummer en klikt u op **Verwijderen**.

Opmerking

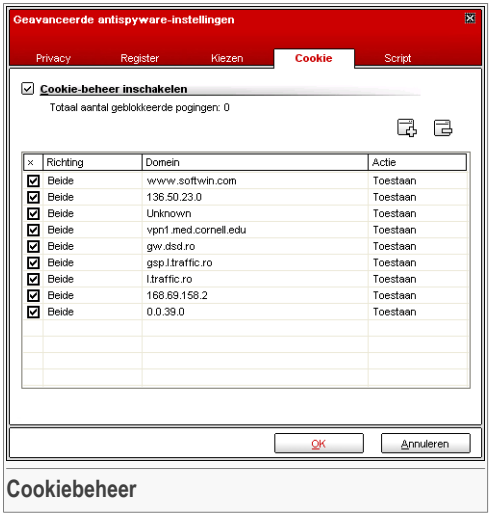
U kunt ook een regel maken die een bepaald programma de toelating geeft alleen bepaalde nummers te bellen (zoals het nummer van uw Internet-provider of uw faxnieuwsdienst).

Klik op **Voltooien**.

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

10.5. Geavanceerde instellingen - Cookiebeheer

Om toegang te krijgen tot dit gedeelte, opent u het venster **Geavanceerde Antispyware-instellingen** (ga naar de **Antispyware**-module, het gedeelte Status en klik op **Geavanceerde instellingen**) en klik op het tabblad **Cookie**.



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.

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.

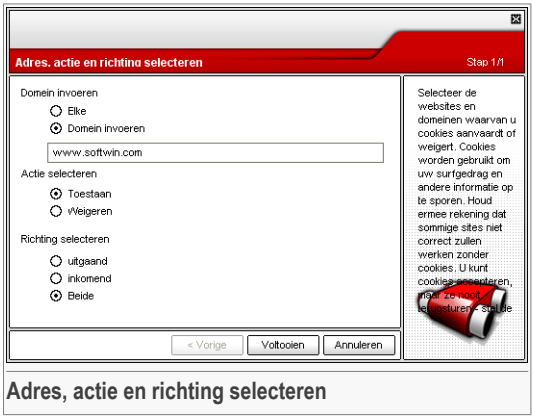
Om een regel te verwijderen, selecteert u de regel en klikt u op de knop **Verwijderen** Om een parameter van een regel te wijzigen, dubbelklikt u op zijn veld en brengt u de gewenste wijziging aan. Als u een regel tijdelijk wilt uitschakelen zonder deze te verwijderen, moet u het overeenkomende selectievakje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

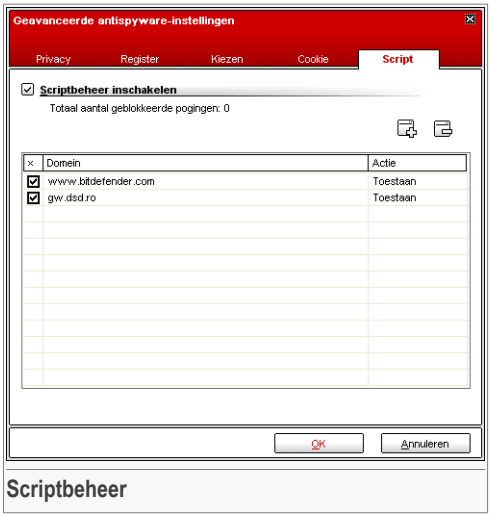
Opmerking

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.

10.6. Geavanceerde instellingen - Scriptbeheer

Om toegang te krijgen tot dit gedeelte, opent u het venster **Geavanceerde Antispyware-instellingen** (ga naar de **Antispyware**-module, het gedeelte Status en klik op **Geavanceerde instellingen**) en klik op het tabblad **Script**.



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.

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.

10.6.1. 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.

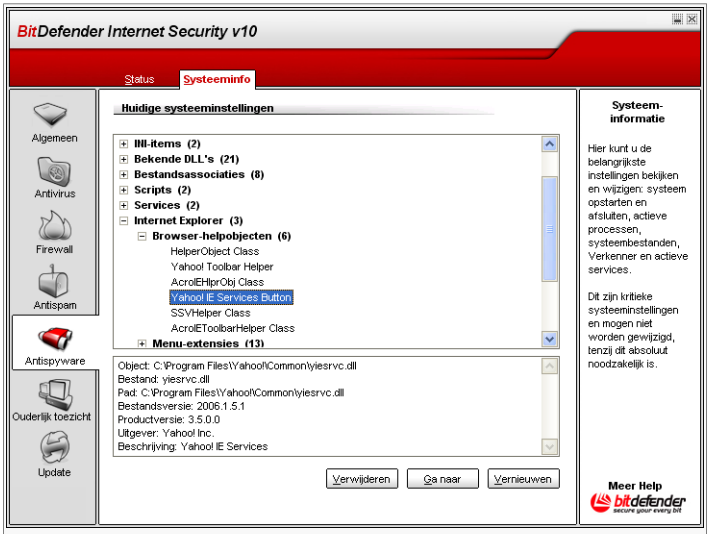
Actie	Beschrijving
Toestaan	De scripts op dat domein zullen worden uitgevoerd.
Weigeren	De scripts op dat domein zullen niet worden uitgevoerd.

Klik op **Voltooien**.

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

10.7. Systeeminformatie

Om dit gedeelte te openen, klikt u op het tabblad **Systeeminfo** in de module **Antispyware**.



Systeeminformatie

Hier kunt u de belangrijkste informatie-instellingen bekijken en wijzigen.

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

11. Module Ouderlijk toezicht

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

- Status Ouderlijk toezicht
- Webbeheer
- Toepassingsbeheer
- Trefwoordfiltering
- Webtijdbeperking

Opmerking

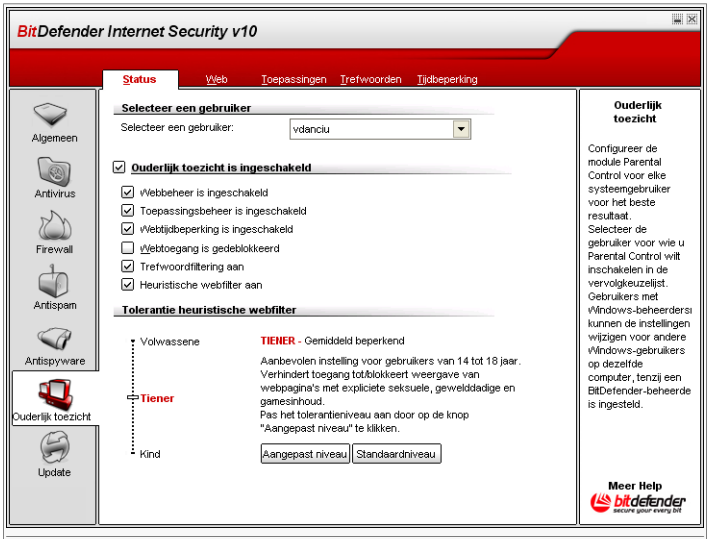
Meer details over de module **Ouderlijk toezicht** kunt u vinden in de beschrijving van "*Module Ouderlijk toezicht*" (p. 34).

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.

11.1. Status Ouderlijk toezicht

Om dit gedeelte te openen, klikt u op het tabblad **Status** in de module **Ouderlijk toezicht**.



Status Ouderlijk toezicht

In dit gedeelte kunt u het algemene beveiligingsniveau van het **Ouderlijk toezicht** configureren voor een geselecteerde gebruiker.

Belangrijk

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

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. Om een wachtwoord in te stellen, gaat u naar de module **Algemeen**, opent u het gedeelte Instellingen en activeert u de optie **Wachtwoordbeveiliging voor productinstellingen inschakelen**.

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.

11.1.1. Tolerantie heuristische webfilter

Sleep de schuifregelaar langs de schaal om het beschermingsniveau in te stellen dat volgens u geschikt is voor de geselecteerde gebruiker.

