

# TOTAL SECURITY 2013



Bitdefender®

Handleiding

## Bitdefender Total Security 2013 *Handleiding*

Publication date 07/17/2012

Copyright© 2012 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 als de bron van het citaat wordt vermeld. De inhoud mag op geen enkele manier worden gewijzigd.

**Waarschuwing en ontkenning.** Dit product en de bijbehorende documentatie worden beschermd door copyright. De informatie in dit document wordt verschaft "zoals hij is", zonder enige garantie. Hoewel er alle voorzorgsmaatregelen zijn genomen bij de voorbereiding van dit document, hebben de auteurs geen enkele wettelijke verantwoordelijkheid aan welke persoon of entiteit dan ook met betrekking tot enig verlies of schade, direct of indirect veroorzaakt of vermeend veroorzaakt door de gegevens in dit werk.

Dit boek bevat links naar websites van derden die niet onder het beheer van Bitdefender staan. Bitdefender is daarom niet verantwoordelijk voor de inhoud van deze gelinkte sites. Als u een website van derden die in dit document is vermeld bezoekt, doet u dit op eigen risico. Bitdefender verschaft deze links enkel voor uw gemak en het opnemen van de link houdt niet in dat Bitdefender de inhoud van de site van de derde partij onderschrijft of er enige verantwoordelijkheid voor accepteert.

**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

Installatie .....	1
1. Voorbereiden voor installatie .....	2
2. Systeemvereisten .....	3
2.1. Minimale systeemvereisten .....	3
2.2. Aanbevolen systeemvereisten .....	3
2.3. Softwarevereisten .....	3
3. Installatieschema's .....	5
4. Uw Bitdefender-product installeren .....	6
Aan de slag .....	12
5. De basisfuncties .....	13
5.1. Open het Bitdefender-venster .....	13
5.2. Problemen aan het oplossen .....	13
5.2.1. Wizard alle problemen herstellen .....	14
5.2.2. Statuswaarschuwingen configureren .....	15
5.3. Gebeurtenissen .....	16
5.4. Autopilot .....	17
5.5. Spelmodus en Laptop-modus .....	18
5.5.1. Spelmodus .....	18
5.5.2. Laptop-modus .....	20
5.6. Wachtwoordbeveiligde Bitdefender-instellingen .....	20
5.7. Anonieme gebruiksrapporten .....	21
6. Bitdefender-interface .....	23
6.1. Systeemvakpictogram .....	23
6.2. Hoofdvenster .....	24
6.2.1. Werkbalk boven .....	25
6.2.2. Panelengebied .....	26
6.3. Venster Overzicht instellingen .....	30
6.4. Beveiligingswidget .....	31
6.4.1. Bestanden en mappen scannen .....	33
6.4.2. Beveiligingswidget tonen/verbergen .....	33
7. Bitdefender registreren .....	34
7.1. Uw licentiesleutel invoeren .....	34
7.2. Licentiesleutels kopen of vernieuwen .....	35
8. MyBitdefender-account .....	36
8.1. Uw computer koppelen met MyBitdefender .....	37
9. Bitdefender up-to-date houden .....	39
9.1. Controleren of Bitdefender up-to-date is .....	39
9.2. Een update uitvoeren .....	40
9.3. De automatische update in- of uitschakelen .....	40

9.4. De update-instellingen aanpassen .....	41
<b>Zo werkt het .....</b>	<b>43</b>
10. Installatie .....	44
10.1. Hoe installeer ik Bitdefender op een tweede computer? .....	44
10.2. Wanneer moet ik Bitdefender opnieuw installeren? .....	44
10.3. Hoe kan ik schakelen van het ene Bitdefender 2013-product naar het andere? .....	45
11. Registratie .....	46
11.1. Welk Bitdefender-product gebruik ik? .....	46
11.2. Een evaluatieversie registreren .....	46
11.3. Wanneer verloopt mijn Bitdefender-bescherming? .....	46
11.4. Hoe kan ik Bitdefender registreren zonder internetverbinding? .....	47
11.5. Hoe kan ik mijn Bitdefender-beveiliging vernieuwen? .....	47
12. Scannen met Bitdefender .....	49
12.1. Een bestand of map scannen .....	49
12.2. Hoe kan ik mijn systeem scannen? .....	49
12.3. Een aangepaste scantaak maken .....	49
12.4. Een map uitsluiten van de scan .....	50
12.5. Wat moet ik doen wanneer Bitdefender een schoon bestand als geïnfecteerd beschouwt? .....	51
12.6. Hoe kan ik controleren welke virussen Bitdefender heeft gedetecteerd? .....	51
13. Ouderlijk Toezicht .....	53
13.1. Mijn kinderen beschermen tegen online bedreigingen .....	53
13.2. Hoe kan ik de internettoegang beperken voor mijn kind? .....	53
13.3. Hoe blokkeer ik de toegang van mijn kind tot een website? .....	54
13.4. Hoe verhinder ik dat mijn kind een spel speelt? .....	55
13.5. Windows-gebruikersaccounts maken .....	55
14. Privacybeheer .....	57
14.1. Hoe kan ik controleren of mij online transactie beveiligd is? .....	57
14.2. Wat kan ik doen als mijn systeem gestolen wordt? .....	57
14.3. Hoe kan ik mijn Facebook-account beschermen? .....	58
14.4. Bestandskluisen gebruiken .....	58
14.5. Hoe kan ik een bestand definitief verwijderen met Bitdefender? .....	60
15. Tune-up .....	61
15.1. Mijn systeemprestaties verbeteren .....	61
15.1.1. Uw harde schijf defragmenteren .....	61
15.1.2. Uw pc opruimen .....	61
15.1.3. Windows-register opruimen .....	62
15.1.4. Scan uw systeem periodiek .....	62
16. Online back-up Safebox .....	63
16.1. Hoe kan ik vanaf een andere computer toegang krijgen tot mijn back-upbestanden? .....	63
16.2. Hoe kan ik bestanden delen met mijn vrienden? .....	63
16.3. Waar kan ik de resterende ruimte op mijn Safebox zien? .....	63

16.4. Hoe maak ik ruimte vrij op mijn Safebox? .....	64
<b>17. Nuttige informatie .....</b>	<b>65</b>
17.1. Hoe kan ik de computer automatisch afsluiten nadat het scannen is voltooid? .....	65
17.2. Bitdefender configureren voor het gebruik van een proxy-internetverbinding .....	65
17.3. Gebruik ik een 32- of 64-bits versie van Windows? .....	66
17.4. Verborgen objecten weergeven in Windows .....	67
17.5. Andere beveiligingsoplossingen verwijderen .....	67
17.6. Systeemherstel gebruiken in Windows .....	68
17.7. Opnieuw opstarten in Veiilige modus .....	69

## **Uw beveiliging beheren .....**

**70**

<b>18. Antivirusbeveiliging .....</b>	<b>71</b>
18.1. Scannen bij toegang (real time-beveiliging) .....	72
18.1.1. De real time-beveiliging in- of uitschakelen .....	72
18.1.2. Het real time-beveiligingsniveau aanpassen .....	73
18.1.3. De instellingen voor de realtime beveiliging configureren .....	73
18.1.4. De standaardinstellingen herstellen .....	77
18.2. Scannen op aanvraag .....	77
18.2.1. Autoscan .....	78
18.2.2. Een bestand of map scannen op malware .....	78
18.2.3. Een snelle scan uitvoeren .....	78
18.2.4. Een systeemscan uitvoeren .....	79
18.2.5. Een aangepaste scan configureren .....	79
18.2.6. Antivirusscanwizard .....	82
18.2.7. Scanlogboeken controleren .....	85
18.3. Automatisch scannen van verwisselbare media .....	86
18.3.1. Hoe werkt het? .....	86
18.3.2. Scan verwisselbare media beheren .....	87
18.4. Scanuitsluitingen configureren .....	88
18.4.1. Bestanden of mappen uitsluiten van het scannen .....	88
18.4.2. Bestandsextensies uitsluiten van het scannen .....	89
18.4.3. Scanuitsluitingen beheren .....	90
18.5. Bestanden in quarantaine beheren .....	90
18.6. Actief virusbeheer .....	91
18.6.1. Gedetecteerde toepassingen controleren .....	92
18.6.2. Actief virusbeheer in- of uitschakelen .....	92
18.6.3. De bescherming van Antivirusbeheer aanpassen .....	92
18.6.4. Uitgesloten processen beheren .....	93
18.7. Systeemkwetsbaarheden oplossen .....	94
18.7.1. Uw systeem scannen op kwetsbaarheden .....	94
18.7.2. De automatische kwetsbaarheidsbewaking gebruiken .....	95
<b>19. Antispam .....</b>	<b>98</b>
19.1. Antispam-begrippen .....	99
19.1.1. Antispam-filters .....	99
19.1.2. Antispamgebruik .....	100

19.1.3. Antispam-updates .....	101
19.1.4. Ondersteunde e-mailclients en protocollen .....	101
19.2. De antispambeveiliging in- of uitschakelen .....	101
19.3. De antispam-werkbalk in het venster van uw e-mailclient gebruiken .....	102
19.3.1. Detectiefouten aangeven .....	103
19.3.2. Niet-gedetectedeerde spamberichten aangeven .....	103
19.3.3. Werkbalkinstellingen configureren .....	104
19.4. De Vriendenlijst configureren .....	104
19.5. Spammerslijst configureren .....	105
19.6. Het gevoeligheidsniveau aanpassen .....	106
19.7. De lokale antispamfilters configureren .....	107
19.8. In-the-cloud detectie configureren .....	107
<b>20. Privacybeheer .....</b>	<b>109</b>
20.1. Antiphishing-beveiliging .....	109
20.1.1. Bitdefender-bescherming in de webbrowser .....	111
20.1.2. Bitdefender waarschuwt in de browser .....	112
20.2. IM encryptie .....	112
20.3. Bestandscodering .....	113
20.3.1. Bestandskluisen beheren vanaf de Bitdefender-interface .....	113
20.3.2. Bestandskluisen beheren vanaf Windows .....	118
20.4. Bestanden definitief verwijderen .....	122
<b>21. Firewall .....</b>	<b>124</b>
21.1. De firewall-beveiliging in- of uitschakelen .....	125
21.2. Verbindingsinstellingen beheren .....	125
21.3. Firewall-regels beheren .....	126
21.3.1. Algemene regels .....	126
21.3.2. Toepassingsregels .....	127
21.3.3. Adapterregels .....	130
21.4. De netwerkactiviteit bewaken .....	131
21.5. Intensiteit waarschuwingen configureren .....	132
21.6. Geavanceerde instellingen configureren .....	133
21.6.1. Inbraakdetectiesysteem .....	133
21.6.2. Overige instellingen .....	133
<b>22. Safepay veilige online transacties .....</b>	<b>135</b>
22.1. Bitdefender Safepay gebruiken .....	135
22.2. Instellingen configureren .....	136
22.3. Favorieten beheren .....	136
22.4. Hotspotbeveiliging voor onbeveiligde netwerken .....	137
<b>23. Ouderlijk Toezicht .....</b>	<b>138</b>
23.1. Het dashboard van Ouderlijk toezicht openen .....	138
23.2. Het profiel van uw kind toevoegen .....	139
23.2.1. De activiteit van de kind bewaken .....	139
23.2.2. E-mailmeldingen configureren .....	140
23.3. Ouderlijk toezicht configureren .....	140
23.3.1. Webbeheer .....	141
23.3.2. Toepassings- beheer .....	142
23.3.3. Facebook-beveiliging .....	143

