



bitdefender
antivirus **2010**

Handleiding

BitDefender Antivirus 2010 *Handleiding*

Uitgegeven 2009.09.02

Copyright © 2009 BitDefender

Wettelijke bepaling

Alle rechten voorbehouden. Geen enkel deel van dit boek mag worden gereproduceerd of overgedragen in enige vorm of door enig middel, hetzij elektronisch of mechanisch, met inbegrip van het fotokopiëren, opnemen, gegevensopslag of het opslaan in een retrievalssysteem zonder de schriftelijke toestemming van een erkende vertegenwoordiger van BitDefender. Het overnemen van korte citaten in besprekingen kan alleen mogelijk zijn mits het vermelden van de geciteerde bron. De inhoud mag op geen enkele manier worden gewijzigd.

Waarschuwing en ontkenning. Dit product en de bijhorende documentatie zijn auteursrechtelijk beschermd. De informatie in dit document wordt geleverd "zoals hij is", zonder enige garantie. Hoewel alle maatregelen werden genomen bij de voorbereiding van dit document, zullen de auteurs niet aansprakelijk zijn tegenover enige personen of entiteiten met betrekking tot enig verlies of enige schade die direct of indirect is veroorzaakt of vermoedelijk is veroorzaakt door de informatie die in dit document is opgenomen.

Dit boek bevat koppelingen naar websites van derden die niet onder het beheer van BitDefender staan. BitDefender is daarom niet verantwoordelijk voor de inhoud van gekoppelde sites. Als u een website van derden die in dit document is vermeld bezoekt, doet u dit op eigen risico. BitDefender biedt deze koppelingen alleen voor uw informatie en het opnemen van de koppeling impliceert niet dat BitDefender de inhoud van de sites van derden goedkeurt of hiervoor enige verantwoordelijkheid aanvaardt.

Merken. Dit boek kan namen van handelsmerken vermelden. Alle geregistreerde en niet-geregistreerde handelsmerken in dit document zijn de exclusieve eigendom van hun respectievelijke eigenaars en worden met respect erkend.



Inhoudsopgave

Licentieovereenkomst voor eindgebruikers	ix
Voorwoord	xv
1. Conventies die in dit boek worden gebruikt	xv
1.1. Typografische conventies	xv
1.2. Waarschuwing	xvi
2. Boekstructuur	xvi
3. Verzoek om commentaar	xvii
 Installeren en verwijderen	 1
1. Systeemvereisten	2
1.1. Minimale systeemvereisten	2
1.2. Aanbevolen systeemvereisten	2
1.3. Ondersteunde software	2
2. Voorbereiden voor de installatie	4
2.1. Installatie van BitDefender op een NetBook/mini-pc	4
3. BitDefender installeren	5
3.1. Registratiewizard	8
3.1.1. Stap 1 - BitDefender Antivirus 2010 registreren	9
3.1.2. Stap 2 - Een BitDefender-account creëren	11
3.2. Configuratiewizard	13
3.2.1. Stap 1 - Selecteer het gebruiksprofiel	14
3.2.2. Stap 2 - Beschrijf de computer	15
3.2.3. Stap 3 - De gebruikersinterface selecteren	16
3.2.4. Stap 4 - BitDefender netwerk configureren	17
3.2.5. Stap 5 - De uit te voeren taken selecteren	18
3.2.6. Stap 6 - Voltooien	20
4. Upgrade	21
5. BitDefender repareren of verwijderen	22
 Aan de slag	 23
6. Overzicht	24
6.1. BitDefender openen	24
6.2. Weergavemodi gebruikersinterface	24
6.2.1. Beginnersmodus	25
6.2.2. Gemiddelde modus	28
6.2.3. Expert-modus	29
6.3. Systeemvakpictogram	32
6.4. Scan activiteitenbalk	33
6.4.1. Bestanden en mappen scannen	33
6.4.2. De balk Scanactiviteit verbergen/weergeven	34
6.5. BitDefender Handmatig scannen	34
6.6. Spelmodus en Laptop-modus	36

6.6.1. Spelmodus	36
6.6.2. Laptop-modus	37
6.7. Automatische apparaatdetectie	38
7. Problemen herstellen	40
7.1. Wizard Alle problemen herstellen	40
7.2. Het opsporen van problemen configureren	42
8. De basisinstellingen configureren	44
8.1. Instellingen gebruikersinterface	46
8.2. Beveiligingsinstellingen	47
8.3. Algemene instellingen	48
9. Geschiedenis en gebeurtenissen	50
10. Registratie en Mijn account	52
10.1. BitDefender Antivirus 2010 registreren	52
10.2. BitDefender activeren	54
10.3. Licentiesleutels aanschaffen	57
10.4. Uw licentie vernieuwen	57
11. Wizards	58
11.1. Antivirusscanwizard	58
11.1.1. Stap 1/3 - Scannen	58
11.1.2. Stap 2/3 - Acties selecteren	60
11.1.3. Stap 3/3 - Resultaten weergeven	61
11.2. Wizard Aangepaste scan	63
11.2.1. Stap 1/6 - Welkomstvenster	63
11.2.2. Stap 2/6 - Doel selecteren	64
11.2.3. Stap 3/6 - Acties selecteren	65
11.2.4. Stap 4/6 - Extra instellingen	68
11.2.5. Stap 5/6 - Scannen	68
11.2.6. Stap 6/6 - Resultaten weergeven	69
11.3. Wizard Kwetsbaarheidscontrole	70
11.3.1. Stap 1/6 - Te controleren kwetsbaarheden selecteren	71
11.3.2. Stap 2/6 - Op kwetsbaarheden controleren	72
11.3.3. Stap 3/6 - Windows bijwerken	73
11.3.4. Stap 4/6 - Applicaties updaten	74
11.3.5. Stap 5/6 - Zwakke wachtwoorden wijzigen	75
11.3.6. Stap 6/6 - Resultaten weergeven	76
Gemiddelde modus	77
12. Dashboard	78
13. Antivirus	80
13.1. Statusgebied	80
13.1.1. Statustracing configureren	81
13.2. Snelle taken	82
13.2.1. Updaten BitDefender	82
13.2.2. Scannen met BitDefender	83

14. Antiphishing	85
14.1. Statusgebied	85
14.2. Snelle taken	86
14.2.1. Updaten BitDefender	86
14.2.2. Scannen met BitDefender	87
15. Kwetsbaarheid	89
15.1. Statusgebied	90
15.2. Snelle taken	90
16. Netwerk	92
16.1. Snelle taken	92
16.1.1. Het BitDefender netwerk koppelen	93
16.1.2. bezig met toevoegen van computers aan het BitDefender netwerk	93
16.1.3. Het BitDefender netwerk beheren	95
16.1.4. Alle computers scannen	97
16.1.5. Alle computers updaten	98
16.1.6. Alle computers registreren	99
Expert-modus	101
17. Algemeen	102
17.1. Dashboard	102
17.1.1. Algemene status	103
17.1.2. Statistieken	105
17.1.3. Overzicht	106
17.2. Instellingen	106
17.2.1. Algemene instellingen	107
17.2.2. Virusrapportinstellingen	109
17.3. Systeem- informatie	109
18. Antivirus	111
18.1. Real-time beveiliging	111
18.1.1. Het beveiligingsniveau configureren	112
18.1.2. Het beveiligingsniveau aanpassen	113
18.1.3. Instellingen Actief virusbeheer configureren	118
18.1.4. Real time-beveiliging uitschakelen	120
18.1.5. Antiphishing bescherming configureren	121
18.2. Scannen op aanvraag	122
18.2.1. Scantaken	123
18.2.2. Het snelmenu gebruiken	125
18.2.3. Scantaken maken	126
18.2.4. Scantaken configureren	126
18.2.5. Bestanden en mappen scannen	138
18.2.6. Scanlogs weergeven	146
18.3. Uitgesloten objecten van het scannen	147
18.3.1. Paden uitsluiten van het scannen	149
18.3.2. Extensies uitsluiten van het scannen	152
18.4. Quarantainegebied	156
18.4.1. Bestanden in quarantaine beheren	157

18.4.2. Quarantaine-instellingen configureren	158
19. Privacybeheer	160
19.1. Privacybeheer Statistieken	160
19.1.1. Het beveiligingsniveau configureren	162
19.2. Identiteitscontrole	162
19.2.1. Privacyregels maken	165
19.2.2. Uitsluitingen definiëren	170
19.2.3. Regels beheren	172
19.2.4. Regels die door andere beheerders zijn gedefinieerd	173
19.3. Registerbeheer	173
19.4. Cookiebeheer	176
19.4.1. Configuratievenster	178
19.5. Scriptbeheer	179
19.5.1. Configuratievenster	182
20. Kwetsbaarheid	184
20.1. Status	184
20.1.1. Zwakke punten verwijderen	185
20.2. Instellingen	185
21. Instant Messaging (IM) encryptie	187
21.1. Encryptie uitschakelen voor specifieke gebruikers	188
22. Spel- / Laptop-modus	190
22.1. Spelmodus	190
22.1.1. Automatische Spelmodus configureren	192
22.1.2. De spellenlijst beheren	192
22.1.3. Spelmodus instellingen configureren	194
22.1.4. Veranderen van de Spelmodus sneltoets	194
22.2. Laptop-modus	195
22.2.1. Laptop-modus instellingen configureren	196
23. Thuisnetwerk	197
23.1. Het BitDefender netwerk koppelen	197
23.2. bezig met toevoegen van computers aan het BitDefender netwerk	198
23.3. Het BitDefender netwerk beheren	200
24. Update	203
24.1. Automatische update	203
24.1.1. Een update aanvragen	205
24.1.2. Automatische update uitschakelen	205
24.2. Update- instellingen	205
24.2.1. Updatelocaties instellen	206
24.2.2. Automatische update configureren	207
24.2.3. Handmatige update configureren	207
24.2.4. Geavanceerde instellingen configureren	207
24.2.5. Proxy's beheren	208
25. Registratie	211
25.1. BitDefender Antivirus 2010 registreren	212
25.2. Een BitDefender-account creëren	213

Integratie in Windows en software van derden	217
26. Integratie in het contextmenu van Windows.	218
26.1. Scannen met BitDefender	218
27. Integratie in webbrowsers	220
28. Integratie in programma's voor expresberichten	223
Zo werkt het	224
29. Bestanden en mappen scannen	225
29.1. Het contextmenu van Windows gebruiken	225
29.2. Scantaken gebruiken	225
29.3. BitDefender Handmatig scannen gebruiken	228
29.4. De balk voor de scanactiviteit gebruiken	229
30. Een computerscan plannen	230
Problemen oplossen en hulp vragen	232
31. Problemen oplossen	233
31.1. Installatieproblemen	233
31.1.1. Validatiefouten installatie	233
31.1.2. Mislukte installatie	234
31.2. De BitDefender-services reageren niet	236
31.3. Het verwijderen van BitDefender is mislukt	237
32. Supportcentrum	238
BitDefender reddingsschijf	241
33. Overzicht	242
33.1. Systeemvereisten	242
33.2. Bijgeleverde software	243
34. De BitDefender reddingsschijf gebruiken	246
34.1. BitDefender reddingsschijf starten	246
34.2. BitDefender reddingsschijf stoppen	247
34.3. Hoe kan ik een antivirusscan uitvoeren?	248
34.4. Hoe configureer ik de internetverbinding?	249
34.5. Hoe kan ik BitDefender updaten?	250
34.5.1. Hoe kan ik BitDefender updaten over een proxy?	251
34.6. Hoe kan ik mijn gegevens opslaan?	252
34.7. Hoe moet ik de consolemodus gebruiken?	254
Woordenlijst	255

Licentieovereenkomst voor eindgebruikers

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

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

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

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

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

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

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

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

DESKTOPGEBRUIKERSLICENTIE Deze licentie is van toepassing op de BitDefender-software die kan worden geïnstalleerd op één computer die geen

netwerkdiensten biedt. Elke primaire gebruiker mag deze software installeren op één computer en mag één extra kopie maken op een ander apparaat voor back-updoeleinden. Het toegelaten aantal primaire gebruikers is het aantal gebruikers van de licentie.

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

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

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

AUTEURSRECHT. Alle rechten, aanspraken op en belangen in BitDefender en alle auteursrechten in en voor BitDefender (met inbegrip van, maar niet beperkt tot elke afbeelding, foto, logo, animatie, video, audio, muziek, tekst en "applet" die in BitDefender zijn geïntegreerd), de begeleidende gedrukte materialen en elke kopie van BitDefender zijn eigendom van BITDEFENDER. BitDefender is beschermd door wetten op auteursrecht en internationale verdragsvoorwaarden. U moet BitDefender daarom behandelen als elk ander materiaal dat auteursrechtelijk is beschermd. U mag geen kopieën maken van het gedrukte materiaal, dat bij BitDefender wordt geleverd. U moet alle auteursrechtelijke bepalingen produceren en overnemen in hun oorspronkelijke vorm voor alle gemaakte kopieën, ongeacht de media of de vorm waarin BitDefender bestaat. U mag een licentie van BitDefender niet verhuren, verkopen, leasen of delen. U mag geen reverse engineering toepassen, niet opnieuw compileren, demonteren, afgeleide werken maken, vertalen, of enige poging ondernemen om de broncode van BitDefender te onthullen.

BEPERKTE GARANTIE. BITDEFENDER garandeert dat de media waarop BitDefender wordt verdeeld, vrij is van defecten gedurende een periode van dertig dagen vanaf de datum waarop BitDefender aan u werd geleverd. Uw enig verhaal bij een inbreuk op deze garantie, is dat BITDEFENDER, volgens eigen voorkeur, de defecte media

vervangt na ontvangst van de beschadigde media, of het bedrag, dat u voor BitDefender hebt betaald, terugbetaalt. BITDEFENDER biedt geen garantie dat BitDefender ongestoord of vrij van fouten zal werken, of dat de fouten zullen worden gecorrigeerd. BITDEFENDER garandeert niet dat BitDefender zal voldoen aan uw behoeften.

TENZIJ UITDRUKKELIJK UITEENGEZET IN DEZE OVEREENKOMST, WIJST BITDEFENDER ALLE ANDERE GARANTIES, UITDRUKKELIJK OF IMPLICIET, AF MET BETREKKING TOT DE PRODUCTEN, VERBETERINGEN, ONDERHOUD OF ONDERSTEUNING DIE HIERMEE VERWANT IS OF ALLE ANDERE MATERIALEN (TASTBAAR OF NIET-TASTBAAR) DIE DOOR BITDEFENDER ZIJN GELEVERD. BITDEFENDER WIJST HIERBIJ UITDRUKKELIJK ALLE IMPLICIETE GARANTIES EN BEPALINGEN AF, MET INBEGRIIP 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, UITSCHAKELLEN OF VERWIJDEREN VAN DERGELIJKE SOFTWARE VAN DERDEN, SPYWARE, ADWARE, COOKIES, E-MAILS, DOCUMENTEN, ADVERTENTIES OF GELIJKSOORTIGE ZAKEN, ONGEACHT OF ZE VOORTVLOEIEN UIT STATUTEN, WETTEN, HANDELSWIJZEN, DOUANE EN PRAKTIJKEN, OF HANDELSGEBRUIK.

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

SOMMIGE LANDEN STAAN DE BEPERKING OF UITSLUITING VAN AANSPRAKELIJKHEID VOOR INCIDENTELE OF GEVOLGSCHADE NIET TOE. DE BOVENSTAANDE BEPERKING OF UITSLUITING ZAL BIJGEVOLG MOGELIJK NIET VAN TOEPASSING ZIJN OP U.

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

BELANGRIJKE MEDEDELING AAN GEBRUIKERS. DEZE SOFTWARE IS NIET FOUT-TOLERANT EN IS NIET ONTWIKKELD OF BEDOELD VOOR GEBRUIK IN EEN GEVAARLIJKE OMGEVING DIE EEN STORINGSVEILIGE PRESTATIE OF WERKING VEREIST. DEZE SOFTWARE IS NIET VOOR GEBRUIK BIJ DE BEDIENING VAN VliegTuiGNavigatie, Nucleaire Faciliteiten of Communicatiesystemen, Wapensystemen, Directe of Indirecte Life-Supportsystemen, Luchtverkeersleiding, of elke toepassing of installatie waar defecten de dood, ernstige lichamelijke letsels of materiële schade kunnen veroorzaken.

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

TECHNOLOGIE VOOR HET VERZAMELEN VAN GEGEVENS - BitDefender brengt u op de hoogte van het feit dat zij in bepaalde programma of producten, de technologie voor de verzameling van gegevens kan gebruiken om technische informatie te verzamelen (inclusief verdachte bestanden) met het oog op de verbetering van de producten, om verwante services te leveren, ze aan te passen, het niet-gelicenseerd of illegaal gebruik van het product te voorkomen of schade die voortvloeit uit de malwareproducten te verhinderen. U accepteert dat BitDefender dergelijke informatie mag gebruiken als onderdeel van de diensten die zijn geleverd met betrekking tot het product en om de malwareprogramma's die op uw computer worden uitgevoerd, te voorkomen en te stoppen.

U erkent en accepteert dat BitDefender updates of aanvullingen aan het programma of product kan leveren, die automatisch naar uw computer worden gedownload.

Door deze overeenkomst te accepteren, stemt u ermee in de uitvoerbare bestanden te uploaden zodat ze door de BitDefender-servers kunnen worden gescand. Met het oog op het afsluiten van contracten en het gebruik van het programma, zult u BitDefender mogelijk bepaalde persoonlijke gegevens moeten leveren. BitDefender verklaart dat zij uw persoonlijke gegevens zal behandelen in overeenkomst met de huidige toepasselijke wetgeving en zoals vastgesteld in haar privacybeleid.

GEGEVENSVERZAMELING. De toegang tot de website door de gebruiker en de verwerving van producten en diensten, en het gebruik van hulpprogramma's of inhoud via de website impliceert de verwerking van persoonlijke gegevens. De naleving van de wetgeving die de verwerking bepaalt van persoonlijke gegevens en ISS-services (information society services) en elektronische handel, is van het grootste belang voor BitDefender. Om toegang te krijgen tot producten, services, inhoud of hulpprogramma's, zult u soms bepaalde persoonlijke details moeten opgeven. BitDefender garandeert dat dergelijke gegevens vertrouwelijk zullen worden behandeld en in overeenstemming met de wetgeving die de bescherming bepaalt van persoonlijke informatie en van ISS-services (information society services) en elektronische handel.

BitDefender leeft de toepasselijke wetgeving op gegevensbeveiliging toe en heeft de administratieve en technische stappen ondernomen die nodig zijn om de veiligheid van de persoonlijke gegevens die ze verzamelt, te garanderen.

U verklaart dat alle gegevens die u levert, echt en nauwkeurig zijn en dat u BitDefender op de hoogte zult brengen van alle wijzigingen aan deze gegevens. U hebt het recht bezwaar aan te tekenen tegen de verwerking van de gegevens die niet essentieel zijn voor de uitvoering van de overeenkomst en tegen het gebruik van de gegevens voor een ander doel dan het onderhoud van de contractuele relatie.

In het geval u details van derden opgeeft, zal BitDefender niet aansprakelijk zijn voor het naleven van de principes van informatie en toestemming, en zult u daarom degene zijn die garandeert dat u de eigenaar van de gegevens eerder hebt geïnformeerd en de toestemming van hem/haar hebt gekregen met betrekking tot het meedelen van dergelijke gegevens.

BitDefender en haar filialen en partners zullen alleen marketinginformatie via e-mail of andere elektronische middelen verzenden naar die gebruikers die hun uitdrukkelijke toestemming hebben gegeven om communicatie te ontvangen met betrekking tot producten, services of nieuwsbrieven van BitDefender.

Het privacybeleid van BitDefender garandeert u het recht tot het openen, rechtzetten, verwijderen en weigeren van de verwerking van de gegevens door BitDefender via e-mail op de hoogte te brengen op: juridic@bitdefender.com.

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.

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

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

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

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

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

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

Voorwoord

Deze handleiding is bedoeld voor alle gebruikers die voor **BitDefender Antivirus 2010** 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.

In dit boek vindt u een beschrijving van BitDefender Antivirus 2010 en wordt u begeleid doorheen het installatieproces met uitleg over de configuraties. U zult leren hoe u BitDefender Antivirus 2010 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 volgende tabel voorgesteld.

Weergave	Beschrijving
<code>sample syntax</code>	Syntaxisvoorbeelden zijn gedrukt in enklspatietekens.
http://www.bitdefender.com	De URL-koppeling wijst naar een externe locatie op http- of ftp-servers.
sales@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 enklspatielettertype.
option	Alle productopties worden afgedrukt met harde tekens.
<code>sample code listing</code>	De codeweergave wordt gedrukt met enklspatietekens.

1.2. Waarschuwing.

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. Boekstructuur

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

Installeren en verwijderen. Stapsgewijze instructies voor het installeren van BitDefender op een pc. 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.

Aan de slag. Bevat alle informatie die u nodig hebt om te starten met BitDefender. U maakt kennis met de BitDefender-interface en leert hoe u problemen kunt oplossen, basisinstellingen kunt configureren en uw product kunt registreren.

Gemiddelde modus. Stelt de interface van de Gemiddelde modus van BitDefender voor.

Expert-modus. Een gedetailleerde voorstelling van de interface van de Expert-modus van BitDefender. U wordt geleerd hoe u alle BitDefender-modules te configureren en gebruiken om uw computer op een efficiënte manier te beveiligen tegen elk type malwarebedreiging (virussen, spyware, rootkits, enz.).

Integratie in Windows en software van derden. Biedt uitleg over het gebruik van de BitDefender-opties in het snelmenu van Windows en de BitDefender-werkbalken die in ondersteunde programma's van derden zijn geïntegreerd.

Zo werkt het. Biedt procedures waarmee u snel de meest gebruikelijke taken in BitDefender kunt uitvoeren.

Problemen oplossen en hulp vragen. Informatie over waar u om hulp kunt vragen indien er zich onverwachte problemen voordoen.

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

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

3. Verzoek om commentaar

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

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



Belangrijk

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

Installeren en verwijderen

1. Systeemvereisten

U kunt BitDefender Antivirus 2010 uitsluitend installeren op computers met de volgende besturingssystemen:

- Windows XP (32/64-bits) met Service Pack 2 of hoger
- Windows Vista (32/64-bits) of Windows Vista met Service Pack 1 of hoger
- Windows 7 (32/64-bits)

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



Opmerking

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

1.1. Minimale systeemvereisten

- 450 MB beschikbare harde schijfruimte
- Processor 800 MHz
- RAM-geheugen:
 - ▶ 512 MB voor Windows XP
 - ▶ 1 GB voor Windows Vista en Windows 7
- Internet Explorer 6.0
- .NET Framework 1.1 (ook aanwezig in het installatiepakket)

1.2. Aanbevolen systeemvereisten

- 600 MB beschikbare harde schijfruimte
- Intel CORE Duo (1,66 GHz) of equivalente processor
- RAM-geheugen:
 - ▶ 1 GB voor Windows XP en Windows 7
 - ▶ 1,5 GB voor Windows Vista
- Internet Explorer 7 (of hoger)
- .NET Framework 1.1 (ook aanwezig in het installatiepakket)

1.3. Ondersteunde software

Antiphishing-beveiliging is alleen aanwezig voor:

- Internet Explorer 6.0 of hoger
- Mozilla Firefox 2.5
- Yahoo Messenger 8.5
- Yahoo Messenger 8.5

Instant Messaging (IM) encryptie is alleen aanwezig voor:

- Yahoo Messenger 8.5
- Yahoo Messenger 8.5

2. Voorbereiden voor de installatie

Voordat u BitDefender Antivirus 2010 installeert, moet u deze voorbereidingen voltooien om ervoor te zorgen dat de installatie vlot verloopt:

- Controleer of de computer waarop u BitDefender wilt installeren, voldoet aan de minimale systeemvereisten. Als de computer niet voldoet aan alle minimale systeemvereisten, wordt BitDefender niet geïnstalleerd. Als het programma als is geïnstalleerd, zal het niet goed werken en zal het systeem vertragen en instabiel worden. Raadpleeg "*Systeemvereisten*" (p. 2) voor een complete lijst van systeemvereisten.
- Meld u aan bij de computer met een beheerdersaccount.
- Verwijder alle andere beveiligingssoftware van de computer. Als u twee beveiligingsprogramma's tegelijk uitvoert, kan dit hun werking beïnvloeden en ernstige problemen met het systeem veroorzaken. Windows Defender wordt standaard uitgeschakeld voordat de installatie wordt gestart.

2.1. Installatie van BitDefender op een NetBook/mini-pc

BitDefender Antivirus 2010 kan voor thuisgebruik op 3 pc's worden geïnstalleerd, of op alle pc's die zich op hetzelfde postadres bevinden. Indien u beschikt over een mini-pc, kunt u voor de installatie van uw BitDefender software kiezen uit twee mogelijkheden:

- Plaats de dvd van BitDefender 2010 in het dvd-station van een pc. Kies na het opstarten van het installatievenster, het BitDefender programma dat u hebt aangeschaft. Kies de optie **Kopiëren naar een USB-disk** om de installatiebestanden van BitDefender te kopiëren naar een USB-apparaat, dat u vervolgens op een mini-pc kunt aansluiten. Kopieer de installatiebestanden op uw mini-pc, installeer uw BitDefender programma en activeer de software met behulp van de licentiesleutel die u bij de aankoop van het programma hebt ontvangen.
- Download het BitDefender 2010 programma dat u hebt aangeschaft rechtstreeks vanuit de internetbrowser van uw mini-pc, door op de website <http://www.bitdefender.com/nl> de rubriek Downloads aan te klikken. Installeer vervolgens het BitDefender programma van uw keuze en activeer de software met behulp van de licentiesleutel die u bij de aankoop van het programma hebt ontvangen.

3. BitDefender installeren

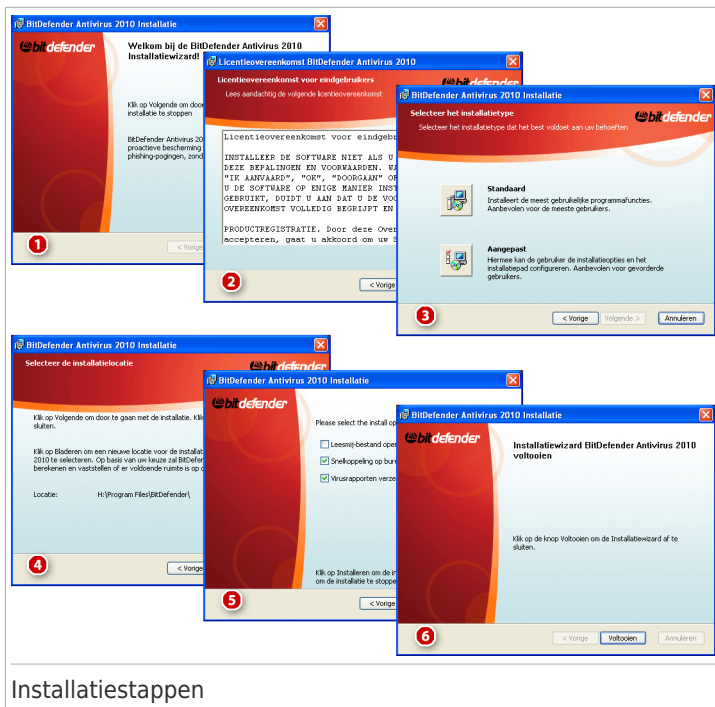
U kunt BitDefender installeren vanaf de BitDefender-installatie-cd, met het installatiebestand dat u van de BitDefender-website hebt gedownload naar uw computer, of van andere gemachtigde websites (bijvoorbeeld de website van een BitDefender-partner of een online winkel). U kunt het installatiebestand downloaden van de BitDefender-website op het volgende adres: <http://www.bitdefender.com/site/Downloads/>.

- Om BitDefender vanaf de cd te installeren, plaatst u de cd in het station. Na enkele ogenblikken zou een welkomstscherf moeten worden weergegeven. Volg de instructies om de installatie te starten.

Als het welkomstscherf niet verschijnt, volgt u dit pad `Products\Antivirus\install\en\` vanaf de hoofdmap van de cd en dubbelklikt u op `runsetup.exe`.

- Om BitDefender te installeren met het installatiebestand dat op uw computer is gedownload, zoekt u het bestand en dubbelklikt u erop.

Het installatieprogramma zal uw systeem eerst controleren om de installatie te valideren. Als de installatie is gevalideerd, verschijnt de installatiewizard. De volgende afbeelding toont de stappen van de installatiewizard.



Volg deze stappen om BitDefender Antivirus 2010 te installeren:

1. Klik op **Volgende**. U kunt de installatie op elk ogenblik annuleren door op **Annuleren** te klikken.

BitDefender Antivirus 2010 waarschuwt u als er andere antivirusproducten op uw computer zijn geïnstalleerd. Klik op **Verwijderen** om het overeenkomende product te verwijderen. Klik op **Volgende** als u wilt doorgaan zonder de gedetecteerde producten te verwijderen.



Waarschuwing

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

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



Belangrijk

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

3. Selecteer het type installatie dat moet worden uitgevoerd.
 - **Standaard** - om het programma onmiddellijk te installeren, gebruikt u de standaard installatie-opties. Ga verder naar Stap 6 als u deze optie kiest.
 - **Aangepast** - om de installatie-opties te configureren en het programma vervolgens te installeren. Met deze optie kunt u het installatiepad wijzigen.
4. BitDefender Antivirus 2010 wordt standaard geïnstalleerd onder C:\Program Files\BitDefender\BitDefender 2010. Als u het installatiepad wilt wijzigen, klikt u op **Bladeren** en selecteert u de map waarin u BitDefender wilt installeren. Klik op **Volgende**.
5. Selecteer de opties met betrekking tot het installatieproces. Sommige worden standaard geselecteerd:
 - **Leesmij-bestand openen** - hiermee opent u het leesmij-bestand aan het einde van de installatie.
 - **Een snelkoppeling op het bureaublad plaatsen** - hiermee plaatst u een snelkoppeling naar BitDefender Antivirus 2010 op het bureaublad aan het einde van de installatie.
 - **Cd uitwerpen nadat installatie is voltooid** - om de cd uit te werpen aan het einde van de installatie. Deze optie verschijnt wanneer u het product vanaf de cd installeert.
 - **DNS cache uitschakelen** - hiermee kunt u het in cache opslaan van de DNS (Domain Name System) uitschakelen. De DNS Client Service kan gebruikt worden door kwaadwillende applicaties om informatie te versturen over uw netwerk zonder uw toestemming.
 - **Windows Defender uitschakelen** - hiermee wordt Windows Defender uitgeschakeld. Deze optie verschijnt alleen in Windows Vista.Klik op **Installeren** om de installatie van het product te starten. Als .NET Framework 1.1 nog niet is geïnstalleerd, zal BitDefender dit eerst installeren.
6. Wacht tot de installatie volledig wordt uitgevoerd en klik dan **Voltooien**. U wordt gevraagd uw systeem opnieuw te starten zodat het installatieprogramma de installatie kan voltooien. Wij adviseren dit zo snel mogelijk te doen.



Belangrijk

Na de installatie en het opnieuw starten van de computer verschijnen een **registratiewizard** en een **configuratiewizard**. Voltooi deze wizards om BitDefender

Antivirus 2010 te registreren en te configureren en een BitDefender-account te creëren.

Als u de standaardinstellingen voor het installatiepad hebt geaccepteerd, ziet u in Program Files een nieuwe map, genaamd BitDefender, met daarin de submap BitDefender 2010.

3.1. Registratiewizard

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

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



Opmerking

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

3.1.1. Stap 1 - BitDefender Antivirus 2010 registreren

BitDefender Antivirus 2010

Registratiewizard

BitDefender-registratie

☒ Ik wil BitDefender evalueren

☐ Ik wil BitDefender registreren met een licentiesleutel

Licentiesleutel invoeren:

Licentiesleutel:

[Nu kopen...](#)

Geen licentiesleutel? Nu kopen.

Beweeg de muis over het venster om meer informatie te lezen over elke optie die in de BitDefender-gebruikersinterface w gebied wordt de helptekst weergegeven.

[Annuleren](#) [Volgende](#)

Registratie

BitDefender Antivirus 2010 begint met een 30-dagen proefperiode. Om door te gaan met de evaluatie van het product, selecteert u **Ik wil BitDefender evalueren** en klikt u op **Volgende**.

BitDefender Antivirus 2010 registreren:

1. Selecteer **ik wil bitdefender met een ander sleutel registreren**.
2. Typ de licentiesleutel in het bewerkingsveld.



Opmerking

U kan uw licentiesleutel vinden:

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

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

3. Klik op **Nu registreren**.

4. Klik op **Volgende**.

Als een geldige BitDefender-licentiesleutel op uw systeem wordt gedetecteerd, kunt u doorgaan met het gebruik van deze sleutel door op **Volgende** te klikken.

3.1.2. Stap 2 - Een BitDefender-account creëren

BitDefender Antivirus 2010

Registratiewizard

BitDefender-account

Activeer uw BitDefender nu om toegang tot technische dienst te krijgen. Ook geeft <http://myaccount.Bitdefender.com> u verloren licentiesleutel terug te krijgen en krijgt u het voordeel uit de speciale BitDefender aanbiedingen.

☒ Een nieuwe account maken

E-mailadres:

Wachtwoord: Wachtwoord herhalen:

E-mailopties:

☐ Aanmelden (eerder gemaakte account)

☐ Later registreren (de registratie is verplicht)

Voer hier het e-mailadres in dat uw BitDefender-account zal identificeren. Het e-mailadres zal de gebruikersnaam van de...

Account creëren

Als u momenteel geen BitDefender-account wilt maken, selecteert u **Later registreren** en klikt u op **Voltoeien**. Ga anders te werk zoals past bij uw situatie:

- “Ik heb geen BitDefender-account” (p. 12)
- “Ik heb al een BitDefender-account” (p. 12)



Belangrijk

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

Ik heb geen BitDefender-account

Volg deze stappen om een BitDefender-account te maken:

1. Selecteer **Een nieuwe account maken**.
2. Typ de vereiste informatie in de overeenkomende velden. De gegevens die u hier opgeeft blijven vertrouwelijk.
 - **E-mailadres** - voer uw e-mailadres in.
 - **Wachtwoord** - voer een wachtwoord voor uw BitDefender-account in. Het wachtwoord moet 6 tot 16 tekens lang zijn.
 - **Wachtwoord opnieuw** - voer het zojuist gebruikte wachtwoord opnieuw in.



Opmerking

Zodra de account is geactiveerd, kunt u het bijgeleverde e-mailadres en het wachtwoord gebruiken om u aan te melden bij uw account op <http://myaccount.bitdefender.com>.

3. Optioneel kan BitDefender u informeren over speciale aanbiedingen via het e-mailadres van uw account. Selecteer een van de beschikbare opties in het menu:
 - **Mij alle berichten sturen**
 - **Mij alleen berichten met betrekking tot producten sturen**
 - **Stuur mij geen berichten**
4. Klik op **Maken**.
5. Klik op **Voltooien** om de wizard te voltooien.
6. **Uw account activeren**. Voordat u uw account kunt gebruiken, moet u deze activeren. Controleer uw e-mail en volg de instructies in de e-mail die u van de registratieservice van BitDefender hebt ontvangen.

Ik heb al een BitDefender-account

BitDefender detecteert automatisch of u al een BitDefender-account hebt geregistreerd op uw computer. Geef in dit geval het wachtwoord van uw account op en klik op **Aanmelden**. Klik op **Voltooien** om de wizard te voltooien.

Als u al een actieve account hebt, maar BitDefender deze niet detecteert, moet u deze stappen volgen om het product voor die account te registreren:

1. Selecteer **Aanmelden (eerder gemaakte account)**.
2. Voer het e-mailadres en wachtwoord van uw account in de overeenkomende velden in.



Opmerking

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

3. Optioneel kan BitDefender u informeren over speciale aanbiedingen via het e-mailadres van uw account. Selecteer een van de beschikbare opties in het menu:
 - **Mij alle berichten sturen**
 - **Mij alleen berichten met betrekking tot producten sturen**
 - **Stuur mij geen berichten**
4. Klik op **Aanmelden**.
5. Klik op **Voltooien** om de wizard te voltooien.

3.2. Configuratiewizard

Na het voltooien van de registratiewizard verschijnt een configuratiewizard. Deze wizard helpt u bij het configureren van de hoofdinstellingen van BitDefender en van de gebruikersinterface zodat ze beter geschikt zijn voor uw vereisten. Aan het einde van de wizard kunt u de productbestanden en malwarehandtekeningen bijwerken en de systeembestanden en toepassingen scannen om zeker te zijn dat ze niet geïnficeerd.

De wizard bestaat uit enkele eenvoudige stappen. Het aantal stappen is afhankelijk van de keuzen die u maakt. Alle stappen worden hier voorgesteld, maar er wordt een melding weergegeven wanneer uw keuze hun aantal beïnvloeden.

U bent niet verplicht deze wizard te voltooien. Wij raden u echter aan dit toch te doen om tijd te besparen en zeker te zijn dat uw systeem veilig is, zelfs voordat BitDefender Antivirus 2010 is geïnstalleerd. Als u de wizard niet wilt volgen, klik dan op **Annuleren**. Als u de gebruikersinterface opent, geeft BitDefender aan welke componenten u moet configureren.

3.2.1. Stap 1 - Selecteer het gebruiksprofiel



Klik op de knop die het best de activiteiten beschrijft die op deze computer worden uitgevoerd (het gebruiksprofiel).

Optie	Beschrijving
Typical	Klik hier als u deze pc gebruikt voor het zoeken en voor multimedia-activiteiten.
Gamer	Klik hier als u deze pc vooral gebruikt voor het spelen van spelletjes.
Aangepast	Klik hier als u alle hoofdinstantellingen van BitDefender wilt configureren.

U kunt het gebruiksprofiel later opnieuw instellen vanaf de productinterface.

3.2.2. Stap 2 - Beschrijf de computer



Selecteer de opties die van toepassing zijn op uw computer:

- **Deze computer zit in een thuisnetwerk.** Selecteer deze optie als u het BitDefender-product dat op deze computer is geïnstalleerd, op afstand wilt beheren (vanaf een andere computer). Een extra stap van de wizard zal u de mogelijkheid bieden de module Thuisnetwerkbeheer te configureren.
- **Deze computer is een laptop.** Selecteer deze optie als u wilt dat de Laptopmodus standaard wordt ingeschakeld. Terwijl u in de Laptopmodus bent, worden geplande taken niet uitgevoerd omdat ze meer systeembronnen vereisen en hierdoor ook het stroomverbruik verhogen.

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

3.2.3. Stap 3 - De gebruikersinterface selecteren



Klik op de knop die het beste uw computervaardigheden beschrijft om een geschikte modus voor de weergave van de gebruikersinterface te selecteren. U kunt kiezen om de gebruikersinterface in een van de drie modi weer te geven, afhankelijk van uw computervaardigheden en op uw eerdere ervaring met BitDefender.

Modus	Beschrijving
Beginnersmodus	Geschikt voor beginnende computergebruiker en mensen die willen dat BitDefender hun computer en gegevens beschermt zonder dat ze zich hoeven druk te maken. Deze modus is gemakkelijk te gebruiken en vereist een minimale interactie van uw kant. U hoeft alleen de bestaande problemen op te lossen wanneer dit door BitDefender wordt aangegeven. Een gebruikersvriendelijke wizard helpt u stapsgewijs bij het oplossen van problemen. Daarnaast kunt u algemene taken uitvoeren, zoals het bijwerken van de BitDefender-virushandtekening en productbestanden of het scannen van de computer.

Modus	Beschrijving
Gemiddelde modus	Deze modus is gericht op gebruikers met gemiddelde computervaardigheden en biedt meer mogelijkheden dan in de Beginnersmodus. U kunt problemen afzonderlijk oplossen en kiezen welke zaken moeten worden bewaakt. Bovendien kunt u de BitDefender-producten die op de computers van uw gezin zijn geïnstalleerd, extern beheren.
Expert-modus	Deze modus is geschikt voor meer technisch gerichte gebruikers en bieden u de mogelijkheid elke functie van BitDefender volledig te configureren. U kunt ook alle geleverde taken gebruiken om uw computer en gegevens te beschermen.

3.2.4. Stap 4 - BitDefender netwerk configureren



Opmerking

Deze stap verschijnt alleen als u in stap 2 hebt opgegeven dat de computer verbonden is met een thuisnetwerk.

BitDefender Antivirus 2010

BitDefender Configuratiewizard

Configuratie thuisnetwerkbeheer

BitDefender Antivirus 2010 Bevat Thuisbeheer waarmee u een virtueel netwerk kunt maken van alle computers in uw huishouden en alle BitDefender-producten die op dit netwerk zijn geïnstalleerd, te beheren. U kunt optreden als beheerder van een netwerk dat u maakt of u kunt deel uitmaken van een netwerk dat vanaf een andere computer is gemaakt en beheerd.

☒ Thuisnetwerk inschakelen

Thuisbeheer wachtwoord:

Wachtwoord herhalen:

Beweeg de muis over het venster om meer informatie te lezen over elke optie die in de BitDefender-gebruikersinterface wordt weergegeven. In dit gebied wordt de helptekst weergegeven.

BitDefender netwerkconfiguratie

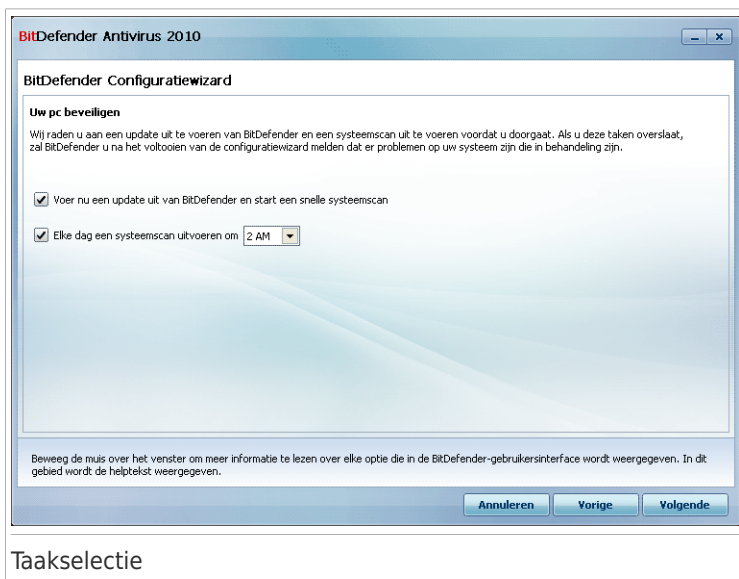
Met BitDefender kan u een virtueel netwerk van de computers in uw huishouden creëren en de op dit netwerk geïnstalleerde BitDefender producten beheren.

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

1. Selecteer **Thuisnetwerk inschakelen**.
2. Voer hetzelfde administrator wachtwoord in elk van de bewerkingsvelden in. Met het wachtwoord kan een administrator dit BitDefender product beheren vanaf een andere computer.

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

3.2.5. Stap 5 – De uit te voeren taken selecteren



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

- **BitDefender nu bijwerken en een snelle systeemscan uitvoeren** - tijdens de volgende stap worden de virushandtekeningen en productbestanden van BitDefender bijgewerkt om uw computer te beschermen tegen de recentste bedreigingen. Onmiddellijk nadat de update is voltooid, zal BitDefender de bestanden van de mappen Windows en Program Files scannen om zeker te zijn dat ze niet zijn geïnfecteerd. Deze mappen bevatten bestanden van het

besturingssysteem en van geïnstalleerde toepassingen en ze worden meestal als eerste geïnfecteerd.

- **Elke dag om 2 AM een systeemscan uitvoeren** - stelt BitDefender in om elke dag om 2 AM een standaard scan uit te voeren. Om het tijdstip waarop de scan wordt uitgevoerd te wijzigen, klikt u op het menu en selecteert u de gewenste starttijd. Als de computer wordt uitgeschakeld wanneer de planning is ingesteld, wordt de scan de volgende keer dat u de computer opstart, uitgevoerd.



Opmerking

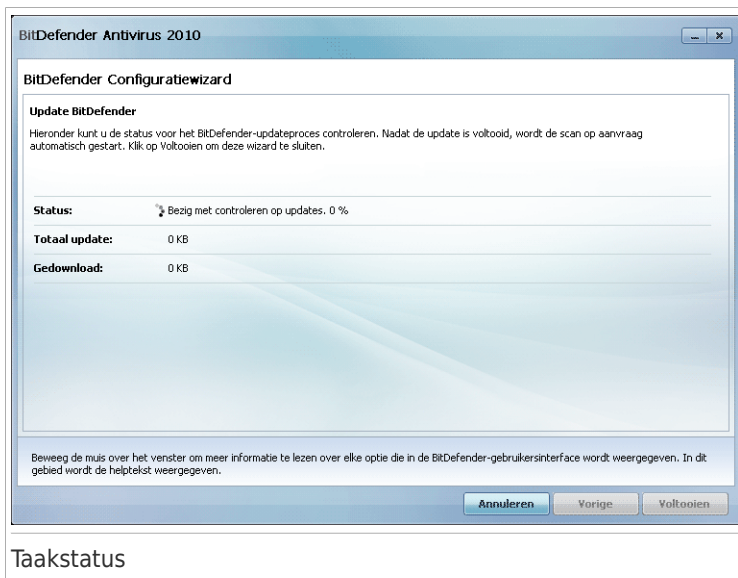
Als u het tijdstip waarop het uitvoeren van de scan is gepland later wilt wijzigen, volgt u de onderstaande stappen:

1. Open BitDefender en schakel de gebruikersinterface naar de Expert-modus.
2. Klik in het menu aan de linkerkant op **Antivirus**.
3. Klik op het tabblad **Virusscan**.
4. Klik met de rechtermuisknop op de taak **Systeemscan** en selecteer **Planning**. Een nieuw venster wordt weergegeven.
5. Wijzig de frequentie en de starttijd zoals nodig.
6. Klik op **OK** om de wijzigingen op te slaan.