Er zijn 3 beveiligingsniveaus:

Beveiligingsniveau	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 **Aangepast** om uw eigen filterregels in te stellen. Selecteer in het venster dat wordt weergegeven, de inhoudscategorieën (gokken, hacken, porno, enz.) waarvoor de toegang van de gebruiker tot het internet door BitDefender moet worden geblokkeerd en klik op **OK**.

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

11.2. Webbeheer

Om dit gedeelte te openen, klikt u op het tabblad **Web** in de module **Ouderlijk toezicht**.

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

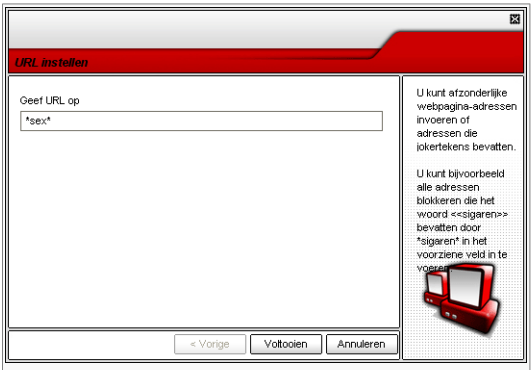
Selecteer **Toegang tot deze pagina's toestaan/Toegang tot deze pagina's blokkeren** om een lijst van toegelaten/geblokkeerde sites weer te geven. Klik op **Uitzonderingen...** om een venster te openen waarin u de aanvullende lijst kunt bekijken.

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.

11.2.1. 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;

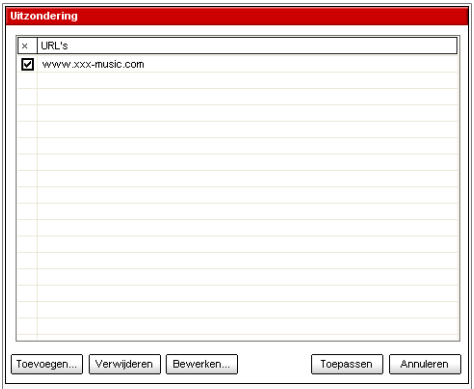
Klik op **Toepassen** om de wijzigingen op te slaan.

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.

11.2.2. 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.

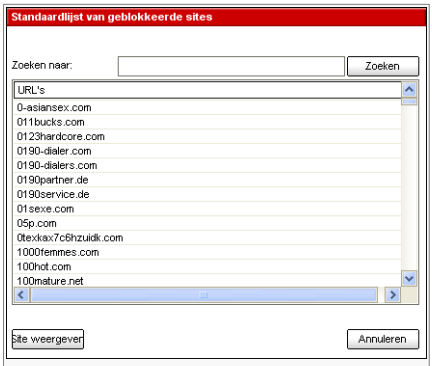
Klik op **Toepassen** om de wijzigingen op te slaan.

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.

11.2.3. 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.

U kunt het aantal geblokkeerde sites bekijken. Om de geblokkeerde pagina's te zien, klikt u op de knop **Standaardlijst**. Het volgende venster wordt geopend:



Zwarte lijst web BitDefender

Selecteer een site en klik op **Site weergeven** om de inhoud weer te geven.

Als u een site wilt blokkeren, kunt u eerst controleren of deze site als in de zwarte lijst is opgenomen. Typ het adres of de eerste letters ervan in het bewerkingsveld en klik op **Zoeken**. Als de tekenreeks overeenkomt met een gegeven, wordt dat gegeven weergegeven.

11.3. Toepassingsbeheer

Om dit gedeelte te openen, klikt u op het tabblad **Toepassingen** in de module **Ouderlijk toezicht**.

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.

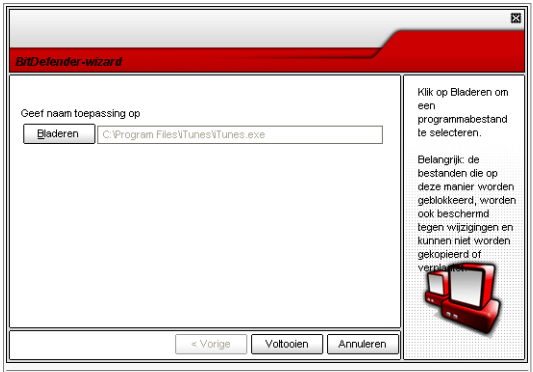
Om deze beveiliging in te schakelen, selecteert u het selectievakje naast **Toepassingsbeheer inschakelen**.

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

11.3.1. Configuratiewizard

De configuratiewizard is een procedure die uit 1 stap bestaat.

Stap 1/1 - Te blokkeren toepassing selecteren



Te blokkeren toepassing selecteren

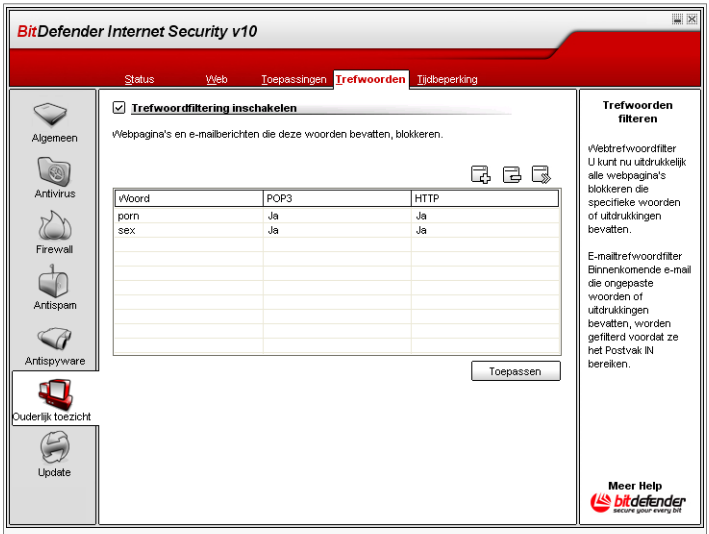
Klik op **Bladeren**, selecteer de toepassing die moet worden geblokkeerd en klik op **Voltooien**.

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.

11.4. Trefwoordfilter

Om dit gedeelte te openen, klikt u op het tabblad **Trefwoorden** in de module **Ouderlijk toezicht**.



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.

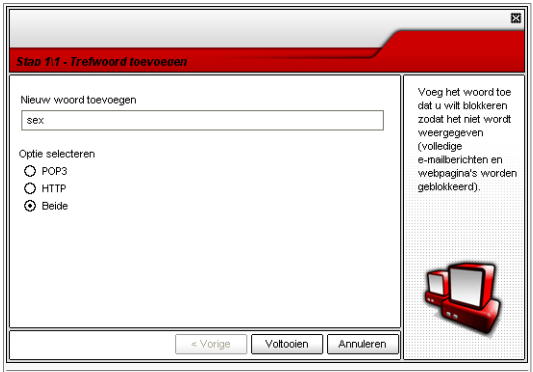
Om deze beveiliging in te schakelen, selecteert u het selectievakje naast **Trefwoordfilter**.

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

11.4.1. 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:

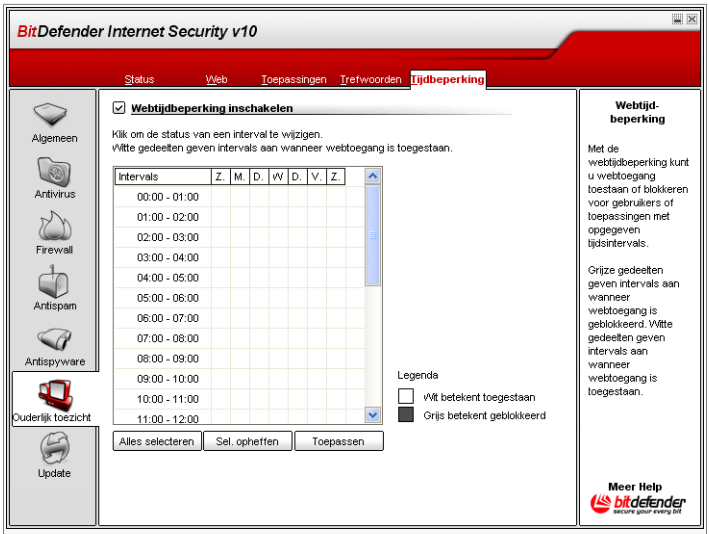
Optie	Beschrijving
POP3	E-mailberichten die het trefwoord bevatten, worden geblokkeerd.
HTTP	Webpagina's die het trefwoord bevatten, worden geblokkeerd.
Beide	E-mailberichten en webpagina's die het trefwoord bevatten, worden geblokkeerd.

