



bitdefender
internet security **2010**

Handleiding

BitDefender Internet Security 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 retrievalsysteem 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	xi
Voorwoord	xvii
1. Conventies die in dit boek worden gebruikt	xvii
1.1. Typografische conventies	xvii
1.2. Waarschuwing	xviii
2. Boekstructuur	xviii
3. Verzoek om commentaar	xix
 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 Internet Security 2010 registreren	9
3.1.2. Stap 2 - Een BitDefender-account creëren	10
3.2. Configuratiewizard	12
3.2.1. Stap 1 - Selecteer het gebruiksprofiel	12
3.2.2. Stap 2 - Beschrijf de computer	13
3.2.3. Stap 3 - De gebruikersinterface selecteren	14
3.2.4. Stap 4 - Ouderlijk Toezicht configureren	15
3.2.5. Stap 5 - BitDefender netwerk configureren	16
3.2.6. Stap 6 - De uit te voeren taken selecteren	18
3.2.7. Stap 7 - Voltooien	19
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	38
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	45
8.2. Beveiligingsinstellingen	46
8.3. Algemene instellingen	48
9. Geschiedenis en gebeurtenissen	50
10. Registratie en Mijn account	52
10.1. BitDefender Internet Security 2010 registreren	52
10.2. BitDefender activeren	53
10.3. Licentiesleutels aanschaffen	56
10.4. Uw licentie vernieuwen	56
11. Wizards	57
11.1. Antivirusscanwizard	57
11.1.1. Stap 1/3 - Scannen	57
11.1.2. Stap 2/3 - Acties selecteren	59
11.1.3. Stap 3/3 - Resultaten weergeven	60
11.2. Wizard Aangepaste scan	62
11.2.1. Stap 1/6 - Welkomstvenster	62
11.2.2. Stap 2/6 - Doel selecteren	63
11.2.3. Stap 3/6 - Acties selecteren	64
11.2.4. Stap 4/6 - Extra instellingen	67
11.2.5. Stap 5/6 - Scannen	67
11.2.6. Stap 6/6 - Resultaten weergeven	68
11.3. Wizard Kwetsbaarheidscontrole	69
11.3.1. Stap 1/6 - Te controleren kwetsbaarheden selecteren	70
11.3.2. Stap 2/6 - Op kwetsbaarheden controleren	71
11.3.3. Stap 3/6 - Windows bijwerken	72
11.3.4. Stap 4/6 - Applicaties updaten	73
11.3.5. Stap 5/6 - Zwakke wachtwoorden wijzigen	74
11.3.6. Stap 6/6 - Resultaten weergeven	75
11.4. Wizards Bestandskluis	76
11.4.1. Bestanden toevoegen aan kluis	76
11.4.2. Kluisbestanden wissen	82
11.4.3. Bestandskluis weergeven	87
11.4.4. Bestandskluis vergrendelen	91
Gemiddelde modus	95
12. Dashboard	96
13. Beveiliging	98

13.1. Statusgebied	98
13.1.1. Statustracering configureren	99
13.2. Snelle taken	101
13.2.1. Updaten BitDefender	101
13.2.2. Scannen met BitDefender	102
13.2.3. Bezig met zoeken van kwetsbaarheden	103
14. Ouderlijk	105
14.1. Statusgebied	105
14.2. Snelle taken	106
14.2.1. Updaten BitDefender	106
14.2.2. Scannen met BitDefender	107
15. Bestandskluis	109
15.1. Statusgebied	110
15.2. Snelle taken	111
16. Netwerk	112
16.1. Snelle taken	112
16.1.1. Het BitDefender netwerk koppelen	113
16.1.2. Bezig met toevoegen van computers aan het BitDefender netwerk ..	113
16.1.3. Het BitDefender netwerk beheren	115
16.1.4. Alle computers scannen	117
16.1.5. Alle computers updaten	118
16.1.6. Alle computers registreren	119
Expert-modus	120
17. Algemeen	121
17.1. Dashboard	121
17.1.1. Algemene status	122
17.1.2. Statistieken	124
17.1.3. Overzicht	125
17.2. Instellingen	126
17.2.1. Algemene instellingen	126
17.2.2. Virusrapportinstellingen	128
17.3. Systeem- informatie	128
18. Antivirus	130
18.1. Real-time beveiliging	130
18.1.1. Het beveiligingsniveau configureren	131
18.1.2. Het beveiligingsniveau aanpassen	132
18.1.3. Instellingen Actief virusbeheer configureren	137
18.1.4. Real time-beveiliging uitschakelen	139
18.1.5. Antiphishing bescherming configureren	140
18.2. Scannen op aanvraag	141
18.2.1. Scantaken	142
18.2.2. Het snelmenu gebruiken	144
18.2.3. Scantaken maken	145
18.2.4. Scantaken configureren	145
18.2.5. Bestanden en mappen scannen	157

18.2.6. Scanlogs weergeven	165
18.3. Uitgesloten objecten van het scannen	166
18.3.1. Paden uitsluiten van het scannen	168
18.3.2. Extensies uitsluiten van het scannen	171
18.4. Quarantainegebied	175
18.4.1. Bestanden in quarantaine beheren	176
18.4.2. Quarantaine-instellingen configureren	177
19. Antispam	179
19.1. Antispam-begrippen	179
19.1.1. Antispamfilters	179
19.1.2. Antispamgebruik	181
19.1.3. Antispam-updates	182
19.2. Status	183
19.2.1. Het beveiligingsniveau instellen	183
19.2.2. De Vriendenlijst configureren	184
19.2.3. Spammerslijst configureren	186
19.3. Instellingen	188
19.3.1. Antispaminstellingen	189
19.3.2. Standaard antispamfilters	190
19.3.3. Geavanceerde antispamfilters	190
20. Ouderlijk Toezicht	191
20.1. Ouderlijk toezicht configureren voor een gebruiker	192
20.1.1. Instellingen Ouderlijk Toezicht Beveiligen	194
20.1.2. De leeftijdscategorie instellen	195
20.2. De activiteit van de kinderen bewaken	198
20.2.1. Bezochte websites controleren	198
20.2.2. E-mailmeldingen configureren	198
20.3. Webbeheer	200
20.3.1. Regels voor webbeheer maken	200
20.3.2. Regels voor webbeheer beheren	201
20.4. Webtijd- beperking	202
20.5. Toepassings- beheer	203
20.5.1. Regels voor Toepassingsbeheer maken	204
20.5.2. Regels voor toepassingsbeheer beheren	205
20.6. Beheer trefwoorden	206
20.6.1. Regels voor het trefwoordenbeheer maken	207
20.6.2. Regels beheren voor trefwoordenbeheer	208
20.7. Instant Messaging (IM) beheer	208
20.7.1. Regels voor het beheer van instant messaging (IM) maken	209
20.7.2. Regels voor het beheer van instant messaging (IM) beheren	209
21. Privacybeheer	211
21.1. Privacybeheer Statistieken	211
21.1.1. Het beveiligingsniveau configureren	212
21.2. Identiteitscontrole	212
21.2.1. Privacyregels maken	214
21.2.2. Uitsluitingen definiëren	218
21.2.3. Regels beheren	219
21.2.4. Regels die door andere beheerders zijn gedefinieerd	219

21.3. Registerbeheer	220
21.4. Cookiebeheer	221
21.4.1. Configuratievenster	223
21.5. Scriptbeheer	225
21.5.1. Configuratievenster	226
22. Firewall	228
22.1. Instellingen	228
22.1.1. De standaard actie instellen	229
22.1.2. Geavanceerde firewall-instellingen configureren	230
22.2. Netwerk	232
22.2.1. Het vertrouwdeheidsniveau veranderen	234
22.2.2. De stealth-modus configureren	234
22.2.3. Algemene instellingen configureren	235
22.2.4. Netwerkkzones	235
22.3. Regels	236
22.3.1. Regels automatisch toevoegen	238
22.3.2. Regels verwijderen en opnieuw instellen	239
22.3.3. Regels maken en wijzigen	239
22.3.4. Geavanceerd regelbeheer	243
22.4. Verbindingsbeheer	244
23. Kwetsbaarheid	247
23.1. Status	247
23.1.1. Zwakke punten verwijderen	248
23.2. Instellingen	248
24. Encryptie	250
24.1. Instant Messaging (IM) encryptie	250
24.1.1. Encryptie uitschakelen voor specifieke gebruikers	251
24.2. File Encryptie	252
24.2.1. Een kluis creëren	253
24.2.2. Een kluis openen	255
24.2.3. Een kluis vergrendelen	255
24.2.4. Wachtwoord van kluis veranderen	256
24.2.5. Bestanden toevoegen aan een kluis	257
24.2.6. Bestanden verwijderen uit een kluis	257
25. Spel- / Laptop-modus	259
25.1. Spelmodus	259
25.1.1. Automatische Spelmodus configureren	260
25.1.2. De spellenlijst beheren	261
25.1.3. Spelmodus instellingen configureren	262
25.1.4. Veranderen van de Spelmodus sneltoets	263
25.2. Laptop-modus	263
25.2.1. Laptop-modus instellingen configureren	264
26. Thuisnetwerk	266
26.1. Het BitDefender netwerk koppelen	266
26.2. bezig met toevoegen van computers aan het BitDefender netwerk	267
26.3. Het BitDefender netwerk beheren	269

27. Update	272
27.1. Automatische update	272
27.1.1. Een update aanvragen	274
27.1.2. Automatische update uitschakelen	274
27.2. Update- instellingen	274
27.2.1. Updatelocaties instellen	275
27.2.2. Automatische update configureren	276
27.2.3. Handmatige update configureren	276
27.2.4. Geavanceerde instellingen configureren	276
27.2.5. Proxy's beheren	277
28. Registratie	280
28.1. BitDefender Internet Security 2010 registreren	280
28.2. Een BitDefender-account creëren	281
Integratie in Windows en software van derden	285
29. Integratie in het contextmenu van Windows.	286
29.1. Scannen met BitDefender	286
29.2. BitDefender bestandskluis	287
29.2.1. Kluis creëren	288
29.2.2. Kluis openen	289
29.2.3. Kluis vergrendelen	290
29.2.4. Toevoegen aan Bestandssafe	291
29.2.5. Verwijderen uit Bestandssafe	291
29.2.6. Wachtwoord van kluis veranderen	292
30. Integratie in webbrowsers	293
31. Integratie in programma's voor expresberichten	296
32. Integratie in mailclients	298
32.1. Configuratiewizard voor Antispam	298
32.1.1. Stap 1/6 - Welkomstvenster	299
32.1.2. Stap 2/6 - De Vriendenlijst opstellen	300
32.1.3. Stap 3/6 - De Bayes-database verwijderen	301
32.1.4. Stap 4/6 - De Bayes-filter opleiden met rechtmatige e-mail	302
32.1.5. Stap 5/6 - De Bayes-filter opleiden met spam	303
32.1.6. Stap 6/6 - Overzicht	304
32.2. Antispamwerkbalk	304
Zo werkt het	313
33. Bestanden en mappen scannen	314
33.1. Het contextmenu van Windows gebruiken	314
33.2. Scantaken gebruiken	314
33.3. BitDefender Handmatig scannen gebruiken	317
33.4. De balk voor de scanactiviteit gebruiken	318
34. Een computerscan plannen	319

Problemen oplossen en hulp vragen	321
35. Problemen oplossen	322
35.1. Installatieproblemen	322
35.1.1. Validatiefouten installatie	322
35.1.2. Mislukte installatie	323
35.2. De BitDefender-services reageren niet	325
35.3. Het delen van een bestand en printer in een Wi-Fi-netwerk (draadloos) werkt niet	326
35.3.1. Oplossing "Vertrouwde computer"	327
35.3.2. Oplossing "Veilig netwerk"	328
35.4. De antisпамfilter werkt niet goed	330
35.4.1. Rechtmatige berichten worden gemarkeerd als [spam]	330
35.4.2. Er worden veel spamberichten niet gedetecteerd	333
35.4.3. De antisпамfilter detecteert geen spamberichten	336
35.5. Het verwijderen van BitDefender is mislukt	337
36. Supportcentrum	338
BitDefender reddingsschijf	341
37. Overzicht	342
37.1. Systeemvereisten	342
37.2. Bijgeleverde software	343
38. De BitDefender reddingsschijf gebruiken	346
38.1. BitDefender reddingsschijf starten	346
38.2. BitDefender reddingsschijf stoppen	347
38.3. Hoe kan ik een antivirusscan uitvoeren?	348
38.4. Hoe configureer ik de internetverbinding?	349
38.5. Hoe kan ik BitDefender updaten?	350
38.5.1. Hoe kan ik BitDefender updaten over een proxy?	351
38.6. Hoe kan ik mijn gegevens opslaan?	352
38.7. Hoe moet ik de consolemodus gebruiken?	354
Woordenlijst	355

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 INBEGRIJ 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 Internet Security 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 Internet Security 2010 en wordt u begeleid doorheen het installatieproces met uitleg over de configuraties. U zult leren hoe u BitDefender Internet Security 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. xvii)	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 alle BitDefender-modules te configureren en gebruiken om uw computer op een efficiënte manier te beveiligen tegen elk type bedreiging (malware, spam, hackers, ongepaste inhoud, enz.).

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 kan BitDefender Internet Security 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

Antispam bescherming is aanwezig voor alle POP3/SMTP e-mailclients. De BitDefender Antispam werkbalk is echter alleen geïntegreerd in:

- Microsoft Outlook 2000 / 2003 / 2007
- Microsoft Outlook Express
- Microsoft Windows Mail
- Thunderbird 2.0.0.17

2. Voorbereiden voor de installatie

Voordat u BitDefender Internet Security 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.
- Schakel alle firewall-programma's die mogelijk op uw computer worden uitgevoerd uit of verwijder ze. Als u twee firewallprogramma's tegelijk uitvoert, kan dit hun werking beïnvloeden en ernstige problemen met het systeem veroorzaken. Windows Firewall wordt standaard uitgeschakeld voordat de installatie wordt gestart.

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

BitDefender Internet Security 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

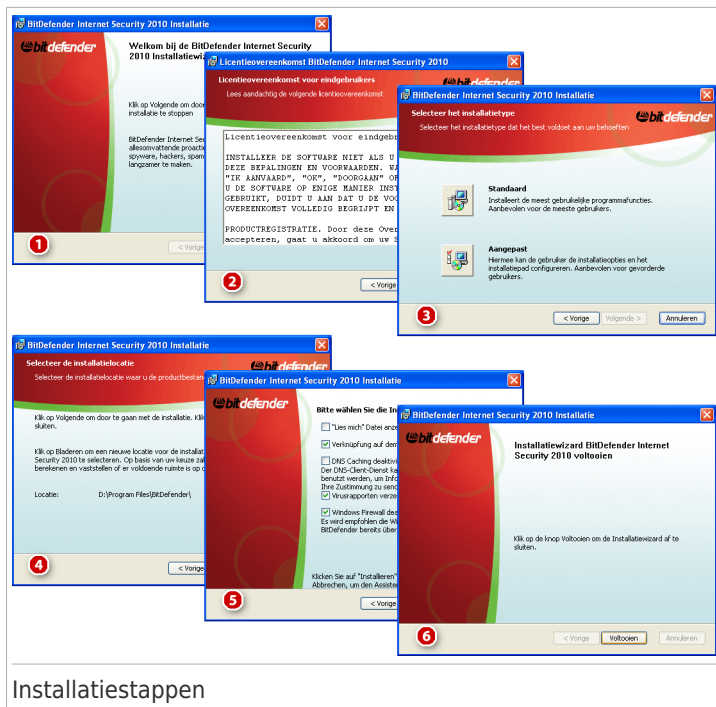
U kunt BitDefender installeren vanaf de BitDefender-installatie-cd, met het installatiebestand dat u van de BitDefender-website hebt gedownload naar uw computer, of van andere gemachtigde websites (bijvoorbeeld de website van een BitDefender-partner of een online winkel). U kunt het installatiebestand 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\InternetSecurity\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.



Installatiestappen

Volg deze stappen om BitDefender Internet Security 2010 te installeren:

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

BitDefender Internet Security 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 Internet Security 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 Internet Security 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 Firewall uitschakelen** - hiermee schakelt u de Windows Firewall uit.



Belangrijk

Wij adviseren aan Windows Firewall uit te schakelen omdat BitDefender Internet Security 2010 al een geavanceerde firewall bevat. De werking van twee firewalls op dezelfde computer kan problemen veroorzaken.

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

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

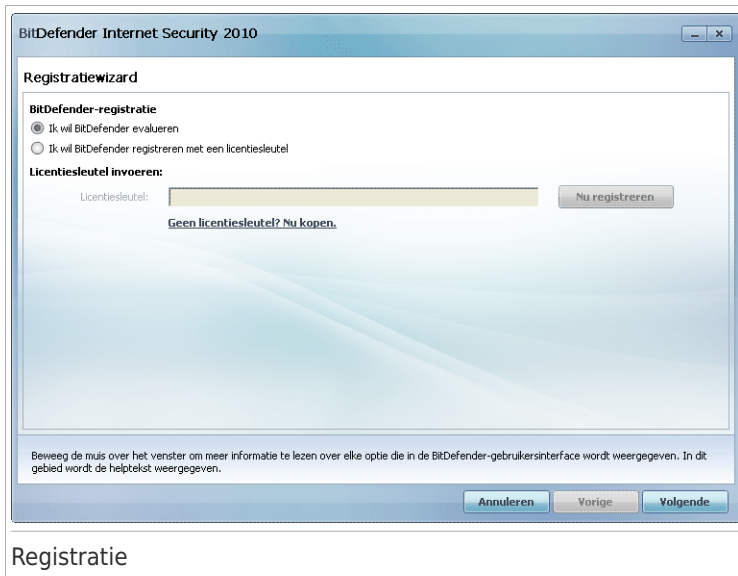
U MOET een BitDefender-account maken om BitDefender-updates te ontvangen. De BitDefender-account biedt u ook toegang tot de gratis technische ondersteuning en speciale aanbiedingen en promoties. Als u uw licentiesleutel kwijt bent, kunt u inloggen op uw account op <http://myaccount.bitdefender.com> om 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 Internet Security 2010 registreren



The screenshot shows the 'Registratiewizard' (Registration Wizard) window for BitDefender Internet Security 2010. The window has a title bar with the text 'BitDefender Internet Security 2010' and standard window controls. The main content area is titled 'Registratiewizard' and contains the following elements:

- A section titled 'BitDefender-registratie' with two radio buttons:
 - ☒ Ik wil BitDefender evalueren (I want to evaluate BitDefender)
 - ☐ Ik wil BitDefender registreren met een licentiesleutel (I want to register BitDefender with a license key)
- A section titled 'Licentiesleutel invoeren:' (Enter license key:) with a text input field labeled 'Licentiesleutel:' and a 'Nu registreren' (Register now) button.
- A link below the input field: [Geen licentiesleutel? Nu kopen.](#) (No license key? Buy now.)
- A footer area with a small text block: '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 helpetekst weergegeven.' (Move the mouse over the window to read more information about each option displayed in the BitDefender user interface. In this area, the help text is displayed.) and three buttons: 'Annuleren' (Cancel), 'Vorige' (Previous), and 'Volgende' (Next).

Below the window, the word 'Registratie' (Registration) is written.

BitDefender Internet Security 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 Internet Security 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

Account creëren

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

- “Ik heb geen BitDefender-account” (p. 10)
- “Ik heb al een BitDefender-account” (p. 11)



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 geïnfecteerd.

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 adviseren echter dit toch te doen om tijd te besparen en er zeker van te zijn dat uw systeem veilig is, zelfs voordat BitDefender Internet Security 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.
Ouder	Klik hier als deze pc wordt gebruikt door kinderen en u hun toegang tot internet wilt beheren via de module Ouderlijk toezicht.
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

BitDefender Internet Security 2010

BITDefender Configuratiewizard

Kies welke van deze opties van toepassing is tot deze pc

In deze stap kunt u het Thuisnetwerkbeheer en de Laptopmodus van BitDefender configureren. Schakel de selectievakjes in die overeenkomen met de beschrijving van deze pc.

☐ Deze computer zit in een thuisnetwerk.

Selecteer deze optie als u via de gebruikersinterface gemakkelijk toegang wilt hebben tot de module Thuisnetwerkbeheer. Met deze module kunt u andere BitDefender-producten in uw thuisnetwerk op afstand beheren.

☐ Deze computer is een laptop

Selecteer deze optie als u wilt dat de Laptopmodus standaard wordt ingeschakeld. Deze modus zorgt voor een langere gebruiksduur van de batterij van uw laptop door taken die extra stroom vereisen, niet uit te voeren.

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 helpetekst weergegeven.

Annuleren Vorige Volgende

Computerbeschrijving

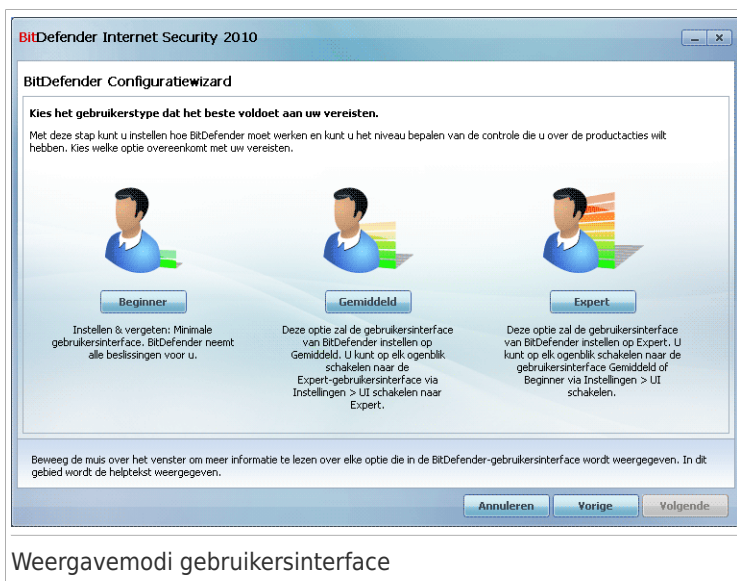
Selecteer de opties die van toepassing zijn op uw computer:

- **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



Weergavemodi gebruikersinterface

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	<p>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.</p> <p>U hoeft alleen de bestaande problemen op te lossen wanneer dit door BitDefender wordt aangegeven. Een gebruikersvriendelijke wizard helpt u stapsgewijs bij het</p>

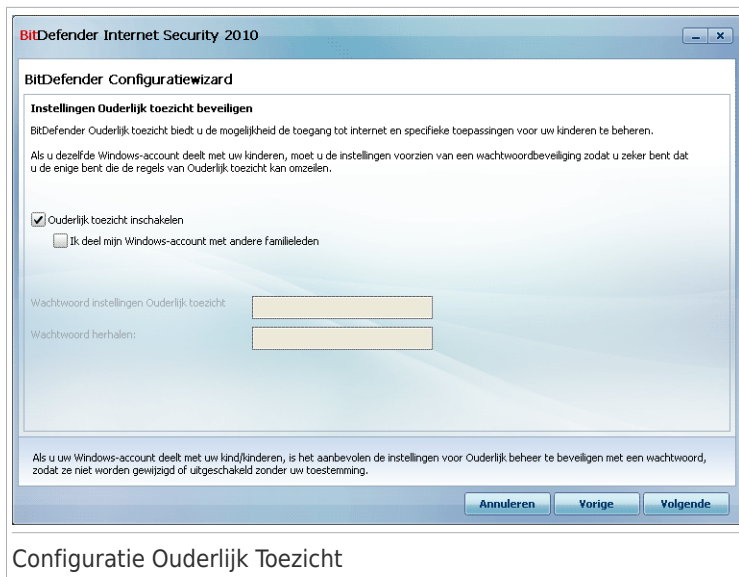
Modus	Beschrijving
	oplossen van problemen. Daarnaast kunt u algemene taken uitvoeren, zoals het bijwerken van de BitDefender-virushandtekening en productbestanden of het scannen van de computer.
Gemiddelde modus	<p>Deze modus is gericht op gebruikers met gemiddelde computervaardigheden en biedt meer mogelijkheden dan in de Beginnersmodus.</p> <p>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.</p>
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 - Ouderlijk Toezicht configureren



Opmerking

Deze stap verschijnt alleen als u de optie **Aangepast** hebt geselecteerd in stap 1.



Met bitDefender Ouderlijk Toezicht kan u de toegang tot het Internet en tot specifieke toepassingen beheren voor elke gebruiker die een gebruikersaccount op het systeem heeft.

Volg deze stappen als u Ouderlijk Toezicht wilt gebruiken:

1. Select **Ouderlijk toezicht inschakelen**.
2. Als u uw Windows-gebruikersaccount met uw kinderen deelt, schakelt u het overeenkomende selectievakje in en voert u een wachtwoord in de overeenkomende velden in om de instellingen voor Ouderlijk toezicht te beveiligen. Iedereen die probeert de instellingen voor Ouderlijk toezicht te wijzigen, moet u eerst het wachtwoord dat u hebt geconfigureerd, opgeven.

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

3.2.5. Stap 5 - BitDefender netwerk configureren



Opmerking

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



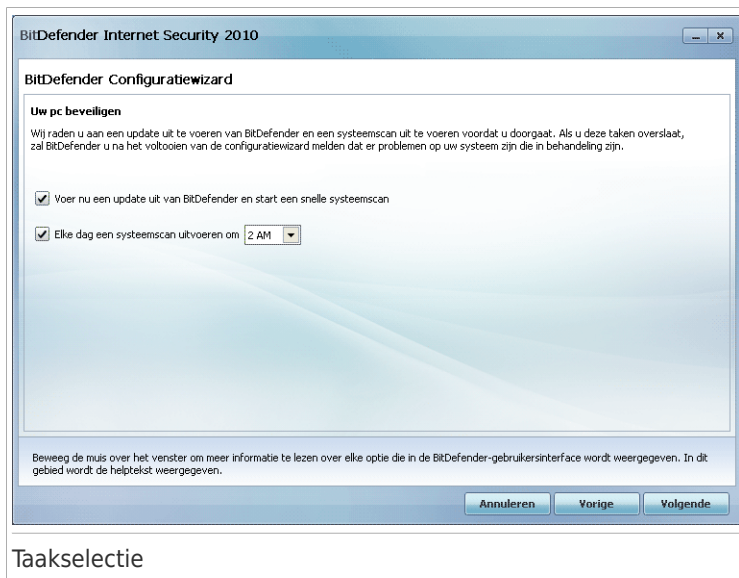
Met BitDefender kan u een virtueel netwerk van de computers in uw huishouden creëren en de op dit netwerk geïnstalleerde BitDefender producten beheren.

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.

3.2.6. Stap 6 – 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:

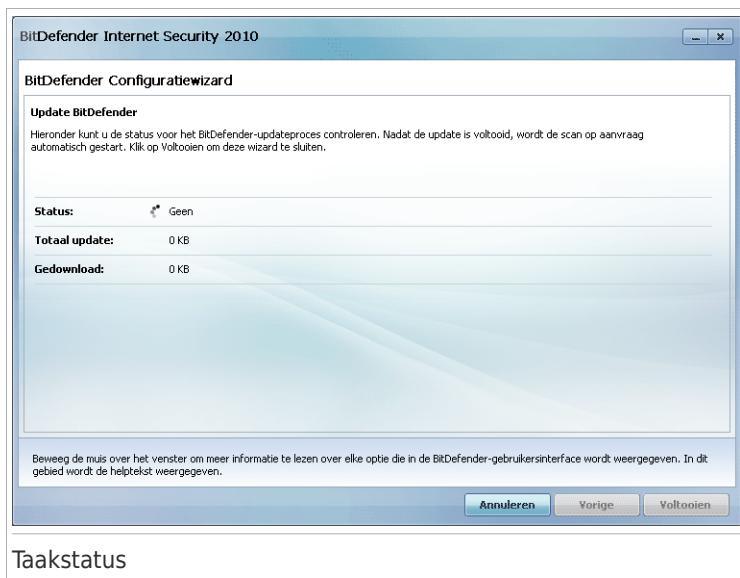
1. Open BitDefender en schakel de gebruikersinterface naar de Expert-modus.
2. Klik in het menu aan de linkerkant op **Antivirus**.

3. Klik op het tabblad **Virusscan**.
4. Klik met de rechtermuisknop op de taak **Systeemsan** 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 **Voltoeien** om de wizard te voltooien.

3.2.7. Stap 7 - Voltoeien



Wacht tot BitDefender de update heeft uitgevoerd van zijn malwarehandtekeningen en scanengines. Zodra de update is voltooid, wordt een snelle systeemsan 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 **Voltoeien** 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 systeemsan uitvoeren.

4. Upgrade

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

Er zijn twee manieren om de upgrade uit te voeren:

- BitDefender Internet Security 2010 rechtstreeks over de oudere versie installeren.
Als u rechtstreeks over de versie 2009 installeert, worden de vrienden- en spammerslijsten en 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 Internet Security 2010 wilt repareren of verwijderen, volgt u het volgende 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 Internet Security 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

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

Klik op **Verwijderen** om het verwijderen van BitDefender Internet Security 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 Internet Security 2010 is toegankelijk via het volgende pad vanaf het menu Start van Windows: **Start** → **Programma's** → **BitDefender 2010** → **BitDefender Internet Security 2010**. Dit kan ook sneller door in het systeemvak te dubbelklikken op het BitDefender-pictogram .

6.2. Weergavemodi gebruikersinterface

BitDefender Internet Security 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	<p>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.</p> <p>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</p>

Modus	Beschrijving
	algemene taken uitvoeren, zoals het bijwerken van de BitDefender-virushandtekening en productbestanden of het scannen van de computer.
Gemiddelde modus	<p>Deze modus is gericht op gebruikers met gemiddelde computervaardigheden en biedt meer mogelijkheden dan in de Beginnersmodus.</p> <p>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.</p>
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 gebruikersprofiel.
 - ▶ 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. 57) 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. 69) voor meer gedetailleerde informatie.

- ▶ Wanneer het profiel **Ouder** is geselecteerd, kunt u via de knop **Ouderlijk toezicht** de instellingen voor Ouderlijk toezicht configureren. Ouderlijk toezicht beperkt de computer- en online-activiteiten van uw kinderen op basis van de regels die u hebt gedefinieerd. Beperkingen kunnen het blokkeren van ongeschikte websites inhouden, maar ook het beperken van het spelen van spelletjes en van internettoegang volgens een specifiek schema. Raadpleeg "*Ouderlijk Toezicht*" (p. 191) voor more informatie over de manier waarop u Ouderlijk toezicht wilt configureren.
- ▶ 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.
 - ▶ **Bestand toevoegen aan kluis** start de wizard waarmee u belangrijke bestanden/documenten privé kan opslaan door ze te crypteren op een speciale beschermde schijf.
 - ▶ **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.
- **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 Internet Security 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. 95) 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
Security	Toont de status van de veiligheidsmodules (antivirus, antiphishing, firewall, antispam, IM encryptie, privacy, kwetsbaarheidscontrole en update modules), tezamen met de links naar de antivirus-, update- en kwetsbaarheidscontroletaken.
Parental	Toont de status van de module Ouderlijk toezicht. Met Ouderlijk toezicht kunt u de toegang van uw kinderen tot het internet en specifieke toepassingen beperken.
Bestandssafe	Toont de status van de bestandskluis tezamen met links naar de bestandskluis.
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 Internet Security 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.

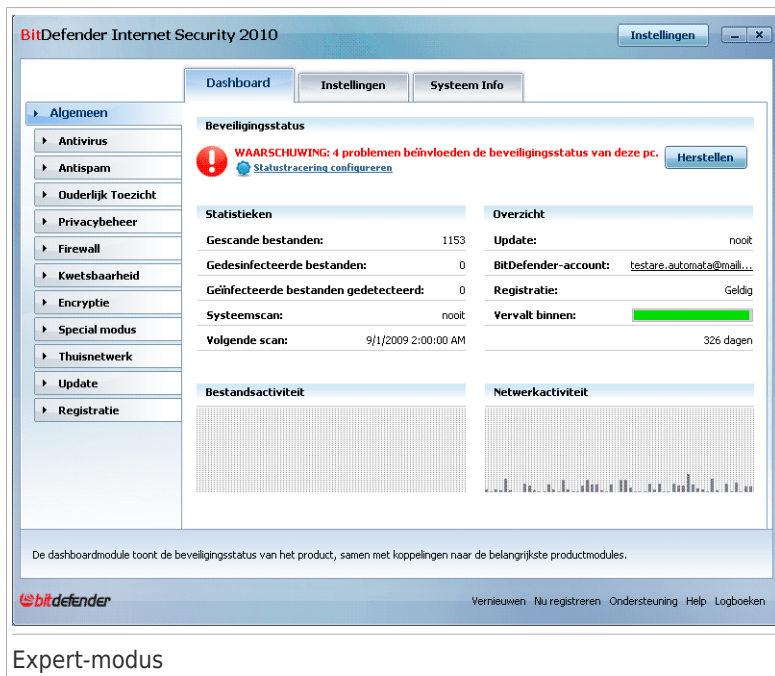
6.2.3. Expert-modus

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. 120) 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
Antispam	Hiermee kunt u uw Postvak IN spamvrij houden en de antispaminstellingen in detail configureren.
Ouderlijk toezicht	Hiermee kan u uw kinderen beschermen tegen ongepaste inhoud door uw eigen computertoegangsregels te gebruiken.
Privacybeheer	Hiermee voorkomt u diefstal van data van uw computer en beschermt u uw privacy als u online bent.
Firewall	Hiermee beschermt u uw computer tegen onbevoegde binnenkomende en uitgaande verbindingspogingen. Deze functie is te vergelijken met een schildwacht bij de poort. Hij houdt een waakzaam oog op uw Internetverbinding en volgt op wie hij toegang kan verlenen tot het Internet en wie hij moet blokkeren.
Kwetsbaarheid	Hiermee kan u de cruciale software op uw PC up-to-date houden.
Encryptie	Hiermee kan u Yahoo en Windows Live (MSN) Messenger verbindingen crypteren en kan u ook lokaal uw belangrijke bestanden, mappen of partities crypteren.
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 Internet Security 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.

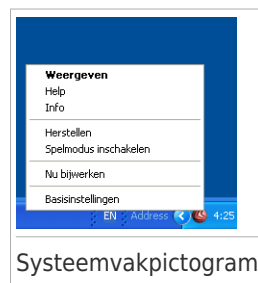
Koppeling	Beschrijving
Kopen/Verlengen	Opent een webpagina waar u een licentiesleutel voor uw BitDefender Internet Security 2010-product kunt aanschaffen.

Koppeling	Beschrijving
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 Internet Security 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.

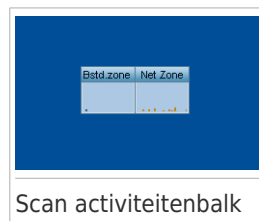
 **Letter G:** Het product werkt op **Spelmodus**.

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

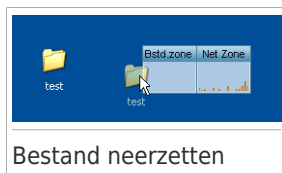
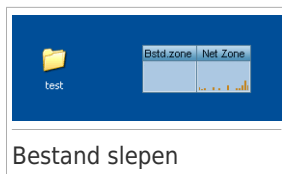


Opmerking

De scanactiviteitenbalk geeft aan wanneer de real time-beveiliging of de firewall is uitgeschakeld, door een rood kruis over de overeenkomende zone (**Bestand** of **Netzone**) weer te geven.

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.



De Antivirusscanwizard wordt weergegeven en begeleidt u doorheen het scanproces. Raadpleeg "*Antivirusscanwizard*" (p. 57) 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:

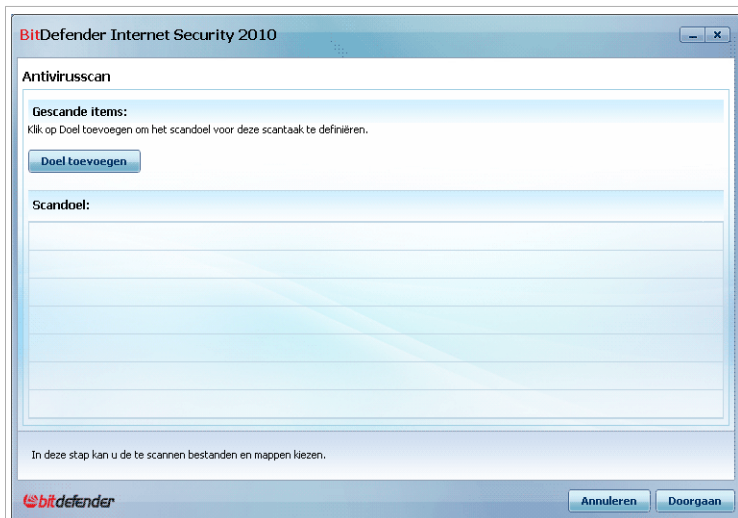
1. BitDefender openen.
2. Klik in de rechterbovenhoek van het venster op **Instellingen**.
3. Schakel in de categorie Algemene instellingen het selectievakje naast **Balk Scanactiviteit** in.
4. Klik op **OK** om de wijzigingen op te slaan en toe te passen.

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. 57) 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 Internet Security 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 linkerzijde 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. 57) 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. 145).
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**.



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 traceringsysteem 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. 69) 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 traceringssysteem 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 traceringssysteem worden geconfigureerd vanaf afzonderlijke locaties. Volg deze stappen:
 1. Ga naar het tabblad **Beveiliging, Ouderlijk toezicht** of **Bestandskluis**.
 2. Klik op **Statustracing configureren**.
 3. Schakel de selectievakjes in naast de items die u wilt bewaken.


Raadpleeg het gedeelte *"Gemiddelde modus"* (p. 95) 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 **Statustracing configureren**.
 3. Schakel de selectievakjes in naast de items die u wilt bewaken.

Raadpleeg hoofdstuk "*Dashboard*" (p. 121) voor meer gedetailleerde informatie.

8. De basisinstellingen configureren

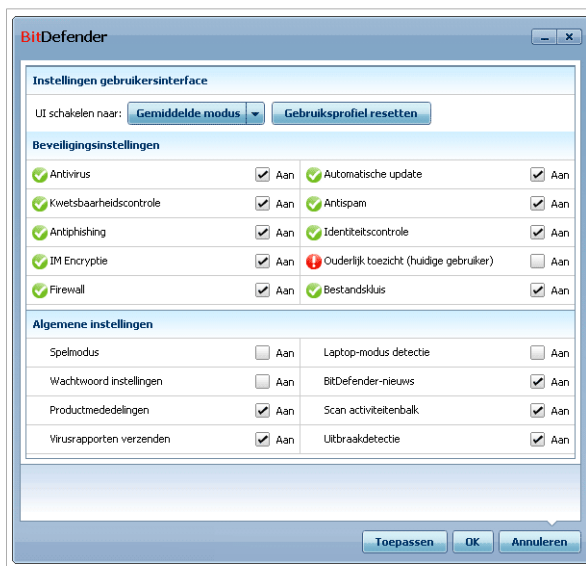
U kunt de hoofdstellingen van het product (inclusief het wijzigen van de weergavemodus voor de gebruikersinterface) configureren vanaf het venster met de basisinstellingen. Voer een van de volgende bewerkingen uit om het venster te openen:

- 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. 120) van deze handleiding voor gedetailleerde informatie.