23.3.4. Instant Messaging beheer .....	143
24. Safego-beveiliging voor sociale netwerken .....	145
25. Antidiefstalinstrument .....	147
26. Bitdefender USB Immunizer .....	149
27. Uw computer op afstand beheren .....	150
27.1. MyBitdefender openen .....	150
27.2. Taken uitvoeren op de computers .....	150
<b>Tune-up en back-up .....</b>	<b>152</b>
28. Tune-up .....	153
28.1. Uw PC opruimen .....	153
28.2. Harde schijven defragmenteren .....	154
28.3. Dubbele bestanden zoeken .....	155
28.4. Windows-register opruimen .....	156
28.5. Opgeruimd register herstellen .....	157
28.6. Prestatiebewaking .....	158
29. Online back-up en synchronisatie Safebox .....	159
29.1. Safebox activeren .....	159
29.2. SafeBox beheren vanaf het Bitdefender-venster .....	160
29.3. Safebox beheren vanaf Windows .....	161
29.3.1. Mappen toevoegen aan Safebox .....	161
29.3.2. Mappen uit Safebox verwijderen .....	161
29.3.3. Bestanden die uit Safebox zijn verwijderd, herstellen .....	162
29.4. Safebox beheren vanaf MyBitdefender .....	162
29.5. Bestanden synchroniseren tussen uw computers .....	162
29.6. Uw online ruimte upgraden .....	163
29.7. Bestanden permanent verwijderen .....	163
29.8. Limiet bandbreedte toewijzing .....	164
<b>Problemen oplossen .....</b>	<b>165</b>
30. Algemene problemen oplossen .....	166
30.1. Mijn systeem lijkt traag .....	166
30.2. Het scannen start niet .....	167
30.3. Ik kan de toepassing niet meer gebruiken .....	168
30.4. Ik kan geen verbinding maken met internet .....	169
30.5. Ik kan geen toegang krijgen tot een apparaat op mijn netwerk .....	170
30.6. Mijn internetverbinding is langzaam .....	171
30.7. Bitdefender updaten bij een langzame internetverbinding .....	172
30.8. Mijn computer is niet verbonden met internet. Hoe kan ik Bitdefender updaten? .....	173
30.9. De Bitdefender-services reageren niet .....	173
30.10. De antispamfilter werkt niet goed .....	174
30.10.1. Rechtmatige berichten worden gemarkeerd als [spam] .....	174
30.10.2. Veel spamberichten worden niet gedetecteerd .....	176



30.10.3. De antispamfilter detecteert geen enkel spambericht .....	178
30.11. Het verwijderen van Bitdefender is mislukt .....	179
30.12. Mijn systeem start niet op na het installeren van Bitdefender .....	179
<b>31. Malware van uw systeem verwijderen .....</b>	<b>182</b>
31.1. Helpmodus Bitdefender .....	182
31.2. Wat moet er gebeuren wanneer Bitdefender virussen op uw computer vindt? .....	184
31.3. Een virus in een archief opruimen .....	185
31.4. Een virus in een e-mailarchief opruimen .....	186
31.5. Wat moet ik doen als ik vermoed dat een bestand gevaarlijk is? .....	187
31.6. De geïnfecteerde bestanden van de Systeemvolume-informatie opruimen ..	187
31.7. Wat zijn de wachtwoordbeveiligde bestanden in het scanlogboek? .....	189
31.8. Wat zijn de overgeslagen items in het scanlogboek? .....	189
31.9. Wat zijn de overgecomprimeerde bestanden in het scanlogboek? .....	190
31.10. Waarom heeft Bitdefender een geïnfecteerd bestand automatisch verwijderd? .....	190
<b>Contact opnemen met ons .....</b>	<b>191</b>
<b>32. Hulp vragen .....</b>	<b>192</b>
32.1. Supportcentrum .....	193
<b>33. Online bronnen .....</b>	<b>196</b>
33.1. Bitdefender-ondersteuningscentrum .....	196
33.2. Bitdefender-ondersteuningsforum .....	196
33.3. HOTforSecurity-portaal .....	197
<b>34. Contactinformatie .....</b>	<b>198</b>
34.1. Webadressen .....	198
34.2. Lokale verdelers .....	198
34.3. Bitdefender-kantoren .....	198
<b>Woordenlijst .....</b>	<b>201</b>

## Installatie

## 1. Voorbereiden voor installatie

Voordat u Bitdefender Total Security 2013 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. 3) voor een complete lijst van systeemvereisten.
- Meld u aan bij de computer met een beheerdersaccount.
- Verwijder alle gelijksoortige software van de computer. Als u twee beveiligingsprogramma's tegelijk uitvoert, kan dit hun werking beïnvloeden en ernstige problemen met het systeem veroorzaken. Windows Defender zal uitgeschakeld zijn tijdens de installatie.
- 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 zal uitgeschakeld zijn tijdens de installatie.
- Het wordt aanbevolen uw computer verbonden te laten met internet tijdens de installatie, zelfs wanneer u vanaf een cd/dvd installeert. Indien er nieuwere versies van de toepassingsbestanden in het installatiepakket beschikbaar zijn, kan Bitdefender deze downloaden en installeren.

## 2. Systeemvereisten

U kan Bitdefender Total Security 2013 uitsluitend installeren op computers met de volgende besturingssystemen:

- Windows XP met Service Pack 3 (32-bit)
- Windows Vista met Service Pack 2
- Windows 7 met Service Pack 1
- Windows 8

Controleer vóór de installatie of uw computer voldoet aan de minimum systeemvereisten.



### 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.

### 2.1. Minimale systeemvereisten

- 1,8 Gb beschikbare vrije ruimte op de harddisk (ten minste 800 Mb op de systeemschijf)
- Processor 800 MHz
- 1 Gb geheugen (RAM)

### 2.2. Aanbevolen systeemvereisten

- 2,8 Gb beschikbare vrije ruimte op de harddisk (ten minste 800 Mb op de systeemschijf)
- Intel CORE Duo (1,66 GHz) of equivalente processor
- Geheugen (RAM):
  - ▶ 1 Gb voor Windows XP
  - ▶ 1.5 Gb voor Windows Vista en Windows 7

### 2.3. Softwarevereisten

Om Bitdefender te kunnen gebruiken, evenals alle functies ervan, moet uw computer voldoen aan de volgende softwarevereisten:

- Internet Explorer 7 of hoger
- Mozilla Firefox 3.6 of hoger
- Yahoo! Messenger 8.1 of hoger
- Microsoft Outlook 2007 / 2010
- Microsoft Outlook Express en Windows Mail (op 32-bits systemen)
- Mozilla Thunderbird 3.0.4

- .NET Framework 3.5 (automatisch geïnstalleerd met Bitdefender indien ontbrekend)

## 3. Installatieschema's

### Installatie vernieuwen

Er is geen oudere versie van Bitdefender op de computer geïnstalleerd. Ga in dit geval verder volgens de instructies in "*Uw Bitdefender-product installeren*" (p. 6).

### Installatie upgraden

Er is al een oudere versie op de computer geïnstalleerd en u upgradet naar Bitdefender 2013. In dit geval moet de oudere versie worden verwijderd voor de installatie.

Verwijder bijvoorbeeld Bitdefender 2012 voor de installatie van Bitdefender Total Security 2013:

1. Volg dit pad vanuit het Startmenu van Windows: **Start** → **Alle programma's** → **Bitdefender 2012** → **Herstellen of verwijderen**.
2. Selecteer **Verwijderen**.
3. Wacht tot Bitdefender de door u geselecteerde actie heeft voltooid. Dit kan enkele minuten duren.
4. Start de computer opnieuw op om het proces te voltooien.

Indien u de oudere versie niet verwijdert voordat u begint met de installatie van Bitdefender Total Security 2013, zult u eraan worden herinnert bij de start van het installatieproces. Volg de instructies om de verwijdering van de oudere versie te voltooien.

## 4. Uw Bitdefender-product installeren

U kunt Bitdefender installeren vanaf de installatie-cd van Bitdefender, met het webinstallatiebestand dat u van de Bitdefender-website hebt gedownload naar uw computer of vanaf 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.nl/Downloads/>.

Indien uw aankoop voor meer dan één computer is (u kocht bijvoorbeeld Bitdefender Total Security 2013 voor 3 pc's), herhaal het installatieproces dan en registreer uw product met de licentiesleutel op elke computer.

- Om Bitdefender te installeren vanaf de installatieschijf, plaatst u de schijf in het optische station. Na enkele ogenblikken zou een welkomstschermbloot moeten worden weergegeven. Volg de instructies om de installatie te starten.



### Opmerking

Het welkomstschermbloot biedt een optie voor het kopiëren van het installatiepakket vanaf de installatieschijf naar een USB-opslagapparaat. Dit is nuttig als u Bitdefender moet installeren op een computer die geen schijfstation heeft (bijv. op een netbook). Voeg het opslagapparaat in de USB rit in en klik dan **Kopie naar USB**. Ga daarna naar de computer zonder schijfstation, plaats het opslagapparaat in het USB-station en dubbelklik op `runsetup.exe` in de map waarin u het installatiepakket hebt opgeslagen.

Als het welkomstschermbloot niet verschijnt, gebruikt u Windows Verkenner om naar de rootdirectory van de schijf te gaan en dubbelklikt u op het bestand `autorun.exe`.

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

## Bevestigen van de installatie

Bitdefender zal uw systeem eerst controleren om de installatie te valideren.

Als uw systeem niet voldoet aan de minimumvereisten voor het installeren van Bitdefender, wordt u op de hoogte gebracht van de gebieden die moeten worden verbeterd voordat u kunt doorgaan.

Als een niet-compatibel antivirusprogramma of een oudere versie van Bitdefender wordt gedetecteerd, wordt u gevraagd dit van uw systeem te verwijderen. Volg de richtlijnen om de software uit uw systeem te verwijderen, zodat problemen op een later tijdstip worden vermeden. U zult mogelijk uw computer opnieuw moeten opstarten om het verwijderen van de gedetecteerde antivirusprogramma's te voltooien.