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.

11.5. Webtijdbeperking

Om dit gedeelte te openen, klikt u op het tabblad **Tijdbeperking** in de module **Ouderlijk toezicht**.



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 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. Module Update

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

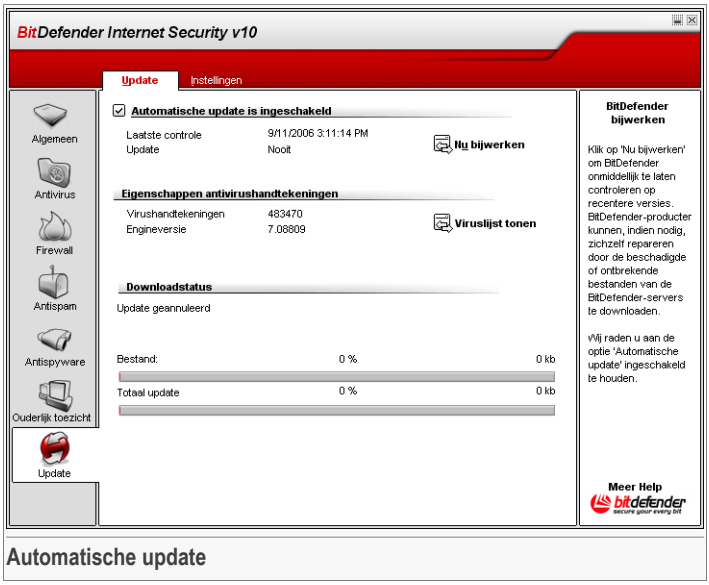
- Automatische update
- Handmatige update
- Update-instellingen

Opmerking

Meer details over de module **Update** kunt u vinden in de beschrijving van "*Module Update*" (p. 34).

12.1. Automatische update

Om dit gedeelte te openen, klikt u op het tabblad **Update** in de module **Update**.



Automatische update

In dit gedeelte kunt u informatie met betrekking tot de updates weergeven en updates uitvoeren.

Belangrijk

Houd **Automatische update** ingeschakeld om tegen de meest recente gevaren te worden beschermd.

Als u via breedband of DSL verbonden bent met het Internet, zal BitDefender deze taak op zich nemen. Het programma controleert 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-opties, gevraagd de update te bevestigen of wordt de update automatisch uitgevoerd.

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 verbonden bent met het Internet via een inbelverbinding, raden wij u aan er een gewoonte van te maken regelmatig een update te maken van BitDefender via de optie Update op aanvraag van de gebruiker.

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. Klik opnieuw op **Viruslijst weergeven** om de lijst te zien. 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.

12.2. Handmatige update

Met deze methode kunt u de laatste virusdefinities installeren. Gebruik de optie Automatische update om een productupgrade van de nieuwste versie te installeren.

Belangrijk

Gebruik de handmatige update als de automatische update niet kan worden uitgevoerd of wanneer de computer niet met het internet is verbonden.

Er zijn 2 manieren om de handmatige update uit te voeren:

- met het bestand `weekly.exe`;
- met `zip-archieven`.

12.2.1. Handmatige update met `weekly.exe`

Het updatepakket `weekly.exe` wordt elke vrijdag uitgegeven en bevat alle updates van virusdefinities en scanengines die tot de uitgiftedatum beschikbaar zijn.

Als u BitDefender wilt bijwerken met het bestand `weekly.exe`, volgt u de onderstaande stappen:

1. Download weekly.exe en sla het bestand lokaal op uw harde schijf op.
2. Zoek het gedownloade bestand en dubbelklik erop om de update-wizard te starten.
3. Klik op **Volgende**.
4. Selecteer **Ik aanvaard de voorwaarden van de Licentieovereenkomst** en klik op **Volgende**.
5. Klik op **Installeren**.
6. Klik op **Voltooien**.

12.2.2. Handmatige update met `zip-archieven`

Er zijn twee zip-archieven op de updateserver, die de updates van de scanengines en virushandtekeningen bevatten: `cumulative.zip` en `daily.zip`.

- `cumulative.zip` wordt elke maandag uitgegeven en bevat alle updates van virusdefinities en scanengines tot de uitgiftedatum.
- `daily.zip` wordt dagelijks uitgegeven en bevat alle updates van virusdefinities en scanengines sinds de laatste cumul en tot de huidige datum.

BitDefender maakt gebruik van een op service gebaseerde architectuur. Hierdoor verschilt de procedure voor het vervangen van virusdefinities afhankelijk van het besturingssysteem.

- Windows 2000, Windows XP.

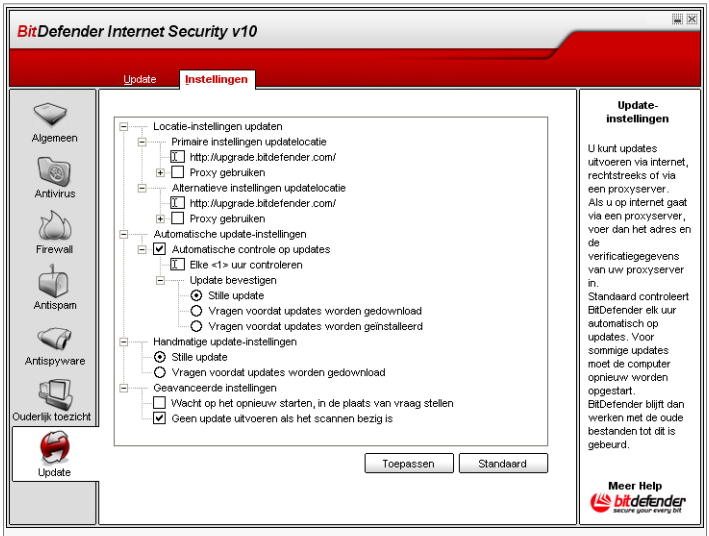
Windows 2000, Windows XP

Uit te voeren stappen:

1. **Download de juiste update.** Als het maandag is, download dan het bestand cumulative.zip en sla het op uw schijf op wanneer u dit wordt gevraagd. Als het een andere dag is, download dan het bestand daily.zip en sla het op uw schijf op. Als dit de eerste keer is dat u een update uitvoert met de handmatige update, moet u beide archieven downloaden.
2. **De antivirusbeveiliging van BitDefender stoppen.**
   - **BitDefender-beheersconsole afsluiten.** Klik met de rechtermuisknop op het pictogram van BitDefender in het systeemvak en selecteer **Afsluiten**.
   - **Services openen.** Klik op **Start**, **Configuratiescherm**, dubbelklik op **Systeembeheer** en klik op **Services**.
   - **De Virus Shield-service van BitDefender stoppen.** Selecteer de service **BitDefender Virus Shield** in de lijst en klik op **Stoppen**.
   - **De Scan Server-service van BitDefender stoppen.** Selecteer de service **BitDefender Scan Server** in de lijst en klik op **Stoppen**.
3. **De archief-inhoud uitpakken.** Begin met `cumulative.zip` wanneer beide update-archieven beschikbaar zijn. Pak de inhoud uit in de map `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` en accepteer het overschrijven van de bestaande bestanden.
4. **De antivirusbeveiliging van BitDefender opnieuw starten.**
   - **De Scan Server-service van BitDefender starten.** Selecteer de service **BitDefender Scan Server** in de lijst en klik op **Start**.
   - **De Virus Shield-service van BitDefender starten.** Selecteer de service **BitDefender Virus Shield** in de lijst en klik op **Start**.
   - **Open de BitDefender-beheerconsole.**

12.3. Update-instellingen

Om dit gedeelte te openen, klikt u op het tabblad **Update** in de module **Instellingen**.