Wij raden u aan deze opties in te schakelen voordat u naar de volgende stap gaat, zodat de beveiliging van uw systeem gegarandeerd is. Klik op **Volgende** om door te gaan.

Als u het eerste selectievakje uitschakelt, moeten er geen taken worden uitgevoerd in de laatste stap van de wizard. Klik op **Voltooien** om de wizard te voltooien.

3.2.6. Stap 6 - Voltooien



Wacht tot BitDefender de update heeft uitgevoerd van zijn malwarehandtekeningen en scanengines. Zodra de update is voltooid, wordt een snelle systeemscan gestart. De scan wordt stil uitgevoerd, op de achtergrond. U kunt het pictogram voor de scanvoortgang  zien in het **systeemvak**. U kunt op dit pictogram klikken om het scanvenster te openen en de scanvoortgang te bekijken.

Klik op **Voltooien** om de wizard te voltooien. U hoeft niet te wachten tot het scannen is voltooid.



Opmerking

Het scannen zal enkele minuten duren. Open het scanvenster nadat het scannen is voltooid en controleer de scanresultaten om te zien of uw systeem is opgeruimd. Als er tijdens het scannen virussen worden gedetecteerd, moet u BitDefender onmiddellijk openen en een volledige systeemscan uitvoeren.

4. Upgrade

Als u BitDefender Antivirus 2010 beta of de versie 2008 of 2009 gebruikt, kunt u upgraden naar BitDefender Antivirus 2010.

Er zijn twee manieren om de upgrade uit te voeren:

- BitDefender Antivirus 2010 rechtstreeks over de oudere versie installeren. Indien u rechtstreeks over de 2009 versie installeert, wordt de Quarantaine automatisch geïmporteerd.
- Verwijder de oudere versie. Start de computer opnieuw op en installeer de nieuwe versie, zoals beschreven in hoofdstuk “*BitDefender installeren*” (p. 5). Er zullen geen productinstellingen worden opgeslagen. Gebruik deze upgrademethode als de andere mislukt.

5. BitDefender repareren of verwijderen

Als u BitDefender Antivirus 2010 wilt repareren of verwijderen, volgt u het pad vanaf het menu Start van Windows: **Start** → **Programma's** → **BitDefender 2010** → **Repareren of verwijderen**.

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

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

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

Start de computer opnieuw op nadat u dit wordt gevraagd en klik daarna op **Installeren** om BitDefender Antivirus 2010 opnieuw te installeren.

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

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



Opmerking

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

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



Belangrijk

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

Klik op **Verwijderen** om het verwijderen van BitDefender Antivirus 2010 van uw computer te starten.

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



Opmerking

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

Aan de slag

6. Overzicht

Zodra u BitDefender hebt geïnstalleerd is uw computer beschermd. Als u de **configuratiewizard** niet hebt voltooid, moet u zo snel mogelijk BitDefender openen en de bestaande problemen oplossen. U zult mogelijk specifieke BitDefender-componenten moeten configureren of preventieve acties ondernemen om uw computer en gegevens te beschermen. Als u dat wilt, kunt u BitDefender configureren om u geen waarschuwing te sturen over specifieke problemen.

Als u het product niet hebt geregistreerd (en geen BitDefender-account hebt gemaakt), moet u dit doen voordat de evaluatieperiode verloopt. U moet een account maken binnen de 15 dagen na het installeren van BitDefender (als u het product registreert met een licentiesleutel, wordt de deadline verlengd tot 30 dagen). Anders zullen er geen updates van BitDefender meer worden uitgevoerd. Raadpleeg *"Registratie en Mijn account"* (p. 52) voor meer informatie over het registratieproces.

6.1. BitDefender openen

De hoofdinterface van BitDefender Antivirus 2010 is toegankelijk via het volgende pad vanaf het menu Start van Windows: **Start → Programma's → BitDefender 2010 → BitDefender Antivirus 2010**. Dit kan ook sneller door in het systeemvak te dubbelklikken op het BitDefender-pictogram .

6.2. Weergavemodi gebruikersinterface

BitDefender Antivirus 2010 voldoet niet alleen aan de behoeften van beginnende computergebruikers, maar ook aan de eisen van bijzonder technische gebruikers. De grafische gebruikersinterface is ontworpen zodat elke categorie gebruikers deze probleemloos kunnen gebruiken.

U kunt kiezen om de gebruikersinterface in een van de drie modi weer te geven, afhankelijk van uw computervaardigheden en op uw eerdere ervaring met BitDefender.

Modus	Beschrijving
Beginnersmodus	Geschikt voor beginnende computergebruiker en mensen die willen dat BitDefender hun computer en gegevens beschermt zonder dat ze zich hoeven druk te maken. Deze modus is gemakkelijk te gebruiken en vereist een minimale interactie van uw kant. U hoeft alleen de bestaande problemen op te lossen wanneer dit door BitDefender wordt aangegeven. Een gebruikersvriendelijke wizard helpt u stapsgewijs bij het oplossen van problemen. Daarnaast kunt u

Modus	Beschrijving
	algemene taken uitvoeren, zoals het bijwerken van de BitDefender-virushandtekening en productbestanden of het scannen van de computer.
Gemiddelde modus	Deze modus is gericht op gebruikers met gemiddelde computervaardigheden en biedt meer mogelijkheden dan in de Beginnersmodus. U kunt problemen afzonderlijk oplossen en kiezen welke zaken moeten worden bewaakt. Bovendien kunt u de BitDefender-producten die op de computers van uw gezin zijn geïnstalleerd, extern beheren.
Expert-modus	Deze modus is geschikt voor meer technisch gerichte gebruikers en bieden u de mogelijkheid elke functie van BitDefender volledig te configureren. U kunt ook alle geleverde taken gebruiken om uw computer en gegevens te beschermen.

De gebruikersinterfacemodus is geselecteerd in de configuratiewizard. Wanneer u de computer de eerste keer opstart nadat u het product hebt geïnstalleerd, verschijnt deze wizard na de registratiewizard. Indien u de configuratiewizard annuleert, zal de gebruikersinterfacemodus standaard naar de Intermediate modus schakellen.

Volg de onderstaande stappen om naar andere gebruikersinterfacemodus te gaan:

1. BitDefender openen.
2. Klik in de rechterbovenhoek van het venster op **Instellingen**.
3. Klik in categorie Instellingen gebruikersinterface op de pijl  op de knop en selecteer de gewenste modus in het menu.
4. Klik op **OK** om de wijzigingen op te slaan en toe te passen.

6.2.1. Beginnersmodus

Als u een beginnende computergebruiker bent is het aanbevolen de gebruikersinterface weer te geven in de Beginnersmodus. Deze modus is gemakkelijk te gebruiken en vereist een minimale interactie van uw kant.



Beginnersmodus

Het venster wordt in vier hoofdonderdelen georganiseerd:

- **Beveiligingsstatus** informeert u over de problemen die de beveiliging van uw computer beïnvloeden en helpt u ze op te lossen. Wanneer u op **Alle problemen herstellen** klikt, verschijnt een wizard die u zal helpen eventuele bedreigingen voor uw computer- en gegevensbeveiliging te verwijderen. Raadpleeg "*Problemen herstellen*" (p. 40) voor meer gedetailleerde informatie.
- Onder **Uw pc beveiligen** vindt u de taken die nodig zijn voor het beschermen van uw computer en gegevens. De beschikbare taken die u kunt uitvoeren, verschillen afhankelijk van het geselecteerde gebruiksprofiel.
 - De knop **Nu scannen** start een standaardscan van uw systeem op virussen, spyware en andere malware. De Antivirusscanwizard wordt weergegeven en begeleidt u doorheen het scanproces. Raadpleeg "*Antivirusscanwizard*" (p. 58) voor gedetailleerde informatie over deze wizard.

- ▶ De knop **Nu bijwerken** helpt u bij het bijwerken van de virushandtekening en productbestanden van BitDefender. Een nieuw venster verschijnt waarin u de updatestatus kan zien. Als er updates zijn gedetecteerd, worden ze automatisch gedownload en geïnstalleerd op uw computer.
- ▶ Wanneer het profiel **Standaard** is geselecteerd, start de knop **Kwetsbaarheidscontrole** een wizard die u helpt bij het zoeken en herstellen van systeemkwetsbaarheden, zoals verouderde software of ontbrekende Windows-updates. Raadpleeg sectie *“Wizard Kwetsbaarheidscontrole”* (p. 70) voor meer gedetailleerde informatie.
- ▶ Wanneer het profiel **Speler** is geselecteerd, kunt u met de knop **Spelmodus in-/uitschakelen** de **Spelmodus** in- en uitschakelen. De Spelmodus verandert tijdelijk de beveiligingsinstellingen om de snelheid van het systeem zo weinig mogelijk te beïnvloeden.
- Onder **Uw pc onderhouden** vindt u de extra taken voor het beschermen van uw computer en gegevens.
 - ▶ **Diepe systeemscan** start een uitgebreide scan van uw systeem op alle types malware.
 - ▶ **Mijn documenten scannen** voert een scan uit op virussen en andere malware in uw vaakst gebruikte mappen: Mijn documenten en Bureaublad. Dit zal de veiligheid van uw documenten, een veilige werkruimte en opgeruimde toepassingen bij het opstarten garanderen.
 - ▶ **Automatisch scannen bij aanmelden** scant de items die worden uitgevoerd wanneer u zich aanmeldt bij Windows.
- **Gebruik Profiel** duidt het gebruikprofiel aan dat momenteel wordt geselecteerd. Het gebruiksprofiel toont de belangrijkste activiteiten die op de computer worden uitgevoerd. Afhankelijk van het gebruiksprofiel wordt de productinterface geordend zodat u gemakkelijk toegang krijgt tot de taken van uw voorkeur.

Als u naar een ander profiel wilt schakelen of het profiel dat u momenteel gebruikt wilt wijzigen, klikt u op het profiel en volgt u de **configuratiewizard**.

In de rechterbovenhoek van het venster ziet u de knop **Instellingen**. Hiermee opent u een venster waarin u de gebruikersinterfacemodus kunt wijzigen en de hoofdininstellingen van BitDefender kunt in- of uitschakelen. Raadpleeg *“De basisinstellingen configureren”* (p. 44) voor meer gedetailleerde informatie.

In de hoek rechtsonder van het venster vindt u verschillende nuttige koppelingen.

Koppeling	Beschrijving
Kopen/Verlengen	Opent een webpagina waar u een licentiesleutel voor uw BitDefender Antivirus 2010-product kunt aanschaffen.

Koppeling	Beschrijving
Registratie	Hier kan u een nieuwe licentiesleutel invoeren of de huidige licentiesleutel en de registratiestatus zien.
Help & ondersteuning	Biedt u toegang tot een Help-bestand dat u toont hoe u BitDefender moet gebruiken.

6.2.2. Gemiddelde modus

De Gemiddelde modus is gericht op gebruikers met gemiddelde computervaardigheden en biedt een eenvoudige interface waarmee u toegang hebt tot alle modules op basisniveau. Hier moet u de waarschuwingen en kritieke alarmsignalen bijhouden en ongewenste situaties oplossen.



Het venster Gemiddelde modus bestaat uit vijf tabbladen. In de volgende tabel vindt u een korte beschrijving van elk tabblad. Raadpleeg het gedeelte “Gemiddelde modus” (p. 77) van deze handleiding voor gedetailleerde informatie.

Tab	Beschrijving
Dashboard	Toont de beveiligingsstatus van uw systeem en biedt u de mogelijkheid het gebruiksprofiel opnieuw in te stellen.

Tab	Beschrijving
Antivirus	Toont de status van de antivirusmodule die u helpt BitDefender up-to-date en uw computer virusvrij te houden.
Antiphishing	Toont de status van de modules die u beschermen tegen phishing (diefstal van persoonlijke gegevens) terwijl u online bent.
Kwetsbaarheid	Toont de status van de kwetsbaarheidsmodule die helpt de cruciale software op uw PC up-to-date te houden. Hier kunt u gemakkelijk elke kwetsbaarheid die de beveiliging van uw computer kan beïnvloeden, oplossen.
Network	Toont de structuur van het BitDefender thuisnetwerk. Hier kunt u verschillende acties uitvoeren om de BitDefender-producten die op uw thuisnetwerk zijn geïnstalleerd, te configureren en te beheren. Hierdoor kunt u de beveiliging van uw thuisnetwerk beheren vanaf één computer.

In de rechterbovenhoek van het venster ziet u de knop **Instellingen**. Hiermee opent u een venster waarin u de gebruikersinterfacemodus kunt wijzigen en de hoofdinstellingen van BitDefender kunt in- of uitschakelen. Raadpleeg *“De basisinstellingen configureren”* (p. 44) voor meer gedetailleerde informatie.

In de hoek rechtsonder van het venster vindt u verschillende nuttige koppelingen.

Koppeling	Beschrijving
Kopen/Verlengen	Opent een webpagina waar u een licentiesleutel voor uw BitDefender Antivirus 2010-product kunt aanschaffen.
Registreren	Hier kan u een nieuwe licentiesleutel invoeren of de huidige licentiesleutel en de registratiestatus zien.
Ondersteuning	Hiermee kan u contact maken met het BitDefender-ondersteuningsteam.
Help	Biedt u toegang tot een Help-bestand dat u toont hoe u BitDefender moet gebruiken.
Logboeken weergeven	Hier ziet u een gedetailleerde geschiedenis van alle door BitDefender op uw systeem uitgevoerde taken.

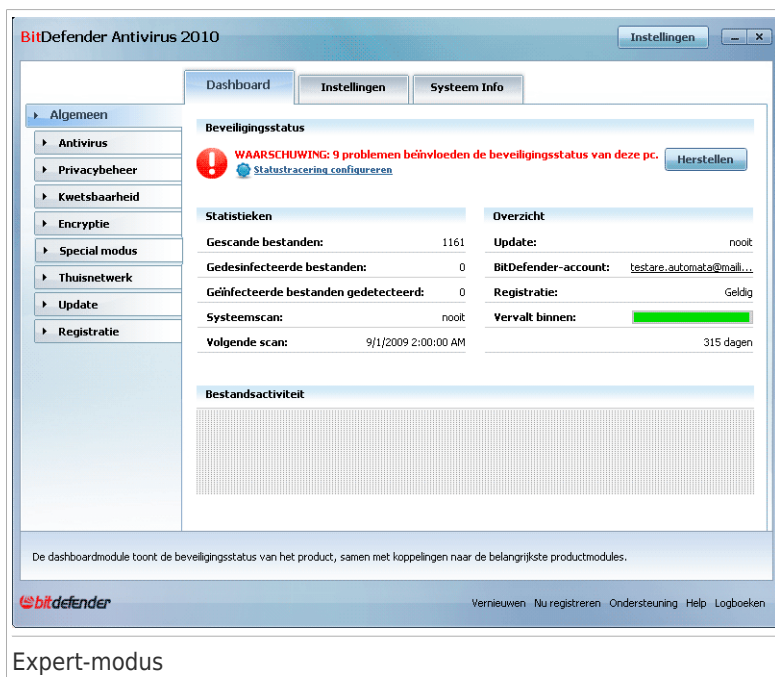
6.2.3. Expert-modus

De Expert-modus biedt u toegang tot elke specifieke component van BitDefender. Hier kunt u BitDefender in detail configureren.



Opmerking

De Expert-modus is geschikt voor gebruikers met een meer dan gemiddelde computerkennis, die weten aan welke types bedreigingen de computer wordt blootgesteld en hoe het beveiligingsprogramma werkt.



Expert-modus

Aan de linkerzijde van het venster ziet u een menu met alle beveiligingsmodules. Elke module heeft een of meer tabbladen waarop u de overeenkomende beveiligingsinstellingen kunt configureren of beveiligings- of beheertaken kunt uitvoeren. In de volgende tabel vindt u een korte beschrijving van elke module. Raadpleeg het gedeelte “Expert-modus” (p. 101) van deze handleiding voor gedetailleerde informatie.

Module	Beschrijving
Algemeen	Hiermee gaat u naar de algemene instellingen of ziet u het dashboard en gedetailleerde systeeminformatie.
Antivirus	Hiermee kan u uw virusschild en de scanning operaties in detail configureren, de uitzonderingen instellen en de quarantaine module configureren.

Module	Beschrijving
Privacybeheer	Hiermee voorkomt u diefstal van data van uw computer en beschermt u uw privacy als u online bent.
Kwetsbaarheid	Hiermee kan u de cruciale software op uw PC up-to-date houden.
Encryptie	Hiermee encrypteert u Yahoo en Windows Live (MSN) Messenger verbindingen.
Spel-/Laptop-modus	Hiermee kan u de geprogrammeerde BitDefender taken uitstellen als uw laptop op de accu werkt en verschijnen er geen waarschuwingen en pop-ups tijdens het spelen.
Netwerk	Hiermee kan u de computers in uw huishouden configureren en beheren.
Update	Hiermee kan u informatie krijgen over de laatste updates, voor het updaten van het product en voor het configureren van de details van het updateproces.
Registratie	Hiermee kunt u BitDefender Antivirus 2010 registreren, de licentiesleutel wijzigen of een BitDefender-account maken.

In de rechterbovenhoek van het venster ziet u de knop **Instellingen**. Hiermee opent u een venster waarin u de gebruikersinterfacemodus kunt wijzigen en de hoofdinstellingen van BitDefender kunt in- of uitschakelen. Raadpleeg *“De basisinstellingen configureren”* (p. 44) voor meer gedetailleerde informatie.

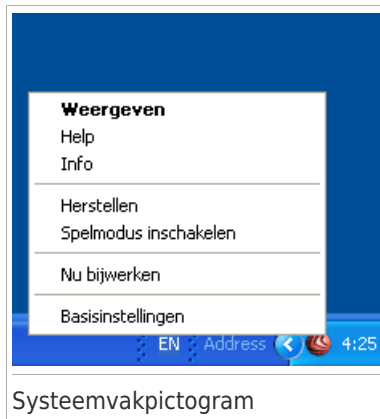
In de hoek rechtsonder van het venster vindt u verschillende nuttige koppelingen.

Koppeling	Beschrijving
Kopen/Verlengen	Opent een webpagina waar u een licentiesleutel voor uw BitDefender Antivirus 2010-product kunt aanschaffen.
Registreren	Hier kan u een nieuwe licentiesleutel invoeren of de huidige licentiesleutel en de registratiestatus zien.
Ondersteuning	Hiermee kan u contact maken met het BitDefender-ondersteuningsteam.
Help	Biedt u toegang tot een Help-bestand dat u toont hoe u BitDefender moet gebruiken.
Logboeken weergeven	Hier ziet u een gedetailleerde geschiedenis van alle door BitDefender op uw systeem uitgevoerde taken.

6.3. Systeemvakpictogram

Om het volledige product sneller te beheren, kunt u het BitDefender-pictogram in het systeemvak gebruiken. Wanneer u dubbelklikt op dit pictogram, wordt BitDefender geopend. Door met de rechterknop op het pictogram te klikken, verschijnt een snelmenu waarmee u het BitDefender-product snel kunt beheren.

- **Weergeven** - opent de hoofdinterface van BitDefender.
- **Help** - opent het Help-bestand dat in detail uitlegt hoe u BitDefender Antivirus 2010 kunt configureren en gebruiken.
- **Info** - opent een venster waar u informatie over BitDefender kunt bekijken en waar u hulp kunt zoeken wanneer er zich een onverwachte gebeurtenis voordoet.
- **Alle problemen herstellen** - helpt u de huidige zwakke punten in de beveiliging te verwijderen. Als de optie niet beschikbaar is, moeten er geen problemen worden opgelost. Raadpleeg "*Problemen herstellen*" (p. 40) voor meer gedetailleerde informatie.



- **Spelmodus in-/uitschakelen** - schakelt de **Spelmodus** in/uit.
- **Update nu** - start een directe update. Een nieuw venster verschijnt waarin u de updatestatus kan zien.
- **Basisinstellingen** - opent een venster waarin u de gebruikersinterfacemodus kunt wijzigen en de hoofdininstellingen van het product kunt in- of uitschakelen. Meer informatie vindt u onder "*De basisinstellingen configureren*" (p. 44).

Het systeemvakpictogram van BitDefender brengt u door middel van een speciaal pictogram op de hoogte van problemen die uw computer beïnvloeden of van de manier waarop het product werkt. Deze symbolen zijn de volgende:

- **Rode driehoek met een uitroepteken:** Kritieke problemen beïnvloeden de beveiliging van uw systeem. Ze vereisen uw onmiddellijke aandacht en moeten zo snel mogelijk worden hersteld.
- **Gele driehoek met een uitroepteken:** Niet-kritieke problemen beïnvloeden de beveiliging van uw systeem. U moet ze controleren en herstellen wanneer u tijd hebt.
- **Letter G:** Het product werkt op **Spelmodus**.

Als BitDefender niet werkt, wordt het systeemvakpictogram grijs weergegeven. Dit doet zich doorgaans voor wanneer de licentiesleutel vervalst. Dit kan ook optreden

wanneer de BitDefender-services niet reageren of wanneer andere fouten de normale werking van BitDefender beïnvloeden.

6.4. Scan activiteitenbalk

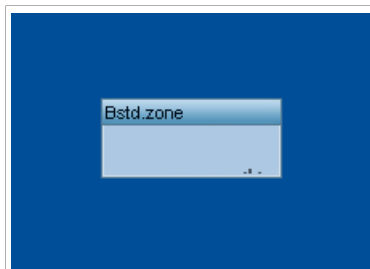
De **balk Scanactiviteit** is een grafische voorstelling van de scanactiviteit op uw systeem. Dit kleine venster is standaard alleen beschikbaar in de **Expert-modus**.

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



Opmerking

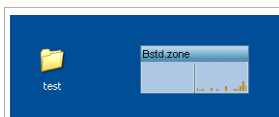
De balk voor de scanactiviteit zal aangeven wanneer de real time-beveiliging is uitgeschakeld door een rood kruis over de **Bestand** weer te geven



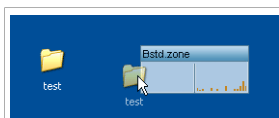
Scan activiteitenbalk

6.4.1. Bestanden en mappen scannen

U kunt de balk voor de scanactiviteit gebruiken om snel bestanden en mappen te scannen. Sleep het bestand of de map die u wilt scannen naar de **balk Scanactiviteit** zoals hieronder weergegeven.



Bestand slepen



Bestand neerzetten

De Antivirusscanwizard wordt weergegeven en begeleidt u doorheen het scanproces. Raadpleeg "**Antivirusscanwizard**" (p. 58) voor gedetailleerde informatie over deze wizard.

Scanopties. De scanopties zijn vooraf geconfigureerd voor de beste detectieresultaten. Als er geïnfecteerde bestanden wordt gedetecteerd, zal

BitDefender proberen ze te desinfecteren (de malwarecode verwijderen). Als de desinfectie mislukt, kunt u met de Antivirusscanwizard andere acties opgeven die moeten worden ondernemen op geïnfecteerde bestanden. De scanopties zijn standaard en u kunt ze niet wijzigen.

6.4.2. De balk Scanactiviteit verbergen/weergeven

Als u deze grafische voorstelling niet langer wilt zien, klik er dan op met de rechtermuisknop en selecteer **Verbergen**. Volg deze stappen om de balk met de Scanactiviteit opnieuw weer te geven:

1. BitDefender openen.
2. Klik in de rechterbovenhoek van het venster op **Instellingen**.
3. Schakel in de categorie Algemene instellingen het selectievakje naast **Balk Scanactiviteit** in.
4. Klik op **OK** om de wijzigingen op te slaan en toe te passen.

6.5. BitDefender Handmatig scannen

Met BitDefender Handmatig scannen kunt u een specifieke map of harde schijfpartitie scannen zonder dat u een scantaak hoeft te maken. Deze functie is ontwikkeld om te worden gebruikt wanneer Windows in Veilige modus wordt uitgevoerd. Als uw systeem is geïnfecteerd met een hardnekkig virus, kunt u proberen het virus te verwijderen door Windows op te starten in de Veilige modus en elke harde schijfpartitie te scannen met BitDefender Handmatig scannen.

Om toegang te krijgen tot BitDefender Handmatig scannen, gebruikt u het menu Start van Windows via het pad **Start → Programmas → BitDefender 2010 → BitDefender Handmatig scannen**. Het volgende venster wordt geopend:



BitDefender Handmatig scannen

Klik op **Map toevoegen**, selecteer de locatie die u wilt scannen en klik op **OK**. Als u meerdere mappen wilt scannen, herhaalt u deze actie voor elke extra locatie.

De paden naar de geselecteerde locaties zullen verschijnen in de kolom **Scandoel**. Als u de locatie toch niet wilt gebruiken, klik dan op de knop **Verwijderen** ernaast. Klik op de knop **Alle paden verwijderen** om alle locaties die aan de lijst zijn toegevoegd, te verwijderen.

Klik op **Doorgaan** wanneer u klaar bent met het selecteren van de locaties. De Antivirusscanwizard wordt weergegeven en begeleidt u doorheen het scanproces. Raadpleeg "*Antivirusscanwizard*" (p. 58) voor gedetailleerde informatie over deze wizard.

Scanopties. De scanopties zijn vooraf geconfigureerd voor de beste detectieresultaten. Als er geïnfecteerde bestanden wordt gedetecteerd, zal BitDefender proberen ze te desinfecteren (de malwarecode verwijderen). Als de desinfectie mislukt, kunt u met de Antivirusscanwizard andere acties opgeven die moeten worden ondernemen op geïnfecteerde bestanden. De scanopties zijn standaard en u kunt ze niet wijzigen.

Wat is de Veilige modus?

De Veilige modus is een speciale manier om Windows te starten en wordt hoofdzakelijk gebruikt om problemen die de normale werking van Windows beïnvloeden, op te lossen. Dergelijke problemen kunnen lopen van conflicterende stuurprogramma's tot virussen die verhinderen dat Windows normaal wordt gestart.

In de Veilige modus laadt Windows slechts een minimum aan componenten van het besturingssysteem en de basisstuurprogramma's. Slechts enkele toepassingen werken in de Veilige modus. Daarom zijn de meeste virussen inactief wanneer Windows in de Veilige modus wordt gebruikt en kunnen ze gemakkelijk worden verwijderd.

Om Windows in de Veilige modus te starten, start u de computer opnieuw op en drukt u op de F8-toets tot het menu Geavanceerde opties voor Windows verschijnt. U kunt kiezen tussen verschillende opties voor het starten van Windows in de Veilige modus. Wij raden u aan **Veilige modus met netwerkmogelijkheden** te selecteren om toegang te krijgen tot het internet.



Opmerking

Meer informatie over de Veilige modus vindt u in het Help en ondersteuningscentrum van Windows (Klik in het menu Start op **Help en ondersteuning**). U kunt ook nuttige informatie vinden door op het internet te zoeken.

6.6. Spelmodus en Laptop-modus

Sommige computeractiviteiten, zoals games of presentaties, vereiste een hoger reactievermogen en betere prestaties van het systeem zonder enige onderbrekingen. Wanneer uw laptop werkt op batterijvermogen, is het aanbevolen minder dringende bewerkingen die extra stroom zullen verbruiken, worden uitgesteld tot de laptop opnieuw op de netstroom is aangesloten.

Om zich aan deze specifieke situaties aan te passen, bevat BitDefender Antivirus 2010 twee speciale gebruiksmodi:

- Spelmodus
- Laptop-modus

6.6.1. Spelmodus

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

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

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

Gebruik van de Spelmodus

Standaard gaat BitDefender automatisch in de Spelmodus als u een spel start uit de lijst van BitDefender's bekende spelen of als een applicatie overgaat op volledig scherm. BitDefender zal automatisch terugkeren naar de normale gebruiksmodus wanneer u het spel afsluit of wanneer de gedetecteerde toepassing het volledig scherm afsluit.

Als u de Spelmodus handmatig wilt inschakelen, moet u een van de volgende methoden gebruiken:

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



Belangrijk

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

Veranderen van de Spelmodus sneltoets

Volg deze stappen als u de sneltoets wilt veranderen:

1. Open BitDefender en schakel de gebruikersinterface naar de Expert-modus.
2. Klik in het menu aan de linkerkant op **Spel/laptopmodus**.
3. Klik op het tabblad **Spelmodus**.
4. Klik op de knop **Geavanceerde instellingen**.
5. Stel de gewenste sneltoets in onder de **Sneltoets gebruiken** optie:
 - Kies de gewijzigde toetsen die u wilt gebruiken door één van de volgende aan te kruisen: Control toets (**Ctrl**), Shift toets (**Shift**) of Alternate toets (**Alt**).
 - Typ in het invulveld de letter van de normale toets die u wilt gebruiken.

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



Opmerking

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

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

6.6.2. Laptop-modus

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

deze apparaten op de accu werken. Terwijl u in de Laptopmodus bent, worden geplande taken niet uitgevoerd omdat ze meer systeembronnen vereisen en hierdoor ook het stroomverbruik verhogen.

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

Om de Laptopmodus te gebruiken, moet u in de **configuratiewizard** opgeven dat u een laptop gebruikt. Als u de geschikte optie niet selecteert tijdens het uitvoeren van de wizard, kunt u de Laptopmodus later als volgt inschakelen:

1. BitDefender openen.
2. Klik in de rechterbovenhoek van het venster op **Instellingen**.
3. Schakel in de categorie Algemene instellingen het selectievakje naast **Laptop-modus detectie** in.
4. Klik op **OK** om de wijzigingen op te slaan en toe te passen.

6.7. Automatische apparaatdetectie

BitDefender detecteert automatisch wanneer u een verwisselbaar opslagapparaat aansluit op uw computer en biedt u aan het te scannen voordat u de bestanden van dit apparaat opent. Dit is aanbevolen om infecties van uw computer door virussen en andere malware te voorkomen.

Gedetecteerde apparaten vallen in een van deze categorieën:

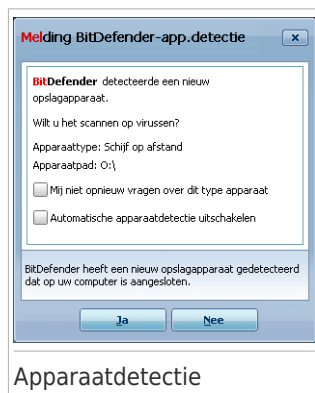
- Cd's/dvd's
- USB-opslagapparaten, zoals flashpennen en externe harde schijven
- toegewezen (externe) netwerkstations

Wanneer een dergelijk apparaat wordt gedetecteerd, verschijnt een waarschuwingsvenster.

Om het opslagapparaat te scannen, hoeft u alleen op **Ja** te klikken. De Antivirusscanwizard wordt weergegeven en begeleidt u doorheen het scanproces. Raadpleeg "**Antivirusscanwizard**" (p. 58) voor gedetailleerde informatie over deze wizard.

Als u het apparaat niet wilt scannen, klikt u op **Nee**. In dat geval kan een van deze opties nuttig zijn:

- **Mij niet meer vragen bij dit type apparaat** - BitDefender zal niet langer aanbieden opslagapparaten van dit type te scannen wanneer ze op de computer worden aangesloten.



- **Automatische apparaatdetectie uitschakelen** - U wordt niet langer gevraagd nieuwe opslagapparaten te scannen wanneer ze op de computer worden aangesloten.

Volg de onderstaande stappen als u de automatische apparaatdetectie per ongeluk hebt uitgeschakeld en deze opnieuw wilt inschakelen, of als u de instellingen hiervoor wilt configureren:

1. Open BitDefender en schakel de gebruikersinterface naar de Expert-modus.
2. Ga naar **Antivirus>Virusscan**.
3. Zoek in de lijst met scantaken naar de taak **Scan apparaatdetectie**.
4. Klik met de rechtermuisknop op de taak en selecteer **Openen**. Een nieuw venster wordt weergegeven.
5. Configureer de benodigde scanopties op het tabblad **Overzicht**. Meer informatie vindt u onder *"Scaninstellingen configureren"* (p. 126).
6. Kies de types opslagapparaten die moeten worden gedetecteerd op het tabblad **Detectie**.
7. Klik op **OK** om de wijzigingen op te slaan en toe te passen.

7. Problemen herstellen

BitDefender gebruikt een systeem voor het opsporen van problemen en brengt u op de hoogte van de problemen die de veiligheid van uw computer en gegevens kunnen beïnvloeden. Standaard zal het programma alleen een reeks problemen bewaken die als zeer belangrijk worden beschouwd. U kunt dit echter configureren volgens uw behoeften, waarbij u specifieke problemen kunt kiezen waarvan u op de hoogte wilt worden gebracht.

Problemen in behandeling worden op de volgende manier gemeld:

- Er wordt een speciaal symbool weergegeven boven het BitDefender-pictogram in het **systeemvak** om problemen in behandeling aan te geven.

 **Rode driehoek met een uitroepteken:** Kritieke problemen beïnvloeden de beveiliging van uw systeem. Ze vereisen uw onmiddellijke aandacht en moeten zo snel mogelijk worden hersteld.

 **Gele driehoek met een uitroepteken:** Niet-kritieke problemen beïnvloeden de beveiliging van uw systeem. U moet ze controleren en herstellen wanneer u tijd hebt.

Als u de muiscursor over het pictogram beweegt, verschijnt bovendien een pop-up dat het bestaan van problemen in behandeling bevestigt.

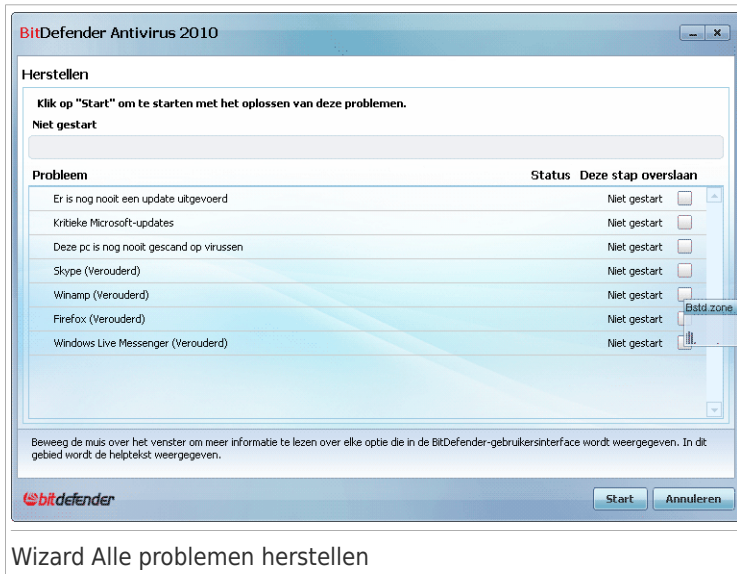
- Wanneer u BitDefender opent, geeft het gebied Beveiligingsstatus het aantal problemen dat uw systeem beïnvloedt aan.
 - ▶ In de Gemiddelde modus wordt de beveiligingsstatus weergegeven op het tabblad **Dashboard**.
 - ▶ Ga in de Expert-modus naar **Algemeen>Dashboard** om de beveiligingsstatus te controleren.

7.1. Wizard Alle problemen herstellen

De eenvoudigste manier om de bestaande problemen op te lossen is het volgen van de stapsgewijze wizard **Alle problemen herstellen**. Met deze wizard kunt u alle bedreigingen voor uw computer en gegevensbeveiliging probleemloos verwijderen. Voer een van de volgende bewerkingen uit om de wizard te openen:

- Klik met de rechtermuisknop op het BitDefender-pictogram  in het **systeemvak** en selecteer **Alle problemen herstellen**.
- BitDefender openen. Afhankelijk van de gebruikersinterfacemodus, gaat u als volgt te werk:
 - ▶ Klik in de Beginnersmodus op **Alle problemen herstellen**.
 - ▶ Ga in de Gemiddelde modus naar het tabblad **Dashboard** en klik op **Alle problemen herstellen**.

- Ga in de Expert-modus naar **Algemeen>Dashboard** en klik op **Alle problemen herstellen**.



Wizard Alle problemen herstellen

De wizard toont de lijst met bestaande kwetsbaarheden van de beveiliging op uw computer.

Alle huidige problemen zijn geselecteerd om te worden opgelost. Als er een probleem is dat u niet wilt oplossen, schakelt u het overeenkomende selectievakje uit. Hierdoor verandert zijn status naar **Overslaan**.



Opmerking

Als u niet op de hoogte wilt worden gebracht van specifieke problemen, moet u het traceringsstelsel overeenkomstig configureren zoals beschreven in de volgende sectie.

Om de geselecteerde problemen op te lossen, klikt u op **Start**. Sommige problemen worden onmiddellijk opgelost. Bij andere problemen wordt u geholpen door een wizard om ze op te lossen.

De problemen die deze wizard u helpt oplossen kunnen in deze hoofdcategorieën worden gegroepeerd.

- **Uitgeschakelde beveiligingsinstellingen.** Dergelijke problemen worden onmiddellijk opgelost door hun respectievelijke beveiligingsinstellingen in te schakelen.

- **Preventieve beveiligingstaken die u moet uitvoeren.** Een voorbeeld van een dergelijke taak is het scannen van uw computer. Het is aanbevolen uw computer minstens één keer per week te scannen. In de meeste gevallen zal BitDefender dat automatisch voor u doen. Als u de scanplanning echter hebt gewijzigd of als de planning niet is voltooid, wordt u op de hoogte gebracht van dit probleem.

Wanneer u dergelijke problemen oplost, helpt een wizard u bij het voltooien van de taak.

- **Systeemkwetsbaarheden.** BitDefender controleert uw systeem automatisch op kwetsbaarheden en breng u hiervan op de hoogte. Systeemkwetsbaarheden omvatten het volgende:

- ▶ zwakke wachtwoorden voor Windows-gebruikersaccounts.
- ▶ verouderde software op uw computer.
- ▶ ontbrekende Windows-updates.
- ▶ Automatische Windows-updates is uitgeschakeld.

Wanneer dergelijke problemen moeten worden opgelost, wordt de wizard voor het scannen op kwetsbaarheid gestart. Deze wizard helpt u bij het oplossen van de gedetecteerde systeemkwetsbaarheden. Raadpleeg sectie *"Wizard Kwetsbaarheidscontrole"* (p. 70) voor meer gedetailleerde informatie.

7.2. Het opsporen van problemen configureren

Het systeem voor het opsporen van problemen is vooraf geconfigureerd voor de bewaking en om u te waarschuwen voor de belangrijkste problemen die de veiligheid van uw computer en gegevens kunnen beïnvloeden. Er kunnen meer problemen worden bewaakt op basis van de keuzen die u maakt in de *configuratiewizard* (wanneer u uw gebruikersprofiel configureert). Naast de problemen die standaard worden bewaakt, zijn er verschillende andere problemen waarover u op de hoogte kunt worden gebracht.

U kunt het traceringsstelsel configureren om optimaal te voldoen aan uw beveiligingsbehoeften door te kiezen over welke problemen u op de hoogte wilt worden gebracht. U kunt dit in de Gemiddelde of Expert-modus uitvoeren.

- In de Gemiddelde modus kan het traceringsstelsel worden geconfigureerd vanaf afzonderlijke locaties. Volg deze stappen:
 1. Ga naar het tabblad **Antivirus, Antiphishing of Kwetsbaarheid**.
 2. Klik op **Statustracing configureren**.
 3. Schakel de selectievakjes in naast de items die u wilt bewaken.

Raadpleeg het gedeelte *"Gemiddelde modus"* (p. 77) van deze handleiding voor gedetailleerde informatie.

- In de Expert-modus kan het traceringsysteem worden geconfigureerd vanaf een centrale locatie. Volg deze stappen:
 1. Ga naar **Algemeen>Dashboard**.
 2. Klik op **Statustracering configureren**.
 3. Schakel de selectievakjes in naast de items die u wilt bewaken.

Raadpleeg hoofdstuk "*Dashboard*" (p. 102) voor meer gedetailleerde informatie.

8. De basisinstellingen configureren

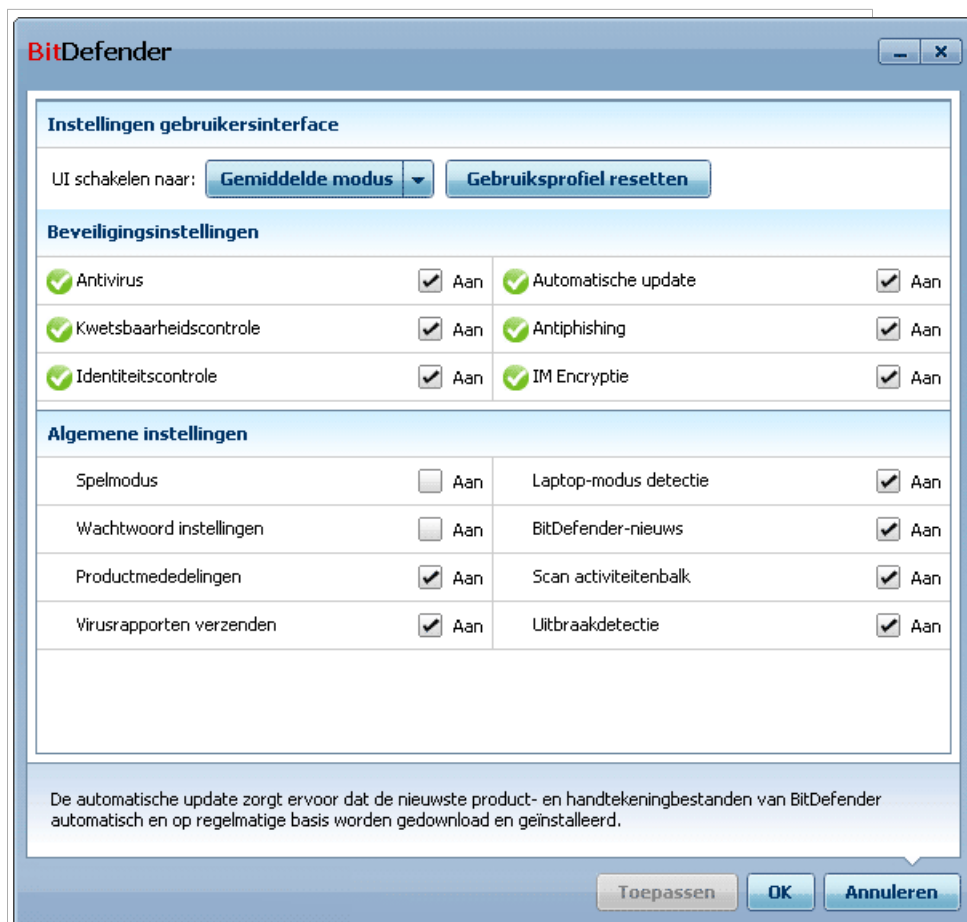
U kunt de hoofdininstellingen van het product (inclusief het wijzigen van de weergavemodus voor de gebruikersinterface) configureren vanaf het venster met de basisinstellingen. Voer een van de volgende bewerkingen uit om het venster te openen:

- Open BitDefender en klik in de rechterbovenhoek van het venster op **Instellingen**.
- Klik met de rechtermuisknop op het BitDefender-pictogram  in het **systeemvak** en selecteer **Basisinstellingen**.



Opmerking

Gebruik de interface Expert-modus om de productinstellingen in detail te configureren. Raadpleeg het gedeelte “**Expert-modus**” (p. 101) van deze handleiding voor gedetailleerde informatie.



Basisinstellingen

De instellingen zijn geordend in drie categorieën:

- **Instellingen gebruikersinterface**
- **Beveiligingsinstellingen**
- **Algemene instellingen**

Klik op **OK** om de configuratiewijzigingen die u uitvoert, toe te passen en op te slaan. Klik op **Annuleren** om het venster te sluiten zonder de wijzigingen op te slaan.

8.1. Instellingen gebruikersinterface

In dit gebied kunt u de weergavemodus van de gebruikersinterface schakelen en het gebruiksprofiel opnieuw instellen.

De weergavemodus voor de gebruikersinterface schakelen. Zoals beschreven in sectie *"Weergavemodi gebruikersinterface"* (p. 24), zijn er drie modi voor het weergeven van de gebruikersinterface. Elke gebruikersinterfacemodus is ontworpen voor een specifieke categorie gebruikers op basis van hun computervaardigheden. Op deze manier is de gebruikersinterface geschikt voor elk type gebruikers, van beginnende computergebruikers tot bijzonder technische gebruikers.

De eerste knop toont de weergavemodus van de huidige gebruikersinterface. Om de gebruikersinterfacemodus te wijzigen, klikt u op de pijl  op de knop en selecteert u de gewenste modus in het menu.

Modus	Beschrijving
Beginnersmodus	Geschikt voor beginnende computergebruiker en mensen die willen dat BitDefender hun computer en gegevens beschermt zonder dat ze zich hoeven druk te maken. Deze modus is gemakkelijk te gebruiken en vereist een minimale interactie van uw kant. U hoeft alleen de bestaande problemen op te lossen wanneer dit door BitDefender wordt aangegeven. Een gebruikersvriendelijke wizard helpt u stapsgewijs bij het oplossen van problemen. Daarnaast kunt u algemene taken uitvoeren, zoals het bijwerken van de BitDefender-virushandtekening en productbestanden of het scannen van de computer.
Gemiddelde modus	Deze modus is gericht op gebruikers met gemiddelde computervaardigheden en biedt meer mogelijkheden dan in de Beginnersmodus. U kunt problemen afzonderlijk oplossen en kiezen welke zaken moeten worden bewaakt. Bovendien kunt u de BitDefender-producten die op de computers van uw gezin zijn geïnstalleerd, extern beheren.
Expert-modus	Deze modus is geschikt voor meer technisch gerichte gebruikers en bieden u de mogelijkheid elke functie van BitDefender volledig te configureren. U kunt ook alle geleverde taken gebruiken om uw computer en gegevens te beschermen.