Het Bitdefender Total Security 2013 installatiepakket wordt voortdurend bijgewerkt. Indien u installeert vanaf een cd/dvd, kan Bitdefender de nieuwste versies van de bestanden downloaden tijdens de installatie. Klik op **Ja** wanneer daarom wordt gevraagd om Bitdefender toe te staan de bestanden te downloaden, zodat u zeker weet dat u de allernieuwste versie van de software installeert.



## Opmerking

Het downloaden van de installatiebestanden kan lang duren, vooral bij tragere internetverbindingen.

Zodra de installatie is bevestigd, verschijnt de set-upwizard. Volg de stappen om Bitdefender Total Security 2013 te installeren.

## Stap 1 - Welkom

In het welkomstscherm kunt u kiezen welk soort installatie u wilt uitvoeren.

Voor een volledig probleemloze installatie-ervaring, klikt u gewoon op de knop **Installeren**. Bitdefender zal worden geïnstalleerd in de standaardlocatie en met de standaardinstellingen en u zult rechtstreeks naar **Stap 3** van de wizard gaan.

Indien u de installatie-instellingen wilt configureren, selecteert u **Ik wil mijn installatie aanpassen** en daarna klikt u op **Installeren** om naar de volgende stap te gaan.

Er kunnen tijdens deze stap twee extra taken worden uitgevoerd:

- Lees a.u.b. de Licentie-overeenkomst voor Eindgebruikers voordat u doorgaat met de installatie. De licentieovereenkomst bevat de voorwaarden en bepalingen voor uw gebruik van Bitdefender Total Security 2013.

Sluit het venster als u niet akkoord gaat met deze voorwaarden. Het installatieproces wordt afgebroken en u verlaat de installatie.

- Verzenden van **Anonieme gebruikersverslagen** inschakelen. Door deze optie in te schakelen, worden rapporten met informatie over uw gebruik van het product naar de Bitdefender-servers verzonden. Deze informatie is van essentieel belang om het product te verbeteren en kan ons helpen u in de toekomst een betere ervaring te bieden. Merk op dat deze rapporten geen vertrouwelijke gegevens, zoals uw naam of IP-adres, bevatten en niet zullen worden gebruikt voor commerciële doeleinden.

## Stap 2 - Installatie-instellingen aanpassen



## Opmerking

Deze stap verschijnt alleen indien u er tijdens de vorige stap voor hebt gekozen de installatie aan te passen.



De volgende opties zijn beschikbaar:

## Installatiepad

Standaard wordt Bitdefender Total Security 2013 geïnstalleerd in C:\Program Files\Bitdefender\Bitdefender 2013. Als u het installatiepad wilt wijzigen, klikt u op **Wijzigen** en selecteert u de map waarin u Bitdefender wilt installeren.

## Proxy-instellingen configureren

Bitdefender Total Security 2013 vereist internettoegang voor productregistratie, het downloaden van beveiligings- en productupdates, "in-the-cloud"-detectie van componenten, enz. Als u een Proxyverbinding gebruikt in plaats van een directe internetverbinding, moet u deze optie selecteren en de proxy-instellingen configureren.

De instellingen kunnen worden geïmporteerd vanaf de standaardbrowser of u kunt ze handmatig invoeren.

## P2P update inschakelen

U kunt de productbestanden en handtekeningen met andere Bitdefender-gebruikers delen. Op deze manier kunnen Bitdefender-updates sneller worden uitgevoerd. Als u deze functie niet wilt inschakelen, schakelt u het overeenkomende selectievakje in.



### Opmerking

Als deze functie is ingeschakeld, wordt er geen persoonlijke identificeerbare informatie gedeeld.

Als u de invloed van het netwerkverkeer op uw systeemprestaties tijdens updates wilt minimaliseren, kunt u de optie voor het delen van updates gebruiken. Bitdefender gebruikt poorten 8880 - 8889 voor peer-to-peer update.

Klik op **Installeren met aangepaste instellingen** om uw voorkeuren te bevestigen en de installatie te starten.

## Stap 3 - Installatie bezig

Wacht tot de installatie is voltooid. Er wordt gedetailleerde informatie over de voortgang weergegeven.

Kritieke zones op uw systeem worden gescand op virussen, de nieuwste versies van de toepassingsbestanden worden gedownload en geïnstalleerd en de services van Bitdefender worden gestart. Deze stap kan enkele minuten duren.

## Stap 4 - Installatie voltooid

Er wordt een overzicht van de installatie weergegeven. Als tijdens de installatie een actieve malware wordt gedetecteerd en verwijderd, kan het opnieuw opstarten van het systeem nodig zijn.

U kunt het venster sluiten, of doorgaan met de eerste set-up van uw software door te klikken op **Starten**.

## Stap 5 - Uw product registreren



### Opmerking

Deze stap verschijnt alleen indien u Starten hebt geselecteerd tijdens de vorige stap.

Om de registratie van uw product te voltooien, dient u een licentiesleutel in te voeren. Er is een actieve internetverbinding vereist.

Ga verder volgens uw situatie:

### ● **Ik heb het product gekocht**

Registreer het product in dit geval door de volgende stappen te volgen:

1. Selecteer **Ik heb Bitdefender gekocht en ik wil het nu registreren**.
2. Typ de licentiesleutel in het overeenkomstige veld in.



### Opmerking

U kan uw licentiesleutel vinden:

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

3. Klik op **Nu registreren**.

### ● **Ik wil graag Bitdefender evalueren**

In dit geval kunt u het product gedurende 30 dagen gebruiken. Om de evaluatieperiode te starten, selecteert u **Ik wil dit product evalueren**.

Klik op **Volgende**.

## Stap 6 - Gedrag van het product configureren

Bitdefender kan worden geconfigureerd om automatisch uw beveiliging op permanente wijze of in bepaalde situaties te beheren. Gebruik de wissels om **Autopilot**, **Automatische laptopmodus** en **Automatische spelmodus** in of uit te schakelen.

Autopilot inschakelen voor volledig geruisloze beveiliging. Indien Bitdefender op Autopilot staat, worden alle beveiligingsbesluiten voor u genomen en hoeft u geen instellingen te configureren. Meer informatie vindt u onder "**Autopilot**" (p. 17).

Indien u een game speelt, schakel dan de Automatische Spelmodus in en Bitdefender zal detecteren wanneer u een game start en op de Spelmodus overgaan, waarbij de instellingen zo worden gewijzigd dat de invloed op uw systeemprestaties

tot een minimum beperkt blijven. Meer informatie vindt u onder "*Spelmodus*" (p. 18).

Laptopgebruikers kunnen de Automatische Laptopmodus inschakelen, zodat Bitdefender overschakelt op de laptopmodus zodra wordt gedetecteerd dat uw laptop werkt op de accu. De wijzigingen worden dan zo gewijzigd dat de invloed op het accuverbruik tot een minimum wordt beperkt. Meer informatie vindt u onder "*Laptop-modus*" (p. 20).

Klik op **Volgende**.

## Stap 7 - Verbindingsfilters configureren

Hier kunt u selecteren welke beveiligingsfilters u wilt activeren. Dit zijn de filters die er actief voor zorgen dat u beschermd bent tijdens uw internetactiviteiten en terwijl u verbonden bent met netwerken.

Gebruik de wissels om in/uit te schakelen:

- Antispam
- Firewall
- Web Antimalware
- Antiphishing
- Antifraude
- Search Advisor

U kunt de filters op elk ogenblik in- of uitschakelen na de installatie van de Bitdefender-interface. Om het beste beveiligingsniveau te bereiken, is het aanbevolen alle filters te activeren.

Activeer de antispamfilter alleen als u een e-mailclient gebruikt die geconfigureerd is om e-mailberichten te ontvangen via het POP3-protocol.

Klik op **Volgende**.

## Stap 8 - Inloggen op MyBitdefender

Er is een MyBitdefender-account vereist om de online functies van uw product te gebruiken. Meer informatie vindt u onder "*MyBitdefender-account*" (p. 36).

Ga verder volgens uw situatie.

### **Ik wil een MyBitdefender-account maken.**

Volg deze stappen om een MyBitdefender-account te maken:

1. Selecteer **Nieuwe account aanmaken**.

Een nieuw venster wordt weergegeven.

2. Typ de vereiste informatie in de overeenkomende velden. De gegevens die u hier opgeeft blijven vertrouwelijk.

- **E-mail** - voer uw e-mailadres in.
- **Gebruikersnaam** - voer een gebruikersnaam voor uw account in.
- **Wachtwoord** - voer een wachtwoord in voor uw account. Het wachtwoord moet minstens 6 tekens lang zijn.
- **Wachtwoord bevestigen** - typ het wachtwoord opnieuw.



#### Opmerking

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

3. Klik op **Maken**.

4. Voordat u uw account kunt gebruiken, moet u de registratie voltooien. Controleer uw e-mail en volg de instructies in de bevestigings-e-mail die u ontvangen hebt van Bitdefender.

### **Ik wil mij aanmelden met mijn Facebook- of Google-account**

Volg deze stappen om u aan te melden bij uw Facebook- of Google-account.

1. Selecteer de service die u wilt gebruiken. U wordt omgeleid naar de aanmeldingspagina van die service.
2. Volg de instructies die door de geselecteerde service worden gegeven om uw account te koppelen aan Bitdefender.



#### Opmerking

Bitdefender krijgt geen toegang tot vertrouwelijke informatie, zoals het wachtwoord van de account die u gebruikt om aan te melden of de persoonlijke informatie van uw vrienden en contactpersonen.

### **Ik heb al een MyBitdefender-account**

Indien u eerder hebt ingelogd op een account vanaf uw product, zal Bitdefender dit detecteren en u vragen het wachtwoord in te voeren om in te loggen op die account.

Indien u al een actieve account hebt, maar Bitdefender detecteert deze niet of u wilt gewoon inloggen op een andere account, voer dan het e-mailadres en wachtwoord in en klik op **Inloggen op MyBitdefender**.

### **Uitstellen tot later**

Indien u deze taak voor een andere keer wilt laten liggen, klik dan op **Later vragen**. Denk eraan dat u moet inloggen op een account om de online functies van het product te gebruiken.

Aan de slag

## 5. De basisfuncties

Nadat u Bitdefender Total Security 2013 hebt geïnstalleerd, wordt uw computer beschermd tegen alle types malware (zoals virussen, spyware en Trojaanse paarden) en internetbedreigingen (zoals hackers, phishing en spam).

U kunt **Autopilot** inschakelen om te genieten van een complete stille beveiliging en u hoeft geen instellingen te configureren. U kunt echter voordeel halen uit de Bitdefender-instellingen om uw beveiliging fijn af te stemmen en te verbeteren.