Update-instellingen

De updates kunnen worden uitgevoerd vanaf het netwerk, via het Internet, rechtstreeks of via een proxyserver.

Het venster met de update-instellingen bevat 4 optiecategorieën (**Locatie-instellingen updaten**, **Automatische update-instellingen**, **Handmatige update-instellingen** en **Geavanceerde opties**) die in een uitvouwbaar menu zijn geordend, zoals in 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.

12.3.1. Locatie-instellingen updaten

Voor betrouwbaardere en snellere updates kunt u twee update-locaties configureren: een **Primaire update-locatie** en een **Alternatieve update-locatie**. Voor beide instellingen moet u de volgende opties configureren:

- **Update locatie** -Als u verbonden bent met een lokaal netwerk dat lokaal over virushandtekeningen van BitDefender beschikt, kunt u de updates naar deze locatie verplaatsen. Standaard is dat: http://upgrade.bitdefender.com.

- **Proxy gebruiken** - Selecteer deze optie als het bedrijf een proxyserver gebruikt. U moet de volgende instellingen definiëren:
  - **Proxy stelt xxx in**- typ het IP-adres of de naam van de proxyserver en de poort die door BitDefender wordt gebruikt om een verbinding te maken met de proxyserver.

    Belangrijk

    Syntaxis: `naam:poort` of `ip:poort`.

  - **Proxygebruiker** - typ een gebruikersnaam die door de proxy wordt herkend.

    Belangrijk

    Syntaxis: `domein\gebruiker`.

  - **Proxywachtwoord** - Typ het geldige wachtwoord voor de eerder opgegeven gebruiker.

12.3.2. Opties automatische update

- **Automatische controle op updates** - BitDefender controleert onze servers automatisch op beschikbare updates.
- **Elke x uur controleren** - Stelt in hoe vaak BitDefender controleert op updates. Het standaard tijdinterval is 1 uur.
- **Stille update** - BitDefender downloadt en implementeert automatisch de update.
- **Bevestiging vragen voor downloaden** - Telkens wanneer update beschikbaar is, wordt u een bevestiging gevraagd voor het downloaden.
- **Bevestiging vragen voor installatie** - Telkens wanneer update wordt gedownload, wordt u een bevestiging gevraagd voor de installatie.

Belangrijk

Als u **Bevestiging vragen voor downloaden** of **Bevestiging vragen voor installatie** selecteert en de beheerconsole afsluit, wordt de automatische update niet uitgevoerd.

12.3.3. Handmatige update-instellingen

- **Stille update** - De handmatige update zal automatisch op de achtergrond worden uitgevoerd.

- **Bevestiging vragen voor downloaden** - Telkens wanneer u een handmatige update uitvoert, wordt u om bevestiging gevraagd voordat de updates worden gedownload en geinstalleerd.

Belangrijk

Als u **Bevestiging vragen voor downloaden** selecteert en de beheerconsole afsluit, wordt de handmatige update niet uitgevoerd.

12.3.4. Geavanceerde opties

- **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.

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

Beste praktische toepassingen

13. Beste praktische toepassingen

Het gedeelte **Beste praktische toepassingen** in deze gebruiksaanwijzing bevat de volgende onderwerpen:

- Uw computer die met het internet is verbonden, beschermen
- Uw computer beschermen tegen malware-bedreigingen
- Een scantaak configureren
- De Firewall-module configureren
- Uw computer vrijwaren van spam
- Uw kind beschermen tegen ongepaste inhoud

13.1. Uw computer die met het internet is verbonden, beschermen

Volg deze stappen om uw computer die met het internet is verbonden, te beschermen.

1. **Voltooi de initiële configuratiewizard.** Tijdens het installatieproces verschijnt een wizard. Deze wizard zal u helpen bij het registreren van BitDefender en een BitDefender-account maken om te kunnen genieten van de gratis technische ondersteuning. Deze zal u ook helpen bij het controleren of uw systeem veilig is, door een update en een snelle systeemscan uit te voeren. Daarnaast kunt u ook eenmaal per week een volledige systeemscan plannen.

   Belangrijk

   Als u een reddingsschijf hebt van BitDefender Internet Security v10, kunt u het systeem scannen voordat u BitDefender installeert om zeker te zijn dat er nog geen malware in uw systeem is genesteld.

2. **BitDefender updaten.** Als u de initiële configuratiewizard niet hebt voltooid tijdens de installatieprocedure, voer dan een update op aanvraag van de gebruiker uit (ga naar de module **Update** in het gedeelte Update en klik op **Nu bijwerken**).
3. **Een volledige systeemscan uitvoeren.** Open de **Antivirus**-module, Shield en klik op **Nu scannen**.

   Opmerking

   U kunt een volledige systeemscan ook starten via het gedeelte Scan. Selecteer de taak **Volledige systeemscan** en klik op **Taak uitvoeren**.

4. **Infecties voorkomen.** Houd in het gedeelte **Shield** de real-time-beveiliging ingeschakeld om tegen virussen, spyware en andere malware te zijn beveiligd. Stel het beveiligingsniveau in dat het best overeenkomt met uw behoeften. U kunt dit niveau aanpassen volgens uw voorkeur door te klikken op **Aangepast niveau**.

   Belangrijk

   Programmeer BitDefender om uw systeem minstens een keer per week te scannen door het plannen van een **Volledige systeemscan** in het gedeelte Scan.

5. **Houd BitDefender up-to-date.** In de **Update**-module onder het gedeelte Update moet u de optie **Automatische update** ingeschakeld houden om u tegen de laatste bedreigingen te beschermen.
6. **Internetaanvallen voorkomen.** Configureer de BitDefender-firewall om u tegen internetaanvallen te beschermen.
7. **Spyware-hulpprogramma's blokkeren.** Houd in de **Antispyware**-module onder het gedeelte Status de bescherming op het aanbevolen niveau of hoger. Hierdoor bent u beschermd tegen onrechtmatige programma's die proberen registergegevens te wijzigen en tegen dure dialers. Als u uw vertrouwelijke gegevens wilt beveiligen, schakel dan het Privacybeheer in en maak de gepaste regels.
8. **Spam weghouden.** Als u een e-mailaccount hebt die u wilt beschermen, configureer dan de Antispam-module.
9. **Toegang tot ongepaste inhoud blokkeren.** Als uw kinderen de computer gebruiken, kunt u ze beschermen tegen ongepaste inhoud door de module Ouderlijk toezicht te configureren .

13.2. Uw computer beschermen tegen malware-bedreigingen

Volg deze stappen om uw computer te beschermen tegen virussen, spyware en andere malware.

1. **Voltooi de initiële configuratiewizard.** Tijdens het installatieproces verschijnt een wizard. Deze wizard zal u helpen bij het registreren van BitDefender en een BitDefender-account maken om te kunnen genieten van de gratis technische ondersteuning. Deze zal u ook helpen bij het controleren of uw systeem veilig is, door een update en een snelle systeemscan uit te voeren. Daarnaast kunt u ook eenmaal per week een volledige systeemscan plannen.

Belangrijk

Als u een reddingsschijf hebt van BitDefender, kunt u het systeem scannen voordat u BitDefender installeert om zeker te zijn dat er nog geen malware in uw systeem is genesteld.

2. **BitDefender updaten.** Als u de initiële configuratiewizard niet hebt voltooid tijdens de installatieprocedure, voer dan een update op aanvraag van de gebruiker uit (ga naar de module **Update** in het gedeelte Update en klik op **Nu bijwerken**).
3. **Een volledige systeemscan uitvoeren.** Open de **Antivirus**-module, Shield en klik op **Nu scannen**.

Opmerking

U kunt een volledige systeemscan ook starten via het gedeelte Scan. Selecteer de taak **Volledige systeemscan** en klik op **Taak uitvoeren**.

4. **Infecties voorkomen.** Houd in het gedeelte **Shield** de real-time-beveiliging ingeschakeld om tegen virussen, spyware en andere malware te zijn beveiligd. Stel het beveiligingsniveau in dat het best overeenkomt met uw behoeften. U kunt dit niveau aanpassen volgens uw voorkeur door te klikken op **Aangepast niveau**.