Het gebruiksprofiel opnieuw instellen. Het gebruiksprofiel toont de belangrijkste activiteiten die op de computer worden uitgevoerd. Afhankelijk van het gebruiksprofiel wordt de productinterface geordend zodat u gemakkelijk toegang krijgt tot de taken van uw voorkeur.

Om het gebruiksprofiel opnieuw te configureren, klikt u op **Gebruiksprofiel resetten** en volgt u de configuratiewizard.

8.2. Beveiligingsinstellingen

In dit gebied kunt u productinstellingen die verschillende aspecten van computer- en gegevensbeveiliging dekken, in- of uitschakelen. De huidige status van een instelling wordt aangeduid met een van de volgende pictogrammen:

 **Groene cirkel met een vinkje:** de instelling is ingeschakeld.

 **Rode cirkel met een uitroepteken:** de instelling is uitgeschakeld.

Om de instelling in/uit te schakelen, schakelt u het overeenkomende selectievakje **Inschakelen** in/uit.



Waarschuwing

Wees voorzichtig wanneer u de real time antivirusbescherming of de automatische update uitschakelt. Het uitschakelen van deze functies kan de beveiliging van uw computer in gevaar brengen. Als u ze werkelijk moet uitschakelen, denk er dan aan ze zo snel mogelijk opnieuw in te schakelen.

De volledige lijst met instellingen en hun beschrijving vindt u in de volgende tabel:

Instelling	Beschrijving
Antivirus	Real time-beveiliging garandeert dat alle bestanden worden gescand als zij worden benaderd door u of door een toepassing op dit systeem.
Automatische update	De automatische update zorgt ervoor dat de nieuwste product- en handtekeningbestanden van BitDefender automatisch en op regelmatige basis worden gedownload en geïnstalleerd.
Kwetsbaarheidscontrole	De automatische controle op zwakke punten zorgt ervoor dat cruciale software op uw pc up-to-date is.
Antiphishing	Antiphishing detecteert en waarschuwt in real time als een webpagina is ingesteld voor diefstal van persoonlijke informatie.
Identiteitscontrole	Identiteitscontrole helpt u te verhinderen dat uw persoonlijke gegevens zonder uw toestemming via internet worden verzonden. Dit blokkeert alle

Instelling	Beschrijving
	expresberichten, e-mailberichten of webformulieren die de gegevens die u als persoonlijk hebt gedefinieerd, worden verzonden naar onbevoegde ontvangers (adressen).
IM encryptie	Met IM-codering (Instant Messaging) kunt u uw conversaties via Yahoo! Messenger en Windows Live Messenger beveiligen, op voorwaarde dat uw IM-contactpersonen een compatibel BitDefender-product en compatibele IM-software gebruiken.

De status van sommige instellingen kan worden bewaakt door het systeem voor het opsporen van problemen van BitDefender. Als u een bewaakte instelling uitschakelt, zal BitDefender dit aanduiden als een probleem dat u moet oplossen.

Als u niet wilt dat een bewaakte instelling die u hebt uitgeschakeld, als probleem wordt weergegeven, moet u het traceringsysteem overeenkomstig configureren. U kunt dit in de Gemiddelde of Expert-modus uitvoeren.

- In de Gemiddelde modus kan het traceringssysteem worden geconfigureerd vanaf afzonderlijke locaties, gebaseerd op instellingscategorieën. Raadpleeg het gedeelte **“Gemiddelde modus”** (p. 77) van deze handleiding voor gedetailleerde informatie.
- In de Expert-modus kan het traceringsysteem worden geconfigureerd vanaf een centrale locatie. Volg deze stappen:
 1. Ga naar **Algemeen>Dashboard**.
 2. Klik op **Status tracering configureren**.
 3. Schakel het selectievakje in naast de items die u niet wilt bewaken.

Raadpleeg hoofdstuk **“Dashboard”** (p. 102) voor meer gedetailleerde informatie.

8.3. Algemene instellingen

In dit gebied kunt u de instellingen die het productgedrag en de gebruikerservaring beïnvloeden in-/uitschakelen. Om de instelling in/uit te schakelen, schakelt u het overeenkomende selectievakje **Inschakelen** in/uit.

De volledige lijst met instellingen en hun beschrijving vindt u in de volgende tabel:

Instelling	Beschrijving
Spelmodus	Spelmodus wijzigt tijdelijk de beveiligingsinstellingen om de snelheid van uw systeem zo weinig mogelijk te beïnvloeden.

Instelling	Beschrijving
Laptop-modus detectie	Laptop-modus wijzigt tijdelijk de beveiligingsinstellingen om de accu van uw laptop zo weinig mogelijk te belasten.
Instellingen wachtwoord	Dit garandeert dat de BitDefender instellingen alleen kunnen worden veranderd door degene die dit wachtwoord kent. Wanneer u deze optie inschakelt, wordt u gevraagd het instelwachtwoord te configureren. Voer het gewenste wachtwoord in beide velden in en klik op OK om het wachtwoord in te stellen.
BitDefender News	Als u deze optie inschakelt, ontvangt u belangrijk nieuws over bedrijf, product updates of nieuwe bedreigingen van de veiligheid.
Waarschuwingen productmeldingen	Als u deze optie inschakelt, ontvangt u waarschuwingeninformatie.
Scanactiviteitenbalk	De balk Scanactiviteit is een klein, transparant venster dat de voortgang van de BitDefender-scanactiviteit aangeeft. Raadpleeg " <i>Scan activiteitenbalk</i> " (p. 33) voor meer informatie.
Virusrapporten verzenden	Als u deze optie inschakelt, worden virusscanrapporten verzonden naar BitDefender labs voor analyse. Merk op dat deze rapporten geen vertrouwelijke data bevatten, zoals uw naam of IP-adres, en evenmin worden gebruikt voor commerciële doeleinden.
Uitbraakdetectie	Als u deze optie inschakelt, worden rapporten over potentiële virusuitbraken verzonden naar BitDefender labs voor analyse. Merk op dat deze rapporten geen vertrouwelijke data bevatten, zoals uw naam of IP-adres, en evenmin worden gebruikt voor commerciële doeleinden.

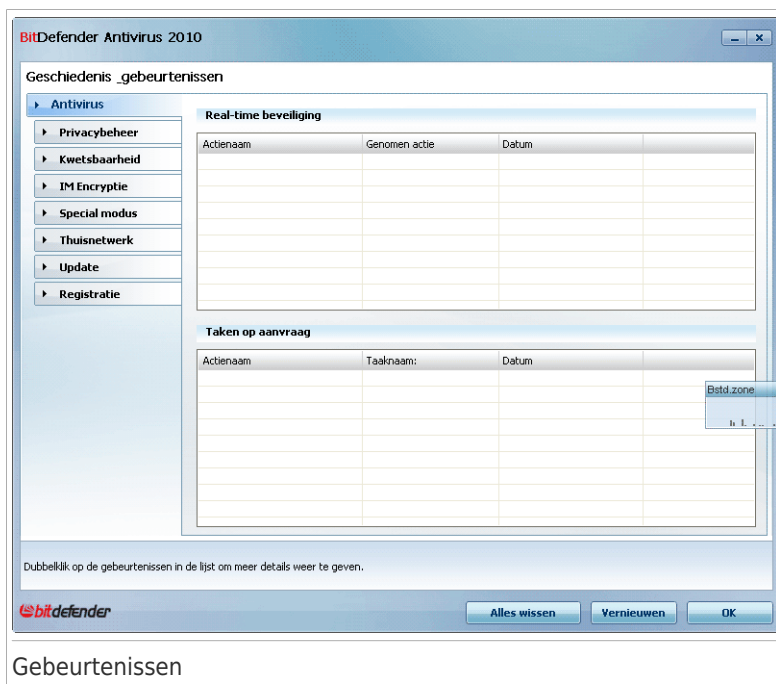
9. Geschiedenis en gebeurtenissen

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



Opmerking

De koppeling is alleen toegankelijk in de Gemiddelde of Expert-modus.



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

- **Antivirus**
- **Privacybeheer**
- **Kwetsbaarheid**
- **IM encryptie**
- **Spel-/Laptopmodus**

- **Thuisnetwerk**
- **Update**
- **Registratie**
- **Internet Log**

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

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

10. Registratie en Mijn account

BitDefender Antivirus 2010 begint met een 30-dagen proefperiode. Tijdens de evaluatieperiode is het product volledig functioneel en kunt u het testen om te zien of het voldoet aan uw verwachtingen. Na een evaluatie van 15 dagen wordt het updaten van het product gestopt, tenzij u een BitDefender-account maakt. Een BitDefender-account is een verplicht onderdeel van het registratieproces.

Voordat de evaluatieperiode voorbij is, moet u het product registreren om uw computer beschermd te houden. De registratie is een proces in twee stappen:

1. **Productactivering (registratie van een BitDefender-account).** U moet een BitDefender-account maken voor het ontvangen van updates en toegang tot gratis technische ondersteuning. Als u al een BitDefender-account hebt, moet u uw BitDefender-product registreren voor die account. BitDefender zal u op de hoogte brengen om uw product te activeren en u helpen bij het oplossen van dit probleem.



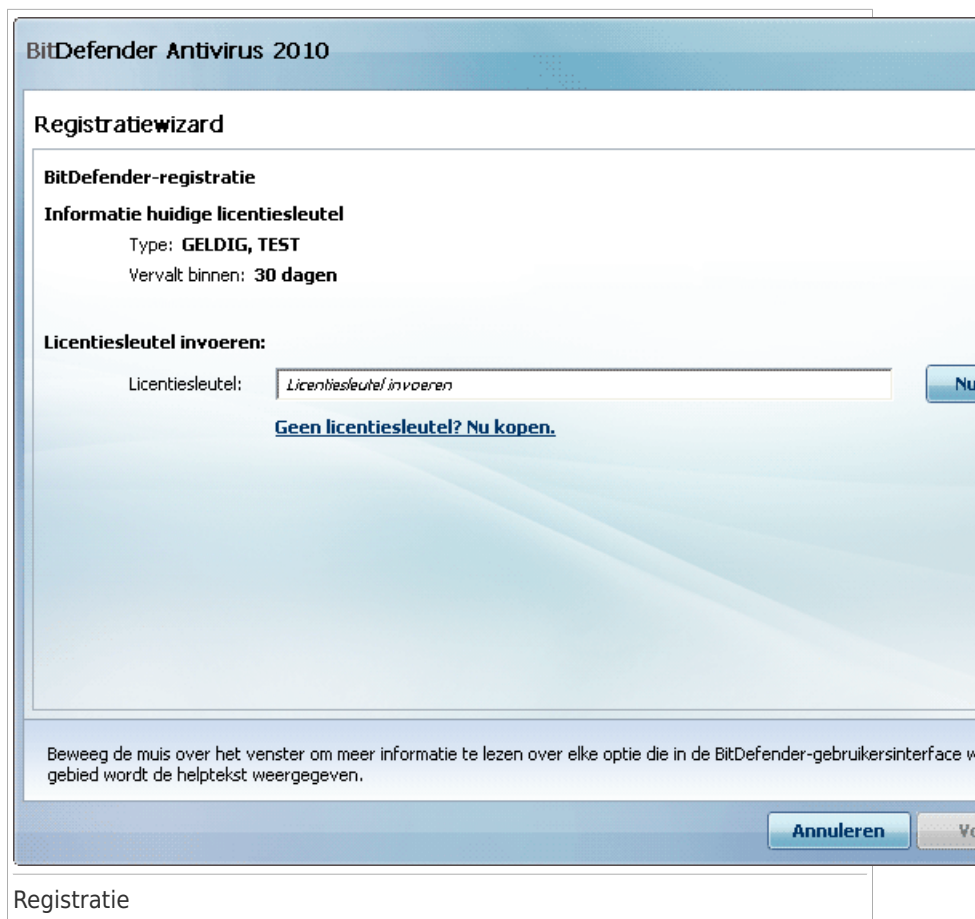
Belangrijk

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

2. **Registratie met een licentiesleutel.** De licentiesleutel bepaalt hoelang u het recht hebt het product te gebruiken. Zodra de licentiesleutel vervalt, stopt BitDefender met het uitvoeren van zijn functies en het beschermen van uw computer. U moet het product registreren met een licentiesleutel wanneer de evaluatieperiode eindigt. Enkele dagen voordat de huidige licentiesleutel aanschaft of vernieuwt, moet u een licentiesleutel aanschaffen of uw licentie vernieuwen.

10.1. BitDefender Antivirus 2010 registreren

Als u het product wilt registreren met een licentiesleutel of als u de huidige licentiesleutel wilt wijzigen, klikt u op de koppeling **Nu registreren** onderaan in het BitDefender-venster. Het venster met de productregistratie verschijnt.



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

BitDefender Antivirus 2010 registreren:

1. Typ de licentiesleutel in het bewerkingsveld.



Opmerking

U kan uw licentiesleutel vinden:

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

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

2. Klik op **Nu registreren**.
3. Klik op **Voltooien**.

10.2. BitDefender activeren

Om BitDefender te activeren, moet u een BitDefender-account maken of u aanmelden bij een bestaande account. Als u geen BitDefender-account hebt geregistreerd tijdens het uitvoeren van de eerste registratiewizard, kunt u dat als volgt doen:

- Klik in de Beginnersmodus op **Alle problemen herstellen**. De wizard zal u helpen bij het oplossen van alle problemen in behandeling, inclusief het activeren van het product.
- Ga in de Gemiddelde modus naar het tabblad **Beveiliging** en klik op de knop **Herstellen** naast het probleem met betrekking tot de productactivering.
- Ga in de Expert-modus naar **Registratie** en klik op de knop **Product activeren**.

Het venster met de accountregistratie wordt geopend. Hier kunt u een BitDefender-account maken of aanmelden bij een account om uw product te activeren.

BitDefender Antivirus 2010

Registratiewizard

BitDefender-account

Activeer uw BitDefender nu om toegang tot technische dienst te krijgen. Ook geeft <http://myaccount.Bitdefender.com> u verloren licentiesleutel terug te krijgen en krijgt u het voordeel uit de speciale BitDefender aanbiedingen.

☒ Een nieuwe account maken

E-mailadres:

Wachtwoord: Wachtwoord herhalen:

E-mailopties:

☐ Aanmelden (eerder gemaakte account)

☐ Later registreren (de registratie is verplicht)

Beweeg de muis over het venster om meer informatie te lezen over elke optie die in de BitDefender-gebruikersinterface w gebied wordt de helptekst weergegeven.

Account creëren

Als u momenteel geen BitDefender-account wilt maken, selecteert u **Later registreren** en klikt u op **Voltooiën**. Ga anders te werk zoals past bij uw situatie:

- “Ik heb geen BitDefender-account” (p. 56)
- “Ik heb al een BitDefender-account” (p. 56)



Belangrijk

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

Ik heb geen BitDefender-account

Volg deze stappen om een BitDefender-account te maken:

1. Selecteer **Een nieuwe account maken**.
2. Typ de vereiste informatie in de overeenkomende velden. De gegevens die u hier opgeeft blijven vertrouwelijk.
 - **E-mailadres** - voer uw e-mailadres in.
 - **Wachtwoord** - voer een wachtwoord voor uw BitDefender-account in. Het wachtwoord moet 6 tot 16 tekens lang zijn.
 - **Wachtwoord opnieuw** - voer het zojuist gebruikte wachtwoord opnieuw in.



Opmerking

Zodra de account is geactiveerd, kunt u het bijgeleverde e-mailadres en het wachtwoord gebruiken om u aan te melden bij uw account op <http://myaccount.bitdefender.com>.

3. Optioneel kan BitDefender u informeren over speciale aanbiedingen via het e-mailadres van uw account. Selecteer een van de beschikbare opties in het menu:
 - **Mij alle berichten sturen**
 - **Mij alleen berichten met betrekking tot producten sturen**
 - **Stuur mij geen berichten**
4. Klik op **Maken**.
5. Klik op **Voltooien** om de wizard te voltooien.
6. **Uw account activeren**. Voordat u uw account kunt gebruiken, moet u deze activeren. Controleer uw e-mail en volg de instructies in de e-mail die u van de registratieservice van BitDefender hebt ontvangen.

Ik heb al een BitDefender-account

BitDefender detecteert automatisch of u al een BitDefender-account hebt geregistreerd op uw computer. Geef in dit geval het wachtwoord van uw account op en klik op **Aanmelden**. Klik op **Voltooien** om de wizard te voltooien.

Als u al een actieve account hebt, maar BitDefender deze niet detecteert, moet u deze stappen volgen om het product voor die account te registreren:

1. Selecteer **Aanmelden (eerder gemaakte account)**.
2. Voer het e-mailadres en wachtwoord van uw account in de overeenkomende velden in.



Opmerking

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

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

- **Mij alle berichten sturen**
- **Mij alleen berichten met betrekking tot producten sturen**
- **Stuur mij geen berichten**

4. Klik op **Aanmelden**.

5. Klik op **Voltooien** om de wizard te voltooien.

10.3. Licentiesleutels aanschaffen

Als de evaluatieperiode binnenkort zal eindigen, moet u een licentiesleutel aanschaffen en uw product registreren. Open BitDefender en klik onderaan in het venster op de koppeling **Kopen/verlengen**. De koppeling neemt u mee naar een webpagina waar u een licentiesleutel kunt aanschaffen voor uw BitDefender-product.

10.4. Uw licentie vernieuwen

Als BitDefender-klant komt u in aanmerking voor een korting wanneer u de licentie van uw BitDefender-product vernieuwt. U kunt uw product ook met een speciale korting of gratis upgraden naar de huidige versie.

Als uw huidige licentiesleutel binnenkort vervalt, moet u uw licentie vernieuwen. Open BitDefender en klik onderaan in het venster op de koppeling **Kopen/verlengen**. De koppeling neemt u mee naar een webpagina waar u uw licentie kunt verlengen.

11. Wizards

Om BitDefender gebruikersvriendelijk te maken, zijn er verschillende wizards voorzien om u te helpen bij het uitvoeren van specifieke beveiligingstaken of het configureren van meer complexe productinstellingen. Dit hoofdstuk beschrijft de wizards die kunnen verschijnen wanneer u problemen oplost of specifieke taken uitvoert met BitDefender. Andere configuratiewizards zijn afzonderlijk beschreven in het gedeelte “Expert-modus” (p. 101).

11.1. Antivirusscanwizard

Telkens wanneer u een scan op aanvraag start (bijvoorbeeld klik met de rechtermuisknop op een map en selecteer **Scannen met BitDefender**), verschijnt de Antivirusscanwizard van BitDefender. Volg de begeleide procedure van drie stappen om het scanproces te voltooien.

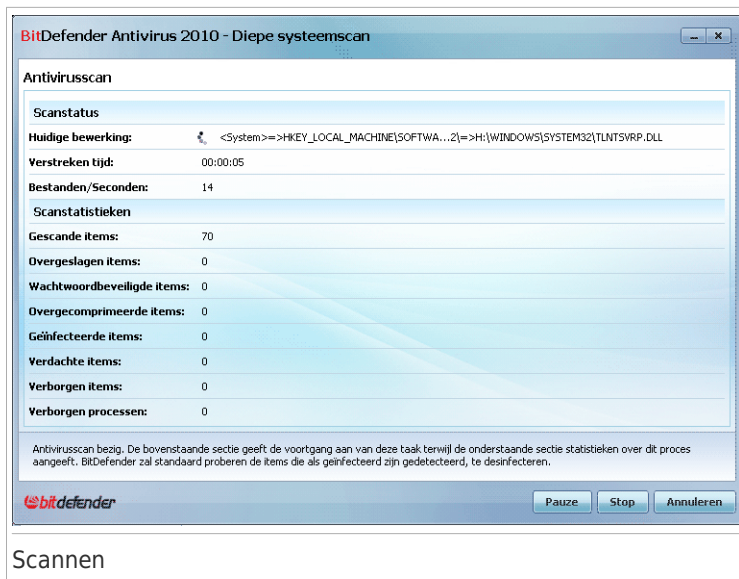


Opmerking

Als de scanwizard niet verschijnt, kan de scan worden geconfigureerd om stil te worden uitgevoerd op de achtergrond. Zoek het pictogram voor de scanvoortgang  in het **systeemvak**. U kunt op dit pictogram klikken om het scanvenster te openen en de scanvoortgang te bekijken.

11.1.1. Stap 1/3 - Scannen

BitDefender start het scannen van de geselecteerde objecten.



Scannen

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

Wacht tot BitDefender het scannen beëindigt.



Opmerking

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

Wachtwoordbeveiligde archieven. Als BitDefender een wachtwoordbeveiligd archief detecteert tijdens een scan en de standaardactie **Wachtwoord vragen** is, wordt u gevraagd het wachtwoord in te voeren. Met een wachtwoord beveiligde archieven kunnen niet worden gescand, tenzij u het wachtwoord opgeeft. De volgende opties zijn beschikbaar:

- **Ik wil het wachtwoord voor dit object invoeren.** Als u wilt dat BitDefender het archief scant, moet u deze optie selecteren en het wachtwoord invoeren. Als u het wachtwoord niet kent, kies dan een van de andere opties.
- **Ik wil het wachtwoord voor dit object niet invoeren.** Selecteer deze optie om het scannen van dit archief over te slaan.
- **Ik wil voor geen enkel object een wachtwoord invoeren (alle wachtwoordbeveiligde objecten overslaan).** Selecteer deze optie als u niet wilt worden lastig gevallen met betrekking tot wachtwoordbeveiligde archieven.

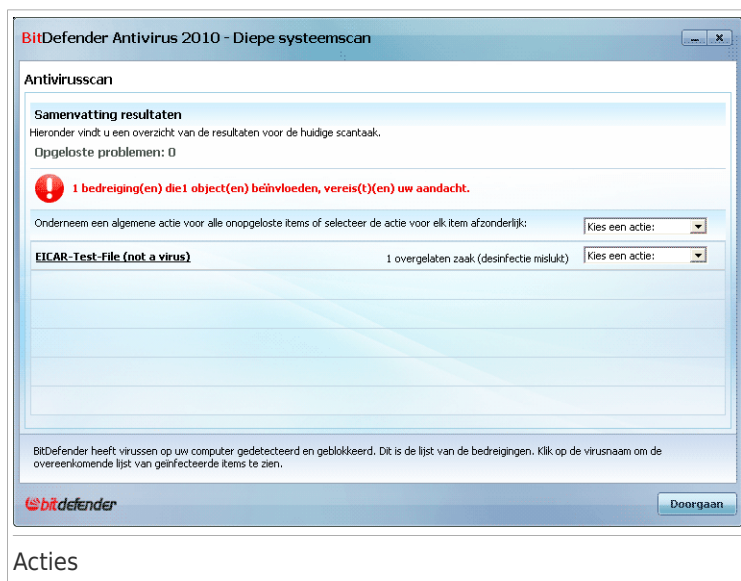
BitDefender zal ze niet kunnen scannen, maar er wordt wel een gegeven bewaard in het scanlogboek.

Klik op **OK** om door te gaan met scannen.

De scan stoppen of pauzeren. U kunt het scannen op elk ogenblik stoppen door op **Stop&Ja** te klikken. U gaat dan rechtstreeks naar de laatste stap van de wizard. Klik op **Pauze** om het scanproces tijdelijk te stoppen. Om het scannen te hervatten, klikt u op **Hervatten**.

11.1.2. Stap 2/3 - Acties selecteren

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



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

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

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

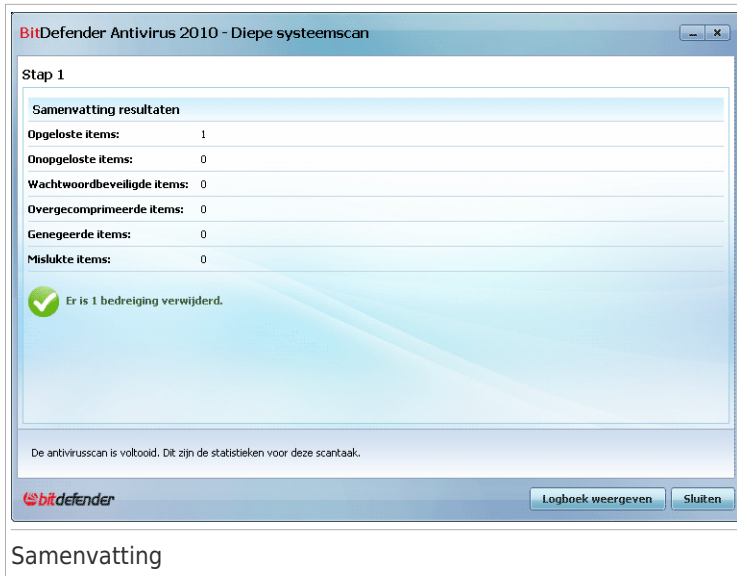
Een of meerdere van de volgende opties kunnen in het menu verschijnen.

Actie	Beschrijving
Geen actie nemen	Er wordt geen actie ondernomen voor de geïnfecteerde bestanden. Als de scan is voltooid, kan u het scanlogbestand openen om informatie over deze bestanden te zien.
Desinfecteren	Verwijdert de malwarecode uit geïnfecteerde bestanden.
Verwijderen	Verwijdert gedetecteerde bestanden.
Naar quarantaine verplaatsen	Verplaatst gedetecteerde bestanden naar de quarantaine. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer.
Naam bestanden wijzigen	Wijzigt de naam van verborgen bestanden door .bd.ren toe te voegen aan hun naam. Hierdoor zult u dergelijke bestanden op uw computer kunnen zoeken en vinden, als die er zijn. Houd ermee rekening dat deze verborgen bestanden geen bestanden zijn die u opzettelijk verbergt voor Windows. Het zijn de bestanden die worden verborgen door speciale programma's, bekend als rootkits. Rootkits zijn in wezen niet kwaadaardig. Ze worden echter algemeen gebruikt om ervoor te zorgen dat virussen en spyware niet detecteerbaar zijn voor normale antivirusprogramma's.

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

11.1.3. Stap 3/3 - Resultaten weergeven

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



U kan een samenvatting van de resultaten zien. Als u uitgebreide informatie over het scanproces wenst, klikt u op **Logbestand tonen** om het scanlogboek weer te geven.



Belangrijk

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

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

BitDefender kon bepaalde problemen niet oplossen

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

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

BitDefender detecteerde verdachte bestanden

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

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

11.2. Wizard Aangepaste scan

Wanneer u BitDefender in de Gemiddelde modus gebruikt, kunt u met de wizard Aangepaste scan een aangepaste scantaak maken en uitvoeren en deze optioneel opslaan als een Snelle taak.

Om een aangepaste scantaak uit te voeren met de wizard Aangepaste scan, moet u deze stappen volgen:

1. Intermediate mode ga naar het **Antivirus** tab.
2. In de snel start venster , de druk op **Costum scan**.
3. Volg de begeleide procedure van zes stappen om het scanproces te voltooien.

11.2.1. Stap 1/6 – Welkomstvenster

Dit is een welkomstvenster.



Als u dit venster wilt overslaan wanneer u deze wizard in de toekomst uitvoert, moet u het selectievakje **Deze stap niet meer weergeven wanneer de wizard de volgende keer wordt uitgevoerd** inschakelen.

Klik op **Volgende**.

11.2.2. Stap 2/6 - Doel selecteren

Hier kunt u de bestanden of mappen die moeten worden gescand opgeven, evenals de scanopties.

BitDefender Antivirus 2010

Scan Wizard

Gescande items:
Klik op Doel toevoegen om het scandoel voor deze scantaak te definiëren.

Doel toevoegen

Scandoel:

Scan Opties:
Alle bestanden scannen

De extensies moeten worden gescheiden met een puntkomma (bijv.: exe;.com;.vxd;)

Annuleren Vorige Volgende

Doel selecteren

Klik op **Doel toevoegen**, selecteer de bestanden of mappen die u wilt scannen en klik op **OK**. De paden naar de geselecteerde locaties zullen verschijnen in de kolom **Scandoel**. Als u de locatie toch niet wilt gebruiken, klik dan op de knop **Verwijderen** ernaast. Klik op de knop **Alles verwijderen** om alle locaties die aan de lijst zijn toegevoegd, te verwijderen.

Wanneer u klaar bent met het selecteren van de locaties, kunt u de **Scanopties** instellen. De volgende opties zijn beschikbaar:

Optie	Beschrijving
Alle bestanden scannen	Selecteer deze optie om alle bestanden in de geselecteerde mappen te scannen.
Alleen bestanden met toepassingsextensies 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;

Optie	Beschrijving
	.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.
Alleen 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 ",".

Klik op **Volgende**.

11.2.3. Stap 3/6 - Acties selecteren

Hier kunt u de scannerinstellingen en het scanniveau opgeven.

BitDefender Antivirus 2010

Scan Wizard

Actie-opties
Kies de geschikte scannerinstellingen en stel het scanniveau in.

Te nemen acties voor geïnfecteerde bestanden:

Eerste actie:

Tweede actie:

Te nemen acties voor verdachte bestanden:

Eerste actie:

Tweede actie:

Te nemen actie voor verborgen (rootkit) bestanden:

Actie:

Scanniveau
Selecteer het agressiviteitsniveau van de scanner met behulp van de schuifregelaar.

Agressief **Standaard** **Toegeeflijk** **Aangepast**

- Standaard, gemiddeld bronverbruik
- Scannen van bestanden
- Scannen op virussen en spyware

Annuleren **Vorige** **Volgende**

Acties selecteren

- Selecteer de acties die moeten worden genomen voor de gedetecteerde geïnfecteerde en verdachte bestanden. De volgende opties zijn beschikbaar:

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

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

Actie	Beschrijving
Geen actie nemen	Er wordt geen actie ondernomen voor verborgen bestanden. Deze bestanden zullen verschijnen in het rapportbestand.
Rename	Wijzigt de naam van verborgen bestanden door .bd .ren toe te voegen aan hun naam. Hierdoor zult u dergelijke bestanden op uw computer kunnen zoeken en vinden, als die er zijn.

- Configureer de agressiviteit van de scanner. U hebt de keuze uit 3 niveaus. Sleep de schuifregelaar langs de schaal om het geschikte beveiligingsniveau in te stellen:

Scanniveau	Beschrijving
Toegeeflijk	Alleen toepassingsbestanden worden gescand. Ze worden alleen op virussen gescand. Het verbruiksniveau van de bron is laag.
Standaard	Het verbruiksniveau van de bron is gemiddeld. Alle bestanden worden gescand op virussen en spyware.
Agressief	Alle bestanden (inclusief archieven) worden gescand op virussen en spyware. Verborgen bestanden en processen worden opgenomen in de scan. Het niveau van het bronverbruik is hoger.

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

Sleep de schuifregelaar om **Aangepast** te selecteren en klik vervolgens op de knop **Aangepast niveau**. Een venster wordt weergegeven. Geef het type malware op dat BitDefender moet scannen door de geschikte opties te selecteren:

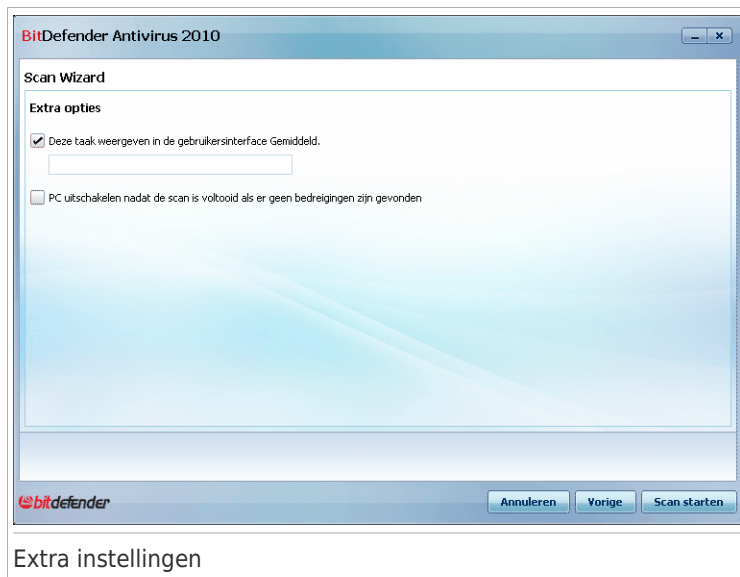
Optie	Beschrijving
Scannen op virussen	Scant op bekende virussen. BitDefender detecteert ook onvolledige virussen waardoor elke mogelijke bedreiging die de beveiliging van uw systeem kan beïnvloeden, wordt verwijderd.
Scannen op adware	Scant op adware-bedreigingen. Gedetecteerde bestanden zullen worden behandeld als geïnfecteerd. Software die adware-componenten bevat, zal mogelijk niet meer werken als deze optie is ingeschakeld.
Scannen op spyware	Scant op bekende spyware-bedreigingen. Gedetecteerde bestanden zullen worden behandeld als geïnfecteerd.
Scannen op applications	Scannen op legitieme applicaties die kunnen worden gebruikt voor spionage, voor het verbergen van kwaadwillende applicaties of voor andere kwaadwillende bedoelingen.
Scannen op dialers	Scant op toepassingen die dure nummers belt. Gedetecteerde bestanden zullen worden behandeld als geïnfecteerd. Software die dialer-componenten bevat, zal mogelijk niet meer werken als deze optie is ingeschakeld.
Scannen op rootkits	Scant op verborgen objecten (bestanden en processen), algemeen bekend als rootkits.
Scannen op keyloggers	Scan voor kwaadaardige toepassingen die toets aanslagen registreren.

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

Klik op **Volgende**.

11.2.4. Stap 4/6 - Extra instellingen

Voordat het scannen begint, zijn extra opties beschikbaar:



- Om de aangepaste taak die u voor toekomstig gebruik maakt op te slaan, schakelt u het selectievakje **Deze taak weergeven in de gebruikersinterface Gemiddeld** in en voert u de naam in voor de taak in het beschikbare bewerkingsveld.

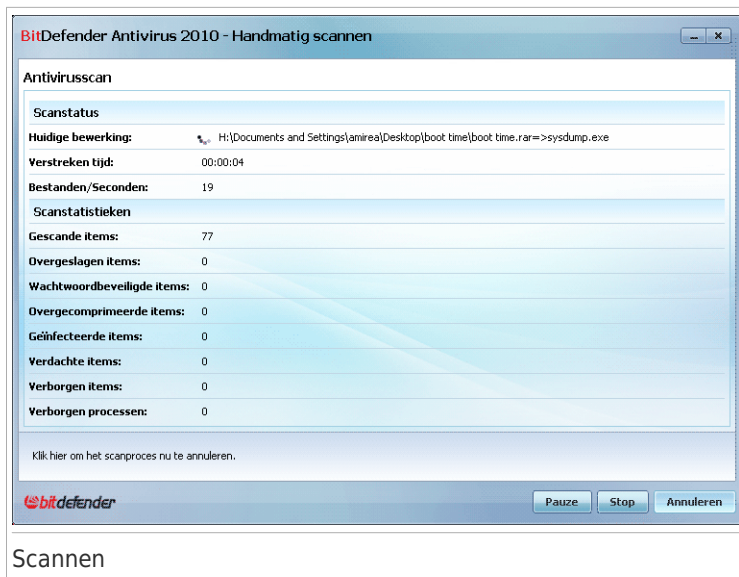
De taak zal aan de lijst van Vlugge Taken reeds verkrijgbaar in het Veiligheidslabel worden toegevoegd en zal ook verschijnen in **Deskundige Modus > Antivirus > Virus onderzoekende Blik**.

- Om de computer uit te schakelen nadat het scannen is voltooid, schakelt u het selectievakje **PC uitschakelen nadat de scan is voltooid als er geen bedreigingen zijn gevonden** in.

Klik op **Scannen starten**.

11.2.5. Stap 5/6 - Scannen

BitDefender start het scannen van de geselecteerde objecten:

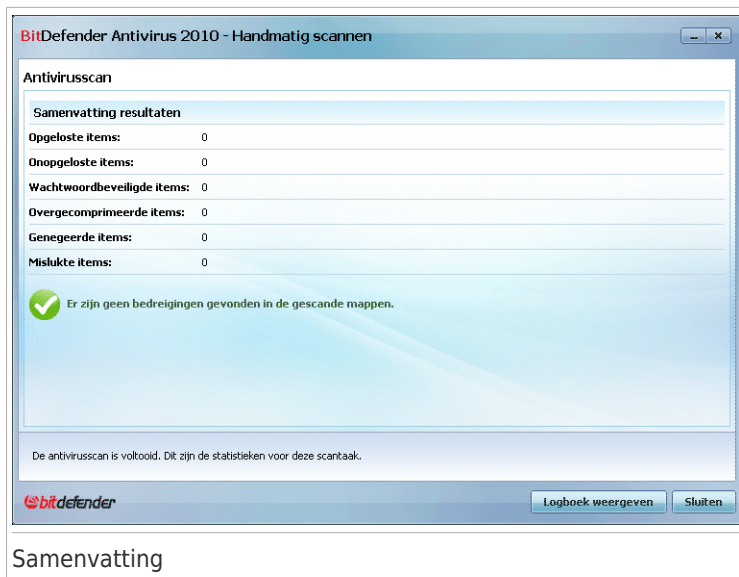


Opmerking

Afhankelijk van de complexiteit van de scan, kan het scanproces enige tijd in beslag nemen. U kunt op het pictogram voor de scanvoortgang  in het **stelsysteemvak** klikken om het scanvenster te openen en de scanvoortgang te bekijken.

11.2.6. Stap 6/6 - Resultaten weergeven

Wanneer BitDefender het scanproces voltooit, verschijnen de scanresultaten in een nieuw venster.



U kunt een samenvatting van de resultaten zien. Als u uitgebreide informatie over het scanproces wenst, klikt u op **Logboek weergeven** om het scanlogboek weer te geven.



Belangrijk

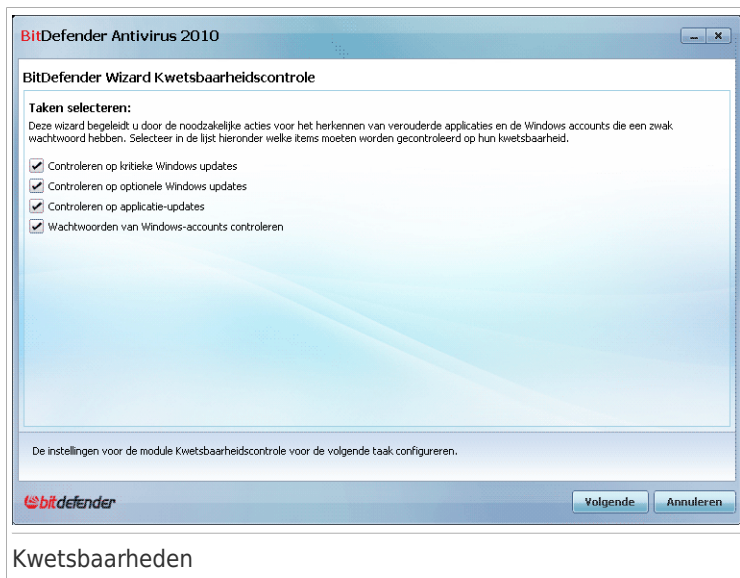
Start indien nodig uw systeem opnieuw, zodat het installatieprogramma de installatie kan voltooien.

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

11.3. Wizard Kwetsbaarheidscontrole

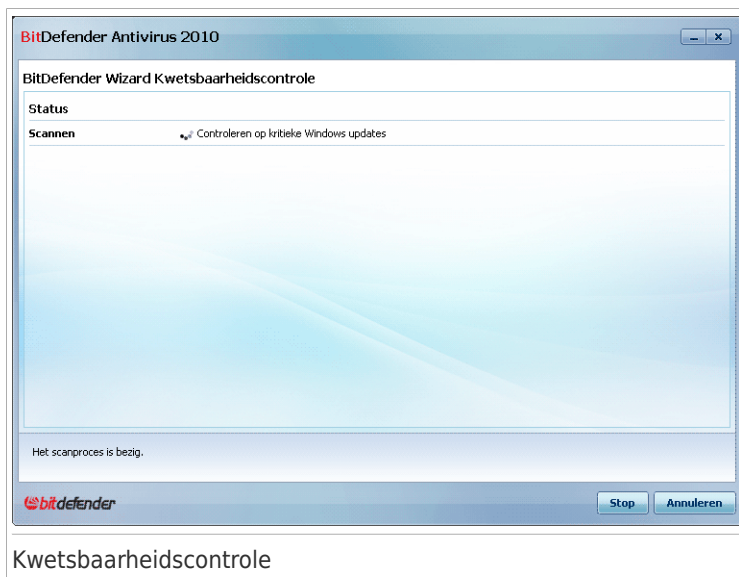
Deze wizard controleert het systeem op kwetsbaarheden en helpt u ze op te lossen.

11.3.1. Stap 1/6 - Te controleren kwetsbaarheden selecteren



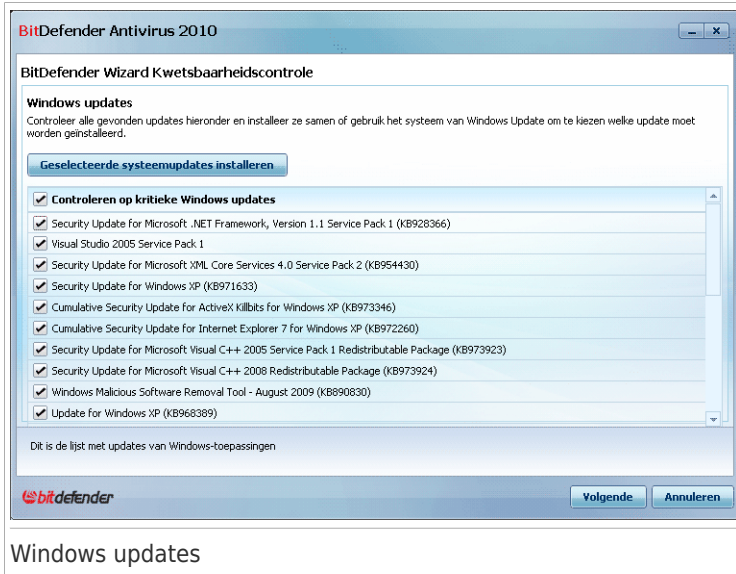
Klik op **Volgende** om het systeem op de geselecteerde kwetsbaarheden te controleren.

11.3.2. Stap 2/6 - Op kwetsbaarheden controleren



Wacht tot BitDefender de kwetsbaarheidscontrole heeft voltooid.

11.3.3. Stap 3/6 – Windows bijwerken



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

Klik op **Volgende**.

11.3.4. Stap 4/6 - Applicaties updaten



Applicaties

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

Klik op **Volgende**.

11.3.5. Stap 5/6 - Zwakke wachtwoorden wijzigen



U ziet de lijst van Windows gebruikersaccounts die zijn geconfigureerd op uw computer en de beschermingsniveaus van de wachtwoorden. Een wachtwoord kan **sterk** (moeilijk te raden) of **zwak** (gemakkelijk te kraken door boosaardige mensen met gespecialiseerde software) zijn.

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



Selecteer de methode voor het herstellen van dit probleem:

- **Gebruiker dwingen wachtwoord te veranderen bij volgend inloggen.** BitDefender vraagt de gebruiker het wachtwoord te veranderen als hij zich de volgende keer aanmeldt bij Windows.
- **Gebruikerswachtwoord veranderen.** U moet het nieuwe wachtwoord in de overeenkomende velden invoeren. Zorg dat u de gebruiker op de hoogte brengt van de wachtwoordwijziging.



Opmerking

Voor een sterk wachtwoord gebruikt u een combinatie van hoofdletters en kleine letters, getallen en speciale tekens (zoals #, \$ of @). U kunt op internet zoeken naar meer informatie en tips over het maken van sterke wachtwoorden.

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

Klik op **Volgende**.

11.3.6. Stap 6/6 - Resultaten weergeven



Klik op **Sluiten**.

Gemiddelde modus

12. Dashboard

Het tabblad Dashboard biedt informatie met betrekking tot de beveiligingsstatus van uw computer en biedt u de mogelijkheid problemen in behandeling op te lossen.



Het dashboard bestaat uit de volgende delen:

- **Algemene status** - geeft het aantal problemen aan dat uw computer beïnvloedt en helpt u ze op te lossen. Als er problemen in behandeling zijn, ziet u een **rode cirkel met een uitroepteken** en de knop **Alle problemen herstellen**. Klik op de knop om de wizard **Alle problemen herstellen** te starten.
- **Statusdetail** - Geeft de status aan van elke hoofdmodule door middel van uitdrukkelijke zinnen en een van de volgende pictogrammen:
 - ✔ **Groene cirkel met een vinkje:** Er zijn geen problemen die de beveiligingsstatus beïnvloeden. Uw computer en gegevens zijn beveiligd.
 - ⊗ **Grijze cirkel met een uitroepteken:** De activiteit van de componenten van deze module wordt niet bewaakt. Er is dan ook geen informatie beschikbaar met betrekking tot hun beveiligingsstatus. Er kunnen specifieke problemen zijn met betrekking tot deze module.
 - ❗ **Rode cirkel met een uitroepteken:** Er zijn problemen die de beveiliging van uw systeem beïnvloeden. Kritieke problemen vereisen uw onmiddellijke

aandacht. Niet-kritieke problemen moeten ook zo snel mogelijk worden aangepakt.