BitDefender

Instellingen gebruikersinterface

UI schakelen naar: **Gemiddelde modus** **Gebruiksprofiel resetten**

Beveiligingsinstellingen

<input checked="" type="checkbox"/> Antivirus	<input checked="" type="checkbox"/> Aan	<input checked="" type="checkbox"/> Automatische update	<input checked="" type="checkbox"/> Aan
<input checked="" type="checkbox"/> Kwetsbaarheidscontrole	<input checked="" type="checkbox"/> Aan	<input checked="" type="checkbox"/> Antispam	<input checked="" type="checkbox"/> Aan
<input checked="" type="checkbox"/> Antiphishing	<input checked="" type="checkbox"/> Aan	<input checked="" type="checkbox"/> Identiteitscontrole	<input checked="" type="checkbox"/> Aan
<input checked="" type="checkbox"/> IM Encryptie	<input checked="" type="checkbox"/> Aan	<input checked="" type="checkbox"/> Ouderlijk toezicht (huidige gebruiker)	<input type="checkbox"/> Aan
<input checked="" type="checkbox"/> Firewall	<input checked="" type="checkbox"/> Aan	<input checked="" type="checkbox"/> Bestandskluus	<input checked="" type="checkbox"/> Aan

Algemene instellingen

Spelmodus	<input type="checkbox"/> Aan	Laptop-modus detectie	<input type="checkbox"/> Aan
Wachtwoord instellingen	<input type="checkbox"/> Aan	BitDefender-nieuws	<input checked="" type="checkbox"/> Aan
Productmededelingen	<input checked="" type="checkbox"/> Aan	Scan activiteitenbalk	<input checked="" type="checkbox"/> Aan
Virusrapporten verzenden	<input checked="" type="checkbox"/> Aan	Uitbraakdetectie	<input checked="" type="checkbox"/> Aan

Toepassen **OK** **Annuleren**

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	<p>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.</p> <p>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.</p>
Gemiddelde modus	<p>Deze modus is gericht op gebruikers met gemiddelde computervaardigheden en biedt meer mogelijkheden dan in de Beginnersmodus.</p> <p>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.</p>
Expert-modus	<p>Deze modus is geschikt voor meer technisch gerichte gebruikers en bieden u de mogelijkheid elke functie van BitDefender volledig te configureren. U kunt ook</p>

Modus	Beschrijving
	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, de firewall 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.

Instelling	Beschrijving
Antispam	Antispam filtert de e-mailberichten die u ontvangt en markeert ongewenste e-mail en junkmail als SPAM.
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 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.
Ouderlijk toezicht	Ouderlijk toezicht beperkt de computer- en online-activiteiten van uw kinderen op basis van de regels die u hebt gedefinieerd. Beperkingen kunnen het blokkeren van ongeschikte websites inhouden, maar ook het beperken van het spelen van spelletjes en van internettoegang volgens een specifiek schema.
Firewall	Firewall beschermt uw computer tegen hackers en kwaadwillende aanvallen van buitenaf.
File encryptie	Bestandscodering houdt uw documenten persoonlijk door ze te coderen in speciale stations met "kluizen". Als u Bestandscodering uitschakelt, worden alle bestandskluizen vergrendeld kan u de bestanden erin niet meer openen.

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 traceringsysteem worden geconfigureerd vanaf afzonderlijke locaties, gebaseerd op instellingscategorieën. Raadpleeg het gedeelte "**Gemiddelde modus**" (p. 95) 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 het selectievakje in naast de items die u niet wilt bewaken.

Raadpleeg hoofdstuk "**Dashboard**" (p. 121) 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.
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 " Scan activiteitenbalk " (p. 33) voor meer informatie.

Instelling	Beschrijving
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.

Geschiedenis _gebeurtenissen

- Antivirus
 - Antispam
 - Ouderlijk Toezicht
 - Privacybeheer
 - Firewall
 - Kwetsbaarheid
 - IM Encryptie
 - Bestandskluis
 - Special modus
 - Thuisnetwerk
 - Update
 - Registratie
 - Internetlogboek

Real-time beveiliging

Actienaam	Genomen actie	Datum

Taken op aanvraag

Actienaam	Taaknaam	Datum

Bewoog 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 helpelst weergegeven.

Alles wissen Vernieuwen OK

Gebeurtenissen

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

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

- **Kwetsbaarheid**
- **IM encryptie**
- **File 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 Internet Security 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 Internet Security 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.



Registratie

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

BitDefender Internet Security 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.

Account creëren

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

- “Ik heb geen BitDefender-account” (p. 55)
- “Ik heb al een BitDefender-account” (p. 55)



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. 120).

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.

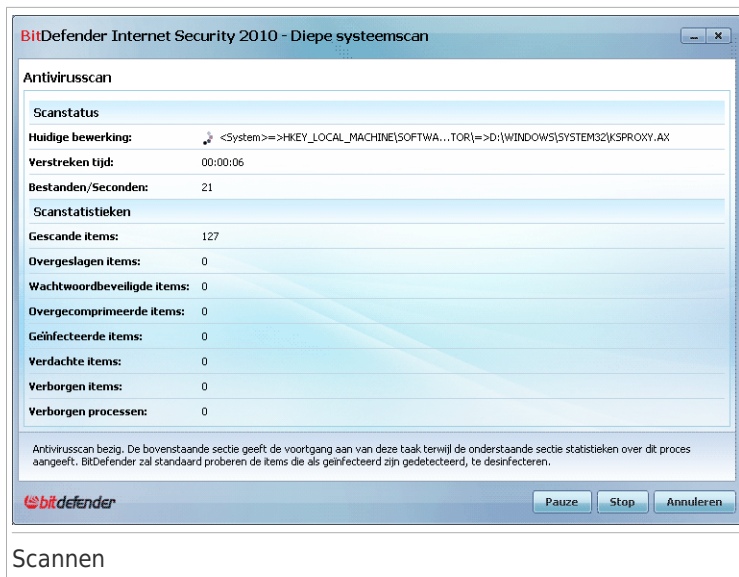


Opmerking

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.



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.

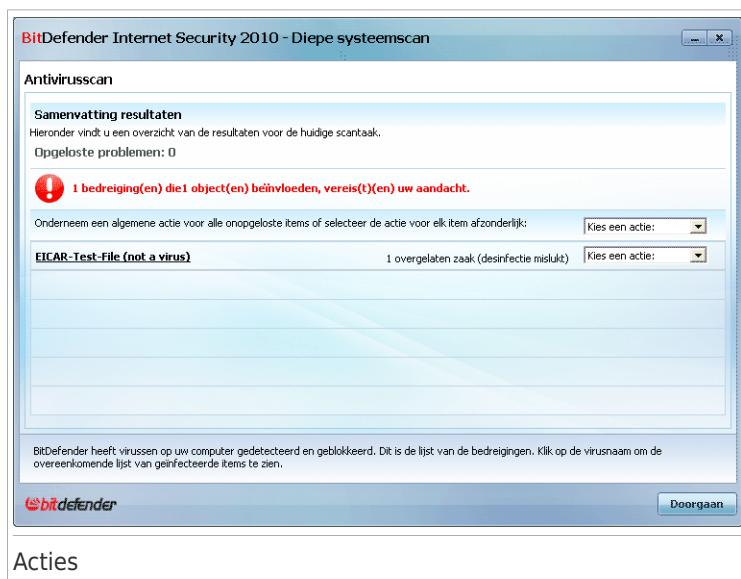
BitDefender zal ze niet kunnen scannen, maar er wordt wel een gegeven bewaard in het scanlogboek.

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.



Acties

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

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

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

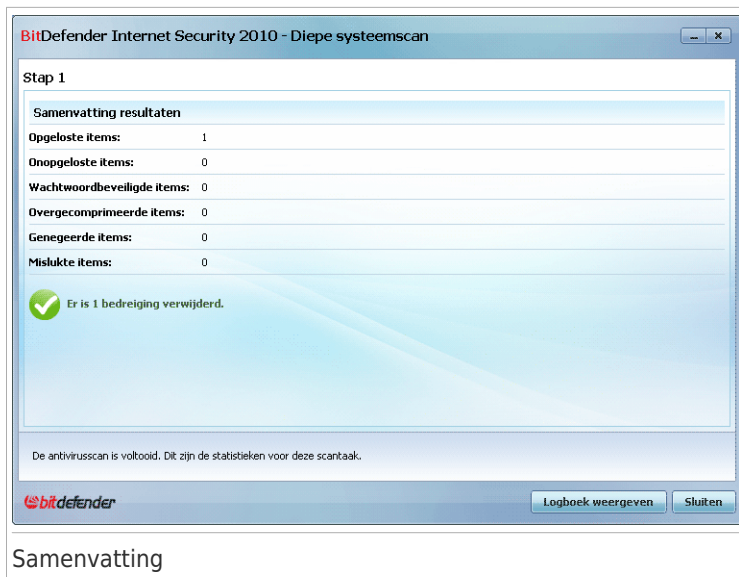
Een of meerdere van de volgende opties kunnen in het menu verschijnen.

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	<p>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.</p> <p>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.</p>

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. Ga in de Gemiddelde modus naar het tabblad **Beveiliging**.
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 Internet Security 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;ivd;)

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 Internet Security 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** **Toegevoegd** **Aangepast**

Standaard

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

Deze stap biedt toegang tot de scanopties.

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.

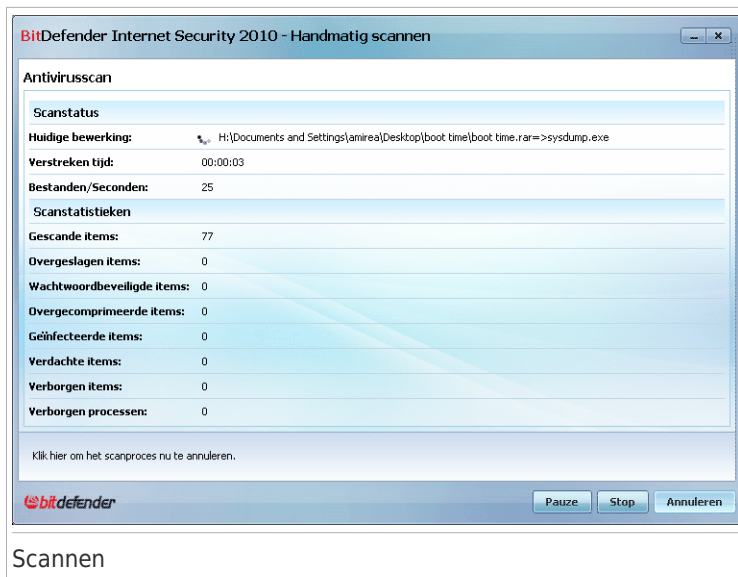
De taak zal aan de lijst van Vlugge Taken reeds verkrijgbaar in het Veiligheidslabel worden toegevoegd en zal ook verschijnen in **Deskundige Modus > Antivirus > Virus onderzoekende Blik**.

- 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:

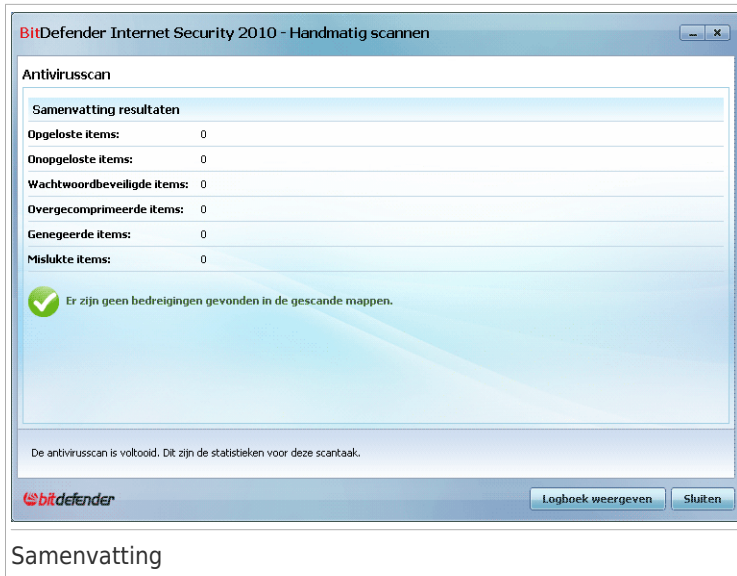


Opmerking

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 **systeemvak** 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

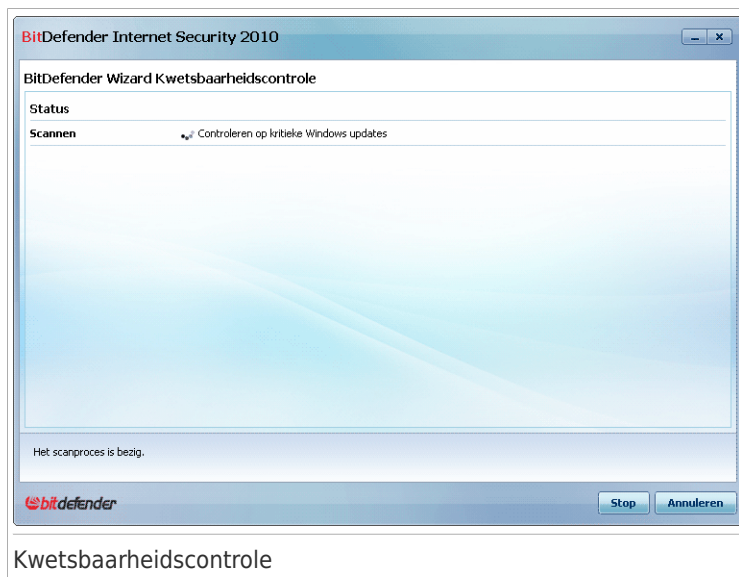
Deze wizard controleert het systeem op kwetsbaarheden en helpt u ze op te lossen.

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**.

11.4. Wizards Bestandskluis

Met de wizards Bestandskluis kunt u BitDefender-bestandskluizen maken en beheren. Een bestandskluis is een gecodeerde opslagruimte op uw computer waar u belangrijke bestanden, documenten en zelfs volledige mappen veilig kunt opslaan.

Deze wizards verschijnen niet wanneer u problemen oplost omdat de bestandskluizen een optionele methode zijn voor het beschermen van uw gegevens. Ze kunnen alleen op de volgende manier worden gestart vanaf de interface van de Gemiddelde modus van BitDefender via het tabblad **Bestandsopslag**:

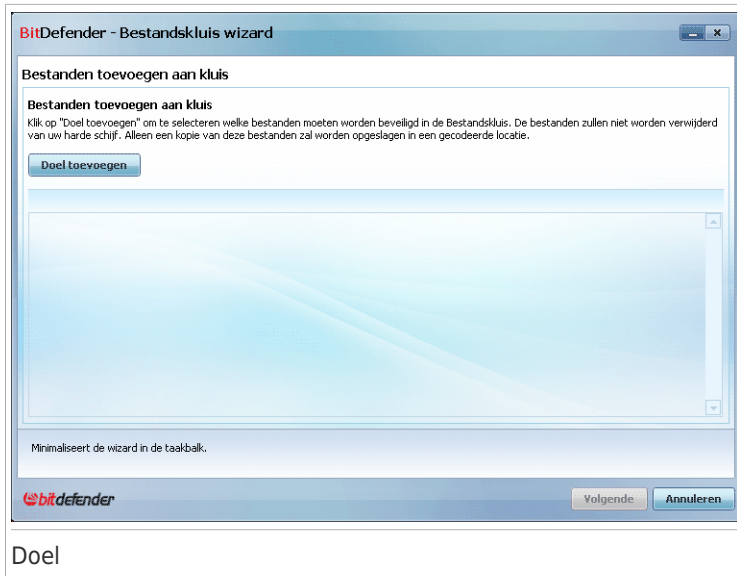
- **Bestand toevoegen aan kluis** - start de wizard waarmee u belangrijke bestanden/documenten privé kan opslaan door ze te crypteren op een speciale beschermde schijf.
- **Kluisbestanden verwijderen** - start de wizard waarmee u data van de bestandskluis kan wissen.
- **Bestandskluis weergeven** - start de wizard waarmee u de inhoud van uw bestandskluizen kunt weergeven.
- **Bestandskluis vergrendelen** - start de wizard waarmee u een open bestandskluis kunt vergrendelen om zijn inhoud te beschermen.

11.4.1. Bestanden toevoegen aan kluis

De wizard helpt u bij het maken van een bestandskluis en bestanden aan de kluis toe te voegen om ze veilig op te slaan op uw computer.

Stap 1/6 - Doel selecteren

Hier kan u de bestanden of mappen die moeten worden toegevoegd aan de kluis, opgeven.



Klik op **Doel toevoegen**, selecteer het bestand of de map die u wilt toevoegen en klik op **OK**. Het pad naar de geselecteerde locatie zal verschijnen in de kolom **Pad**. Als u de locatie toch niet wilt gebruiken, klik dan op de knop **Verwijderen** ernaast.



Opmerking

U kunt een of meerdere locaties selecteren.

Klik op **Volgende**.

Stap 2/6 - Kluis selecteren

Hier kan u een nieuwe kluis creëren of een bestaande kluis kiezen.



Selecteer kluis

Als u **Bladeren naar een bestandskluis** selecteert, moet u klikken op **Bladeren** en de bestandskluis selecteren. U gaat dan ofwel naar stap 5 als de geselecteerde kluis open is, ofwel naar stap 4 als deze vergrendeld is.

Als u klikt op **Een bestaande bestandskluis selecteren**, dan moet u klikken op de naam van de gewenste kluis. U gaat dan ofwel naar stap 5 als de geselecteerde kluis open is, ofwel naar stap 4 als deze vergrendeld is.

Selecteer **Nieuwe bestandskluis creëren** als geen van de bestaande kluizen voor u geschikt is. U gaat dan naar stap 3.

Klik op **Volgende**.

Stap 3/6 - Kluis creëren

Hier kan u informatie over de nieuwe kluis opgeven.

Bestanden toevoegen aan kluis

Creëer bestandskluis

Geef het nieuwe wachtwoord voor de Bestandskluis op en configureer de opslaglocatie en grootte van de Bestandskluis.

Voer het pad in voor de

Bestandskluis: Schijfletter:

A: Het wachtwoord moet minstens 8 tekens lang zijn.

Wachtwoord: Het wachtwoord moet minstens 8 tekens lang zijn.

Wachtwoord herhalen:

Voer de grootte van de Typ alleen cijfers.

Bestandskluis in (*MB):

Bepaalt de stationsletter (label) die deze Bestandskluis zal identificeren.

Kluis creëren

Volg deze stappen om de informatie over de kluis te voltooien:

1. Klik op **Bladeren** en kies een locatie voor het bvd-bestand.



Opmerking

Het kluisbestand is een gecrypteerd bestand op uw computer met de extensie bvd.

2. Selecteer de schijfletter voor de nieuwe bestandskluis in het overeenkomende afromenu.



Opmerking

Wanneer u het bvd-bestand opent, verschijnt een nieuwe logische partitie (een nieuwe schijf).

3. Voer een wachtwoord voor de bestandskluis in het overeenkomende veld in.



Opmerking

Het wachtwoord moet minstens 8 tekens bevatten.

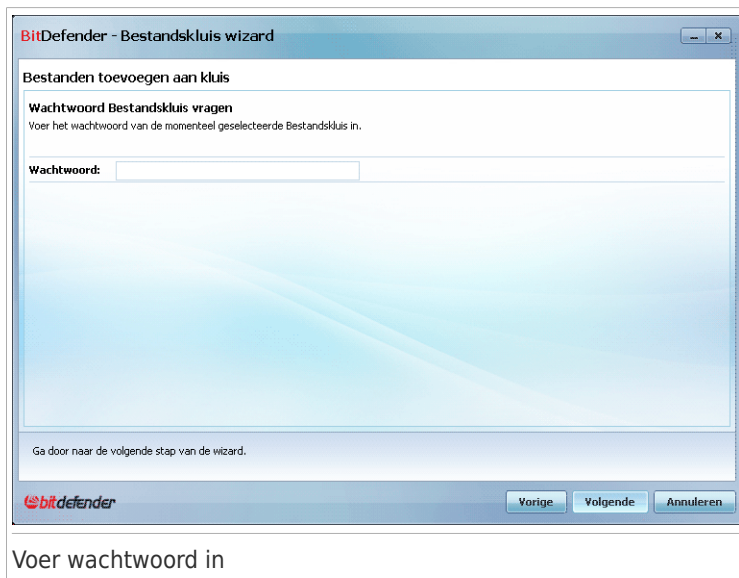
4. Herhaal het wachtwoord.
5. Stel de grootte van de bestandskluis (in MB) in door een getal te typen in het overeenkomende veld.

Klik op **Volgende**.

U gaat naar stap 5.

Stap 4/6 - Wachtwoord

Hier wordt u gevraagd het wachtwoord van de geselecteerde kluis in te voeren.



The screenshot shows a window titled "BitDefender - Bestandskluis wizard". Inside, the main heading is "Bestanden toevoegen aan kluis". Below this, a section titled "Wachtwoord Bestandskluis vragen" contains the instruction "Voer het wachtwoord van de momenteel geselecteerde Bestandskluis in." and a text input field labeled "Wachtwoord:". At the bottom of the window, there is a status bar with the BitDefender logo on the left and three buttons: "Vorige", "Volgende", and "Annuleren".

Bestanden toevoegen aan kluis

Wachtwoord Bestandskluis vragen
Voer het wachtwoord van de momenteel geselecteerde Bestandskluis in.

Wachtwoord:

Ga door naar de volgende stap van de wizard.

bitdefender

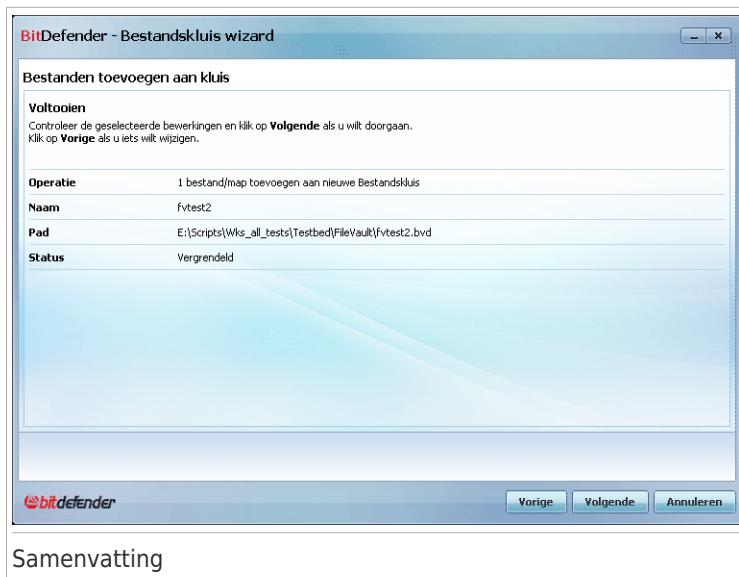
Vorige Volgende Annuleren

Voer wachtwoord in

Typ het wachtwoord in het overeenkomende veld en klik op **Volgende**.

Stap 5/6 – Overzicht

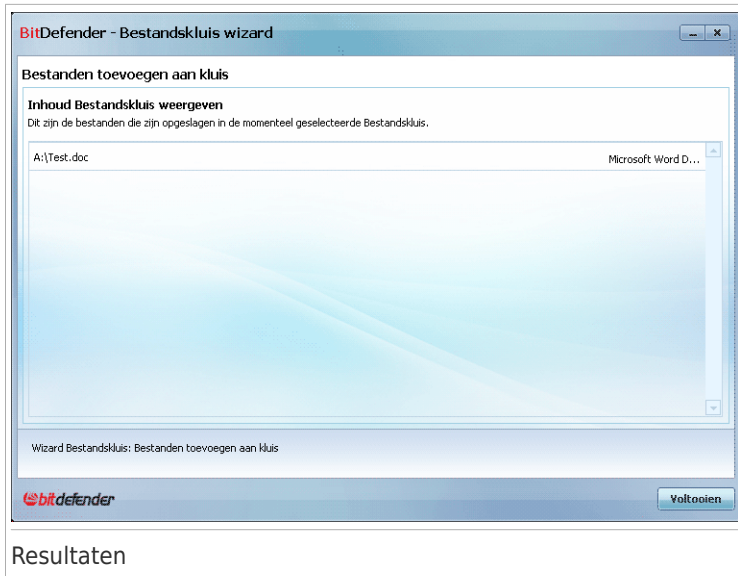
Hier kan u de gekozen acties controleren.



Klik op **Volgende**.

Stap 6/6 - Resultaten

Hier kan u de inhoud van de kluis zien.



Klik op **Voltooien**.

11.4.2. Kluisbestanden wissen

Deze wizard helpt u bij het verwijderen van bestanden uit een specifieke bestandskluis.

Stap 1/5 - Kluis selecteren

Hier kan u de kluis selecteren van waaruit u bestanden wilt verwijderen.



Selecteer kluis

Als u **Bladeren naar een bestandskluis** selecteert, moet u klikken op **Bladeren** en de bestandskluis selecteren. U gaat dan ofwel naar stap 3 als de geselecteerde kluis open is, ofwel naar stap 2 als deze vergrendeld is.

Als u klikt op **Een bestaande bestandskluis selecteren**, dan moet u klikken op de naam van de gewenste kluis. U gaat dan ofwel naar stap 3 als de geselecteerde kluis open is, ofwel naar stap 2 als deze vergrendeld is.

Klik op **Volgende**.

Stap 2/5 - Wachtwoord

Hier wordt u gevraagd het wachtwoord van de geselecteerde kluis in te voeren.

BitDefender - Bestandskluis wizard

Kluisbest.wissen

Wachtwoord Bestandskluis vragen
Voer het wachtwoord van de momenteel geselecteerde Bestandskluis in.

Wachtwoord:

Ga door naar de volgende stap van de wizard.

bitdefender

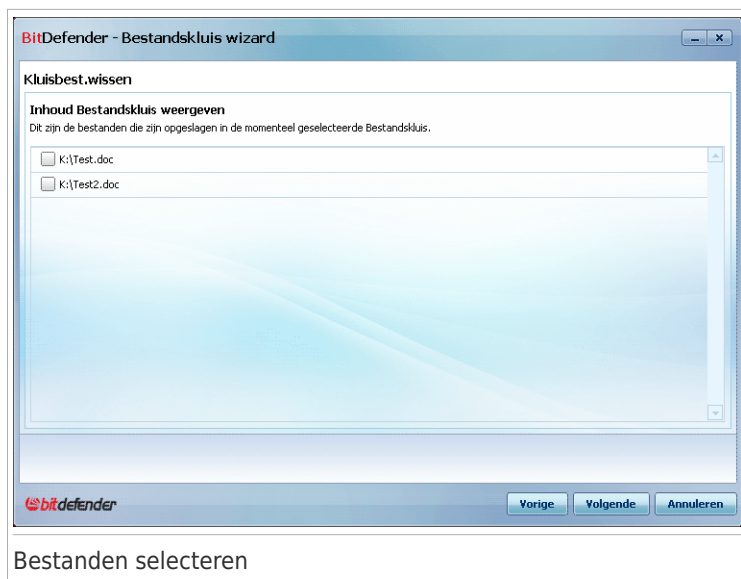
Vorige Volgende Annuleren

Voer wachtwoord in

Typ het wachtwoord in het overeenkomende veld en klik op **Volgende**.

Stap 3/5 - Bestanden selecteren

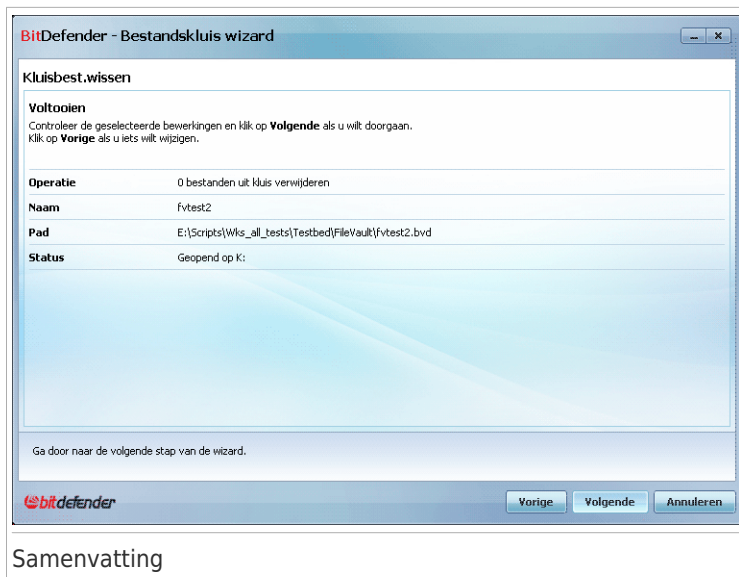
Hier krijgt u de lijst van de bestanden van de hiervoor geselecteerde kluis.



Klik op de te verwijderen bestanden en klik op **Volgende**.

Stap 4/5 - Overzicht

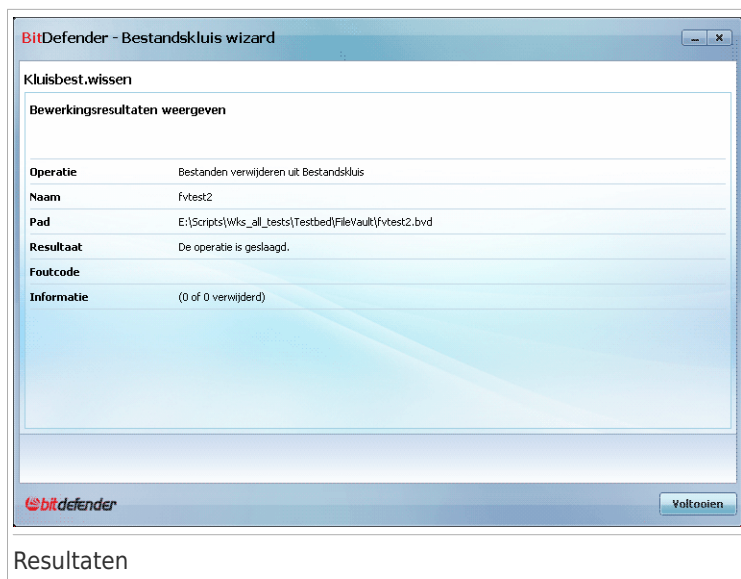
Hier kan u de gekozen acties controleren.



Klik op **Volgende**.

Stap 5/5 - Resultaten

Hier kan u het resultaat van de actie zien.



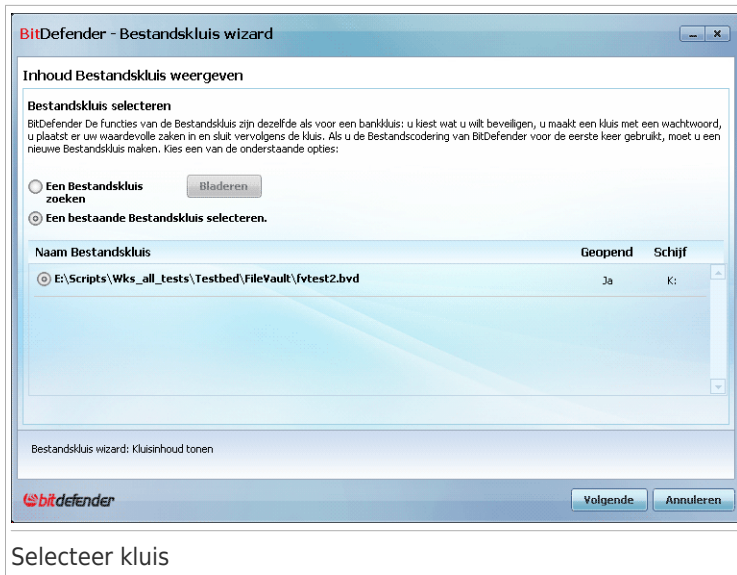
Klik op **Voltooien**.

11.4.3. Bestandskluis weergeven

Deze wizard helpt u bij het openen van een specifieke bestandskluis en het weergeven van de bestanden die de kluis bevat.

Stap 1/4 - Kluis selecteren

Hier kan de kluis waarvan u de bestanden wilt zien, opgeven.



Selecteer kluis

Als u **Bladeren naar een bestandskluis** selecteert, moet u klikken op **Bladeren** en de bestandskluis selecteren. U gaat dan ofwel naar stap 3 als de geselecteerde kluis open is, ofwel naar stap 2 als deze vergrendeld is.

Als u klikt op **Een bestaande bestandskluis selecteren**, dan moet u klikken op de naam van de gewenste kluis. U gaat dan ofwel naar stap 3 als de geselecteerde kluis open is, ofwel naar stap 2 als deze vergrendeld is.

Klik op **Volgende**.

Stap 2/4 - Wachtwoord

Hier wordt u gevraagd het wachtwoord van de geselecteerde kluis in te voeren.

BitDefender - Bestandskluiz wizard

Inhoud Bestandskluiz weergeven

Wachtwoord Bestandskluiz vragen
Voer het wachtwoord van de momenteel geselecteerde Bestandskluiz in.

Wachtwoord:

Het wachtwoord van het kluizbestand opgeven.

bitdefender

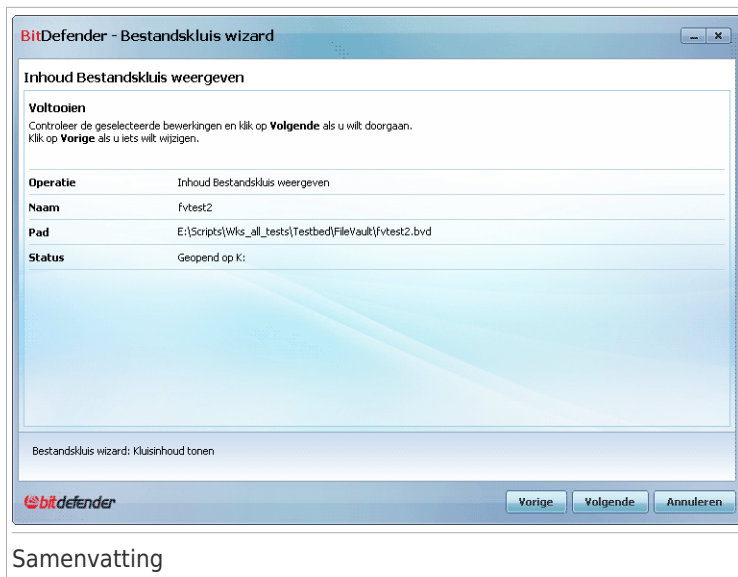
Vorige Volgende Annuleren

Voer wachtwoord in

Typ het wachtwoord in het overeenkomende veld en klik op **Volgende**.

Stap 3/4 - Overzicht

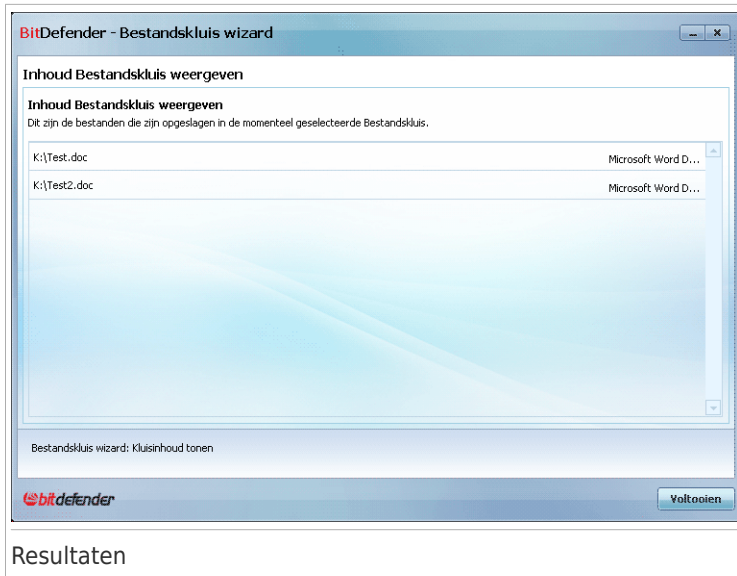
Hier kan u de gekozen acties controleren.



Klik op **Volgende**.

Stap 4/4 - Resultaten

Hier kan u de bestanden van de kluis bekijken.



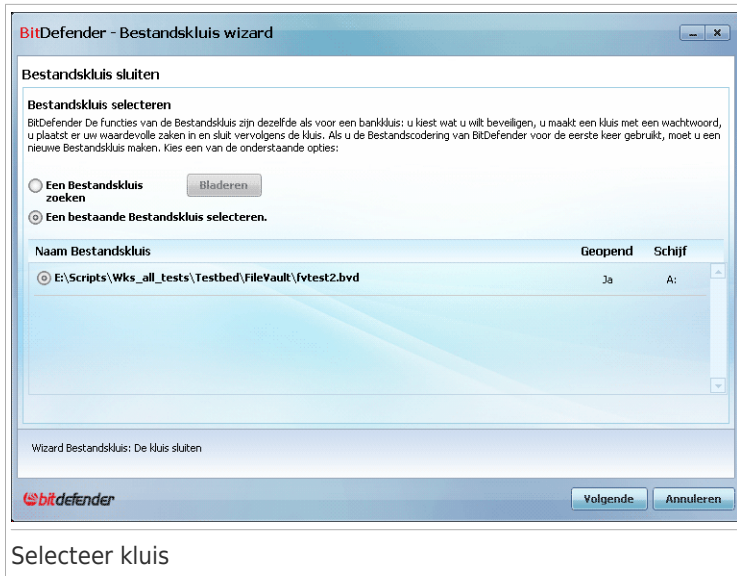
Klik op **Voltooien**.

11.4.4. Bestandskluis vergrendelen

Deze wizard helpt u bij het vergrendelen van een specifieke bestandskluis om zijn inhoud te beschermen.

Stap 1/3 - Kluis selecteren

Hier kan u de te vergrendelen kluis opgeven.



Selecteer kluis

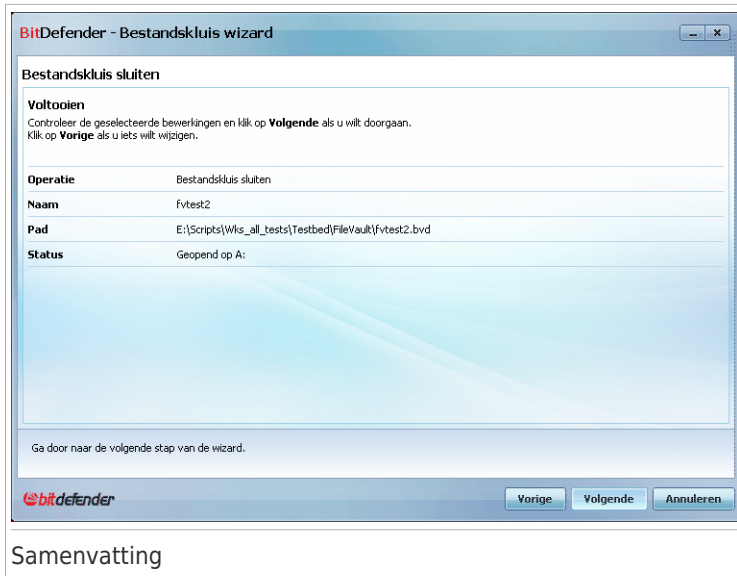
Als u **Bladeren naar een bestandskluis** selecteert, moet u klikken op **Bladeren** en de bestandskluis selecteren.