Belangrijk

Programmeer BitDefender Internet Security v10 om uw systeem minstens een keer per week te scannen door het plannen van een **Volledige systeemscan** in het gedeelte Scan.

5. **Houd BitDefender up-to-date.** In de **Update**-module onder het gedeelte Update moet u de optie **Automatische update** ingeschakeld houden om u tegen de laatste bedreigingen te beschermen.
6. **Een volledige systeemscan plannen.** Ga naar het gedeelte **Scan** en programmeer BitDefender om uw systeem minstens eenmaal per week te scannen door het plannen van een **Volledige systeemscan**.

13.3. Een scantaak configureren

Volg deze stappen om een scantaak te maken en te configureren:

1. **Een nieuwe taak maken.** Ga naar het gedeelte Scan en klik op **Nieuwe taak**. Het venster Eigenschappen wordt weergegeven.

Opmerking

U kunt ook een nieuwe taak maken door een bestaande taak te dupliceren. Klik hiervoor met de rechtermuisknop op een taak en selecteer **Dupliceren** in het snelmenu. Dubbelklik op het duplicaat om het venster **Eigenschappen** te openen.

2. **Het scanniveau instellen.** Ga naar het gedeelte **Overzicht** om het scanniveau in te stellen. Als u dat wenst, kunt u de scaninstellingen aanpassen door op **Aangepast** te klikken.
3. **Het scandoel instellen.** Ga naar het gedeelte **Scanpad** en kies de objecten die u wilt scannen.
4. **De taak plannen.** Als de scantaak complex is, is het wellicht beter deze taak voor een later tijdstip te scannen wanneer uw computer inactief is. Dit zal BitDefender helpen een nauwkeurige systeemscan uit te voeren. Ga naar het gedeelte **Planner** om de taak te plannen.

13.4. De Firewall-module configureren

Volg deze stappen om de **Firewall**-module te configureren:

1. **Een netwerkprofiel maken.** Telkens wanneer u zich aanmeldt op een nieuw netwerk, verschijnt een wizard. Voltooi de firewall-wizard om een reeks standaard firewallregels voor het netwerkprofiel te maken.

   Opmerking

   De wizard kan ook op elk ogenblik worden gestart door te klikken op de knop **Profiel opnieuw configureren** in het onderdeel Verkeer.

2. **Beveiligingsniveau instellen.** Ga in het gedeelte **Status** naar de instelling voor het firewall-beleid (**Alles weigeren**, **Alles toestaan**, **Witte lijst toestaan**, **Vragen**).

   Belangrijk

   Wij raden u aan de beveiliging op het niveau **Witte lijst toestaan** te houden. Op deze manier zal BitDefender regels maken voor de meeste gebruikelijke toepassingen zonder dat u hierdoor wordt gehinderd.

3. **Regels maken.** Ga naar het gedeelte **Verkeer** en klik op de knop **Toevoegen** om regels te maken voor uw meest gebruikte toepassingen. U moet de parameters voor de regels opgeven.
4. **Geavanceerde firewall-opties instellen.** Ga naar het gedeelte **Geavanceerd** om de filterregels op te geven voor het ICMP-verkeer en andere firewall-instellingen.

13.5. Uw computer vrijwaren van spam

Volg deze stappen om uw computer te vrijwaren van spam:

1. **Het tolerantieniveau instellen.** Open de **Antispam**-module in het gedeelte Status om het tolerantieniveau in te stellen. De keuze van het geschikte tolerantieniveau zal helpen alle rechtmatige e-mails in uw Postvak IN te plaatsen, ongeacht of u doorgaans veel rechtmatige commerciële e-mails of hoge volumes spam ontvangt.
2. **De configuratiewizard voor antispam voltooien.** Als u Microsoft Outlook of Microsoft Outlook Express / Windows Mail gebruikt, volg dan de configuratiewizard die wordt geopend wanneer u uw e-mailclient voor het eerst opent. U kunt de wizard ook openen vanaf de Antispam-werkbalk.
3. **De Vriendenlijst opstellen.** Open de **Antispam**-module in het gedeelte Status en klik op of op de knop **Vrienden** in de Antispam-werkbalk om de **Vriendenlijst** te openen. Voeg de adressen van de mensen van wie u absoluut e-mail wilt ontvangen toe aan de Vriendenlijst.

   Opmerking

   BitDefender blokkeert geen berichten van de namen in de lijst. Door het toevoegen van vrienden bent u zeker dat rechtmatige berichten worden doorgelaten.

4. **De Leerengine (Bayes) opleiden.** Telkens wanneer u een e-mail ontvangt die u als spam beschouwt, maar BitDefender niet als spam heeft gelabeld, selecteert u de e-mail en klikt u op de knop **Is spam** in de antispam-werkbalk. Toekomstige berichten die voldoen aan hetzelfde patroon, worden gelabeld als SPAM.

   Opmerking

   De **Leerengine** wordt alleen geactiveerd nadat u deze engine op meer dan 60 rechtmatige e-mailberichten hebt geoefend. Hiervoor moet u de configuratiewizard volgen.

5. **Houd BitDefender up-to-date.** In de **Update**-module onder het gedeelte Update moet u de optie **Automatische update** ingeschakeld houden om u tegen de laatste bedreigingen te beschermen.

   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.

6. **De tekensetfilter configureren.** De meeste spamberichten zijn geschreven in Cyrillische en/of Aziatische tekensets. Open de **Antispam**-module in het gedeelte Instellingen en selecteer **Aziatisch blokkeren/Cyrillisch blokkeren** als u alle e-mailberichten wilt weigeren die in deze tekensets zijn geschreven.

Opmerking

U kunt elk van de antispamfilters inschakelen/uitschakelen door het gedeelte Instellingen te selecteren in de **Antispam**-module.

13.6. Uw kind beschermen tegen ongepaste inhoud

Volg deze stappen om uw kind te beschermen tegen ongepaste inhoud:

1. **Een beperkte gebruikersaccount voor Windows maken.** Om te verhinderen dat uw kind toegang krijgt tot de module **Ouderlijk toezicht** of de instellingen kan wijzigen, moeten de rechten van het kind op uw systeem worden beperkt.
2. **Gebruiker selecteren.** De lijst van de mensen die de computer gebruiken, wordt weergegeven in het onderdeel Status. Kies de gebruiker die u wilt beschermen in deze lijst via **Ouderlijk toezicht**.
3. **De algemene beveiliging instellen.** Ga naar het onderdeel **Status** om de beveiligingsbeheeropties in te schakelen voor uw kind. Als u de **heuristische webfilter** hebt ingeschakeld, moet u het geschikte beveiligingsniveau instellen.
4. **Sites blokkeren.** Ga naar het onderdeel **Web** om een lijst te maken van de websites die u wilt verbieden of toestaan voor uw kind. Waar nodig, kunt u uitzonderingen opgeven. U kunt de toegang ook blokkeren tot een lijst van websites die door BitDefender is geleverd. Deze websites hebben mogelijk ongepaste of gevaarlijke inhoud.
5. **Toepassingen blokkeren.** Ga naar het onderdeel **Toepassingen** om de toegang te blokkeren tot toepassingen die u niet door uw kind wilt laten gebruiken.

Opmerking

Als u vindt dat uw kind teveel tijd besteedt aan spelletjes, het gebruik van media of messaging-software of sommige andere toepassingen, kunt u hun toegang tot deze toepassingen blokkeren.

6. **Woorden blokkeren.** Om te voorkomen dat uw kind potentieel gevaarlijke inhoud ziet op het weg of in de e-mail, kunt u de **Trefwoordfilter** gebruiken om specifieke woorden of uitdrukkingen te zoeken die een dergelijke inhoud aangeven. Ga naar het gedeelte **Trefwoord** om de regels te definiëren die de toegang tot websites of

e-mailberichten blokkeren , of de toegang tot beide onderdelen blokkeren als ze specifieke tekenreeksen bevatten.