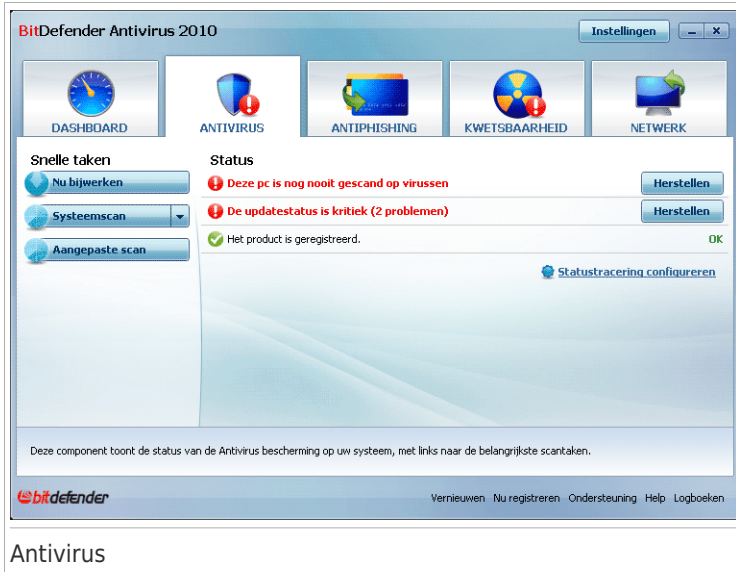
Klik op de naam van een module om meer details te zien over zijn status en om het opsporen van de status voor zijn componenten te configureren.

- **Gebruiksprofiel** - Geeft het gebruiksprofiel aan dat momenteel is geselecteerd en biedt een koppeling naar een relevant taak voor dat profiel:
 - ▶ Wanneer het profiel **Standaard** is geselecteerd, biedt de knop **Nu scannen** u de mogelijkheid een systeemscan uit te voeren met de **Antivirusscanwizard**. Het volledige systeem wordt gescand, behalve de archieven. In de standaardconfiguratie scant het systeem op alle types malware, behalve op **rootkits**.
 - ▶ Wanneer het profiel **Speler** is geselecteerd, kunt u met de knop **Spelmodus in-/uitschakelen** de **Spelmodus** in- en uitschakelen. De Spelmodus verandert tijdelijk de beveiligingsinstellingen om de snelheid van het systeem zo weinig mogelijk te beïnvloeden.
 - ▶ Wanneer het profiel **Aangepast** is geselecteerd, kunt u met de knop **Nu bijwerken** onmiddellijk een update starten. Een nieuw venster verschijnt waarin u de updatestatus kan zien.

Als u naar een ander profiel wilt schakelen of het profiel dat u momenteel gebruikt wilt wijzigen, klikt u op het profiel en volgt u de **configuratiewizard**.

13. Antivirus

BitDefender wordt geleverd met een Antivirusmodule waarmee u uw BitDefender up-to-date en uw computer virusvrij houdt. Klik op het tabblad **Antivirus** om de Antivirusmodule te openen.



De Antivirusmodule bestaat uit twee delen:

- **Statusgebied** - Toont de huidige status van de bewaakte beveiligingscomponenten en biedt u de mogelijkheid te kiezen welke componenten moeten worden bewaakt.
- **Snelle taken** - Hier vindt u koppelingen naar de belangrijkste beveiligingstaken: Nu bijwerken, Mijn documenten scannen, Systeem scannen, Diepe systeemsan en Aangepast scan.

13.1. Statusgebied

In het statusgebied vindt u de volledige lijst met componenten van de beveiligingsmodule en hun huidige status. Door elke beveiligingsmodule te bewaken, laat BitDefender u niet alleen weten wanneer u de instellingen configureert die de beveiliging van uw computer kunnen beïnvloeden, maar ook wanneer u belangrijke taken vergeet uit te voeren.

De huidige status van een component wordt aangeduid met expliciete zinnen en een van de volgende pictogrammen:

✓ **Groene cirkel met een vinkje:** Er zijn geen problemen die de component beïnvloeden.

❗ **Rode cirkel met een uitroepteken:** Er zijn problemen die de component beïnvloeden.

De zinnen die problemen beschrijven, worden in het rood geschreven. Klik op de knop **Herstellen** die overeenkomt met een zin om het gemelde probleem te herstellen. Als een probleem niet ter plaatse wordt opgelost, moet u de wizard volgen om het op te lossen.

13.1.1. Statustracing configureren

Om de componenten te selecteren die door BitDefender moeten worden bewaakt, klikt u op **Statustracing configureren** en schakelt u het selectievakje **Waarschuwingen inschakelen** in dat overeenkomt met de functies die u wilt volgen.



Belangrijk

Om zeker te zijn dat uw systeem volledig is beveiligd, moet u de tracing voor alle componenten inschakelen en alle gemelde problemen herstellen.

De status van de volgende beveiligingscomponenten kan door BitDefender worden gevolgd.

- **Antivirus** - BitDefender bewaakt de status van de twee componenten en de Antivirus-functie: real time-beveiliging en een scan op aanvraag. De meest algemene problemen die voor deze component zijn gerapporteerd, worden weergegeven in de volgende tabel.

Probleem	Beschrijving
Real-time bescherming is uitgeschakeld	De bestanden worden niet gescand omdat ze zijn geopend door u of door een toepassing die op dit systeem wordt uitgevoerd.
Deze pc is nog nooit gescand op virussen	Een systeemscan op aanvraag is nooit uitgevoerd om te controleren of de bestanden die op uw computer zijn opgeslagen, vrij zijn van malware.
De laatste systeemscan die u hebt gestart, is afgebroken voordat deze werd voltooid	Er is een volledige systeemscan gestart, maar niet voltooid.

Probleem	Beschrijving
Antivirus is in een kritieke status	De real time-beveiliging is uitgeschakeld en een systeemscan is te laat.

- **Update** - BitDefender controleert of de malwarehandtekeningen up-to-date zijn. De meest algemene problemen die voor deze component zijn gerapporteerd, worden weergegeven in de volgende tabel.

Probleem	Beschrijving
Automatische Update is uitgeschakeld	De malwarehandtekeningen van uw BitDefender-product worden niet automatisch bijgewerkt op regelmatige basis.
De update is niet uitgevoerd gedurende x dag(en).	De malware-handtekeningen van uw BitDefender-product zijn verouderd.

13.2. Snelle taken

Hier vindt u koppelingen naar de belangrijkste beveiligingstaken:

- **Update nu** - start een directe update.
- **Systeemscan** - start een volledige scan van uw computer (archieven uitgesloten). Voor extra scantaken op aanvraag, klikt u op deze knop  en selecteert u een andere scantaak: Mijn documenten scannen of Diepe systeemscan.
- **Aangepaste scan** - start een wizard waarmee u een aangepaste scantaak kunt maken en uitvoeren.

13.2.1. Updaten BitDefender

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

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



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

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

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



Opmerking

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

Start de computer indien nodig opnieuw op. Als het een belangrijke update betreft, wordt u gevraagd de computer opnieuw op te starten: Klik op **Herstarten** om uw systeem direct opnieuw op te starten.

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

13.2.2. Scannen met BitDefender

Om uw computer op malware te scannen, voert u een specifieke scantask uit door op de overeenkomende knop te klikken of door de taak in het vervolgkeuzemenu

te selecteren. In de volgende tabel staan de beschikbare scantaken met hun beschrijving:

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



Opmerking

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

Wanneer u Systeemscan, Diepe systeemscan of Mijn documenten scannen uitvoert, verschijnt de Antivirusscanwizard. Volg de begeleide procedure van drie stappen om het scanproces te voltooien. Raadpleeg "*Antivirusscanwizard*" (p. 58) voor gedetailleerde informatie over deze wizard.

Wanneer u een Aangepaste scan uitvoert, zal de wizard Aangepaste scan u begeleiden doorheen het scanproces. Volg de begeleide procedure van zes stappen om specifieke bestanden of mappen te scannen. Raadpleeg "*Wizard Aangepaste scan*" (p. 63) voor gedetailleerde informatie over deze wizard.

14. Antiphishing

BitDefender wordt geleverd met een Antiphishing-module die ervoor zorgt dat alle webpagina's die u bezoekt via Internet Explorer of Firefox, veilig zijn. Klik op het tabblad **Antiphishing** om de antiphishingmodule te openen.



De antiphishingmodule bestaat uit twee delen:

- **Statusgebied** - Toont de huidige status van de antiphishing-module en biedt u de mogelijkheid het volgen van de activiteit van deze module in/uit te schakelen.
- **Snelle taken** - Hier vindt u koppelingen naar belangrijke beveiligingstaken: Nu bijwerken, Systeemscaan en Diepe systeemscaan.

14.1. Statusgebied

De huidige status van een component wordt aangeduid met expliciete zinnen en een van de volgende pictogrammen:

- ✓ **Groene cirkel met een vinkje:** Er zijn geen problemen die de component beïnvloeden.
- ❗ **Rode cirkel met een uitroepteken:** Er zijn problemen die de component beïnvloeden.

De zinnen die problemen beschrijven, worden in het rood geschreven. Klik op de knop **Herstellen** die overeenkomt met een zin om het gemelde probleem te herstellen.

Het vaakst gemelde probleem voor deze module is **Antiphishing is uitgeschakeld**. Dit betekent dat Antiphishing niet is ingeschakeld voor alle of enkele van de volgende ondersteunde toepassingen. Internet Explorer, Mozilla Firefox, Yahoo! Messenger of Windows Live Messenger.

14.2. Snelle taken

Hier vindt u koppelingen naar de belangrijkste beveiligingstaken:

- **Update nu** - start een directe update.
- **Systeemscan** - start een volledige scan van uw computer (archieven uitgesloten).
- **Diepe systeemscan** - start een volledige scan van uw computer (inclusief archieven).

14.2.1. Updaten BitDefender

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

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



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

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

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



Opmerking

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

Start de computer indien nodig opnieuw op. Als het een belangrijke update betreft, wordt u gevraagd de computer opnieuw op te starten: Klik op **Herstarten** om uw systeem direct opnieuw op te starten.

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

14.2.2. Scannen met BitDefender

Om uw computer op malware te scannen, voert u een specifieke scantask uit door op de overeenkomende knop te klikken of door de taak in het vervolgkeuzemenu

te selecteren. In de volgende tabel staan de beschikbare scantaken met hun beschrijving:

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



Opmerking

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

Wanneer u een Systeemscan of Diepe systeemscan uitvoert, verschijnt de Antivirusscanwizard. Volg de begeleide procedure van drie stappen om het scanproces te voltooien. Raadpleeg "**Antivirusscanwizard**" (p. 58) voor gedetailleerde informatie over deze wizard.

15. Kwetsbaarheid

BitDefender heeft een kwetsbaarheidsmodule die helpt de cruciale software op uw PC up-to-date te houden. Om de zwakke punten van uw systeem te bewaken en op te lossen, klikt u op het tabblad **Kwetsbaarheid**.



De Kwetsbaarheidsmodule bestaat uit twee delen:

- **Statusgebied** - Toont de huidige status van de module Kwetsbaarheidscontrole en biedt u de mogelijkheid het volgen van de activiteit van deze module in/uit te schakelen.

- **Snelle taken** - Hier vindt u een koppeling naar de wizard Kwetsbaarheidscontrole:

15.1. Statusgebied

De huidige status van een component wordt aangeduid met expliciete zinnen en een van de volgende pictogrammen:

✓ **Groene cirkel met een vinkje:** Er zijn geen problemen die de component beïnvloeden.

! **Rode cirkel met een uitroepteken:** Er zijn problemen die de component beïnvloeden.

De zinnen die problemen beschrijven, worden in het rood geschreven. Klik op de knop **Herstellen** of **installeren** die overeenkomt met een zin om het gemelde probleem te herstellen.

De meest algemene problemen die voor deze component zijn gerapporteerd, worden weergegeven in de volgende tabel.

Status	Beschrijving
Kwetsbaarheidscontrole is uitgeschakeld	BitDefender controleert niet op potentiële kwetsbaarheden met betrekking tot ontbrekende Windows-updates, toepassingsupdates of zwakke wachtwoorden.
Er zijn meerdere kwetsbaarheden gedetecteerd	BitDefender heeft ontbrekende Windows/toepassingsupdates en/of zwakke wachtwoorden gevonden.
Kritieke Microsoft updates	Kritieke Microsoft-updates zijn beschikbaar, maar niet geïnstalleerd.
Andere Microsoft updates	Niet-kritieke Microsoft-updates zijn beschikbaar, maar niet geïnstalleerd.
Automatische Windows-updates zijn uitgeschakeld	De beveiligingsupdates van Windows worden niet automatisch geïnstalleerd zodra ze beschikbaar worden.
Toepassing (verouderd)	Er is een nieuwe versie van de Toepassing beschikbaar, maar niet geïnstalleerd.
Gebruiker (zwak wachtwoord)	Een gebruikerswachtwoord kan gemakkelijk worden gekraakt door boosaardige mensen met gespecialiseerde software.

15.2. Snelle taken

Er is slechts één taak beschikbaar:

- **Kwetsbaarheid scannen** - start een wizard die uw systeem controleert op zwakke punten en u helpt ze op te lossen.

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

Om uw computer te controleren op kwetsbaarheden, klikt u op **Kwetsbaarheidsscan** en volgt u de "*Wizard Kwetsbaarheidscontrole*" (p. 70).

16. Netwerk

Met de Netwerkmodule kan u de BitDefender producten die zijn geïnstalleerd op uw thuiscomputers beheren vanaf één enkele computer. Klik op het tabblad **Netwerk** om de netwerkmodule te openen.



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

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

16.1. Snelle taken

Aan het begin is er maar één knop beschikbaar.

- **Netwerk inschakelen** - hiermee kunt u het netwerkwachtwoord instellen en zo het netwerk maken of deelnemen aan het netwerk.

Na het koppelen van het netwerk verschijnen meer knoppen.

- **Netwerk uitschakelen** - hiermee kunt u het netwerk verlaten.
- **Computer toevoegen** - hiermee kunt u computers toevoegen aan uw netwerk.
- **Alles scannen** - hiermee kan u alle beheerde computers tegelijk scannen.
- **Alles updaten** - hiermee kan u alle beheerde computers tegelijk updaten.
- **Alles registreren** - hiermee kan u alle beheerde computers tegelijk registreren.

16.1.1. Het BitDefender netwerk koppelen

Volg deze stappen om het BitDefender thuisnetwerk te koppelen:

1. Klik op **Netwerk inschakelen**. U wordt gevraagd het thuisbeheer wachtwoord te configureren.



The screenshot shows a Windows-style dialog box titled 'BitDefender' with a close button (X) in the top right corner. The main title inside the dialog is 'Wachtwoord thuisnetwerk invoeren'. Below the title is a paragraph of text: 'Vanwege beveiligingsredenen is er een wachtwoord vereist om toe te treden tot een netwerk of om een netwerk te maken. Het zal de toegang tot uw computer via het thuisnetwerk beveiligen.' There are two text input fields: the first is labeled 'Wachtwoord:' and the second is labeled 'Wachtwoord herhalen:'. At the bottom of the dialog are two buttons: 'OK' and 'Annuleren'.

Wachtwoord configureren

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

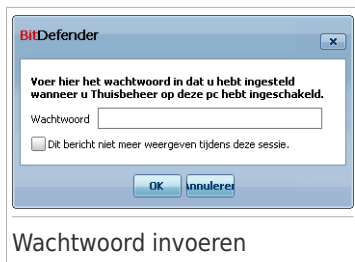
U ziet de naam van de computer in de netwerkmap.

16.1.2. bezig met toevoegen van computers aan het BitDefender netwerk

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

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

1. Klik op **Computer toevoegen**. U wordt gevraagd het lokale thuisbeheer wachtwoord in te voeren.



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



- U ziet de lijst van computers in het netwerk. Het pictogram betekent:
-  Een online computer zonder BitDefender producten.
 -  Een online computer met BitDefender producten.
 -  Een offline computer met BitDefender producten.
3. U kunt een van de volgende methoden gebruiken:
- In de lijst de naam van de toe te voegen computer selecteren.
 - Het IP-adres of de naam van de computer in het overeenkomende veld invoeren.
4. Klik op **Toevoegen**. U wordt gevraagd het thuismanagement wachtwoord van de betreffende computer in te voeren.



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

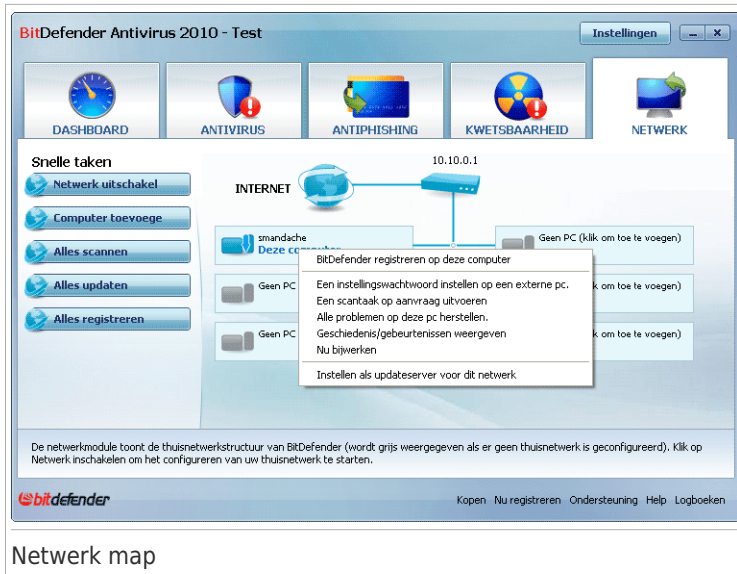


Opmerking

U kan maximaal vijf computers toevoegen aan de netwerkmap.

16.1.3. Het BitDefender netwerk beheren

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



Netwerk map

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

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

● **PC uit thuisnetwerk verwijderen**

Hiermee kunt u een pc uit het netwerk verwijderen.

● **BitDefender registreren op deze computer**

Hiermee kunt u BitDefender op deze computer registreren door een licentiesleutel in te voeren.

● **Een instellingswachtwoord instellen op een externe pc**

Hiermee kunt u een wachtwoord maken om de toegang tot de BitDefender-instellingen op deze pc te beperken.

● **Een scantaak op aanvraag uitvoeren**

Hiermee kunt u een scan op aanvraag maken op de externe computer. U kunt elk van de volgende scantaken uitvoeren: Mijn documenten scannen, Systeemscan of Diepe systeemscan.

● **Alle problemen op deze pc herstellen**

Hiermee kunt u de problemen die de veiligheid van uw computer beïnvloeden oplossen door de wizard **Alle problemen oplossen** te volgen.

● **Geschiedenis/gebeurtenissen weergeven**

Hiermee krijgt u toegang tot de module **Geschiedenis&gebeurtenissen** van het BitDefender-product dat op deze computer is geïnstalleerd.

● **Nu bijwerken**

Start het updateproces voor het BitDefender-product dat op deze computer is geïnstalleerd.

● **Instellen als updateserver voor dit netwerk**

Hiermee kunt u deze computer instellen als de updateserver voor alle BitDefender-producten die op de computers in dit netwerk zijn geïnstalleerd. Het gebruik van deze optie zal het internetverkeer beperken omdat slechts één computer in het netwerk een verbinding zal maken met internet om updates te downloaden.

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



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



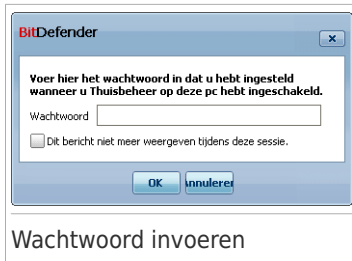
Opmerking

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

16.1.4. Alle computers scannen

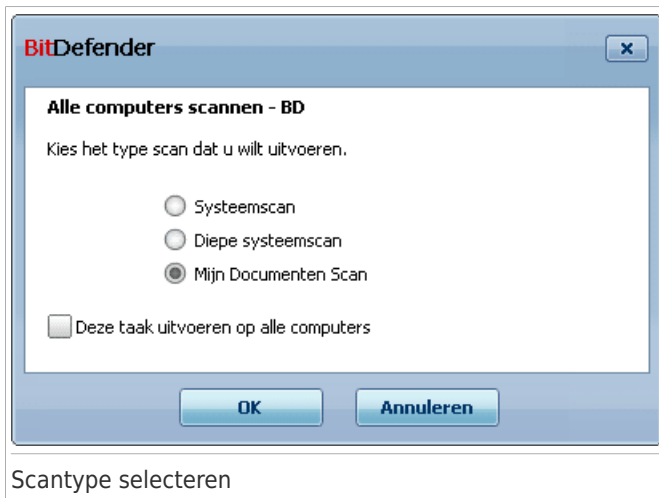
Volg deze stappen om alle beheerde computers te scannen:

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



2. Selecteer een scantype.

- **Systeemscan** - start een volledige scan van uw computer (archieven uitgesloten).
- **Diepe systeemscan** - start een complete scan van uw computer (inclusief archiefbestanden).
- **Mijn documenten scannen** - start een snelscan van uw documenten en instellingen.

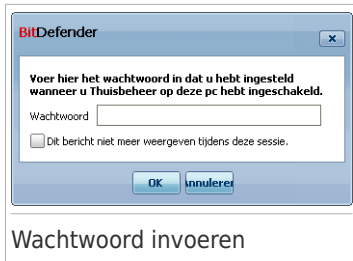


3. Klik op **OK**.

16.1.5. Alle computers updaten

Volg deze stappen om alle beheerde computer te updaten:

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

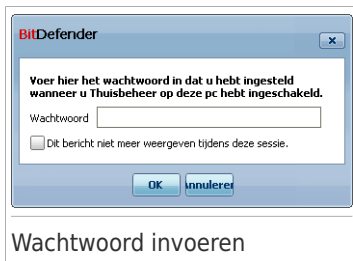


2. Klik op **OK**.

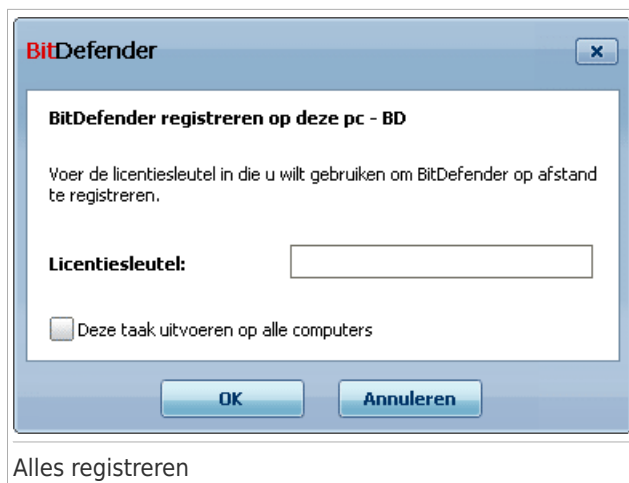
16.1.6. Alle computers registreren

Volg deze stappen om alle beheerde computers te registreren:

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



2. Voer de sleutel in waarmee u wilt registreren.



3. Klik op **OK**.

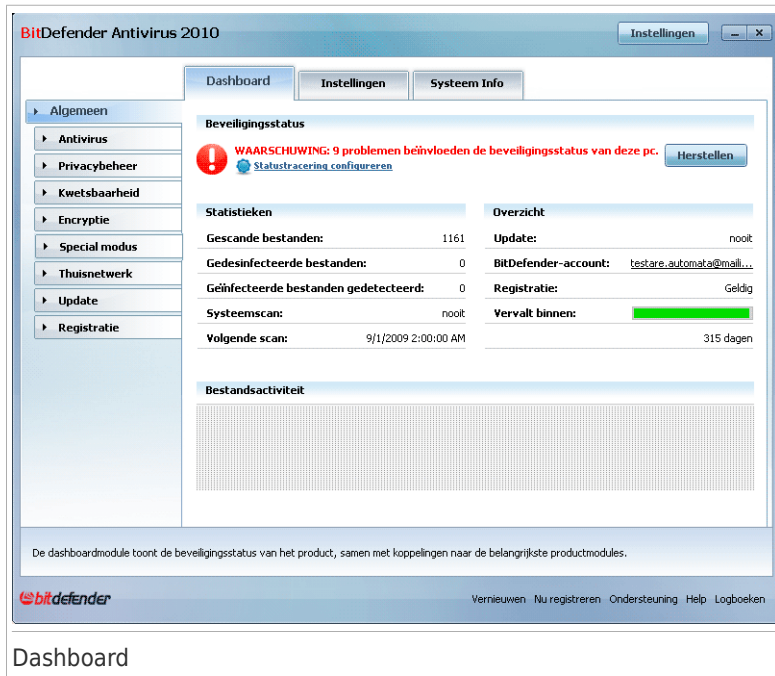
Expert-modus

17. Algemeen

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

17.1. Dashboard

Ga naar **Algemeen>Dashboard** in de Expert-modus om te zien of er problemen zijn die uw computer beïnvloeden. Hier ziet u ook statistieken van de productactiviteiten en uw registratiestatus.



Het dashboard bestaat uit verschillende delen:

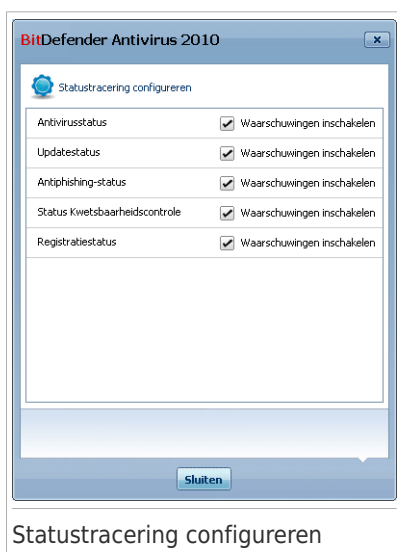
- **Algemene status** - Informeert u over problemen die de beveiliging van uw computer beïnvloeden.
- **Statistieken** - Toont belangrijke informatie over de BitDefender activiteit.
- **Overzicht** - Toont de updatestatus, uw accountstatus, registratie en licentie-informatie.

- **Bestandsactiviteit** - geeft de evolutie aan van het aantal objecten dat door BitDefender Antimalware is gescand. De hoogte van de balk geeft de intensiteit aan van het verkeer tijdens dat tijdsinterval.

17.1.1. Algemene status

Dit is waar u kunt zien hoeveel problemen de veiligheid van uw computer bedrijft. Klik op **Alle problemen herstellen** om alle bedreigingen te verwijderen. Hiermee wordt de wizard **Alle problemen herstellen** gestart.

Klik op **Statustracering configureren** om in te stellen welke modules zullen worden gevolgd door BitDefender Antivirus 2010. Een nieuw venster wordt weergegeven:



Indien u wilt dat BitDefender bepaalde componenten controleert, selecteer het **alarmselectievakje** dat beantwoordt aan die component. De status van de volgende beveiligingscomponenten kan door BitDefender worden gevolgd.

- **Antivirus** - BitDefender controleert de status van de twee componenten van de Antivirus module: en biedt direct bescherming en onderzoekt ook op nauwkeurig. De meest algemene problemen die voor deze component zijn gerapporteerd, worden weergegeven in de volgende tabel.

Probleem	Beschrijving
Real-time bescherming is uitgeschakeld	De bestanden worden niet gescand omdat ze zijn geopend door u of door een toepassing die op dit systeem wordt uitgevoerd.
U hebt uw computer nog nooit gescand op malware	Een systeemscan op aanvraag is nooit uitgevoerd om te controleren of de bestanden die op uw computer zijn opgeslagen, vrij zijn van malware.
De laatste systeemscan die u hebt gestart, is afgebroken voordat deze werd voltooid	Er is een volledige systeemscan gestart, maar niet voltooid.
Antivirus is in een kritieke status	De real time-beveiliging is uitgeschakeld en een systeemscan is te laat.

- **Update** - BitDefender controleert of de malwarehandtekeningen up-to-date zijn. De meest algemene problemen die voor deze component zijn gerapporteerd, worden weergegeven in de volgende tabel.

Probleem	Beschrijving
Automatische Update is uitgeschakeld	De malwarehandtekeningen van uw BitDefender-product worden niet automatisch bijgewerkt op regelmatige basis.
De update is niet uitgevoerd gedurende x dag(en).	De malware-handtekeningen van uw BitDefender-product zijn verouderd.

- **Antiphishing** - BitDefender bewaakt de status van de Antiphishing-functie. Als deze niet is ingeschakeld voor alle ondersteunde toepassingen, wordt het probleem **Antiphishing is uitgeschakeld** gerapporteerd.
- **Kwetsbaarheidscontrole** - BitDefender volgt de functie Kwetsbaarheidscontrole. Kwetsbaarheidscontrole laat u weten of u Windows-updates of toepassingsupdates moet installeren of als u wachtwoorden moet versterken.

De meest algemene problemen die voor deze component zijn gerapporteerd, worden weergegeven in de volgende tabel.

Status	Beschrijving
Kwetsbaarheidscontrole is uitgeschakeld	BitDefender controleert niet op potentiële kwetsbaarheden met betrekking tot ontbrekende

Status	Beschrijving
	Windows-updates, toepassingsupdates of zwakke wachtwoorden.
Er zijn meerdere kwetsbaarheden gedetecteerd	BitDefender heeft ontbrekende Windows/toepassingsupdates en/of zwakke wachtwoorden gevonden.
Kritieke Microsoft updates	Kritieke Microsoft-updates zijn beschikbaar, maar niet geïnstalleerd.
Andere Microsoft updates	Niet-kritieke Microsoft-updates zijn beschikbaar, maar niet geïnstalleerd.
Automatische Windows-updates zijn uitgeschakeld	De beveiligingsupdates van Windows worden niet automatisch geïnstalleerd zodra ze beschikbaar worden.
Toepassing (verouderd)	Er is een nieuwe versie van de Toepassing beschikbaar, maar niet geïnstalleerd.
Gebruiker (zwak wachtwoord)	Een gebruikerswachtwoord kan gemakkelijk worden gekraakt door boosaardige mensen met gespecialiseerde software.



Belangrijk

Om zeker te zijn dat uw systeem volledig is beveiligd, moet u de tracering voor alle componenten inschakelen en alle gemelde problemen herstellen.

17.1.2. Statistieken

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

Item	Beschrijving
Gescande bestanden	Geeft het aantal op malware gecontroleerde bestanden tijdens de laatste scan.
Gedesinfecteerde bestanden	Geeft het aantal gedesinfecteerde bestanden tijdens de laatste scan.
Geïnfecteerde bestanden gedetecteerd	Geeft het aantal geïnfecteerde bestanden aan dat op uw systeem is gevonden tijdens de laatste scan.
Laatste systeemscan	Geeft aan wanneer uw computer de laatste keer werd gescand. Als de laatste scan meer dan een week geleden is uitgevoerd, moet u uw computer zo snel mogelijk

Item	Beschrijving
	scannen. Om de volledige computer te scannen, gaat u naar Antivirus , tabblad Virusscan en voert u een Volledige systeemscan of een Diepe systeemscan uit.
Volgende scan	Geeft het volgende tijdstip aan waarop uw computer zal worden gescand.

17.1.3. Overzicht

Hier kunt u de updatestatus, uw accountstatus, registratie- en licentie-informatie weergeven.

Item	Beschrijving
Laatste update	Geeft aan wanneer uw BitDefender-product de laatste keer werd bijgewerkt. Voer regelmatige updates uit zodat u over een volledig beveiligd systeem beschikt.
BitDefender account	Geeft het e-mailadres dat u kan gebruiken om uw online account te openen en uw verloren BitDefender licentiesleutel op te halen, of te profiteren van BitDefender ondersteuning en andere aangepaste diensten. U moet een BitDefender-account maken om uw product te kunnen activeren. Raadpleeg " Registratie en Mijn account " (p. 52) voor meer informatie over de BitDefender-account
Registratie	Geeft het type en de status van uw licentiesleutel. Om uw systeem veilig te houden moet u BitDefender vernieuwen of upgraden als uw sleutel is verlopen.
Verloopt over	Geeft het aantal dagen tot het verlopen van uw licentiesleutel. Als uw licentiesleutel in de loop van de volgende dagen vervalst, moet u het product registreren met een nieuwe licentiesleutel. Om een licentiesleutel aan te schaffen of uw licentie te vernieuwen, klikt u onderaan in het venster op de koppeling Kopen/Verlengen .

17.2. Instellingen

Om de algemene instellingen voor BitDefender te configureren en zijn instellingen te beheren, gaat u in de Expert-modus naar **Algemeen>Instellingen**.



Algemene instellingen

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

17.2.1. Algemene instellingen

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



Opmerking

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

Als u deze optie selecteert, verschijnt het volgende venster:



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

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



Belangrijk

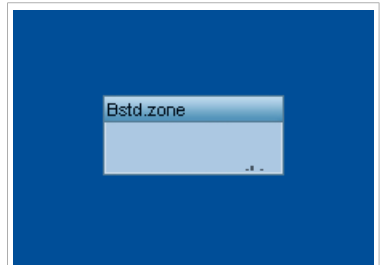
Als u uw wachtwoord vergeten bent, zult u het product moeten repareren om de BitDefender-configuratie te wijzigen.

- **BitDefender-nieuws weergeven (berichten i.v.m. beveiliging)** - toont af en toe beveiligingsberichten die door de BitDefender-server zijn verzonden met betrekking tot de uitbraak van virussen.
- **Pop-ups weergeven (notities op het scherm)** - toont pop-upvensters die betrekking hebben op de productstatus. U kunt BitDefender configureren om pop-ups alleen weer te geven wanneer de interface in de Beginnersmodus/Gemiddelde modus of alleen wanneer de interface in de Expert-modus is.
- **De balk Scanactiviteit weergeven (grafiek van productactiviteit op het scherm)** - toont de balk **Scanactiviteit** wanneer u zich aanmeldt bij Windows. Maak dit vakje leeg als u de Scanactiviteit balk niet langer wilt zien.



Opmerking

Deze optie kan alleen worden geconfigureerd voor de huidige Windows gebruiker. De balk Scanactiviteit is alleen beschikbaar wanneer de interface in de Expert-modus is.



Scan activiteitenbalk

17.2.2. Virusrapportinstellingen

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

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

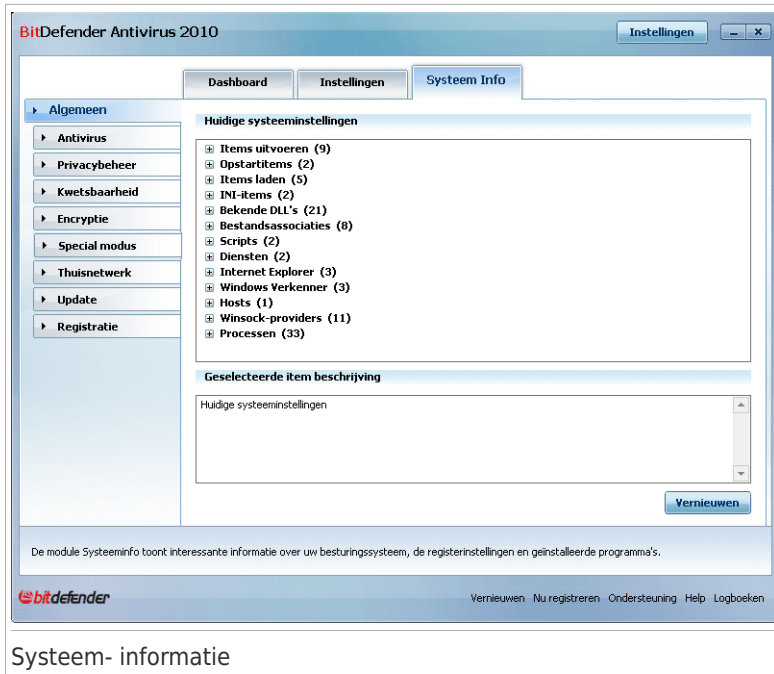
- **Uitbraakdetectie BitDefender inschakelen** - verzendt rapporten met betrekking tot potentiële virusuitbraken naar de BitDefender Labs.

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

17.3. Systeem- informatie

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

Om systeem informatie te verkrijgen, gaat u in de Expert-modus naar **Algemeen>Systeeminfo**.



Systeem- informatie

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

Er zijn drie knoppen beschikbaar:

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



Opmerking

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

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

18. Antivirus

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

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



Opmerking

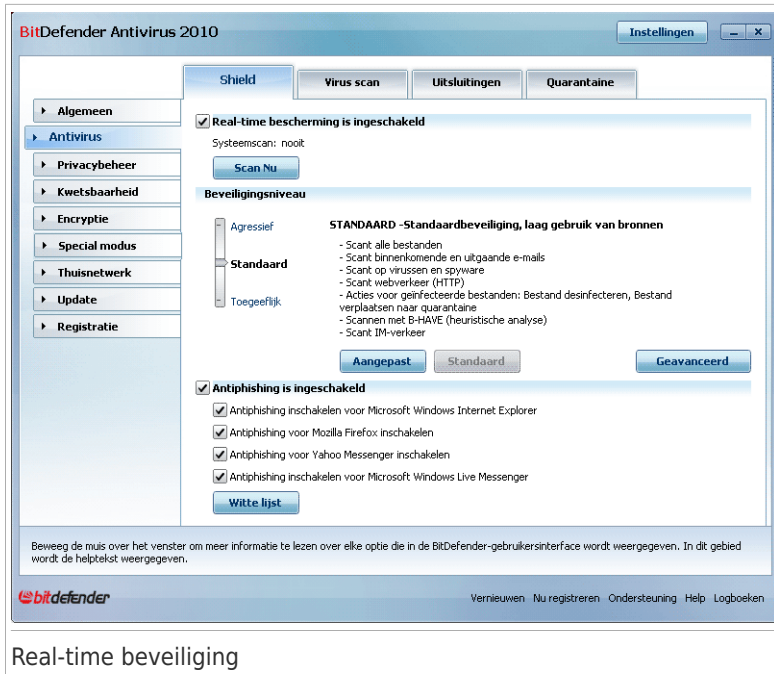
Real-time bescherming wordt ook wel on-access scannen geneemd - bestanden worden gescand als de gebruikers deze openen.

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

18.1. Real-time beveiliging

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

Ga naar **Antivirus>Shield** in de Expert-modus om de real time-beveiliging en BitDefender Antiphishing te configureren.



Real-time beveiliging

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



Belangrijk

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

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

18.1.1. Het beveiligingsniveau configureren

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

Er zijn 3 beveiligingsniveaus:

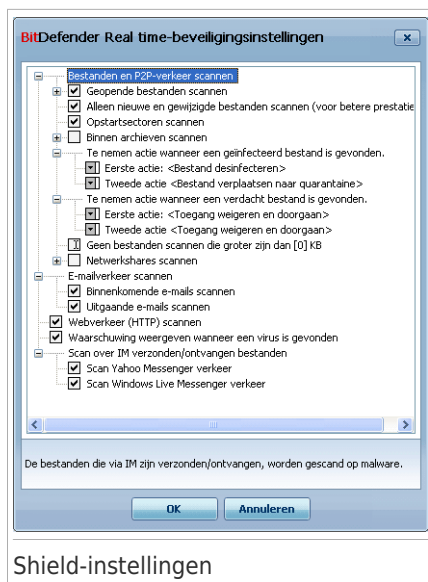
Beveiligingsniveau	Beschrijving
Toegeeflijk	Dekt de basisbehoeften aan beveiliging. Het verbruiksniveau van de bron is zeer laag. Alleen programma's en binnenkomende e-mailberichten worden op virussen gescand. Naast de klassieke op handtekeningen gebaseerde scan, wordt ook de heuristische analyse gebruikt.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

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

18.1.2. Het beveiligingsniveau aanpassen

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

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



Shield-instellingen

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



Opmerking

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

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

Optie	Beschrijving
Geopende bestanden scannen	Alle geopende bestanden worden gescand, ongeacht hun type.
Alleen toepassingen 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 ";".
Scannen op riskware	Scannen op riskware. Gedetecteerde bestanden zullen worden behandeld als geïnfecteerd. Software die adware-componenten bevat, zal mogelijk niet meer werken als deze optie is ingeschakeld. Selecteer Dialers en toepassingen overslaan bij het scannen en/of Keyloggers overslaan bij het scannen als u dit type bestanden wilt uitsluiten van de scan.
Alleen nieuwe en gewijzigde bestanden scannen	Scant alleen bestanden die niet eerder werden gescand of die werden gewijzigd sinds ze de laatste keer werden gescand. Door deze optie te selecteren, kunt u de algemene reactiviteit van uw systeem aanzienlijk verbeteren met een minimale inlevering op het vlak van beveiliging.
Opstartsectoren scannen	Scant de opstartsector van het systeem.
Binnen archieven scannen	De geopende archieven worden gescand. Wanneer u deze optie inschakelt, zal de computer langzamer werken. U kunt de maximale grootte voor te scannen archieven (in kilobytes; voer 0 in als u wilt dat alle archieven worden gescand) en de maximale archiefdiepte die moet worden gescand instellen.

Optie		Beschrijving
Eerste actie		Selecteer de eerste actie die moet worden genomen op geïnfecteerde en verdachte bestanden in het vervolgkeuzemenu.
	Toegang weigeren en doorgaan	Wanneer een geïnfecteerd bestand is gedetecteerd, zal de toegang tot dit bestand worden geweigerd.
	B e s t a n d desinfecteren	Verwijdert de malwarecode uit geïnfecteerde bestanden.
	B e s t a n d verwijderen	Verwijdert onmiddellijk de geïnfecteerde bestanden, zonder enige waarschuwing.
	B e s t a n d verplaatsen naar quarantaine	Verplaatst de geïnfecteerde bestanden naar de quarantaine. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer.
Tweede actie		Selecteer in het vervolgkeuzemenu de tweede actie die moet worden genomen op geïnfecteerde bestanden in het geval de eerste actie mislukt.
	Toegang weigeren en doorgaan	Wanneer een geïnfecteerd bestand is gedetecteerd, zal de toegang tot dit bestand worden geweigerd.
	B e s t a n d verwijderen	Verwijdert onmiddellijk de geïnfecteerde bestanden, zonder enige waarschuwing.
	B e s t a n d verplaatsen naar quarantaine	Verplaatst de geïnfecteerde bestanden naar de quarantaine. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer.
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.
Netwerkshares scannen	Alle bestanden scannen	Alle geopende bestanden van het netwerk worden gescand, ongeacht hun type.
	A l l e e n toepassingen scannen	Alleen de programmabestanden worden gescand. Dit betekent alleen bestanden met de volgende extensies: .exe; .bat; .com;

Optie	Beschrijving
	.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 ";".

● **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.

● **Webverkeer (HTTP) scannen** - scant het http-verkeer.

● **Waarschuwing weergeven wanneer een virus is gevonden** - opent een waarschuwingsvenster wanneer een virus wordt gevonden in een bestand of in een e-mailbericht.

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

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

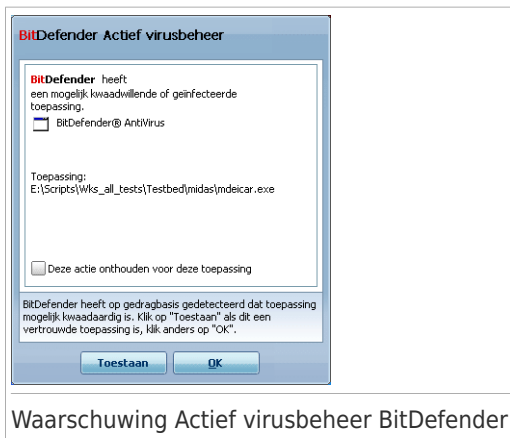
● **Via IM ontvangen/verzonden bestanden scannen.** Selecteer de overeenkomende vakjes om bestanden te scannen die u ontvangt of verzendt via Yahoo Messenger of Windows Live Messenger.

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

18.1.3. Instellingen Actief virusbeheer configureren

Actief virusbeheer van BitDefender biedt een beschermingslaag tegen nieuwe bedreigingen waarvan nog geen signatures bekend zijn. Hij bewaakt en analyseert voortdurend het gedrag van de applicaties op uw computer en waarschuwt als een applicatie zich verdacht gedraagt.

Actief virusbeheer kan worden geconfigureerd om u te waarschuwen en u te vragen actie te ondernemen wanneer een toepassing probeert een mogelijk boosaardige actie uit te voeren.

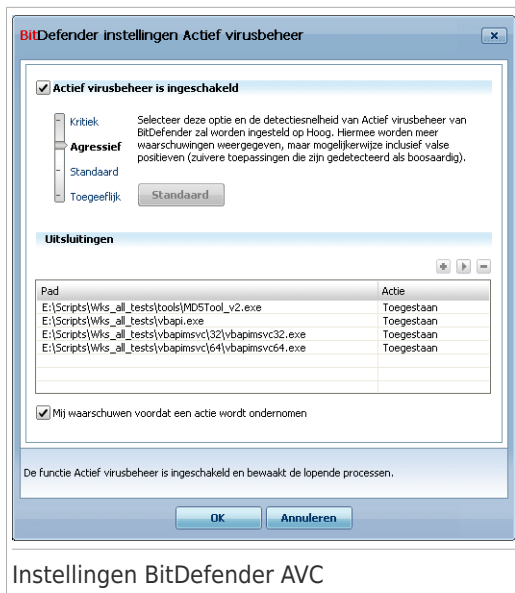


Klik op **Toestaan** als u de gedetecteerde applicatie vertrouwt.

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

Schakel het selectievakje **Deze actie onthouden voor deze toepassing** in voordat u een keuze maakt. Hierdoor zal BitDefender in de toekomst dezelfde actie ondernemen voor de gedetecteerde toepassing. De regel die op deze manier wordt gemaakt, wordt weergegeven in de tabel onder **Uitsluitingen**.

Om Actief virusbeheer te configureren, klikt u op **BD AVC-instellingen**.



Schakel het overeenkomende selectievakje in om Actief virusbeheer in te schakelen.