Als u klikt op **Een bestaande bestandskluis selecteren**, dan moet u klikken op de naam van de gewenste kluis.

Klik op **Volgende**.

Stap 2/3 – Overzicht

Hier kan u de gekozen acties controleren.



Klik op **Volgende**.

Stap 3/3 - Resultaten

Hier kan u het resultaat van de actie zien.



Klik op **Voltooien**.

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 **Ouder** is geselecteerd, kunt u via de knop **Ouderlijk toezicht** de instellingen voor Ouderlijk toezicht configureren. Raadpleeg "**Ouderlijk Toezicht**" (p. 191) voor more informatie over de manier waarop u Ouderlijk toezicht wilt configureren.
 - ▶ 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. Beveiliging

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



De beveiligingsmodule 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, Systeemsan, Mijn documenten scannen, Diepe systeemsan, Aangepaste scan, Kwetsbaarheidsscan.

13.1. Statusgebied

In het statusgebied vindt u de volledige lijst met componenten van de bewaakte beveiligingscomponenten 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

U moet de statustracing inschakelen voor een component als u op de hoogte wilt worden gebracht wanneer problemen de beveiliging van die component beïnvloeden. 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.
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.

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.

- **Firewall** - BitDefender bewaakt de status van de Firewall-functie. Als deze niet is ingeschakeld, wordt het probleem **Firewall is uitgeschakeld** gerapporteerd.
- **Antispam** - BitDefender bewaakt de status van de Antispam-functie. Als deze niet is ingeschakeld, wordt het probleem **Antispam is uitgeschakeld** gerapporteerd.
- **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 Windows-updates, toepassingsupdates of zwakke wachtwoorden.
Er zijn meerdere kwetsbaarheden gedetecteerd	BitDefender heeft ontbrekende Windows/toepassingsupdates en/of zwakke wachtwoorden gevonden.

Status	Beschrijving
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.

13.2. Snelle taken

Hier vindt u koppelingen naar de belangrijkste beveiligingstaken:

- **Update nu** - start een directe update.
- **Systeemsan** - start een standaard scan van uw computer (archieven uitgesloten). Voor extra scantaken op aanvraag, klikt u op de pijl op deze knop  en selecteert u een andere scantaak: Mijn documenten scannen of Diepe systeemsan.
- **Aangepaste scan** - start een wizard waarmee u een aangepaste scantaak kunt maken en uitvoeren.
- **Kwetsbaarheid scannen** - start een wizard die uw systeem controleert op zwakke punten en u helpt ze op te lossen.

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
Systeemsan	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 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.
Aangepast scannen	Gebruik deze taak om specifieke bestanden en mappen te kiezen die moeten worden gescand.



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.

Wanneer u Systeemsan, Diepe systeemsan of Mijn documenten scannen uitvoert, verschijnt de Antivirusscanwizard. Volg de begeleide procedure van drie stappen om het scanproces te voltooien. Raadpleeg "*Antivirusscanwizard*" (p. 57) 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. 62) voor gedetailleerde informatie over deze wizard.

13.2.3. Bezig met zoeken van kwetsbaarheden

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

Om uw computer te controleren op kwetsbaarheden, klikt u op **Kwetsbaarheidsscan** en volgt u de begeleide procedure van zes stappen. Meer informatie vindt u onder *“Zwakke punten verwijderen”* (p. 248).

14. Ouderlijk

BitDefender Internet Security 2010 bevat een module Ouderlijk toezicht. Met Ouderlijk toezicht kunt u de toegang van uw kinderen tot het internet en specifieke toepassingen beperken. Om de status van Ouderlijk toezicht te controleren, klikt u op het tabblad **Ouderlijk**.



De Ouderlijke module bestaat uit twee delen:

- **Statusgebied** - Hiermee kunt u zien of Ouderlijk toezicht is geconfigureerd en kunt u het volgen van de activiteiten van deze module in- of uitschakelen.
- **Snelle taken** - Hier vindt u koppelingen naar de belangrijkste beveiligingstaken: Systemscan, Diepe scan, Nu bijwerken.

14.1. Statusgebied

De huidige status van de module Ouderlijk toezicht 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 **Ouderlijk toezicht is niet geconfigureerd**.

Als u wilt dat BitDefender de module Ouderlijk toezicht bewaakt, klikt u op **Statustracering configureren** en schakelt u het selectievakje **Waarschuwingen inschakelen** in voor deze module.

14.2. Snelle taken

Hier vindt u koppelingen naar de belangrijkste beveiligingstaken:

- **Update nu** - start een directe update.
- **Systeemsan** - start een volledige scan van uw computer (archieven uitgesloten).
- **Diepe systeemsan** - start een complete scan van uw computer (inclusief archiefbestanden).

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

Taak	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.



Opmerking

Omdat de taken **Diepe systeemsan** en **Volledige 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.

Wanneer u een scan uitvoert, verschijnt de Antivirusscanwizard. Volg de begeleide procedure van drie stappen om het scanproces te voltooien. Raadpleeg "**Antivirusscanwizard**" (p. 57) voor gedetailleerde informatie over deze wizard.

15. Bestandskluis

BitDefender is uitgerust met een module Bestandskluis waarmee u uw gegevens zowel veilig als vertrouwelijk kunt houden. Om dit doel te bereiken, kunt u bestands codering gebruiken.

Met deze functie kunt u bestanden beschermen door ze in bestandskluizen te plaatsen.

- De bestandskluis is een veilige opslagplaats voor persoonlijke informatie of gevoelige bestanden.
- De bestandskluis is een gecrypteerd bestand op uw computer met de extensie bvd. Omdat het gecrypteerd is, is de data erin ongevoelig voor diefstal of voor een gat in de beveiliging.
- Als u dit bvd bestand opent, verschijnt een nieuwe logische partitie (een nieuwe schijf). Vergelijk dit met het openen van een ISO beeld als virtuele cd.

Open Deze Computer en u ziet een nieuwe schijf: uw bestandskluis. Hierop kan u bestandshandelingen doen (kopiëren, verwijderen, veranderen, enz). De bestanden zijn beveiligd zolang ze op deze schijf staan (omdat een wachtwoord nodig is bij het openen).

Als u klaar bent, vergrendelt (sluit) u de kluis zodat de inhoud ervan weer veilig is.

Klik op het tabblad **Bestandssafe** om de Bestandssafe-module te openen.



De Bestandssafe-module bestaat uit twee delen:

- **Statusgebied** - Hiermee kunt u een volledige lijst van de bewaakte componenten weergeven. U kunt kiezen welke componenten moeten worden bewaakt. Het is aanbevolen de bewakingsoptie in te schakelen voor alle componenten.
- **Snelle taken** - Hier vindt u koppelingen naar de belangrijkste beveiligingstaken: toevoegen, weergeven, vergrendelen en bestandssafes verwijderen.

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** 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.

Het statusgebied op het tabblad Bestandskluis biedt informatie over de status van de module **Bestandsclustering**.

Als u wilt dat BitDefender de module Bestandscodering bewaakt, klikt u op **Statustracing configureren** en schakelt u het selectievakje **Waarschuwingen inschakelen** in.

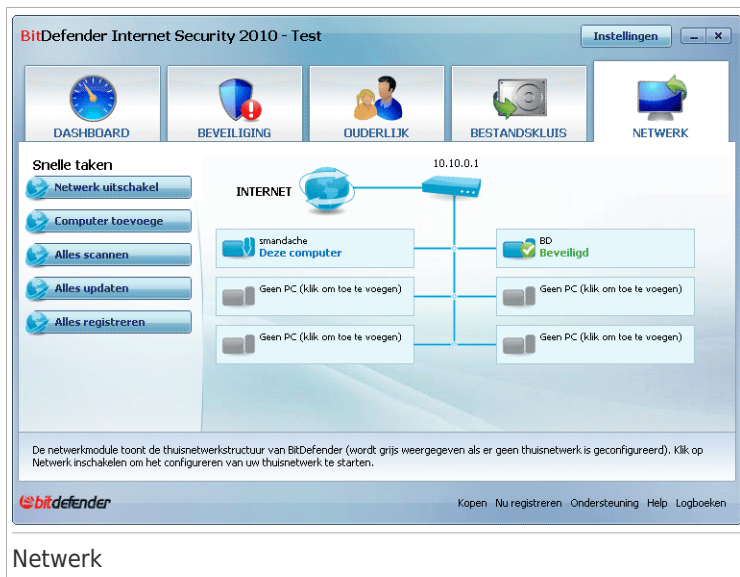
15.2. Snelle taken

De volgende knoppen zijn beschikbaar:

- **Bestand toevoegen aan kluis** - start de wizard waarmee u belangrijke bestanden/documenten privé kan opslaan door ze te crypteren op een speciale beschermde schijf. Meer informatie vindt u onder "*Bestanden toevoegen aan kluis*" (p. 76).
- **Kluisbestanden verwijderen** - start de wizard waarmee u data van de bestandskluis kan wissen. Meer informatie vindt u onder "*Kluisbestanden wissen*" (p. 82).
- **Bestandskluis weergeven** - start de wizard waarmee u de inhoud van uw bestandskluizen kunt weergeven. Meer informatie vindt u onder "*Bestandskluis weergeven*" (p. 87).
- **Bestandskluis vergrendelen** - start de wizard waarmee u een bestandskluis kunt vergrendelen om te starten met het beschermen van zijn inhoud. Meer informatie vindt u onder "*Bestandskluis vergrendelen*" (p. 91).

16. Network

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.



Wachtwoord thuisnetwerk invoeren

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.

Wachtwoord:

Wachtwoord herhalen:

OK Annuleren

Wachtwoord configureren

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

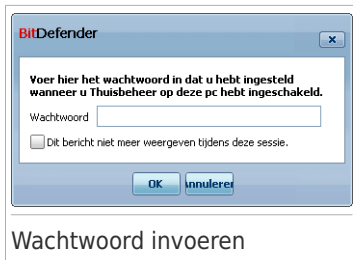
U ziet de naam van de computer in de netwerkmap.

16.1.2. bezig met toevoegen van computers aan het BitDefender netwerk

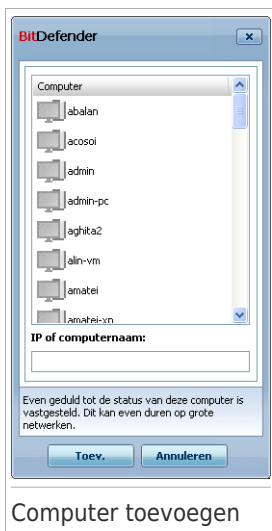
Voordat u een computer kan toevoegen aan het BitDefender thuisnetwerk, moet u het BitDefender thuisbeheer wachtwoord configureren op de betreffende computer.

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.

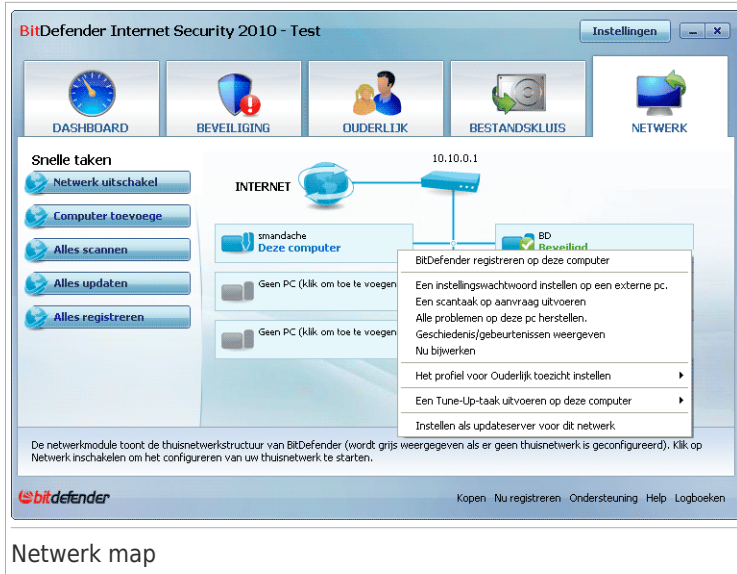


Opmerking

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.

● **Het profiel voor Ouderlijk toezicht instellen**

Hiermee kunt u de leeftijdscategorie instellen die moet worden gebruikt door de webfilter Ouderlijk toezicht op deze computer: kind, tiener of volwassene.

● **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 text reads: "Voer hier het wachtwoord in dat u hebt ingesteld wanneer u Thuisbeheer op deze pc hebt ingeschakeld." Below this is a text input field labeled "Wachtwoord". Under the input field is a checkbox with the text "Dit bericht niet meer weergeven tijdens deze sessie." At the bottom of the dialog are two buttons: "OK" and "Innuleren". Below the dialog box, the text "Wachtwoord invoeren" is displayed.

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



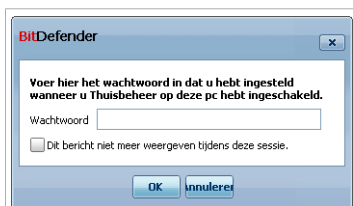
Opmerking

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

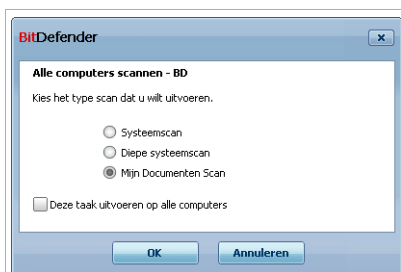
Volg deze stappen om alle beheerde computers te scannen:

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



Wachtwoord invoeren

2. Selecteer een scantype.
 - **Systeemsan** - start een volledige scan van uw computer (archieven uitgesloten).
 - **Diepe systeemsan** - start een complete scan van uw computer (inclusief archiefbestanden).
 - **Mijn documenten scannen** - start een snelscan van uw documenten en instellingen.



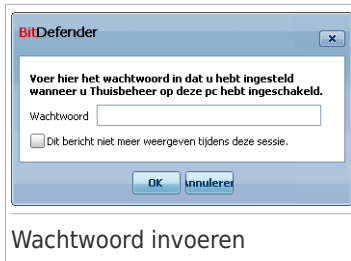
Scantype selecteren

3. Klik op **OK**.

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.

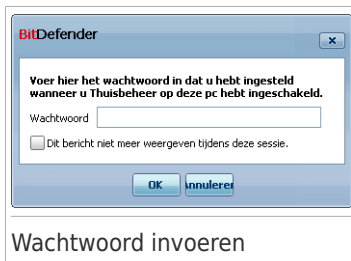


2. Klik op **OK**.

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.

BitDefender Internet Security 2010

Instellingen

Dashboard Instellingen Systeem Info

Algemeen

Antivirus

Antispam

Ouderlijk Toezicht

Privacybeheer

Firewall

Kwetsbaarheid

Encryptie

Special modus

Thuisnetwerk

Update

Registratie

Beveiligingsstatus

WAARSCHUWING: 4 problemen beïnvloeden de beveiligingsstatus van deze pc. [Herstellen](#)

Statustracering configureren

Statistieken

Gescande bestanden: 1153

Gedesinfecteerde bestanden: 0

Geïnfecteerde bestanden gedetecteerd: 0

Systeemscaan: noot

Volgende scan: 9/1/2009 2:00:00 AM

Overzicht

Update: noot

BitDefender-account: testare.automata@mail...

Registratie: Geldig

Vervalt binnen: 326 dagen

Bestandsactiviteit

Netwerkmactiviteit

De dashboardmodule toont de beveiligingsstatus van het product, samen met koppelingen naar de belangrijkste productmodules.

bitdefender

Vernieuwen Nu registreren Ondersteuning Help Logboeken

Dashboard

Het dashboard bestaat uit verschillende delen:

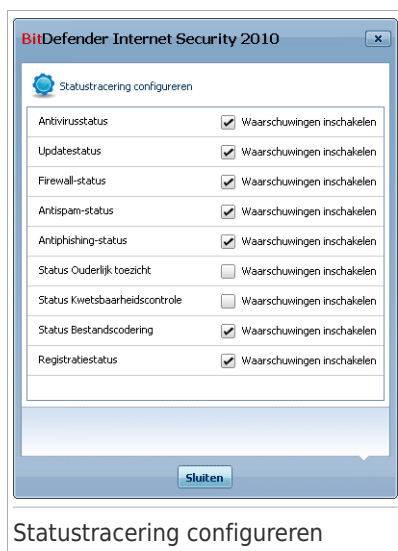
- **Algemene status** - Informeert u over problemen die de beveiliging van uw computer beïnvloeden.
- **Statistieken** - Toont belangrijke informatie over de BitDefender activiteit.
- **Overzicht** - Toont de updatestatus, uw accountstatus, registratie en licentie-informatie.

- **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.
- **Netwerkactiviteit** - Geeft de evolutie aan van het netwerkverkeer, gefilterd door BitDefender Firewall. 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 Internet Security 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 bied 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.

- **Firewall** - BitDefender bewaakt de status van de Firewall-functie. Als deze niet is ingeschakeld, wordt het probleem **Firewall is uitgeschakeld** gerapporteerd.
- **Antispam** - BitDefender bewaakt de status van de Antispam-functie. Als deze niet is ingeschakeld, wordt het probleem **Antispam is uitgeschakeld** gerapporteerd.
- **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.
- **Ouderlijk toezicht** - BitDefender bewaakt de status van de functie Ouderlijk toezicht. Als deze niet is ingeschakeld, wordt het probleem **Ouderlijk toezicht is niet geconfigureerd** 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 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.

- **Bestandscodering** bewaakt de status van de Bestandskluis. Als deze niet is ingeschakeld, wordt het probleem **Bestandscodering is uitgeschakeld** gerapporteerd.



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 systeemsan	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 scannen. Om de volledige computer te scannen, gaat u naar Antivirus , tabblad Virusscan en voert u een Volledige systeemsan of een Diepe systeemsan 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

Item	Beschrijving
	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**.



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:

Voer wachtwoord in

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

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

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



Belangrijk

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

- **Wachtwoord vragen voor inschakelen Ouderlijk Toezicht** - als deze optie is ingeschakeld en er is geen wachtwoord ingesteld, wordt u gevraagd een wachtwoord in te stellen bij het inschakelen van Ouderlijk Toezicht. Door het instellen van een wachtwoord, voorkomt u dat andere gebruikers met beheerdersrechten de instellingen van Ouderlijk Toezicht, die u voor een bepaalde gebruiker hebt geconfigureerd, kunnen wijzigen.
- **BitDefender-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

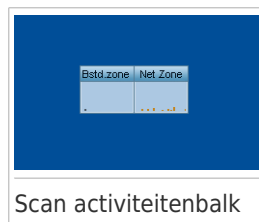
Beginnersmodus/Gemiddelde modus of alleen wanneer de interface in de Expert-modus is.

- **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.



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**.



Systeme- 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

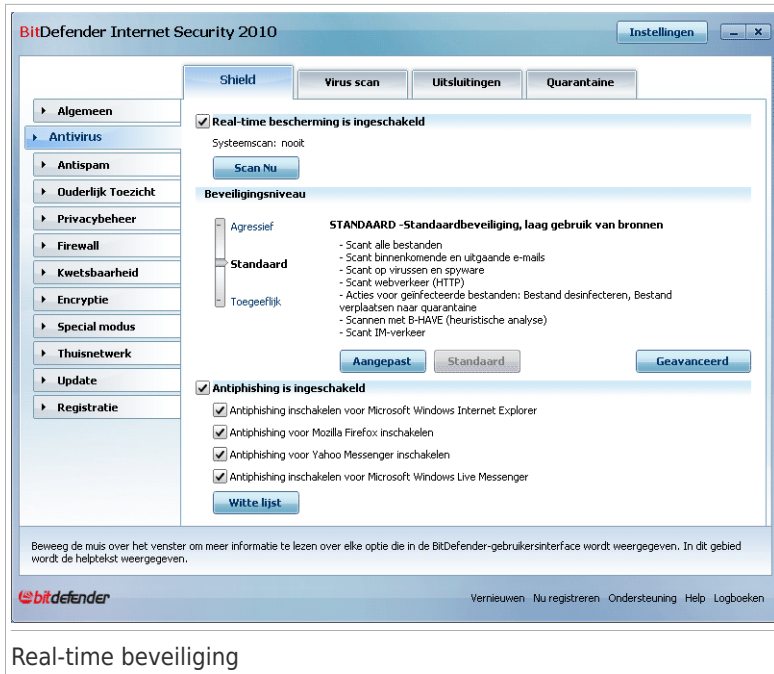
Real-time bescherming wordt ook wel on-access scannen geneemd - bestanden worden gescand als de gebruikers deze openen.

- **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.



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:

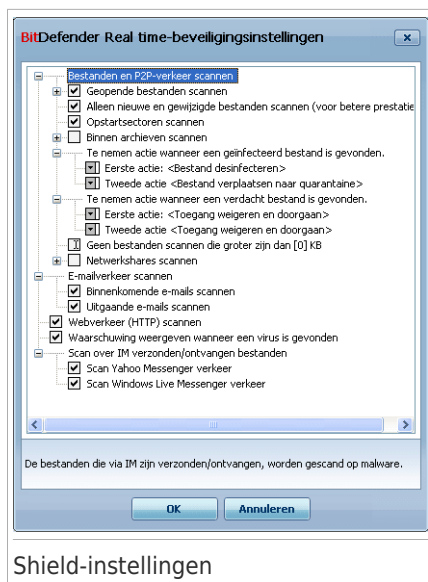
Beveiligingsniveau	Beschrijving
Toegeeflijk	<p>Dekt de basisbehoeften aan beveiliging. Het verbruiksniveau van de bron is zeer laag.</p> <p>Alleen programma's en binnenkomende e-mailberichten worden op virussen gescand. Naast de klassieke op handtekeningen gebaseerde scan, wordt ook de heuristische analyse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

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
	<p>.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.</p>
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	<p>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.</p> <p>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.</p>
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	<p>De geopende archieven worden gescand. Wanneer u deze optie inschakelt, zal de computer langzamer werken.</p> <p>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.</p>

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.



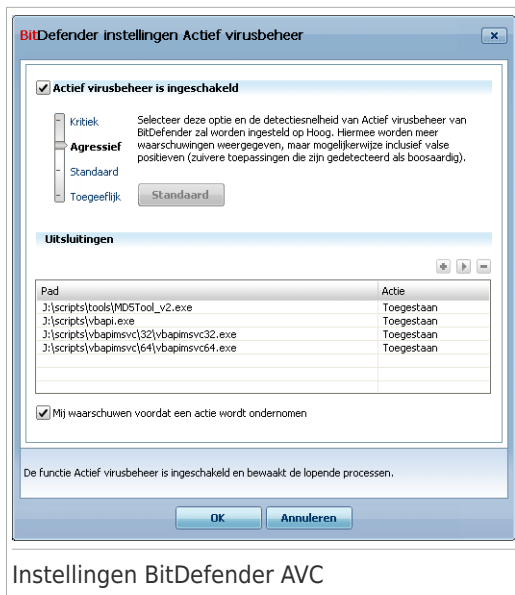
Waarschuwing Actief virusbeheer BitDefender

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 ij 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. 293).

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

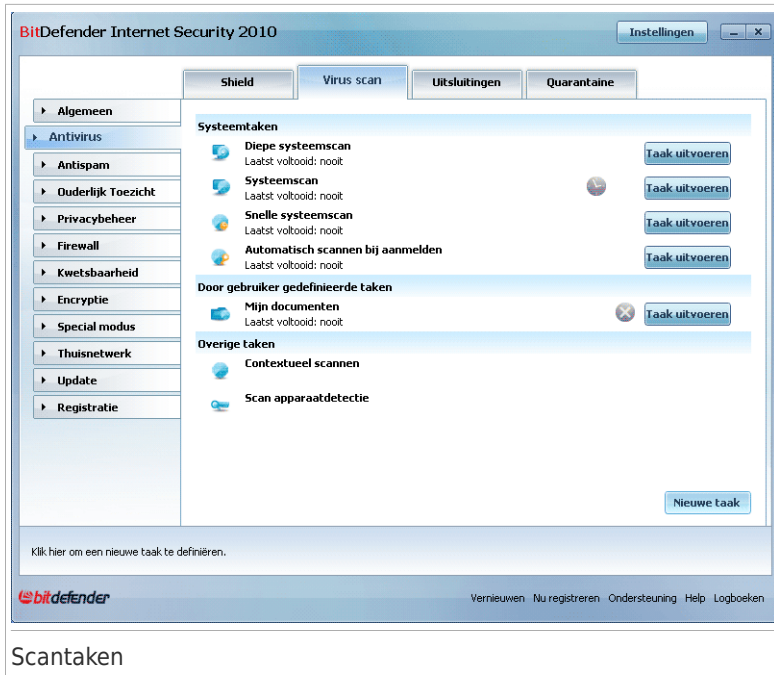
Klik op **Save** om de wijzigingen op te slaan en het venster te sluiten.

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. 145).

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	<p>Scant de items die worden uitgevoerd als een gebruiker zich aanmeldt bij Windows. Standaard is het automatisch scannen bij het aanmelden uitgeschakeld.</p> <p>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).</p>



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

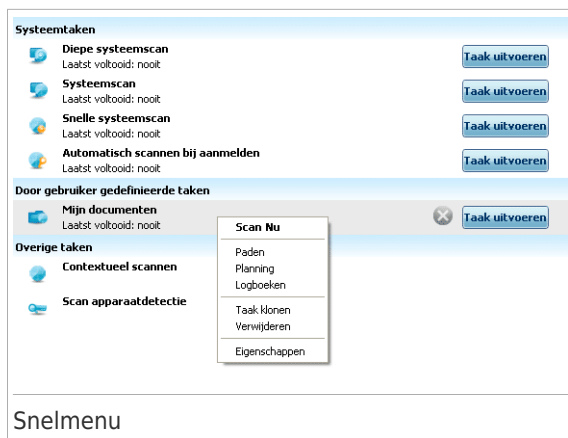
Niet beschikbaar voor systeemtaken. U kunt geen systeemtaak verwijderen.

-  **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 dupliceert 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. 165).

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
Toegankelijk	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.

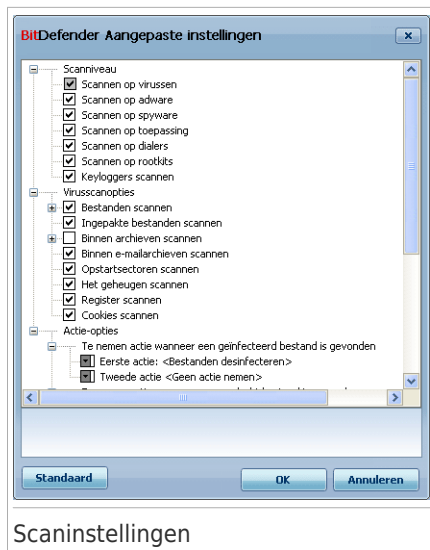
- **De taak uitvoeren met lage prioriteit.** Verlaagt de prioriteit van het scanproces. U zult andere programma's sneller kunnen uitvoeren en de tijd die nodig is om het scanproces te voltooien, verlengen.
- **Scanwizard minimaliseren naar taakbalk.** Minimaliseert het scanvenster naar het **systeemvak**.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

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

Het scanniveau aanpassen

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

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



Scaninstellingen

De scanopties zijn georganiseerd als een 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 gearchiveerde 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

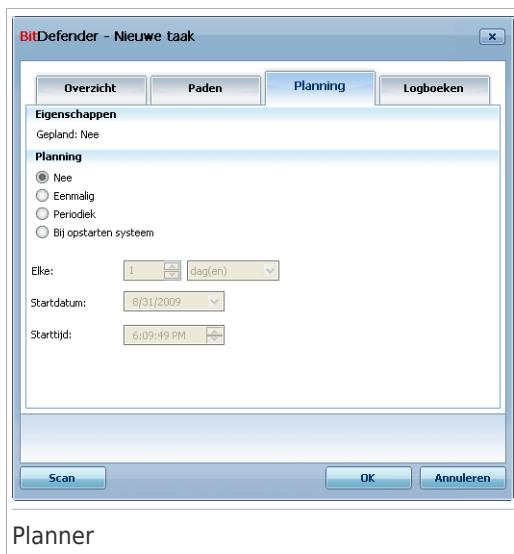
Systeemscaan en **Diepe systeemscaan** zal alle lokale stations scannen, terwijl **Snelle systeemscaan** alleen de mappen van Windows en van Program Files zal scannen.

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.

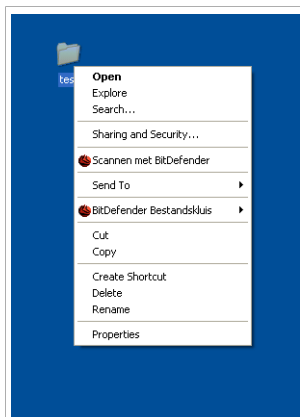
Gebruik een van de volgende methoden om een scantaak uit te voeren:

- 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.



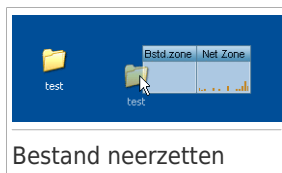
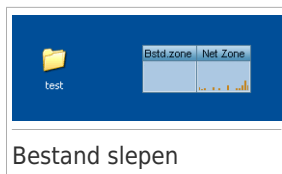
Contextueel scannen

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 **Contextmenuscan** 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.

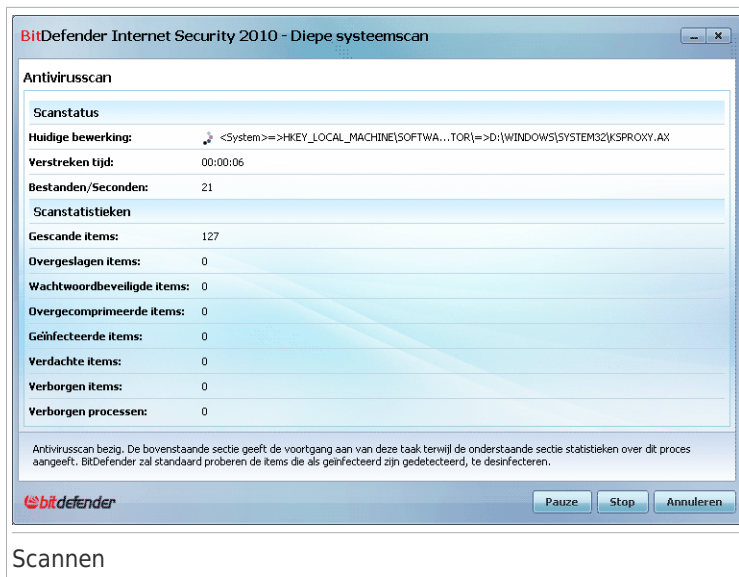


Opmerking

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.



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:

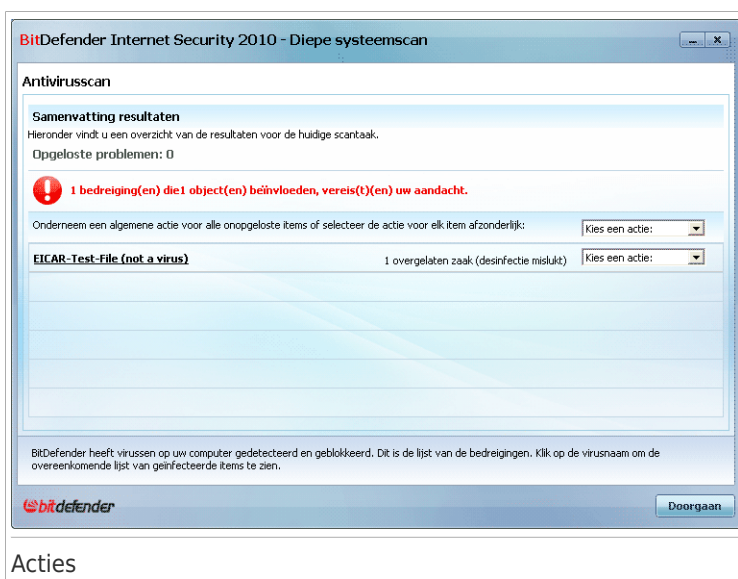
- **Wachtwoord.** Als u wilt dat BitDefender het archief scant, moet u deze optie selecteren en het wachtwoord invoeren. Als u het wachtwoord niet kent, kies dan een van de andere opties.
- **Geen wachtwoord vragen en dit object overslaan bij het scannen.** Selecteer deze optie om het scannen van dit 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.



Acties

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

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

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

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

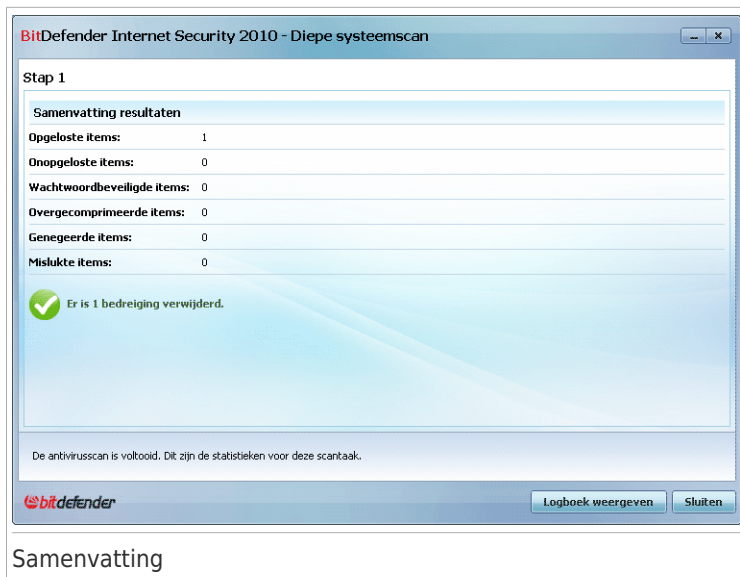
Actie	Beschrijving
Geen actie nemen	Er wordt geen actie ondernomen voor de geïnfecteerde bestanden. Als de scan is voltooid, kan u het

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	<p>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.</p> <p>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.</p>

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.



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.

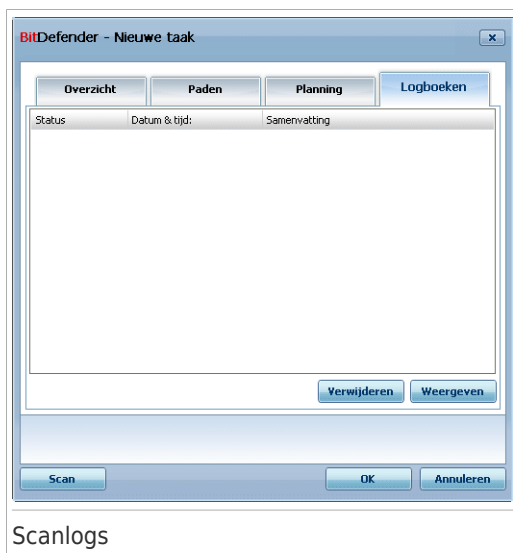
BitDefender detecteerde verdachte bestanden

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.



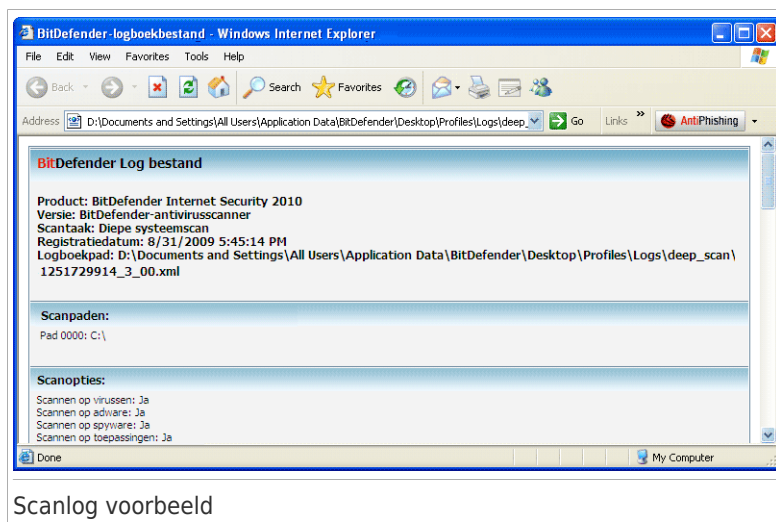
Opmerking

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:

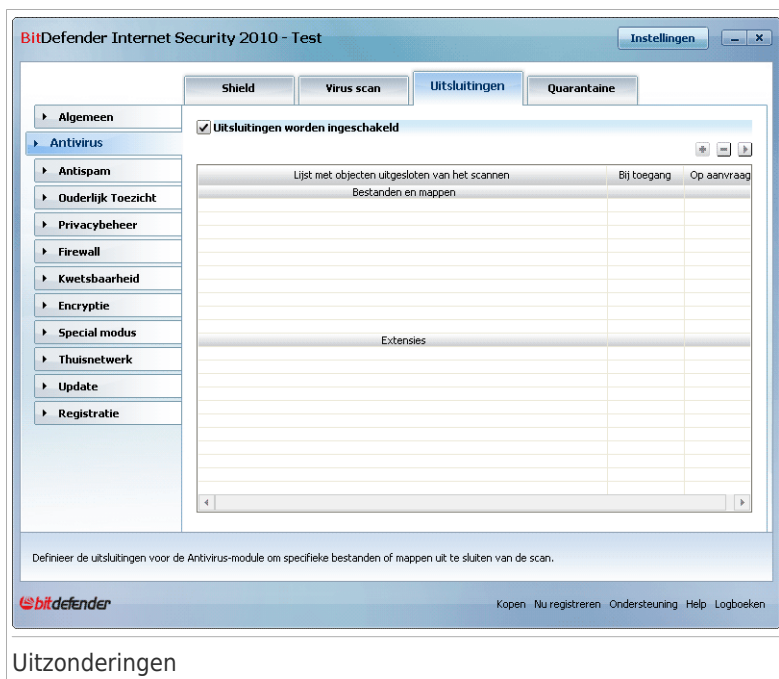
- **Paden** - het bestand of de map (inclusief alle objecten die erin zijn opgenomen) die is aangegeven door een opgegeven pad, wordt uitgesloten van het scannen.
- **Extensies** - alle bestanden met een specifieke extensie worden uitgesloten van het scannen.