Bitdefender zal de meeste beslissingen met betrekking tot de beveiliging voor u nemen en zal zelden pop-upwaarschuwingen weergeven. Details over acties die worden ondernomen en informatie over de programmabediening zijn beschikbaar in het venster Gebeurtenissen. Meer informatie vindt u onder "**Gebeurtenissen**" (p. 16).

Het is aanbevolen Bitdefender af en toe te openen en de bestaande problemen te herstellen. U zult mogelijk specifieke Bitdefender-componenten moeten configureren of preventieve acties ondernemen om uw computer en gegevens te beschermen.

Als u het product niet hebt geregistreerd, moet u dit doen voordat de evaluatieperiode verloopt. Meer informatie vindt u onder "**Bitdefender registreren**" (p. 34).

Om de online functies van Bitdefender Total Security 2013 te gebruiken, moet u uw computer koppelen aan een MyBitdefender-account. Meer informatie vindt u onder "**MyBitdefender-account**" (p. 36).

Indien u problemen ondervindt bij het gebruik van Bitdefender, controleer dan het "**Algemene problemen oplossen**" (p. 166) deel met mogelijke oplossingen voor de problemen die het vaakst voorkomen. In het "**Zo werkt het**" (p. 43) deel vindt u stap-voor-stap instructies over het uitvoeren van vaak voorkomende taken.

### 5.1. Open het Bitdefender-venster.

De hoofdinterface van Bitdefender Total Security 2013, is toegankelijk via het volgende pad vanaf het menu Start van Windows: **Start** → **Alle programma's** → **Bitdefender 2013** → **Bitdefender Total Security 2013** Dit kan sneller door in het systeemvak te dubbelklikken op het Bitdefender-pictogram .

Meer informatie over het Bitdefender-venster en -pictogram in het systeemvak, vindt u op "**Bitdefender-interface**" (p. 23).

### 5.2. Problemen aan het oplossen

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.

De gedetecteerde problemen bevatten belangrijke beveiligingsinstellingen die worden uitgeschakeld en andere omstandigheden die een beveiligingsrisico kunnen betekenen. Ze zijn gegroepeerd in twee categorieën:

- **Kritieke problemen** - verhinderen dat Bitdefender u beveiligt tegen malware of vormen een belangrijk beveiligingsrisico.
- **Minder belangrijke (niet-kritieke) problemen** - kan uw beveiliging in de nabije toekomst beïnvloeden.

Het Bitdefender-pictogram in het **stysteemvak** geeft problemen in behandeling aan door de kleur als volgt te wijzigen:

**B Rood:** Kritieke problemen beïnvloeden de veiligheid van uw systeem. Ze vereisten uw onmiddellijke aandacht en moeten zo snel mogelijk worden hersteld.

**B Geel:** 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 het Bitdefender-venster opent, geeft het gebied Beveiligingsstatus in de werkbalk bovenaan het aantal en de aard van de problemen die uw systeem beïnvloeden aan.

## 5.2.1. Wizard alle problemen herstellen

Volg de wizard **Alle problemen herstellen** om de gedetecteerde problemen op te lossen.

1. Voer een van de volgende bewerkingen uit om de wizard te openen:

- Klik met de rechtermuisknop op het Bitdefender-pictogram in het **stysteemvak** en selecteer **Alle problemen herstellen**. Afhankelijk van de gedetecteerde problemen is het pictogram rood **B** (wat wijst op kritieke problemen) of geel **B** (wat wijst op niet-kritieke problemen).
- Open het Bitdefender-venster en klik op een willekeurige plaats binnen het gebied Beveiligingsstatus in de werkbalk bovenaan (u kunt bijvoorbeeld op de knop  **Alle problemen herstellen** klikken).

2. U kunt de problemen zien die de veiligheid van uw computer en gegevens beïnvloeden. Alle huidige problemen zijn geselecteerd om te worden opgelost.

Als u een specifiek probleem niet meteen wilt oplossen, schakelt u het overeenkomende selectievakje uit. U wordt gevraagd op te geven hoelang het

oplossen van het probleem kan worden uitgesteld. Kies de gewenste optie in het menu en klik op **OK**. Kies **Permanent** om de bewaking van de respectieve problemencategorie te stoppen.

De status van het probleem verandert naar **Uitstellen** en er wordt geen actie ondernomen om het probleem op te lossen.

3. 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.** Wanneer u dergelijke problemen oplost, helpt een wizard u bij het voltooiën van de taak.

## 5.2.2. Statuswaarschuwingen configureren

Bitdefender kan u informeren wanneer er problemen worden gedetecteerd in de verrichtingen van de volgende programmaonderdelen:

- Firewall
- Antispam
- Antivirus
- Update
- Browserveiligheid

U kunt het waarschuwingssysteem configureren om optimaal te voldoen aan uw beveiligingsbehoeften door te kiezen over welke problemen u op de hoogte wilt worden gebracht. Volg deze stappen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Algemeen**.
4. Selecteer in het venster met **Algemene instellingen** de tab **Geavanceerd**.
5. Klik op de link **Statuswaarschuwingen configureren**.
6. Klik op de schakelaars om de statuswaarschuwingen volgens uw voorkeuren in of uit te schakelen.



## 5.3. Gebeurtenissen

Bitdefender houdt een gedetailleerd logboek bij van gebeurtenissen met betrekking tot de activiteiten van uw computer. Wanneer er iets belangrijks gebeurt met de veiligheid van uw systeem of gegevens, wordt er een nieuw bericht toegevoegd aan Systeemgebeurtenissen van het Bitdefender, net zoals er nieuwe e-mails verschijnen in uw Postvak IN.

Gebeurtenissen zijn een zeer belangrijk hulpmiddel bij het bewaken en beheren van uw Bitdefender-beveiliging. U kan bijvoorbeeld gemakkelijk controleren of de update is gelukt, of er malware op uw computer is gevonden, enz. Daarnaast kunt u zo nodig verdere acties ondernemen of acties die door Bitdefender zijn ondernomen, wijzigen.


Volg deze stappen om toegang te krijgen tot het gebeurtenissenlogboek:

1. Het **Bitdefender-venster** openen.
2. Klik in de werkbalk bovenaan op **Gebeurtenissen** om het venster **Overzicht gebeurtenissen** te openen.

Worden de berichten gegroepeerd volgens de Bitdefender-module waar hun activiteiten aan gerelateerd zijn:

- **Antivirus**
- **Antispam**
- **Privacybeheer**
- **Firewall**
- **Tune-up**
- **Safebox**
- **Update**
- **Safego**
- **File encryptie**

**Gebeurtenissteller** wordt weergegeven in de interface van Bitdefender zodat gemakkelijk herkend kan worden in welke gebieden er openstaande gebeurtenissen zijn. Dit zijn pictogrammen die verschijnen op specifieke modules die aangeven hoeveel ongelezen kritieke gebeurtenissen gerelateerd aan de activiteit van een module er zijn.

Als er bijvoorbeeld een ongelezen kritieke gebeurtenis gerelateerd aan de activiteit van de updatemodule is, verschijnt het pictogram  op het updatepaneel.

Een teller die het totaal aantal ongelezen berichten van alle modules toont, verschijnt op de knop 'Gebeurtenissen' in het hoofdvenster.

Voor elke categorie is een lijst gebeurtenissen beschikbaar. U kunt meer informatie over een specifieke gebeurtenis in de lijst weergeven door erop te klikken. Details over de gebeurtenis worden weergegeven in het onderste deel van het venster. 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. Er kunnen opties worden geboden voor het ondernemen van verdere actie.

U kunt gebeurtenissen filteren volgens hun belang. Er zijn drie types gebeurtenissen. Elk type wordt aangeduid door een specifiek pictogram:

-  Gebeurtenissen van het type **Informatie** duiden op een geslaagde bewerking.
-  Gebeurtenissen van het type **Waarschuwing** wijzen op niet-kritieke problemen. U moet ze controleren en herstellen wanneer u tijd hebt.
-  **Kritieke** gebeurtenissen wijzen op kritieke problemen. U moet ze onmiddellijk controleren.





Om u te helpen geregistreerde gebeurtenissen gemakkelijker te beheren, biedt elk deel van het venster Gebeurtenissen opties waarmee alle gebeurtenissen in dat deel kunnen worden verwijderd of gemarkeerd als gelezen.

## 5.4. Autopilot

Voor alle gebruikers die van hun beveiligingsoplossing alleen vragen dat ze worden beschermd zonder te worden gehinderd, werd Bitdefender Total Security 2013 ontworpen met een ingebouwde Autopilot-modus.


Wanneer u in de modus Autopilot bent, past Bitdefender een optimale beveiligingsconfiguratie toe en neemt de toepassing alle beslissingen met betrekking tot de beveiliging voor u. Dit betekent dat u geen pop-upberichten of waarschuwingen zult zien en dat u geen enkele instelling zult moeten configureren.

In de modus Autopilot, lost Bitdefender automatisch kritieke problemen op en beheert het op de achtergrond:

-  Antivirusbeveiliging, geleverd door Scannen bij toegang en Doorlopend scannen.
-  Firewallbeveiliging.
-  Privacybescherming, geleverd door antiphishing- en antimailware-filters voor het surfen op het web.
-  Automatische updates.

Volg deze stappen om Autopilot in of uit te schakelen:

1. Het **Bitdefender-venster** openen.
2. Klik op de schakelaar **Gebruikersmodus / Autopilot** in de werkbalk bovenaan. Wanneer de schakelaar in de positie Gebruikersmodus staat, is Autopilot uit.

Zolang Auto pilot is ingeschakeld, verandert het Bitdefender-pictogram in het systeemvak naar .



## Belangrijk

Wanneer Autopilot is ingeschakeld en u instellingen die door deze toepassing worden beheerd wijzigt, zal Auto Pilot worden uitgeschakeld.

Open het venster **Gebeurtenissen** om de geschiedenis te zien van acties die door Bitdefender zijn ondernomen terwijl Autopilot is ingeschakeld.