7. **Webtoegang beheren.** Ga naar het gedeelte **Tijdbeperking** om het tijdschema op te geven volgens de persoon voor wie de webtoegang is toegestaan.
8. **Uw instellingen beveiligen met een wachtwoord.** Open de module **Algemeen** in het gedeelte Instellingen en selecteer **Wachtwoordbeveiliging voor productinstellingen inschakelen**. Alleen gebruikers die het wachtwoord kennen, zullen in staat zijn de instellingen te wijzigen die u op een bepaalde gebruiker hebt opgelegd.

BitDefender reddingsschijf

BitDefender Internet Security v10 wordt geleverd met een opstartbare CD (BitDefender reddingsschijf op basis van LinuxDefender) 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.

LinuxDefender is een door BitDefender herwerkte Knoppix-distributie die de meest recente versie van BitDefender integreert voor een Linux-beveiligingsoplossing in de GNU/Linux Knoppix Live CD, die een onmiddellijke SMTP antivirus/antispambeveiliging biedt en een desktopantivirus levert dat in staat is bestaande harde schijven (inclusief Windows NTFS-partities), externe Samba/Windows-shares of NFS-montagepunten te desinfecteren. Er is ook een op het web gebaseerde configuratie-interface voor BitDefender-oplossingen inbegrepen.

14. Overzicht

Belangrijke functies

- Onmiddellijke e-mailbescherming (antivirus & antispam)
- Antivirusoplossingen voor uw harde schijf
- Ondersteuning voor NTFS write (met Captive project)
- Desinfectie van geinfecteerde bestanden van Windows XP-partities

14.1. Wat is KNOPPIX?

Uittreksel uit http://knopper.net/knoppix:

“ KNOPPIX is a bootable CD with a collection of GNU/Linux (http://www.linux.com/) software, automatic hardware detection, and support for many graphic cards, sound cards, SCSI and USB devices and other peripherals. KNOPPIX can be used as a Linux demo, educational CD, rescue system, or adapted and used as a platform for commercial software product demos. It is not necessary to install anything on a hard disk. ”

14.2. Systeemvereisten

Voordat u LinuxDefender opstart, moet u eerst controleren of uw systeem voldoet aan de volgende vereisten.

Processor type
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.

Memory
De minimale aanvaardbare waarde is 64MB, maar 128MB is aanbevolen voor betere prestaties.

CD-ROM
LinuxDefender wordt uitgevoerd vanaf een cd-rom. Daarom is een cd-rom en een BIOS waarvan kan worden opgestart vereist.

Internet connection
Hoewel LinuxDefender 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.

Graphical resolution

Een grafische resolutie van minstens 800x600 is vereist voor het op het web gebaseerde beheer.

14.3. Bijgeleverde software

De BitDefender reddingsschijf bevat de volgende softwarepakketten.

- BitDefender SMTP Proxy (Antispam & Antivirus)
- BitDefender Remote Admin (op het web gebaseerde configuratie)
- BitDefender Linux Edition (antivirusscanner) + GTK-interface
- BitDefender-documentatie (PDF- & HTML-indeling)
- BitDefender Extra's (grafisch materiaal, brochures)
- Linux-Kernel 2.6
- Captive NTFS write project
- LUFS - Linux Userland File System
- Hulpprogramma's voor gegevensherstel en systeemreparaties, zelfs voor andere besturingssystemen
- Hulpprogramma's voor netwerk- en beveiligingsanalyse voor netwerkbeheerders
- Amanda back-upoplossing
- thttpd
- Etherische analyseprogramma voor netwerkbeheer, IPTraf IP LAN-monitor
- Nessus netwerkbeveiligingsauditor
- Parted, QTParted en partimage, partitieherschaling, opslag- en hersteloplossing
- Adobe Acrobat Reader
- Mozilla Firefox-webbrowser

14.4. BitDefender Linux-beveiligingsoplossingen

De LinuxDefender-cd bevat BitDefender SMTP Proxy Antivirus/Antispam voor Linux, BitDefender Remote Admin (een op het web gebaseerde interface voor het configureren van BitDefender SMTP Proxy) en BitDefender Linux Edition antivirusscanner op aanvraag.

14.4.1. BitDefender SMTP Proxy

BitDefender voor Linux-e-mailservers - SMTP Proxy is een oplossing voor de inspectie van een veilige inhoud, die antivirus- en antispambeveiliging op gatewayniveau biedt door al het e-mailverkeer te scannen op bekende en onbekende malware. Door de unieke eigen technologie is BitDefender voor e-mailservers compatibel met de meeste bestaande e-mailplatforms en heeft het programma het "RedHat Ready"-certificaat.

Deze antivirus- en antispamoplossing scant, desinfecteert en filtert e-mailverkeer voor elke bestaande e-mailserver, ongeacht het platform en het besturingssysteem. BitDefender SMTP Proxy wordt gestart op de opstarttijd en scant al het binnenkomende e-mailverkeer. Om BitDefender SMTP Proxy te configureren, moet u BitDefender Remote Admin gebruiken volgens de onderstaande instructies.

14.4.2. BitDefender Remote Admin

U kunt de BitDefender-services op afstand (nadat u het netwerk hebt geconfigureerd) of lokaal configureren met de volgende stappen:

1. Start Firefox browser en laad BitDefender Remote Admin URL: https://localhost:8139 (of dubbelklik op het pictogram van BitDefender Remote Admin op uw bureaublad)
2. Meld u aan met de gebruikersnaam "bd" en het wachtwoord "bd"
3. Kies "SMTP Proxy" in het menu aan de linkerkant
4. Stel de Real SMTP-server en de luisterende poort in
5. E-maildomeinen aan relay toevoegen
6. Netwerkdomeinen aan relay toevoegen
7. Kies "AntiSpam" in het menu aan de linkerkant om de antispammogelijkheden te configureren.
8. Kies "AntiVirus" om de BitDefender Antivirus-acties te configureren (wat er moet gebeuren wanneer een virus is gevonden, de locatie van de quarantaine)
9. Daarnaast kunt u de "e-mailmeldingen" en de aanmeldingsmogelijkheden configureren ("Logboek")

14.4.3. BitDefender Linux Edition

De antivirusscanner die bij LinuxDefender wordt geleverd, wordt rechtstreeks op het bureaublad geintegreerd. Deze versie beschikt over een GTK+ grafische interface.

Blader door uw harde schijf (of de gemonteerde externe shares), klik met de rechtermuisknop op een bestand of map en selecteer "Scannen met BitDefender". BitDefender Linux Edition zal de geselecteerde items scannen en een statusrapport weergeven. Voor fijngekorrelde opties kunt u de documentatie van BitDefender Linux Edition (in de map BitDefender Documentation of in de handleiding) en het programma **/opt/BitDefender/lib/bdc** raadplegen.

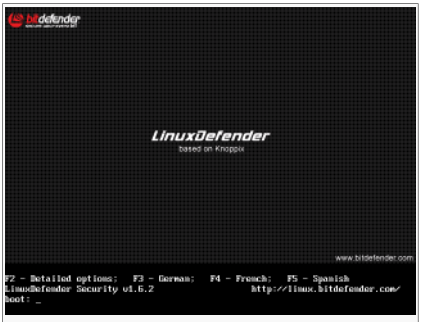
15. LinuxDefender howto

15.1. Start en stop

15.1.1. LinuxDefender 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.

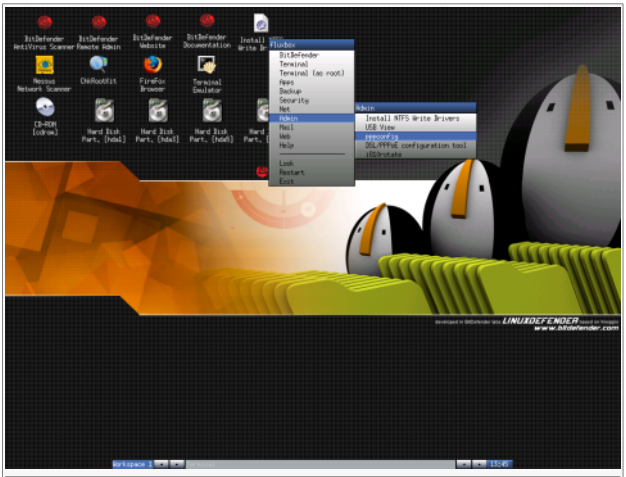
Wacht tot het volgende scherm wordt getoond en volg de instructies op het scherm om LinuxDefender te starten.