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

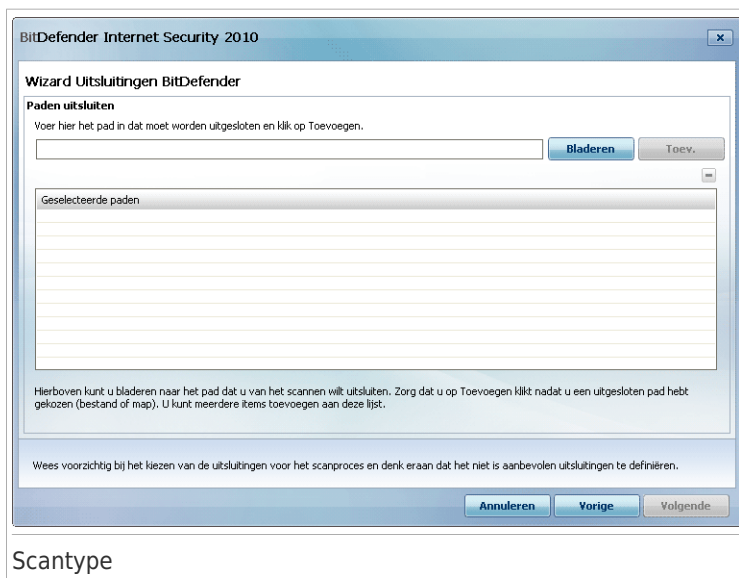
Als het opgegeven pad niet bestaat, verschijnt een foutbericht. Klik op **OK** en controleer het pad.

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 1/4 - Objecttype selecteren



Objecttype

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

Klik op **Volgende**.

Stap 2/4 - Uitgesloten extensies opgeven

BitDefender Internet Security 2010

Wizard Uitsluitingen BitDefender

Wizard Uitsluitingen BitDefender

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

.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.

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

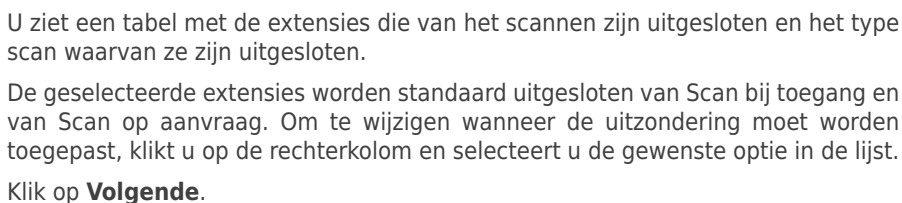
Het menu bevat een lijst met alle extensies die op uw systeem zijn geregistreerd. Wanneer u een extensie selecteert, kan u de beschrijving zien, indien deze beschikbaar is.

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

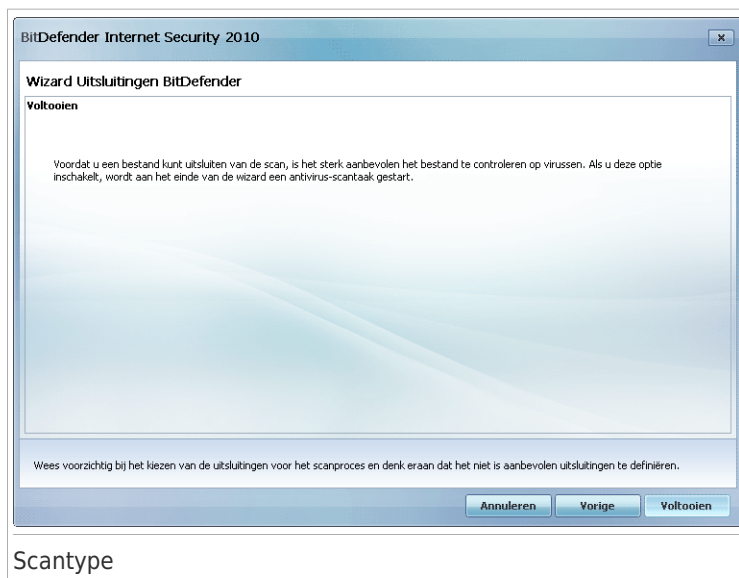
De extensies verschijnen in de tabel wanneer u ze toevoegt. U kan zoveel extensies toevoegen als u wilt.

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

Klik op **Volgende**.



Stap 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.

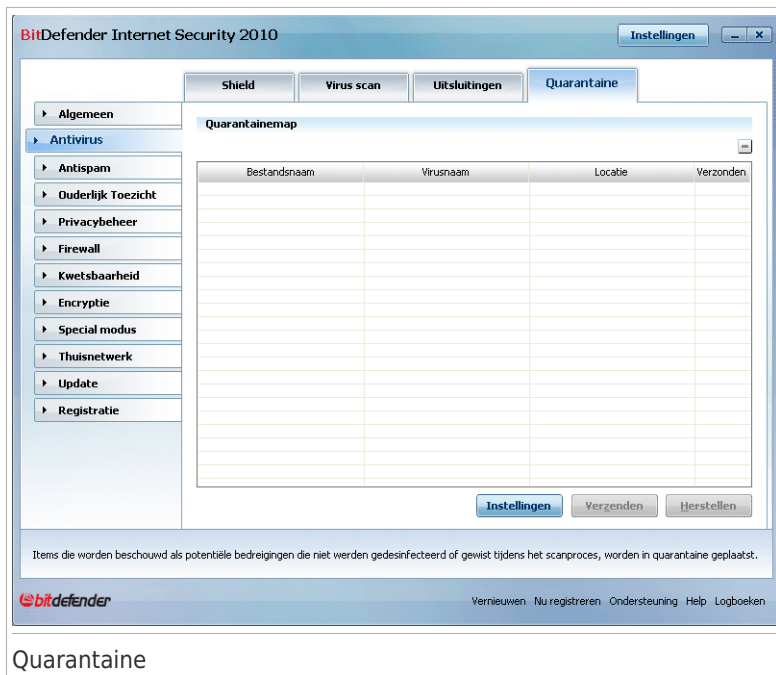
Klik op **Voltooien**.

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.

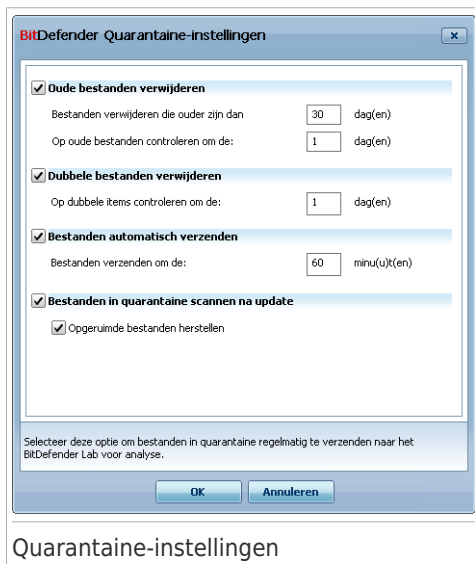
Om een geselecteerd bestand uit de quarantaine te verwijderen, klikt u op de knop **Verwijderen**. Als u een geselecteerd bestand wilt terugzetten op zijn oorspronkelijke locatie, klikt u op **Herstellen**.

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. Antispam

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

19.1. Antispam-begrippen

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

19.1.1. Antispamfilters

De BitDefender Antispam-engine bevat verschillende filters die garanderen dat uw Postvak IN vrij blijft van SPAM: **Vriendenlijst**, **Spammerslijst**, **Tekensetfilter**, **Afbeeldingsfilter**, **URL-filter**, **NeuNet (Heuristisch) filter** en **Bayes-filter**.



Opmerking

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

Vriendenlijst / Spammerslijst

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

De vrienden-/spammerslijst kan worden beheerd in de interface van de **Expert-modus** interface of via de **Antispam-werkbalk** die in sommige van de vaakst gebruikte e-mailclients is geïntegreerd.



Opmerking

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

Tekensetfilter

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

Afbeeldingsfilter

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

URL-filter

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

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

NeuNet (Heuristische) filter

De **NeuNet (Heuristische) filter** voert een aantal tests uit op alle componenten van het bericht (dus niet alleen op de koptekst, maar ook op het hoofdbericht in HTML- of tekstindeling). Hierbij wordt gezocht naar woorden, zinnen, koppelingen of andere kenmerken van SPAM. Op basis van de resultaten van de analyse, voegt het programma een SPAM-score aan het bericht toe.

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



Opmerking

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

Bayes-filter

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

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

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



Belangrijk

U kunt de Bayes-filter corrigeren met de knoppen **Is spam** en **Geen spam** in de **Antispam-werkbalk**.

19.1.2. Antispamgebruik

De BitDefender Antispam-engine gebruikt alle antispamfilters samen om vast te stellen of een bepaald e-mailbericht in uw **Postvak IN** moet belanden.



Belangrijk

De spamberichten die door BitDefender worden gedetecteerd, zijn gemarkeerd met de prefix [SPAM] in de onderwerpregel. BitDefender verplaatst spamberichten automatisch naar een specifieke map, zoals hieronder beschreven:

- In Microsoft Outlook worden spamberichten verplaatst naar een map **Spam** die zich in de map **Verwijderde items** bevindt. De map **Spam** wordt gemaakt tijdens de installatie van BitDefender.
- In Outlook Express en Windows Mail worden spamberichten direct naar **Verwijderde items** verplaatst.
- In Mozilla Thunderbird worden spamberichten verplaatst naar een map **Spam** die zich in de map **Trash** bevindt. De map **Spam** wordt gemaakt tijdens de installatie van BitDefender.

Als u andere e-mailclients gebruikt, moet u een regel maken om e-mailberichten met de markering [SPAM] door BitDefender te laten verplaatsen naar een aangepaste quarantainemap.

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

Anders zal de filter **Spammerslijst** de e-mail overnemen om te controleren of het adres van de afzender in zijn lijst voorkomt. De e-mail zal worden gelabeld als SPAM

en naar de map **Spam** worden verplaatst (bevindt zich in **Microsoft Outlook**) als een overeenkomst wordt gevonden.

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

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

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

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



Opmerking

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

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

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

19.1.3. Antispam-updates

Telkens wanneer u een update uitvoert:

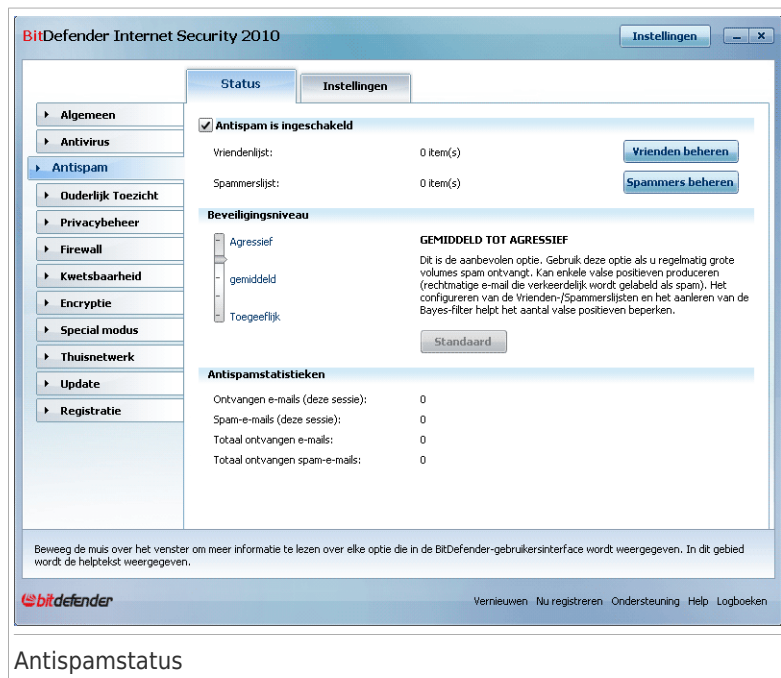
- worden nieuwe afbeeldingshandtekeningen toegevoegd aan de **Afbeeldingsfilter**.
- worden nieuwe koppelingen toegevoegd aan de **URL-filter**.
- Er worden nieuwe regels toegevoegd aan de **NeuNet (heuristische) filter**.

Dit zal de doeltreffendheid van uw Antispam-engine verbeteren.

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

19.2. Status

Om de antispambeveiliging te configureren, gaat u naar **Antispam>Status** in de Expert-modus.



Antispamstatus

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



Belangrijk

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

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

19.2.1. Het beveiligingsniveau instellen

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

Er zijn 5 beveiligingsniveaus:

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

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

19.2.2. De Vriendenlijst configureren

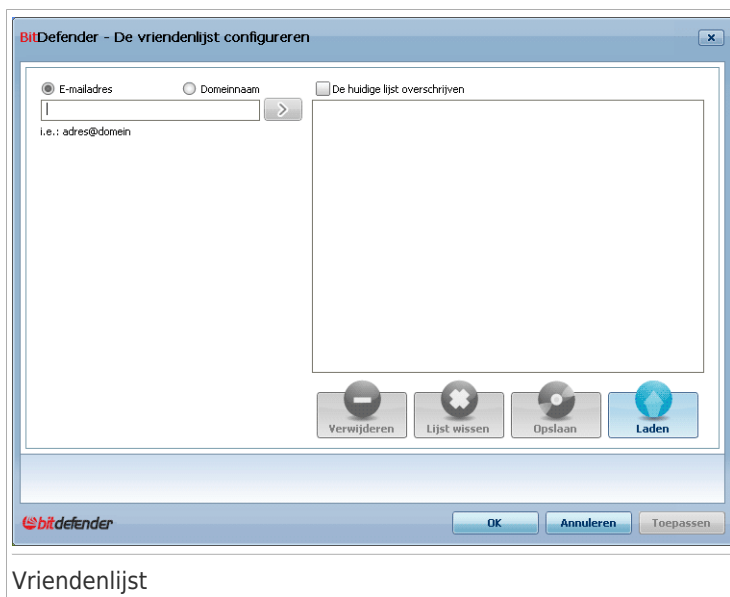
De **Vriendenlijst** is een lijst van alle e-mailadressen waarvan u altijd berichten wilt ontvangen, ongeacht hun inhoud. Berichten van uw vrienden zijn niet als spam gelabeld, zelfs wanneer de inhoud op spam lijkt.



Opmerking

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

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



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

Als u een e-mailadres wilt toevoegen, schakelt u de optie **E-mailadres** in. Typ vervolgens het adres en klik op . Het adres verschijnt in de **Vriendenlijst**.



Belangrijk

Syntaxis: naam@domein.com.

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



Belangrijk

Syntaxis:

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

- *com* - alle ontvangen e-mailberichten die het domeinachtervoegsel com hebben, zullen uw **Postvak IN** bereiken, ongeacht hun inhoud;

Om een item uit de lijst te verwijderen, selecteert u het item en klikt u op de knop **Verwijderen**. Om alle gegevens uit de lijst te verwijderen, klikt u op de knop **Lijst wissen** en vervolgens op **Ja** om te bevestigen.

U kunt de vriendenlijst opslaan naar een bestand zodat u het kunt gebruiken op een andere computer of na het opnieuw installeren van het product. Om de vriendenlijst op te slaan, klikt u op de knop **Opslaan** en slaat u het op naar de gewenste locatie. Het bestand zal de extensie **.bwl** hebben.

Om een eerder opgeslagen vriendenlijst te laden, klikt u op de knop **Laden** en opent u het overeenkomende bwl-bestand. Om de inhoud van de huidige lijst opnieuw in te stellen wanneer u een eerder opgeslagen lijst laadt, selecteert u **De huidige lijst overschrijven**.



Opmerking

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

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

19.2.3. Spammerslijst configureren

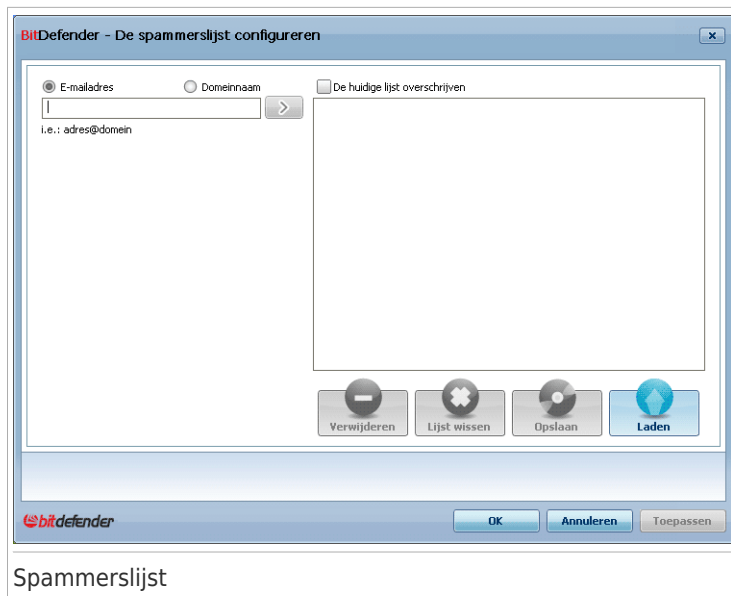
De **Spammerslijst** is een lijst van alle e-mailadressen waarvan u geen berichten wilt ontvangen, ongeacht hun inhoud.



Opmerking

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

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



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

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



Belangrijk

Syntaxis: naam@domein.com.

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



Belangrijk

Syntaxis:

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



Waarschuwing

Voeg geen domein van rechtmatige e-mailservices via het web (zoals Yahoo, Gmail, Hotmail of andere) toe aan de Spammerslijst. Anders zullen de e-mailberichten die

zijn ontvangen van een geregistreerde gebruiker van een dergelijke service, als spam worden gedetecteerd. Als u bijvoorbeeld **yahoo . com** toevoegt aan de spammerslijst, worden alle e-mailberichten die van adressen van **yahoo . com** afkomstig zijn, als [spam] gemarkeerd.

Om een item uit de lijst te verwijderen, selecteert u het item en klikt u op de knop **Verwijderen**. Om alle gegevens uit de lijst te verwijderen, klikt u op de knop **Lijst wissen** en vervolgens op **Ja** om te bevestigen.

U kunt de spammerslijst opslaan naar een bestand zodat u het kunt gebruiken op een andere computer of na het opnieuw installeren van het product. Om de spammerslijst op te slaan, klikt u op de knop **Opslaan** en slaat u het op naar de gewenste locatie. Het bestand zal de extensie **. bwl** hebben.

Om een eerder opgeslagen Spammerslijst te laden, klikt u op de knop **Laden** en opent u het overeenkomende **bwl**-bestand. Om de inhoud van de huidige lijst opnieuw in te stellen wanneer u een eerder opgeslagen lijst laadt, selecteert u **De huidige lijst overschrijven**.

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

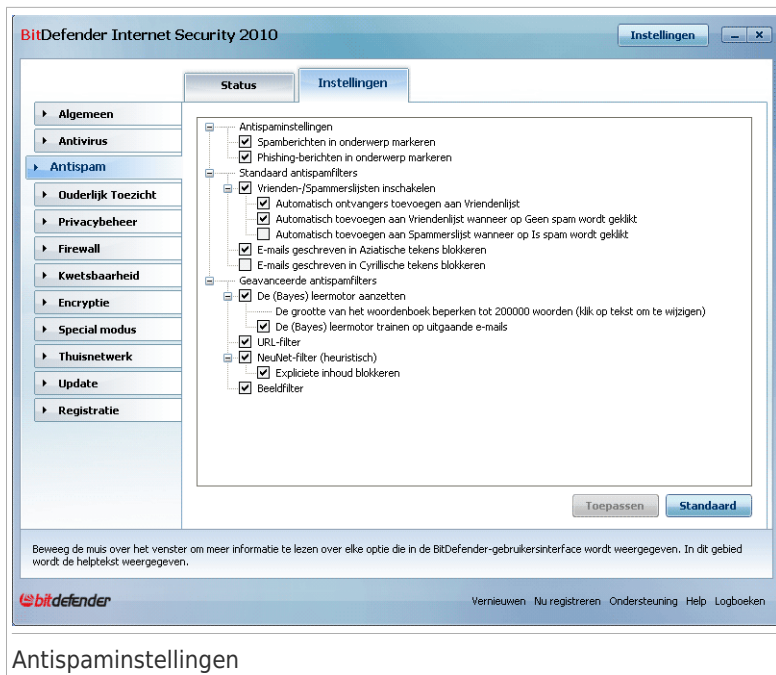


Belangrijk

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

19.3. Instellingen

Om de antispaminstellingen en filters te configureren, gaat u naar **Antispam>Instellingen** in de Expert-modus.



Antispaminstellingen

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



Opmerking

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

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

Om de standaardinstellingen toe te passen, klikt u op **Standaard**.

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

19.3.1. Antispaminstellingen



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

19.3.2. Standaard antispamfilters

- **Vrienden-/Spammerslijsten inschakelen** - met deze optie worden e-mailberichten gefilterd met behulp van de **Vrienden-/Spammerslijsten**.
 - ▶ **Geadresseerden automatisch toevoegen aan Vriendenlijst** - voeg automatisch geadresseerden van verzonden e-mail toe aan de Vriendenlijst.
 - ▶ **Automatisch toevoegen aan Vriendenlijst** - wanneer u op de knop  **Geen spam** klikt in de **Antispam-werkbalk**, wordt de afzender van de geselecteerde e-mail automatisch toegevoegd aan de Vriendenlijst.
 - ▶ **Automatisch toevoegen aan Spammerslijst** - wanneer u op de knop  **Is spam** klikt in de **Antispam-werkbalk**, wordt de afzender van de geselecteerde e-mail automatisch toegevoegd aan de Spammerslijst.



Opmerking

De knoppen  **Geen spam** en  **Is spam** worden gebruikt om het **Bayes-filter** te trainen.

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

19.3.3. Geavanceerde antispamfilters

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



Opmerking

De aanbevolen grootte is: 200.000 woorden.

- ▶ **De Leerengine (Bayes) oefenen op uitgaande e-mails** - oefent de Leerengine (bayes) op uitgaande e-mails.
- **URL-filter** - activeert/deactiveert de **URL-filter**.
- **NeuNet (Heuristische) filter** - activeert/deactiveert de **NeuNet (Heuristische) filter**.
 - ▶ **Expliciete inhoud blokkeren** - activeert/deactiveert de detectie van berichten met de melding SEXUALLY EXPLICIT in de onderwerpregel.
- **Afbeeldingsfilter** - activeert/deactiveert de **Afbeeldingsfilter**.

20. Ouderlijk Toezicht

Met bitDefender Ouderlijk Toezicht kan u de toegang tot het Internet en tot specifieke toepassingen beheren voor elke gebruiker die een gebruikersaccount op het systeem heeft.

U kan Ouderlijk Toezicht configureren voor het blokkeren van:

- ongeschikte webpagina's.
- Toegang tot het Internet gedurende een bepaalde periode (bijvoorbeeld als het tijd is om huiswerk te maken).
- webpagina's, e-mailberichten en instant messages die bepaalde sleutelwoorden bevatten.
- applicaties zoals spelletjes, chatten, programma's die bestanden uitwisselen en dergelijke.
- instant messages van andere dan de toegelaten IM contacten.



Belangrijk

Alleen gebruikers met beheerdersrechten (administrators) op het systeem kunnen Ouderlijk Toezicht openen en configureren. Om er zeker van te zijn dat alleen u de instellingen van Ouderlijk Toezicht kan veranderen, kan u deze beveiligen met een wachtwoord. U wordt gevraagd het wachtwoord in te voeren als u Ouderlijk Toezicht voor een specifieke gebruiker inschakelt.

Om met succes Ouderlijk Toezicht te gebruiken om de computer en online activiteiten van uw kinderen te beperken, moet u de volgende hoofdtaken voltooien:

1. Creëer beperkte (standaard) Windows gebruikersaccounts voor uw kinderen.

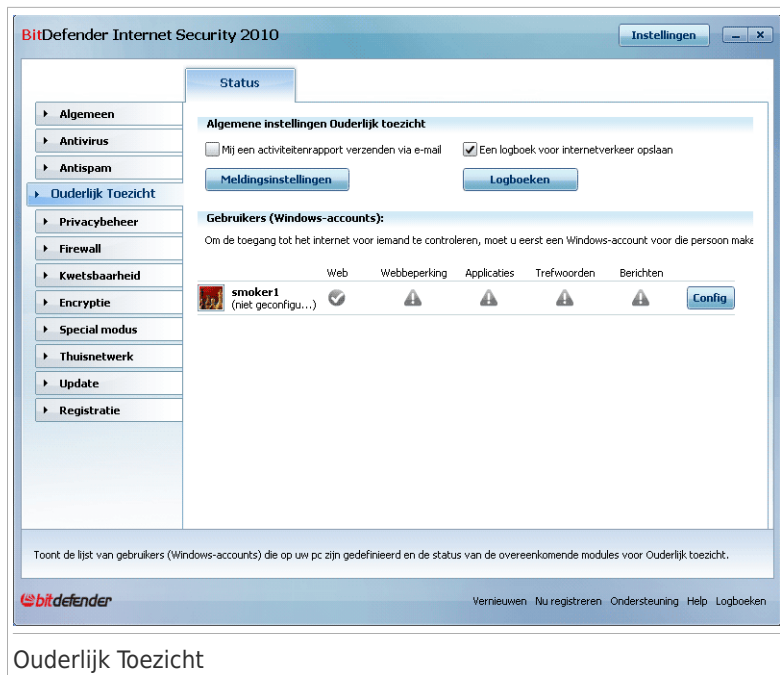


Opmerking

Om te leren Windows gebruikersaccounts te creëren, gaat u naar het Windows Help en ondersteuning centrum (in het Start menu, klik op **Help en ondersteuning**).

2. Configureer Ouderlijk Toezicht voor de Windows gebruikersaccounts van uw kinderen.

Om Ouderlijk toezicht te configureren, gaat u naar **Ouderlijk toezicht** in de Expert-modus.



U ziet informatie over de status van Ouderlijk toezicht voor elke Windows-gebruikersaccount. Wanneer Ouderlijk toezicht is ingeschakeld, wordt de leeftijdscategorie onder elke gebruikersnaam weergegeven. Als Ouderlijk toezicht is uitgeschakeld, is de status **niet geconfigureerd**.

Daarnaast ziet u per gebruiker de status van elke functie van Ouderlijk toezicht:

✓ **Groene cirkel met een vinkje:** De functie is ingeschakeld.

! **Rode cirkel met een uitroepteken:** De functie is uitgeschakeld.

Klik op de knop **Wijzigen** naast een gebruikersnaam om hier het venster te openen waarin u de instellingen voor Ouderlijk toezicht voor de respectieve gebruikersaccount kunt configureren.

In de volgende paragrafen van dit hoofdstuk staan de details van het Ouderlijk Toezicht en hoe u deze configureert.

20.1. Ouderlijk toezicht configureren voor een gebruiker

Om Ouderlijk toezicht te configureren voor een specifieke gebruikersaccount, klikt u op de knop **Wijzigen** die overeenkomt met die gebruikersaccount en klikt u op het tabblad **Status**.



Volg deze stappen om Ouderlijk Toezicht voor deze gebruikersaccount te configureren:

1. Schakel Ouderlijk toezicht in voor deze gebruikersaccount door het selectievakje **Ouderlijk toezicht** in te schakelen.



Belangrijk

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

2. Een wachtwoord instellen om uw Ouderlijk Toezicht instellingen te beveiligen. Meer informatie vindt u onder "*Instellingen Ouderlijk Toezicht Beveiligen*" (p. 194).
3. Stel de leeftijdscategorie in om uw kind alleen de toestemming te geven voor toegang tot websites die geschikt zijn voor zijn/haar leeftijd. Meer informatie vindt u onder "*De leeftijdscategorie instellen*" (p. 195).
4. Configureer de bewakingsopties voor deze gebruiker, zoals nodig:
 - **Mij een activiteitenrapport verzenden via e-mail.** Telkens wanneer Ouderlijk toezicht van BitDefender een activiteit voor deze gebruiker blokkeert, wordt een e-mailmelding verzonden.

- **Een logboek voor internetverkeer opslaan.** Registreert de websites die door de gebruiker zijn bezocht.

Meer informatie vindt u onder "*De activiteit van de kinderen bewaken*" (p. 198).

5. Klik op een pictogram of tabblad om de overeenkomende functie van Ouderlijk toezicht te configureren:

- **Web** - voor het filteren van de webnavigatie volgens de regels die door u zijn ingesteld in de sectie **Web**.
- **Toepassingen** - voor het blokkeren van de toegang tot de toepassingen die door u zijn opgegeven in de sectie **Toepassingen**.
- **Trefwoorden** - voor het filteren van de toegang tot het web, e-mail en expresberichten volgens de regels die door u zijn ingesteld in de sectie **Trefwoorden**.
- **IM** - hiermee kunt u chat met IM-contactpersonen toestaan of blokkeren volgens de regels die door u zijn ingesteld in de sectie **IM-verkeer**.
- **Tijdbeperking** - hiermee biedt u webtoegang in overeenstemming met het tijdschema dat u hebt ingesteld in de sectie **Tijdbeperking**.



Opmerking

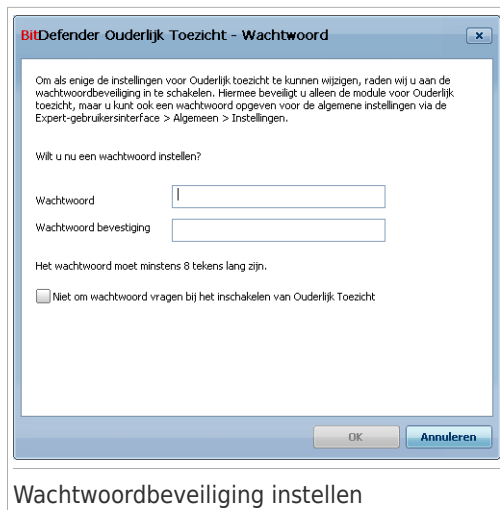
Raadpleeg voor informatie over het configureren ervan, de volgende onderwerpen in dit hoofdstuk.

Om de toegang tot internet volledig te blokkeren, klikt u op de knop **Internet blokkeren**.

20.1.1. Instellingen Ouderlijk Toezicht Beveiligen

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

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



Wachtwoordbeveiliging instellen

Stel de wachtwoordbeveiliging op de volgende manier in:

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

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



Opmerking

Dit wachtwoord beveilgt geen andere instellingen van BitDefender.

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

20.1.2. De leeftijdscategorie instellen

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

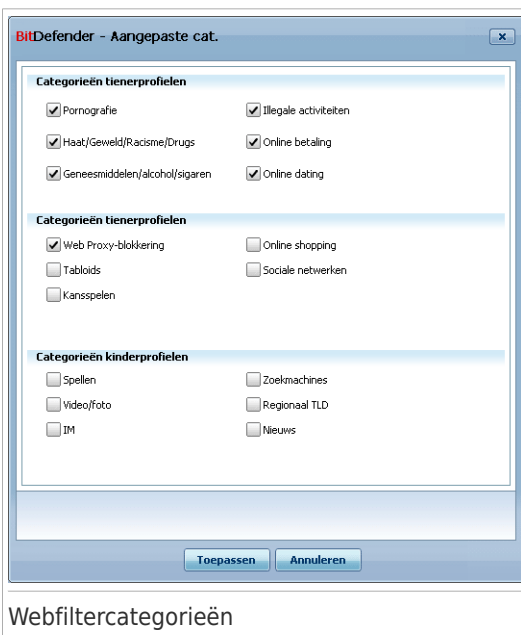
Om webtoegang te filteren met een leeftijdgebonden filter, moet u een bepaald tolerantieniveau instellen. Versleep de schuiver over de schaal om het juiste tolerantieniveau voor de geselecteerde gebruiker in te stellen.

Er zijn 3 tolerantieniveaus:

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

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

Als u meer controle wilt over het type inhoud waaraan de gebruiker op internet is blootgesteld, kunt u de categorieën opgeven van webinhoud die door de webfilter zullen worden geblokkeerd. Om te kiezen welke types webinhoud worden geblokkeerd, klikt u op **Aangepaste categorieën**. Een nieuw venster wordt weergegeven:



Schakel het selectievakje in dat overeenkomt met een categorie die u wilt blokkeren. De gebruiker zal niet langer de toegang krijgen tot de websites die overeenkomen met die categorie. Om uw selectie te vergemakkelijken, worden de categorieën met webinhoud weergegeven volgens de leeftijdsgroep waarvoor ze als geschikt worden beschouwd.

- **Categorieën kinderprofielen** bevat inhoud waarvoor kinderen die jonger zijn dan 14 jaar, toegang hebben.

Categorie	Beschrijving
Games	Websites die browsergames, gamediscussieforums, gamedownloads, cheats, walkthroughs, enz. bevatten.
Video/foto	Websites waarop video- of fotogalerieën worden bewaard.
IM	Instant messaging-toepassingen.
Zoekmachines	Zoekmachines en zoekportalen.
Regionaal TLD	Websites die een domeinnaam buiten uw regio hebben.
News	Online kranten.

- **Categorieën tienerprofielen** bevat inhoud die als veilig kan worden beschouwd voor tieners tussen 14 en 18 jaar.

Categorie	Beschrijving
Web Proxy-blokkering	Websites die worden gebruikt om de URL van een gevraagde website te verbergen.
Tabloids	Online tijdschriften.
Gambling	Online casino's, websites met kansspelen, website die tips voor kansspelen bieden, gokforums, enz.
Online shopping	Online winkels.
Sociale netwerken	Websites van sociale netwerken

- **Categorieën volwassenenprofielen** bevat inhoud die ongeschikt is voor kinderen en tieners.

Categorie	Beschrijving
Pornografie	Website met pornografische inhoud.

Categorie	Beschrijving
Haat/Geweld/Racisme/Drugs	Websites met gewelddadige of racistische inhoud, die promotie maakt voor terrorisme of het gebruik van verdovende middelen.
Geneesmiddelen/alcohol/sigaren	Websites die drugs, alcohol of tabaksproducten verkopen of adverteren
Illegale activiteiten	Websites die piraterij of ongeldige inhoud bevatten.
Online betaling	Webinhoud voor online betaling en kassasecties van online winkels. De gebruiker kan surfen op online winkels, maar aankoop pogingen worden geblokkeerd.
Online dating	Dating-websites voor volwassenen met het delen van chats, video's of foto's.

Klik op **Toepassen** om de categorieën van webinhoud die voor de gebruiker zijn geblokkeerd, op te slaan.

20.2. De activiteit van de kinderen bewaken

BitDefender helpt u bij het volgen wat uw kinderen op de computer doen, zelfs als u niet thuis bent. Er kunnen u waarschuwingen via e-mail worden verzonden wanneer de module Ouderlijk toezicht een activiteit blokkeert. Er kan ook een logboek worden opgeslagen met de geschiedenis van de bezochte websites.

Selecteer de opties die u wilt inschakelen:

- **Mij een activiteitenrapport verzenden via e-mail.** Telkens wanneer Ouderlijk toezicht van BitDefender een activiteit blokkeert, wordt een e-mailmelding verzonden.
- **Een logboek voor internetverkeer opslaan.** Registreert de websites die zijn bezocht door gebruikers waarvoor Ouderlijk toezicht is ingeschakeld.

20.2.1. Bezochte websites controleren

BitDefender registreert standaard de websites die door uw kinderen worden bezocht.

Om de logboeken weer te geven, klikt u op **Logboeken weergeven** om Geschiedenis&gebeurtenissen te openen en selecteert u **Internetlogboek**.

20.2.2. E-mailmeldingen configureren

Om e-mailmeldingen te ontvangen wanneer Ouderlijk toezicht een activiteit blokkeert, selecteert u **Mij een activiteitenrapport verzenden via e-mail** in het algemene configuratievenster van Ouderlijk toezicht. U wordt gevraagd de

instellingen van uw e-mailaccount te configureren. Klik op **Ja** om het configuratievenster te openen.



Opmerking

U kunt het configuratievenster ook later openen door op **Meldingsinstellingen** te klikken.

BitDefender - Meldingen Ouderlijk toezicht

☐ E-mailmeldingen zijn uitgeschakeld

Uitgaande SMTP-server: Poort:

E-mailadres afzender:

E-mailadres ontvanger:

☐ Mijn SMTP-server vereist verificatie

Gebruikersnaam: Wachtwoord:

Testinstellingen OK Annuleren

E-mailinstellingen

U moet de instellingen van uw e-mailaccount als volgt instellen:

- **Uitgaande SMTP-server** - typ het adres van de e-mailserver in die wordt gebruikt om e-mailberichten te verzenden.
- Als de server een andere poort dan de standaard poort 25 gebruikt, moet u het nummer in het overeenkomende veld invoeren.
- **E-mailadres afzender** - typ het adres dat u wilt weergeven in het veld **Van** van de e-mail.
- **E-mailadres ontvanger** - typ het adres waarnaar de e-mail met de rapporten moet worden verzonden.
- Als de server verificatie vereist, schakelt u het selectievakje **Mijn SMTP-server vereist verificatie** in en voert u uw gebruikersnaam en wachtwoord in de overeenkomende velden in.



Opmerking

Als u deze instellingen niet kent, opent u uw e-mailclient en controleert u de instellingen van uw e-mailaccount.

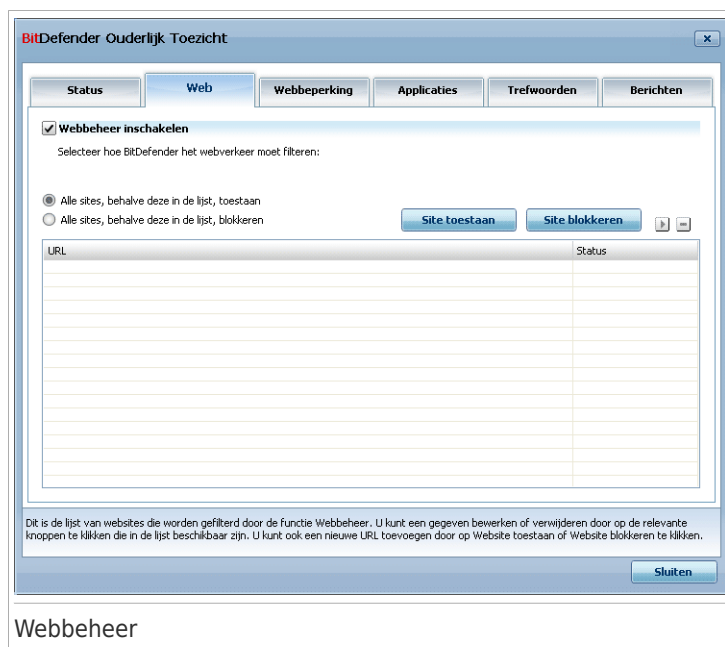
Klik op de knop **Testinstellingen** om de configuratie te valideren. Als er problemen zijn gevonden tijdens de validatie, zal BitDefender u informeren over de gebieden die uw aandacht vereisen.

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

20.3. Webbeheer

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

Om Webbeheer te configureren voor een specifieke gebruikersaccount, klikt u op de knop **Wijzigen** die overeenkomt met die gebruikersaccount en klikt u op het tabblad **Web**.

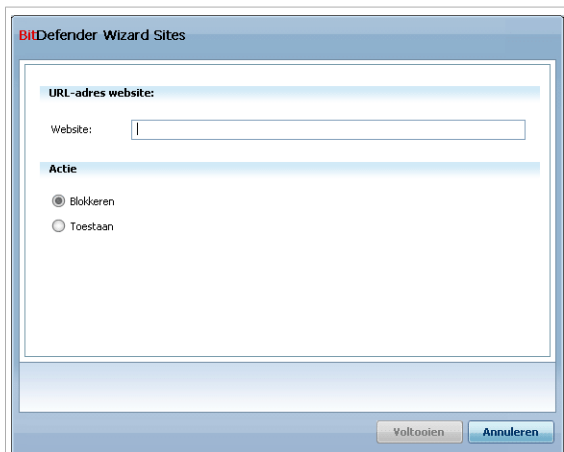


Om deze bescherming in te schakelen, schakelt u het selectievakje naast **Webbeheer inschakelen** in.