## 5.5. 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 Total Security 2013 twee speciale gebruiksmodi:

- **Spelmodus**
- **Laptop-modus**

### 5.5.1. Spelmodus

De Spelmodus verandert tijdelijk de beveiligingsinstellingen om de snelheid van het systeem zo weinig mogelijk te beïnvloeden. De volgende instellingen worden toegepast wanneer de Spelmodus is ingeschakeld:

- Alle Bitdefender waarschuwingen en pop-ups zijn uitgeschakeld.
- **Scannen bij toegang** is ingesteld op het beschermingsniveau **Toegeeflijk**.
- Autoscan is uitgeschakeld. Autoscan zoekt en gebruikt tijdsegmenten wanneer het gebruik van de systeembronnen daalt onder een bepaalde drempel om terugkerende scans van het volledige systeem uit te voeren.
- De Bitdefender-firewall is ingesteld op de normale modus (**Paranoïde-modus** is uitgeschakeld). Dit betekent dat alle nieuwe verbindingen (inkomend en uitgaand) automatisch zijn toegestaan, ongeacht de poort en het gebruikte protocol.
- Auto update is uitgeschakeld.
- **Safebox** Auto Sync is uitgeschakeld.
- De Bitdefender-werkbalk in uw webbrowser wordt uitgeschakeld wanneer u op browser gebaseerde online spelletjes speelt.

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**.
- Schakel het gebruik van de **sneltoets** Spelmodus in. Druk op **Ctrl+Shift+Alt+G** (de standaard sneltoets).



### Belangrijk

Vergeet niet de Spelmodus uit te schakelen wanneer u klaar bent. Gebruik hiervoor dezelfde methoden die u hebt gebruikt voor het inschakelen.

## Snelkoppeling toetsenbord Spelmodus

Volg deze stappen voor het instellen en gebruiken van een sneltoets voor het openen/sluiten van de Spelmodus:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Algemeen**.
4. Selecteer in het venster met **Algemene instellingen** de tab **Algemeen**.
5. Controleer of de schakelaar voor de sneltoets Spelmodus is ingeschakeld.
6. Stel de gewenste combinatie in.

- a. De standaard combinatie is **Ctrl+Alt+Shift+G**.

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**).

- b. 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

Om de sneltoets uit te schakelen, schakelt u de optie **Sneltoets Spelmodus inschakelen** uit.

## De automatische spelmodus in- of uitschakelen

Volg deze stappen om de automatische spelmodus in of uit te schakelen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Algemeen**.
4. Selecteer in het venster met **Algemene instellingen** de tab **Algemeen**.
5. Schakel de automatische spelmodus in of uit door op de overeenkomende schakelaar te klikken.

## 5.5.2. Laptop-modus

De Laptop-modus is speciaal ontworpen voor laptop- en notebookgebruikers. Het doel hiervan is het minimaliseren van de impact van het Bitdefender op het energieverbruik terwijl deze apparaten werken op batterij. Wanneer Bitdefender werkt in de Laptop-modus, worden de functies Autoscan, Auto update en Auto sync uitgeschakeld 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.

Volg deze stappen om de automatische laptop-modus in of uit te schakelen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Algemeen**.
4. Selecteer in het venster met **Algemene instellingen** de tab **Algemeen**.
5. Schakel de automatische laptopmodus in of uit door op de overeenkomende schakelaar te klikken.

Als Bitdefender niet is geïnstalleerd op een laptop, moet u de automatische laptop-modus uitschakelen.

## 5.6. Wachtwoordbeveiligde Bitdefender-instellingen

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.

Volg de onderstaande stappen om de wachtwoordbeveiliging voor de instellingen van Bitdefender te beheren:

1. Het **Bitdefender-venster** openen.

2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Algemeen**.
4. Selecteer in het venster met **Algemene instellingen** de tab **Algemeen**.
5. Schakel de wachtwoordbeveiliging in door op de schakelaar te klikken.
6. Klik op de koppeling **Wachtwoord wijzigen**.
7. Voer het wachtwoord in de twee velden in en klik op **OK**. Het wachtwoord moet minstens 8 tekens lang zijn.

Zodra u een wachtwoord hebt ingesteld, zal iedereen die de Bitdefender-instellingen probeert te wijzigen, eerst het wachtwoord moeten opgeven.



## Belangrijk

Zorg dat u uw wachtwoord onthoudt of bewaar het op een veilige plaats. Als u het wachtwoord vergeten bent, moet u het programma opnieuw installeren of contact opnemen met Bitdefender voor ondersteuning.

Volg deze stappen om de wachtwoordbeveiliging te verwijderen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Algemeen**.
4. Selecteer in het venster met **Algemene instellingen** de tab **Algemeen**.
5. Schakel de wachtwoordbeveiliging uit door op de schakelaar te klikken. Voer het wachtwoord in en klik op **OK**.

## 5.7. Anonieme gebruiksrapporten

Standaard verzendt Bitdefender rapporten met informatie over uw gebruik van het programma naar de Bitdefender-servers. Deze informatie is van essentieel belang om het product te verbeteren en kan ons helpen u in de toekomst een betere ervaring te bieden. Merk op dat deze rapporten geen vertrouwelijke gegevens, zoals uw naam of IP-adres, bevatten en niet zullen worden gebruikt voor commerciële doeleinden.

Volg deze stappen als u het verzenden van anonieme gebruiksrapporten wilt stopzetten:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Algemeen**.
4. Selecteer in het venster met **Algemene instellingen** de tab **Geavanceerd**.

5. Klik op de schakelaar om Anonieme gebruikersverslagen uit te schakelen.

## 6. Bitdefender-interface


Bitdefender Total Security 2013 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.

Om de status van het product te zien en essentiële taken uit te voeren, is het **stysteemvakpictogram** van Bitdefender op elk ogenblik beschikbaar.

Het **hoofdvenster** biedt u toegang tot belangrijke productinformatie, de programmamodules en biedt u de mogelijkheid algemene taken uit te voeren. Vanaf het hoofdvenster krijgt u toegang tot het **venster Instellingen** voor een gedetailleerde configuratie en geavanceerde administratieve taken en tot het venster **Gebeurtenissen** voor een diepgaande logboekregistratie van de Bitdefender-activiteiten.

Als u altijd een oogje wilt houden op essentiële beveiligingsinformatie en snel toegang wilt krijgen tot belangrijke instellingen, kunt u de **Beveiligingswidget** weergeven op het bureaublad.


### 6.1. Systeemvakpictogram

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



#### Opmerking

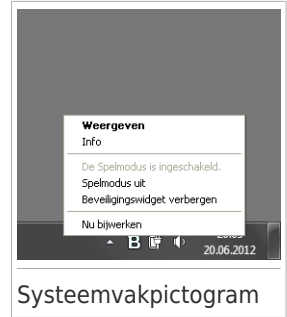
Als u Windows Vista of Windows 7 gebruikt, zal het pictogram Bitdefender mogelijk niet altijd zichtbaar zijn. Volg deze stappen om het pictogram permanent weer te geven:

1. Klik onderaan rechts op het scherm op de pijl .
2. Klik op **Aanpassen...** om het venster met de systeemvakpictogrammen te openen.
3. Selecteer de optie **Pictogrammen en meldingen weergeven** voor het pictogram **Bitdefender-agent**.

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 het hoofdvenster van Bitdefender.
- **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 aan het oplossen*" (p. 13) voor meer gedetailleerde informatie.
- **Spelmodus in-/uitschakelen** - schakelt de **Spelmodus** in/uit.
- **Beveiligingswidget tonen/verbergen** - hiermee schakelt u de **Beveiligingswidget** in/uit.
- **Update nu** - start een directe update. U kunt de updatestatus volgen in het paneel Update van het hoofdvenster van Bitdefender.



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:

**B** Kritieke problemen beïnvloeden de beveiliging van uw systeem. Ze vereisen uw onmiddellijke aandacht en moeten zo snel mogelijk worden hersteld.

**B** Niet-kritieke problemen beïnvloeden de beveiliging van uw systeem. U moet ze controleren en herstellen wanneer u tijd hebt.

**B** Het product werkt op **Spelmodus**.

**B** Bitdefender **Autopilot** is ingeschakeld.

Als Bitdefender niet werkt, verschijnt het systeemvakpictogram op een grijze achtergrond: **B**. Dit doet zich doorgaans voor wanneer de licentiesleutel vervalt. Dit kan ook optreden wanneer de Bitdefender-services niet reageren of wanneer andere fouten de normale werking van Bitdefender beïnvloeden.

## 6.2. Hoofdvenster

Via het hoofdvenster van Bitdefender kunt u algemene taken uitvoeren, snel beveiligingsproblemen oplossen, informatie over gebeurtenissen in het productgebruik weergeven en productinstellingen aanpassen. U kunt het allemaal met slechts enkele klikken op de knop.

Het venster is geordend in twee hoofdgebieden:

## Werkbalk boven

Hier kunt u de beveiligingsstatus van de computer controleren en krijgt u toegang tot belangrijke taken.

## Panelengebied

Hier kunt u de belangrijkste Bitdefender-modules beheren.

Via het vervolgkeuzemenu **MyBitdefender** bovenaan in het venster, kunt u uw account beheren en krijgt u vanaf het accountdashboard toegang tot de online functies van uw product.

Daarnaast vindt u in het onderste deel van het venster verschillende nuttige koppelingen. Deze koppelingen zijn ook beschikbaar in de vensters **Gebeurtenissen** en **Instellingen**.

Koppeling	Beschrijving
<b>Resterend aantal dagen</b>	De resterende tijd tot uw huidige licentie verval, wordt weergegeven. Klik op de koppeling om een venster te openen waarin u meer informatie ziet over uw licentiesleutel of waarin u uw product kunt registreren met een nieuwe licentiesleutel.
<b>Opmerkingen</b>	Opent een webpagina in uw browser waar u een korte vragenlijst kunt invullen met betrekking tot uw ervaring bij het gebruik van het product. Wij baseren ons op uw feedback bij onze voortdurende inzet om de Bitdefender-producten te verbeteren.
<b>Support</b>	Klik op deze koppeling als u hulp nodig hebt bij Bitdefender. Er verschijnt een nieuw venster. In dit venster kunt u het Help-bestand van het product openen, naar het ondersteuningscentrum gaan of contact opnemen met de ondersteuning.
	Voegt vraagtekens toe in verschillende gebieden van het Bitdefender-venster om u te helpen gemakkelijk informatie te vinden over de verschillende interface-elementen.  Beweeg uw muiscursor over een markering om snelle informatie over het element ernaast te zien.

## 6.2.1. Werkbalk boven

De werkbalk bovenaan bevat de volgende elementen:

- **Het gebied Beveiligingsstatus** aan de linkerzijde van de werkbalk informeert u als er problemen zijn die de beveiliging van uw computer beïnvloeden en helpt u bij het oplossen van het probleem.

De kleur van het gebied van de beveiligingsstatus verandert afhankelijk van de gedetecteerde problemen en er worden verschillende berichten weergegeven:

- ▶ **Het gebied wordt groen gekleurd.** Er zijn geen problemen om op te lossen. Uw computer en gegevens zijn beveiligd.
- ▶ **Het gebied wordt geel gekleurd.** Niet-kritieke problemen beïnvloeden de beveiliging van uw systeem. U moet ze controleren en herstellen wanneer u tijd hebt.
- ▶ **Het gebied wordt rood gekleurd.** Kritieke problemen beïnvloeden de beveiliging van uw systeem. U moet deze problemen onmiddellijk aanpakken.