Splash-opstartscherm

Druk op `F2` voor gedetailleerde opties. Druk op `F3` voor gedetailleerde opties in het Duits. Druk op `F4` voor gedetailleerde opties in het Frans. Druk op `F5` voor gedetailleerde opties in het Spaans. Om snel op te starten met de standaardopties, drukt u gewoon op `ENTER`.

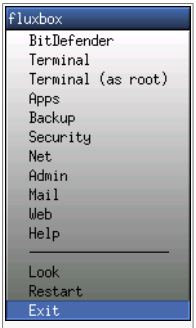
Wanneer het opstartproces is voltooid, ziet u het volgende bureaublad. U kunt nu starten met LinuxDefender.



Het bureaublad

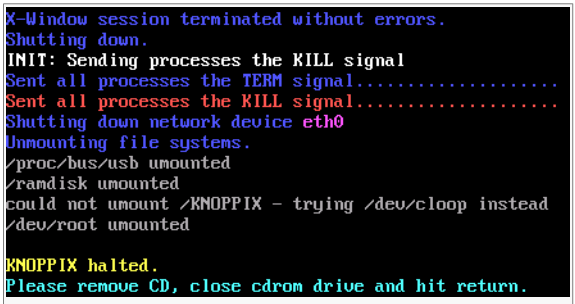
15.1.2. LinuxDefender stoppen

To properly exit from LinuxDefender it's recommended to unmount all mounted partitions using **umount** command or by right-clicking the partition icons on the desktop and select **Unmount**. Then you can safely shut down your computer by selecting **Exit** from the LinuxDefender menu (right-click to open it) or by issuing the **halt** command in a terminal.



Kies "AFSLUITEN"

Wanneer LinuxDefender alle programma's met succes heeft afgesloten, wordt een scherm weergegeven zoals in de volgende afbeelding. U kunt de cd verwijderen om op te starten vanaf uw harde schijf. U kunt nu uw computer veilig uitschakelen of opnieuw opstarten.



Wacht op dit bericht wanneer u afsluit.

15.2. De internetverbinding configureren

Als u in een DHCP-netwerk bent en een ethernet-netwerkkaart hebt, moet de internetverbinding al gedetecteerd en geconfigureerd zijn. Volg de onderstaande stappen voor een handmatige configuratie.

1. Open the LinuxDefender menu (right-click) and select **Terminal** to open a console.
2. Typ **netcardconfig** in de open terminal om het hulpprogramma voor de netwerkconfiguratie te starten.
3. If your network is using DHCP, select **yes** (if you're not sure, ask your network administrator). Otherwise, see below.
4. De netwerkverbinding zou nu automatisch moeten geconfigureerd zijn. Met de opdracht **ifconfig** kunt u uw IP- en netwerkkaartinstellingen zien.
5. If you have a static IP (you're not using DHCP), choose **No** at the DHCP question.
6. Volg de richtlijnen op het scherm. Als u niet zeker bent wat u moet schrijven, neem dan contact op met uw systeem- of netwerkbeheerder voor details.

Als alles goed gaat, kunt u uw internetverbinding testen door `bitdefender.com` te "pingen".

```
$ ping -c 3 bitdefender.com
```

If you're using a dial-up connection, choose **pppconfig** from the LinuxDefender / Admin menu. Then follow the on-screen instruction to set up a PPP Internet connection.

15.3. Update BitDefender

De BitDefender-pakketten voor LinuxDefender maken gebruik van de ramdisk van het systeem voor bestanden die kunnen worden geüpdatet. Hierdoor kunt u alle virushandtekeningen, scanengines of antispamdatabases bijwerken, zelfs als u het systeem uitvoert vanaf media die alleen-lezen zijn, zoals de LinuxDefender-cd.

Make sure that you have a working Internet connection. First open BitDefender Remote Admin and select **Live! Update** from the left menu. Press **Update Now** to check for new updates.

U kunt ook de volgende opdracht in een terminal geven.

```
# /opt/BitDefender/bin/bd  update
```

Alle updateprocessen worden geregistreerd in het standaard logboek van BitDefender. U kunt dit logboek bekijken met de volgende opdracht.

```
# tail  -f /ramdisk/BitDefender/var/log/bd.log
```

If you're using a proxy for outbound connections, configure the Proxy settings in the **Live! Update** menu, **Configuration** tab.

15.4. Virusscan

15.4.1. Hoe kan ik toegang krijgen tot mijn Windows-gegevens?

Ondersteuning NTFS Write

Ondersteuning voor NTFS write is beschikbaar met het Captive NTFS write project. U hebt twee stuurprogrammabestanden van uw Windows-installatie nodig: `ntoskrnl.exe` en `ntfs.sys`. Op dit ogenblik worden alleen Windows XP-stuurprogramma's ondersteund. U kunt ze ook gebruiken om toegang te krijgen tot partities van Windows 2000/NT/2003.

NTFS-stuurprogramma's installeren

Om toegang te krijgen tot de NTFS Windows-partities en er gegevens op te schrijven, moet u eerste de NTFS-stuurprogramma's installeren. Als u niet NTFS, maar FAT gebruikt voor uw Windows-partities, of als u alleen-lezen toegang nodig hebt tot uw

gegevens, kunt u de stations direct monteren en de Windows-stations openen zoals elk Linux-station.

Om ondersteuning toe te voegen voor NTFS-partities, moet u eerst de NTFS-stuurprogramma's installeren vanaf uw harde schijven, externe shares, USB-sticks of via Windows Update. Het is aanbevolen stuurprogramma's te gebruiken van een locatie waarvan u weet dat deze veilig is, omdat de lokale stuurprogramma's van de Windows-host geinfecteerd of beschadigd kunnen zijn.

Double-click **Install NTFS Write Drivers** desktop icon to run the **BitDefender Captive NTFS Installer**. Select the first option if you want to install the drivers from the local hard drive.

If the drivers are in a common location, use **Quick search** to find the drivers.

U kunt ook opgeven waar uw stuurprogramma's te vinden zijn. Of u kunt de stuurprogramma's downloaden van Windows Update SP1.

De stuurprogramma's worden niet geinstalleerd op de harde schijf, maar worden tijdelijk gebruikt door LinuxDefender om toegang te krijgen tot de NTFS-partities van Windows. Als het programma de NTFS-stuurprogramma's installeert, kunt u dubbelklikken op de bureaubladpictogrammen van de NTFS-partities en door de inhoud bladeren. Voor een krachtig bestandsbeheer raden wij u aan Midnight Commander te gebruiken in het menu LinuxDefender (of typ de opdracht **mc** in een console).

15.4.2. Hoe kan ik een antivirusscan uitvoeren?

Browse your folders, right-click a file or directory and select **Send to**. Then choose **BitDefender Scanner**.

Or you can issue the next command as root, from a terminal. The **BitDefender Antivirus Scanner** will start with the selected file or folder as default location to scan.

```
# /opt/BitDefender/bin/bdgtk2 /path/to/scan/
```

Then click **Start Scan**.

If you want to configure the antivirus options, select **Configure Antivirus** tab from the left panel of the program.

15.5. Een direct e-mailfilter-toaster maken

U kunt LinuxDefender gebruiken om een ad hoc e-mailfilteroplossing te maken, zonder enige software te installeren of de e-mailserver te wijzigen. De idee hierachter is een

LinuxDefender-systeem voor uw e-mailserver te plaatsen, zodat BitDefender al het SMTP-verkeer kan scannen op spam en virussen en dit verkeer kan doorsturen naar de echte e-mailserver.

15.5.1. Vereisten

U hebt een pc nodig met een Pentium 3-compatibele CPU of nieuwer, minstens 256MB RAM en een cd/dvd-station waarvan kan worden opgestart. Het LinuxDefender-systeem zal het SMTP-verkeer moeten ontvangen in plaats van de echte e-mailserver. U kunt deze instelling op verschillende manieren definiëren.