20.3.1. Regels voor webbeheer maken

Volg deze stappen om de toegang tot een website toe te staan of te blokkeren:

1. Klik op **Site toestaan** of **Site blokkeren**. Een nieuw venster wordt weergegeven:



Website opgeven

2. Voer het websiteadres in het veld **Website** in.



Syntaxis:

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

3. Selecteer de gewenste actie voor deze regel - **Toestaan** of **Blokkeren**.
4. Klik op **Voltooien** om de regel toe te voegen.

20.3.2. Regels voor webbeheer beheren

De regels voor Websitebeheer die zijn geconfigureerd, worden weergegeven in de tabel onderaan in het venster. Het websiteadres en de huidige status worden weergegeven voor elke regel van het Webbeheer.

Om een regel te bewerken, selecteert u de regel en klikt u op de knop  **Bewerken**. Breng de benodigde wijzigingen aan in het configuratievenster. Om een regel te verwijderen, selecteert u deze en klikt u op de knop  **Verwijderen**.

U moet ook selecteren welke actie Ouderlijk toezicht van BitDefender moet nemen op websites waarvoor er geen regels voor Webbeheer zijn:

- **Alle sites, behalve deze in de lijst, toestaan.** Selecteer deze optie om de toegang tot alle websites toe te staan, behalve tot sites waarvoor u de actie **Blokkeren** hebt ingesteld.
- **Alle sites, behalve deze in de lijst, blokkeren.** Selecteer deze optie om de toegang tot alle websites te blokkeren, behalve tot sites waarvoor u de actie **Toestaan** hebt ingesteld.

20.4. Webtijd- beperking

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



Opmerking

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

Om Webtijdbeperking te configureren voor een specifieke gebruiker, klikt u op de knop **Wijzigen** die overeenkomt met die gebruikersaccount en klikt u op het tabblad **Webtijdbeperking**.

BitDefender Ouderlijk Toezicht

Status Web **Webbeperking** Applicaties Trefwoorden Berichten

☒ **Webtijdbeperking inschakelen**

Klik op het raster om toegang te blokkeren tijdens het geselecteerde tijdsinterval.
Wit betekent toegestaan, grijs betekent geblokkeerd.

Dag/uur	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Zondag																								
Maandag																								
Dinsdag																								
Woensdag																								
Donderdag																								
Vrijdag																								
Zaterdag																								

☐ Tijdsinterval toegestaan ☐ Tijdsinterval geblokkeerd

Webtijd- beperking

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

Selecteer de tijdintervallen voor het blokkeren van alle internetverbindingen. U kunt op individuele cellen klikken of klikken en slepen om langere perioden te dekken. U kunt ook op **Alles blokkeren** klikken om alle cellen te selecteren en alle webtoegang onvoorwaardelijk blokkeren. Als u op **Alles toestaan** klikt, worden de internetverbindingen altijd toegestaan.



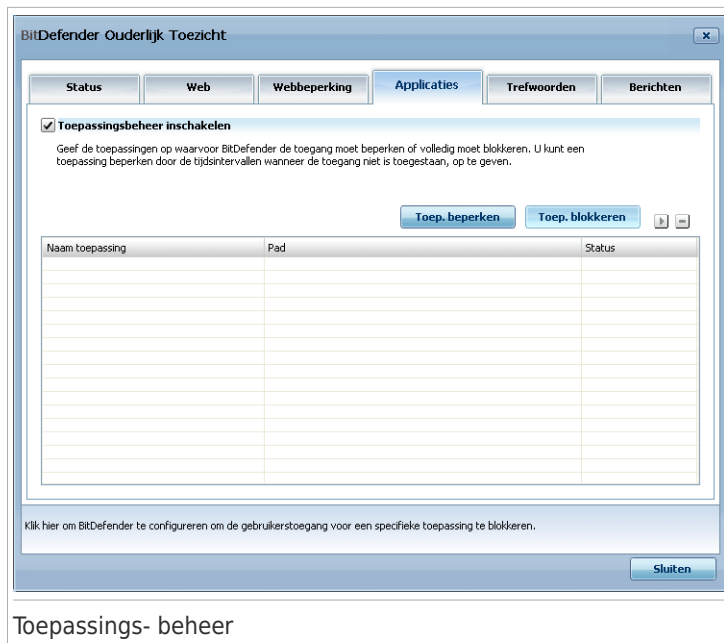
Belangrijk

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

20.5. Toepassings- beheer

Het **Toepassingsbeheer** helpt u het uitvoeren van toepassingen te blokkeren. Games, media en messaging software, maar ook andere categorieën van software en malware kunnen op deze manier worden geblokkeerd. Toepassingen die op deze manier worden geblokkeerd, worden ook beschermd tegen wijzigingen en kunnen niet worden gekopieerd of verplaatst. U kunt toepassingen permanent of alleen gedurende bepaalde tijdsintervallen blokkeren, bijvoorbeeld wanneer uw kinderen hun huiswerk zouden moeten doen.

Om Toepassingsbeheer te configureren voor een specifieke gebruikersaccount, klikt u op de knop **Wijzigen** die overeenkomt met die gebruikersaccount en klikt u op het tabblad **Toepassingen**.



Om deze bescherming in te schakelen, schakelt u het selectievakje naast **Toepassingbeheer inschakelen** in.

20.5.1. Regels voor Toepassingsbeheer maken

Volg deze stappen om de toegang tot een toepassing te blokkeren of te beperken:

1. Klik op **Toepassing blokkeren** of **Toepassing beperken**. Een nieuw venster wordt weergegeven:

BitDefender - Wizard toepassingsbeheer

Informatie toepassing

Naam toepassing:

Toepassingspad: **Bladeren...**

Actie

☒ Permanent blokkeren

☐ Blokkeren op basis van deze planning:

Dag/uur	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Zondag																								
Maandag																								
Dinsdag																								
Woensdag																								
Donderdag																								
Vrijdag																								
Zaterdag																								

Sel. opheffen **Alles sel.** ☐ Toegestaan ☒ Geblokkeerd

Voer een relevante naam in voor deze regel. De regel zal op de volgende manier in de lijst met regels worden geïdentificeerd.

Opslaan **Annuleren**

De toepassing opgeven

- Klik op **Bladeren** om de toepassing waarvoor u de toegang wilt blokkeren/beperken te zoeken.
- Selecteer de regelactie:

- **Permanent blokkeren** om de toegang tot de toepassing volledig te blokkeren.
- **Blokkeren op basis van deze planning** voor het beperken van de toegang tot bepaalde tijdsintervallen.

Als u ervoor kiest de toegang te beperken in plaats van de toepassing volledig te blokkeren, moet u ook de dagen en tijdsintervallen voor het blokkeren van de toegang selecteren in het raster. U kunt op individuele cellen klikken of klikken en slepen om langere perioden te dekken. U kunt ook op **Alles controleren** klikken om alle cellen te selecteren en, impliciet, de toepassing volledig te blokkeren. Als u op **Alle selecties opheffen** klikt, wordt de toegang altijd toegestaan.

- Klik op **Voltooiën** om de regel toe te voegen.

20.5.2. Regels voor toepassingsbeheer beheren

De regels voor Toegangsbeheer die zijn geconfigureerd, worden weergegeven in de tabel onderaan in het venster. De naam van de toepassing, het pad en de huidige status worden weergegeven voor elke regel van het Toepassingsbeheer.

Om een regel te bewerken, selecteert u de regel en klikt u op de knop  **Bewerken**. Breng de benodigde wijzigingen aan in het configuratievenster. Om een regel te verwijderen, selecteert u deze en klikt u op de knop  **Verwijderen**.

20.6. Beheer trefwoorden

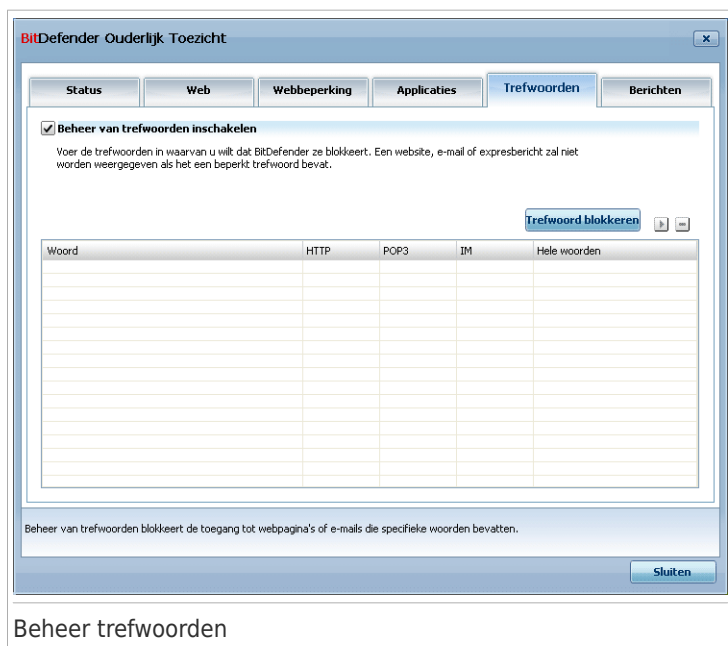
Trefwoordenbeheer helpt u bij het blokkeren van de toegang van gebruikers tot e-mailberichten, webpagina's en instant messaging die specifieke woorden bevatten. Met Trefwoordenbeheer kunt u voorkomen dat kinderen ongepaste woorden en zinnen zien wanneer ze online zijn.



Opmerking

Het trefwoordenbeheer voor instant messaging-toepassingen is alleen beschikbaar voor Yahoo Messenger en Windows Live (MSN) Messenger.

Om Trefwoordenbeheer te configureren voor een specifieke gebruikersaccount, klikt u op de knop **Wijzigen** die overeenkomt met die gebruikersaccount en klikt u op het tabblad **Trefwoorden**.



Schakel het selectievakje **Beheer van trefwoorden inschakelen** in als u deze beheerfunctie wilt gebruiken.

20.6.1. Regels voor het trefwoordenbeheer maken

Volg deze stappen om een woord of zin te blokkeren:

1. Klik op **Trefwoord blokkeren**. Een nieuw venster wordt weergegeven:



Trefwoord opgeven

2. Type het woord of de zin in die u wilt blokkeren in het bewerkingsveld. Als u wilt dat alleen volledige woorden worden gedetecteerd, schakelt u het selectievakje **Hele woorden** in.
3. Selecteer het verkeerstype waarin BitDefender moet scannen op het opgegeven woord.

Optie	Beschrijving
HTTP	Webpagina's die het trefwoord bevatten, worden geblokkeerd.
POP3	E-mailberichten die het trefwoord bevatten, worden geblokkeerd.
Instant Messaging	Instant messages die het trefwoord bevatten, worden geblokkeerd.

4. Klik op **Voltooien** om de regel toe te voegen.

20.6.2. Regels beheren voor trefwoordenbeheer

De regels voor Trefwoordenbeheer die zijn geconfigureerd, worden weergegeven in de tabel onderaan in het venster. De woorden en de huidige status voor de verschillende verkeerstypes worden weergegeven voor elke regel van het trefwoordenbeheer.

Om een regel te bewerken, selecteert u de regel en klikt u op de knop  **Bewerken**. Breng de benodigde wijzigingen aan in het configuratievenster. Om een regel te verwijderen, selecteert u deze en klikt u op de knop  **Verwijderen**.

20.7. Instant Messaging (IM) beheer

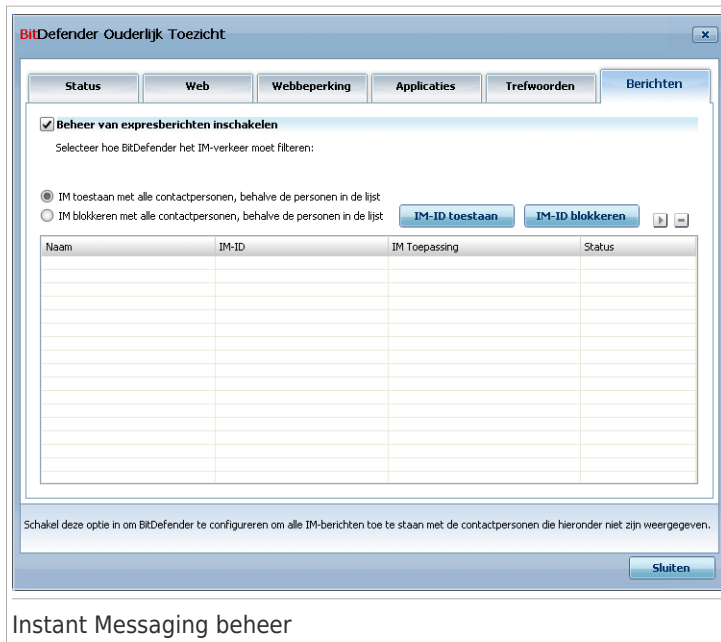
Met Instant Messaging (IM) beheer kan u de IM contacten aangeven waarmee uw kinderen mogen chatten.



Opmerking

IM beheer is alleen beschikbaar voor Yahoo Messenger en Windows Live (MSN) Messenger.

Om IM-beheer te configureren voor een specifieke gebruikersaccount, klikt u op de knop **Wijzigen** die overeenkomt met die gebruikersaccount en klikt u op het tabblad **Berichten**.



Selecteer het vakje **Instand Messaging beheer inschakelen** als u deze beveiliging wilt gebruiken.

20.7.1. Regels voor het beheer van instant messaging (IM) maken

Volg deze stappen om instant messaging met een contactpersoon toe te staan of te blokkeren:

1. Klik op **IM-ID blokkeren** of **IM-ID toestaan**. Een nieuw venster wordt weergegeven:

BitDefender Wizard Instant Messaging

IM-contactgegevens

Naam:

E-mail of IM-ID:

IM-toepassing:

Actie

☐ Blokkeren

☒ Toestaan

Contactpersonen toevoegen aan de lijst van gecontroleerde IM-contactpersonen om expresberichten die naar hen zijn verzonden/van hen zijn ontvangen te blokkeren of toe te staan.

IM contact toevoegen

2. Voer de naam van de contactpersoon in het veld **Naam** in.
3. Voer het e-mailadres of de gebruikersnaam die door de IM-contactpersoon wordt gebruikt in het veld **E-mail of IM-ID** in.
4. Kies het IM programma dat het contact gebruikt.
5. Selecteer de actie voor deze regel - **Blokkeren** of **Toestaan**
6. Klik op **Voltooien** om de regel toe te voegen.

20.7.2. Regels voor het beheer van instant messaging (IM) beheren

De regels voor IM-beheer die zijn geconfigureerd, worden weergegeven in de tabel onderaan in het venster. De naam, de IM-ID, de IM-toepassing en de huidige status worden weergegeven voor elke regel van het IM-beheer.

Om een regel te bewerken, selecteert u de regel en klikt u op de knop  **Bewerken**. Breng de benodigde wijzigingen aan in het configuratievenster. Om een regel te verwijderen, selecteert u deze en klikt u op de knop  **Verwijderen**.

U moet ook kiezen welke actie BitDefender Ouderlijk toezicht moet ondernemen op IM-contactpersonen waarvoor geen regels zijn gemaakt. Selecteer **Blokkeren** of **IM toestaan met alle contactpersonen, behalve de personen in de lijst**.

21. 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.

21.1. 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.



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**.

21.1.1. 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.

21.2. 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.

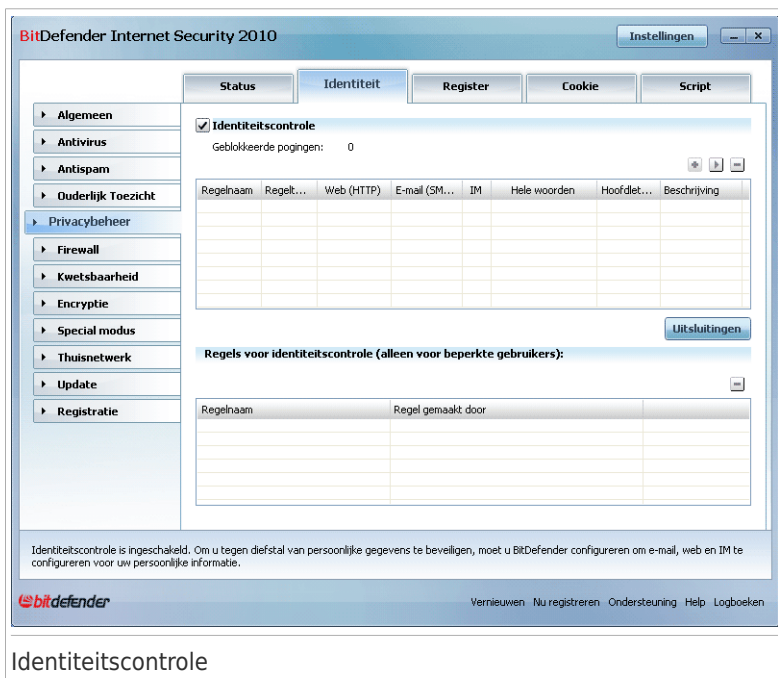
In het geval dat zo'n applicatie erin slaagt om door de antivirusdetectie te glijpen, kan het de gestolen data niet verzenden via e-mail, web of instant messages als u de juiste identiteitscontrole-regels hebt gecreëerd.

- 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.



Volg deze stappen als u Identiteitscontrole wilt gebruiken:

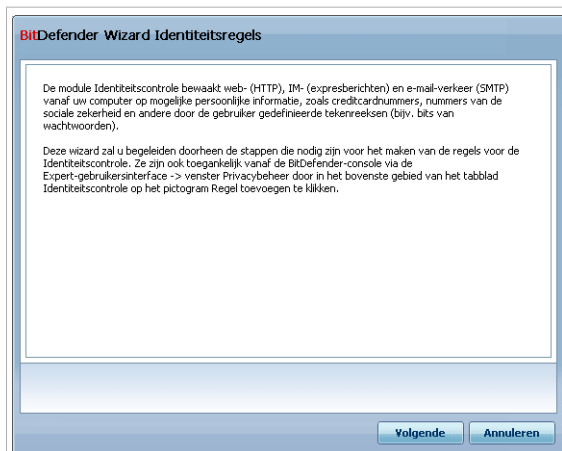
1. Schakel het selectievakje **Identiteitscontrole inschakelen** in.
2. Creëer regels om uw gevoelige data te beschermen. Meer informatie vindt u onder *"Privacyregels maken"* (p. 214).
3. Definieer, indien nodig, specifieke uitsluitingen van de regels die u hebt gemaakt. Meer informatie vindt u onder *"Uitsluitingen definiëren"* (p. 218).
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. 219).

21.2.1. Privacyregels maken

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

Stap 1/4 - Welkomstvenster



Welkomstvenster

Klik op **Volgende**.

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



Type en gegevens van de regel instellen

U moet de volgende parameters instellen:

- **Regelnaam** - voer de naam van de regel in dit bewerkingsveld in.
- **Regeltype** - kies het type regel (adres, naam, creditcard, PIN, BSN, enz.).
- **Regeldata** - voer de te beveiligen data in dit bewerkingsveld in. Bijvoorbeeld, als u uw creditcardnummer 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

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

BitDefender Wizard Identiteitsregels

Regelbeschrijving

I

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.

Voer hier de beschrijving van de regel in. De wizard zal u niet toestaan hier de gegevens die u wilt beveiligen, in te voeren.

Vorige Voltooien Annuleren

Regel beschrijven

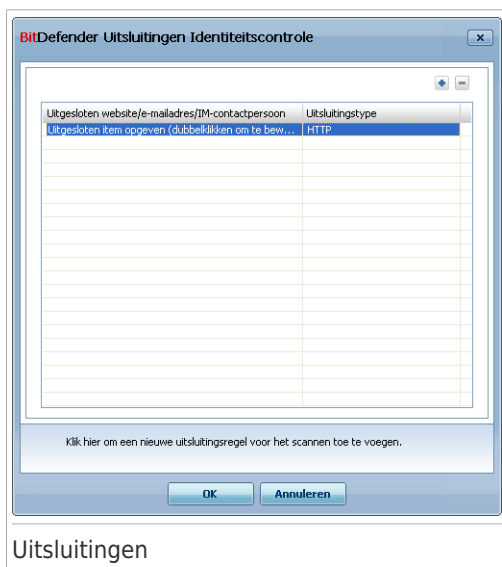
Voer een korte beschrijving in van de regel in het bewerkingsveld. Omdat de geblokkeerde data (tekenreeks) niet in normale tekst zichtbaar is als u de regel opent, kan u deze met de beschrijving beter herkennen.

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

21.2.2. 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**.

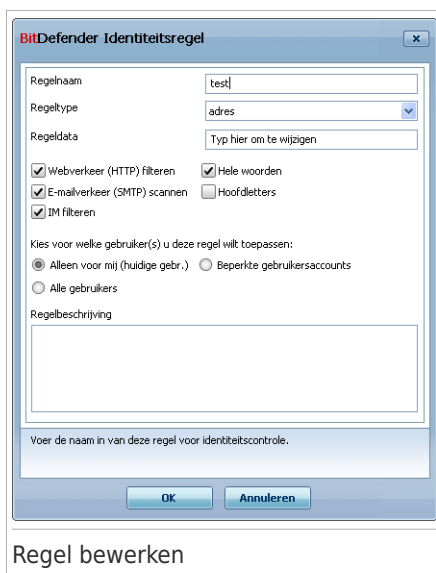
Klik op **OK** om de wijzigingen op te slaan.

21.2.3. 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 the 'BitDefender Identiteitsregel' (Identity Rule) dialog box. It has a title bar with the BitDefender logo and a close button. The dialog contains several fields and checkboxes:


- Regelnaam** (Rule name): A text box containing 'test'.
- Regeltype** (Rule type): A dropdown menu showing 'adres'.
- Regeldata** (Rule data): A text box with the placeholder 'Typ hier om te wijzigen' (Type here to change).
- Filters**: A group of checkboxes:
 - ☒ Webverkeer (HTTP) filteren
 - ☒ E-mailverkeer (SMTP) scannen
 - ☒ IM filteren
 - ☒ Hele woorden
 - ☐ Hoofdletters
- Kies voor welke gebruiker(s) u deze regel wilt toepassen:** (Choose for which user(s) you want to apply this rule):
 - ☒ Alleen voor mij (huidige gebr.)
 - ☐ Beperkte gebruikersaccounts
 - ☐ Alle gebruikers
- Regelbeschrijving** (Rule description): A large empty text area.
- Footer**: A light blue bar with the text 'Voer de naam in van deze regel voor identiteitscontrole.' (Enter the name of this rule for identity control.) and two buttons: 'OK' and 'Annuleren'.

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.

21.2.4. 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**.

21.3. Registerbeheer

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

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

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



Registerwaarschuwing

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

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.

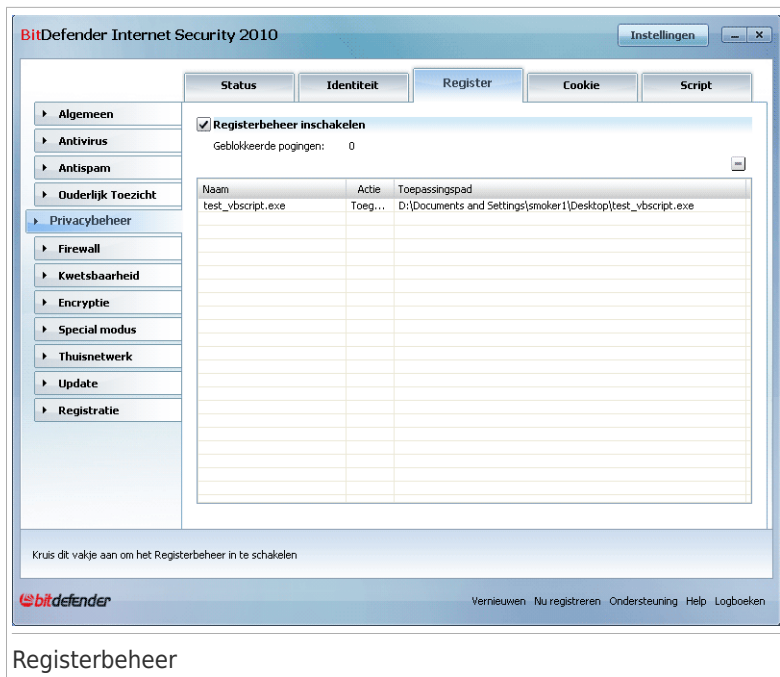
Afhankelijk van uw antwoord, wordt een regels gemaakt en weergegeven in de tabel met regels. Dezelfde actie wordt telkens toegepast wanneer dit programma een registergegeven probeert te wijzigen.



Opmerking

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

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



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**.

21.4. 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.

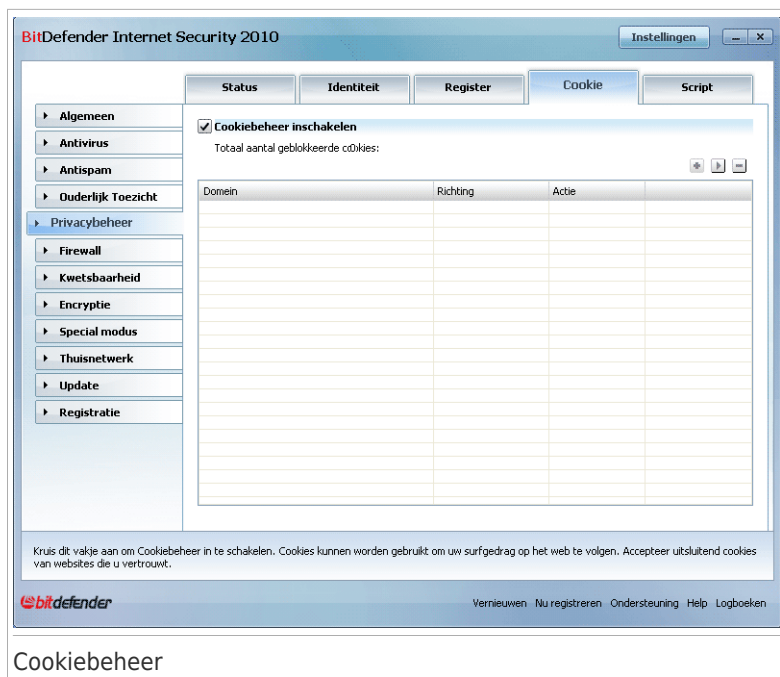
Dit helpt bij het kiezen van de websites die u wel of niet vertrouwt.



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.



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



Belangrijk

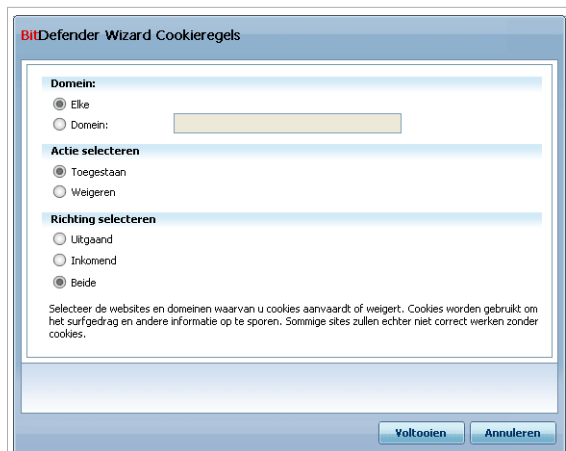
De regels worden vanaf boven weergegeven in volgorde van prioriteit, wat betekent dat de eerste regel de hoogste prioriteit heeft. U kunt de regels slepen & neerzetten om hun prioriteit te wijzigen.

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.

21.4.1. Configuratievenster

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



Adres, actie en richting selecteren

U kunt de volgende parameters instellen:

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

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

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

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



Opmerking

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

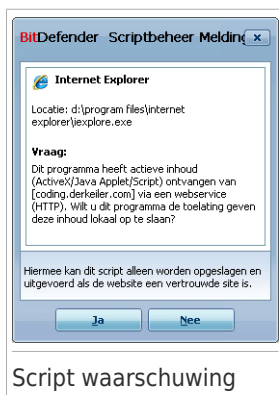
Klik op **Voltooien**.

21.5. 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.

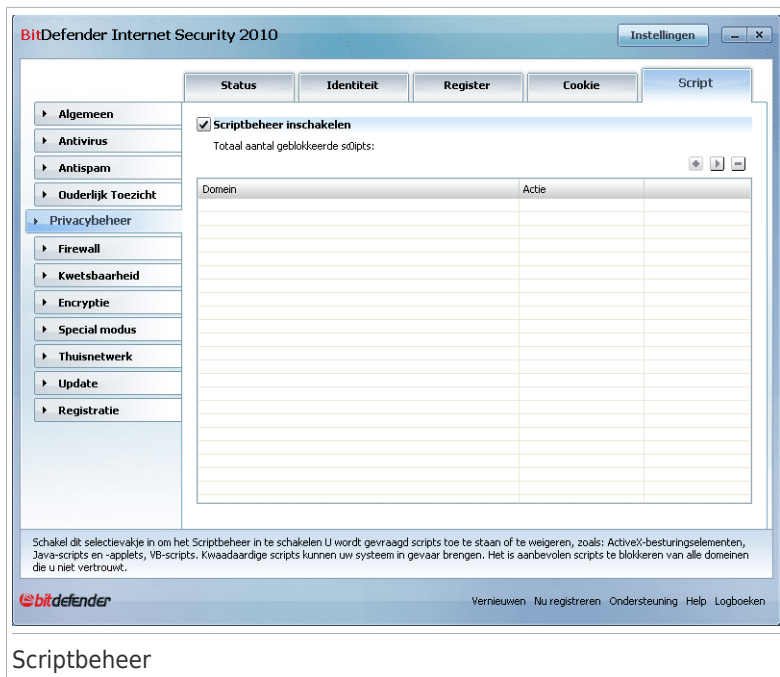
Met het **Scriptbeheer** bepaalt u zelf welke websites u vertrouwt en welke niet. BitDefender zal telkens uw toestemming vragen wanneer een website een script of andere actieve inhoud probeert te activeren.



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.






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.

21.5.1. Configuratievenster

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

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**.

22. Firewall

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



Opmerking

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

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

22.1. Instellingen

Om de firewallbeveiliging te configureren, gaat u naar **Firewall>Instellingen** in de Expert-modus.

BitDefender Internet Security 2010

Instellingen

Instellingen Thuisnetwerk Regels Activiteit

Algemeen
Antivirus
Antispam
Ouderlijk Toezicht
Privacybeheer
Firewall
Kwetsbaarheid
Encryptie
Special modus
Thuisnetwerk
Update
Registratie

☒ Firewall is ingeschakeld

Computernaam: SMOKE1
Computer-IPs: 10.10.15.62/16
Gateways: 10.10.0.1

Verzonden bytes: 500,2 KB (0,0 B/s)
Verzonden bytes: 23,9 MB (6,5 KB/s)
Poortscan gedetecteerd: 0
Ontvangen pakketten: 1794
Geopende poorten: 16
Binnenkomende verbindings: 0
Uitgaande verbindings: 1

Standaard actie:

☐ Alles toestaan (Spelmodus)
☒ Bekende programma's toestaan
☐ Rapport
☐ Alles weigeren

Geavanceerd
Witte lijst

Inkomend: 6.47K
Uitgaand: 0B

Firewall beschermt uw computer tegen pogingen door onbevoegden om ingaande en uitgaande verbindings tot stand te brengen. Ook beschermt hij tegen hackers en kwaadwillende aanvallen van buitenaf.

bitdefender

Vernieuwen Nu registreren Ondersteuning Help Logboeken

Firewall instellingen

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



Belangrijk

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

Er zijn twee categorieën van informatie:

- **Netwerkconfiguratie overzicht.** U ziet de naam van uw computer, het IP-adres ervan en de standaard gateway. Als u meer dan één netwerkadapter heeft (dat wil zeggen dat u verbonden bent met meer dan één netwerk), ziet u het IP-adres en de gateway die zijn geconfigureerd voor elke netwerkadapter.
- **Statistieken.** U kan verschillende statistieken met betrekking tot de firewall activiteiten zien.
 - ▶ aantal verzonden bytes.
 - ▶ aantal ontvangen bytes.
 - ▶ aantal door BitDefender gedetecteerde en geblokkeerde poortscans. Poortscans worden vaak door hackers gebruikt om geopende poorten op uw computer te vinden, met de bedoeling deze te misbruiken.
 - ▶ aantal ontvangen pakketten.
 - ▶ aantal open poorten.
 - ▶ aantal actieve binnenkomende verbindingen.
 - ▶ aantal actieve uitgaande verbindingen.

Om de actieve verbindingen en open poorten te zien, gaat u naar het tabblad **Activiteit**.

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



Opmerking

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

22.1.1. De standaard actie instellen

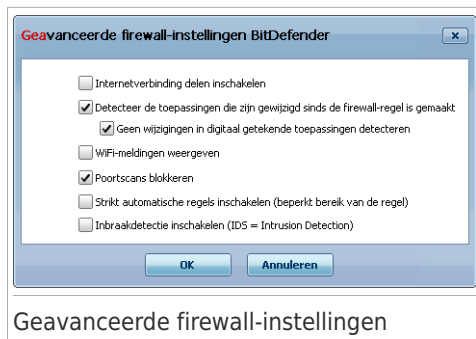
Standaard geeft BitDefender automatisch alle bekende programma's van de witte lijst toegang tot netwerkservices en het internet. Voor alle andere programma's vraagt BitDefender via een waarschuwingsvenster welke actie moet worden genomen. De actie die u aangeeft wordt elke keer toegepast wanneer het betreffende programma netwerk/internet toegang vraagt.

Sleep de schuifregelaar langs de schaal om de standaardactie in te stellen die wordt toegepast wanneer het betreffende programma netwerk/internet toegang vraagt. De volgende standaardacties zijn beschikbaar:

Standaardacties	Beschrijving
Alles toestaan	Past de huidige regels toe en staat alle verkeerspogingen toe die niet overeenkomen met een van de huidige regels, zonder u te waarschuwen. Dit beleid wordt sterk afgeraden, maar kan handig zijn voor netwerkbeheerders en gamers.
Bekende programma's toestaan	<p>Past de huidige regels toe en laat alle uitgaande verbindingspogingen van programma's die bij BitDefender bekend zijn als rechtmatig (witte lijst), zonder u te waarschuwen. Voor de rest van de verbindingspogingen, zal BitDefender u vragen om uw toestemming.</p> <p>Programma's op de witte lijst zijn de meest gebruikte toepassingen in de hele wereld. Zij omvatten de meeste bekende webbrowsers, audio- en videospelers, chatprogramma's en programma's voor het delen van bestanden, evenals serverclients en besturingssystemen. Klik op Witte lijst weergeven om de volledige witte lijst weer te geven.</p>
Rapport	Past de huidige regels toe en raadpleegt u bij alle verkeerspogingen die niet overeenkomen met een van de huidige regels.
Alles weigeren	Past de huidige regels toe en verbiedt alle verkeerspogingen die niet overeenkomen met een van de huidige regels.

22.1.2. Geavanceerde firewall-instellingen configureren

U kunt op **Geavanceerde instellingen** klikken om de geavanceerde firewall-instellingen te configureren.



De volgende opties zijn beschikbaar:

- **ICS-ondersteuning (Internet Connection Sharing) inschakelen** - schakelt de ondersteuning in voor ICS (Internet Connection Sharing).



Opmerking

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

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

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

- **Toepassingen detecteren die sinds het maken van de firewall-regels zijn gewijzigd** - controleert elke toepassing die probeert een verbinding te maken met internet om te zien of deze werd gewijzigd sinds de regel die de toegang van deze toepassing bepaalt, werd toegevoegd. Als de toepassing werd gewijzigd, wordt een waarschuwing weergegeven met de vraag of u de toegang tot het internet wilt toestaan of blokkeren voor de toepassing.

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



Opmerking

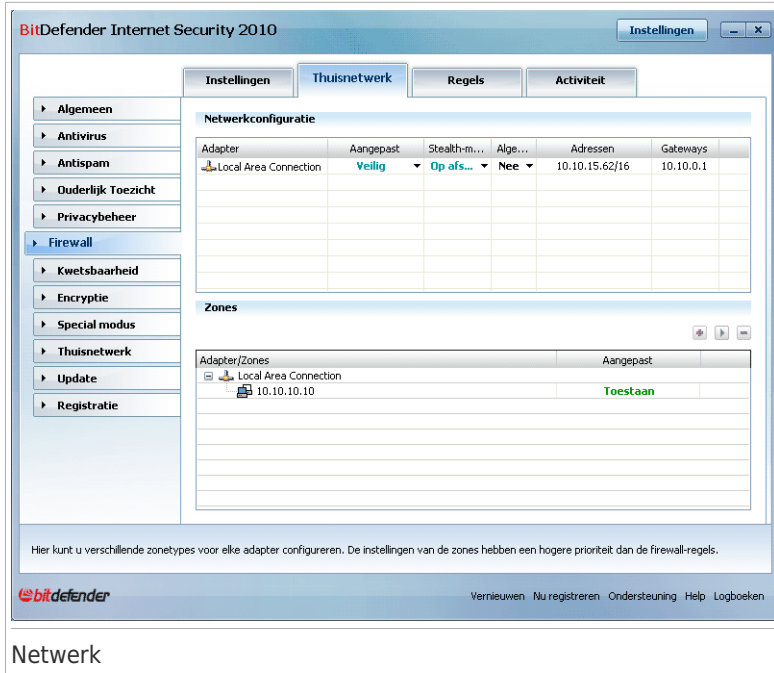
Wij raden u aan deze optie geselecteerd te houden en de toegang alleen toe te staan voor de toepassingen waarvan u verwacht dat ze zijn gewijzigd, nadat de regel die hun toegang beheert, werd gemaakt.

Getekende toepassingen worden verondersteld vertrouwd te zijn en hebben een hogere beveiligingsgraad. U kunt **Geen wijzigingen detecteren in digitaal ondertekende toepassingen** inschakelen om gewijzigde getekende toepassingen toe te staan een verbinding te maken met het internet zonder dat u een waarschuwing over deze gebeurtenis ontvangt.

- **WiFi-meldingen weergeven** - als u verbonden bent met een draadloos netwerk, worden informatievensters weergegeven met betrekking tot specifieke netwerkgebeurtenissen (bijvoorbeeld, wanneer een nieuwe computer bij het netwerk is gekomen).
- **Poort scans blokkeren** - detecteert en blokkeert pogingen om uit te vinden welke poorten open zijn.
Poortscans worden vaak door hackers gebruikt om geopende poorten op uw computer te vinden. Als zij een minder veilige of kwetsbare poort vinden kunnen zij inbreken in uw computer.
- **Strikte automatische regels inschakelen** - maakt strikte regels via het venster met de firewall-waarschuwing. Als deze optie is geselecteerd, vraagt BitDefender u om actie en creëert het regels voor elk verschillend proces dat de applicatie opent met het verzoek van netwerk- of internettoegang.
- **Inbraakdetectie inschakelen (IDS = Intrusion Detection)** - activeert de heuristische bewaking van de toepassingen die proberen toegang te krijgen tot de netwerkservices of internet.