Door te klikken op **Problemen weergeven**  in de midden van de werkbalk of op een willekeurige plaats in het gebied met de beveiligingsstatus aan de linkerkant, krijgt u toegang tot een wizard waarmee u bedreigingen gemakkelijk van uw computer kunt verwijderen. Raadpleeg "*Problemen aan het oplossen*" (p. 13) voor meer gedetailleerde informatie.


- Met **Gebeurtenissen** krijgt u toegang tot een gedetailleerde geschiedenis van relevante gebeurtenissen die zich hebben voorgedaan tijdens de activiteiten van het product. Raadpleeg "*Gebeurtenissen*" (p. 16) voor meer gedetailleerde informatie.
- Met **Instellingen** krijgt u toegang tot het instellingsvenster waarin u de productinstellingen kunt configureren. Raadpleeg "*Venster Overzicht instellingen*" (p. 30) voor meer gedetailleerde informatie.
- Met **Autopilot / Gebruikersmodus** kunt u de Autopilot inschakelen en genieten van een volledig stille beveiliging. Raadpleeg "*Autopilot*" (p. 17) voor meer gedetailleerde informatie.

## 6.2.2. Panelengebied


In het panelengebied kunt u de Bitdefender-modules direct beheren.

Om te bladeren door de panelen, gebruikt u de schuifregelaar onder het panelengebied of de pijlen aan de rechter- en linkerkant.

Elk modulepaneel bevat de volgende elementen:



- De naam van de module en een statusbericht.
- Een pictogram  is beschikbaar in de hoek rechtsboven van de meeste panelen. Wanneer u hierop klikt, gaat u direct naar het venster met de geavanceerde instellingen van die module.
- Het pictogram van de module.

Als er gebeurtenissen zijn die betrekking hebben op de activiteit van een module die u nog niet hebt gelezen, wordt een gebeurtenissteller weergegeven naar

het modulepictogram. Als er bijvoorbeeld een ongelezen gebeurtenis gerelateerd aan de activiteit van de updatemodule is, verschijnt het pictogram  op het updatepaneel. Klik op de teller om direct naar het venster Gebeurtenissen van die module te gaan.

- Een knop waarmee u belangrijke taken met betrekking tot de module kunt uitvoeren.
- Op bepaalde panelen is er een selectievakje beschikbaar waarmee u een belangrijke functie van de module kunt in- of uitschakelen.

Volg deze stappen om de panelen te ordenen volgens uw voorkeur:

1. Klik links van de schuifregelaar onder de panelen op  om het venster Overzicht modules te openen.
2. Sleep individuele modulepanelen naar andere sleuven om het gebied opnieuw te schikken volgens uw behoeften.
3. Klik op  om terug te keren naar het hoofdvenster.

De beschikbare panelen in dit gebied zijn:

## Antivirus

Antivirusbescherming is de basis van uw beveiliging. Bitdefender beschermt u in real time en op aanvraag tegen elk type malware, zoals virussen, Trojaanse paarden, spyware, adware, enz.

Via het paneel Antivirus krijgt u gemakkelijk toegang tot de belangrijke scantaken. Klik op **Nu scannen** en selecteer een taak in het vervolgkeuzemenu.

- Quick Scan
- Volledige systeemscaan
- Aangepast scannen
- Kwetsbaarheidsscaan
- Helpmodus

Via de schakelaar **Autoscan** kunt u de functie Auto scan in- of uitschakelen.

Raadpleeg "*Antivirusbeveiliging*" (p. 71) voor meer informatie over scantaken en het configureren van de antivirusbeveiliging.

## Antispam

De Bitdefender-antispammodule zorgt ervoor dat uw Postvak IN vrij blijft van ongewenste e-mails door het POP3-mailverkeer te filteren.

Antispambeveiliging is standaard niet ingeschakeld. De modulecomponenten worden geïnstalleerd wanneer u deze module de eerste keer inschakelt via het selectievakje Antispam.

Zodra de module is ingeschakeld, kunt u op **Beheren** klikken in het paneel Antispam en kunt Vrienden of Spammers selecteren in het vervolgkeuzemenu om de overeenkomende adressenlijst te bewerken.

Meer informatie over het configureren van de antispambeveiliging, vindt u onder "*Antispam*" (p. 98).

## Privacy

De module voor privacybeheer helpt u belangrijke persoonlijke gegevens privé te houden. Hiermee wordt u beschermd terwijl u met internet verbonden bent tegen phishingaanvallen, fraudepogingen, het lekken van persoonlijke gegevens, en meer.

Klik in het paneel Privacybeheer op de knop **Configureren** en selecteer een taak in het vervolgkeuzemenu:

- **Bestandsvernietiging** - start een wizard waarmee u bestanden permanent kunt verwijderen.

Via het selectievakje Antiphishing kunt u de antiphishing-beveiliging in- of uitschakelen.

Meer informatie over het configureren van Bitdefender om uw privacy te beschermen, vindt u op "*Privacybeheer*" (p. 109).

## Firewall

De firewall beschermt u terwijl u verbonden bent met netwerken en internet door alle verbindingspogingen te filteren.

Door in het paneel Firewall te klikken op **Adapters beheren**, kunt u de algemene verbindinginstellingen voor netwerkadapters configureren.

Via het selectievakje Firewall kunt u de firewallbeveiliging in- of uitschakelen.



### Waarschuwing

Omdat het uw computer blootstelt voor onbevoegde verbindingen, mag het uitschakelen van de firewall slechts een tijdelijke maatregel zijn. Schakel de firewall zo snel mogelijk opnieuw in.

Meer informatie over de firewallconfiguratie, vindt u onder "*Firewall*" (p. 124).

## Tune-up

Bitdefender Total Security 2013 biedt niet alleen beveiliging, maar helpt u ook optimale prestaties van uw computer te behouden.

Wanneer u in het paneel Tune-Up op **Optimaliseren** klikt, krijgt u toegang tot een aantal nuttige hulpprogramma's:

- PC-opruiming
- Schijfdefragmentatie
- Kopiezoeker
- Registeropruiming

- Registerherstel

Meer informatie over de hulpprogramma's voor het optimaliseren van de prestaties, vindt u onder "*Tune-up*" (p. 153).

## Safebox

Met Safebox kunt u een back-up van uw belangrijke bestanden maken op beveiligde online servers, ze synchroniseren tussen uw apparaten en ze delen met uw vrienden.

Klik op **Beheren** en selecteer een taak in het vervolgkeuzemenu:

- **Mappen beheren** - hiermee kunt u Safebox-mappen toevoegen, verwijderen en synchroniseren.
- **Beheer gedeelde bestanden** - hiermee kunt u bestanden delen door ze te uploaden naar Safebox en koppelingen te maken die vanaf overal toegankelijk zijn.
- **Ga naar dashboard** - hiermee kunt u uw Safebox-back-ups direct beheren vanaf het MyBitdefender-dashboard in uw webbrowser.

Via de schakelaar Auto sync kunt u de automatische synchronisatie in- of uitschakelen voor Safebox-mappen.

Meer informatie vindt u onder "*Online back-up en synchronisatie Safebox*" (p. 159).

## Update

In een wereld waar cybercriminelen voortdurend nieuwe manieren uitzoeken om schade te veroorzaken, is het van cruciaal belang uw beveiligingsoplossing up-to-date te houden om hen een stap voor te blijven.

Bitdefender is standaard ingesteld om elk uur te controleren op updates. Als u automatische updates wilt uitschakelen, kunt u de schakelaar **Auto Update** op het panel Update gebruiken.



### Waarschuwing

Dit is een kritiek beveiligingsprobleem. Wij raden u aan 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.

Klik op het paneel **Nu bijwerken** om een onmiddellijke update te starten.

Meer informatie over het configureren van updates, vindt u onder "*Bitdefender up-to-date houden*" (p. 39).

## Safego

Om uw veiligheid op sociale netwerken te verbeteren, kunt u Safego, de Bitdefender beveiligingsoplossing voor sociale netwerken, direct vanaf Bitdefender Total Security 2013 openen.

Klik in het paneel Safego op de knop **Beheren** en selecteer een taak in het vervolgkeuzemenu:

- **Activeren voor Facebook** via uw MyBitdefender-account. Als Safego al is geactiveerd, zult u toegang krijgen tot statistieken betreffende zijn activiteit door **Verslagen weergeven voor Facebook** te selecteren in het menu.
- **Activeren voor Facebook** via uw MyBitdefender-account. Als Safego al is geactiveerd, zult u toegang krijgen tot statistieken betreffende zijn activiteit door **Verslagen weergeven voor Twitter** te selecteren in het menu.

Meer informatie vindt u onder "*Safego-beveiliging voor sociale netwerken*" (p. 145).

## File encryptie

Maak gecodeerde, door een wachtwoord beveiligde logische schijven (of kluizen) op uw computer waar u uw confidentiële en gevoelige documenten veilig kunt opslaan.

Klik in het paneel Bestandscodering op de knop **Coderen** en selecteer een taak in het vervolgkeuzemenu:

- **Bestand toevoegen aan kluis** - start een wizard waarmee u belangrijke bestanden kunt toevoegen aan een beveiligde, gecodeerde bestandskluis.
- **Bestanden uit kluis verwijderen** - hiermee wordt een wizard gestart waarmee u bestanden uit een kluis kunt verwijderen.
- **Kluisbestanden tonen** - hiermee start u een wizard waarmee u de inhoud van een bestandskluis kunt weergeven.
- **Kluis vergrendelen** - hiermee start u een wizard waarmee u een kluis kunt vergrendelen.

## 6.3. Venster Overzicht instellingen

Het venster Overzicht instellingen biedt u toegang tot de geavanceerde instellingen van uw product. Hier kunt u Bitdefender in detail configureren.

Selecteer een module voor het configureren van zijn instellingen of voer beveiligings- of administratieve taken uit. In de volgende lijst vindt u een korte beschrijving van elke module.

### Algemeen

Hiermee kunt u de algemene productinstellingen, zoals het instellingswachtwoord, de spelmodus, de laptopmodus, de proxy-instellingen en de statuswaarschuwingen, configureren.

## Antivirus

Hiermee kunt u uw bescherming tegen malware configureren, kwetsbaarheid van uw systeem detecteren en oplossen, scansuitsluitingen instellen en bestanden in quarantaine beheren.

## Antispam

Hiermee kunt u uw Postvak IN spamvrij houden en de antispaminstellingen in detail configureren.

## Privacybeheer

Hiermee voorkomt u diefstal van data van uw computer en beschermt u uw privacy als u online bent. De beveiliging configureren voor uw webbrowser, IM-software, het beheren van uw gegevensbeveiliging, en meer.