1. Wijzig het IP van uw echte e-mailserver en wijs het oude IP toe aan het LinuxDefender-systeem
2. Wijzig uw DNS-records zo, dat het MX-gegeven voor uw domeinen naar het LinuxDefender-systeem wijst
3. Stel uw e-mailclients in om het nieuwe LinuxDefender-systeem als SMTP-server te gebruiken
4. Wijzig uw firewall-instellingen om alle SMTP-verbindingen door te sturen/om te leiden naar het LinuxDefender-systeem in plaats van naar de echte e-mailserver.

LinuxDefender howto zal geen uitleg geven over de bovenstaande zaken. Voor meer informatie kunt u terecht op Linux Networking guides en Netfilterdocumentatie.

15.5.2. De e-mail-toaster

Start uw LinuxDefender-cd op en wacht tot het X-Windows-systeem is geladen en werkt.

To configure BitDefender SMTP Proxy, double-click the **BitDefender Remote Admin** icon from the desktop. The following window will appear. Use `bd` username and `bd` password to log into BitDefender Remote Admin.

Als het aanmelden is gelukt, kunt u BitDefender SMTP Proxy configureren.

Choose **SMTP Proxy** to configure the real mail server you want to protect against spam and viruses.

Select **Email domains** tab to enter all email domains you want to accept email for.

Press the **Add Email Domain** or **Add Bulk Domains** and follow the on-screen instructions to set the relay email domains.

Select **Net domains** tab to enter all networks you want to relay email for.

Press the **Add Net Domain** or **Add Bulk Net Domains** and follow the on-screen instructions to set the relay network domains.

Select **Antivirus** from the left menu, to choose what to do when a virus is found and to configure other antivirus options.

Al het SMTP-verkeer wordt nu gescand en gefilterd door BitDefender. Standaard worden alle berichten met virussen opgeruimd of verwijderd en worden alle spamberichten die door BitDefender zijn gevonden in het Onderwerp gelabeld met het woord `[SPAM]`. Een e-mailkoptekst (`X-BitDefender-Spam: Ja/Nee`) wordt aan alle e-mails toegevoegd om het filteren aan de kant van de klant te vergemakkelijken.

15.6. Een netwerkbeveiligingscontrole uitvoeren

Naast de anti-malware, het gegevensherstel en de e-mailfilter, biedt LinuxDefender ook een reeks hulpprogramma's die een grondige beveiligingscontrole van de host en het netwerk uitvoeren. Ook forensische analyse van geinfecteerde systemen is mogelijk met de beveiligingshulpprogramma's die in LinuxDefender zijn inbegrepen. Lees deze korte handleiding om te leren hoe u een snelle beveiligingscontrole van uw hosts of netwerken kunt starten.

15.6.1. Controle op rootkits

Before start looking for security issues on networked computers, first be sure that the LinuxDefender host is not compromised. You can perform a virus scanning of installed hard-drives, as shown in **Scan for viruses** tutorial or you can scan for Unix rootkits.

First, mount all your hard-disk partition, double-clicking their desktop icons or by using **mount** command in the console. Then double click the **ChkRootKit** icon to check the CD content or launch the **chkrootkit** command in the console, using `-r NEWROOT` de parameter om de nieuw / (hoofd)map van de host op te geven.

```
# chkrootkit -r /dev/hda3
```

If a rootkit is found, chkrootkit will show the finding in **BOLD**, using capital letters.

15.6.2. Nessus - de netwerkscanner

> Nessus is de populairste open-source-kwetsbaarheidsscanner in de wereld die in meer den 75.000 organisaties wereldwijd wordt gebruikt. Een groot aantal van de grootste organisaties ter wereld besparen aanzienlijke kosten door Nessus te gebruiken voor de bedrijfskritieke apparaten en toepassingen van de onderneming.
>
> —*www.nessus.org*

Nessus kan worden gebruikt om uw netwerkcomputers vanop afstand te scannen tegen verschillende zwakke punten. Dit systeem raadt ook bepaalde maatregelen aan

die u kunt nemen om de beveiligingsrisico's te beperken en beveiligingsincidenten te voorkomen.

Double-click the **Nessus Security Scanner** desktop icon or run **startnessus** from a terminal. Wait until the following window is shown. Depending on your hardware resources, it may take up to 10 minutes for Nessus to load, along its more than 5000 plugins containing vulnerability databases. Use `knoppix` user and `knoppix` password to log in.

Click the **Target selection** tab and enter the computer IP or hostnames you want to scan for vulnerabilities. Make sure you customize all scan options according to your nework or system configuration before you start the scan in order to save tons of bandwidth and resources and have a more accurate scan result. Then click **Start the scan**.

Nadat het scanproces is voltooid, toont Nessus de resultaten en de aanbevelingen. U kunt het rapport in verschillende formaten opslaan, inclusief HTML met cirkeldiagrammen en grafieken. Het opgeslagen rapport kan worden weergegeven in uw favoriete browser.

15.7. De gezondheid van de RAM van uw systeem controleren

Wanneer uw systeem een onverwacht gedrag vertoont (blijft hangen of voert af en toe zelf een reset uit), wijst dit doorgaans op een probleem met het geheugen. U kunt de RAM-modules testen met het programma **memtest**, zoals hieronder beschreven.

Start your computer and boot from LinuxDefender CD. Type **memtest** at boot-time and press Enter.

Het Memtest-programma wordt onmiddellijk gestart en voert verschillende tests uit om de RAM-status te controleren. U kunt de tests die moeten worden uitgevoerd en andere Memtest-opties configureren door op `c` te drukken.

Het voltooien van een volledige Memtest kan tot 8 uren duren, afhankelijk van de RAM-capaciteit en snelheid van uw systeem. Wij raden u aan Memtest al zijn tests te laten doen om een volledige controle op RAM-fouten uit te voeren. U kunt de test op elk ogenblik afsluiten door op `ESC` te drukken.

Als u van plan bent nieuwe hardware aan te schaffen (een volledig nieuw systeem of slechts enkele onderdelen), is het aanbevolen LinuxDefender en memtest te gebruiken om te controleren op fouten of compatibiliteitsproblemen.

Hulp vragen

16. Ondersteuning

16.1. Ondersteuningsafdeling

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.

16.2. Online help

16.2.1. 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.

16.3. Contactinformatie

Efficiënte communicatie is de sleutel naar het succes. Gedurende de laatste 10 jaar heeft SOFTWIN 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.

16.3.1. 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>
Carrieremogelijkheden: <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

16.3.2. 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:

Duitsland

Softwin GmbH
Hoofdkantoor West-Europa
Karlsdorferstrasse 56
88069 Tettnang
Duitsland
Tel: +49 7542 9444 44
Fax: +49 7542 9444 99
E-mail: <info@bitdefender.com>

Verkoop: <sales@bitdefender.com>
Web: http://www.bitdefender.com
Technische ondersteuning: <support@bitdefender.com>

UK en Ierland

One Victoria Square
Birmingham
B1 1BD
Tel: +44 845 130 5096
Fax: +44 845 130 5069
E-mail: <info@bitdefender.com>
Verkoop: <sales@bitdefender.com>
Web: http://www.bitdefender.co.uk
Technische ondersteuning <support@bitdefender.com>

Spanje

Constelación Negocial, S.L
C/ Balmes 195, 2a planta, 08006
Barcelona
Technische ondersteuning: <soporte@bitdefender-es.com>
Verkoop: <comercial@bitdefender-es.com>
Telefoon: +34 932189615
Fax: +34 932179128
Website product: http://www.bitdefender-es.com

V.S.A.

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Technische ondersteuning
E-mail: <support@bitdefender.com>
Klantendienst: 954-776-6262
http://www.bitdefender.com

Roemenië

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Boekarest

Technische ondersteuning <suport@bitdefender.ro>
Verkoop: <sales@bitdefender.ro>
Telefoon: +40 21 2330780
Fax: +40 21 2330763
Website product: http://www.bitdefender.ro

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 geinstalleerd 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 beinvloeden. 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 geinfecteerd 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 geinfecteerd.

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 geinfecteerde 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 geinstalleerd, 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 geinstalleerd. 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.