Belangrijk

Houd Actief virusbeheer ingeschakeld om beschermd te zijn tegen onbekende virussen.

Als u wilt dat Actief virusbeheer u waarschuwt en u vraagt actie te ondernemen wanneer een toepassing probeert een mogelijk boosaardige actie te ondernemen, schakelt u het selectievakje **Mij waarschuwen voordat een actie wordt ondernomen** in.

Het beschermingsniveau configureren

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



Opmerking

Als u het huidige real time-beschermingsniveau verandert, moet u ermee rekening houden dat het beschermingsniveau van Actief virusbeheer overeenkomstig verandert. Als u een real time beveiliging instelt op **Toegeeflijk**, wordt Actief virusbeheer van BitDefender automatisch uitgeschakeld en kunt u dit niet configureren.

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

Beveiligingsniveau	Beschrijving
Kritiek	Strikte bewaking van alle toepassingen voor mogelijke kwaadaardige acties.
Standaard	De detectiepercentages zijn hoog en valse positieven zijn mogelijk.
Gemiddeld	Er is een gematigde bewaking van de toepassing en sommige valse positieven zijn nog steeds mogelijk.
Toegeeflijk	De detectiepercentages zijn laag en er zijn geen valse positieven.

De lijst van vertrouwde/niet-vertrouwde toepassingen beheren

U kunt toepassingen die u kent en vertrouwt toevoegen aan de lijst met vertrouwde toepassingen. Deze toepassingen zullen niet langer door Actief virusbeheer van BitDefender worden gecontroleerd en zullen automatisch toegang krijgen. Toepassingen waarvoor u de toegang altijd wilt weigeren, kunnen op dezelfde manier worden toegevoegd aan de lijst met niet-vertrouwde toepassingen en Actief virusbeheer van BitDefender zal ze automatisch blokkeren.

De toepassingen waarvoor u regels hebt gemaakt, worden weergegeven in de tabel onder **Uitsluitingen**. Het pad naar de toepassing en de actie die u hiervoor hebt ingesteld (Toegelaten of Geblokkeerd) wordt weergegeven voor elke regel.

Om de lijst te beheren gebruikt u de knoppen die boven de tabel zijn geplaatst.

-  **Toevoegen** - hiermee kunt u een nieuwe toepassing toevoegen aan de lijst.
-  **Verwijderen** - een toepassing verwijderen uit de lijst.
-  **Bewerken** - een toepassingsregel bewerken.

18.1.4. Real time-beveiliging uitschakelen

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



Waarschuwing

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

18.1.5. Antiphishing bescherming configureren

BitDefender biedt real-time antiphishing bescherming voor:

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

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

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



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

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



Opmerking

Met behulp van de werkbalk van BitDefender Antiphishing, die in uw webbrowser is geïntegreerd, kan u gemakkelijk websites toevoegen aan de witte lijst. Meer informatie vindt u onder "*Integratie in webbrowsers*" (p. 220).

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

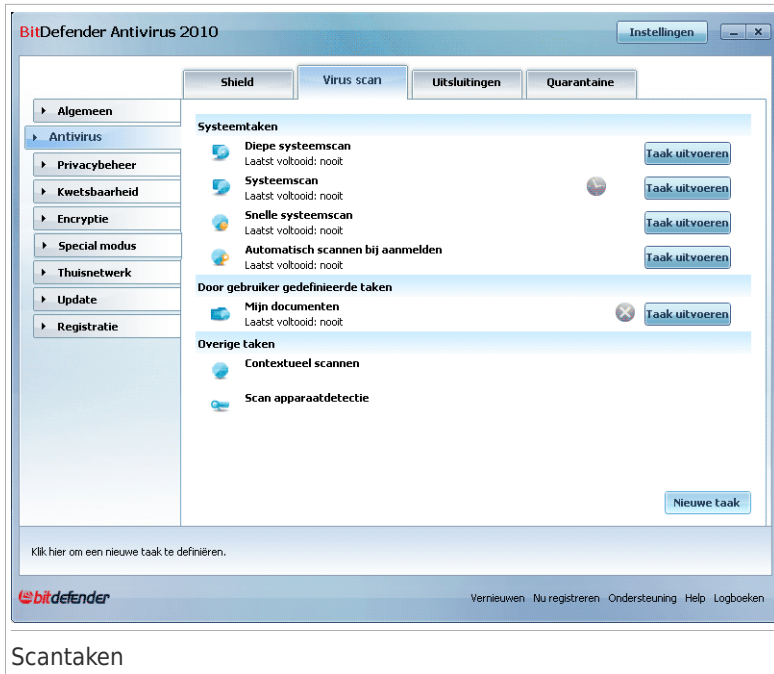
Klik op **Save** om de wijzigingen op te slaan en het venster te sluiten.

18.2. Scannen op aanvraag

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

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

Ga naar **Antivirus>Virusscan** in de Expert-modus om scannen op aanvraag te configureren en te starten.



Scantaken

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

18.2.1. Scantaken

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

Elke taak heeft een venster **Eigenschappen** waarmee u de taak kunt configureren en de scanresultaten kunt weergeven. Meer informatie vindt u onder "*Scantaken configureren*" (p. 126).

Er zijn drie categorieën scantaken:

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

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



Opmerking

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

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

Er wordt een taak geleverd met de naam **Mijn documenten**. Gebruik deze taak om belangrijke mappen van de huidige gebruiker te scannen. **Mijn documenten**, **Bureaublad** en **Opstarten**. Dit zal de veiligheid van uw documenten, een veilige werkruimte en opgeruimde toepassingen bij het opstarten garanderen.

● **Diverse taken** - bevat een lijst van diverse scantaken. Deze scantaken verwijzen naar alternatieve scantypes die vanaf dit venster kunnen worden uitgevoerd. U kunt alleen hun instellingen wijzigen of de scanrapporten weergeven.

Rechts van elke taak zijn drie knoppen beschikbaar:

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



Opmerking

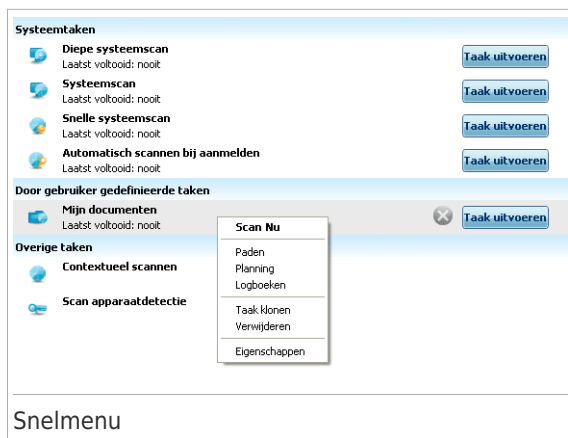
Niet beschikbaar voor systeemtaken. U kunt geen systeemtaak verwijderen.

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

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

18.2.2. Het snelmenu gebruiken

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



De volgende opdrachten zijn beschikbaar in het snelmenu:

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



Opmerking

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

- **Planning** - opent het venster **Eigenschappen**. Klik op het tabblad **Planner** waar u de geselecteerde taak kunt plannen.
- **Logboeken weergeven** - hiermee opent u het venster **Eigenschappen**. Op het tabblad **Logboeken** kunt u de rapporten zien die worden gegenereerd nadat de geselecteerde taak is uitgevoerd.
- **Taak klonen** - hiermee dupliciert u de geselecteerde taak. Dit is nuttig wanneer u nieuwe taken maakt omdat u de instellingen van een duplicaat van de taak kunt wijzigen.
- **Verwijderen** - verwijdert de geselecteerde taak.



Opmerking

Niet beschikbaar voor systeemtaken. U kunt geen systeemtaak verwijderen.

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



Opmerking

Door de specifieke aard van de categorie **Overige taken**, zijn alleen de opties **Logboeken weergeven** en **Eigenschappen** beschikbaar in dit geval.

18.2.3. Scantaken maken

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

- U kunt een bestaande taak **Klonen**, de naam van de taak wijzigen en de nodige wijzigingen aanbrengen in het venster **Eigenschappen**.
- Klik op **Nieuwe taak** om een nieuwe taak te maken en te configureren.

18.2.4. Scantaken configureren

Elke scantaak heeft zijn eigen venster **Eigenschappen** waarin u de scanopties kunt configureren, het scandoel kunt instellen, de taak kunt plannen of rapporten kunt weergeven. Klik links van de taak op de knop **Eigenschappen** (of klik met de rechtermuisknop op de taak en klik vervolgens op **Eigenschappen**) om dit venster te openen.



Opmerking

Meer informatie over het weergeven van logboeken en het tabblad **Logboeken**, vindt u onder "**Scanlogs weergeven**" (p. 146).

Scaninstellingen configureren

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



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

Het scanniveau selecteren

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

Er zijn 3 scanniveaus:

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

Beveiligingsniveau	Beschrijving
	Alle bestanden en archieven worden gescand op virussen en spyware. Naast de klassieke op handtekeningen gebaseerde scan, wordt ook de heuristische analyse gebruikt.

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

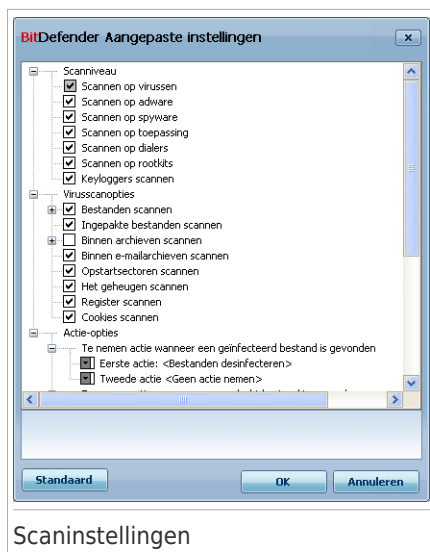
- **De taak uitvoeren met lage prioriteit.** Verlaagt de prioriteit van het scanproces. U zult andere programma's sneller kunnen uitvoeren en de tijd die nodig is om het scanproces te voltooien, verlengen.
- **Scanwizard minimaliseren naar taakbalk.** Minimaliseert het scanvenster naar het **systeembak**.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

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

Het scanniveau aanpassen

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

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



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

De scanopties zijn gegroepeerd in drie categorieën:

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

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

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

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

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

Optie	Beschrijving
	chm-archieven in als u wilt dat deze bestandstypes worden gescand. Scannen van gearhiveerde bestanden verlengt de scantijd en vereist meer systeembronnen. U kunt de maximale grootte van de archieven die moeten worden gescand instellen in kilobytes (KB) door de grootte in het veld Gescand archiefbestand beperken tot in te voeren.
Binnen e-mailarchieven scannen	Scant binnen e-mailarchieven.
Opstartsectoren scannen	Scant de opstartsector van het systeem.
Geheugen scannen	Scant het geheugen op virussen en andere malware.
Register scannen	Scant registergegevens.
Cookies scannen	Scant cookiebestanden.

- **Actie-opties.** Geef de acties op die moeten worden ondernomen voor elke categorie gedetecteerde bestanden met de opties in deze categorie.



Opmerking

Om een nieuwe actie in te stellen, klikt u op de huidige **Eerste actie** en selecteert u de gewenste optie in het menu. Geef een **Tweede actie** op die moet worden ondernomen in het geval de eerste mislukt.

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

Actie	Beschrijving
Geen actie nemen	Er wordt geen actie ondernomen voor geïnfecteerde bestanden. Deze bestanden zullen verschijnen in het rapportbestand.
Bestanden desinfecteren	De malware code van de geïnfecteerde bestanden verwijderen.
Bestanden verwijderen	Verwijdert onmiddellijk de geïnfecteerde bestanden, zonder enige waarschuwing.
Bestanden verplaatsen naar quarantaine	Verplaatst de geïnfecteerde bestanden naar de quarantaine. In quarantaine geplaatst bestanden

Actie	Beschrijving
	kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer.

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

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



Opmerking

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

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

Actie	Beschrijving
Geen actie nemen	Er wordt geen actie ondernomen voor verborgen bestanden. Deze bestanden zullen verschijnen in het rapportbestand.
Naam bestanden wijzigen	Wijzigt de naam van verborgen bestanden door .bd. ren toe te voegen aan hun naam. Hierdoor zult u dergelijke bestanden op uw computer kunnen zoeken en vinden, als die er zijn.
Bestanden verplaatsen naar quarantaine	Verplaatst de verborgen bestanden naar de quarantaine. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer.



Opmerking

Houd ermee rekening dat deze verborgen bestanden geen bestanden zijn die u opzettelijk verbergt voor Windows. Het zijn de bestanden die worden verborgen door speciale programma's, bekend als rootkits. Rootkits zijn in wezen niet kwaadaardig. Ze worden echter algemeen gebruikt om ervoor te zorgen dat virussen en spyware niet detecteerbaar zijn voor normale antivirusprogramma's.

► Actieopties voor wachtwoordbeveiligde en gecodeerde bestanden.

Bestanden die met Windows zijn gecodeerd, kunnen belangrijk zijn voor u. Dat is de reden waarom u verschillende acties kunt configureren die moeten worden ondernomen op de geïnfecteerde of verdachte bestanden die met Windows zijn gecodeerd. De wachtwoordbeveiligde archieven vormen een andere categorie van bestanden die speciale acties vereisen. Met een wachtwoord beveiligde archieven kunnen niet worden gescand, tenzij u het wachtwoord opgeeft. Gebruik deze opties om de acties te configureren die moeten worden ondernomen op wachtwoordbeveiligde archieven en op met Windows gecodeerde bestanden;

- **Te nemen actie wanneer een geïnfecteerd gecrypteerd bestand is gevonden.** Selecteer de actie die moet worden ondernomen op geïnfecteerde bestanden die met Windows zijn gecodeerd. De volgende opties zijn beschikbaar:

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

- **Te nemen actie wanneer een verdacht gecrypteerd bestand is gevonden.** Selecteer de actie die moet worden ondernomen op verdachte bestanden die met Windows zijn gecodeerd. De volgende opties zijn beschikbaar:

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

- **Te nemen actie wanneer een met een wachtwoord beveiligd bestand is gevonden.** Selecteer de actie die moet worden genomen voor de met een wachtwoord beschermde bestanden. De volgende opties zijn beschikbaar:

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

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

Het scandoel instellen

Om het scandoel van een specifieke scantaak van de gebruiker in te stellen, klikt u met de rechtermuisknop op de taak en selecteert u **Paden**. Als u al in het venster Eigenschappen van een taak bent, kunt u ook het tabblad **Paden** selecteren. Het volgende venster wordt geopend:



Scandoel

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

Dit onderdeel bevat de volgende knoppen:

- **Map(pen) toevoegen** - opent een zoekvenster waarin u de bestanden/mappen die u wilt scannen, kunt selecteren.



Opmerking

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

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



Opmerking

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

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

- **Lokale stations** - om de lokale stations te scannen.
- **Netwerkstations** - om alle netwerkstations te scannen.

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



Opmerking

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

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

Scandoel van systeemtaken bekijken

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

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



Scandoel van Volledige systeemscaan

Systeemscaan en **Diepe systeemscaan** zal alle lokale stations scannen, terwijl **Snelle systeemscaan** alleen de mappen van Windows en van Program Files zal scannen.

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

Scantaken plannen

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

Om de planning van een specifieke taak weer te geven of te wijzigen, klikt u met de rechtermuisknop op de taak en selecteert u **Planning**. Als u al in het venster Eigenschappen van een taak bent, selecteert u het tabblad **Planner**. Het volgende venster wordt geopend:



Als er een taakplanning is, kunt u deze bekijken.

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

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

Selecteer **Periodiek** als u wilt dat het scannen met bepaalde intervallen wordt herhaald en geef het aantal minuten/uren/dagen/weken/maanden/jaren op in het bewerkingsvak **Elke** om de frequentie van dit proces aan te geven. U moet ook de startdatum en het starttijdstip opgeven in de velden **Startdatum/Starttijd**.

- **Bij opstarten van het systeem** - start de scan na het aangegeven aantal minuten nadat de gebruiker zich heeft aangemeld bij Windows.

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

18.2.5. Bestanden en mappen scannen

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



Opmerking

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

Scantips

Hier vindt u enkele scantips die wellicht nuttig zijn voor u:

- Afhankelijk van de grootte van uw harde schijf, kan het uitvoeren van een uitgebreide scan van uw computer (zoals een Diepe systeemscan of een Systeemscan) enige tijd in beslag nemen (tot één uur of zelfs langer). Wij raden u daarom aan dergelijke scans uit te voeren wanneer u de computer gedurende langere tijd niet zult gebruiken (bijvoorbeeld 's nachts).

U kunt de start **het scannen plannen** op een geschikter tijdstip. Zorg dat u de computer ingeschakeld houdt. Met Windows Vista moet u ervoor zorgen dat uw computer niet in de slaapstand is op het ogenblik waarop de geplande taak wordt uitgevoerd.

- Als u vaak bestanden downloadt van internet naar een specifieke map, moet u een nieuwe scantaak maken en **die map instellen als scandoel**. De taak plannen om dagelijks of vaker te worden uitgevoerd.
- Er bestaat een soort malware dat zichzelf instelt om te worden uitgevoerd bij het opstarten van het systeem door de Windows-instellingen te wijzigen. Om uw computer tegen dergelijke malware te beschermen, kunt u de taak **Automatisch scannen bij aanmelden** plannen om te worden uitgevoerd bij het opstarten van het systeem. Houd ermee rekening dat het automatisch scannen bij aanmelden de systeemprestaties voor een korte tijd na het opstarten kan beïnvloeden.

Scanmethoden

BitDefender biedt u vier types voor het scannen op aanvraag:

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

Onmiddellijk scannen

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

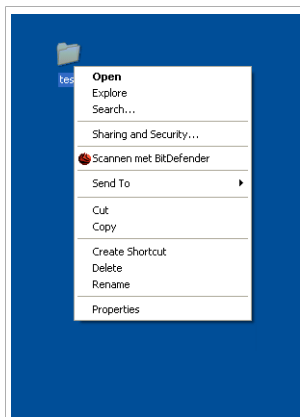
Gebruik een van de volgende methoden om een scantaak uit te voeren:

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

De **Antivirusscanwizard** wordt weergegeven en begeleidt u doorheen het scanproces.

Contextueel scannen

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



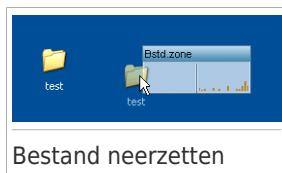
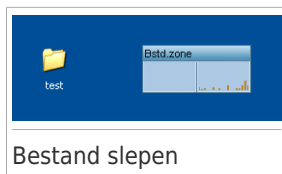
Contextueel scannen

Klik met de rechtermuisknop op het bestand of de map die u wilt scannen en selecteer **Scannen met BitDefender**. De **Antivirusscanwizard** wordt weergegeven en begeleidt u doorheen het scanproces.

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

Scannen door slepen & neerzetten

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



De **Antivirusscanwizard** wordt weergegeven en begeleidt u doorheen het scanproces.

Handmatig scannen

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



Opmerking

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

Om het object dat door BitDefender moet worden gescand te selecteren, gebruikt u het menu Start van Windows en volgt u het pad **Start** → **Programma's** → **BitDefender 2010** → **BitDefender Handmatig scannen**. Het volgende venster wordt geopend:



Handmatig scannen

Klik op **Map toevoegen**, selecteer de locatie die u wilt scannen en klik op **OK**. Als u meerdere mappen wilt scannen, herhaalt u deze actie voor elke extra locatie.

De paden naar de geselecteerde locaties zullen verschijnen in de kolom **Scandoel**. Als u de locatie toch niet wilt gebruiken, klik dan op de knop **Verwijderen** ernaast. Klik op de knop **Alle paden verwijderen** om alle locaties die aan de lijst zijn toegevoegd, te verwijderen.

Klik op **Doorgaan** wanneer u klaar bent met het selecteren van de locaties. De **Antivirusscanwizard** wordt weergegeven en begeleidt u doorheen het scanproces.

Antivirusscanwizard

Wanneer u een scan op aanvraag start, verschijnt de Antivirusscanwizard. Volg de begeleide procedure van drie stappen om het scanproces te voltooien.

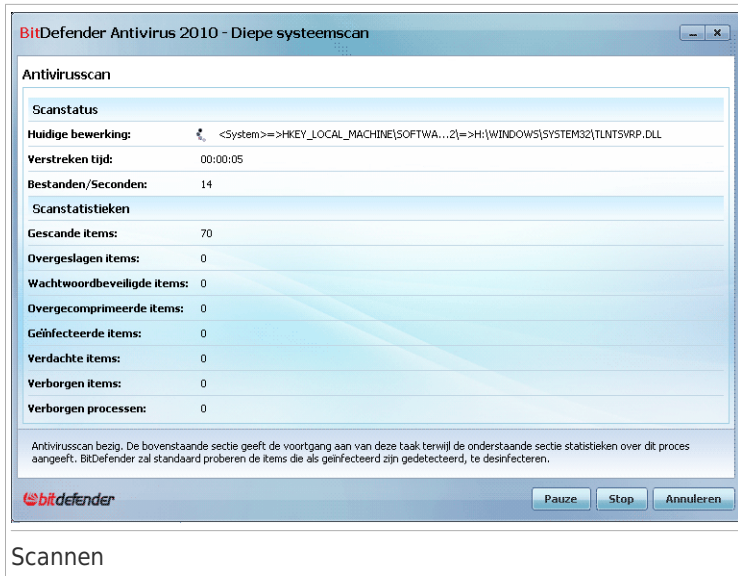


Opmerking

Als de scanwizard niet verschijnt, kan de scan worden geconfigureerd om stil te worden uitgevoerd op de achtergrond. Zoek het pictogram voor de scanvoortgang  in het **systeemvak**. U kunt op dit pictogram klikken om het scanvenster te openen en de scanvoortgang te bekijken.

Stap 1/3 - Scannen

BitDefender start het scannen van de geselecteerde objecten.



Scannen

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

Wacht tot BitDefender het scannen beëindigt.



Opmerking

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

Wachtwoordbeveiligde archieven. Als BitDefender een wachtwoordbeveiligd archief detecteert tijdens een scan en de standaardactie **Wachtwoord vragen** is, wordt u gevraagd het wachtwoord in te voeren. Met een wachtwoord beveiligde archieven kunnen niet worden gescand, tenzij u het wachtwoord opgeeft. De volgende opties zijn beschikbaar:

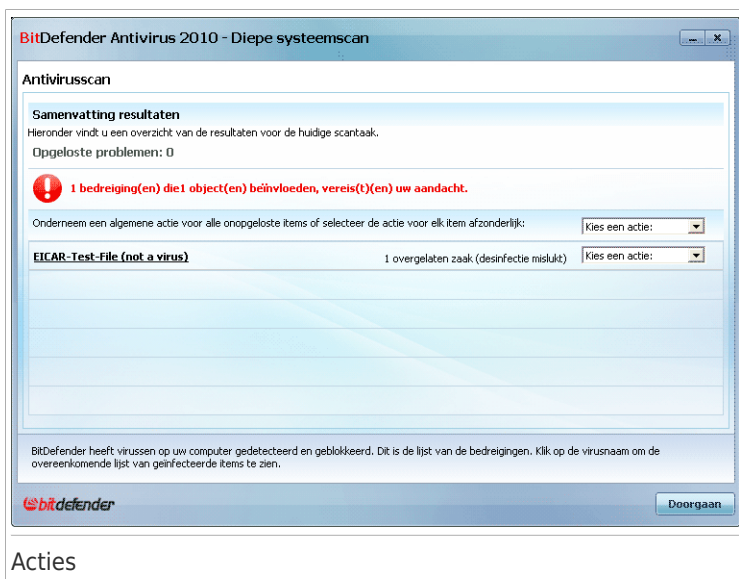
- **Wachtwoord.** Als u wilt dat BitDefender het archief scant, moet u deze optie selecteren en het wachtwoord invoeren. Als u het wachtwoord niet kent, kies dan een van de andere opties.
- **Geen wachtwoord vragen en dit object overslaan bij het scannen.** Selecteer deze optie om het scannen van dit archief over te slaan.
- **Alle wachtwoordbeveiligde items overslaan zonder ze te scannen.** Selecteer deze optie als u niet wilt worden lastig gevallen met betrekking tot wachtwoordbeveiligde archieven. BitDefender zal ze niet kunnen scannen, maar er wordt wel een gegeven bewaard in het scanlogboek.

Klik op **OK** om door te gaan met scannen.

De scan stoppen of pauzeren. U kunt het scannen op elk ogenblik stoppen door op **Stop&Ja** te klikken. U gaat dan rechtstreeks naar de laatste stap van de wizard. Klik op **Pauze** om het scanproces tijdelijk te stoppen. Om het scannen te hervatten, klikt u op **Hervatten**.

Stap 2/3 - Acties selecteren

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



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

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

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

Een of meerdere van de volgende opties kunnen in het menu verschijnen.

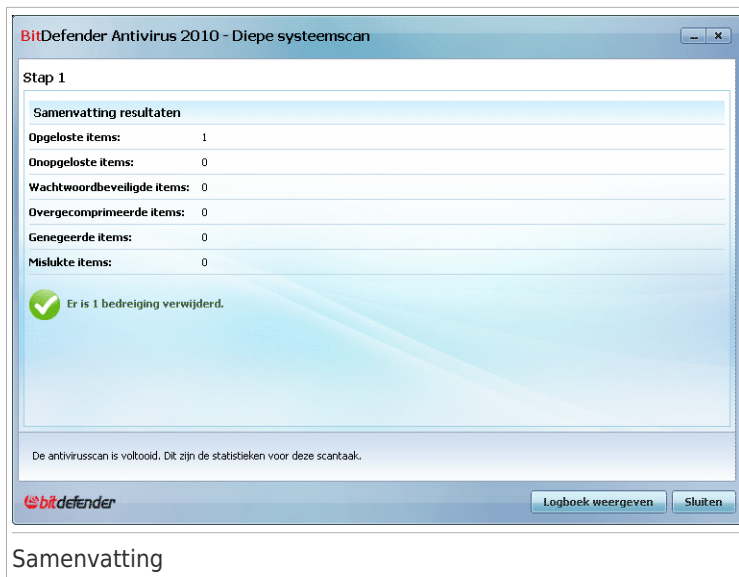
Actie	Beschrijving
Geen actie nemen	Er wordt geen actie ondernomen voor de geïnfecteerde bestanden. Als de scan is voltooid, kan u het

Actie	Beschrijving
	scanlogbestand openen om informatie over deze bestanden te zien.
Desinfecteren	Verwijdert de malwarecode uit geïnfecteerde bestanden.
Verwijderen	Verwijdert gedetecteerde bestanden.
Naar quarantaine verplaatsen	Verplaatst gedetecteerde bestanden naar de quarantaine. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer.
Naam bestanden wijzigen	Wijzigt de naam van verborgen bestanden door .bd . ren toe te voegen aan hun naam. Hierdoor zult u dergelijke bestanden op uw computer kunnen zoeken en vinden, als die er zijn. Houd ermee rekening dat deze verborgen bestanden geen bestanden zijn die u opzettelijk verbergt voor Windows. Het zijn de bestanden die worden verborgen door speciale programma's, bekend als rootkits. Rootkits zijn in wezen niet kwaadaardig. Ze worden echter algemeen gebruikt om ervoor te zorgen dat virussen en spyware niet detecteerbaar zijn voor normale antivirusprogramma's.

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

Stap 3/3 - Resultaten weergeven

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



Samenvatting

U kan een samenvatting van de resultaten zien. Als u uitgebreide informatie over het scanproces wenst, klikt u op **Logboek weergeven** om het scanlogboek weer te geven.



Belangrijk

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

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

BitDefender kon bepaalde problemen niet oplossen

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

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

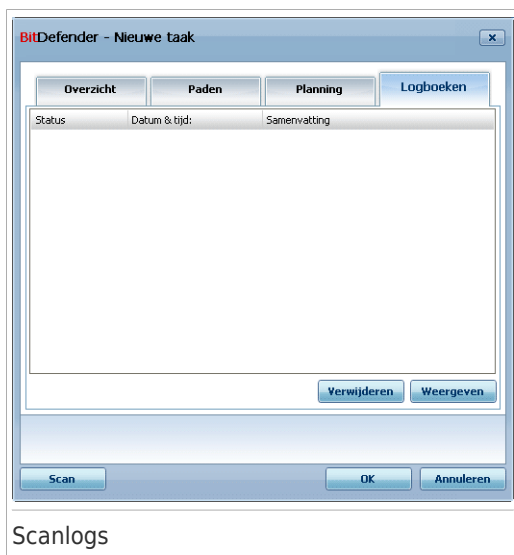
BitDefender detecteerde verdachte bestanden

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

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

18.2.6. Scanlogs weergeven

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



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

Er zijn twee knoppen beschikbaar:

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



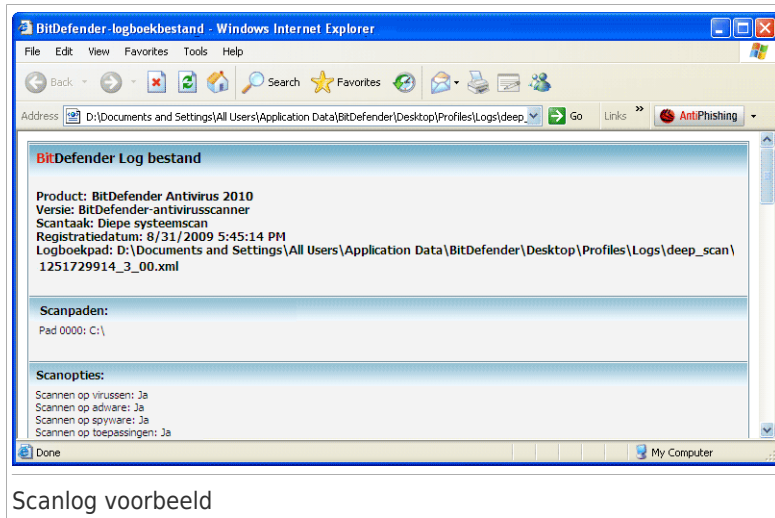
Opmerking

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

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

Scanlog voorbeeld

De volgende afbeelding is een voorbeeld van een scanlog:



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

18.3. Uitgesloten objecten van het scannen

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

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

Er kunnen twee types objecten worden uitgesloten van het scannen:

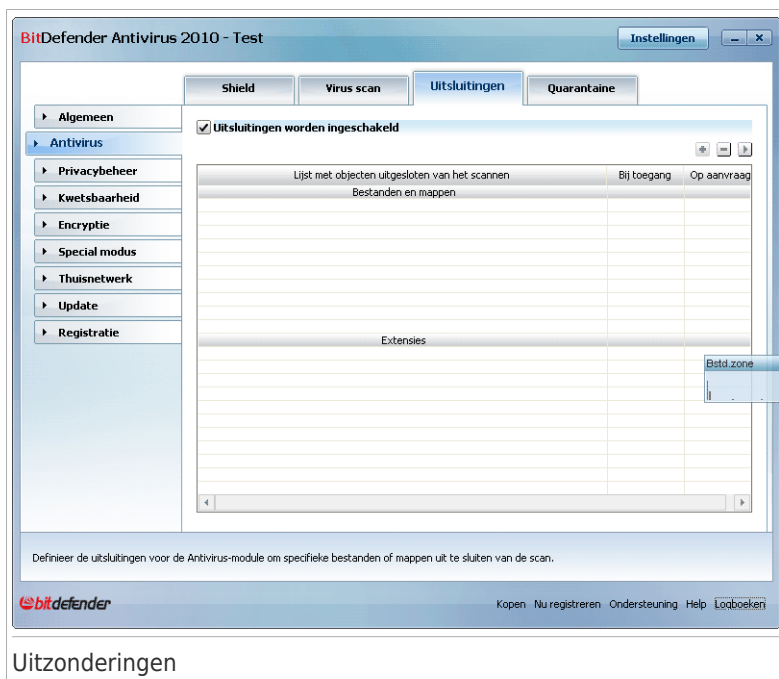
- **Paden** - het bestand of de map (inclusief alle objecten die erin zijn opgenomen) die is aangegeven door een opgegeven pad, wordt uitgesloten van het scannen.
- **Extensies** - alle bestanden met een specifieke extensie worden uitgesloten van het scannen.



Opmerking

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

Ga naar **Antivirus>Uitzonderingen** in de Expert-modus om de objecten die zijn uitgesloten van het scannen, weer te geven en te beheren.



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



Opmerking

De uitzonderingen die hier zijn opgegeven, zijn NIET van toepassing voor contextueel scannen. Contextueel scannen is een type van scannen op aanvraag. Klik met de rechtermuisknop op het bestand of de map die u wilt scannen en selecteer **Scannen met BitDefender**.

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

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



Opmerking

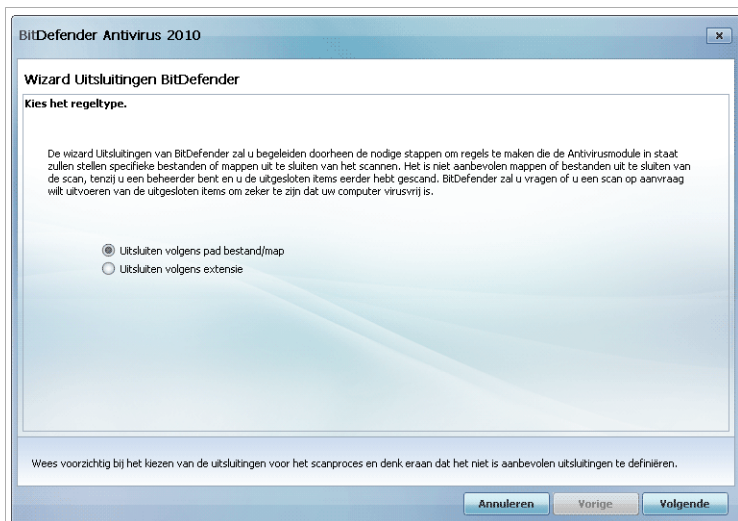
U kan ook met de rechtermuisknop op een object klikken en de opties in het snelmenu gebruiken om het object te bewerken of te verwijderen.

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

18.3.1. Paden uitsluiten van het scannen

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

Stap 1/4 - Objecttype selecteren



Objecttype

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

Klik op **Volgende**.

Stap 2/4 - Uitgesloten paden opgeven

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

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



Opmerking

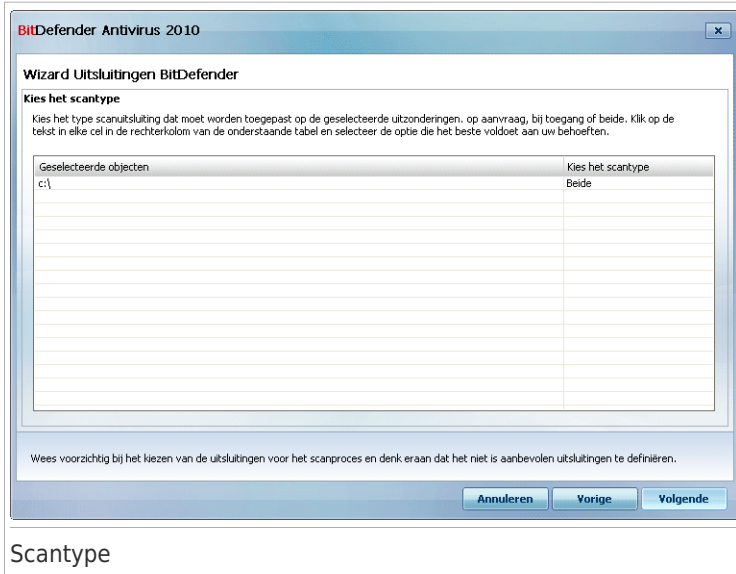
Als het opgegeven pad niet bestaat, verschijnt een foutbericht. Klik op **OK** en controleer het pad.

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

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

Klik op **Volgende**.

Stap 3/4 - Scantype selecteren



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

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

Klik op **Volgende**.

Stap 4/4 - Uitgesloten bestanden scannen



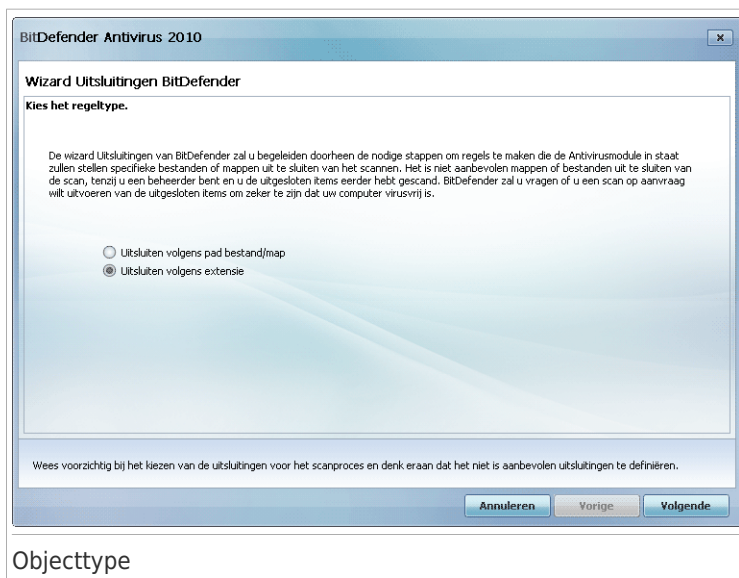
Wij adviseren met kracht de bestanden in de aangegeven paden te scannen, om er zeker van te zijn dat zij niet geïnfecteerd zijn. Kruis het vakje aan om deze bestanden te scannen voordat zij worden uitgesloten van het scannen.

Klik op **Voltooien**.

18.3.2. Extensies uitsluiten van het scannen

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

Stap 1/4 - Objecttype selecteren



Selecteer de optie om extensies uit te sluiten van de scan.

Klik op **Volgende**.

Stap 2/4 - Uitgesloten extensies opgeven

BitDefender Antivirus 2010

Wizard Uitsluitingen BitDefender

Wizard Uitsluitingen BitDefender

Voer hier de extensies in die niet moeten worden gescand en klik op Toevoegen.

.com

.com (Commando (geheugenbeeld van uitvoerbaar programma) (DOS)) wordt niet gescand

Geselecteerde extensies

Hierboven kunt u de extensies selecteren die u van het scannen wilt uitsluiten. Zorg dat u op Toevoegen klikt nadat u een extensie hebt gekozen. U kunt meerdere items toevoegen aan deze lijst.

Wees voorzichtig bij het kiezen van de uitsluitingen voor het scanproces en denk eraan dat het niet is aanbevolen uitsluitingen te definiëren.

Uitgesloten extensies

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

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



Opmerking

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

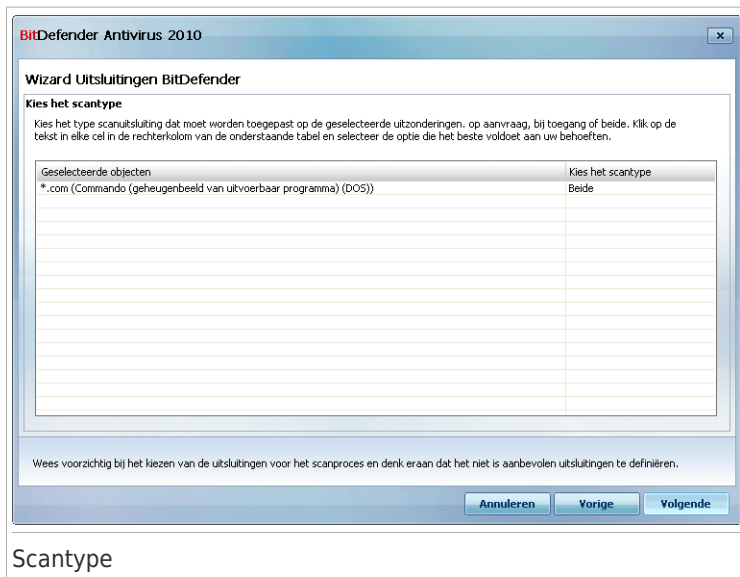
- Voer de extensie die u van het scannen wilt uitsluiten in het bewerkingsveld in en klik op **Toevoegen**.

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

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

Klik op **Volgende**.

Stap 3/4 - Scantype selecteren

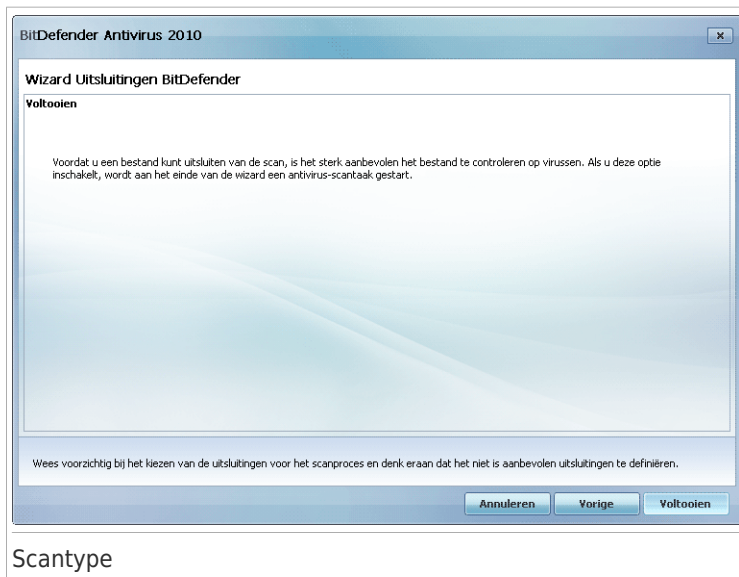


U ziet een tabel met de extensies die van het scannen zijn uitgesloten en het type scan waarvan ze zijn uitgesloten.

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

Klik op **Volgende**.

Stap 4/4 - Scantype selecteren



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

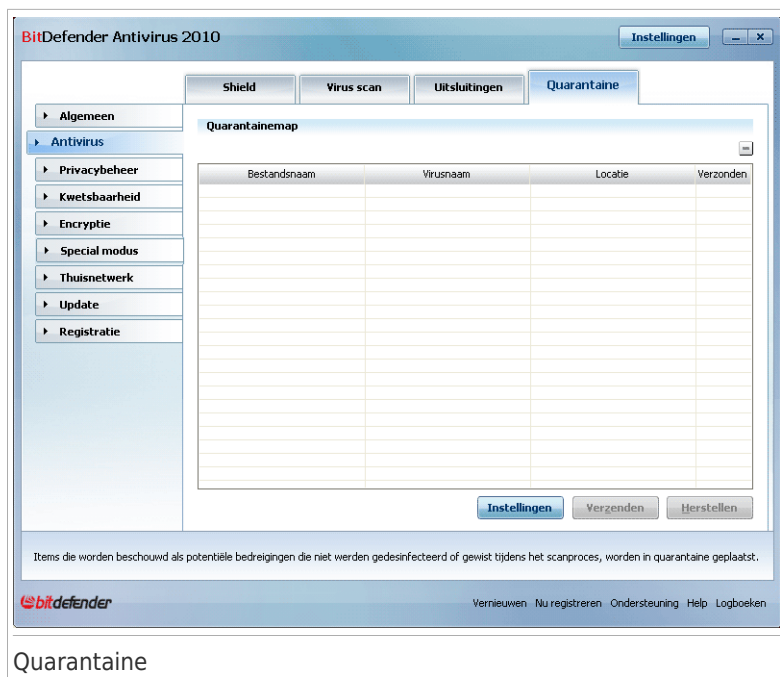
Klik op **Voltooien**.

18.4. Quarantainegebied

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

Daarnaast scant BitDefender de bestanden in quarantaine na elke update van malware-handtekening. Opgeruimde bestanden worden automatisch terug naar hun originele locatie verplaatst.

Ga naar **Antivirus>Quarantaine** in de Expert-modus om bestanden in quarantaine weer te geven en te beheren en om de quarantaine-instellingen te configureren.



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



Opmerking

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

18.4.1. Bestanden in quarantaine beheren

U kan elk geselecteerd bestand van de quarantaine verzenden naar het BitDefender Lab door te klikken op **Verzenden**. Standaard verzendt BitDefender de bestanden in quarantaine automatisch elke 60 minuten.

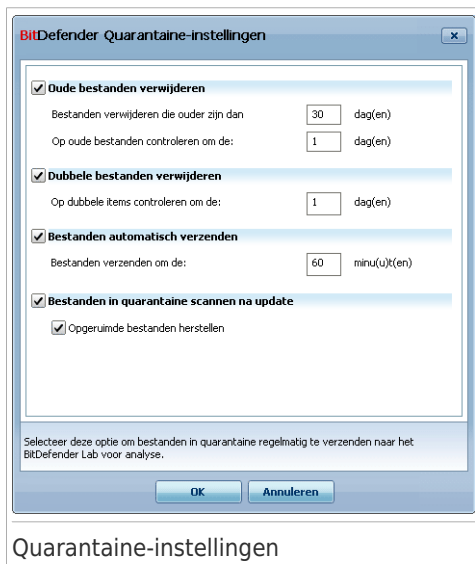
Om een geselecteerd bestand uit de quarantaine te verwijderen, klikt u op de knop **Verwijderen**. Als u een geselecteerd bestand wilt terugzetten op zijn oorspronkelijke locatie, klikt u op **Herstellen**.

Contextafhankelijk menu. Er is een contextafhankelijk menu beschikbaar waarmee u de bestanden in quarantaine gemakkelijk kan beheren. Dezelfde opties

zoals eerder vermeld, zijn beschikbaar. U kan ook **Vernieuwen** selecteren om de quarantainesectie te vernieuwen.

18.4.2. Quarantaine-instellingen configureren

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



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

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



Opmerking

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

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



Opmerking

Standaard zal BitDefender dagelijks controleren op dubbele bestanden in quarantaine.