## Firewall

Hiermee kunt u de algemene firewallinstellingen, firewallregels, inbraakdetectie en netwerkbewakingsactiviteiten configureren.

## Tune-up

Hiermee kunt u de prestaties van uw computer bewaken en een oogje houden op het bronverbruik.

## Safebox

Hiermee kunt u een back-up maken van uw belangrijke gegevens op beveiligde online servers, bestanden synchroniseren tussen uw apparaten en bestanden delen met uw vrienden.

## Update

Hiermee kunt u het updateproces in detail configureren.

## File encryptie

Hiermee kunt u gecodeerde opslagstations waar u vertrouwelijke gegevens veilig kunt maken en beheren.

Om terug te keren naar het **hoofdvenster**, klikt u op de knop  in de linkerbovenhoek van het venster.

## 6.4. Beveiligingswidget

**Beveiligingswidget** is de snelle en eenvoudige manier voor het bewaken en beheren van Bitdefender Total Security 2013. Wanneer u deze kleine en weinig opdringerige widget toevoegt aan uw bureaublad, kunt u op elk ogenblik kritieke informatie zien en belangrijke taken uitvoeren.

- Scanactiviteit bewaken in real time.
- Firewall-activiteit bewaken in real time.
- De beveiligingsstatus van uw systeem bewaken en eventuele bestaande problemen oplossen.



- Meldingen weergeven en toegang krijgen tot de recentste gebeurtenissen die zijn gemeld door Bitdefender.
- Toegang met één klik op de knop tot uw MyBitdefender-account.
- Bestanden of mappen scannen door een of meerdere items te slepen en boven de widget neer te zetten.



Beveiligingswidget

De algemene beveiligingsstatus van uw computer wordt weergegeven **in het midden** van de widget. De status wordt aangeduid door de kleur en vorm van het pictogram dat in dit gebied wordt weergegeven.



Kritieke problemen beïnvloeden de veiligheid van uw systeem.

Ze vereisen uw onmiddellijke aandacht en moeten zo snel mogelijk worden hersteld. Klik op het statuspictogram om het oplossen van de gemelde problemen te starten.



Niet-kritieke problemen beïnvloeden de beveiliging van uw systeem. U moet ze controleren en herstellen wanneer u tijd hebt. Klik op het statuspictogram om het oplossen van de gemelde problemen te starten.



Uw systeem is beveiligd.




Wanneer een scantaak op aanvraag bezig is, wordt dit geanimeerde pictogram weergegeven.

Wanneer er problemen worden gemeld, klikt u op het statuspictogram om de wizard Problemen herstellen te starten.

De knop **links** van de widget biedt u directe toegang tot het venster Firewall-instellingen en wordt ook gebruikt voor een grafische voorstelling van de firewall-activiteit in real time. Wanneer een blauwe balk verschijnt op deze knop, betekent dit dat de firewallmodule de netwerkverbinding actief filtert. Hoe groter de blauwe balk, hoe intenser de activiteit van deze module.

**De bovenzijde** van de widget toont de teller van de ongelezen gebeurtenissen (het aantal openstaande gebeurtenissen dat is gemeld door Bitdefender, als er zijn).

Klik op de gebeurtenissteller, bijvoorbeeld  voor één ongelezen gebeurtenis, om het venster Overzicht gebeurtenissen te openen. Meer informatie vindt u onder "*Gebeurtenissen*" (p. 16).

De knop **rechts** van de widget biedt u directe toegang tot het venster Antivirusinstellingen en wordt ook gebruikt voor een grafische voorstelling van de scanactiviteit in real time. Wanneer op deze knop een blauwe balk verschijnt, geeft dit aan dat de activiteit van het scannen op virussen in real time bezig is. Hoe groter de blauwe balk, hoe intenser de activiteit van deze module.


De knop **aan de onderzijde** van de widget start het bedieningspaneel van uw MyBitdefender-account in het venster van een webbrowser. Meer informatie vindt u onder "*MyBitdefender-account*" (p. 36).

## 6.4.1. Bestanden en mappen scannen

U kunt de Beveiligingswidget gebruiken om snel bestanden en mappen te scannen. Sleep een bestand of map die u wilt scannen en zet deze neer boven de **Beveiligingswidget**.

De **Antivirusscanwizard** wordt weergegeven en begeleidt u doorheen het scanproces. De scanopties zijn vooraf geconfigureerd voor de beste detectieresultaten en kunnen niet worden gewijzigd. Als er geïnfecteerde bestanden worden 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.

## 6.4.2. Beveiligingswidget tonen/verbergen

Wanneer u de widget niet meer wilt zien, klikt u op .

Volg deze stappen om de Beveiligingswidget opnieuw weer te geven:

1. Klik met de rechtermuisknop op het Bitdefender-pictogram in het systeemvak.
2. Klik op **Beveiligingswidget tonen** in het contextmenu dat verschijnt.

## 7. Bitdefender registreren

Om te worden beveiligd door Bitdefender, dient u uw product te registreren met een licentiesleutel. De licentiesleutel bepaalt hoelang u het product mag gebruiken. Zodra de licentiesleutel vervalst, stopt Bitdefender met het uitvoeren van zijn functies en het beschermen van uw computer.

Enkele dagen voordat de huidige licentiesleutel aanschafft of vernieuwt, moet u een licentiesleutel aanschaffen of uw licentie vernieuwen. Meer informatie vindt u onder "*Licentiesleutels kopen of vernieuwen*" (p. 35). Als u een evaluatieversie van Bitdefender gebruikt, moet u deze registreren met een licentiesleutel als u product wilt blijven gebruiken nadat de evaluatieperiode is verlopen.

### 7.1. Uw licentiesleutel invoeren

Als u tijdens de installatie hebt gekozen om het product te evalueren, kunt u dit gedurende een evaluatieperiode van 30 dagen gebruiken. Om Bitdefender verder te blijven gebruiken na het verlopen van de evaluatieperiode, moet u het registreren met een licentiesleutel.

Een link die het aantal resterende dagen van uw licentie weergeeft, verschijnt onderaan het Bitdefender-venster. Klik op deze link om het registratievenster te openen.

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

Bitdefender Total Security 2013 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, klikt u op de koppeling die in het venster is voorzien om een webpagina te openen waar u een sleutel kunt aanschaffen.

2. Klik op **Nu registreren**.

Zelfs nadat u een licentiesleutel hebt gekocht, verschijnt Bitdefender Total Security 2013 in een demoversie totdat u de registratie binnen het product met de sleutel hebt voltooid.

## 7.2. Licentiesleutels kopen of vernieuwen

Als de evaluatieperiode binnenkort zal eindigen, moet u een licentiesleutel aanschaffen en uw product registreren. Zo moet u ook uw licentie vernieuwen als uw huidige licentiesleutel binnenkort vervalst.

Bitdefender zal u waarschuwen wanneer de vervaldatum van uw huidige licentie nadert. Volg de instructies in de waarschuwing om een nieuwe licentie aan te schaffen.

U kunt een webpagina bezoeken waar u op elk ogenblik een licentiesleutel kunt aanschaffen door deze stappen te volgen:

1. Het **Bitdefender-venster** openen.
2. Klik op de link die het aantal resterende dagen van uw licentie aangeeft en die zich bevindt onderaan het Bitdefender-venster, om het registratievenster van het product te openen.
3. Klik op **Geen licentiesleutel? Nu kopen.**
4. Er wordt een webpagina geopend op uw webbrowser waar u een Bitdefender-licentiesleutel kunt aanschaffen.

## 8. MyBitdefender-account

De online functies van uw product en extra Bitdefender-services zijn exclusief beschikbaar via MyBitdefender. U moet uw computer koppelen met MyBitdefender door bij een account aan te melden vanaf Bitdefender Total Security 2013 om een van de volgende bewerkingen uit te voeren:

- U kunt uw licentiesleutel ophalen als u deze ooit zou vergeten.
- Configureer de instellingen voor **Ouderlijk toezicht** voor de Windows-accounts van uw kinderen en bewaak hun activiteiten, waar u ook bent.
- Gebruik **Safebox** om een back-up te maken van uw belangrijke bestanden op online servers en om ze te synchroniseren.
- Geniet van bescherming van uw Facebook- en Twitter-account met **Safego**.
- Bescherm uw computer en gegevens tegen diefstal of verlies met **Antidiefstal**.
- Bitdefender Total Security 2013 **op afstand** beheren.

Er kunnen meerdere Bitdefender-beveiligingsoplossingen voor pc's, evenals andere platforms worden geïntegreerd in MyBitdefender. U kunt de beveiliging van alle apparaten die aan uw account zijn gekoppeld, beheren vanaf één gecentraliseerd dashboard.

Uw MyBitdefender-account is toegankelijk vanaf elk apparaat dat met internet is verbonden op <https://my.bitdefender.com>.

U kunt uw account ook direct vanaf uw product openen en beheren:

1. Het **Bitdefender-venster** openen.
2. Klik bovenaan in het venster op **MyBitdefender** en selecteer een optie in het vervolgkeuzemenu:
  - **Accountinstellingen**  
Meld u aan bij een account, maak een nieuwe account, configureer het gedrag van MyBitdefender.
  - **Dashboard**  
Start het MyBitdefender-dashboard in uw browser.
  - **Ouderlijk Toezicht**  
Het gebruik van de computer door uw kinderen bewaken en beheren.
  - **Anti-Theft**  
Bescherm uw computer en gegevens tegen diefstal of verlies.

## 8.1. Uw computer koppelen met MyBitdefender

Om uw computer te koppelen met een MyBitdefender-account, moet u aanmelden bij een account van Bitdefender Total Security 2013. Zolang u uw computer niet koppelt met MyBitdefender, zult u telkens worden gevraagd aan te melden bij MyBitdefender wanneer u een functie wilt gebruiken die een account vereist.

Volg de onderstaande stappen om het venster MyBitdefender te openen waarin u een account kunt maken of kunt aanmelden bij een account:

1. Het **Bitdefender-venster** openen.
2. Klik bovenaan in het venster op **MyBitdefender** en selecteer vervolgens **Accountinstellingen** in het vervolgkeuzemenu.

Als u al bent aangemeld bij een account, wordt de account waarbij u bent aangemeld, weergegeven. Klik op **Ga naar MyBitdefender** om naar uw dashboard te gaan. Om de account die met de computer is gekoppeld te wijzigen, moet u aanmelden bij een andere account.

Als u niet bent aangemeld bij een account, kunt u doorgaan in overeenstemming met uw situatie.

### Ik wil een MyBitdefender-account maken.

Volg deze stappen om een MyBitdefender-account te maken:

1. Selecteer **Een nieuwe account maken**.

Een nieuw venster wordt weergegeven.