22.2. Netwerk

Om de firewallinstellingen te configureren, gaat u naar **Firewall>Netwerk** in de Expert-modus.



Netwerk

In de kolommen in de **Netwerkconfiguratie** tabel staat gedetailleerde informatie over het netwerk waarmee u bent verbonden:

- **Adapter** - de netwerkadapter die uw computer gebruikt om een verbinding te maken met het netwerk of het internet.
- **Vertrouwheidsniveau** - het niveau van vertrouwen dat is toegewezen aan de netwerkadapter. Afhankelijk van de configuratie van de netwerkadapter, zal BitDefender het vertrouwheidsniveau van de adapter automatisch toewijzen, of u om meer informatie vragen.
- **Stealth-modus** - hiermee kunt u instellen of u door andere computers kunt worden gedetecteerd.
- **Generiek profiel** - hiermee kunt u instellen of er generieke regels moeten worden toegepast op deze verbinding.
- **Adres** - het IP-adres van de adapter.
- **Gateway** - het IP-adres dat uw computer gebruikt voor de verbinding met het internet.

22.2.1. Het vertrouwdeheidsniveau veranderen

BitDefender wijst aan elke netwerkadapter een vertrouwdeheidsniveau toe. Het aan de adapter toegewezen vertrouwdeheidsniveau geeft aan hoe betrouwbaar het betreffende netwerk is

Op basis van het vertrouwdeheidsniveau, worden regels gecreëerd voor de adapter met betrekking op de manier waarop het systeem en BitDefender processen naar het netwerk en het internet gaan.

U ziet het vertrouwdeheidsniveau dat geconfigureerd is voor elke adapter in de tabel **Netwerkconfiguratie** in de kolom **Vertrouwdeheidsniveau**. Om het vertrouwdeheidsniveau te wijzigen, klikt u op de pijl in de kolom **Vertrouwdeheidsniveau** en selecteert u het gewenste niveau.

Vertrouwdeheidsniveau	Beschrijving
Volledig vertrouwen	De firewall voor de betreffende adapter uitschakelen.
Lokaal vertrouwd	Alle verkeer tussen uw computer en computers in het netwerk toestaan.
Veilig	Bronnen delen met computers in het lokale netwerk toestaan. Dit niveau is automatisch ingesteld voor lokale (thuis of kantoor) netwerken.
Onveilig	Netwerk of internet computers verbieden verbinding te maken met uw computer. Dit niveau is automatisch ingesteld voor openbare netwerken (als u een IP-adres hebt gekregen van een Internet Service Provider).
Lokaal geblokkeerd	Alle verkeer tussen uw computer en computers in het lokale netwerk blokkeren, tijdens het verzorgen van toegang tot het internet. Dit vertrouwdeheidsniveau is automatisch ingesteld voor onveilige (open) draadloze netwerken.
Geblokkeerd	Netwerk- en internetverkeer door de betreffende adapter compleet blokkeren.

22.2.2. De stealth-modus configureren

De stealth-modus maakt uw computer onzichtbaar voor kwaadaardige software en hackers in het netwerk of het internet. Om de stealth-modus te configureren, klikt u op de pijl ▼ van de kolom **Stealth** en selecteert u de gewenste optie.

Stealth-optie	Beschrijving
Klik op Aan .	Stealth-modus is aan. Uw computer is niet zichtbaar in zowel het lokale netwerk als het internet.
Uit	Stealth-modus is uit. Iemand op het lokale netwerk of het internet kan pingen en uw computer detecteren.
Ver	Uw computer kan niet gedetecteerd worden vanaf het internet. Lokale netwerk gebruikers kunnen pingen en uw computer detecteren.

22.2.3. Algemene instellingen configureren

Als het IP-adres van een netwerkadapter wordt veranderd, verandert BitDefender het vertrouwdeheidsniveau overeenkomstig. Als u hetzelfde vertrouwdeheidsniveau wilt behouden, klikt u op de pijl ▼ van de kolom **Algemeen** en selecteert u **Ja**.

22.2.4. Netwerkzones

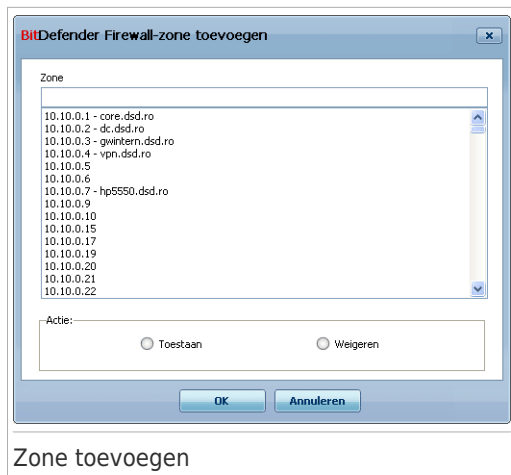
U kan toegelaten of geblokkeerde computers toevoegen voor een specifieke adapter.

Een vertrouwde zone is een computer die u volledig vertrouwt. Al het verkeer tussen uw computer en een vertrouwde computer is toegestaan. Om bronnen te delen met specifieke computers in een onbeveiligd draadloos netwerk, voegt u ze toe als toegestane computers.

Een geblokkeerde zone is een computer die u in het geheel niet met uw computer wilt laten communiceren.

De tabel **Zones** toont de huidige netwerkzones per adapter.

Om een zone toe te voegen, klikt u op de knop  **Toevoegen**.

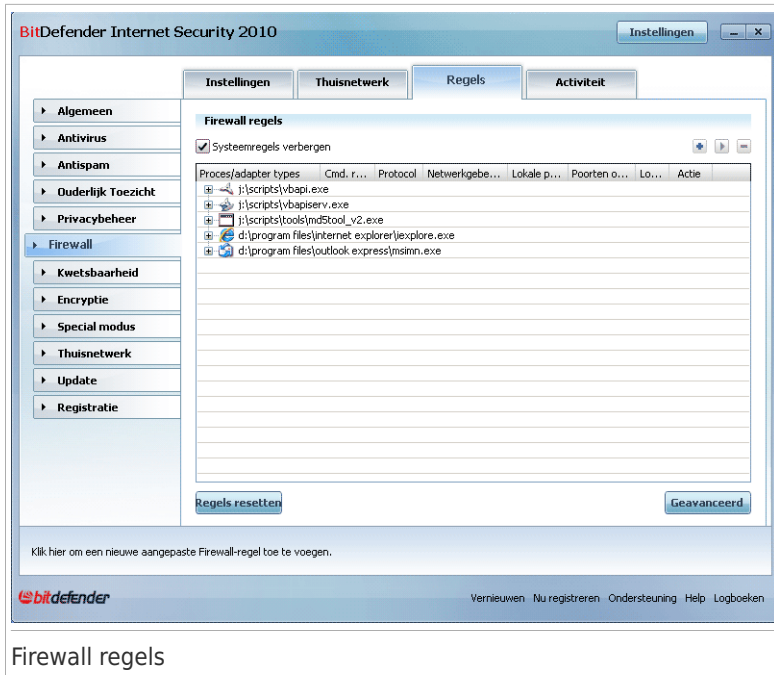


Ga als volgt te werk:

1. Het IP-adres van de toe te voegen computer selecteren.
2. De actie selecteren:
 - **Toestaanscannen** - om alle verkeer tussen uw computer en de geselecteerde computer toe te staan.
 - **Verbieden** - om alle verkeer tussen uw computer en de geselecteerde computer te blokkeren.
3. Klik op **OK**.

22.3. Regels

Ga naar **Firewall>Regels** in de Expert-modus voor het beheren van de firewallregels die de toegang van toepassingen tot netwerkbronnen en internet controleren.



Firewall regels

U ziet de applicaties (processen) waarvoor firewall regels zijn gemaakt. Schakel het selectievakje **Systeemregels verbergen** uit als u ook de regels met betrekking tot de systeem- of de BitDefenderprocessen wilt zien.

Om de regels voor een specifieke applicatie te zien, klikt u op het vakje + naast de betreffende applicatie. U ziet gedetailleerde informatie over elke regel, zoals aangegeven door de tabelkolommen:

- **Process/Adapter Types** - de proces- en netwerkadaptertypes waarvoor de regel geldt. Regels zijn automatisch gecreëerd voor het filteren van netwerk- of internettoegang via elke adapter. U kan handmatig regels creëren of bewerken voor het filteren van de netwerk- of internettoegang van een applicatie via een specifieke adapter (bijvoorbeeld een draadloze netwerkadapter)
- **Commandoregel** - het commando dat wordt gebruikt voor het starten van het process in de Windows commandoregel interface (**cmd**).
- **Protocol** - het IP-protocol waarvoor de regel geldt. U kan een van de volgende dingen zien:

Protocol	Beschrijving
Alle	Omvat alle IP-protocollen.
TCP	Transmission Control Protocol - TCP activeert twee hosts om een verbinding tot stand te brengen en gegevensstromen uit te wisselen. TCP garandeert het afleveren van gegevens en verzekert eveneens dat de pakketten worden afgeleverd in dezelfde volgorde waarin ze worden verzonden.
UDP	User Datagram Protocol - UDP is een transport gebaseerd op IP en ontwikkeld voor hoge prestaties. Games en andere op video gebaseerde toepassingen gebruiken vaak UDP.
Een getal	Geeft een specifiek IP-protocol aan (ander dan TCP en UDP). U vindt de complete lijst van toegewezen IP-protocolnummers op www.iana.org/assignments/protocol-numbers .

- **Netwerkgebeurtenissen** - de netwerkgebeurtenissen waarvoor de regel geldt. De volgende gebeurtenissen kunnen verwerkt worden:

Gebeurtenis	Beschrijving
Verbinden	Voor-uitwisseling van standaardberichten die worden gebruikt door verbinding-georiënteerde protocollen (zoals TCP) om een verbinding tot stand te brengen. Met connectie-georiënteerde protocollen, vindt dataverkeer tussen twee computers alleen plaats nadat een verbinding tot stand is gebracht.
Verkeer	Datastroom tussen twee computers.
Luisteren	Staat waarin een applicatie het netwerk bewaakt in afwachting van het tot stand brengen van een verbinding of voor het ontvangen van informatie van en peer applicatie.

- **Lokale poorten** - de poorten op uw computer waarvoor de regel geldt.
- **Verre poorten** - de poorten op de verre computer waarvoor de regel geldt.
- of **Lokaal** - of de regel alleen geldt voor computers in het lokale netwerk.
- **Actie** - of de toepassing wel of niet netwerk- of internettoegang krijgt onder de opgegeven omstandigheden.

22.3.1. Regels automatisch toevoegen

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



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

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

Op basis van uw antwoord wordt een regel gemaakt, toegepast en weergegeven in de tabel.

Wanneer de toepassing de volgende keer probeert een verbinding te maken, wordt deze regels standaard toegepast.



Belangrijk

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

22.3.2. Regels verwijderen en opnieuw instellen

Om een regel te verwijderen, selecteert u deze en klikt u op de knop **Regel verwijderen**. U kan een of meer regels tegelijk selecteren en verwijderen.

Om een alle regels voor een specifieke applicatie te verwijderen, selecteert u de applicatie in de lijst en klikt u op de knop **Regel verwijderen**.

Als u de standaard regelset voor het geselecteerde vertrouwdsniveau wilt laden, klikt u op **Regels resetten**.

22.3.3. Regels maken en wijzigen

Het handmatig creëren van nieuwe regels en het wijzigen van bestaande regels, gebeurt door het configureren van de regelparameters in het configuratievenster.

Regels maken. Volg deze stappen om gegevens handmatig een regel te creëren:

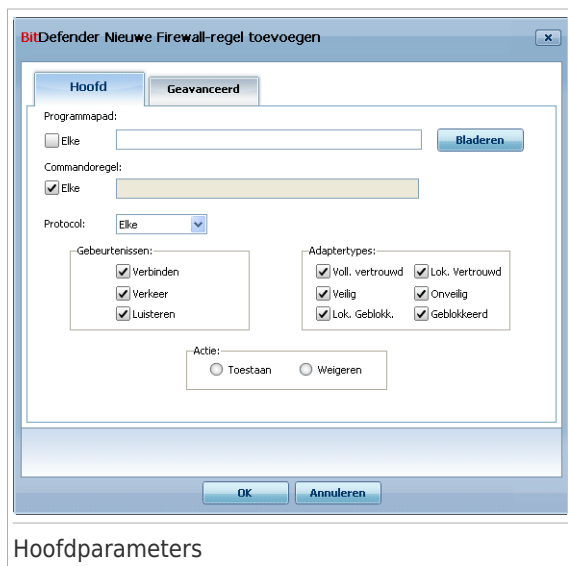
1. Klik op de knop **Regel toevoegen**. Het configuratievenster wordt weergegeven.
2. Configureer de hoofd- en de geavanceerde parameters zoals nodig is.
3. Klik op **OK** om de nieuwe regel toe te voegen.

Regels wijzigen. Volg deze stappen om een bestaande regel te wijzigen:

1. Klik op de knop ► **Regel bewerken** of dubbelklik op de regel. Het configuratievenster wordt weergegeven.
2. Configureer de hoofd- en de geavanceerde parameters zoals nodig is.
3. Klik op **OK** om de wijzigingen op te slaan.

Hoofdparameters configureren

Met het tabblad **Hoofd** van het configuratievenster kan u de hoofdparameters van de regel configureren.



Hoofdparameters

U kan de volgende parameters configureren:

- **Programmapad.** Klik op **Bladeren** en selecteer de applicatie waarvoor de regel geldt. Klik op **Alle** als u de regel voor alle applicaties wilt laten gelden.
- **Opdrachtregel.** Als u de regel alleen wilt laten gelden als de geselecteerde applicatie is geopend met een specifiek commando in de Windows commandoregel interface, schakel het selectievakje **Alle** uit en typ het betreffende commando in het bewerkingsveld.
- **Protocol.** Selecteer in het menu het IP-protocol waarvoor de regel geldt.
 - Als u een regel voor alle protocollen wilt laten gelden, schakelt u het selectievakje **Alle** in.
 - Als u wilt dat de regel van toepassing is op TCP, selecteert u **TCP**.

- ▶ Als u wilt dat de regel van toepassing is op UDP, selecteert u **UDP**.
- ▶ Als u een regel voor specifiek protocol wilt laten gelden, schakelt u het selectievakje **Andere** in. Een bewerkingsveld verschijnt. Typ het nummer dat is toegewezen aan het protocol dat u wilt filteren in het bewerkingsveld.



Opmerking

IP-protocolnummers worden toegewezen door de Internet Assigned Numbers Authority (IANA). U vindt de complete lijst van toegewezen IP-protocolnummers op www.iana.org/assignments/protocol-numbers.

- **Gebeurtenissen.** Afhankelijk van het geselecteerde protocol, selecteert u de netwerkgebeurtenissen waarop de regel geldt. De volgende gebeurtenissen kunnen verwerkt worden:

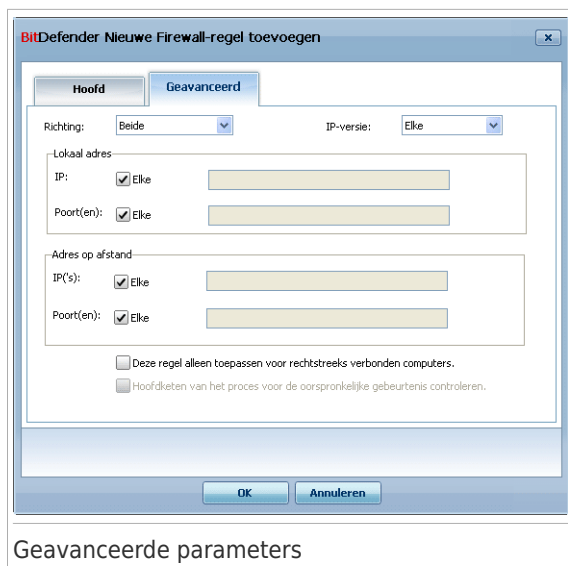
Gebeurtenis	Beschrijving
Verbinden	Voor-uitwisseling van standaardberichten die worden gebruikt door verbinding-georiënteerde protocollen (zoals TCP) om een verbinding tot stand te brengen. Met connectie-georiënteerde protocollen, vindt dataverkeer tussen twee computers alleen plaats nadat een verbinding tot stand is gebracht.
Verkeer	Datastroom tussen twee computers.
Luisteren	Staat waarin een applicatie het netwerk bewaakt in afwachting van het tot stand brengen van een verbinding of voor het ontvangen van informatie van een peer applicatie.

- **Adaptertypes.** Selecteer de adaptertypes waarvoor de regel geldt.
- **Actie.** Selecteer een van de beschikbare acties:

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

Geavanceerde parameters configureren

Met het tabblad **Geavanceerd** van het configuratievenster kan u de geavanceerde parameters van de regel configureren.



Geavanceerde parameters

U kan de volgende geavanceerde parameters configureren:

- **Richting.** Selecteer in het menu de verkeersrichting waarvoor de regel geldt.

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

- **IP-versie.** Selecteer in het menu de IP-versie (IPv4, IPv6 of alle) waarvoor de regel geldt.
- **Lokaal adres.** Geef het lokale IP-adres en poort waarvoor de regel geldt als volgt op:
 - ▶ Als u meer dan een netwerkadapter hebt, schakelt u het selectievakje **Alle** uit en typt u een specifiek IP-adres.
 - ▶ Als u TCP of UDP hebt geselecteerd als protocol, kunt u een specifieke poort of een bereik tussen 0 en 65535 instellen. Als u wilt dat de regel van toepassing is op alle poorten, selecteert u **Alle**.

- **Adres op afstand.** Geef het verre IP-adres en poort waarvoor de regel geldt, als volgt op:
 - ▶ Om het verkeer te filteren tussen uw computer en een specifieke computer, schakelt u het selectievakje **Alle** uit en typt u u het IP-adres.
 - ▶ Als u TCP of UDP hebt geselecteerd als protocol, kunt u een specifieke poort of een bereik tussen 0 en 65535 instellen. Als u wilt dat de regel van toepassing is op alle poorten, selecteert u **Alle**.
- **Deze regel alleen toepassen op rechtstreeks verbonden computers.** Selecteer deze optie als u de regel alleen wilt laten gelden op lokaal verkeer.
- **Process parent chain voor de oorspronkelijke gebeurtenis controleren.** U kan deze parameter alleen wijzigen al u **Strikt automatische regels** hebt geselecteerd (ga naar het tabblad **Instellingen** en klik op **Geavanceerde instellingen**). Strikte regels betekent dat BitDefender u om actie vraagt wanneer een applicatie netwerk-/internettoegang vraagt telkens als het parent process verschillend is.

22.3.4. Geavanceerd regelbeheer

Als u geavanceerd beheer over de firewall-regels nodig hebt, klikt u op **Geavanceerd**. Een nieuw venster wordt weergegeven.

BitDefender Geavanceerde firewall-regels bewerken

Filtreren op: **Eke adapter**

Index	Toepassing	Cmd. regel	Ouders...	Adapter	Protocol	Lokaal adres	Adres op afstand	IP-versie	Lokaal	Richting	Netwerkgebe...	Actie
1	svchost.exe	Eke	Nee	Eke adapter	UDP	Eke IP : DHCP-client	Eke IP : DHCP-server	Eke	Nee	Beide	Alle	Toesta...
2	svchost.exe	Eke	Nee	Eke adapter	UDP	Eke IP : DHCP-server	Eke IP : DHCP-client	Eke	Ja	Beide	Alle	Toesta...
3	svchost.exe	Eke	Nee	Eke adapter	UDP	Eke IP : 1024-65535	Eke IP : DNS	Eke	Nee	Beide	Alle	Toesta...
4	svchost.exe	Eke	Nee	Eke adapter	TCP	Eke IP : 1024-65535	Eke IP : DNS	Eke	Nee	Beide	Verbinden, Ve...	Toesta...
5	Eke	Eke	Nee	Vol. vertro...	Eke	Eke IP : Eke poort	Eke IP : Eke poort	Eke	Nee	Beide	Alle	Toesta...
6	Eke	Eke	Nee	Lok. vertro...	Eke	Eke IP : Eke poort	Eke IP : Eke poort	Eke	Ja	Beide	Alle	Toesta...
7	Eke	Eke	Nee	Lok. Geblokk.	Eke	Eke IP : Eke poort	Eke IP : Eke poort	Eke	Ja	Beide	Alle	Weiger...
8	Eke	Eke	Nee	Geblokk.	Eke	Eke IP : Eke poort	Eke IP : Eke poort	Eke	Nee	Beide	Alle	Weiger...
9	Eke	Eke	Nee	Eke adapter	IGMP	Eke IP : Eke poort	Eke IP : Eke poort	Eke	Nee	Beide	Verkeer	Toesta...
10	Eke	Eke	Nee	Eke adapter	GRE	Eke IP : Eke poort	Eke IP : Eke poort	Eke	Nee	Beide	Verkeer	Toesta...
11	Eke	Eke	Nee	Eke adapter	AH	Eke IP : Eke poort	Eke IP : Eke poort	Eke	Nee	Beide	Verkeer	Toesta...
12	Eke	Eke	Nee	Eke adapter	ESP	Eke IP : Eke poort	Eke IP : Eke poort	Eke	Nee	Beide	Verkeer	Toesta...
13	System	Eke	Nee	Eke adapter	ICMP	Eke IP : Eke poort	Eke IP : Eke poort	IPv4	Nee	Beide	Verkeer	Toesta...
14	System	Eke	Nee	Eke adapter	ICMP6	Eke IP : Eke poort	Eke IP : Eke poort	IPv6	Nee	Beide	Verkeer	Toesta...
15	Eke	Eke	Nee	Eke adapter	VRMP	Eke IP : Eke poort	Eke IP : Eke poort	Eke	Nee	Beide	Verkeer	Toesta...
16	svchost.exe	Eke	Nee	Eke adapter	UDP	Eke IP : DNS	Eke IP : 1024-65535	Eke	Ja	Beide	Alle	Toesta...
17	svchost.exe	Eke	Nee	Eke adapter	TCP	Eke IP : DNS	Eke IP : 1024-65535	Eke	Ja	Beide	Verkeer, Lust...	Toesta...
18	svchost.exe	Eke	Nee	Eke adapter	TCP	Eke IP : 1024-65535	Eke IP : RPC	Eke	Ja	Beide	Verbinden, Ve...	Toesta...
19	svchost.exe	Eke	Nee	Eke adapter	TCP	Eke IP : Eke poort	Eke IP : HTTP, HTTPS	Eke	Nee	Beide	Verbinden, Ve...	Toesta...
20	svchost.exe	Eke	Nee	Eke adapter	UDP	Eke IP : NTP, 1024-6...	Eke IP : NTP	Eke	Nee	Beide	Alle	Toesta...
21	svchost.exe	Eke	Nee	Velig	TCP	Eke IP : RPC	Eke IP : Eke poort	Eke	Ja	Beide	Verkeer, Lust...	Toesta...
22	svchost.exe	Eke	Nee	Velig	UDP	Eke IP : 1900, 2177	Eke IP : Eke poort	Eke	Ja	Beide	Alle	Toesta...
23	svchost.exe	Eke	Nee	Velig	TCP	Eke IP : 2177, 3390	Eke IP : Eke poort	Eke	Ja	Beide	Alle	Toesta...
24	svchost.exe	Eke	Nee	Eke adapter	UDP	Eke IP : RDP	Eke IP : 1024-65535	Eke	Nee	Beide	Verkeer, Lust...	Toesta...
25	svchost.exe	Eke	Nee	Eke adapter	Eke	Eke IP : Eke poort	Eke IP : Eke poort	Eke	Nee	Beide	Alle	Weiger...
26	System	Eke	Nee	Eke adapter	UDP	Eke IP : NetBIOS NS	Eke IP : NetBIOS NS	Eke	Ja	Beide	Alle	Toesta...
27	System	Eke	Nee	Eke adapter	TCP	Eke IP : Eke poort	Eke IP : NetBIOS SS...	Eke	Ja	Beide	Verbinden, Ve...	Toesta...
28	System	Eke	Nee	Eke adapter	UDP	Eke IP : LTP, RIE, 4...	Eke IP : 1024-65535	Eke	Nee	Beide	Alle	Toesta...
29	System	Eke	Nee	Eke adapter	TCP	Eke IP : RPTP	Eke IP : 1024-65535	Eke	Nee	Beide	Verkeer, Lust...	Toesta...

Deze tabel toont alle regels die door de firewall zijn geladen voor het filteren van verkeer.

Sluiten

Geavanceerd regelbeheer

U ziet de firewall-regels in de volgorde zoals zij zijn geregistreerd. In de tabelkolommen staat uitgebreide informatie over elke regel.



Opmerking

Als er een poging voor het maken van een verbinding (inkomend of uitgaand) is, voert BitDefender de actie uit van de eerste regel die overeenkomt met de betreffende verbinding. Daarom is de volgorde waarin regels worden geregistreerd erg belangrijk.

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

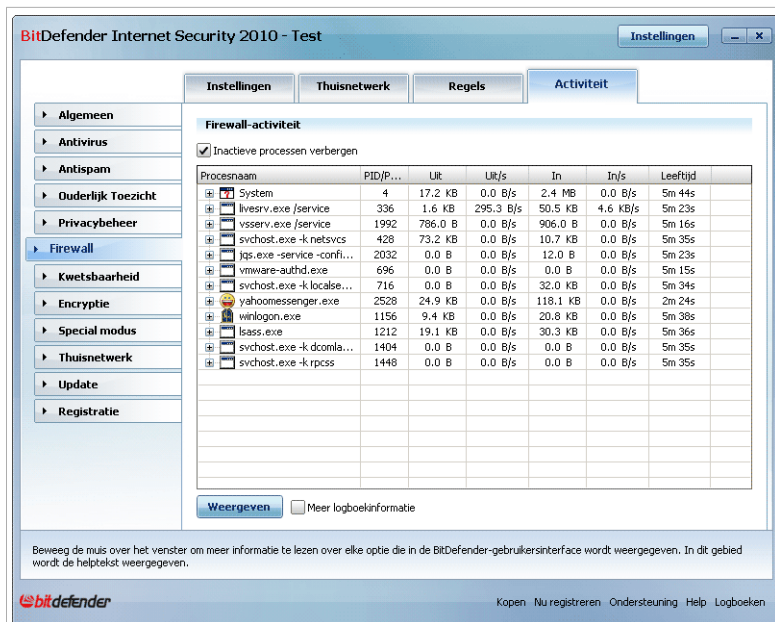
Om een regel te wijzigen, selecteert u deze en klikt u op de knop **Regel bewerken** of dubbelklikt u op de regel.

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

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

22.4. Verbindingsbeheer

Om de huidige netwerk-/internetactiviteit (via TCP en UDP) te bewaken, gesorteerd op toepassing en om het BitDefender Firewall-logboek te openen, gaat u naar **Firewall>Activiteit** in de Expert-modus.



Verbindingsbeheer

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

Als u ook de inactieve processen wilt zien, schakel dan het selectievakje **Inactieve processen verbergen** uit.

De pictogrammen betekenen:

- Geeft een uitgaande verbinding aan.
- Geeft een binnenkomende verbinding aan.
- Geeft een open poort op uw computer aan.

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

Voor een uitgebreide lijst van gebeurtenissen met betrekking tot het gebruik van de Firewall-module (in-/uitschakelen firewall, blokkeren van verkeer, wijzigen van

instellingen) of een lijst die is gegenereerd door activiteiten die door deze module zijn gedetecteerd (scannen van poorten, blokkeren van verbindingspogingen of verkeer volgens de regels), kunt u het Firewall-logboek van BitDefender weergeven door op **Logboek weergeven** te klikken. Het bestand bevindt zich in de map Normale bestanden van de huidige Windows gebruiker, op het pad: ...BitDefender\BitDefender Firewall\bdfirewall.txt.

Schakel het selectievakje **Meer loginformatie** in als u meer informatie in het logbestand wilt hebben.

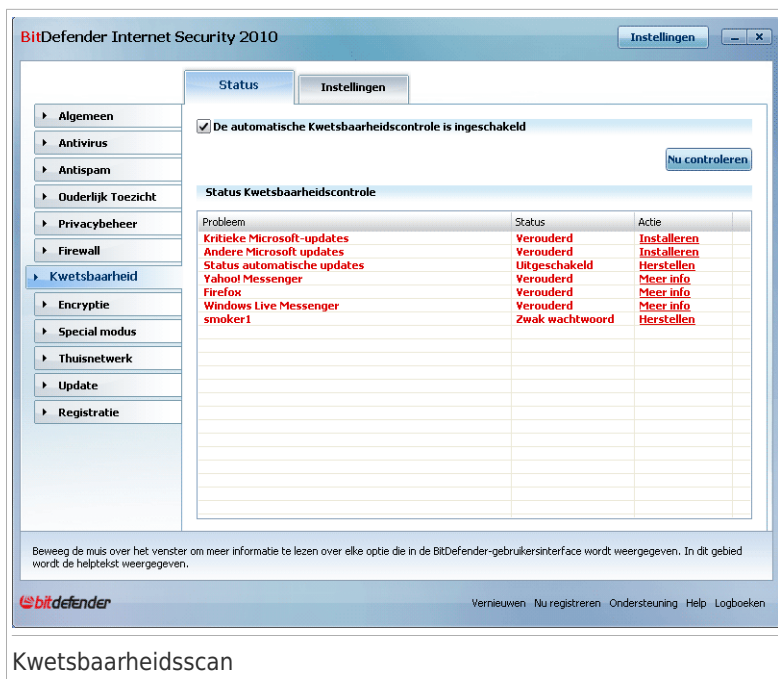
23. Kwetsbaarheid

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.

23.1. Status

Om de automatische kwetsbaarheidscontrole te configureren of om een kwetsbaarheidscontrole uit te voeren, gaat u naar **Kwetsbaarheid>Status** in de Expert-modus.



The screenshot shows the BitDefender Internet Security 2010 interface. The 'Status' tab is selected, and the 'Kwetsbaarheid' (Vulnerability) section is expanded in the left sidebar. The main area displays the 'Status Kwetsbaarheidscontrole' (Vulnerability Control Status) section. A checkbox indicates that automatic vulnerability control is enabled. Below this, a table lists detected vulnerabilities with their status and recommended actions.

Probleem	Status	Actie
Kritieke Microsoft-updates	Verouderd	Installeren
Andere Microsoft updates	Verouderd	Installeren
Status automatische updates	Uitgeschakeld	Herstellen
Yahoo! Messenger	Verouderd	Meer info
Firefox	Verouderd	Meer info
Windows Live Messenger	Verouderd	Meer info
smoker1	Zwak wachtwoord	Herstellen

Below the table, there is a note: '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 helpetekst weergegeven.'

At the bottom of the window, the BitDefender logo is visible on the left, and navigation links 'Vernieuwen', 'Nu registreren', 'Ondersteuning', 'Help', and 'Logboeken' are on the right.

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.

23.1.1. 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. 69).

23.2. 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.

24. Encryptie

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

24.1. 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

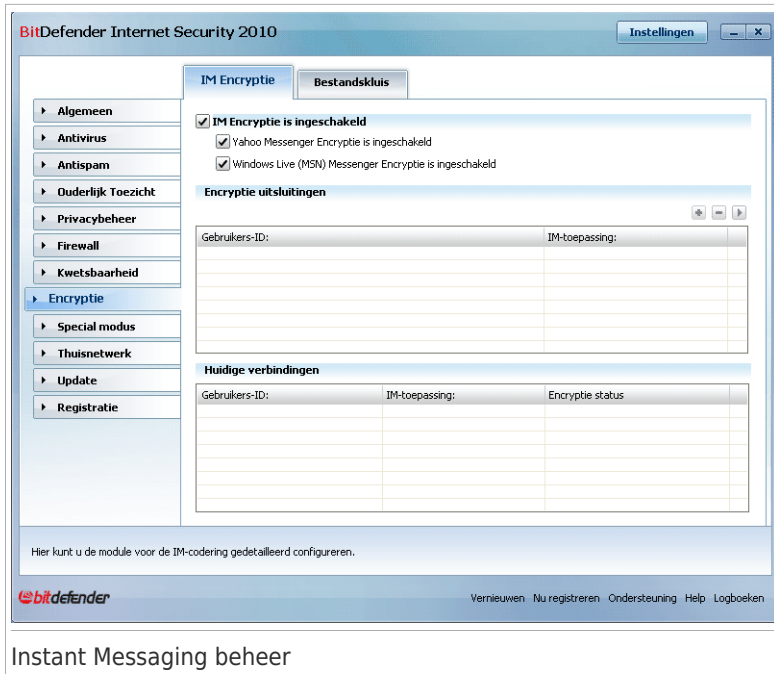
BitDefender zal een conversatie niet coderen als een chatpartner een op het web gebaseerde chattoepassing gebruikt, zoals Meebo, of als een van de chatpartners Yahoo! gebruikt en de andere Windows Live (MSN).

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. 296).



Instant Messaging beheer

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.

24.1.1. 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 beweringsveld.
3. Selecteer de instant messaging applicatie die behoort bij het contact.
4. Klik op **OK**.

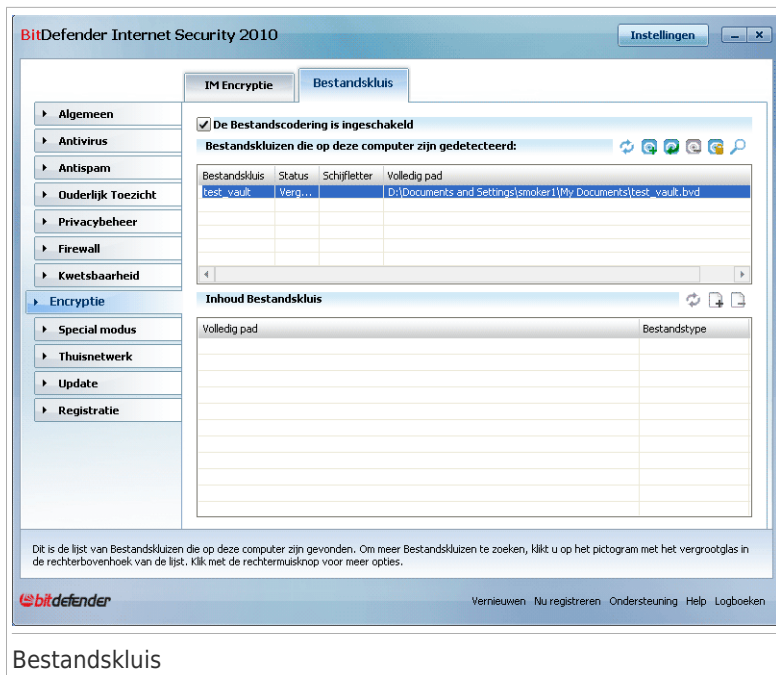
24.2. File Encryptie

Met Bestandscodering van BitDefender kunt u gecodeerde, door een wachtwoord beveiligde logische schijven (of kluizen) op uw computer maken waar u uw confidetiële en gevoelige documenten veilig kunt opslaan. De in de kluizen opgeslagen data zijn alleen toegankelijk voor gebruikers die het wachtwoord kennen.

Met het wachtwoord kan u een kluis openen, data erin opslaan en de kluis weer sluiten zonder dat de beveiliging in gevaar komt. Als een kluis open is, kan u nieuwe bestanden toevoegen, huidige bestanden openen of bewerken.

De kluis is een bestand dat is opgeslagen op de lokale harde schijf met de extensie `bvd`. Ofschoon de fysieke bestanden die de kluisschijven vormen, geopend kunnen worden door een ander besturingssysteem (zoals Linux), kan de informatie erop niet gelezen worden doordat deze is gecrypteerd.

Ga naar **Codering>Bestandscodering** in de Expert-modus om de bestandskluizen op uw computer te beheren.



Om Bestandscodering uit te schakelen, schakelt u het selectievakje **De Bestandscodering is ingeschakeld** uit en klikt u op **Ja** om te bevestigen. Als u bestandskluis uitschakelt, worden alle bestandskluisen vergrendeld kan u de bestanden erin niet meer openen.

In de tabel bovenaan staan de bestandskluisen op uw computer. U ziet de naam, de status (open/vergrendeld), de schijffletter en het volledige pad van de kluis. In de tabel onderaan staat de inhoud van de geselecteerde kluis.

24.2.1. Een kluis creëren

Gebruik een van de volgende methoden om een kluis te creëren:


- Klik op **Kluis creëren**.
- Rechtsklik in de kluis tabel en selecteer **Creëren**.
- Rechtsklik op uw bureaublad of in een map op uw computer, wijs naar **BitDefender bestandskluis** en selecteer **Creëren**.

Een nieuw venster wordt weergegeven.



Ga als volgt te werk:

1. Geef de plaats en de naam van de bestandskluis op.

- Klik op **Bladeren**, selecteer de plaats van de kluis en sla het kluisbestand op met de door u gewenste naam.
- U hoeft alleen de naam van de safe in het overeenkomende veld in te voeren om de safe in Mijn documenten te maken. Om Mijn documenten te openen, klikt u op het menu  Start van Windows en vervolgens op **Mijn documenten**.
- Typ het volledige pad van het kluisbestand op de schijf. Bijvoorbeeld: C:\my_vault.bvd.

2. Kies een schijfletter in het menu. Als u de kluis opent, verschijnt een virtuele schijf met de geselecteerde schijfletter in Deze computer.

3. Typ het gewenste wachtwoord voor de kluis in de velden **Wachtwoord** en **Bevestigen** in. Iedereen die probeert de kluis te openen en naar de bestanden erin te gaan, moet het wachtwoord opgeven.

4. Selecteer **Schijf formatteren** om de virtuele schijf van de kluis te formatteren. U moet het station formatteren voordat u bestanden kunt toevoegen aan de safe.

5. Als u de standaardgrootte (50 MB) van de kluis wilt veranderen, typt u de gewenste waarde in het **Kluisgrootte** veld.

6. Klik op **Creëren** als u de kluis alleen op de geselecteerde locatie wilt creëren. Om de kluis te creëren en weer te geven als een virtuele schijf in Deze computer, klikt u op **Creëren&Openen**.

BitDefender zal u onmiddellijk op de hoogte brengen van het resultaat van de bewerking. Als er een fout is opgetreden, moet u het foutbericht gebruiken om de fout op te lossen. Klik op **OK** om het venster te sluiten.



Opmerking

Het kan nuttig zijn alle bestandssafes op te slaan op dezelfde locatie. Hierdoor kunt u ze sneller vinden.


24.2.2. Een kluis openen

Om bestanden die zijn opgeslagen in een kluis te openen en te bewerken, moet u de kluis openen. Als u de kluis opent, verschijnt een virtuele schijf in Deze computer. De schijf heeft de schijfletter die is toegewezen aan de kluis.

Gebruik een van de volgende methoden om een kluis te openen:

- Selecteer de kluis in de tabel en klik op  **Kluis openen**.
- Rechtsklik op de kluis in de tabel en selecteer **Openen**.
- Rechtsklik op het kluisbestand op uw computer, wijs naar **BitDefender bestandskluis** en selecteer **Openen**.

Een nieuw venster wordt weergegeven.



Bestandskluis openen

Ga als volgt te werk:

1. Kies een schijfletter in het menu.
2. Typ het wachtwoord van de kluis in het **Wachtwoord** veld.
3. Klik op **Openen**.