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



Opmerking

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

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

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

19. Privacybeheer

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

19.1. Privacybeheer Statistieken

Om Privacybeheer te configureren en informatie weer te geven met betrekking tot zijn activiteit, gaat u naar **Privacybeheer>Status** in de Expert-modus.



Privacybeheer Statistieken

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



Belangrijk

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

Het Privacybeheer beveiligt uw computer met 5 belangrijke beveiligingselementen:

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

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

19.1.1. Het beveiligingsniveau configureren

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

Er zijn 3 beveiligingsniveaus:

Beveiligingsniveau	Beschrijving
Toegeeflijk	Alle beveiligingselementen zijn uitgeschakeld.
Standaard	Alleen Identiteitscontrole is uitgeschakeld.
Agressief	Identiteitscontrole , Registerbeheer , Cookiebeheer en Scriptbeheer zijn ingeschakeld.

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

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

19.2. Identiteitscontrole

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

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

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

U kan regels creëren voor het beveiligen van elke persoonlijke of vertrouwelijke informatie, van uw telefoonnummer of e-mailadres tot uw bankrekeninginformatie. Er is ondersteuning voorzien voor meerdere gebruikers, zodat andere gebruikers die zich aanmelden bij hun Windows account hun eigen regels voor de beveiliging kunnen configureren en gebruiken. Als uw Windows-account een beheerdersaccount is, kunnen de regels die u maakt, worden geconfigureerd om deze ook toe te passen wanneer andere gebruikers van de computer zijn aangemeld op hun Windows-gebruikersaccounts.

Waarom Identiteitscontrole gebruiken?

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

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

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

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

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

Om Identiteitscontrole te configureren, gaat u naar **Privacybeheer>Identiteit** in de Expert-modus.

BitDefender Antivirus 2010

Algemeen
Antivirus
Privacybeheer
Kwetsbaarheid
Encryptie
Special modus
Thuisnetwerk
Update
Registratie

Status **Identiteit** Register Cookies

☒ **Identiteitscontrole**
Geblokkeerde pogingen: 0

Regelnaam	Regelt...	Web (HTTP)	E-mail (SM...)	IM	Hele woorden

Regels voor identiteitscontrole (alleen voor beperkte gebruikers):

Regelnaam	Regel gemaakt door

Identiteitscontrole is ingeschakeld. Om u tegen diefstal van persoonlijke gegevens te beveiligen, moet u BitDefender configureren voor uw persoonlijke informatie.

Vernieuwen Nu registreren

Identiteitscontrole

Volg deze stappen als u Identiteitscontrole wilt gebruiken:

1. Schakel het selectievakje **Identiteitscontrole inschakelen** in.

2. Creëer regels om uw gevoelige data te beschermen. Meer informatie vindt u onder "*Privacyregels maken*" (p. 165).
3. Definieer, indien nodig, specifieke uitsluitingen van de regels die u hebt gemaakt. Meer informatie vindt u onder "*Uitsluitingen definiëren*" (p. 170).
4. Als u een beheerder bent op de computer, kunt u zichzelf uitsluiten van de identiteitsregels die door andere beheerders zijn gemaakt.
Meer informatie vindt u onder "*Regels die door andere beheerders zijn gedefinieerd*" (p. 173).

19.2.1. Privacyregels maken

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

Stap 1/4 - Welkomstvenster



Klik op **Volgende**.

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

BitDefender Wizard Identiteitsregels

Regelnaam

Regeltype

Regeldata

Persoonlijke informatie is versleuteld en is door niemand anders dan u te gebruiken. Vul, voor extra veiligheid, slechts een deel van de informatie die u wilt beveiligen in (bijv. om het verkeer te filteren voor het e-mail address: jan.smit@example.com, vult u alleen "jan" in de doeltekst in.)

Voer de naam in van de regel in dit gebied. Dit is de manier waarop u deze regel voor Identiteitscontrole later zult identificeren.

Vorige **Volgende** **Annuleren**

Type en gegevens van de regel instellen

U moet de volgende parameters instellen:

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



Opmerking

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

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

Klik op **Volgende**.

Stap 3/4 - Verkeerstypes en gebruikers selecteren

The screenshot shows the 'BitDefender Wizard Identity Rules' window. It has a title bar with the BitDefender logo and the text 'Wizard Identiteitsregels'. The main area is divided into two columns. The left column is titled 'Scanprotocollen:' and contains five checkboxes: 'Webverkeer (HTTP) scannen' (checked), 'E-mailverkeer (SMTP) scannen' (unchecked), 'IM-verkeer (instant messaging) scannen' (checked), 'Hele woorden' (checked), and 'Hoofdletters' (unchecked). The right column is titled 'Kies voor welke gebruiker(s) u deze regel wilt toepassen:' and contains three radio buttons: 'Alleen voor mij (huidige gebr.)' (selected), 'Beperkte gebruikersaccounts' (unchecked), and 'Alle gebruikers' (unchecked). Below these columns is a text box containing the text: 'Webverkeer (HTTP) en IM-verkeer HTTP (web) verkeer die uw persoonlijke informatie bevat wordt geblokkeerd.' At the bottom of the window, there is a light blue bar with the text 'Schakel dit selectievakje in om het scannen van e-mailverkeer (SMTP) in te schakelen' and three buttons: 'Vorige', 'Volgende', and 'Annuleren'.

Verkeerstypes en gebruikers selecteren

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

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

- **IM-verkeer scannen (Instant Messaging)** - scant het IM-verkeer (expresberichten) en blokkeert de uitgaande chatberichten die de regelgegevens bevatten.

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

Geef de gebruikers op waarvoor de regel van toepassing is.

- **Alleen voor mij (huidige gebruiker)** - de regel zal alleen op uw gebruikersaccount van toepassing zijn.
- **Beperkte gebruikersaccounts** - de regel zal van toepassing zijn op u en alle beperkte Windows-accounts.
- **Alle gebruikers** - de regel zal van toepassing zijn op alle Windows-accounts.

Klik op **Volgende**.

Stap 4/4 - Regel beschrijven



The screenshot shows a window titled "BitDefender Wizard Identiteitsregels". Inside, there is a section labeled "Regelbeschrijving" with a large text input field. Below the field, there is a paragraph of text: "Voer een beschrijving in voor deze regel. De beschrijving moet u of andere beheerders helpen gemakkelijker de informatie te identificeren die u hebt geconfigureerd om te worden geblokkeerd." At the bottom of the window, there is a light blue bar containing three buttons: "Vorige", "Voltooien", and "Annuleren". Below the window, there is a label "Regel beschrijven" next to a text input field.

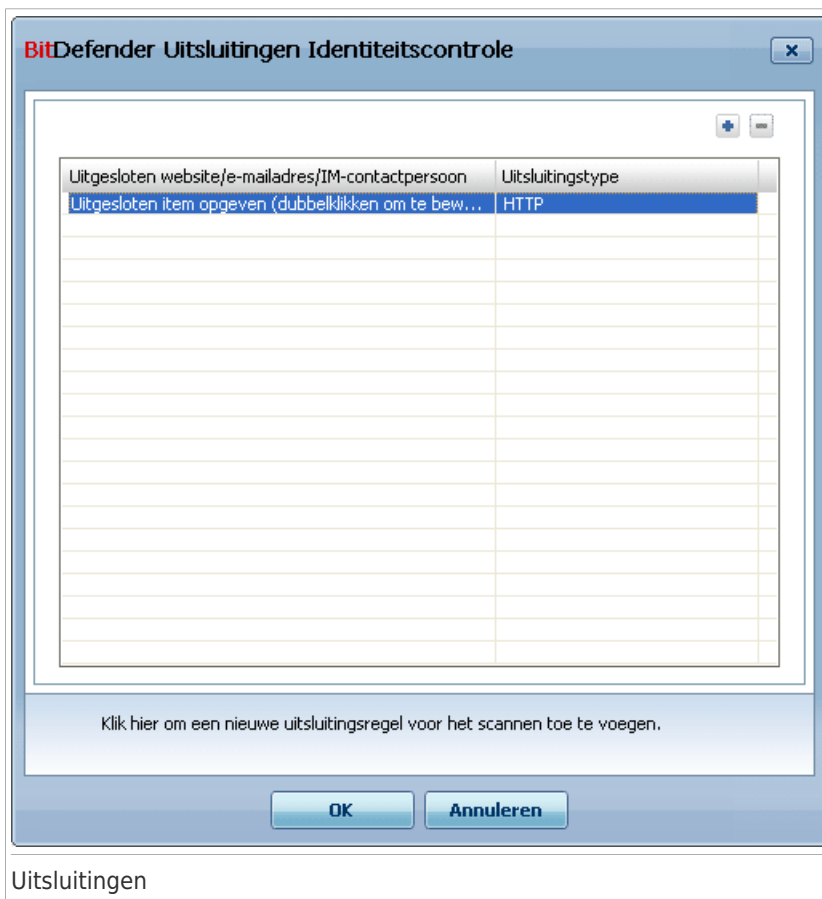
Voer een korte beschrijving in van de regel in het bewerkingsveld. Omdat de geblokkeerde data (tekenreeks) niet in normale tekst zichtbaar is als u de regel opent, kan u deze met de beschrijving beter herkennen.

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

19.2.2. Uitsluitingen definiëren

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

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



Volg deze stappen om een uitzondering toe te voegen:

1. Klik op de knop  **Toevoegen** om een nieuwe invoer in de tabel toe te voegen.
2. Dubbelklik op **Uitgesloten item opgeven** en geef de website, het e-mailadres of de IM-contactpersoon op die u als uitzondering wilt toevoegen.
3. Dubbelklik op **Verkeerstype** en selecteer de optie die overeenkomt met het eerder opgegeven adrestype in het menu.
 - Selecteer **HTTP** als u een webadres hebt opgegeven.
 - Selecteer **E-mail (SMTP)** als u een e-mailadres hebt opgegeven.

- Selecteer **IM** als u een Im contact hebt opgegeven.

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

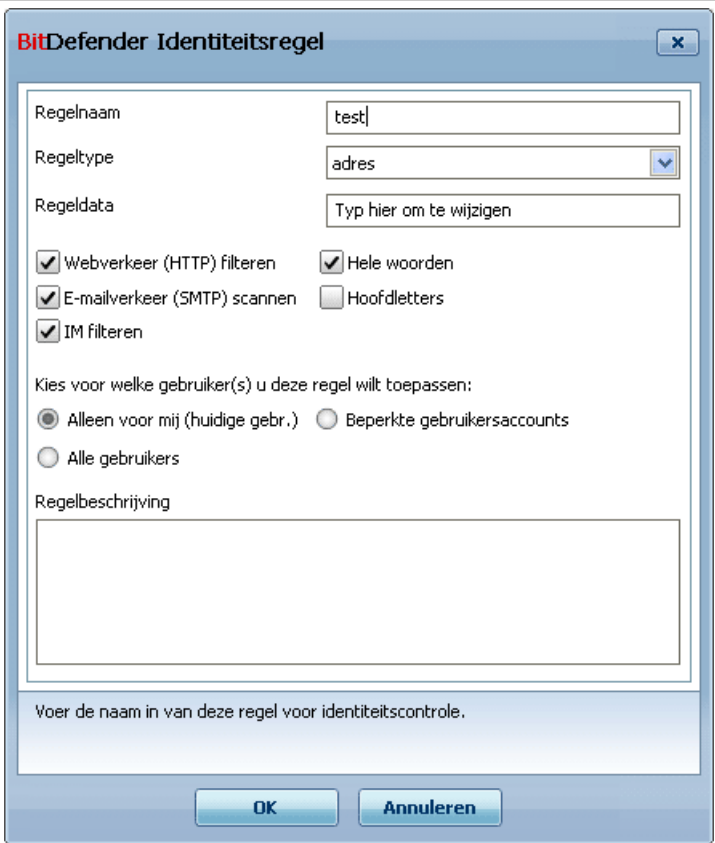
Klik op **OK** om de wijzigingen op te slaan.

19.2.3. Regels beheren

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

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

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



The screenshot shows a dialog box titled "BitDefender Identiteitsregel". It contains several input fields and checkboxes. The "Regelnaam" field contains "test". The "Regeltype" dropdown menu is set to "adres". The "Regeldata" field contains the placeholder text "Typ hier om te wijzigen". There are three checked checkboxes: "Webverkeer (HTTP) filteren", "E-mailverkeer (SMTP) scannen", and "IM filteren". There are also two unchecked checkboxes: "Hele woorden" and "Hoofdletters". Below these is a section titled "Kies voor welke gebruiker(s) u deze regel wilt toepassen:" with three radio button options: "Alleen voor mij (huidige gebr.)" (selected), "Beperkte gebruikersaccounts", and "Alle gebruikers". At the bottom is a large text area labeled "Regelbeschrijving". Below the text area is a light blue bar with the text "Voer de naam in van deze regel voor identiteitscontrole." At the very bottom are two buttons: "OK" and "Annuleren".

Regel bewerken

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

19.2.4. Regels die door andere beheerders zijn gedefinieerd

Wanneer u niet de enige gebruiker bent met beheerdersrechten op uw systeem, kunnen de andere beheerders hun eigen identiteitsregels maken. Als u regels die door andere gebruikers zijn gemaakt, niet wilt toepassen wanneer u bent aangemeld, biedt BitDefender u de mogelijkheid uzelf uit te sluiten van elke regel die u niet hebt gemaakt.

U kunt een lijst weergeven met de regels die door de beheerders in de tabel onder **Regels identiteitscontrole**. Voor elke regel wordt de naam van de regel en de naam van de gebruiker die de regel heeft gemaakt, in de tabel weergegeven.

Om uzelf uit te sluiten van een regel, selecteert u de regel in de tabel en klikt u op de knop  **Verwijderen**.

19.3. Registerbeheer

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

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

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



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

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

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



Opmerking

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

Om Registerbeheer te configureren, gaat u naar **Privacybeheer>Register** in de Expert-modus.

BitDefender Antivirus 2010

Status	Identiteit	Register	Cook...																																																																		
☒ Registerbeheer inschakelen Geblokkeerde pogingen: 0																																																																					
▶ Algemeen ▶ Antivirus ▶ Privacybeheer ▶ Kwetsbaarheid ▶ Encryptie ▶ Special modus ▶ Thuisnetwerk ▶ Update ▶ Registratie	<table border="1"> <thead> <tr> <th>Naam</th><th>Actie</th><th>Toepassingspad</th></tr> </thead> <tbody> <tr> <td>test_vbscript.exe</td><td>Toeg...</td><td>H:\Documents and Settings\amirea\Desktop\...</td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> </tbody> </table>			Naam	Actie	Toepassingspad	test_vbscript.exe	Toeg...	H:\Documents and Settings\amirea\Desktop\...																																																												
Naam	Actie	Toepassingspad																																																																			
test_vbscript.exe	Toeg...	H:\Documents and Settings\amirea\Desktop\...																																																																			
Kruis dit vakje aan om het Registerbeheer in te schakelen																																																																					

Vernieuwen Nu registreren

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

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

19.4. Cookiebeheer

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

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

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

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



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

Klik op **Ja** of **Nee** en een regel wordt gemaakt, toegepast en weergegeven in de tabel met regels.

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



Opmerking

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

Om Cookiebeheer te configureren, gaat u naar **Privacybeheer>Cookie** in de Expert-modus.

[illegible]

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



Belangrijk

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

Om een regel te verwijderen, selecteert u deze en klikt u op de knop **Verwijderen**. Om de parameters voor de regels te wijzigen, selecteert u de regel en klikt u op de knop **Bewerken** of dubbelklikt u op de regel. Voer de gewenste wijzigingen uit in het configuratievenster.

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

19.4.1. Configuratievenster

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

The screenshot shows the 'BitDefender Wizard Cookie regels' window. It has a light blue header with the title. Below the header, there are three sections: 'Domein:', 'Actie selecteren', and 'Richting selecteren'. Each section has radio buttons for selection. At the bottom right, there are two buttons: 'Voltooien' and 'Annuleren'. Below the window, there is a text box with the label 'Adres, actie en richting selecteren'.

BitDefender Wizard Cookie regels

Domein:

☒ Elke

☐ Domein:

Actie selecteren

☒ Toegestaan

☐ Weigeren

Richting selecteren

☐ Uitgaand

☐ Inkomend

☒ Beide

Selecteer de websites en domeinen waarvan u cookies aanvaardt of weigert. Cookies worden gebruikt om het surfgedrag en andere informatie op te sporen. Sommige sites zullen echter niet correct werken zonder cookies.

Voltooien **Annuleren**

Adres, actie en richting selecteren

U kunt de volgende parameters instellen:

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

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

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

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



Opmerking

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

Klik op **Voltooien**.

19.5. Scriptbeheer

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

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

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



De naam van de bron wordt weergegeven.

Klik op **Ja** of **Nee** en een regel wordt gemaakt, toegepast en weergegeven in de tabel met regels.

Om Scriptbeheer te configureren, gaat u naar **Privacybeheer>Script** in de Expert-modus.

BitDefender Antivirus 2010

[illegible]

Scriptbeheer

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



Belangrijk

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

Om een regel te verwijderen, selecteert u deze en klikt u op de knop  **Verwijderen**. Om de parameters voor de regels te wijzigen, selecteert u de regel en klikt u op de knop  **Bewerken** of dubbelklikt u op de regel. Voer de gewenste wijzigingen uit in het configuratievenster.

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

19.5.1. Configuratievenster

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



The screenshot shows the 'BitDefender Wizard Scriptregels' window. It has a title bar with the text 'BitDefender Wizard Scriptregels'. Inside, there are two main sections: 'Domein:' and 'Actie selecteren'. The 'Domein:' section has two radio buttons: 'Elke' (selected) and 'Domein:' (unselected). Next to the 'Domein:' radio button is a text input field. The 'Actie selecteren' section has two radio buttons: 'Toegestaan' (selected) and 'Weigeren' (unselected). Below these sections is a paragraph of text: 'Selecteer het specifieke domein of de domeinen waarvoor u scripts wilt toestaan of blokkeren. We raden u aan deze wizard te gebruiken om domeinen op te geven waarvan u scripts wilt toestaan. Het is aanbevolen scripts te blokkeren van alle domeinen die u niet uitdrukkelijk vertrouwt.' At the bottom right, there are two buttons: 'Voltooien' and 'Annuleren'.

BitDefender Wizard Scriptregels

Domein:

☒ Elke

☐ Domein:

Actie selecteren

☒ Toegestaan

☐ Weigeren

Selecteer het specifieke domein of de domeinen waarvoor u scripts wilt toestaan of blokkeren. We raden u aan deze wizard te gebruiken om domeinen op te geven waarvan u scripts wilt toestaan. Het is aanbevolen scripts te blokkeren van alle domeinen die u niet uitdrukkelijk vertrouwt.

Voltooien **Annuleren**

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**.

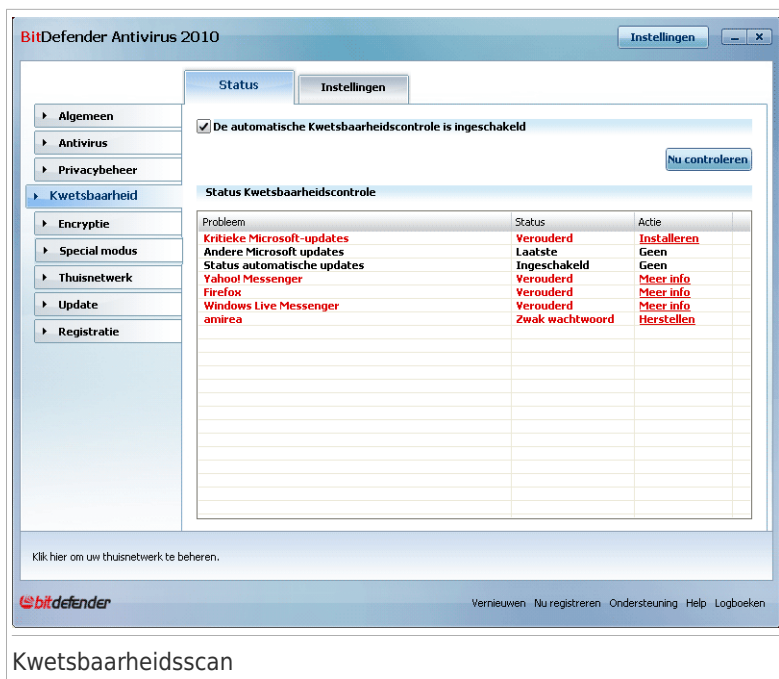
20. Kwetsbaarheid

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

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

20.1. Status

Om de automatische kwetsbaarheidscontrole te configureren of om een kwetsbaarheidscontrole uit te voeren, gaat u naar **Kwetsbaarheid>Status** in de Expert-modus.



BitDefender Antivirus 2010

Instellingen

Status Instellingen

Algemeen

Antivirus

Privacybeheer

Kwetsbaarheid

Encryptie

Special modus

Thuisnetwerk

Update

Registratie

☒ De automatische Kwetsbaarheidscontrole is ingeschakeld

Nu controleren

Status Kwetsbaarheidscontrole

Probleem	Status	Actie
Kritieke Microsoft-updates	Verouderd	Installeren
Andere Microsoft updates	Laatste	Geen
Status automatische updates	Ingeschakeld	Geen
Yahoo! Messenger	Verouderd	Meer info
Firefox	Verouderd	Meer info
Windows Live Messenger	Verouderd	Meer info
amirea	Zwak wachtwoord	Herstellen

Klik hier om uw thuisnetwerk te beheren.

bitdefender

Vernieuwen Nu registreren Ondersteuning Help Logboeken

Kwetsbaarheidsscanner

De tabel toont de problemen die werden aangepakt bij de laatste controle op kwetsbaarheden en hun status; U kunt zien welke actie u moet ondernemen om elk

zwak punt, als dat er al is, uit te schakelen. Als de actie **Geen** is, staat het respectieve probleem niet voor een zwak punt.



Belangrijk

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

20.1.1. Zwakke punten verwijderen

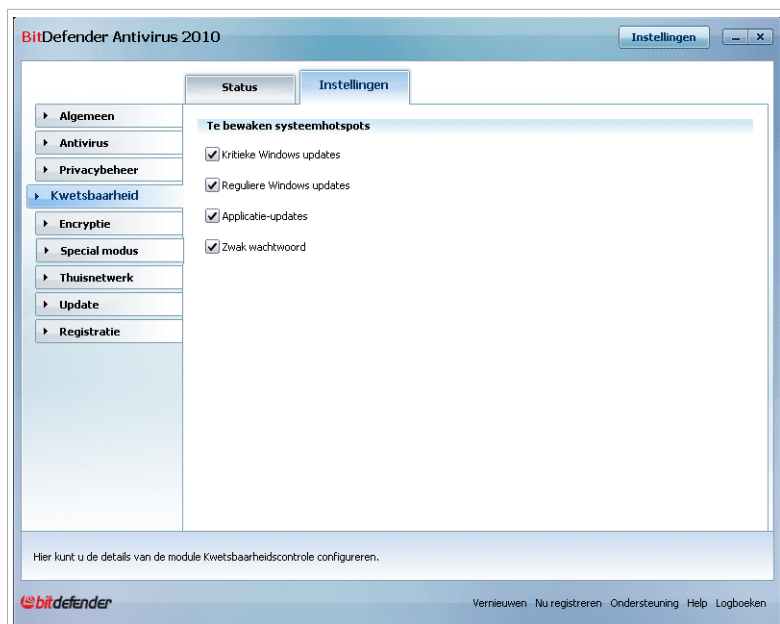
Afhankelijk van het probleem, gaat u als volgt te werk om een specifieke kwetsbaarheid te herstellen:

- Als er Windows-updates beschikbaar zijn, klikt u op **Installeren** in de kolom **Actie** om de updates te installeren.
- Als een toepassing verouderd is, kunt u de koppeling **Startpagina** gebruiken om de nieuwste versie van die toepassing te downloaden en te installeren.
- Als een Windows-gebruikersaccount een zwak wachtwoord heeft, klikt u op **Herstellen** om de gebruiker te forceren het wachtwoord te wijzigen bij de volgende aanmelding of wijzigt u zelf het wachtwoord. Voor een sterk wachtwoord gebruikt u een combinatie van hoofdletters en kleine letters, getallen en speciale tekens (zoals #, \$ of @).

U kunt op **Nu controleren** klikken en de wizard volgen om de zwakke punten stapsgewijs uit te schakelen. Meer informatie vindt u onder "*Wizard Kwetsbaarheidscontrole*" (p. 70).

20.2. Instellingen

Om de instellingen te configureren voor de automatische kwetsbaarheidscontrole, gaat u naar **Kwetsbaarheidscontrole>Instellingen** in de Expert-modus.



Automatische kwetsbaarheidscontrole instellingen

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

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



Opmerking

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

21. Instant Messaging (IM) encryptie

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

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



Belangrijk

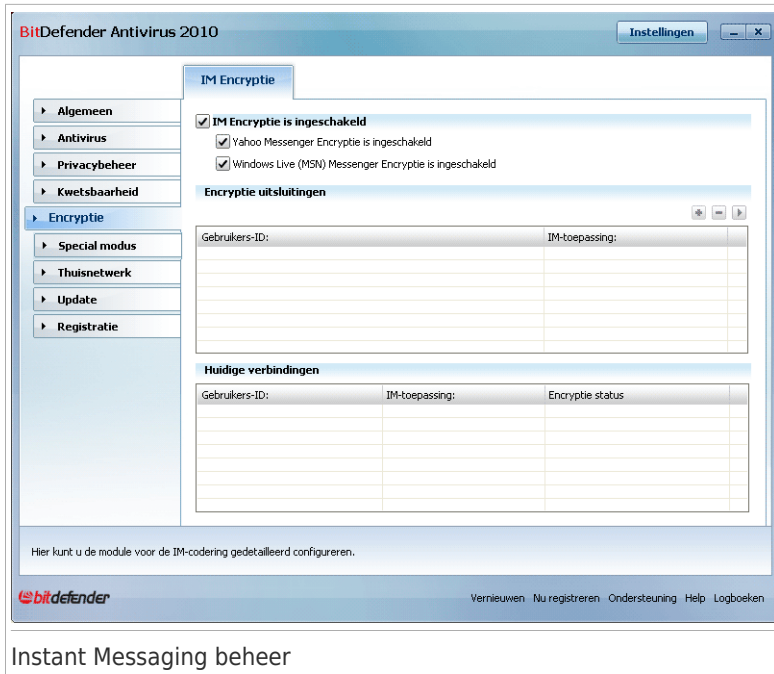
BitDefender zal een conversatie niet coderen als een chatpartner een op het web gebaseerde chattoepassing gebruikt, zoals Meebo, of als een van de chatpartners Yahoo! gebruikt en de andere Windows Live (MSN).

Om de codering van expresberichten te configureren, gaat u naar **Codering>IM-codering** in de Expert-modus.



Opmerking

U kan instant messaging encryptie gemakkelijk configureren met de BitDefender werkbalk in het chatvenster. Meer informatie vindt u onder *"Integratie in programma's voor expresberichten"* (p. 223).



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

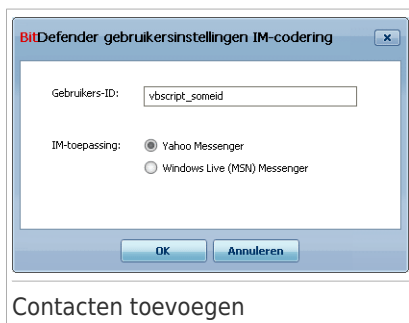
Er worden twee tabellen weergegeven:

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

21.1. Encryptie uitschakelen voor specifieke gebruikers

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

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



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

22. Spel- / Laptop-modus

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

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

22.1. Spelmodus

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

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



Opmerking

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

- Geprogrammeerde scantaken zijn standaard uitgeschakeld.

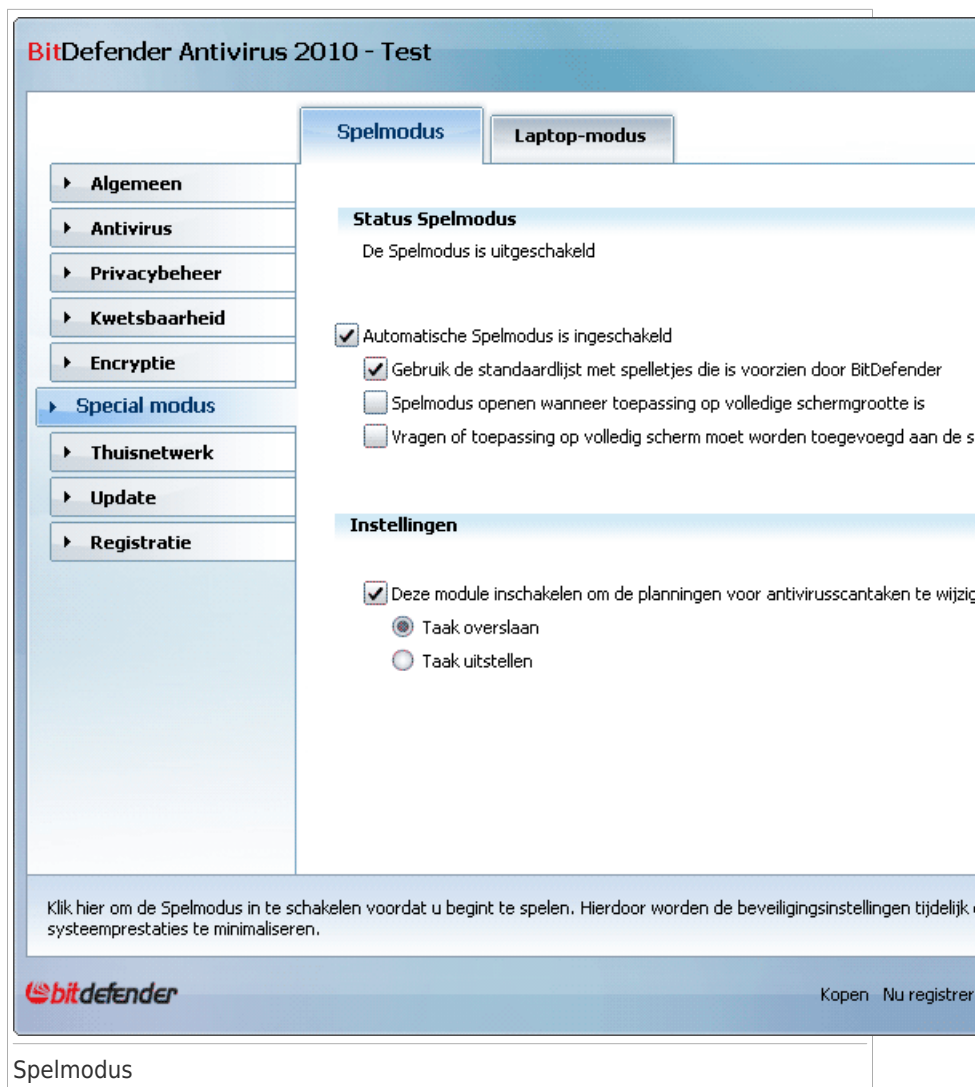
Standaard gaat BitDefender automatisch in de Spelmodus als u een spel start uit de lijst van BitDefender's bekende spelen of als een applicatie overgaat op volledig scherm. U kan de Spelmodus handmatig inschakelen met de standaard sneltoets **Ctrl+Alt+Shift+G**. Wij adviseren krachtig de Spelmodus uit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



Opmerking

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

Om de Spelmodus te configureren, gaat u naar **Spel/Laptop-modus>Spelmodus** in de Expert-modus.



Aan de bovenkant van de sectie kan u de status van de Spelmodus zien. U kunt op **Spelmodus inschakelen** of **Spelmodus uitschakelen** klikken om de huidige status te wijzigen.

22.1.1. Automatische Spelmodus configureren

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

- **De standaard lijst van spellen die door BitDefender is geleverd gebruiken** - Spelmodus wordt automatisch ingeschakeld als u een spel start dat voorkomt in de lijst van BitDefender's bekende spellen. Klik op **Spellen beheren** en vervolgens op **Spelletjeslijst** om deze lijst weer te geven.
- **Spelmodus openen wanneer toepassing op volledige schermgrootte is** - hiermee wordt de spelmodus automatisch geopend wanneer een toepassing naar volledige schermgrootte gaat.
- **Applicatie toevoegen aan de spellenlijst?** - om gevraagd te worden een nieuwe applicatie toe te voegen aan de spellenlijst als u het volledige scherm verlaat. Door een nieuwe applicatie toe te voegen aan de spellenlijst, gaat BitDefender automatisch in de Spelmodus als u de applicatie de volgende keer start.

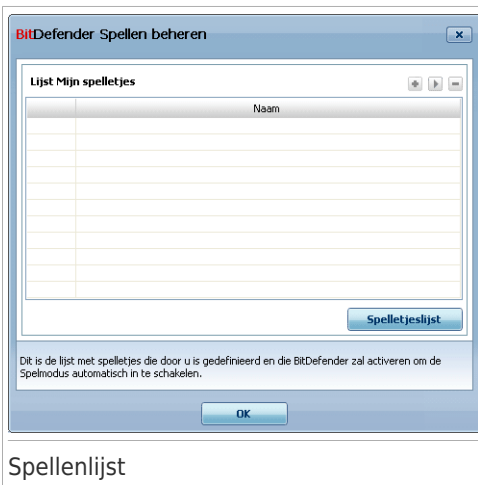


Opmerking

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

22.1.2. De spellenlijst beheren

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



Nieuwe applicaties worden automatisch toegevoegd aan de lijst als:

- U een spel start uit de BitDefender's lijst van bekende spellen. Klik op **Spelletjeslijst** om deze lijst weer te geven.
- Na het verlaten van het volledige scherm, voegt u de applicatie toe aan de spellenlijst vanuit het vraagvenster.

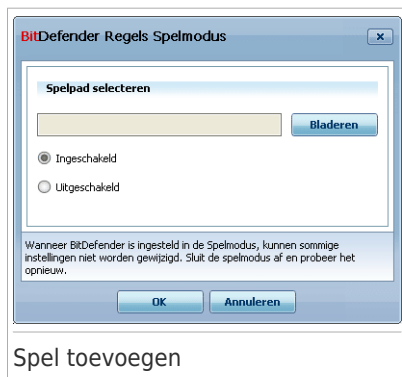
Als u de Automatische Spelmodus wilt uitschakelen voor een specifieke applicatie uit de lijst, schakelt u het overeenkomende selectievakje uit. Schakel de Automatische Spelmodus uit voor applicatie die normaal in volledig scherm werken, zoals webbrowsers en filmspelers.

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

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

Spellen toevoegen of bewerken

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



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

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

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

22.1.3. Spelmodus instellingen configureren

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

- **Deze module toestaan planningen van Antivirus-scantaken te wijzigen**
- hiermee kunt u verhinderen dat scantaken worden uitgevoerd terwijl u in de Spelmodus bent. U kan een van de volgende opties kiezen:

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

22.1.4. Veranderen van de Spelmodus sneltoets

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

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



2. Stel de gewenste sneltoets in onder de **Sneltoetsen gebruiken** optie:

- Kies de gewijzigde toetsen die u wilt gebruiken door één van de volgende aan te kruisen: Control toets (Ctrl), Shift toets (Shift) of Alternate toets (Alt).
- Typ in het invulveld de letter van de normale toets die u wilt gebruiken.
Bijvoorbeeld, als u de Ctrl+Alt+D sneltoets wilt gebruiken, kruist u Ctrl en Alt aan en typt u D.



Opmerking

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

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

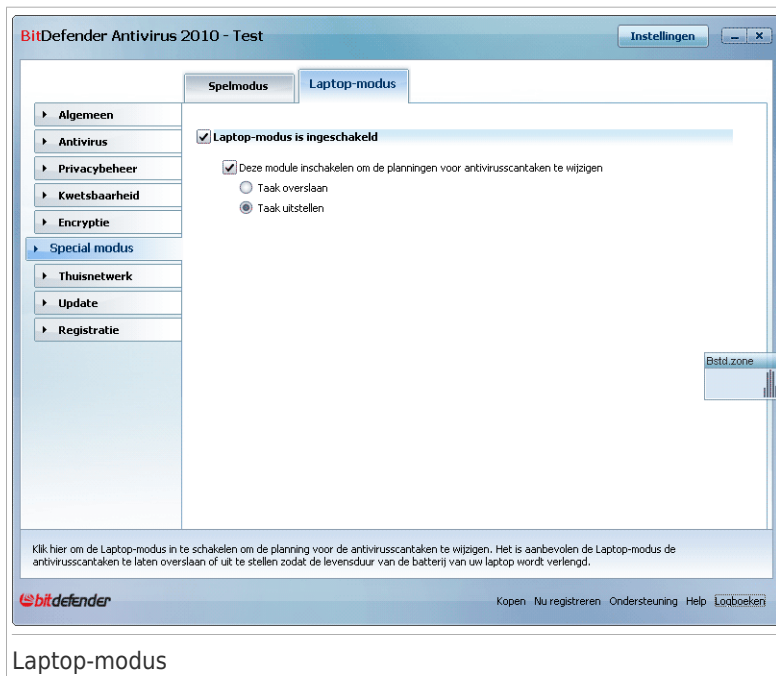
22.2. Laptop-modus

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

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

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

Om de Laptopmodus te configureren, gaat u naar **Spel/Laptop-modus>Laptop-modus** in de Expert-modus.



Laptop-modus

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

22.2.1. Laptop-modus instellingen configureren

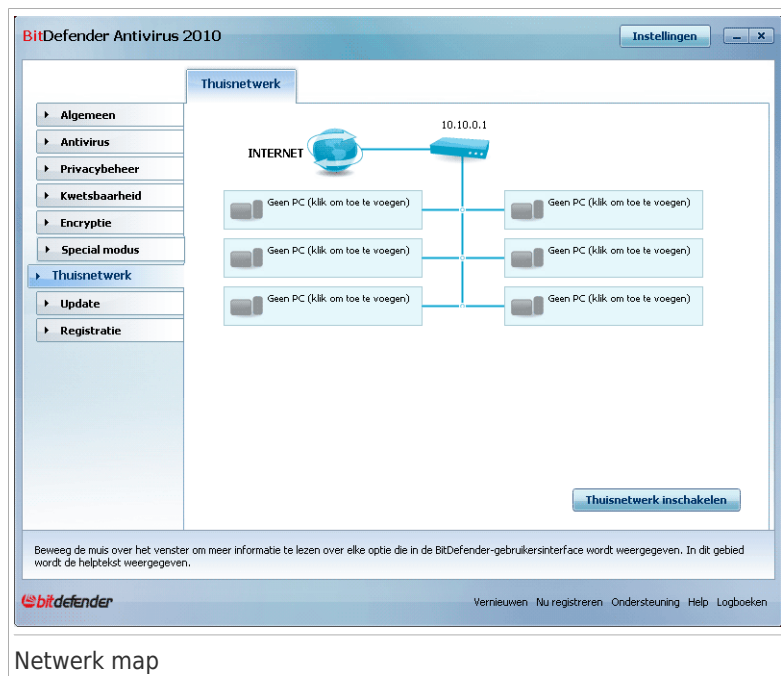
Gebruik deze opties om het gedrag voor geprogrammeerde taken te configureren:

- **Deze module toestaan planningen van Antivirus-scantaken te wijzigen**
- hiermee kunt u verhinderen dat scantaken worden uitgevoerd terwijl u in de Laptop-modus bent. U kan een van de volgende opties kiezen:

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

23. Thuisnetwerk

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



Netwerk map

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

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

23.1. Het BitDefender netwerk koppelen

Volg deze stappen om het BitDefender thuisnetwerk te koppelen:

1. Klik op **Netwerk inschakelen**. U wordt gevraagd het thuisbeheer wachtwoord te configureren.

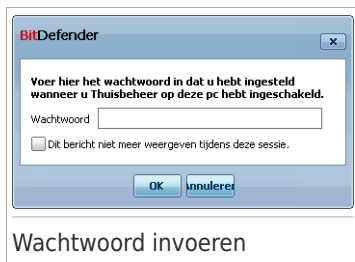


2. Voer hetzelfde wachtwoord in elk van de bewerkingsvelden in.
 3. Klik op **OK**.
- U ziet de naam van de computer in de netwerkmap.

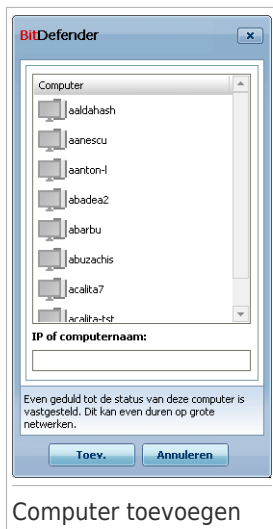
23.2. bezig met toevoegen van computers aan het BitDefender netwerk

Voordat u een computer kan toevoegen aan het BitDefender thuisnetwerk, moet u het BitDefender thuisbeheer wachtwoord configureren op de betreffende computer. Volg deze stappen als u een computer wilt toevoegen aan het BitDefender thuisnetwerk:

1. Klik op **Computer toevoegen**. U wordt gevraagd het lokale thuisbeheer wachtwoord in te voeren.



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



Computer toevoegen

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



Een online computer zonder BitDefender producten.



Een online computer met BitDefender producten.



Een offline computer met BitDefender producten.

3. U kunt een van de volgende methoden gebruiken:

- In de lijst de naam van de toe te voegen computer selecteren.
- Het IP-adres of de naam van de computer in het overeenkomende veld invoeren.

4. Klik op **Toevoegen**. U wordt gevraagd het thuismanagement wachtwoord van de betreffende computer in te voeren.



Identificeren

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

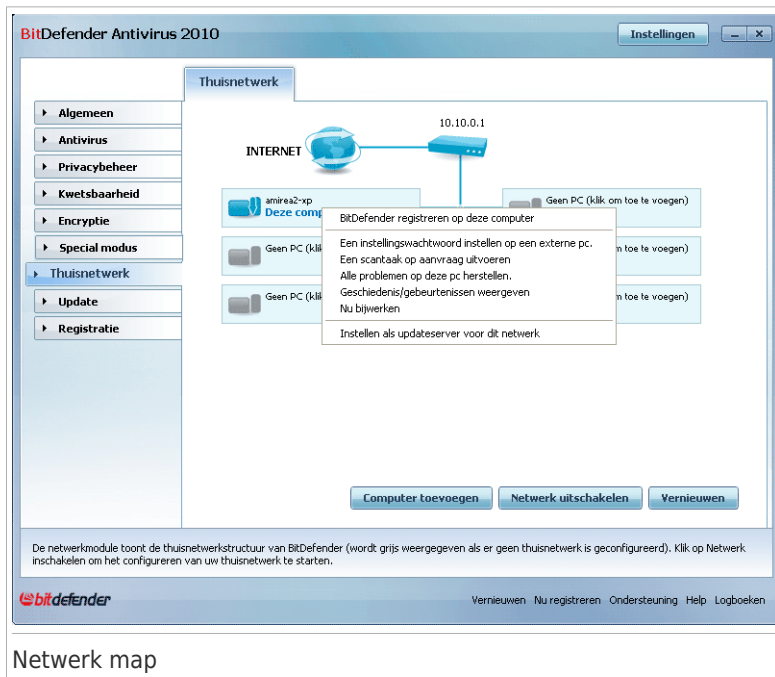


Opmerking

U kan maximaal vijf computers toevoegen aan de netwerkmap.

23.3. Het BitDefender netwerk beheren

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



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

Als u klikt op een computernaam in de netwerkmap, ziet u alle administratieve taken die u op de externe computer kunt uitvoeren.

● PC uit thuisnetwerk verwijderen

Hiermee kunt u een pc uit het netwerk verwijderen.

- **BitDefender registreren op deze computer**

Hiermee kunt u BitDefender op deze computer registreren door een licentiesleutel in te voeren.

- **Een instellingswachtwoord instellen op een externe pc**

Hiermee kunt u een wachtwoord maken om de toegang tot de BitDefender-instellingen op deze pc te beperken.

- **Een scantaak op aanvraag uitvoeren**

Hiermee kunt u een scan op aanvraag maken op de externe computer. U kunt elk van de volgende scantaken uitvoeren: Mijn documenten scannen, Systeemscan of Diepe systeemscan.

- **Alle problemen op deze pc herstellen**

Hiermee kunt u de problemen die de veiligheid van uw computer beïnvloeden oplossen door de wizard **Alle problemen oplossen** te volgen.

- **Geschiedenis/gebeurtenissen weergeven**

Hiermee krijgt u toegang tot de module **Geschiedenis&gebeurtenissen** van het BitDefender-product dat op deze computer is geïnstalleerd.

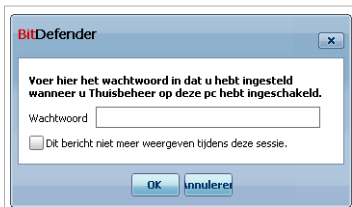
- **Nu bijwerken**

Start het updateproces voor het BitDefender-product dat op deze computer is geïnstalleerd.

- **Instellen als updateserver voor dit netwerk**

Hiermee kunt u deze computer instellen als de updateserver voor alle BitDefender-producten die op de computers in dit netwerk zijn geïnstalleerd. Het gebruik van deze optie zal het internetverkeer beperken omdat slechts één computer in het netwerk een verbinding zal maken met internet om updates te downloaden.

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



The screenshot shows a Windows-style dialog box titled "BitDefender". Inside the dialog, there is a text box with the instruction: "Voer hier het wachtwoord in dat u hebt ingesteld wanneer u Thuisbeheer op deze pc hebt ingeschakeld." Below this is a label "Wachtwoord" followed by a text input field. At the bottom left of the dialog is a checkbox with the text "Dit bericht niet meer weergeven tijdens deze sessie." At the bottom right are two buttons: "OK" and "Annuleren".