BitDefender zal u onmiddellijk op de hoogte brengen van het resultaat van de bewerking. Als er een fout is opgetreden, moet u het foutbericht gebruiken om de fout op te lossen. Klik op **OK** om het venster te sluiten.

24.2.3. Een kluis vergrendelen

Als u klaar bent met het werken in een bestandskluis, moet u de kluis vergrendelen om uw data te beveiligen. Door de safe te vergrendelen, verdwijnt het

overeenkomende schijfstation uit Deze computer. Hierdoor worden de gegevens die in de safe zijn opgeslagen, volledig geblokkeerd.


Gebruik een van de volgende methoden om een kluis te vergrendelen:

- Selecteer de kluis in de tabel en klik op  **Kluis vergrendelen**.
- Rechtsklik op de kluis in de tabel en selecteer **Vergrendelen**.
- Rechtsklik op de betreffende schijf in Deze computer, wijs naar **BitDefender bestandskluis** en selecteer **Vergrendelen**.

BitDefender zal u onmiddellijk op de hoogte brengen van het resultaat van de bewerking. Als er een fout is opgetreden, moet u het foutbericht gebruiken om de fout op te lossen. Klik op **OK** om het venster te sluiten.

24.2.4. Wachtwoord van kluis veranderen

De safe moet vergrendeld zijn voordat u het wachtwoord kunt wijzigen. Gebruik een van de volgende methoden om het wachtwoord van de kluis te veranderen:

- Selecteer de kluis in de tabel en klik op  **Wachtwoord veranderen**.
- Rechtsklik op de kluis in de tabel en selecteer **wachtwoord veranderen**.
- Rechtsklik op het kluisbestand op uw computer, wijs naar **BitDefender Bestandskluis** en selecteer **Wachtwoord van kluis veranderen**.

Een nieuw venster wordt weergegeven.



Wachtwoord van kluis veranderen

Ga als volgt te werk:

1. Typ het huidige wachtwoord in het **Oude wachtwoord** veld.
2. Typ het nieuwe wachtwoord in de velden **Nieuw wachtwoord** en **Nieuw wachtwoord herhalen**.



Opmerking


Het wachtwoord moet minstens 8 tekens bevatten. Voor een sterk wachtwoord gebruikt u een combinatie van hoofdletters en kleine letters, getallen en speciale tekens (zoals #, \$ of @).

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


BitDefender zal u onmiddellijk op de hoogte brengen van het resultaat van de bewerking. Als er een fout is opgetreden, moet u het foutbericht gebruiken om de fout op te lossen. Klik op **OK** om het venster te sluiten.

24.2.5. Bestanden toevoegen aan een kluis

Volg deze stappen om bestanden toe te voegen aan een kluis:


1. Selecteer in de tabel met de safes, de safe waaraan u bestanden wilt toevoegen.
2. Als de safe is vergrendeld, moet u deze eerst openen (klik er met de rechtermuisknop op en selecteer **Safe openen**).
3. Klik op  **Bestand toevoegen**. Een nieuw venster wordt weergegeven.
4. Selecteer de bestanden/mappen die u wilt toegevoegen aan de kluis.
5. Klik op **OK** om de geselecteerde objecten toe te voegen aan de kluis.

Zodra de safe open is, kunt u rechtstreeks gebruik maken van het virtuele schijfstation dat overeenkomt met de safe. Volg deze stappen:

1. Open Deze computer (klik op het menu  Start van Windows en vervolgens op **Deze computer**).
2. Open het virtuele schijfstation dat overeenkomt met de safe. Zoek de stationsletter die u aan de safe hebt toegekend op het ogenblik dat u de safe hebt geopend.
3. U kunt de bestanden en mappen direct kopiëren/plakken of slepen/neerzetten op dit virtuele schijfstation.

24.2.6. Bestanden verwijderen uit een kluis

Volg deze stappen om bestanden te verwijderen uit een kluis:

1. Selecteer in de tabel de kluis waarin zich het te verwijderen bestand bevindt.
2. Als de safe is vergrendeld, moet u deze eerst openen (klik er met de rechtermuisknop op en selecteer **Safe openen**).
3. Selecteer het bestand dat moet worden verwijderd uit de tabel met de kluisinhoud.
4. Klik op  **Bestanden/mappen verwijderen**.

Als de kluis open is, kan u het bestand direct verwijderen van de kluisschijf. Volg deze stappen:

1. Open Deze computer (klik op het menu  Start van Windows en vervolgens op **Deze computer**).
2. Open het virtuele schijfstation dat overeenkomt met de safe. Zoek de stationsletter die u aan de safe hebt toegekend op het ogenblik dat u de safe hebt geopend.
3. Verwijder bestanden of mappen zoals u dat gewoon bent in Windows (klik bijvoorbeeld met de rechtermuisknop op een bestand dat u wilt Verwijderen en selecteer **Verwijderen**).

25. 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.

25.1. 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**.
- De BitDefender firewall is ingesteld op **Alles toestaan**. Dit betekent dat alle nieuwe verbindingen (inkomend en uitgaand) automatisch zijn toegestaan, ongeacht de poort en het gebruikte protocol.
- 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.

25.1.1. 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.

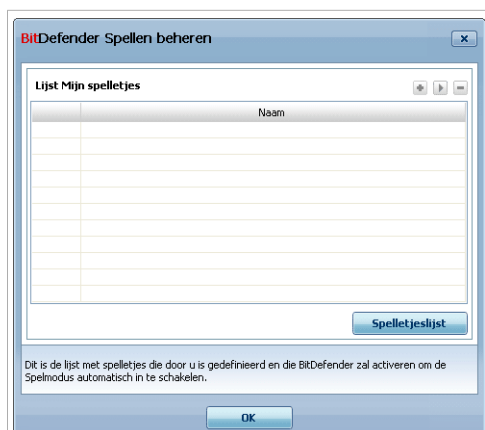


Opmerking

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

25.1.2. De spellenlijst beheren

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






Spellenlijst

Nieuwe applicaties worden automatisch toegevoegd aan de lijst als:

- U een spel start uit de BitDefender's lijst van bekende spellen. 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 bewerkingsveld.

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

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

25.1.3. 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.

Volg deze stappen om de BitDefender firewall automatisch uit te schakelen in de spelmodus:

1. Klik op **Geavanceerde instellingen**. Een nieuw venster wordt weergegeven.
2. Schakel het selectievakje **Firewall instellen op Alles toestaan (Spelmodus) indien in Spelmodus** in.
3. Klik op **OK** om de wijzigingen op te slaan.

25.1.4. 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 **Sneltoetsen gebruiken** te verwijderen, schakelt u de sneltoets uit.

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

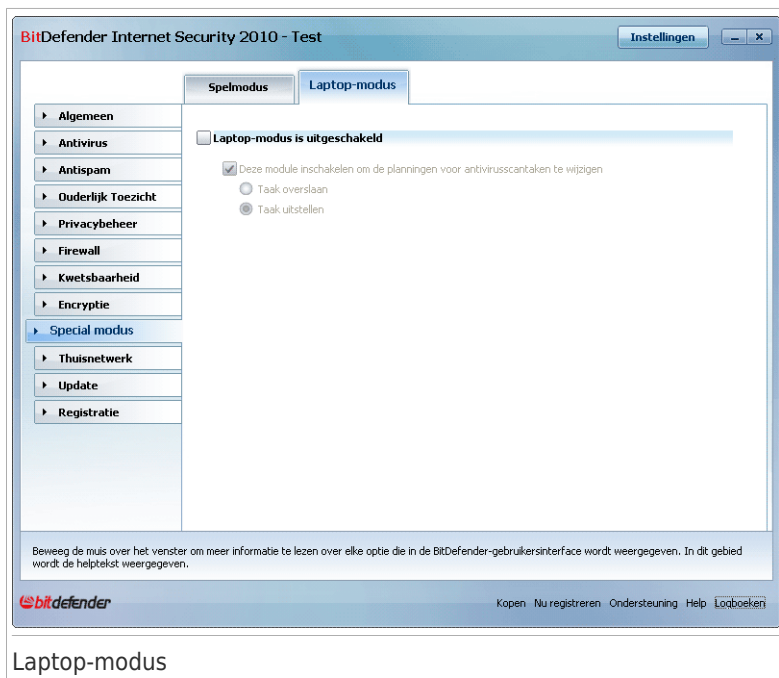
25.2. Laptop-modus

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.



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.

25.2.1. Laptop-modus instellingen configureren

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

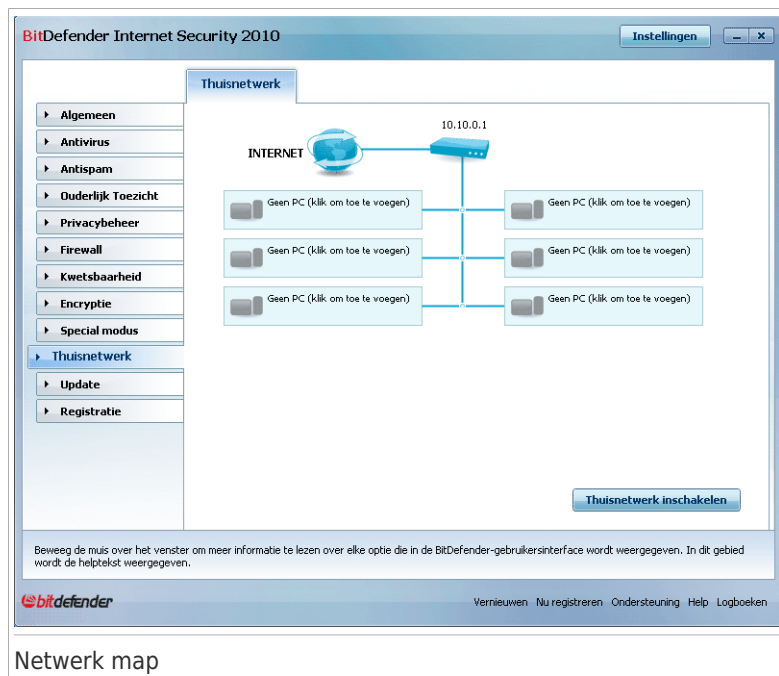
- **Deze module toestaan planningen van Antivirus-scantaken te wijzigen**
- hiermee kunt u verhinderen dat scantaken worden uitgevoerd terwijl u in de Laptop-modus bent. U kan een van de volgende opties kiezen:

Optie	Beschrijving
Taak overslaan	De geprogrammeerde taak wordt helemaal niet uitgevoerd.

Optie	Beschrijving
Taak uitstellen	De geprogrammeerde taak uitvoeren zodra u de Laptop-modus verlaat.

26. Thuisnetwerk

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



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.

26.1. 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.

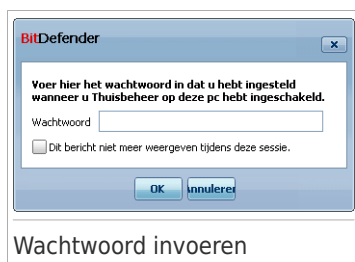


2. Voer hetzelfde wachtwoord in elk van de bewerkingsvelden in.
 3. Klik op **OK**.
- U ziet de naam van de computer in de netwerkmap.

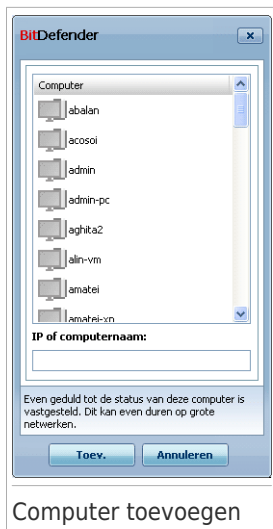
26.2. bezig met toevoegen van computers aan het BitDefender netwerk

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.

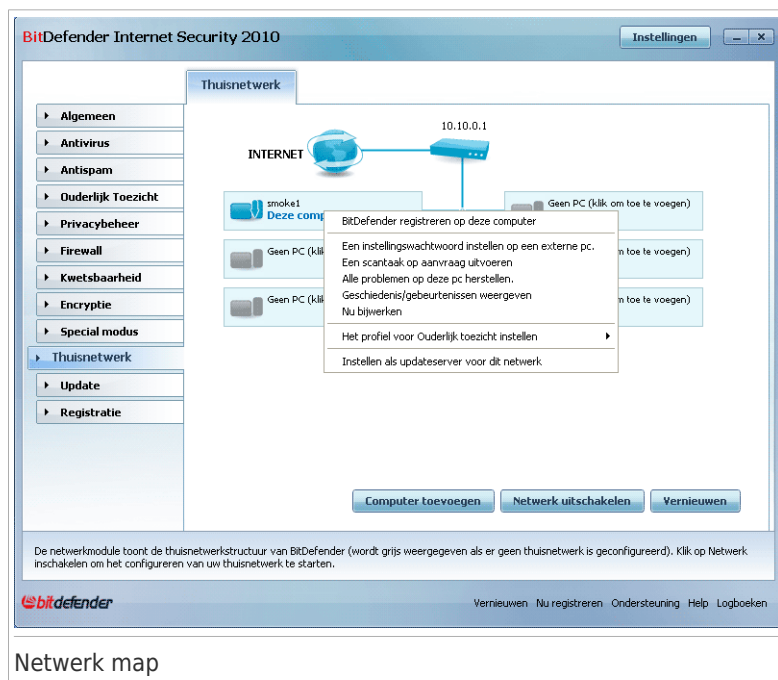


Opmerking

U kan maximaal vijf computers toevoegen aan de netwerkmap.

26.3. 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 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.

- **Het profiel voor Ouderlijk toezicht instellen**

Hiermee kunt u de leeftijdscategorie instellen die moet worden gebruikt door de webfilter Ouderlijk toezicht op deze computer: kind, tiener of volwassene.

- **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.



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.

27. 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**.

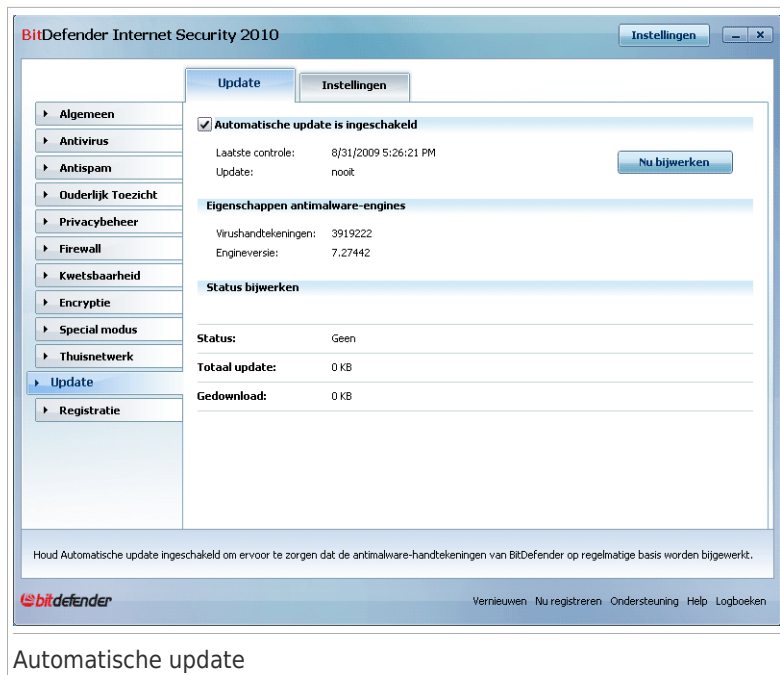
Het updateproces wordt "on the fly" uitgevoerd. Dit betekent dat de bestanden die moeten worden bijgewerkt, progressief worden vervangen. Hierdoor zal het updateproces de productwerking niet beïnvloeden wordt tegelijkertijd elk zwak punt uitgeschakeld.

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 antispam-engines** - er worden nieuwe regels toegevoegd aan de heuristische en URL-filters. Daarnaast worden nieuwe afbeeldingen toegevoegd aan de Afbeeldingsfilter. Dit zal de doeltreffendheid van uw Antispam-engine verbeteren. Dit type update is ook bekend als **Antispam-update**.
- **Updates voor de antispyspyware-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**.

27.1. 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.

27.1.1. 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.

27.1.2. 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.

27.2. 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.



Update- instellingen

De update-instellingen zijn gegroepeerd in 4 categorieën (**Updatelocatie-instellingen**, **Automatische update-instellingen**, **Handmatige update-instellingen** en **Geavanceerde instellingen**). Elke categorie wordt afzonderlijk beschreven.

27.2.1. 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. 277).

27.2.2. 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.

27.2.3. 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.

27.2.4. 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.

27.2.5. 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.

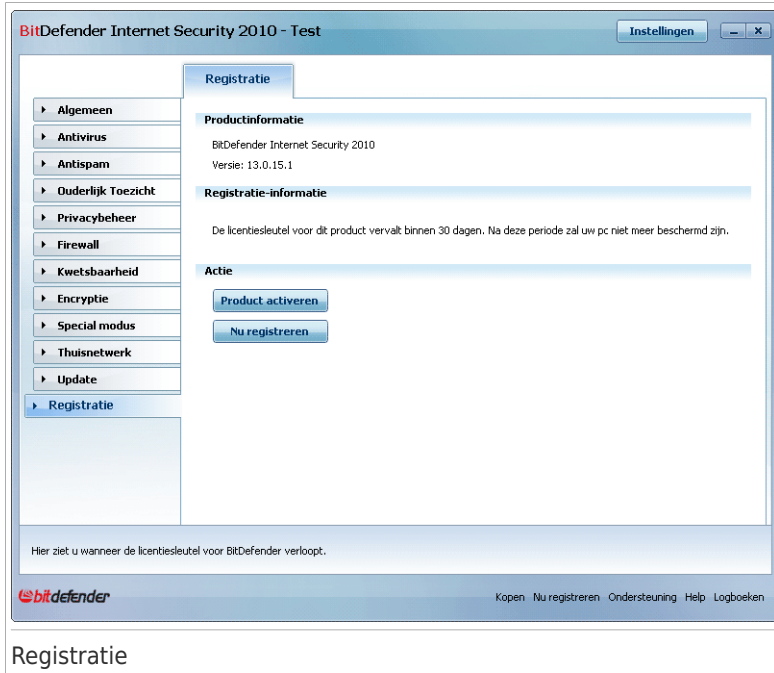
Eerst wordt de reeks met uw persoonlijke proxy-instellingen gebruikt om een verbinding te maken met het internet. Als dat niet werkt, worden daarna de proxy-instellingen die op het tijdstip van de installatie zijn gedetecteerd, geprobeerd. Als dat evenmin werkt, worden tot slot de proxy-instellingen 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.

28. Registratie

Om complete informatie over uw BitDefender-product en de registratiestatus te zoeken, gaat u naar **Registratie** in de Expert-modus.

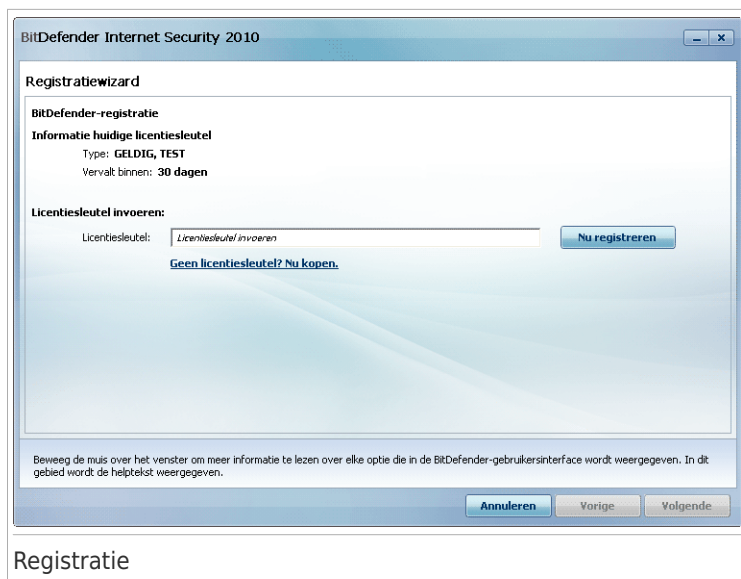


In deze sectie ziet u:

- **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.

28.1. BitDefender Internet Security 2010 registreren

Klik op **Nu registreren** om het venster voor de productregistratie te openen.



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

BitDefender Internet Security 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**.

28.2. 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.

BitDefender Internet Security 2010

Registratiewizard

BitDefender-account

Activeer uw BitDefender nu om toegang tot technische dienst te krijgen. Ook geeft <http://myaccount.BitDefender.com> u de gelegenheid aan om uw 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 wordt weergegeven. In dit gebied wordt de helpetekst weergegeven.

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. 282)
- “Ik heb al een BitDefender-account” (p. 283)

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**

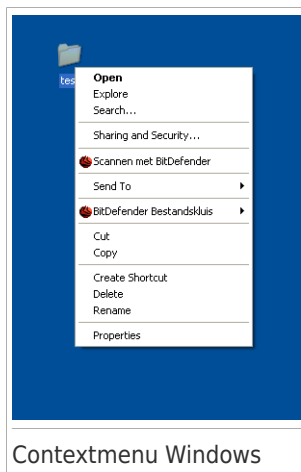
4. Klik op **Aanmelden**.

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

Integratie in Windows en software van derden

29. 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.



Contextmenu Windows

BitDefender integreert zichzelf in het contextmenu van Windows zodat u gemakkelijk bestanden kunt scannen op virussen en andere gebruikers de toegang tot uw vertrouwelijke bestanden kunt weigeren. U kunt de BitDefender-opties in het contextmenu snel vinden door het BitDefender-pictogram te zoeken.

- Scannen met BitDefender
- BitDefender Bestandssafe

29.1. 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 linkerkzijde 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.

29.2. BitDefender bestandskluis

De BitDefender Bestandssafe helpt u bij het veilig opslaan van uw vertrouwelijke documenten op uw computer via het gebruik van bestandssafes.

- De bestandskluis is een veilige opslagplaats voor persoonlijke informatie of gevoelige bestanden.
- De bestandskluis is een gecrypteerd bestand op uw computer met de extensie .bvd. Omdat het gecrypteerd is, is de data erin ongevoelig voor diefstal of voor een gat in de beveiliging.
- Als u dit .bvd bestand opent, verschijnt een nieuwe logische partitie (een nieuwe schijf). Vergelijk dit met het openen van een ISO beeld als virtuele cd.

Open Deze Computer en u ziet een nieuwe schijf: uw bestandskluis. Hierop kan u bestandshandelingen doen (kopiëren, verwijderen, veranderen, enz). De bestanden zijn beveiligd zolang ze op deze schijf staan (omdat een wachtwoord nodig is bij het openen).

Als u klaar bent, vergrendelt (sluit) u de kluis zodat de inhoud ervan weer veilig is.

U kunt de BitDefender-bestandssafes gemakkelijk herkennen op uw computer via het  BitDefender-pictogram en de extensie .bvd.



Opmerking

Deze sectie toont u hoe u BitDefender-bestandssafes kunt maken en beheren waarbij u alleen de opties gebruikt die in het contextmenu van Windows zijn voorzien. U kunt bestandssafes ook direct vanaf de BitDefender-interface maken en beheren.

- Klik in de Gemiddelde modus op het tabblad **Bestandskluis** en gebruik de opties van het gebied **Snelle taken**. Een wizard zal u helpen bij het voltooien van elke taak.
- Voor een rechtlijnige benadering, schakelt u de gebruikersinterface naar de Expert-modus en klikt u in het menu aan de linkerkzijde op **Codering**. Op het tabblad **Bestandscodering** kunt u de bestaande bestandskluizen en hun inhoud zien en beheren.

29.2.1. Kluis creëren

Denk eraan dat een safe in werkelijkheid slechts een bestand is met de extensie .bvd. Alleen wanneer u de safe opent, verschijnt een virtueel schijfstation in Deze computer en kunt u de bestanden veilig opslaan op dit station. Wanneer u een safe maakt, moet u opgeven waar en onder welke naam u deze wilt opslaan op uw computer. U moet ook een wachtwoord opgeven om de inhoud van de safe te beveiligen. Alleen gebruikers die het wachtwoord kennen, kunnen de safe openen en krijgen toegang tot de documenten en gegevens die in de safe zijn opgeslagen.

Volg deze stappen om een safe te maken:

1. Klik met de rechtermuisknop op uw bureaublad of in een map op uw computer, wijs **BitDefender Bestandskluis** aan en selecteer **Bestandskluis maken**. Het volgende venster wordt geopend:

2. Geef de plaats en de naam van de bestandskluis op.

- Klik op **Bladeren**, selecteer de plaats van de kluis en sla het kluisbestand op met de door u gewenste naam.
- U hoeft alleen de naam van de safe in het overeenkomende veld in te voeren om de safe in Mijn documenten te maken. Om Mijn documenten te openen, klikt u op het menu  Start van Windows en vervolgens op **Mijn documenten**.

- Typ het volledige pad van het kluisbestand op de schijf. Bijvoorbeeld:
C:\my_vault.bvd.
- 3. Kies een schijfletter in het menu. Als u de kluis opent, verschijnt een virtuele schijf met de geselecteerde schijfletter in Deze computer.
- 4. Typ het gewenste wachtwoord voor de kluis in de velden **Wachtwoord** en **Bevestigen** in. Iedereen die probeert de kluis te openen en naar de bestanden erin te gaan, moet het wachtwoord opgeven.
- 5. Selecteer **Schijf formatteren** om de virtuele schijf van de kluis te formatteren. U moet het station formatteren voordat u bestanden kunt toevoegen aan de safe.
- 6. Als u de standaardgrootte (50 MB) van de kluis wilt veranderen, typt u de gewenste waarde in het **Kluisgrootte** veld.
- 7. Klik op **Creëren** als u de kluis alleen op de geselecteerde locatie wilt creëren. Om de kluis te creëren en weer te geven als een virtuele schijf in Deze computer, klikt u op **Creëren&Openen**.

BitDefender zal u onmiddellijk op de hoogte brengen van het resultaat van de bewerking. Als er een fout is opgetreden, moet u het foutbericht gebruiken om de fout op te lossen. Klik op **OK** om het venster te sluiten.



Opmerking

Het kan nuttig zijn alle bestandssafes op te slaan op dezelfde locatie. Hierdoor kunt u ze sneller vinden.

29.2.2. Kluis openen

Om bestanden die zijn opgeslagen in een kluis te openen en te bewerken, moet u de kluis openen. Als u de kluis opent, verschijnt een virtuele schijf in Deze computer. De schijf heeft de schijfletter die is toegewezen aan de kluis.

Volg deze stappen om een safe te openen:

1. Zoek op uw computer naar het bvd-bestand dat de safe voorstelt die u wilt openen.
2. Klik met de rechtermuisknop op het bestand, selecteer **BitDefender Bestandssafe** en klik op **Openen**. Om dit sneller te doen, kunt u ook dubbelklikken op het bestand of op het bestand klikken met de rechtermuisknop en **Openen** selecteren. Het volgende venster wordt geopend:



3. Kies een schijfletter in het menu.
4. Typ het wachtwoord van de kluis in het **Wachtwoord** veld.
5. Klik op **Openen**.

BitDefender zal u onmiddellijk op de hoogte brengen van het resultaat van de bewerking. Als er een fout is opgetreden, moet u het foutbericht gebruiken om de fout op te lossen. Klik op **OK** om het venster te sluiten.

29.2.3. Kluis vergrendelen

Als u klaar bent met het werken in een bestandskluis, moet u de kluis vergrendelen om uw data te beveiligen. Door de safe te vergrendelen, verdwijnt het overeenkomende schijfstation uit Deze computer. Hierdoor worden de gegevens die in de safe zijn opgeslagen, volledig geblokkeerd.

Volg deze stappen om een safe te vergrendelen:

1. Open Deze computer (klik op het menu  Start van Windows en vervolgens op **Deze computer**).
2. Identificeer het virtuele schijfstation dat overeenkomt met de safe die u wilt sluiten. Zoek de stationsletter die u aan de safe hebt toegekend op het ogenblik dat u de safe hebt geopend.
3. Klik met de rechtermuisknop op het respectieve virtuele schijfstation, selecteer **BitDefender Bestandssafe** en klik op **Sluiten**.

U kunt ook met de rechtermuisknop klikken op het bestand .bvd dat de kluis voorstelt, **BitDefender Bestandskluis** selecteren en op **Sluiten** klikken.

BitDefender zal u onmiddellijk op de hoogte brengen van het resultaat van de bewerking. Als er een fout is opgetreden, moet u het foutbericht gebruiken om de fout op te lossen. Klik op **OK** om het venster te sluiten.



Opmerking


Als er meerdere kluisen open zijn, zult u wellicht de BitDefender-interface voor de Expert-modus willen gebruiken. Als u naar **Codering** gaat en het tabblad **Bestandscodering** opent, ziet u een tabel die informatie over de bestaande kluisen biedt. Deze informatie vermeldt of de safe open is en, indien ja, welke stationsletter is toegewezen.

29.2.4. Toevoegen aan Bestandssafe

Voordat u bestanden of mappen aan een safe kunt toevoegen, moet u de safe openen. Zodra een safe is geopend, kunt u er gemakkelijk bestanden of mappen in opslaan via het contextmenu. Klik met de rechtermuisknop op het bestand of de map die u naar de kluis wilt kopiëren, selecteer **BitDefender Bestandskluis** en klik op **Toevoegen aan Bestandskluis**.


- Als er slechts één safe open is, wordt het bestand of de map direct naar die safe gekopieerd.
- Als er meerdere safes open zijn, wordt u gevraagd de safe te kiezen waarnaar u het item wilt kopiëren. Selecteer in het menu de stationsletter die overeenkomt met de gewenste safe en klik op **OK** om het item te kopiëren.

U kunt ook het virtuele schijfstation dat overeenkomt met de safe, gebruiken. Volg deze stappen:

1. Open Deze computer (klik op het menu  Start van Windows en vervolgens op **Deze computer**).
2. Open het virtuele schijfstation dat overeenkomt met de safe. Zoek de stationsletter die u aan de safe hebt toegekend op het ogenblik dat u de safe hebt geopend.
3. U kunt de bestanden en mappen direct kopiëren/plakken of slepen/neerzetten op dit virtuele schijfstation.

29.2.5. Verwijderen uit Bestandssafe

Om bestanden of mappen uit een safe te verwijderen, moet de safe open zijn. Volg de onderstaande stappen om bestanden of mappen uit een safe te verwijderen:

1. Open Deze computer (klik op het menu  Start van Windows en vervolgens op **Deze computer**).
2. Open het virtuele schijfstation dat overeenkomt met de safe. Zoek de stationsletter die u aan de safe hebt toegekend op het ogenblik dat u de safe hebt geopend.
3. Verwijder bestanden of mappen zoals u dat gewoon bent in Windows (klik bijvoorbeeld met de rechtermuisknop op een bestand dat u wilt Verwijderen en selecteer **Verwijderen**).

29.2.6. Wachtwoord van kluis veranderen

Het wachtwoord beveiligt de inhoud van een safe tegen onbevoegde toegang. Alleen gebruikers die het wachtwoord kennen, kunnen de safe openen en krijgen toegang tot de documenten en gegevens die in de safe zijn opgeslagen.

De safe moet vergrendeld zijn voordat u het wachtwoord kunt wijzigen. Volg de onderstaande stappen om het wachtwoord van een safe te wijzigen.

1. Zoek op uw computer naar het bvd-bestand dat de safe voorstelt.
2. Klik met de rechtermuisknop op het bestand, selecteer **BitDefender Bestandskluis** en klik op **Wachtwoord kluis wijzigen**. Het volgende venster wordt geopend:



Wachtwoord van kluis veranderen

3. Typ het huidige wachtwoord in het veld **Oud wachtwoord**.
4. Voer het nieuwe wachtwoord voor de kluis in de velden **Nieuw wachtwoord** en **Nieuw wachtwoord bevestigen** in.



Opmerking

Het wachtwoord moet minstens 8 tekens bevatten. Voor een sterk wachtwoord gebruikt u een combinatie van hoofdletters en kleine letters, getallen en speciale tekens (zoals #, \$ of @).

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

BitDefender zal u onmiddellijk op de hoogte brengen van het resultaat van de bewerking. Als er een fout is opgetreden, moet u het foutbericht gebruiken om de fout op te lossen. Klik op **OK** om het venster te sluiten.


30. 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

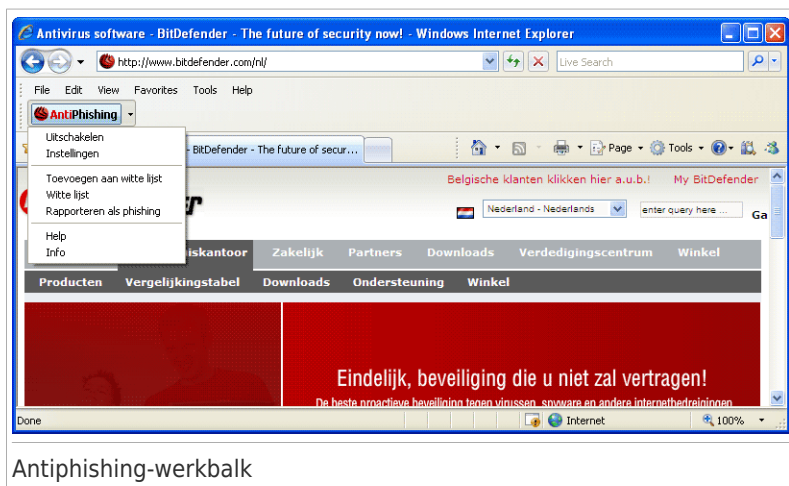
U kan de antiphishing-beveiliging en de Witte lijst gemakkelijk en efficiënt beheren met de werkbalk van BitDefender Antiphishing die in de bovenstaande webbrowsers is geïntegreerd.

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**.



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.

31. 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:

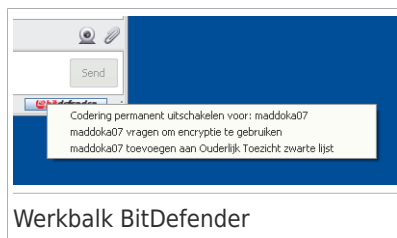
- uw chatpartner een BitDefender-versie heeft geïnstalleerd die IM Encryptie ondersteunt en IM Encryption is ingeschakeld voor de instant messaging applicatie die bij het chatten wordt gebruikt.
- U en uw chatpartner gebruiken ofwel Yahoo Messenger of Windows Live (MSN) Messenger.




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.
- **Contactpersonen toevoegen aan de zwarte lijst van het Ouderlijk toezicht.** Als u de contactpersoon toevoegt aan de zwarte lijst van Ouderlijk toezicht en als Ouderlijk toezicht is ingeschakeld, zult u niet langer de expresberichten zien die door die contactpersoon zijn verzonden. Om de contactpersoon van de zwarte lijst te Verwijderen, klikt u op de werkbalk en

selecteert u **Contactpersoonverwijderen uit de zwarte lijst van Ouderlijk toezicht.**

32. Integratie in mailclients

BitDefender Internet Security 2010 bevat een Antispam-module. Antispam controleert de e-mailberichten die u ontvangt en identificeert de berichten die spam bevatten. De spamberichten die door BitDefender worden gedetecteerd, zijn gemarkeerd met de prefix [SPAM] in de onderwerpregel.



Opmerking

Antispam bescherming is aanwezig voor alle POP3/SMTP e-mailclients.

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

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

BitDefender verplaatst spamberichten automatisch naar een specifieke map, zoals hieronder beschreven:

- In Microsoft Outlook worden spamberichten verplaatst naar een map **Spam** die zich in de map **Verwijderde items** bevindt. De map **Spam** wordt gemaakt tijdens de installatie van BitDefender.
- In Outlook Express en Windows Mail worden spamberichten direct naar **Verwijderde items** verplaatst.
- In Mozilla Thunderbird worden spamberichten verplaatst naar een map **Spam** die zich in de map **Trash** bevindt. De map **Spam** wordt gemaakt tijdens de installatie van BitDefender.


Als u andere e-mailclients gebruikt, moet u een regel maken om e-mailberichten met de markering [SPAM] door BitDefender te laten verplaatsen naar een aangepaste quarantainemap.

32.1. Configuratiewizard voor Antispam

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



Opmerking

U kunt de wizard ook op elk moment starten door op de knop  **Wizard** te klikken in de **Antispam-werkbalk**.

32.1.1. Stap 1/6 – Welkomstvenster



Klik op **Volgende**.

32.1.2. Stap 2/6 – De Vriendenlijst opstellen



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

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

Selecteer **Deze stap overslaan** als u deze configuratiestap wilt overslaan. Klik op **Volgende** om door te gaan.

32.1.3. Stap 3/6 – De Bayes-database verwijderen



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

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

U kunt de Bayes-database opslaan naar een bestand zodat u het kunt gebruiken met een ander BitDefender-product of na het opnieuw installeren van BitDefender. Om de Bayes-database op te slaan, klikt u op de knop **Bayes opslaan** en slaat u het op naar de gewenste locatie. Het bestand zal de extensie **.dat** hebben.

Om een eerder opgeslagen Bayes-database te laden, klikt u op de knop **Bayes laden** en opent u het overeenkomende bestand.

Selecteer **Deze stap overslaan** als u deze configuratiestap wilt overslaan. Klik op **Volgende** om door te gaan.

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



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

Onder de maplijst zijn er twee geavanceerde opties:

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

Selecteer **Deze stap overslaan** als u deze configuratiestap wilt overslaan. Klik op **Volgende** om door te gaan.

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



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



Belangrijk

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

Onder de maplijst zijn er twee geavanceerde opties:

- **Inclusief alle submappen** - om de submappen op te nemen in uw selectie.
- **Automatisch toevoegen aan spammerslijst** - om afzenders toe te voegen aan de Spammerslijst. E-mailberichten van deze afzender zullen altijd als SPAM worden gemarkeerd en overeenkomstig worden verwerkt.

Selecteer **Deze stap overslaan** als u deze configuratiestap wilt overslaan. Klik op **Volgende** om door te gaan.

32.1.6. Stap 6/6 – Overzicht

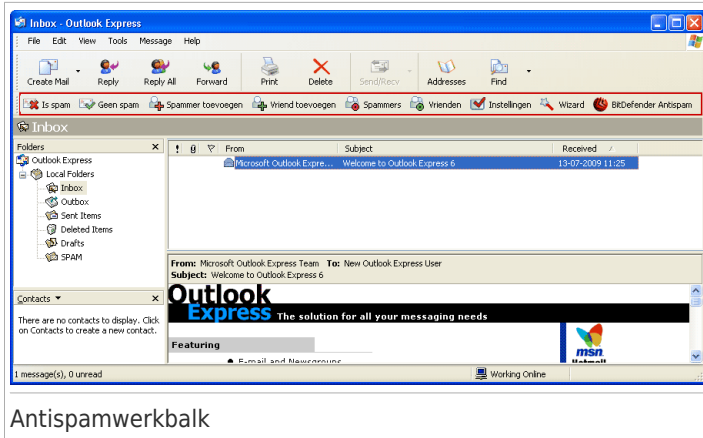


Hier kunt u alle instellingen voor de configuratiewizard bekijken. U kunt eventuele wijzigingen aanbrengen door terug te keren naar de vorige stappen (klik op **Vorige**).