Wachtwoord invoeren

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



Opmerking

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

24. Update

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

Als u via breedband of DSL verbonden bent met het Internet, zal BitDefender deze taak op zich nemen. Het programma controleert standaard op updates wanneer u uw computer inschakelt en daarna ieder **uur**.

Als een update is gedetecteerd, kan u gevraagd worden het updaten te bevestigen, ofwel het updaten wordt automatisch uitgevoerd, afhankelijk van de **automatische update instellingen**.

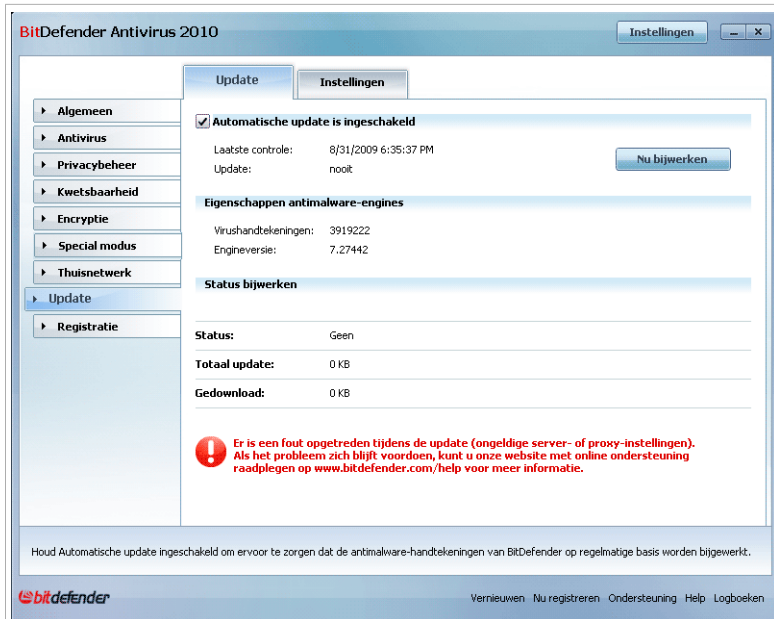
Het updateproces wordt "on the fly" uitgevoerd. Dit betekent dat de bestanden die moeten worden bijgewerkt, progressief worden vervangen. Hierdoor zal het updateproces de productwerking niet beïnvloeden wordt tegelijkertijd elk zwak punt uitgeschakeld.

Updates worden op de volgende manieren beschikbaar gesteld:

- **Updates voor antivirus-engines** - aangezien er steeds nieuwe virussen dreigen, moeten de bestanden met de virushandtekeningen voortdurend worden bijgewerkt om een permanente up-to-date beveiliging te garanderen. Dit type update is ook bekend als **Update virusdefinities**.
- **Updates voor de antispyware-engines** - er worden nieuwe spyware-handtekeningen toegevoegd aan de database. Dit type update is ook bekend als **Antispyware -update**.
- **Product upgrades** - Bij de lancering van een nieuwe productversie worden nieuwe functies en scantechnieken ingevoerd met het oog op een betere prestatie van het product. Dit type update is ook bekend als **Product-update**.

24.1. Automatische update

Ga naar **Update>Update** in de Expert-modus om informatie met betrekking tot de update te zien en automatische updates uit te voeren.



Automatische update

Hier kunt u zien wanneer de laatste controle op updates en de laatste update werd uitgevoerd. Daarnaast vindt u hier ook informatie over de laatst uitgevoerde update (indien gelukt of als er fouten zijn opgetreden). Ook informatie over de huidige engine-versie en het aantal handtekeningen wordt weergegeven.

Als u deze sectie opent tijdens een update, kunt u de downloadstatus zien.



Belangrijk

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

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

24.1.1. Een update aanvragen

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

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



Belangrijk

Het kan noodzakelijk zijn de computer opnieuw op te starten wanneer de update is voltooid. Wij adviseren dit zo snel mogelijk te doen.



Opmerking

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

24.1.2. Automatische update uitschakelen

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



Waarschuwing

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

24.2. Update- instellingen

De updates kunnen worden uitgevoerd vanaf het lokale netwerk, via het Internet, rechtstreeks of via een proxyserver. BitDefender zal standaard elk uur via het internet controleren op updates en de beschikbare updates zonder enige waarschuwing installeren.

Ga naar **Update>Instellingen** in de Expert-modus om de update-instellingen te configureren en proxy's te beheren.



De update-instellingen zijn gegroepeerd in 4 categorieën (**Updatelocatie-instellingen**, **Automatische update-instellingen**, **Handmatige update-instellingen** en **Geavanceerde instellingen**). Elke categorie wordt afzonderlijk beschreven.

24.2.1. Updatelocaties instellen

Gebruik de opties in de categorie **Updatelocatie-instellingen** om de updatelocaties in te stellen.



Opmerking

Configureer deze instellingen alleen als u verbonden bent met een lokaal netwerk dat de malware signaturen van BitDefender lokaal opslaat of als u via een proxyserver met het internet bent verbonden.

Voor betrouwbaardere en snellere updates kunt u twee updatelocaties configureren: een **Primaire updatelocatie** en een **Alternatieve updatelocatie**. Deze locaties zijn standaard dezelfde: <http://upgrade.bitdefender.com>.

Om een van de updatelocaties te wijzigen, geeft u de URL van de lokale spiegel op in het **URL**-veld dat overeenkomt met de locatie die u wilt wijzigen.



Opmerking

Wij adviseren de lokale spiegel in te stellen als de primaire updatelocatie en de alternatieve updatelocatie ongewijzigd te laten als een alternatieve mogelijkheid in het geval de lokale spiegel niet bereikbaar is.

Als het bedrijf een proxyserver gebruikt om een verbinding te maken met het internet, schakelt u het selectievakje **Proxy gebruiken** in en klikt u vervolgens op **Proxy-instellingen** om de proxy-instellingen te configureren. Meer informatie vindt u onder "*Proxy's beheren*" (p. 208).

24.2.2. Automatische update configureren

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

In het veld **Bijwerken elke** kunt u het aantal uren tussen twee opeenvolgende controles op updates opgeven. Het tijdinterval voor de update is standaard ingesteld op 1 uur.

Selecteer een van de volgende opties om op te geven hoe de automatische update moet worden uitgevoerd:

- **Stille update** - BitDefender downloadt en installeert de update automatisch.
- **Vragen voordat updates worden gedownload** - telkens wanneer een update beschikbaar is, wordt uw bevestiging gevraagd voordat de update wordt gedownload.
- **Vragen voordat updates worden geïnstalleerd** - telkens wanneer een update is gedownload, wordt uw bevestiging gevraagd voordat de update wordt geïnstalleerd.

24.2.3. Handmatige update configureren

Selecteer een van de volgende opties in de categorie **Handmatige update-instellingen** om op te geven hoe de handmatige update (update op aanvraag van gebruiker) moet worden uitgevoerd:

- **Stille update** - de handmatige update wordt automatisch uitgevoerd op de achtergrond, zonder enige tussenkomst van de gebruiker.
- **Vragen voordat updates worden gedownload** - telkens wanneer een update beschikbaar is, wordt uw bevestiging gevraagd voordat de update wordt gedownload.

24.2.4. Geavanceerde instellingen configureren

Om ervoor te zorgen dat het updateproces van BitDefender uw werk niet hindert, configureert u de opties in de categorie **Geavanceerde instellingen**:

- **Wacht op het opnieuw starten, in de plaats van vraag te stellen** - Als een update het opnieuw opstarten vereist, zal het product blijven werken met de oude

bestanden tot het systeem opnieuw is opgestart. De gebruiker wordt niet gevraagd om opnieuw op te starten. Daarom zal het updateproces van BitDefender geen invloed hebben op het werk van de gebruiker.

- **Geen update uitvoeren als het scannen bezig is** - BitDefender zal geen update uitvoeren als een scanproces wordt uitgevoerd. Hierdoor zal het updateproces van BitDefender de scantaken niet hinderen.



Opmerking

Als de update van BitDefender wordt uitgevoerd terwijl het scannen bezig is, wordt het scanproces afgebroken.

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

24.2.5. Proxy's beheren

Als uw bedrijf een proxyserver gebruikt om een verbinding te maken met het internet, moet u de proxy-instellingen opgeven zodat BitDefender zichzelf kan updaten. Anders zal het programma gebruik maken van de proxy-instellingen van de beheerder die het product heeft geïnstalleerd of van de eventuele standaardbrowser van de huidige gebruiker.



Opmerking

De proxy-instellingen kunnen alleen worden geconfigureerd door gebruikers met beheerdersrechten op de computer of door hoofdgebruikers (gebruikers die het wachtwoord voor de productinstellingen kennen).

Klik op **Proxy-instellingen** om de proxy-instellingen te beheren. Een nieuw venster wordt weergegeven.

BitDefender Proxy-instellingen

Proxy gedetecteerd op tijdstip van installatie

Adres: Poort: Gebruikersnaam:
Wachtwoord:

Proxy standaardbrowser

Adres: Poort: Gebruikersnaam:
Wachtwoord:

Aangepaste proxy

Adres: Poort: Gebruikersnaam:
Wachtwoord:

Hier kunt u de proxy-instellingen wijzigen die op het installatietijdstip zijn gedetecteerd.

OK Annuleren

Proxybeheer

Er zijn drie reeksen proxy-instellingen:

- **Proxy gedetecteerd op tijdstip van installatie** - proxy-instellingen die op de account van de beheerder zijn gedetecteerd tijdens de installatie en die alleen kunnen worden geconfigureerd als u aangemeld bent bij die account. Als de proxyserver een gebruikersnaam en wachtwoord vereist, moet u deze gegevens opgeven in de overeenkomende velden.
- **Proxy standaardbrowser** - proxy-instellingen van de huidige gebruiker, opgehaald van de standaardbrowser. Als de proxyserver een gebruikersnaam en wachtwoord vereist, moet u deze gegevens opgeven in de overeenkomende velden.



Opmerking

De ondersteunde webbrowsers zijn Internet Explorer, Mozilla Firefox en Opera. Als u standaard een andere browser gebruikt, zal BitDefender de proxy-instellingen van de huidige gebruiker niet kunnen ophalen.

- **Aangepaste proxy** - proxy-instellingen die u kunt configureren wanneer u bent aangemeld als beheerder.

U moet de volgende instellingen definiëren:

- ▶ **Adres** - voer het IP-adres van de proxyserver in.
- ▶ **Poort** - voer de poort in die BitDefender gebruikt om een verbinding te maken met de proxyserver.

- ▶ **Gebruikersnaam** - voer een gebruikersnaam in die wordt herkend door de proxy.
- ▶ **Wachtwoord** - voer het geldige wachtwoord voor de eerder opgegeven gebruiker in.

Wanneer u een verbinding probeert te maken met het internet, wordt elke reeks proxy-instellingen achtereenvolgens geprobeerd, tot BitDefender erin slaagt een verbinding te maken.

Eerst wordt de reeks met uw persoonlijke proxy-instellingen gebruikt om een verbinding te maken met het internet. Als dat niet werkt, worden daarna de proxy-instellingen die op het tijdstip van de installatie zijn gedetecteerd, geprobeerd. Als dat evenmin werkt, worden tot slot de proxy-instellingen van de huidige gebruiker overgenomen van de standaard browser en gebruikt om een verbinding te maken met het internet.

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

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

25. Registratie

Om complete informatie over uw BitDefender-product en de registratiestatus te zoeken, gaat u naar **Registratie** in de Expert-modus.

The screenshot shows the BitDefender Antivirus 2010 - Test interface. On the left is a sidebar with a list of menu items: Algemeen, Antivirus, Privacybeheer, Kwetsbaarheid, Encryptie, Special modus, Thuisnetwerk, Update, and Registratie. The 'Registratie' item is selected and highlighted in blue. The main content area on the right has a tab labeled 'Registratie' at the top. Below this tab, there are three sections: 'Productinformatie' showing 'BitDefender Antivirus 2010' and 'Versie: 13.0.15.1'; 'Registratie-informatie' with a message about the 30-day trial period; and 'Actie' which contains two buttons: 'Product activeren' and 'Nu registreren'. At the bottom of the main area, there is a text link: 'Klik hier om BitDefender te activeren en toegang te krijgen tot de antivirus-updates en de technische ondersteuning.' The footer of the window displays the BitDefender logo on the left and the text 'Kopen Nu registreren' on the right.

BitDefender Antivirus 2010 - Test

Registratie

Productinformatie

BitDefender Antivirus 2010
Versie: 13.0.15.1

Registratie-informatie

De licentiesleutel voor dit product vervalt binnen 30 dagen. Na deze periode zal u...

Actie

[Product activeren](#)

[Nu registreren](#)

Klik hier om BitDefender te activeren en toegang te krijgen tot de antivirus-updates en de technische ondersteuning.

bitdefender

Kopen Nu registreren

Registratie

In deze sectie ziet u:

- **Productinformatie:** het BitDefender product en de versie.
- **Registratie-informatie:** het e-mailadres waarmee u inlogt op uw BitDefender-account (indien geconfigureerd), de huidige licentiesleutel en over hoeveel dagen de licentiesleutel verloopt.

25.1. BitDefender Antivirus 2010 registreren

Klik op **Nu registreren** om het venster voor de productregistratie te openen.

The screenshot shows the 'BitDefender Antivirus 2010' registration wizard. The window has a blue header with the product name. Below the header, the title 'Registratiewizard' is displayed. The main content area is titled 'BitDefender-registratie' and contains the following information:

- Informatie huidige licentiesleutel**
 - Type: **GELDIG, TEST**
 - Vervalt binnen: **30 dagen**
- Licentiesleutel invoeren:**
 - A text input field labeled 'Licentiesleutel:' with the placeholder text 'Licentiesleutel invoeren'.
 - A blue link below the input field: [Geen licentiesleutel? Nu kopen.](#)

At the bottom of the window, there is a blue bar with two buttons: 'Annuleren' and 'Nu registreren' (partially visible). A small text note at the bottom left of the window states: 'Beweeg de muis over het venster om meer informatie te lezen over elke optie die in de BitDefender-gebruikersinterface wordt de helptekst weergegeven.'

Registratie

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

BitDefender Antivirus 2010 registreren:

1. Typ de licentiesleutel in het bewerkingsveld.



Opmerking

U kan uw licentiesleutel vinden:

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

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

2. Klik op **Nu registreren**.

3. Klik op **Voltooien**.

25.2. Een BitDefender-account creëren

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



Belangrijk

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

Als u nog geen BitDefender-account hebt gemaakt, klikt u op **Product activeren** om het venster voor de accountregistratie te openen.

The screenshot shows the 'Registratiewizard' (Registration Wizard) window for BitDefender Antivirus 2010. The window has a blue header with the product name. Below the header, the title 'Registratiewizard' is displayed. The main section is titled 'BitDefender-account'. It contains a paragraph of text explaining the purpose of the account and a URL. There are three radio buttons for account creation: 'Een nieuwe account maken' (selected), 'Aanmelden (eerder gemaakte account)', and 'Later registreren (de registratie is verplicht)'. Below the first option are input fields for 'E-mailadres:', 'Wachtwoord:', 'Wachtwoord herhalen:', and a dropdown for 'E-mailopties:'. A 'Creëren' button is positioned below these fields. At the bottom right, there are 'Annuleren' and 'Voltooiën' buttons. A footer bar at the bottom of the window contains the text 'Account creëren'.

BitDefender Antivirus 2010

Registratiewizard

BitDefender-account

Activeer uw BitDefender nu om toegang tot technische dienst te krijgen. Ook geeft <http://myaccount.Bitdefender.com> u verloren licentiesleutel terug te krijgen en krijgt u het voordeel uit de speciale BitDefender aanbiedingen.

☒ Een nieuwe account maken

E-mailadres:

Wachtwoord: Wachtwoord herhalen:

E-mailopties:

☐ Aanmelden (eerder gemaakte account)

☐ Later registreren (de registratie is verplicht)

Beweeg de muis over het venster om meer informatie te lezen over elke optie die in de BitDefender-gebruikersinterface w gebied wordt de helptekst weergegeven.

Account creëren

Als u momenteel geen BitDefender-account wilt maken, selecteert u **Later registreren** en klikt u op **Voltooiën**. Ga anders te werk zoals past bij uw situatie:

- "Ik heb geen BitDefender-account" (p. 214)
- "Ik heb al een BitDefender-account" (p. 215)

Ik heb geen BitDefender-account

Volg deze stappen om een BitDefender-account te maken:

1. Selecteer **Een nieuwe account maken**.

2. Typ de vereiste informatie in de overeenkomende velden. De gegevens die u hier opgeeft blijven vertrouwelijk.

- **E-mailadres** - voer uw e-mailadres in.
- **Wachtwoord** - voer een wachtwoord voor uw BitDefender-account in. Het wachtwoord moet 6 tot 16 tekens lang zijn.
- **Wachtwoord opnieuw** - voer het zojuist gebruikte wachtwoord opnieuw in.



Opmerking

Zodra de account is geactiveerd, kunt u het bijgeleverde e-mailadres en het wachtwoord gebruiken om u aan te melden bij uw account op <http://myaccount.bitdefender.com>.

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

- **Mij alle berichten sturen**
- **Mij alleen berichten met betrekking tot producten sturen**
- **Stuur mij geen berichten**

4. Klik op **Maken**.
5. Klik op **Voltooien** om de wizard te voltooien.
6. **Uw account activeren**. Voordat u uw account kunt gebruiken, moet u deze activeren. Controleer uw e-mail en volg de instructies in de e-mail die u van de registratieservice van BitDefender hebt ontvangen.

Ik heb al een BitDefender-account

BitDefender detecteert automatisch of u al een BitDefender-account hebt geregistreerd op uw computer. Geef in dit geval het wachtwoord van uw account op en klik op **Aanmelden**. Klik op **Voltooien** om de wizard te voltooien.

Als u al een actieve account hebt, maar BitDefender deze niet detecteert, moet u deze stappen volgen om het product voor die account te registreren:

1. Selecteer **Aanmelden (eerder gemaakte account)**.
2. Voer het e-mailadres en wachtwoord van uw account in de overeenkomende velden in.



Opmerking

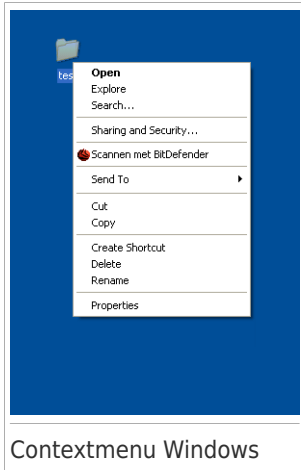
Als u uw wachtwoord bent vergeten, klikt u op **Wachtwoord vergeten?** en volgt u de instructies.

3. Optioneel kan BitDefender u informeren over speciale aanbiedingen via het e-mailadres van uw account. Selecteer een van de beschikbare opties in het menu:
 - **Mij alle berichten sturen**
 - **Mij alleen berichten met betrekking tot producten sturen**
 - **Stuur mij geen berichten**
4. Klik op **Aanmelden**.
5. Klik op **Voltooien** om de wizard te voltooien.

Integratie in Windows en software van derden

26. Integratie in het contextmenu van Windows.

Het contextmenu van Windows verschijnt altijd wanneer u met de rechtermuisknop op een bestand of map van uw computer of op objecten op het bureaublad klikt.



BitDefender integreert zich in het contextmenu van Windows zodat u bestanden gemakkelijker kunt scannen op virussen. U kunt de BitDefender-optie in het contextmenu snel vinden door het BitDefender-pictogram  te zoeken.

26.1. Scannen met BitDefender

U kunt gemakkelijk bestanden, mappen en zelfs volledige harde schijven scannen via het contextmenu van Windows. Klik met de rechtermuisknop op het object dat u wilt scannen en selecteer **Scannen met BitDefender** in het menu. De **Antivirusscanwizard** wordt weergegeven en begeleidt u doorheen het scanproces.

Scanopties. De scanopties zijn vooraf geconfigureerd voor de beste detectieresultaten. Als er geïnfecteerde bestanden wordt gedetecteerd, zal BitDefender proberen ze te desinfecteren (de malwarecode verwijderen). Als de desinfectie mislukt, kunt u met de Antivirusscanwizard andere acties opgeven die moeten worden ondernemen op geïnfecteerde bestanden.

Volg de onderstaande stappen als u de scanopties wilt wijzigen:

1. Open BitDefender en schakel de gebruikersinterface naar de Expert-modus.
2. Klik in het menu aan de linkerzijde op **Antivirus**.
3. Klik op het tabblad **Virusscan**.

4. Klik met de rechtermuisknop op de taak **Contextueel scannen** en selecteer **Openen**. Een venster wordt weergegeven.
5. Klik op **Aangepast** en configureer de scanopties zoals dat nodig is. Om uit te zoeken wat een optie doet, houdt u de muis boven de optie en leest u de beschrijving die onderaan in het venster wordt weergegeven.
6. Klik op **OK** om de wijzigingen op te slaan.
7. Klik op **OK** om de nieuwe scanopties te bevestigen en toe te passen.



Belangrijk

U mag de scanopties van deze scanmethode niet wijzigen tenzij u daarvoor een grondige reden hebt.

27. Integratie in webbrowsers

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

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

- Internet Explorer
- Mozilla Firefox

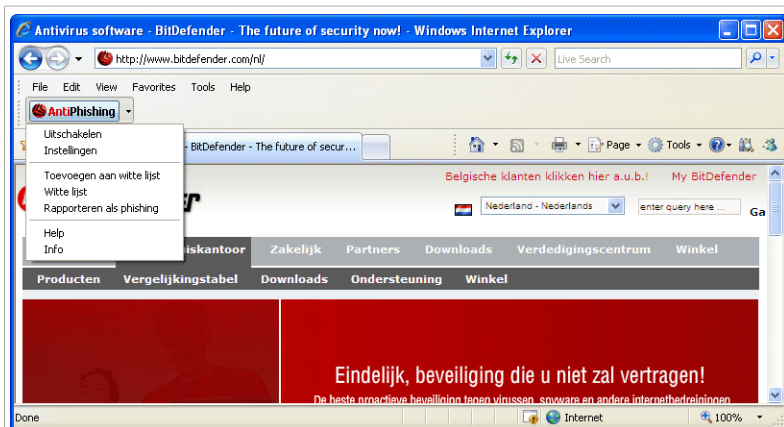
U kan de antiphishing-beveiliging en de Witte lijst gemakkelijk en efficiënt beheren met de werkbalk van BitDefender Antiphishing die in de bovenstaande webbrowsers is geïntegreerd.

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



Opmerking

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



Antiphishing-werkbalk

De volgende opdrachten zijn beschikbaar in het werkbalkmenu:

- **Inschakelen/uitschakelen** - hiermee wordt de antiphishing-bescherming van BitDefender in de huidige webbrowser in/uitgeschakeld.

- **Instellingen** - opent een venster waarin u de instellingen voor de antiphishing-werkbalk kunt opgeven. De volgende opties zijn beschikbaar:
 - ▶ **Real-time antiphishing webbescherming** - detecteert en waarschuwt in real time als een website onderhevig is aan phishing (ingesteld voor diefstal van persoonlijke informatie). Deze optie beheert de antiphishing-beveiliging van BitDefender alleen in de huidige webbrowser.
 - ▶ **Vragen vóór toevoegen aan witte lijst** - vraagt uw bevestiging voordat een website aan de witte lijst wordt toegevoegd.
- **Toevoegen aan Witte lijst** - voegt de huidige website toe aan de Witte lijst.



Opmerking

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

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



Antiphishing Witte lijst

U kunt de lijst weergeven van alle websites die niet door de antiphishing-engines van BitDefender worden gecontroleerd. Als u een site uit de Witte lijst wilt verwijderen, zodat u op de hoogte wordt gebracht van eventuele phishing-bedreigingen op die pagina, klikt u op de knop **Verwijderen** naast de naam van de site.

U kunt de sites die u volledig vertrouwt toevoegen aan de Witte lijst, zodat ze niet langer worden gescand door de antiphishing-engines. Om een site toe te voegen aan de Witte lijst, geeft u het adres van de site op in het overeenkomende veld en kikt u op **Toevoegen**.

- **Rapporteren als phishing** - informeert het BitDefender Lab dat u denkt dat de respectieve website wordt gebruikt voor phishing. Door websites met phishing te rapporteren helpt u andere mensen beschermen tegen identiteitsdiefstal.
- **Help** - opent het Help-bestand.
- **Info** - opent een venster waar u informatie over BitDefender kunt bekijken en waar u hulp kunt zoeken wanneer er zich een onverwachte gebeurtenis voordoet.

28. Integratie in programma's voor expresberichten

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

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

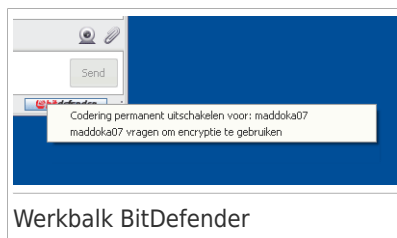
- uw chatpartner een BitDefender-versie heeft geïnstalleerd die IM Encryptie ondersteunt en IM Encryption is ingeschakeld voor de instant messaging applicatie die bij het chatten wordt gebruikt.
- U en uw chatpartner gebruiken ofwel Yahoo Messenger of Windows Live (MSN) Messenger.



Belangrijk

BitDefender zal geen conversatie coderen als een chatpartner een op het web gebaseerde chattoepassing gebruikt, zoals Meebo, of een andere chattoepassing die Yahoo Messenger of MSN ondersteunt.

U kan instant messaging encryptie gemakkelijk configureren met de BitDefender werkbalk in het chatvenster. De werkbalk moet zich onderaan rechts in het chatvenster bevinden. Zoek het BitDefender-logo om de balk te vinden.



Opmerking

De werkbalk geeft aan dat een conversatie gecodeerd is door een kleine sleutel  weer te geven naast het BitDefender-logo.

Wanneer u in de BitDefender-werkbalk klikt, krijgt u de beschikking over de volgende opties:

- **Codering permanent uitschakelen voor contactpersoon.**
- **Contactpersoon uitnodigen om codering te gebruiken.** Om uw conversaties te coderen, moet uw contactpersoon BitDefender installeren en een compatibel IM-programma gebruiken.

Zo werkt het

29. Bestanden en mappen scannen

Het scannen verloopt eenvoudig en flexibel met BitDefender. Er zijn 4 manieren om BitDefender in te stellen voor het scannen van bestanden en mappen op virussen en andere malware.

- Het contextmenu van Windows gebruiken
- Scantaken gebruiken
- BitDefender Handmatig scannen gebruiken
- De balk voor de scanactiviteit gebruiken

Zodra u een scan start, verschijnt de Antivirusscanwizard die u doorheen het proces zal begeleiden. Raadpleeg "*Antivirusscanwizard*" (p. 58) voor gedetailleerde informatie over deze wizard.

29.1. Het contextmenu van Windows gebruiken

Dit is de gemakkelijkste en aanbevolen manier om een bestand of map op uw computer te scannen. Klik met de rechtermuisknop op het object dat u wilt scannen en selecteer **Scannen met BitDefender** in het menu. Volg de Antivirusscanwizard om de scan te voltooien.

Typische situaties voor het gebruik van deze scanmethode zijn ondermeer de volgende:

- U vermoedt dat een specifiek bestand of een specifieke map geïnfecteerd is.
- Wanneer u bestanden waarvan u denkt dat ze mogelijk gevaarlijk zijn, downloadt van internet.
- Scan een netwerkshare voordat u bestanden naar uw computer kopieert.

29.2. Scantaken gebruiken

Als u uw computer of specifieke mappen regelmatig wilt scannen, moet u het gebruik van scantaken overwegen. Scantaken geven BitDefender instructies over de locaties die moeten worden gescand en de scanopties en acties die moeten worden toegepast. Bovendien kunt u ze **plannen** om op regelmatige basis of op een specifiek tijdstip te worden uitgevoerd.

Om uw computer te scannen met scantaken, moet u de BitDefender-interface openen en de gewenste scantaak uitvoeren. Afhankelijk van de weergavemodus van de gebruikersinterface, moeten verschillende stappen worden gevolgd om de scantaak uit te voeren.

Scantaken uitvoeren in de Beginnersmodus

In de Beginnersmodus kunt u alleen een standaard scan van de volledige computer uitvoeren door op **Nu scannen** te klikken. Volg de Antivirusscanwizard om de scan te voltooien.

Scantaken uitvoeren in de Gemiddelde modus

In de Gemiddelde modus kunt u een aantal vooraf geconfigureerde scantaken uitvoeren. U kunt scantaken ook configureren en aangepaste scantaken uitvoeren om specifieke locaties op uw computer te scannen met aangepaste scanopties. Volg deze stappen om een scantaak uit te voeren in de Gemiddelde modus.

1. Klik op het tabblad **Antivirus**.
2. Klik links in het gebied Snelle taken op **Systeemsan** om een standaard scan van de volledige computer te starten. Om een andere scantaak uit te voeren, klikt u op de pijl  op de knop en selecteert u de gewenste scantaak. Klik op **Aangepaste scan** om een aangepaste scan te configureren en uit te voeren. Dit zijn de beschikbare scantaken:

Scantaak	Beschrijving
Systeemsan	Scant het volledige systeem, behalve archieven. In de standaardconfiguratie scant het systeem op alle types malware, behalve op rootkits .
Diepe systeemsan	Scant het volledige systeem. In de standaardconfiguratie wordt er gescand op alle types malware die de beveiliging van uw systeem bedreigen, zoals virussen, spyware, adware, rootkits en andere.
Mijn documenten scannen	Gebruik deze taak om belangrijke mappen van de huidige gebruiker te scannen. Mijn documenten, Bureaublad en Opstarten. Dit zal de veiligheid van uw documenten, een veilige werkruimte en opgeruimde toepassingen bij het opstarten garanderen.
Aangepast scannen	Deze optie helpt u bij het configureren en uitvoeren van een aangepaste scantaak, zodat u kunt opgeven wat u wilt scannen en de algemene scanopties kunt instellen. U kunt aangepaste scantaken opslaan zodat ze later toegankelijk zijn in de Gemiddelde of Expert-modus.

3. Volg de Antivirusscanwizard om de scan te voltooien. Als u ervoor kiest een aangepaste scan uit te voeren, moet u in de plaats daarvan de wizard Aangepaste scan uitvoeren.

Scantaken uitvoeren in de Expert-modus

In de Expert-modus kunt u alle vooraf geconfigureerde scantaken uitvoeren en hun scanopties wijzigen. Bovendien kunt u aangepaste scantaken maken als u specifieke locaties op uw computer wilt scannen. Volg deze stappen om een scantaak uit te voeren in de Expert-modus.

1. Klik in het menu aan de linkerzijde op **Antivirus**.
2. Klik op het tabblad **Virusscan**. Hier vindt u enkele standaard scantaken en kunt u uw persoonlijke scantaken maken. Dit zijn de standaard scantaken die u kunt gebruiken:

Standaardtaak	Beschrijving
Diepe systeemsan	Scant het volledige systeem. In de standaardconfiguratie wordt er gescand op alle types malware die de beveiliging van uw systeem bedreigen, zoals virussen, spyware, adware, rootkits en andere.
Systeemsan	Scant het volledige systeem, behalve archieven. In de standaardconfiguratie scant het systeem op alle types malware, behalve op rootkits .
Snelle systeemsan	Scant de mappen Windows en Program Files. In de standaardconfiguratie wordt gescand op alle types malware, behalve rootkits, maar het geheugen, het register en de cookies worden niet gescand.
Mijn documenten	Gebruik deze taak om belangrijke mappen van de huidige gebruiker te scannen. Mijn documenten, Bureaublad en Opstarten. Dit zal de veiligheid van uw documenten, een veilige werkruimte en opgeruimde toepassingen bij het opstarten garanderen.

3. Dubbelklik op de scantaak die u wilt uitvoeren.
4. Volg de Antivirusscanwizard om de scan te voltooien.

29.3. BitDefender Handmatig scannen gebruiken

Met BitDefender Handmatig scannen kunt u een specifieke map of harde schijfpartitie scannen zonder dat u een scantaak hoeft te maken. Deze functie is ontwikkeld om te worden gebruikt wanneer Windows in Veilige modus wordt uitgevoerd. Als uw systeem is geïnfecteerd met een hardnekkig virus, kunt u proberen het virus te verwijderen door Windows op te starten in de Veilige modus en elke harde schijfpartitie te scannen met BitDefender Handmatig scannen.

Volg deze stappen om uw computer te scannen met BitDefender Handmatig scannen:

1. Volg in het menu  Start van Windows, het pad **Start → Programma's → BitDefender 2010 → BitDefender Handmatig scannen**. Een nieuw venster wordt weergegeven.
2. Klik op **Map toevoegen** om het scandoel te selecteren. Een nieuw venster wordt weergegeven.
3. Het scandoel selecteren:
 - Om uw bureaublad te scannen, hoeft u alleen **Bureaublad** te selecteren.
 - Om een volledige harde schijfpartitie te scannen, selecteert u de partitie in Deze computer.
 - Om een specifieke map te scannen, zoekt en selecteert u de respectieve map.
4. Klik op **OK**.
5. Klik op **Continue** om het scannen te starten.
6. Volg de Antivirusscanwizard om de scan te voltooien.

Wat is de Veilige modus?

De Veilige modus is een speciale manier om Windows te starten en wordt hoofdzakelijk gebruikt om problemen die de normale werking van Windows beïnvloeden, op te lossen. Dergelijke problemen kunnen lopen van conflicterende stuurprogramma's tot virussen die verhinderen dat Windows normaal wordt gestart. In de Veilige modus laadt Windows slechts een minimum aan componenten van het besturingssysteem en de basisstuurprogramma's. Slechts enkele toepassingen werken in de Veilige modus. Daarom zijn de meeste virussen inactief wanneer Windows in de Veilige modus wordt gebruikt en kunnen ze gemakkelijk worden verwijderd.

Om Windows in de Veilige modus te starten, start u de computer opnieuw op en drukt u op de F8-toets tot het menu Geavanceerde opties voor Windows verschijnt. U kunt kiezen tussen verschillende opties voor het starten van Windows in de Veilige modus. Wij raden u aan **Veilige modus met netwerkmogelijkheden** te selecteren om toegang te krijgen tot het internet.



Opmerking

Meer informatie over de Veilige modus vindt u in het Help en ondersteuningscentrum van Windows (Klik in het menu Start op **Help en ondersteuning**). U kunt ook nuttige informatie vinden door op het internet te zoeken.

29.4. De balk voor de scanactiviteit gebruiken

De **balk Scanactiviteit** is een grafische voorstelling van de scanactiviteit op uw systeem. Dit kleine venster is standaard alleen beschikbaar in de **Expert-modus**.

U kunt de balk voor de scanactiviteit gebruiken om snel bestanden en mappen te scannen. U kunt het bestand of de map die u wilt scannen slepen en neerzetten in de balk Scanactiviteit. Volg de Antivirusscanwizard om de scan te voltooien.



Opmerking

Raadpleeg "*Scan activiteitenbalk*" (p. 33) voor meer informatie.

30. Een computerscan plannen

Het periodiek scannen van uw computer is de beste praktijk om uw computer vrij te houden van malware. Met BitDefender kunt u scantaken plannen zodat u uw computer automatisch kunt scannen.

Volg deze stappen om BitDefender te plannen voor het scannen van uw computer:

1. Open BitDefender en schakel de gebruikersinterface naar de Expert-modus.
2. Klik in het menu aan de linkerzijde op **Antivirus**.
3. Klik op het tabblad **Virusscan**. Hier vindt u enkele standaard scantaken en kunt u uw persoonlijke scantaken maken.

- Er zijn systeemtaken beschikbaar die op elke Windows-gebruikersaccount kunnen worden uitgevoerd.
- Gebruikertaken zijn alleen beschikbaar voor en kunnen alleen worden uitgevoerd door de gebruiker die de taken heeft gemaakt.

Dit zijn de standaard scantaken die u kunt plannen:

Standaardtaak	Beschrijving
Diepe systeemscan	Scant het volledige systeem. In de standaardconfiguratie wordt er gescand op alle types malware die de beveiliging van uw systeem bedreigen, zoals virussen, spyware, adware, rootkits en andere.
Systeemscan	Scant het volledige systeem, behalve archieven. In de standaardconfiguratie scant het systeem op alle types malware, behalve op rootkits .
Snelle systeemscan	Scant de mappen Windows en Program Files. In de standaardconfiguratie wordt gescand op alle types malware, behalve rootkits, maar het geheugen, het register en de cookies worden niet gescand.
Autologon Scan	Scant de items die worden uitgevoerd als een gebruiker zich aanmeldt bij Windows. Om deze taak te gebruiken, moet u deze plannen om te worden uitgevoerd bij het opstarten van het systeem. Standaard is het automatisch scannen bij het aanmelden uitgeschakeld.
Mijn documenten	Gebruik deze taak om belangrijke mappen van de huidige gebruiker te scannen. Mijn documenten,

Standaardtaak	Beschrijving
	Bureaublad en Opstarten. Dit zal de veiligheid van uw documenten, een veilige werkruimte en opgeruimde toepassingen bij het opstarten garanderen.

Als geen enkele van deze scantaken aan uw behoeften voldoet, kunt u een nieuwe scantaak maken die u vervolgens kunt plannen om te worden uitgevoerd volgens de behoefte.

4. Klik met de rechtermuisknop op de gewenste scantaak en selecteer **Planning**. Een nieuw venster wordt weergegeven.
5. De taak plannen om te worden uitgevoerd volgens behoefte:
 - Om de scantaak eenmalig uit te voeren, selecteert u **Eenmalig** en geeft u de startdatum en -tijd op.
 - Om de scantaak uit te voeren na het opstarten van het systeem, selecteert u **Bij opstarten van het systeem**. U kunt opgeven hoe lang na het opstarten de taak moet worden gestart (in minuten).
 - Om de scantaak op regelmatige basis uit te voeren, selecteert u **Periodiek** en geeft u de frequentie en de startdatum en -tijd op.



Opmerking

Om uw computer bijvoorbeeld elke zaterdag om 2 uur 's ochtends uit te voeren, moet u de planning als volgt configureren:

- a. Selecteer **Periodiek**.
 - b. Typ 1 in het veld **Elke** en selecteer vervolgens **weken** in het menu. Op deze manier wordt de taak eenmaal per week uitgevoerd.
 - c. Stel de eerstkomende zaterdag in als startdatum.
 - d. Stel 2:00:00 AM in als starttijd.
6. Klik op **OK** om de planning op te slaan. De scantaak wordt automatisch uitgevoerd volgens de planning die u hebt gedefinieerd. Als de computer is uitgeschakeld wanneer de planning is ingesteld, wordt de taak de volgende keer dat u de computer opstart, uitgevoerd.

Problemen oplossen en hulp vragen

31. Problemen oplossen

Dit hoofdstuk beschrijft enkele problemen die zich kunnen voordoen terwijl u BitDefender gebruikt en biedt u mogelijke oplossingen voor deze problemen. De meeste problemen kunnen worden opgelost door de juiste configuratie van de productinstellingen.

Als u het probleem hier niet kunt vinden of als de voorgestelde oplossingen niet werken, kunt u contact opnemen met vertegenwoordigers van de technische ondersteuning van BitDefender zoals beschreven in hoofdstuk "*Supportcentrum*" (p. 238).

31.1. Installatieproblemen

Dit artikel helpt u bij het oplossen van enkele van de meest gebruikelijke installatieproblemen met BitDefender. Deze problemen kunnen worden gegroepeerd in de volgende categorieën:

- **Validatiefouten installatie:** de installatiewizard kan niet worden uitgevoerd vanwege specifieke voorwaarden op uw systeem.
- **Mislukte installaties:** U hebt de installatie gestart vanaf de installatiewizard, maar deze is niet gelukt.

31.1.1. Validatiefouten installatie

Wanneer u de installatiewizard start, worden een aantal voorwaarden gecontroleerd om het starten van de installatie te valideren. In de volgende tabel vindt u de vaakst voorkomende validatiefouten voor de installatie en de oplossingen om ze te overwinnen.

Fout	Beschrijving&oplossing
U hebt onvoldoende bevoegdheden om het programma te installeren.	Om de installatiewizard uit te voeren en BitDefender te installeren, hebt u beheerdersbevoegdheden nodig. Voer een van de volgende bewerkingen uit: ● Meld u aan bij een Windows-beheerdersaccount en voer de installatiewizard opnieuw uit. ● Klik met de rechtermuisknop op het installatiebestand en selecteer Uitvoeren als. Typ de gebruikersnaam en het wachtwoord van een Windows-beheerdersaccount op het systeem.
Het installatieprogramma heeft ontdekt dat een	BitDefender was eerder op uw systeem geïnstalleerd, maar de installatie is niet volledig verwijderd. Deze

Fout	Beschrijving&oplossing
eerdere versie van BitDefender niet goed is verwijderd.	toestand blokkeert een nieuwe installatie van BitDefender. Volg deze stappen om deze fout op te lossen en BitDefender te installeren: 1. Ga naar www.bitdefender.com/uninstall en download het hulpprogramma voor het verwijderen op uw computer. 2. Voer het hulpprogramma voor het verwijderen uit met beheerdersbevoegdheden. 3. Start uw computer opnieuw op. 4. Start de installatiewizard opnieuw om BitDefender te installeren.
Het BitDefender-product is niet compatibel met uw besturingssysteem.	U probeert BitDefender te installeren op een niet-ondersteund besturingssysteem. Raadpleeg "<i>Systeemvereisten</i>" (p. 2) om uit te zoeken op welke besturingssystemen u BitDefender kunt installeren. Als uw besturingssysteem Windows XP met Service Pack 1 of zonder service pack is, kunt u Service Pack 2 of hoger installeren en daarna de installatiewizard opnieuw uitvoeren.
Het installatiebestand is ontworpen voor een ander type processor.	Als een dergelijke fout optreedt, probeert u een onjuiste versie van het installatiebestand uit te voeren. Er zijn twee versies van het installatiebestand van BitDefender: één voor 32-bits processors en een andere voor 64-bits processors. Download het installatiebestand direct van www.bitdefender.com om zeker te zijn dat u de juiste versie voor uw systeem hebt.

31.1.2. Mislukte installatie

Er zijn meerdere oorzaken waardoor de installatie mislukt:

- Tijdens de installatie verschijnt een foutvenster. U kunt worden gevraagd de installatie te annuleren of er kan een knop worden opgegeven voor het uitvoeren van een verwijderingsprogramma dat het systeem zal opruimen.



Opmerking

Onmiddellijk nadat de installatie is gestart, kunt u een melding krijgen dat er onvoldoende vrije schijfruimte is om BitDefender te installeren. Maak in een dergelijk geval de vereiste hoeveelheid schijfruimte vrij op de partitie waar u BitDefender wilt installeren en hervat of herstart vervolgens de installatie.

- De installatie blijft hangen en eventueel loopt uw systeem vast. Het systeem zal alleen opnieuw reageren nadat het opnieuw is opgestart.
- De installatie is voltooid, maar u kunt slechts enkele of helemaal geen BitDefender-functies gebruiken.

Om de oorzaken voor een mislukte installatie op te lossen en BitDefender te installeren, volgt u deze stappen:

1. **Ruim het systeem op nadat de installatie is mislukt.** Als de installatie mislukt, kunnen er enkele registersleutels en bestanden van BitDefender achterblijven op uw systeem. Dergelijke herinneringen kunnen een nieuwe installatie van BitDefender verhinderen. Ze kunnen ook de prestaties en stabiliteit van het systeem beïnvloeden. Daarom moet u ze verwijderen voordat u probeert het product opnieuw te installeren.

Als het foutvenster een knop beschikbaar stelt voor het uitvoeren van een hulpprogramma voor het verwijderen, klikt u op die knop om het systeem op te ruimen. Ga anders als volgt te werk:

- a. Ga naar www.bitdefender.com/uninstall en download het hulpprogramma voor het verwijderen op uw computer.
 - b. Voer het hulpprogramma voor het verwijderen uit met beheerdersbevoegdheden.
 - c. Start uw computer opnieuw op.
2. **Controleer de mogelijke oorzaken van de mislukte installatie.** Voordat u doorgaat met het opnieuw installeren van het product, moet u de mogelijke situaties die het mislukken van de installatie hebben veroorzaakt, controleren en oplossen:
 - a. Controleer of er een andere beveiligingsoplossing is geïnstalleerd. Dit kan de normale werking van BitDefender verstoren. Als dat het geval is, raden wij u aan alle andere beveiligingsoplossingen te verwijderen en vervolgens BitDefender opnieuw te installeren.
 - b. U moet controleren of uw systeem is geïnfecteerd. Voer een van de volgende bewerkingen uit:
 - Gebruik de reddingsschijf van BitDefender om uw computer te scannen en alle bestaande bedreigingen te verwijderen. Meer informatie vindt u onder **"BitDefender reddingsschijf"** (p. 241).

- Open een Internet Explorer-venster, ga naar www.bitdefender.com en voer een online scan uit (klik op de knop **online scannen**).
- 3. Probeer BitDefender opnieuw te installeren. Het is aanbevolen de nieuwste versie van het installatiebestand van www.bitdefender.com te downloaden en uit te voeren.
- 4. Als de installatie opnieuw mislukt, moet u contact opnemen met BitDefender voor ondersteuning, zoals beschreven in "*Supportcentrum*" (p. 238).

31.2. De BitDefender-services reageren niet

Dit artikel helpt u bij het oplossen van de foutmelding *BitDefender-services reageren niet*. U kunt deze fout aantreffen als volgt:

- Het BitDefender-pictogram in het **systeemvak** wordt grijs weergegeven en een pop-upbericht laat u weten dat de BitDefender-services niet reageren.
- Het BitDefender-venster geeft aan dat de BitDefender-services niet reageren.