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

32.2. Antispamwerkbalk

In het bovenste gebied van het venster van de e-mailclient ziet u de werkbalk Antispam. De werkbalk Antispam helpt u de antispambeveiliging direct vanaf uw e-mailclient te beheren. U kunt BitDefender gemakkelijk corrigeren als het programma een rechtmatig bericht als SPAM heeft gemarkeerd.



Elke knop van de BitDefender-werkbalk wordt hieronder uitgelegd.

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

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



Opmerking

U kan één e-mail, of zoveel e-mails als u zelf wilt, selecteren.

- **Geen spam** - verzendt een bericht naar de Bayes-module dat aangeeft dat de geselecteerde e-mail geen spam is en dat BitDefender niet had mogen labelen. De e-mail wordt van de map **Spam** verplaatst naar de map van uw **Postvak IN**.

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




Opmerking

U kan één e-mail, of zoveel e-mails als u zelf wilt, selecteren.



Belangrijk

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

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



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


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

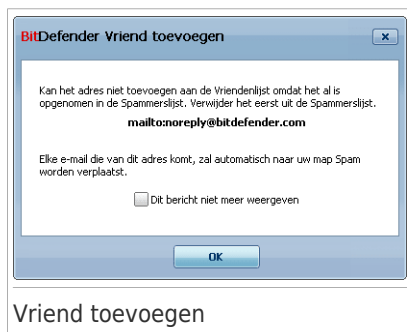
De toekomstige e-mailberichten van dat adres zullen als SPAM worden gelabeld.



Opmerking

U kan één afzender, of zoveel afzenders als u zelf wilt, selecteren.

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



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

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

U ontvangt alle e-mailberichten van dit adres, ongeacht hun inhoud.



Opmerking

U kan één afzender, of zoveel afzenders als u zelf wilt, selecteren.

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



Opmerking

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

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

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



Belangrijk

Syntaxis: naam@domein.com.

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



Belangrijk

Syntaxis:

- ▶ @domain.com, *domain.com and domain.com - alle ontvangen e-mailberichten van domain.com worden als SPAM gelabeld;
- ▶ *domein* - alle ontvangen e-mailberichten van domein (ongeacht de domeinachtersvoegsels) worden als SPAM gelabeld;

- ▶ ***com*** - alle ontvangen e-mailberichten met het domeinachtervoegsel **com** worden als **SPAM** gelabeld.





Waarschuwing

Voeg geen domein van rechtmatige e-mailservices via het web (zoals Yahoo, Gmail, Hotmail of andere) toe aan de Spammerslijst. Anders zullen de e-mailberichten die zijn ontvangen van een geregistreerde gebruiker van een dergelijke service, als spam worden gedetecteerd. Als u bijvoorbeeld **yahoo.com** toevoegt aan de spammerslijst, worden alle e-mailberichten die van adressen van **yahoo.com** afkomstig zijn, als **[spam]** gemarkeerd.

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

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


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

Om een item uit de lijst te verwijderen, selecteert u het item en klikt u op de knop **Verwijderen**. Om alle gegevens uit de lijst te verwijderen, klikt u op de knop **Lijst wissen** en vervolgens op **Ja** om te bevestigen.

U kunt de spammerslijst opslaan naar een bestand zodat u het kunt gebruiken op een andere computer of na het opnieuw installeren van het product. Om de spammerslijst op te slaan, klikt u op de knop **Opslaan** en slaat u het op naar de gewenste locatie. Het bestand zal de extensie **.bwl** hebben.

Om een eerder opgeslagen Spammerslijst te laden, klikt u op de knop **Laden** en opent u het overeenkomende **bwl**-bestand. Om de inhoud van de huidige lijst opnieuw in te stellen wanneer u een eerder opgeslagen lijst laadt, selecteert u **De huidige lijst overschrijven**.

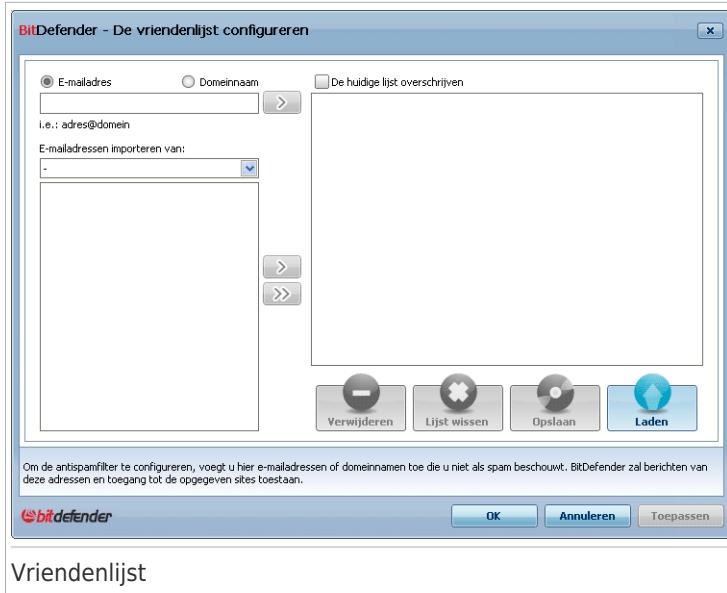
Klik op **Toepassen** en **OK** om de **Spammerslijst** op te slaan en te sluiten.

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




Opmerking

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



Vriendenlijst


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

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



Belangrijk

Syntaxis: naam@domein.com.

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



Belangrijk



Syntaxis:

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

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

Mail, selecteert u de overeenkomende optie in het afrolmenu **E-mailadressen importeren van**.

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

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

Om een item uit de lijst te verwijderen, selecteert u het item en klikt u op de knop **Verwijderen**. Om alle gegevens uit de lijst te verwijderen, klikt u op de knop **Lijst wissen** en vervolgens op **Ja** om te bevestigen.

U kunt de vriendenlijst opslaan naar een bestand zodat u het kunt gebruiken op een andere computer of na het opnieuw installeren van het product. Om de vriendenlijst op te slaan, klikt u op de knop **Opslaan** en slaat u het op naar de gewenste locatie. Het bestand zal de extensie **.bwl** hebben.

Om een eerder opgeslagen vriendenlijst te laden, klikt u op de knop **Laden** en opent u het overeenkomende bwl-bestand. Om de inhoud van de huidige lijst opnieuw in te stellen wanneer u een eerder opgeslagen lijst laadt, selecteert u **De huidige lijst overschrijven**.

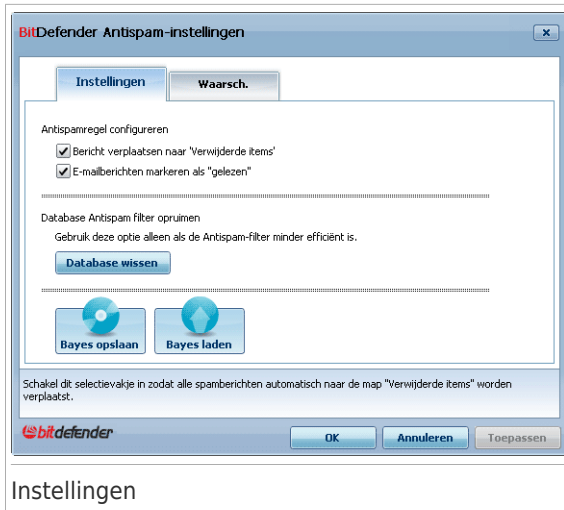


Opmerking

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

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

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



De volgende opties zijn beschikbaar:

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

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

U kunt de Bayes-database opslaan naar een bestand zodat u het kunt gebruiken met een ander BitDefender-product of na het opnieuw installeren van BitDefender. Om de Bayes-database op te slaan, klikt u op de knop **Bayes opslaan** en slaat u het op naar de gewenste locatie. Het bestand zal de extensie **.dat** hebben.

Om een eerder opgeslagen Bayes-database te laden, klikt u op de knop **Bayes laden** en opent u het overeenkomende bestand.

Klik op het tabblad **Waarschu.** als u het gedeelte wilt openen waar u de weergave van bevestigingsvensters kan uitschakelen voor de knoppen **Spammer toevoegen** en **Vriend toevoegen**.



Opmerking

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

-  **Wizard** - opent de wizard voor het configureren van antispam, die u zal helpen de Bayes-filter op te leiden om de efficiëntie van de Antispam-filter van BitDefender verder te verbeteren. U kunt ook adressen van uw Adresboek toevoegen aan uw Vriendenlijst / Spammerslijst.
-  **BitDefender Antispam** - opent de BitDefender gebruikersinterface.

Zo werkt het

33. 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. 57) voor gedetailleerde informatie over deze wizard.

33.1. 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.

33.2. 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 **Beveiliging**.
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.

33.3. 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.



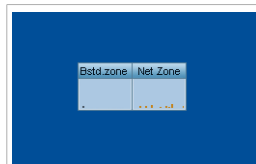
Opmerking

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.

33.4. 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.



Scan activiteitenbalk



Opmerking

Raadpleeg "*Scan activiteitenbalk*" (p. 33) voor meer informatie.

34. 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.
- Gebruikerstaken 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

35. 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. 338).

35.1. 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.

35.1.1. 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.	<p>Om de installatiewizard uit te voeren en BitDefender te installeren, hebt u beheerdersbevoegdheden nodig. Voer een van de volgende bewerkingen uit:</p> <ul style="list-style-type: none"> ● 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.	<p>toestand blokkeert een nieuwe installatie van BitDefender.</p> <p>Volg deze stappen om deze fout op te lossen en BitDefender te installeren:</p> <ol style="list-style-type: none"> 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.	<p>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.</p> <p>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.</p>
Het installatiebestand is ontworpen voor een ander type processor.	<p>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.</p> <p>Download het installatiebestand direct van www.bitdefender.com om zeker te zijn dat u de juiste versie voor uw systeem hebt.</p>

35.1.2. 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. 341).

- 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. 338).

35.2. 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. 338).

35.3. Het delen van een bestand en printer in een Wi-Fi-netwerk (draadloos) werkt niet

Dit artikel helpt u bij het oplossen van de volgende problemen met de firewall van BitDefender in Wi-Fi-netwerken:

- Kan geen bestanden delen met computers in het Wi-Fi-netwerk.
- Kan geen toegang krijgen tot een netwerkprinter die verbonden is met het Wi-Fi-netwerk.
- Kan geen toegang krijgen tot de printer die wordt gedeeld door een computer in het Wi-Fi-netwerk.
- Kan uw printer niet delen met computers in het Wi-Fi-netwerk.

Voordat u begint met het oplossen van deze problemen, moet u enkele zaken weten over beveiliging en de configuratie van de BitDefender-firewall in Wi-Fi-netwerken. Op het vlak van beveiliging vallen Wi-Fi-netwerken in een van deze categorieën.

- **Beveiligde Wi-Fi-netwerken.** Met dit type netwerk kunnen alleen gemachtigde Wi-Fi-apparaten een verbinding maken. De netwerktoegang is afhankelijk van een wachtwoord. Beveiligde Wi-Fi-netwerken zijn bijvoorbeeld netwerken die in kantoornetwerken zijn ingesteld.
- **Wi-Fi-netwerken openen (onbeveiligd).** Elk Wi-Fi-apparaat binnen het bereik van een onbeveiligd Wi-Fi-netwerk kan vrij een verbinding maken met dit netwerk. Onbeveiligde Wi-Fi-netwerken worden op grote schaal gebruikt. Ze omvatten bijna elk openbaar Wi-Fi-netwerk (zoals netwerken op campussen, koffiehuisen, luchthavens, en andere). Ook een thuisnetwerk dat u instelt met een draadloze router is onbeveiligd tot u de beveiliging op de router activeert.

Onbeveiligde Wi-Fi-netwerken vormen een groot beveiligingsrisico omdat uw computer verbonden is met onbekende computers. Zonder de goede bescherming die door een firewall wordt geleverd, kan iedereen die met het netwerk is verbonden, toegang krijgen tot uw gedeelde objecten en zelfs inbreken in uw computer.

Wanneer een verbinding wordt gemaakt met een onbeveiligd Wi-Fi-netwerk, blokkeert BitDefender automatisch de communicatie met de computers in dit netwerk. U kunt alleen toegang krijgen tot internet, maar u kunt geen bestanden of een printer delen met andere gebruikers in het netwerk.

Om de communicatie met een Wi-Fi-netwerk in te schakelen, zijn er twee oplossingen:

- De oplossing "**vertrouwde computer**" maakt het delen van bestanden en printers alleen mogelijk met specifieke computers (vertrouwde computers) in het Wi-Fi-netwerk. Gebruik deze oplossing wanneer u verbonden bent met een openbaar Wi-Fi-netwerk (bijv. een netwerk op een campus of in een koffiewinkel)

en als u bestanden of een printer wilt delen met een vriend of als u toegang wenst tot een Wi-Fi-netwerkprinter.

- Met de oplossing "**veilig netwerk**" kunt u bestanden en printers delen voor het volledige Wi-Fi-netwerk (veilig netwerk). Deze oplossing is niet aanbevolen vanwege beveiligingsredenen, maar kan nuttig zijn in specifieke situaties (u kunt deze oplossing bijvoorbeeld gebruiken voor een Wi-Fi-netwerk thuis of op kantoor).

35.3.1. Oplossing "Vertrouwde computer"

Volg deze stappen om de BitDefender-firewall te configureren voor het delen van bestanden en printers met een computer in het Wi-Fi-netwerk of om toegang te krijgen tot een Wi-Fi-netwerkprinter:

1. Open BitDefender en schakel de gebruikersinterface naar de Expert-modus.
2. Klik in het menu aan de linkerzijde op **Firewall**.
3. Klik op het tabblad **Network**.
4. Selecteer het Wi-Fi-netwerk in de tabel Zones en klik vervolgens op de knop  **Toevoegen**.
5. Selecteer de gewenste computer of de Wi-Fi-netwerkprinter in de lijst van apparaten die in het Wi-Fi-netwerk zijn gedetecteerd. Als die computer of printer niet automatisch wordt gedetecteerd, kunt u het IP-adres van het apparaat invoeren in het veld **Zone**.
6. Selecteer de actie **Toestaan**.
7. Klik op **OK**.

Als u nog steeds geen bestanden of printers kunt delen met de geselecteerde computer, wordt dit zeer waarschijnlijk niet veroorzaakt door de BitDefender-firewall op uw computer. Controleer op andere potentiële oorzaken, zoals hieronder:

- De firewall op de andere computer kan het delen van bestanden en printers delen in onbeveiligde (openbare) Wi-Fi-netwerken.
 - ▶ Als de firewall van een BitDefender 2009- of BitDefender 2010-product, moet dezelfde procedure worden gevolgd op de andere computer zodat het delen van bestanden en printers op uw computer wordt toegestaan.
 - ▶ Als de Windows Firewall wordt gebruikt, kan deze worden geconfigureerd om het delen van bestanden en printers als volgt toe te staan: open het venster met de instellingen van de Windows Firewall, klik op het tabblad **Uitzonderingen** en schakel het selectievakje **Bestands- en printerdeling** in.
 - ▶ Als er een ander firewall-programma wordt gebruikt, moet u de documenten of het Help-bestand van dit programma raadplegen.

- Algemene omstandigheden die het gebruik van of verbinden met de gedeelde printer kunnen verhinderen:
 - ▶ U moet zich mogelijk aanmelden bij een Windows-beheerdersaccount om toegang te krijgen tot de gedeelde printer.
 - ▶ Er zijn machtigingen ingesteld voor de gedeelde printer om de toegang alleen toe te staan tot specifieke computers en gebruikers. Als u uw printer deelt, moet u de machtigingen controleren die voor de printer zijn ingesteld om te zien of de gebruiker op de andere computer toegang heeft tot de printer. Als u probeert een verbinding te maken met een gedeelde printer, moet u bij de gebruiker op de andere computer controleren of u de machtiging hebt om een verbinding te maken met de printer.
 - ▶ De printer die op uw computer of op de andere computer is aangesloten, wordt niet gedeeld.
 - ▶ De gedeelde printer is niet toegevoegd aan de computer.



Opmerking

Om te leren hoe u het delen van printers kunt beheren (een printer delen, machtigingen voor een printer instellen of verwijderen, verbinden met een netwerkprinter of met een gedeelde printer), gaat u naar Windows Help en ondersteuning (klik in het menu Start op **Help en ondersteuning**).

Als u nog steeds geen toegang kunt krijgen tot de Wi-Fi-netwerkprinter, is dit zeer waarschijnlijk niet veroorzaakt door de BitDefender-firewall op uw computer. De toegang tot de Wi-Fi-netwerkprinter is mogelijk beperkt tot specifieke computers of gebruikers. Raadpleeg de beheerder van het Wi-Fi-netwerk om uit te vinden of u de machtiging hebt om een verbinding te maken met die printer.

Als u vermoedt dat het probleem te maken heeft met de BitDefender-firewall, kunt u contact opnemen met BitDefender voor ondersteuning, zoals beschreven in het gedeelte "*Supportcentrum*" (p. 338).

35.3.2. Oplossing "Veilig netwerk"

Het is aanbevolen deze oplossing alleen te gebruiken voor Wi-Fi-netwerken thuis of op kantoor.

Volg deze stappen om de BitDefender-firewall te configureren om het delen van bestanden printers met het volledige Wi-Fi-netwerk toe te staan:

1. Open BitDefender en schakel de gebruikersinterface naar de Expert-modus.
2. Klik in het menu aan de linkerkant op **Firewall**.
3. Klik op het tabblad **Netwerk**.
4. Klik in de tabel Netwerkconfiguratie in de kolom **Vertrouwheidsniveau** op de pijl ▼ in de cel die overeenkomt met het Wi-Fi-netwerk.

5. Afhankelijk van het beveiligingsniveau dat u wilt verkrijgen, kiest u een van de volgende opties:

- **Onveilig** - om toegang te krijgen tot de bestanden en printers die in het Wi-Fi-netwerk worden gedeeld, zonder hierbij toegang toe te staan tot uw gedeelde items.
- **Veilig** - om het delen van bestanden en printers in beide richtingen toe te staan. Dit betekent dat de gebruikers die op het Wi-Fi-netwerk zijn aangesloten, ook toegang kunnen krijgen tot uw gedeelde bestanden of printer.

Als u nog steeds geen bestanden of printers kunt delen met specifieke computers in het Wi-Fi-netwerk, wordt dit zeer waarschijnlijk niet veroorzaakt door de BitDefender-firewall op uw computer. Controleer op andere potentiële oorzaken, zoals hieronder:

- De firewall op de andere computer kan het delen van bestanden en printers delen in onbeveiligde (openbare) Wi-Fi-netwerken.
 - ▶ Als de firewall van een BitDefender 2009- of BitDefender 2010-product, moet dezelfde procedure worden gevolgd op de andere computer zodat het delen van bestanden en printers op uw computer wordt toegestaan.
 - ▶ Als de Windows Firewall wordt gebruikt, kan deze worden geconfigureerd om het delen van bestanden en printers als volgt toe te staan: open het venster met de instellingen van de Windows Firewall, klik op het tabblad **Uitzonderingen** en schakel het selectievakje **Bestands- en printerdeling** in.
 - ▶ Als er een ander firewall-programma wordt gebruikt, moet u de documenten of het Help-bestand van dit programma raadplegen.
- Algemene omstandigheden die het gebruik van of verbinden met de gedeelde printer kunnen verhinderen:
 - ▶ U moet zich mogelijk aanmelden bij een Windows-beheerdersaccount om toegang te krijgen tot de gedeelde printer.
 - ▶ Er zijn machtigingen ingesteld voor de gedeelde printer om de toegang alleen toe te staan tot specifieke computers en gebruikers. Als u uw printer deelt, moet u de machtigingen controleren die voor de printer zijn ingesteld om te zien of de gebruiker op de andere computer toegang heeft tot de printer. Als u probeert een verbinding te maken met een gedeelde printer, moet u bij de gebruiker op de andere computer controleren of u de machtiging hebt om een verbinding te maken met de printer.
 - ▶ De printer die op uw computer of op de andere computer is aangesloten, wordt niet gedeeld.
 - ▶ De gedeelde printer is niet toegevoegd aan de computer.



Opmerking

Om te leren hoe u het delen van printers kunt beheren (een printer delen, machtigingen voor een printer instellen of verwijderen, verbinden met een netwerkprinter of met een gedeelde printer), gaat u naar Windows Help en ondersteuning (klik in het menu Start op **Help en ondersteuning**).

Als u nog steeds geen toegang kunt krijgen tot een Wi-Fi-netwerkprinter, is dit zeer waarschijnlijk niet veroorzaakt door de BitDefender-firewall op uw computer. De toegang tot de Wi-Fi-netwerkprinter is mogelijk beperkt tot specifieke computers of gebruikers. Raadpleeg de beheerder van het Wi-Fi-netwerk om uit te vinden of u de machtiging hebt om een verbinding te maken met die printer.

Als u vermoedt dat het probleem te maken heeft met de BitDefender-firewall, kunt u contact opnemen met BitDefender voor ondersteuning, zoals beschreven in het gedeelte "*Supportcentrum*" (p. 338).

35.4. De antispamfilter werkt niet goed

Dit artikel helpt u bij het oplossen van de volgende problemen met betrekking tot de werking van de antispamfilter van BitDefender:

- Een aantal rechtmatige e-mailberichten wordt gemarkeerd als [spam]..
- Talrijke spamberichten worden niet als dusdanig gemarkeerd door de antispam-filter.
- De antispam-filter detecteert geen enkel spambericht.

35.4.1. Rechtmatige berichten worden gemarkeerd als [spam]

Rechtmatige berichten worden als [spam] gemarkeerd omdat ze eruit zien als spam voor de antispamfilter van BitDefender. U kunt dit probleem oplossen door de antispamfilter op de goede manier te configureren.

BitDefender voegt de ontvangers van uw e-mailberichten automatisch toe aan uw vriendenlijst. De e-mailberichten die zijn ontvangen van de contactpersonen in de vriendenlijst, worden beschouwd als rechtmatig. Ze worden niet gecontroleerd door de antispamfilter en worden daarom ook nooit gemarkeerd als [spam].

De automatische configuratie van de vriendenlijst verhindert niet dat er detectiefouten optreden in deze situaties:

- U ontvangt veel gevraagde commerciële e-mail omdat u zich op verschillende websites hebt geabonneerd. In dit geval bestaat de oplossing eruit de e-mailadressen waarvan u dergelijke e-mailberichten ontvangt, toe te voegen aan de vriendenlijst.
- Een belangrijk deel van uw rechtmatige e-mail komt van mensen naar wie u nog nooit een e-mail hebt gestuurd, zoals klanten, potentiële zakenpartners en anderen. In dit geval zijn andere oplossingen vereist.

Als u een van de e-mailclients waarin BitDefender wordt geïntegreerd, kunt u de volgende oplossingen proberen:

1. **Detectiefouten aangeven.** Dit wordt gebruikt om de leermotor (Bayes) van de antispamfilter te trainen en helpt bij het voorkomen van toekomstige detectiefouten. De leermotor analyseert de aangegeven berichten en leert hun patronen. De toekomstige e-mailberichten die aan dezelfde patronen voldoen, zullen niet als [spam] worden gemarkeerd.
2. **Het antispambeschermingsniveau verlagen.** Door het beschermingsniveau te verlagen, zal de antispamfilter meer spamaanduidingen nodig hebben om een e-mailbericht als spam te klasseren. Probeer deze oplossing alleen als er veel rechtmatige berichten (inclusief gevraagde commerciële berichten) onjuist worden gedetecteerd als spam.
3. **De leermotor (Bayes) opnieuw opleiden.** Probeer deze oplossing alleen als de voorgaande oplossingen geen bevredigende resultaten boden.




Opmerking

BitDefender wordt geïntegreerd in de vaakst gebruikte e-mailclients via een gemakkelijk te gebruiken antispamwerkbalk. Raadpleeg "*Ondersteunde software*" (p. 2) voor een complete lijst van ondersteunde e-mailclients.

Als u een andere e-mailclient gebruikt, kunt u geen detectiefouten aanduiden of geen leermotor aanleren. Om het probleem op te lossen, kunt u proberen het antispambeveiligingsniveau te verlagen.

Contactpersonen toevoegen aan de vriendenlijst


Als u een ondersteunde e-mailclient gebruikt, kunt u de afzenders van rechtmatige berichten gemakkelijk toevoegen aan de vriendenlijst. Volg deze stappen:

1. Selecteer in uw e-mailclient een e-mailbericht van de afzender die u wilt toevoegen aan de vriendenlijst.
2. Klik op de knop  **Vriend toevoegen** in de antispam-werkbalk van BitDefender.
3. U wordt gevraagd de adressen die aan de vriendenlijst zijn toegevoegd, te bevestigen. Selecteer **Dit bericht niet meer weergeven** en klik op **OK**.

U ontvangt alle e-mailberichten van dit adres, ongeacht hun inhoud.

Als u een andere e-mailclient gebruikt, kunt u contactpersonen toevoegen aan de vriendenlijst vanaf de BitDefender-interface. Volg deze stappen:

1. Open BitDefender en schakel de gebruikersinterface naar de Expert-modus.
2. Klik in het menu aan de linkerkzijde op **Antispam**.
3. Klik op het tabblad **Status**.
4. Klik op **Vrienden beheren**. Een configuratievenster wordt weergegeven.

5. Typ het e-mailadres waarvan u altijd e-mailberichten wilt ontvangen en klik op de knop  om het adres toe te voegen aan de vriendenlijst.
6. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

Detectiefouten aangeven

Als u een ondersteunde e-mailclient gebruikt, kunt u de antispamfilter gemakkelijk corrigeren (door aan te geven welke e-mailberichten niet zijn gemarkeerd als [spam]). Hierdoor zult u de efficiëntie van de antispamfilter aanzienlijk verbeteren. Volg deze stappen:

1. Open uw e-mailclient.
2. Ga naar de map met ongewenste e-mails waar uw spamberichten zijn geplaatst.
3. Selecteer het rechtmatige bericht dat door BitDefender verkeerdelijk is gemarkeerd als [spam].
4. Klik op de knop  **Vriend toevoegen** in de antispam-werkbalk van BitDefender om de afzender aan de vriendenlijst toe te voegen. U zult mogelijk op **OK** moeten klikken om te bevestigen. U ontvangt alle e-mailberichten van dit adres, ongeacht hun inhoud.
5. Klik op de knop  **Geen spam** in de antispamwerkbalk van BitDefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient). Dit geeft aan de leermotor aan dat het geselecteerde bericht geen spam is. Het e-mailbericht wordt verplaatst naar de map Postvak IN. De toekomstige e-mailberichten die aan dezelfde patronen voldoen, zullen niet langer als [spam] worden gemarkeerd.

Het antispambeschermingsniveau verlagen

Volg deze stappen om het antispambeschermingsniveau te verlagen:

1. Open BitDefender en schakel de gebruikersinterface naar de Expert-modus.
2. Klik in het menu aan de linkerzijde op **Antispam**.
3. Klik op het tabblad **Status**.
4. Verplaats de schuifregelaar omlaag op de schaal.

Het is aanbevolen de bescherming met slechts één niveau te dalen en dan lang genoeg te wachten om de resultaten te evalueren. Als er veel rechtmatige e-mailberichten nog steeds worden gemarkeerd als [spam], kunt u het beschermingsniveau verder verlagen. Als u merkt dat er veel spamberichten niet worden gedetecteerd, mag u het beschermingsniveau niet verlagen.

De leermotor (Bayes) opnieuw opleiden

Voordat u de leermotor (Bayes) aanleert, bereidt u een map voor die alleen SPAM-berichten bevat en een map die alleen rechtmatige berichten bevat. De leermotor zal ze analyseren en de kenmerken leren die de spam- of rechtmatige berichten die u doorgaans ontvangt, definiëren. Voor een efficiënt resultaat van de opleiding, moeten er meer dan 50 berichten in elke categorie zijn.

Volg deze stappen om de Bayes-database opnieuw in te stellen en de leermotor opnieuw op te leiden:

1. Open uw e-mailclient.
2. Klik in de antispambalk van BitDefender op de knop  **Wizard** om de wizard voor de antispamconfiguratie te starten. Gedetailleerde informatie over deze wizard vindt u in de sectie *“Configuratiewizard voor Antispam”* (p. 298).
3. Klik op **Volgende**.
4. Selecteer **Deze stap overslaan** en klik op **Volgende**.
5. Selecteer **Database antispamfilter opruimen** en klik op **Volgende**.
6. Selecteer de map die de rechtmatige berichten bevat en klik op **Volgende**.
7. Selecteer de map die de SPAM-berichten bevat en klik op **Volgende**.
8. Klik op **Voltooien** om het opleidingsproces te starten.
9. Klik op **Sluiten** wanneer de opleiding is voltooid.

Hulp vragen

Als deze informatie niet nuttig was, kunt u contact opnemen met BitDefender voor ondersteuning, zoals beschreven in de sectie *“Supportcentrum”* (p. 338).

35.4.2. Er worden veel spamberichten niet gedetecteerd

Als u veel spamberichten ontvangt die niet als [spam] zijn gemarkeerd, moet u de antispamfilter van BitDefender configureren om de efficiëntie te verbeteren.

Als u een van de e-mailclients waarin BitDefender wordt geïntegreerd, kunt u de volgende oplossingen één voor één proberen:

1. **Niet-gedetecteerde spamberichten aangeven**. Dit wordt gebruikt om de leermotor (Bayes) van de antispamfilter te trainen en verbetert doorgaans de antispamdetectie. De leermotor analyseert de aangegeven berichten en leert hun patronen. De toekomstige e-mailberichten die aan dezelfde patronen voldoen, zullen als [spam] worden gemarkeerd.
2. **Spammers toevoegen aan de spammerslijst**. De e-mailberichten die zijn ontvangen van adressen in de spammerslijst, worden automatisch gemarkeerd als [spam].

3. **Het antispambeschermingsniveau verhogen.** Door het beschermingsniveau te verhogen, zal de antispamfilter minder spamaanduidingen nodig hebben om een e-mailbericht als spam te klasseren.
4. **De leermotor (Bayes) opnieuw opleiden.** Gebruik deze oplossing wanneer de antispamdetectie meer dan onbevredigend is en het aanduiden van niet-gedetecteerde spamberichten niet langer werkt.



Opmerking

BitDefender wordt geïntegreerd in de vaakst gebruikte e-mailclients via een gemakkelijk te gebruiken antispamwerkbalk. Raadpleeg "*Ondersteunde software*" (p. 2) voor een complete lijst van ondersteunde e-mailclients.

Als u een andere e-mailclient gebruikt, kunt u geen spamberichten aanduiden of geen leermotor aanleren. Om het probleem op te lossen, moet u proberen het antispambeschermingsniveau te verhogen en spammers toe te voegen aan de spammerslijst.


Niet-gedetecteerde spamberichten aangeven

Als u een ondersteunde e-mailclient gebruikt, kunt u gemakkelijk aanduiden welke e-mailberichten niet als spam moeten worden gedetecteerd. Hierdoor zult u de efficiëntie van de antispamfilter aanzienlijk verbeteren. Volg deze stappen:

1. Open uw e-mailclient.
2. Ga naar de map Postvak IN.
3. Selecteer de niet-gedetecteerde spamberichten.
4. Klik op de knop  **Is spam** in de antispamwerkbalk van BitDefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient). Dit geeft aan de leermotor aan dat de geselecteerde berichten spam zijn. Ze worden onmiddellijk als [spam] gemarkeerd en naar de map met ongewenste e-mail verplaatst. De toekomstige e-mailberichten die aan dezelfde patronen voldoen, zullen als [spam] worden gemarkeerd.

Spammers toevoegen aan de spammerslijst

Als u een ondersteunde e-mailclient gebruikt, kunt u de afzenders van de spamberichten gemakkelijk toevoegen aan de spammerslijst. Volg deze stappen:

1. Open uw e-mailclient.
2. Ga naar de map met ongewenste e-mails waar uw spamberichten zijn geplaatst.
3. Selecteer de berichten die door BitDefender zijn gemarkeerd als [spam].
4. Klik op de knop  **Spammer toevoegen** in de antispam-werkbalk van BitDefender.

5. U wordt gevraagd de adressen die aan de spammerslijst zijn toegevoegd, te bevestigen. Selecteer **Dit bericht niet meer weergeven** en klik op **OK**.

Als u een andere e-mailclient gebruikt, kunt u spammers handmatig toevoegen aan de spammerslijst vanaf de BitDefender-interface. Het is handig om dit alleen te doen wanneer u meerdere spamberichten hebt ontvangen van hetzelfde e-mailadres. Volg deze stappen:

1. Open BitDefender en schakel de gebruikersinterface naar de Expert-modus.
2. Klik in het menu aan de linkerzijde op **Antispam**.
3. Klik op het tabblad **Status**.
4. Klik op **Spammers beheren**. Een configuratievenster wordt weergegeven.
5. Typ het e-mailadres van de spammer en klik op de knop  om het adres toe te voegen aan de Spammerslijst.
6. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

Het antispambeschermingsniveau verhogen


Volg deze stappen om het antispambeschermingsniveau te verhogen:

1. Open BitDefender en schakel de gebruikersinterface naar de Expert-modus.
2. Klik in het menu aan de linkerzijde op **Antispam**.
3. Klik op het tabblad **Status**.
4. Verplaats de schuifregelaar omhoog op de schaal.

De leermotor (Bayes) opnieuw opleiden

Voordat u de leermotor (Bayes) aanleert, bereidt u een map voor die alleen SPAM-berichten bevat en een map die alleen rechtmatige berichten bevat. De leermotor zal ze analyseren en de kenmerken leren die de spam- of rechtmatige berichten die u doorgaans ontvangt, definiëren. Voor een efficiënt resultaat van de opleiding, moeten er meer dan 50 berichten in elke categorie zijn.

Volg deze stappen om de Bayes-database opnieuw in te stellen en de leermotor opnieuw op te leiden:

1. Open uw e-mailclient.
2. Klik in de antispambalk van BitDefender op de knop  **Wizard** om de wizard voor de antispamconfiguratie te starten. Gedetailleerde informatie over deze wizard vindt u in de sectie *"Configuratiewizard voor Antispam"* (p. 298).
3. Klik op **Volgende**.
4. Selecteer **Deze stap overslaan** en klik op **Volgende**.
5. Selecteer **Database antispamfilter opruimen** en klik op **Volgende**.

6. Selecteer de map die de rechtmatige berichten bevat en klik op **Volgende**.
7. Selecteer de map die de SPAM-berichten bevat en klik op **Volgende**.
8. Klik op **Voltooien** om het opleidingsproces te starten.
9. Klik op **Sluiten** wanneer de opleiding is voltooid.

Hulp vragen

Als deze informatie niet nuttig was, kunt u contact opnemen met BitDefender voor ondersteuning, zoals beschreven in de sectie *"Supportcentrum"* (p. 338).

35.4.3. De antispamfilter detecteert geen spamberichten

Als er een spambericht als [spam] is gemarkeerd, kan er een probleem zijn met de antispamfilter van BitDefender. Voordat u dit probleem probeert op te lossen, moet u controleren of het niet wordt veroorzaakt door een van de volgende omstandigheden:

- De antispambeveiliging van BitDefender is alleen beschikbaar voor e-mailclients die geconfigureerd zijn om e-mailberichten te ontvangen via het POP3-protocol. Dit betekent het volgende:
 - ▶ E-mailberichten die zijn ontvangen via op het web gebaseerde e-mailservices (zoals Yahoo, Gmail, Hotmail of andere), worden op spam gefilterd door BitDefender.
 - ▶ Als uw e-mailclient is geconfigureerd om e-mailberichten te ontvangen met een ander protocol dan POP3 (bijv. IMAP4), controleert de antispamfilter van BitDefender deze berichten niet op spam.



Opmerking

POP3 is een van de op grootste schaal gebruikte protocollen voor het downloaden van e-mailberichten van een e-mailserver. Als u het protocol dat uw e-mailclient gebruikt om e-mailberichten te downloaden niet kent, kunt u dat vragen aan de persoon die uw e-mailclient heeft geconfigureerd.

- BitDefender Internet Security 2010 scant geen POP3-verkeer van Lotus Notes.

U moet ook de volgende mogelijke oorzaken controleren:

1. Zorg dat Antispam is ingeschakeld.
 - a. BitDefender openen.
 - b. Klik in de rechterbovenhoek van het venster op **Instellingen**.
 - c. Controleer de antispam-status in de categorie Beveiligingsinstellingen.

Als Antispam is uitgeschakeld, is dit de oorzaak van uw probleem. Schakel Antispam in en controleer de antispam-werking om te zien of het probleem is opgelost.

2. Hoewel het zeer onwaarschijnlijk is, is het misschien aanbevolen te controleren of u (of iemand anders) BitDefender hebt geconfigureerd om spamberichten niet als [spam] te markeren.
 - a. Open BitDefender en schakel de gebruikersinterface naar de Expert-modus.
 - b. Klik in het menu aan de linkerzijde op **Antispam** en klik vervolgens op het tabblad **Instellingen**.
 - c. Zorg dat de optie **Spamberichten in onderwerp markeren** is geselecteerd.

Een mogelijke oplossing is het repareren of opnieuw installeren van het product. Het is echter mogelijk dat u contact wilt opnemen met BitDefender voor ondersteuning, zoals beschreven in sectie "*Supportcentrum*" (p. 338).

35.5. 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. 338).

36. 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

37. Overzicht

BitDefender Internet Security 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/

37.1. 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.

37.2. 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](#).

38. 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.

38.1. 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.



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

38.2. 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.

38.3. 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.

```
# bdscan /path/to/scan/
```

38.4. 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.

38.5. Hoe kan ik BitDefender updaten?

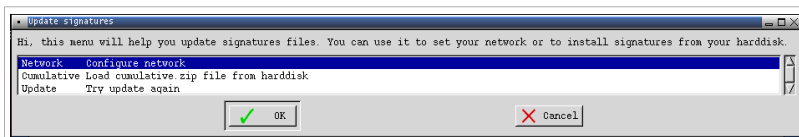
Bij het opstarten wordt de update van de virushandtekeningen automatisch uitgevoerd. Als u deze stap echter hebt overgeslagen of als u gewoon een update wilt uitvoeren na het opstarten, kunt u een van de deze werkwijzen volgen.

● 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**.

38.5.1. 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**.

38.6. 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.



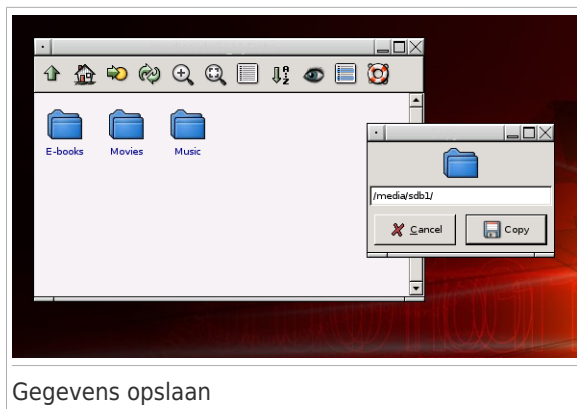
Belangrijk

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.

38.7. 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.