De fout kan worden veroorzaakt door een van de volgende omstandigheden:

- er wordt een belangrijke update geïnstalleerd.
- tijdelijke communicatiefouten tussen de BitDefender-services.
- sommige BitDefender-services zijn gestopt.
- andere beveiligingsoplossingen worden op hetzelfde ogenblik als BitDefender uitgevoerd.
- virussen op uw systeem beïnvloeden de normale werking van BitDefender.

Probeer de volgende oplossingen om deze fouten op te lossen:

1. Wacht enkele ogenblikken en kijk of er iets verandert. De fout kan tijdelijk zijn.
2. Start de computer opnieuw op en wacht enkele ogenblikken tot BitDefender is geladen. Open BitDefender om te zien of de fout blijft bestaan. Het probleem wordt doorgaans opgelost door de computer opnieuw op te starten.
3. Controleer of er een andere beveiligingsoplossing is geïnstalleerd. Dit kan de normale werking van BitDefender verstoren. Als dat het geval is, raden wij u aan alle andere beveiligingsoplossingen te verwijderen en vervolgens BitDefender opnieuw te installeren.
4. Als de fout zich blijft voordoen, kan het een ernstiger probleem vormen (u kunt bijvoorbeeld geïnfecteerd zijn door een virus dat BitDefender hindert). Neem contact op met BitDefender voor ondersteuning, zoals beschreven in sectie "*Supportcentrum*" (p. 238).

31.3. Het verwijderen van BitDefender is mislukt

Dit artikel helpt u bij het oplossen van fouten die zich kunnen voordoen bij het verwijderen van BitDefender. Er zijn twee mogelijke situaties:

- Tijdens het verwijderen, verschijnt een foutvenster. Het scherm biedt een knop voor het uitvoeren van een hulpprogramma voor het verwijderen waarmee het systeem zal worden opgeruimd.
- De procedure voor het verwijderen blijft hangen, uw systeem loopt eventueel vast. Klik op **Annuleren** om het verwijderen af te breken. Start het systeem opnieuw op als dit niet werkt.

Als het verwijderen mislukt, kunnen er enkele registersleutels en bestanden van BitDefender achterblijven op uw systeem. Dergelijke herinneringen kunnen een nieuwe installatie van BitDefender verhinderen. Ze kunnen ook de prestaties en stabiliteit van het systeem beïnvloeden. Om BitDefender volledig van uw systeem te verwijderen, moet u het hulpprogramma voor het verwijderen uitvoeren.

Als het verwijderen mislukt en een foutvenster verschijnt, klikt u op de knop om het hulpprogramma voor het verwijderen uit te voeren om het systeem op te ruimen. Ga anders als volgt te werk:

1. Ga naar www.bitdefender.com/uninstall en download het hulpprogramma voor het verwijderen op uw computer.
2. Voer het hulpprogramma voor het verwijderen uit met beheerdersbevoegdheden. Met het hulpprogramma voor het verwijderen worden alle bestanden en registersleutels verwijderd die niet tijdens het automatisch verwijderen werden verwijderd.
3. Start uw computer opnieuw op.

Als deze informatie niet nuttig was, kunt u contact opnemen met BitDefender voor ondersteuning, zoals beschreven in de sectie "*Supportcentrum*" (p. 238).

32. Supportcentrum

De laboratoria van Editions Profil en BitDefender garanderen een technische ondersteuning voor alle producten die door ons development team worden onderhouden. Het kan zijn dat we u in het kader van een technisch probleem zullen voorstellen de versie van uw product gratis op te waarderen.

Deze service biedt ondersteuning voor vragen of problemen die te maken hebben met standaardtoepassingen voor de eindgebruiker of voor bedrijven, zoals:

- Gepersonaliseerde configuraties van de BitDefender programma's.
- Gebruiksadviezen met betrekking tot individuele werkstations of eenvoudige netwerken.
- Technische problemen na de installatie van BitDefender producten.
- Ondersteuning bij het bestrijden van malware-activiteiten op het systeem.
- Toegang tot onze site met veelgestelde vragen en tot onze site voor gepersonaliseerd onderhoud, die 24u/24 en 7d/7 bereikbaar is via: <http://www.bitdefender.fr/site/KnowledgeBase/liveAssistance>
- Toegang tot onze afdeling internationale ondersteuning, waar onze medewerkers 7d/7 en 365d/jr via online chat-sessies informatie verschaffen en oplossingen bieden. Om toegang te krijgen tot deze ondersteuning, dient u het volgende adres op te geven in uw internetbrowser: <http://www.bitdefender.fr/site/KnowledgeBase/liveAssistance>.

Let op: aangezien het hier gaat om een internationale service, wordt de ondersteuning voornamelijk in het Engels geboden.

Telefonische ondersteuning:

De laboratoria van Editions Profil en BitDefender stellen alles in het werk om de toegang tot telefonische ondersteuning te kunnen garanderen, tijdens plaatselijke werkuren van maandag tot en met vrijdag, met uitzondering van feestdagen.

Telefonische toegang tot de laboratoria van Editions Profil en BitDefender:

- **Belgium:** 070 35 83 04
- **Netherlands:** 020 788 61 50

Zorg voordat u ons belt dat u de volgende zaken binnen handbereik hebt:

- het licentie nummer van uw BitDefender programma. Geef dit nummer door aan een van onze technici zodat hij kan nagaan op welk type ondersteuning u recht hebt.
- de actuele versie van uw besturingssysteem.

- informatie met betrekking tot de merken en modellen van alle op uw computer aangesloten randapparaten en van de software die in het geheugen is geladen of in gebruik is.

In het geval er een virus is ontdekt, kan de technicus u vragen om een lijst met technische informatie en bepaalde bestanden door te sturen, die mogelijk anderszins nodig zijn voor het stellen van een diagnose.

Indien een technicus u om foutmeldingen vraagt, geef dan de exacte inhoud door en het moment waarop de meldingen verschenen, de activiteiten die eraan voorafgingen en de stappen die u zelf reeds hebt ondernomen om het probleem op te lossen.

De technicus zal een strikte procedure opvolgen in een poging het probleem op te sporen.

De volgende elementen vallen niet binnen de service:

- Deze technische ondersteuning heeft geen betrekking op de toepassingen, installaties, de deïnstallatie, de overdracht, preventief onderhoud, de vorming, het beheer op afstand of andere softwareconfiguraties dan diegene die tijdens de interventie specifiek door onze technicus werden vermeld.
- De installatie, de instellingen, de optimalisering en de netwerkconfiguratie of de configuratie op afstand van toepassingen die niet binnen het kader van de geldende ondersteuning vallen.
- Back-ups van software/gegevens. De klant dient zelf een back-up te maken van alle gegevens, software en bestaande programma's die aanwezig zijn op de informatiesystemen waarop onze ondersteuning van toepassing is, alvorens enige dienstprestatie te laten uitvoeren door Editions Profil en BitDefender.

Editions Profil of BitDefender KUNNEN IN GEEN GEVAL AANSPRAKELIJK WORDEN GESTELD VOOR HET VERLIES OF DE RECUPERATIE VAN GEGEVENS, PROGRAMMA'S, OF VOOR HET NIET KUNNEN BENUTTEN VAN SYSTEMEN OF VAN HET NETWERK.

Adviezen beperken zich enkel tot de gestelde vragen en zijn gebaseerd op de door de klant verschaft informatie. De problemen en mogelijke oplossingen kunnen afhangen van het type systeemomgeving en van een groot aantal andere variabelen waarvan Editions Profil of BitDefender niet op de hoogte zijn.

Editions Profil of BitDefender kunnen dan ook in geen geval aansprakelijk worden gesteld voor eventuele schade die voortvloeit uit het gebruik van de verschaft informatie.

Het kan zijn dat het systeem waarop de BitDefender programma's moeten worden geïnstalleerd onstabiel is (eerdere virusinfecties, installatie van meerdere antivirus - of beveiligingsprogramma's, etc.). In betreffende gevallen zal een technicus u mogelijk voorstellen eerst een onderhoudsbeurt op uw systeem te laten uitvoeren, alvorens het probleem kan worden opgelost.

De technische gegevens kunnen wijzigen op het moment dat er nieuwe gegevens beschikbaar zijn. Om die reden raden Editions Profil en BitDefender u dan ook aan regelmatig onze site "Producten" te raadplegen, via <http://www.bitdefender.com/nl> voor upgrades, of onze site met veelgestelde vragen (FAQ) op <http://supportbd.com>.

Editions Profil en BitDefender wijzen elke aansprakelijkheid af voor enige rechtstreekse, onrechtstreekse, bijzondere of accidentele schade, of voor gevolgschade die te wijten is aan het gebruik van de aan u verschaft informatie.

Indien een interventie ter plaatse noodzakelijk is, zal de technicus u meer gedetailleerde informatie verschaffen met betrekking tot de dichtstbijzijnde wederverkoper.

BitDefender reddingsschijf

33. Overzicht

BitDefender Antivirus 2010 wordt geleverd met een opstartbare CD (BitDefender reddingsschijf) die in staat is alle bestaande harde schijven te scannen en te desinfecteren voordat uw besturingssysteem opstart.

Gebruik telkens de BitDefender reddingsschijf wanneer uw besturingssysteem niet correct werkt door virusinfecties. Dit gebeurt doorgaans wanneer u geen antivirusproduct gebruikt.

Telkens wanneer u de BitDefender reddingsschijf opstart, wordt de update van de virussignaturen automatisch uitgevoerd, zonder tussenkomst van de gebruiker.

De BitDefender reddingsschijf is een geremasterde Knoppix-distributie van BitDefender, die de nieuwste BitDefender voor Linux-beveiligingsoplossing integreert in de GNU/Linux Knoppix Live CD en een desktopantivirus biedt die bestaande harde schijven kan scannen en desinfecteren (inclusief Windows NTFS-partities). Op hetzelfde ogenblik kan u de BitDefender reddingsschijf gebruiken om uw waardevolle data te herstellen wanneer u Windows niet kan opstarten.



Opmerking

De BitDefender reddingsschijf kan worden gedownload van deze locatie:
http://download.bitdefender.com/rescue_cd/

33.1. Systeemvereisten

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

Processortype

x86-compatibel, minimum 166 MHz, maar verwacht geen hoge prestaties in dit geval. Een processor van de i686-generatie met 800 MHz is een betere keuze.

Geheugen

Minimum 512 MB RAM-geheugen (1 GB aanbevolen)

Cd-rom

De BitDefender reddingsschijf wordt uitgevoerd vanaf een cd-rom. Daarom is een cd-rom en een BIOS waarmee ervan kan worden opgestart vereist.

Internetverbinding

Hoewel de BitDefender reddingsschijf kan werken zonder internetverbinding, is er toch een actieve http-verbinding vereist voor de updateprocedure, zelfs via een proxyserver. Voor een up-to-date beveiliging is een internetverbinding dus een absolute vereiste.

Grafische resolutie

Standaard SVGA-compatibele grafische kaart.

33.2. Bijgeleverde software

De BitDefender reddingsschijf bevat de volgende softwarepakketten.

Xedit

Dit is een tekstbestandseditor.

Vim

Dit is een krachtige tekstbestandseditor die syntaxmarkering, een GUI en veel meer bevat. Meer informatie vindt u op de [Vim-startpagina](#).

Xcalc

Dit is een rekenmachine.

RoxFiler

RoxFiler is een snel en krachtig grafisch bestandsbeheer.

Meer informatie vindt u op de [RoxFiler-startpagina](#).

MidnightCommander

GNU Midnight Commander (mc) is een beheerprogramma voor tekstmodusbestanden.

Meer informatie vindt u op de [MC-startpagina](#).

Pstree

Pstree toont de actieve processen.

Top

Top toont Linux-taken.

Xkill

Xkill vernietigt een client door middel van zijn X-bronnen.

Partition Image

Met Partition Image kunt u partities in de bestandssysteemformaten EXT2, Reiserfs, NTFS, HPFS, FAT16 en FAT32 opslaan naar een imagebestand. Dit programma kan nuttig zijn voor back-updoeleinden.

Meer informatie vindt u op de [Partimage-startpagina](#).

GtkRecover

GtkRecover is een GTK-versie van het consoleprogrammaherstel. Het helpt u een bestand te herstellen.

Meer informatie vindt u op de [GtkRecover-startpagina](#).

ChkRootKit

ChkRootKit is een hulpprogramma dat u helpt uw computer te scannen op rootkits.

Meer informatie vindt u op de [ChkRootKit-startpagina](#).

Nessus Network Scanner

Nessus is een externe beveiligingsscanter voor Linux, Solaris, FreeBSD en Mac OS X.

Meer informatie vindt u op de [Nessus-startpagina](#).

Iptraf

Iptraf is een programma voor IP-netwerkbewaking.

Meer informatie vindt u op de [Iptraf-startpagina](#).

Iftop

Iftop toont het bandbreedtegebruik op een interface.

Meer informatie vindt u op de [Iftop-startpagina](#).

MTR

MTR is een netwerkdiagnosehulpprogramma.

Meer informatie vindt u op de [MTR-startpagina](#).

PPPStatus

PPPStatus toont statistieken over het binnenkomende en uitgaande TCP/IP-verkeer.

Meer informatie vindt u op de [PPPStatus-startpagina](#).

Wavemon

Wavemon is een bewakingstoepassing voor draadloze netwerkapparaten.

Meer informatie vindt u op de [Wavemon-startpagina](#).

USBView

USBView toont informatie over apparaten die zijn aangesloten op de USB-bus.

Meer informatie vindt u op de [USBView-startpagina](#).

Pppconfig

Pppconfig helpt bij het automatisch tot stand brengen van een ppp-inbelverbinding.

DSL/PPPoE

DSL/PPPoE configureert PPPoE-verbinding (ADSL).

I810rotate

I810rotate schakelt de video-uitvoer op i810-hardware door middel van de i810switch(1).

Meer informatie vindt u op de [I810rotate-startpagina](#).

Mutt

Mutt is een krachtige, op tekst gebaseerde MIME-mailclient.

Meer informatie vindt u op de [Mutt-startpagina](#).

Mozilla Firefox

Mozilla Firefox is een bekende webbrowser.

Meer informatie vindt u op de [Mozilla Firefox-startpagina](#).

Elinks

Elinks is een webbrowser in tekstmodus.

Meer informatie vindt u op de [Elinks-startpagina](#).

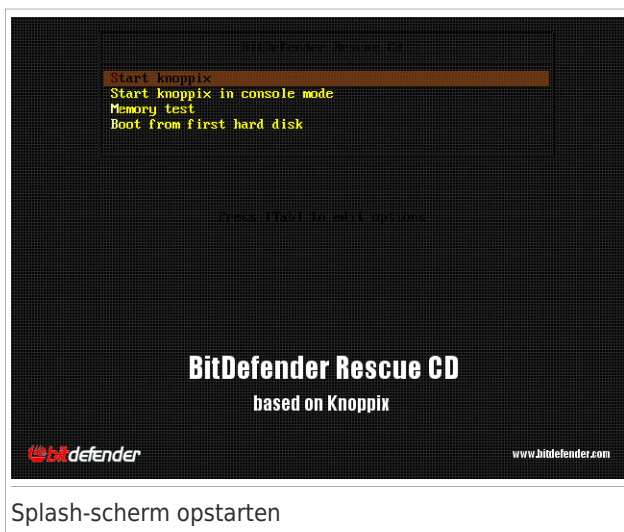
34. De BitDefender reddingsschijf gebruiken

Dit hoofdstuk bevat informatie over het starten en stoppen van de BitDefender reddingsschijf, het scannen van uw computer op malware en het opslaan van gegevens vanaf uw aangetaste Windows-pc naar een verwisselbaar apparaat. Wanneer u de softwaretoepassingen die op de cd zijn geleverd gebruikt, kan u echter veel meer taken uitvoeren dan binnen het bereik van deze handleiding kunnen worden beschreven.

34.1. BitDefender reddingsschijf starten

Om de cd te starten, stelt u de BIOS van uw computer in om te starten vanaf de cd, plaatst u de cd in het cd-romstation en start u de computer opnieuw op. Controleer of uw computer kan opstarten vanaf een cd.

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



Splash-scherm opstarten

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

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



Het bureaublad

34.2. BitDefender reddingsschijf stoppen

Daarna kan u de computer veilig afsluiten door **Afsluiten** te selecteren in het contextafhankelijke menu van de BitDefender reddingsschijf (rechtsklikken om het te openen) of door de opdracht **stoppen** te selecteren op een werkstation.



Kies "AFSLUITEN"

Wanneer de BitDefender reddingsschijf alle programma's met succes heeft afgesloten, ziet u het in de volgende afbeelding weergegeven scherm. U kan de cd verwijderen om opnieuw op te starten vanaf uw harde schijf. U kan nu uw computer veilig uitschakelen of opnieuw opstarten.

```
X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufs) (aufs) (aufs) (aufs)
ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksuspend
) (aio/0) Done.
Waiting for processes to finish.....
Killing processes with signal 9: (init) (aufs) (aufs) (aufs) (aufs)
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/0
A) (khpsbpkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.....
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/in
Turning off swap... Done.
Unmounting remaining file systems.
rootfs unmounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes].
```

Wacht op dit bericht wanneer u afsluit.

34.3. Hoe kan ik een antivirusscan uitvoeren?

Nadat het opstartproces is voltooid, verschijnt een wizard waarmee u een volledige scan van uw computer kunt uitvoeren. Hiervoor hoeft u alleen te klikken op de knop **Start**.



Opmerking

Als uw schermresolutie niet hoog genoeg is, wordt u gevraagd het scannen te starten in de tekstmodus.

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

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



Opmerking

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

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

De problemen worden weergegeven in groepen. Klik op het vakje "+" om een groep te openen of op het vakje "-" om een groep te sluiten.

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

3. U kan een samenvatting van de resultaten zien.

Als u alleen een bepaalde map wilt scannen, kunt u een van de volgende alternatieven gebruiken:

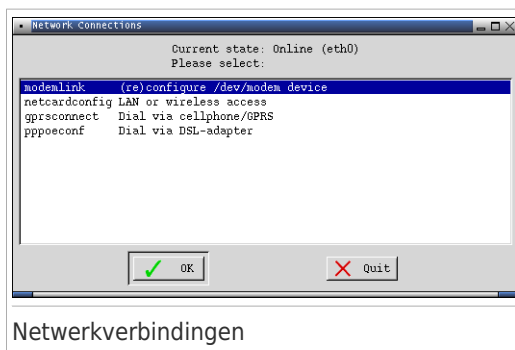
- Gebruik **BitDefender Scanner for Unices**.
 1. Dubbelklik op het bureaublad op het pictogram START SCANNER. Hierdoor wordt **BitDefender Scanner for Unices** gestart.
 2. Klik op **Scanner**. Een nieuw venster wordt weergegeven.
 3. Selecteer de map die u wilt scannen en klik op **Openen** om het scannen te starten met dezelfde wizard die ook is verschenen wanneer u de eerste keer hebt opgestart.
- Gebruik het snelmenu - blader door uw mappen, klik met de rechtermuisknop op een bestand of map en selecteer **Verzenden naar**. Kies vervolgens **BitDefender Scanner**.
- U kunt ook de volgende opdracht als hoofdmap opgeven vanaf een terminal. De **BitDefender Antivirusscanner** zal starten met het geselecteerde bestand of de map als de standaardlocatie voor het scannen.

```
# bdsan /path/to/scan/
```

34.4. Hoe configureer ik de internetverbinding?

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

1. Dubbelklik op de snelkoppeling Netwerkverbindingen op het bureaublad. Het volgende venster verschijnt.



2. Selecteer het type verbinding dat u gebruikt en klik op OK.

Verbinding	Beschrijving
modemlink	Selecteer dit type verbinding als u een modem en een telefoonlijn gebruikt om naar het internet te gaan.
netcardconfig	Selecteer dit type verbinding als u een lokaal netwerk (LAN) gebruikt om naar het internet te gaan. Dit is ook geschikt voor draadloze verbindingen.
gprsconnect	Selecteer dit type verbinding als u naar het internet gaat via een mobiele telefoon met GPRS (General Packet Radio Service) protocol. Natuurlijk kan u ook een RPRS modem gebruiken in plaats van een mobiele telefoon.
pppoeconf	Selecteer dit type verbinding als u een DSL (Digital Subscriber Line) modem gebruikt om naar het internet te gaan.

3. Volg de instructies op het scherm. Als u niet zeker bent wat u moet schrijven, neem dan contact op met uw systeem- of netwerkbeheerder voor details.



Belangrijk

Bedenk dat u alleen het modem activeert door het selecteren van bovengenoemde opties. Volg deze stappen om de netwerkverbinding te configureren.

1. Rechtsklik op het Bureaublad. Het contextafhankelijke menu van de BitDefender reddingsschijf verschijnt.
2. Selecteer **Werkstation (als hoofdmap)**.
3. Typ de volgende commando's:

```
# pppconfig
```

4. Volg de instructies op het scherm. Als u niet zeker bent wat u moet schrijven, neem dan contact op met uw systeem- of netwerkbeheerder voor details.

34.5. Hoe kan ik BitDefender updaten?

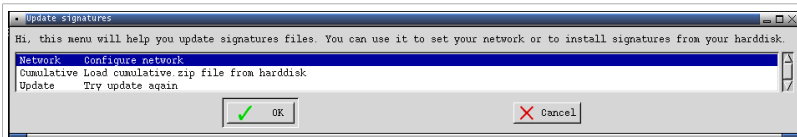
Bij het opstarten wordt de update van de virushandtekeningen automatisch uitgevoerd. Als u deze stap echter hebt overgeslagen of als u gewoon een update wilt uitvoeren na het opstarten, kunt u een van de deze werkwijzen volgen.

● Gebruik **BitDefender Scanner for Unices**.

1. Dubbelklik op het bureaublad op het pictogram START SCANNER. Hierdoor wordt **BitDefender Scanner for Unices** gestart.
2. Klik op **Update**.

● Gebruik de snelkoppeling **Update signaturen** op het bureaublad.

1. Dubbelklik op de snelkoppeling Update signatures op het bureaublad. Het volgende venster verschijnt.



Update signatures

2. U kunt een van de volgende methoden gebruiken:
 - Selecteer **Cumulatief** voor het installeren van reeds op uw harde schijf opgeslagen signaturen door te bladeren in uw computer en het laden van het `cumulative.zip` bestand.
 - Selecteer **Update** om direct verbinding met het internet te maken en de laatste virus signaturen te downloaden.
3. Klik op **OK**.

34.5.1. Hoe kan ik BitDefender updaten over een proxy?

Als er een proxyserver tussen uw computer en internet is, moeten enkele configuraties worden uitgevoerd om de virushandtekeningen bij te werken.

Om BitDefender bij te werken via een proxy, moet u een van de volgende opties gebruiken:

- Gebruik **BitDefender Scanner for Unices**.
 1. Dubbelklik op het bureaublad op het pictogram START SCANNER. Hierdoor wordt **BitDefender Scanner for Unices** gestart.
 2. Klik op **Instellingen**. Een nieuw venster wordt weergegeven.
 3. Schakel onder **Update-instellingen** het selectievakje **HTTP-proxy inschakelen** in. Geef de proxyhost op (als volgt op te geven: `host[:poort]`), Proxygebruiker (als volgt op te geven: `[domein\]gebruikersnaam`) en wachtwoord. Selecteer de **Proxyserver niet gebruiken indien niet beschikbaar** in voor het gebruik van een directe verbinding als de proxyserver niet beschikbaar is.
 4. Klik op **Opslaan**.
 5. Klik op **Update**.
- Terminal gebruiken (als hoofdmap).
 1. Rechtsklik op het Bureaublad. Het contextafhankelijke menu van de BitDefender reddingsschijf verschijnt.
 2. Selecteer **Werkstation (als hoofdmap)**.
 3. Typ het commando: `cd /ramdisk/BitDefender-scanner/etc`.
 4. Typ het commando: `mcedit bdscan.conf` om dit bestand te bewerken met behulp van GNU Midnight Commander (mc).

5. Verwijder de toelichting van de volgende regel: `#HttpProxy =` (verwijder alleen het `#` teken) en geef het domein, gebruikersnaam, wachtwoord en serverpoort van de proxy server aan. De betreffende regel kan er, bijvoorbeeld, als volgt uitzien:
`HttpProxy = myuser:mypassword@proxy.company.com:8080`
6. Druk op **F2** om het actuele bestand op te slaan, bevestig het opslaan, en druk dan op **F10** om het te sluiten.
7. Typ het commando: **bdscan update**.

34.6. Hoe kan ik mijn gegevens opslaan?

Laten we veronderstellen dat u uw Windows-pc door enkele onbekende problemen niet meer kan opstarten. U moet echter tegelijkertijd absoluut toegang krijgen tot enkele belangrijke gegevens op uw computer. Dit is het ogenblik waarop de BitDefender reddingsschijf in actie komt.

Volg deze stappen om gegevens van de computer op te slaan naar een verwisselbaar apparaat, zoals een usb-geheugenstick:

1. Plaats de BitDefender reddingsschijf in het cd-romstation. Steek de geheugenstick in de usb-aansluiting en start de computer opnieuw op.



Opmerking

Als u de geheugenstick op een later moment inpluigt, moet u de hardware op de volgende manier verbinden:

- a. Dubbelklik op de snelkoppeling Terminal emulator op het bureaublad.
- b. Typ het volgende commando:

```
# mount /media/sdb1
```

Afhankelijk van uw computer configuratie kan dit `sda1` zijn, in plaats van `sdb1`.

2. Wacht tot de BitDefender reddingsschijf volledig is opgestart. Het volgende venster verschijnt.



Bureaubladscherm

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



Opmerking

Wanneer u met de BitDefender reddingsschijf werkt, krijgt u te maken met partitienamen van het Linux-type. Zo zal [sda1] waarschijnlijk overeenkomen met de (C:)-partitie van het Windows-type, [sda3] met (F:) en [sdb1] met de geheugenstick.



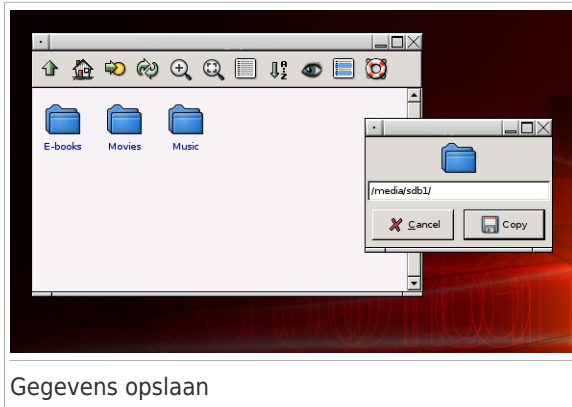
Belangrijk

Als de computer niet correct was afgesloten, is het mogelijk dat sommige partities niet automatisch zijn geopend. Volg deze stappen om een partitie te openen.

- a. Dubbelklik op de snelkoppeling Terminal emulator op het bureaublad.
- b. Typ het volgende commando:

```
# mount /media/partition_name
```

4. Blader door uw mappen en open de gewenste map. Bijvoorbeeld: Mijn gegevens dat de submappen Films, Muziek en E-boeken bevat.
5. Klik met de rechtermuisknop op de gewenste map en selecteer **Kopiëren**. Het volgende venster verschijnt.



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

Afhankelijk van uw computer configuratie kan dit sda1 zijn, in plaats van sdb1.

34.7. Hoe moet ik de consolemodus gebruiken?

Als uw schermresolutie niet hoog genoeg is om de grafische gebruikersinterface uit te voeren, kunt u de BitDefender reddingsschijf in de consolemodus gebruiken. Met de eenvoudige tekstmodus kunt u een volledige scan van uw computer uitvoeren.

Om de cd te starten in de consolemodus, 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. Wacht tot het splashscherm bij het opstarten verschijnt en selecteer **Knoppix starten in de consolemodus**.

Volg de instructies op het scherm na het opstarten om een complete scan van uw computer uit te voeren.

BitDefender detecteert de partities op uw harde schijf en werkt automatisch de database van malwarehandtekeningen bij voordat het scannen wordt gestart. Als er geïnfecteerde bestanden zijn gevonden, zal BitDefender ze desinfecteren. Nadat het scanproces is voltooid, wordt het scanlogboek weergegeven.



Opmerking

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

Woordenlijst

ActiveX

ActiveX is een model voor het schrijven van programma's zodat andere programma's en het besturingssysteem ze kunnen oproepen. De ActiveX-technologie wordt gebruikt bij Microsoft Internet Explorer om interactieve Webpagina's te maken die eruitzien en zich gedragen als computerprogramma's in plaats van statische pagina's. Met ActiveX kunnen gebruikers vragen stellen of beantwoorden, drukknoppen gebruiken en op andere manieren interactief omgaan met de Webpagina. ActiveX-besturingselementen zijn vaak geschreven met de hulp van Visual Basic.

ActiveX is berucht door een compleet gebrek aan beveiligingscontroles; computerbeveiligingsexperts raden het gebruik ervan via het Internet sterk af.

Adware

Adware wordt vaak gecombineerd met een hosttoepassing die gratis wordt aangeboden op voorwaarde dat de gebruiker akkoord gaat met het uitvoeren van de adware. Omdat adware-toepassingen doorgaans worden geïnstalleerd nadat de gebruiker een licentieovereenkomst die het doel van de toepassing vermeldt heeft geaccepteerd, wordt er geen inbreuk gepleegd.

Pop-upadvertenties kunnen echter irritant worden en in sommige gevallen de systeemprestaties negatief beïnvloeden. De gegevens die door sommige van deze toepassingen worden verzameld, kunnen bovendien privacy-problemen veroorzaken voor gebruikers die niet volledig op de hoogte waren van de voorwaarden van de licentieovereenkomst.

Archief

Een schijf, tape, of map die bestanden bevat waarvan een back-up werd gemaakt.

Een bestand dat één of meer bestanden bevat in een gecomprimeerd formaat.

Achterdeur

Een gat in de beveiliging van een systeem, dat opzettelijk werd achtergelaten door ontwikkelaars of beheerders. De motivatie voor dergelijke gaten is niet altijd boosaardig. Sommige besturingssystemen worden bijvoorbeeld geleverd met bevoegde accounts die bedoeld zijn voor gebruik door technici voor service ter plaatse of onderhoudsprogrammeurs van de leverancier.

Opstartsector

Een sector aan het begin van elke schijf die de architectuur van de schijf identificeert (sectorgrootte, clustergrootte, enz.) Bij opstartschijven bevat de opstartsector ook een programma dat het besturingssysteem laadt.

Opstartsectorvirus

Een virus dat de opstartsector van een vaste schijf of een diskette infecteert. Wanneer u probeert op te starten vanaf een diskette die geïnfecteerd is met een opstartsectorvirus, zal het virus actief worden in het geheugen. Wanneer u daarna uw systeem opstart, zal het virus telkens in het geheugen actief zijn.

Browser

De korte naam voor Webbrowser, een softwaretoepassing die wordt gebruikt op Webpagina's te zoeken en weer te geven. De twee populairste browsers zijn Netscape Navigator en Microsoft Internet Explorer. Beide zijn grafische browsers. Dit betekent dat ze zowel grafische beelden als tekst kunnen weergeven. Bovendien kunnen de meeste moderne browsers ook multimedia-informatie weergeven met geluid en video, hoewel voor sommige formaten plug-ins vereist zijn.

Opdrachtregel

In een opdrachtregelinterface typt de gebruiker opdrachten in opdrachttaal rechtstreeks op het scherm in de ruimte die hiervoor wordt geboden.

Cookie

Binnen de Internetindustrie worden cookies beschreven als kleine programma's die informatie bevatten over individuele computers, die door adverteerders wordt geanalyseerd en gebruikt om uw online interesse en smaak te volgen. De cookietechnologie wordt in dit kader nog steeds verder ontwikkeld met het doel reclameberichten rechtstreeks te richten op de interesses die u hebt meegedeeld. Dit is voor veel mensen een mes dat aan twee kanten snijdt. Aan de ene kant is het efficiënt en relevant aangezien u alleen reclames ontvangt voor zaken waarvoor u interesse hebt. Aan de andere kant betekent het ook dat elke plaats die u bezoekt en alles wat u aanklikt wordt "opgespoord" en "gevolgd". Het is dan ook te begrijpen dat er heel wat wordt gedebatteerd over privacy. Bovendien zijn veel mensen verontwaardigd omdat ze het gevoel hebben dat ze als een "SKU-nummer" worden beschouwd (u weet wel, de barcode op de verpakkingen die bij de kassa van het warenhuis wordt gescand). Hoewel dit standpunt misschien nogal extreem is, is het in sommige gevallen wel juist.

Schijfstation

Dit is een apparaat dat gegevens leest van en schrijft naar een schijf.

Een harde-schijfstation leest en schrijft harde schijven.

Een diskettestation opent diskettes.

Schijfstations kunnen intern (binnen de behuizing van een computer) of extern zijn (in een afzonderlijke behuizing die op de computer wordt aangesloten).

Downloaden

Om gegevens (meestal een volledig bestand) te kopiëren van een hoofdbron naar een randapparaat. De term wordt vaak gebruikt om het proces te

beschrijven waarbij een bestand van een on line-service wordt gekopieerd naar de eigen computer. Downloaden kan ook verwijzen naar het kopiëren van een bestand van een netwerkbestandsserver naar een computer in het netwerk.

E-mail

Elektronische post. Een dienst die berichten naar computers verzendt via lokale of globale netwerken.

Gebeurtenissen

Een actie of gebeurtenis die door een programma wordt gedetecteerd. Gebeurtenissen kunnen gebruikersacties zijn, zoals het klikken met de muis of het indrukken van een toets, of systeemgebeurtenissen, zoals een tekort aan geheugen.

Vals positief

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

Bestandsnaamextensie

Het gedeelte van een bestandsnaam achter de punt, waarmee het gegevenstype dat in het bestand is opgeslagen wordt aangeduid.

Heel wat besturingssystemen, zoals Unix, VMS en MS-DOS, maken gebruik van bestandsnaamextensies. Ze gebruiken doorgaans één tot drie letters (sommige oude besturingssystemen ondersteunen niet meer dan drie letters). Voorbeelden hiervan zijn "c" voor C-broncode, "ps" voor PostScript, "txt" voor tekst zonder opmaak.

Heuristisch

Een methode voor het identificeren van nieuwe virussen op basis van regels. Deze scanmethode steunt niet op specifieke virussignatures. Het voordeel van de heuristische scan is dat hij zich niet laat misleiden door een nieuwe variant van een bestaand virus. Dit type kan echter af en toe een verdachte code rapporteren in normale programma's, zodat de zogenoemde "valse positieve" rapporten worden gegenereerd.

IP

Internet Protocol - Een routeerbaar protocol in de TCP/OP-protocolreeks die verantwoordelijk is voor de IP-adressering, routing en de fragmentatie en defragmentatie van IP-pakketten.

Java-applet

Een Java-programma dat is ontwikkeld om alleen op een webpagina te worden uitgevoerd. Om een applet op een webpagina te gebruiken, geeft u de naam van het applet op en de grootte (lengte en breedte in pixels) die het applet kan gebruiken. Wanneer de webpagina wordt geopend, downloadt de browser het applet van een server en voert hij het uit op de computer van de gebruiker (de client). Applets onderscheiden zich van toepassingen omdat ze worden beheerd door een streng beveiligingsprotocol.

Zelfs wanneer applets op de client worden uitgevoerd kunnen ze, bijvoorbeeld, geen gegevens lezen van of schrijven naar de computer van de client. Bovendien worden applets verder beperkt zodat ze alleen gegevens kunnen lezen van en schrijven naar hetzelfde domein waarvan ze worden bediend.

Macrovirus

Een type computervirus dat is gecodeerd als een macro die in een document is ingesloten. Talrijke toepassingen, zoals Microsoft Word en Excel, ondersteunen krachtige macrotalen.

Met deze toepassingen kan u een macro in een document insluiten, en die macro telkens laten uitvoeren wanneer het document wordt geopend.

Mailclient

Een e-mailclient is een toepassing waarmee u e-mail kan verzenden en ontvangen.

Geheugen

Interne opslaggebieden in de computer. De term geheugen staat voor gegevensopslag die in de vorm van chips wordt geleverd. Het woord opslag wordt gebruikt voor geheugen dat aanwezig is op tapes of schijven. Elke computer wordt geleverd met een bepaalde hoeveelheid fysiek geheugen, dat meestal het hoofdgeheugen of RAM wordt genoemd.

Niet-heuristisch

Deze scanmethode steunt op specifieke virussignaturen. Het voordeel van de niet-heuristische scan is dat hij zich niet laat misleiden door iets dat kan lijken op een virus en dat hij geen vals alarm genereert.

Ingepakte programma's

Een bestand in een gecomprimeerd formaat. Talrijke besturingssystemen en toepassingen beschikken over opdrachten waarmee u bestanden kunt inpakken, zodat ze minder geheugen in beslag nemen. Veronderstel bijvoorbeeld dat u een tekstbestand hebt dat tien opeenvolgende spatietekens bevat. Normaal zou dit tien bytes opslagruimte vereisen.

Een programma dat bestanden inpakt kan echter de spatietekens vervangen door een speciaal spatiereeks-teken, gevolgd door het aantal spaties dat wordt vervangen. In dit geval hebben de tien spaties slechts twee bytes nodig. Dit is slechts één inpaktechniek, maar er zijn er veel meer.

Pad

De exacte weg naar een bestand op een computer. Deze weg wordt doorgaans beschreven door middel van het hiërarchische bestandssysteem van boven naar beneden.

De route tussen twee willekeurige punten, zoals het communicatiekanaal tussen twee computers.

Phishing

Het onder valse voorwendselen verzenden van een e-mail aan een gebruiker, waarbij de indruk wordt gewekt dat het bericht afkomstig is van een bestaande onderneming, in een poging de gebruiker persoonlijke gegevens te ontfutselen die zullen worden gebruikt voor identiteitsroof. In het e-mailbericht wordt de gebruiker doorverwezen naar een website voor het updaten van persoonlijke gegevens, zoals wachtwoorden en creditcard-, BSN- en bankrekeningnummers, die reeds in het bezit zijn van de rechtmatige organisatie. De website is echter nep en alleen opgezet om de gebruikersgegevens te stelen.

Polymorf virus

Een virus dat zijn vorm wijzigt bij elk bestand dat het infecteert. Aangezien zij geen consequent binair patroon hebben, zijn dergelijke virussen moeilijk te identificeren.

Poort

Een interface op een computer waarop u een apparaat kan aansluiten. PC's hebben verschillende types poorten. Intern zijn er verschillende poorten voor het aansluiten van schijfstations, beeldschermen en toetsenborden. Extern beschikken PC's over poorten voor het aansluiten van modems, printers, muizen en andere randapparatuur.

Bij TCP/IP- en UDP-netwerken, zijn ze een eindpunt voor een logische verbinding. Het poortnummer duidt aan over welk type poort het gaat. Poort 80 wordt bijvoorbeeld gebruikt voor HTTP-verkeer.

Rapportbestand

Een bestand dat de acties weergeeft die zich hebben voorgedaan. BitDefender houdt een rapportbestand bij met het gescande pad, het aantal gescande mappen, archieven en bestanden, en het aantal gevonden geïnfecteerde en verdachte bestanden.

Rootkit

Een rootkit is een set softwarehulpprogramma's die toegang biedt tot een systeem op beheerniveau. Deze term werd voor het eerst gebruikt voor UNIX-besturingssystemen en verwees naar opnieuw gecompileerde hulpprogramma's die indringers beheerrechten verleende, zodat ze hun aanwezigheid konden verbergen zodat ze onzichtbaar bleven voor systeembeheerders.

De belangrijkste rol van rootkits is het verbergen van processen, bestanden, aanmeldingen en logboeken. Ze kunnen ook gegevens onderscheppen van terminals, netwerkverbindingen of randapparaten als ze de geschikte software bevatten.

Rootkits zijn in wezen niet kwaadaardig. Systemen en zelfs sommige toepassingen verbergen kritieke bestanden met de hulp van rootkits. Ze worden echter het vaakst gebruikt om malware of de aanwezigheid van een indringer

op het systeem te verbergen. In combinatie met malware, vormen rootkits een ernstige bedreiging voor de integriteit en beveiliging van een systeem. Ze kunnen het verkeer controleren, achterpoortjes in het systeem maken, bestanden en logboeken wijzigen en detectie vermijden.

Script

Script, een andere term voor een macro of batchbestand, is een lijst opdrachten die kunnen worden uitgevoerd zonder tussenkomst van de gebruiker.

Spam

Elektronische junkmail of berichten van junknieuwsgroepen. Algemeen bekend als ongewenste e-mail.

Spyware

Elke software die heimelijk gebruikersgegevens verzamelt via de internetverbinding van de gebruikers zonder dat hij/zij zich hiervan bewust is, doorgaans voor reclamedoeleinden. Spywaretoepassingen worden doorgaans gebundeld als een verborgen onderdeel van freeware- of sharewareprogramma's die kunnen worden gedownload van het internet. We moeten echter wel vermelden dat de meeste shareware- en freewaretoepassingen geen spyware bevatten. Zodra de spyware is geïnstalleerd, worden de activiteiten van de gebruiker op het Internet gevolgd en wordt deze informatie op de achtergrond naar iemand anders doorgestuurd. Spyware kan ook informatie verzamelen over e-mailadressen en zelfs wachtwoorden en creditcardnummers.

Spyware is vergelijkbaar met een Trojaans paard omdat gebruikers ook in dit geval het product onbewust installeren wanneer ze een ander programma installeren. Een veel voorkomende manier om slachtoffer te worden van spyware is bepaalde P2P-bestandsuitwisselingsprogramma's te downloaden.

Naast het feit dat deze methode onethisch is en een inbreuk op de privacy van de gebruiker betekent, steelt spyware van de gebruiker door de geheugenbronnen van de computer te gebruiken en bandbreedte te verbruiken wanneer de informatie naar de thuisbasis van de spyware wordt verzonden via de internetverbinding van de gebruiker. Aangezien spyware geheugen- en systeembronnen gebruikt, kunnen de toepassingen die op de achtergrond worden uitgevoerd leiden tot systeemfouten of een algemene systeeminstabiliteit.

Opstartitems

Elk bestand in deze map wordt geopend wanneer de computer wordt gestart. Een opstartitem kan bijvoorbeeld een opstartscherm zijn, een geluidsbestand dat moet worden afgespeeld wanneer de computer voor de eerste maal opstart, een herinneringsagenda of een toepassingsprogramma. In normale omstandigheden wordt een alias van een bestand in deze map geplaatst, en niet het bestand zelf.

Systeemvak

Het systeemvak, dat met Windows 95 werd ingevoerd, bevindt zich in de taakbalk van Windows (doorgaans onderaan naast de klok) en bevat miniatuurpictogrammen die systeemfuncties zoals fax, printer, modem, volume en meer, gemakkelijk toegankelijk maken. Dubbelklik of klik met de rechtermuisknop op een pictogram om de details en de besturingselementen te bekijken en te openen.

TCP/IP

Transmission Control Protocol/Internet Protocol - Een reeks netwerkprotocollen, wijdverspreid gebruikt op het Internet, die communicatie bieden tussen onderling verbonden computernetwerken met verschillende hardware-architecturen en diverse besturingssystemen. TCP/IP bevat standaarden voor de manier waarop computers communiceren en regels voor het aansluiten van netwerken en het routeren van het verkeer.

Trojaans paard

Een destructief programma dat zich voordoeft als een goedaardige toepassing. In tegenstelling tot virussen, maken ze geen kopie van zichzelf, maar ze kunnen wel even vernietigend zijn. Een van de meest verraderlijke types van de Trojaanse paarden is een programma dat beweert dat het uw computer kan bevrijden van virussen, maar dat in werkelijkheid virussen op uw computer installeert.

De term komt uit een verhaal uit de Illias van Homerus, dat vertelt over de Grieken die hun vijanden, de Trojanen een reusachtig houten paard schonken, zogenaamd als een vredesgebaar. Maar nadat de Trojanen het paard binnen de stadsmuren hadden gesleept, kwamen de Griekse soldaten, die in de holle romp van het paard verborgen zaten te voorschijn en openden ze de poorten van de stad, zodat hun landgenoten Troje konden binnendringen en veroveren.

Update

Een nieuwe versie van een software- of hardwareproduct, dat werd ontwikkeld om een oudere versie van hetzelfde product te vervangen. Daarnaast zullen de installatieroutines voor updates vaak controleren of er reeds een oudere versie van het product op uw computer is geïnstalleerd. Is dat niet het geval, dan kunt u de update niet installeren.

BitDefender heeft zijn eigen updatemodule waarmee u handmatig kunt controleren op updates of die het product automatisch kan updaten.

Virus

Een programma of een deel van een code die op uw computer wordt geladen zonder uw medeweten en tegen uw wil wordt uitgevoerd. De meeste virussen kunnen zichzelf ook dupliceren. Alle computervirussen zijn door de mens gemaakt. Een eenvoudig virus dat zichzelf steeds opnieuw kan dupliceren is relatief eenvoudig te maken. Zelfs een dergelijke eenvoudig virus is gevaarlijk aangezien het snel al het beschikbare geheugen zal opgebruiken en het systeem

zal blokkeren; Een nog gevaarlijker type is een virus dat in staat is zichzelf te verzenden via netwerken en beveiligingssystemen te omzeilen.

Virusdefinitie

Het binaire patroon van een virus, dat wordt gebruikt door het antivirusprogramma om het virus te detecteren en uit te schakelen.

Worm

Een programma dat zich verspreidt via een netwerk en zichzelf ondertussen reproduceert. Dit type kan zich niet vasthechten aan andere programma's.