2. Typ de vereiste informatie in de overeenkomende velden. De gegevens die u hier opgeeft blijven vertrouwelijk.

● **E-mail** - voer uw e-mailadres in.

● **Gebruikersnaam** - voer een gebruikersnaam voor uw account in.

● **Wachtwoord** - voer een wachtwoord in voor uw account. Het wachtwoord moet minstens 6 tekens lang zijn.

● **Wachtwoord bevestigen** - typ het wachtwoord opnieuw.

3. Klik op **Maken**.

4. Voordat u uw account kunt gebruiken, moet u de registratie voltooien. Controleer uw e-mail en volg de instructies in de bevestigings-e-mail die u ontvangen hebt van Bitdefender.

### Ik wil mij aanmelden met mijn Facebook- of Google-account

Volg deze stappen om u aan te melden bij uw Facebook- of Google-account.

1. Klik op het pictogram van de service die u wilt gebruiken om aan te melden. U wordt omgeleid naar de aanmeldingspagina van die service.
2. Volg de instructies die door de geselecteerde service worden gegeven om uw account te koppelen aan Bitdefender.



## Opmerking

Bitdefender krijgt geen toegang tot vertrouwelijke informatie, zoals het wachtwoord van de account die u gebruikt om aan te melden of de persoonlijke informatie van uw vrienden en contactpersonen.

## Ik heb al een MyBitdefender-account

Als u al een account hebt, maar nog niet bent aangemeld bij deze account, volgt u deze stappen om aan te melden:

1. 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 om het op te halen.

2. Klik op **Inloggen op MyBitdefender**.

Zodra de computer met een account is gekoppeld, kunt u het bijgeleverde e-mailadres en het wachtwoord gebruiken om u aan te melden bij <https://my.bitdefender.com>.

U kunt ook direct vanaf Bitdefender Total Security 2013 toegang krijgen tot uw account via het vervolgkeuzemenu bovenaan in het venster.

## 9. Bitdefender up-to-date houden

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. Standaard controleert het of er updates zijn als u uw computer aanzet en ieder **uur** daarna. Als er een update is gedetecteerd, wordt deze automatisch gedownload en geïnstalleerd op uw computer.

Het updateproces wordt geleidelijk uitgevoerd, wat betekent dat de te updaten bestanden een voor een worden vervangen. Hierdoor zal het updateproces de productwerking niet beïnvloeden en tegelijkertijd wordt elk zwak punt uitgesloten.



### Belangrijk

Houd Automatische update ingeschakeld om u te beschermen tegen de laatste bedreigingen.

In sommige specifieke situaties is uw tussenkomst vereist om de bescherming van uw Bitdefender up-to-date te houden:

- Als uw computer een internetverbinding maakt via een proxyserver, moet u de proxy-instellingen configureren zoals beschreven in *"Bitdefender configureren voor het gebruik van een proxy-internetverbinding"* (p. 65).
- Als u geen internetverbinding hebt, kunt u Bitdefender handmatig bijwerken zoals beschreven in *"Mijn computer is niet verbonden met internet. Hoe kan ik Bitdefender updaten?"* (p. 173). Het handmatige updatebestand wordt eenmaal per week uitgegeven.
- Er kunnen fouten optreden tijdens het downloaden van updates bij een trage internetverbinding. Raadpleeg *"Bitdefender updaten bij een langzame internetverbinding"* (p. 172) voor meer informatie over het oplossen van dergelijke fouten.
- Als u met het internet bent verbonden via een inbelverbinding, dan adviseren wij Bitdefender regelmatig handmatig te updaten. Meer informatie vindt u onder *"Een update uitvoeren"* (p. 40).

### 9.1. Controleren of Bitdefender up-to-date is

Volg deze stappen om te controleren of uw Bitdefender-bescherming up-to-date is:

1. Het **Bitdefender-venster** openen.
2. Kijk op het **Update**-paneel van wanneer de laatste update dateert, net onder de naam van het paneel.



Controleer de updategebeurtenissen voor gedetailleerde informatie over de laatste updates:


1. Klik in het hoofdvenster op **Gebeurtenissen** in de werkbalk bovenaan.
2. Klik in het venster met het **Gebeurtenissenoverzicht** op **Update**.

U kunt uitzoeken wanneer updates werden gestart en u kunt informatie over de updates weergeven (of ze al dan niet gelukt zijn, of het opnieuw opstarten is vereist om de installatie te voltooien, enz.); Start, indien nodig, het systeem zo snel mogelijk opnieuw op.

## 9.2. Een update uitvoeren

Om updates uit te voeren is een internetverbinding vereist.

Voer een van de volgende bewerkingen uit om een update te starten:

- Open het Bitdefender-venster en klik op **Nu updaten** op het **Update**-paneel .
- Klik met de rechtermuisknop op het Bitdefender-pictogram  in het **stelselvak** en selecteer **Nu bijwerken**.

De module Update maakt een verbinding met de updateserver van Bitdefender en controleert op updates. Als een update is gedetecteerd, wordt u gevraagd de update te bevestigen, of wordt de update automatisch uitgevoerd, afhankelijk van de **Update-instellingen**.



### Belangrijk

Het kan noodzakelijk zijn de computer opnieuw op te starten wanneer de update is voltooid. Wij adviseren dit zo snel mogelijk te doen.

## 9.3. De automatische update in- of uitschakelen

Volg deze stappen om de automatische update in of uit te schakelen:

1. Het **Bitdefender-venster** openen.
2. Op het **Update**-paneel klikt u op de schakelaar **Auto Update**.
3. Er verschijnt een waarschuwingsvenster. U moet uw keuze bevestigen door in het menu te selecteren hoelang u de automatische update wilt uitschakelen. U kunt de automatische update uitschakelen gedurende 5, 15 of 30 minuten, 1 uur, definitief of tot het systeem opnieuw wordt opgestart.



### Waarschuwing

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

## 9.4. De update-instellingen aanpassen

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.

De standaardinstellingen voor de update zijn geschikt voor de meeste gebruikers en u hoeft ze normaal niet te wijzigen.

Volg deze stappen om de update-instellingen te wijzigen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Update**.
4. Pas in het venster met **Update-instellingen** de instellingen volgens uw voorkeuren aan.

### Update-locatie

Bitdefender is geconfigureerd om een update uit te voeren vanaf de Bitdefender-updateservers op internet. De updatelocatie is <http://upgrade.bitdefender.com>, een algemeen internetadres dat automatisch wordt omgeleid naar dichtstbijzijnde Bitdefender-updateserver in uw regio.

Wijzig de updatelocatie niet tenzij u dit wordt aangeraden door een Bitdefender-vertegenwoordiger of door uw netwerkbeheerder (als u verbonden bent met een kantoor netwerk).

U kunt terugkeren naar de algemene locatie voor internetupdates door op **Standaard** te klikken.

### Regels voor behandelen updates

U hebt de keuze uit drie manieren voor het downloaden en installeren van de updates.

- **Stille update** - Bitdefender downloadt en installeert de update automatisch.
- **Herinneren voor het downloaden** - telkens wanneer een update beschikbaar is, wordt uw bevestiging gevraagd voordat de update wordt gedownload.
- **Herinneren voor het installeren** - telkens wanneer een update is gedownload, wordt uw bevestiging gevraagd voordat de update wordt geïnstalleerd.

Voor sommige updates moet het systeem opnieuw worden opgestart om de installatie te voltooien. Als een update het opnieuw opstarten van het systeem vereist, blijft Bitdefender werken met de oude bestanden tot de gebruikers de

computer opnieuw opstart. Hiermee wordt voorkomen dat de Bitdefender-update het werk van de gebruiker hinder.

Als u een vraag om bevestiging wilt wanneer een update het opnieuw opstarten van het systeem vereist, schakelt u de optie **Opnieuw opstarten uitstellen** uit door op de overeenkomende schakelaar te klikken.

## P2P-updates

Naast het normale updatemechanisme, gebruikt Bitdefender ook een slim systeem voor het delen van updates, gebaseerd op een peer-to-peer-protocol (P2P) voor het distribueren van updates van malwarehandtekeningen tussen gebruikers van Bitdefender.

U kunt de opties voor de P2P-update in- of uitschakelen met de overeenkomende schakelaars.

### **P2P-update-systeem gebruiken**

Schakel deze optie in voor het downloaden van updates van malwarehandtekeningen van andere Bitdefender-gebruikers die het P2P-updatesysteem gebruiken. Bitdefender gebruikt poorten 8880 - 8889 voor peer-to-peer update.

### **Bitdefender-bestanden distribueren**

Schakel deze optie in om de nieuwste beschikbare malwarehandtekeningen op uw computer te delen met andere Bitdefender-gebruikers.

Zo werkt het

## 10. Installatie

### 10.1. Hoe installeer ik Bitdefender op een tweede computer?

Als u een licentiesleutel voor meer dan één computer hebt aangeschaft, kunt u dezelfde licentiesleutel gebruiken voor het registreren van een tweede pc.

Volg deze stappen om Bitdefender correct te installeren op een tweede computer:

1. Installeer Bitdefender vanaf de cd/dvd of met het installatieprogramma dat is geleverd bij de e-mail van de online aankoop en volg dezelfde installatiestappen.
2. Wanneer het registratievenster verschijnt, voert u de licentiesleutel in en klikt u op **Nu registreren**.
3. In de volgende stap kunt u aanmelden bij uw MyBitdefender-account of een nieuwe MyBitdefender-account maken.

U kunt er ook voor kiezen later een MyBitdefender-account te maken.

4. Wacht tot het installatieproces is voltooid en sluit het venster.

### 10.2. Wanneer moet ik Bitdefender opnieuw installeren?

In sommige situaties zult u mogelijk uw Bitdefender-product opnieuw moeten installeren.

Typische situaties waarin u Bitdefender opnieuw moet installeren, zijn ondermeer de volgende:

- u hebt het besturingssysteem opnieuw geïnstalleerd.
- u hebt een nieuwe computer aangeschaft
- u wilt de weergavetaal van de Bitdefender-interface wijzigen

Om Bitdefender opnieuw te installeren, kunt u de installatieschijf gebruiken die u hebt aangeschaft of kunt u een nieuwe versie downloaden van de [Bitdefender-website](#).

Tijdens de installatie wordt u gevraagd het product te registreren met uw licentiesleutel.

Als u uw licentiesleutel niet kunt vinden, kunt u zich aanmelden bij <https://my.bitdefender.com> om de sleutel op te halen. Voer het e-mailadres en wachtwoord van uw account in de overeenkomende velden in.

## 10.3. Hoe kan ik schakelen van het ene Bitdefender 2013-product naar het andere?

U kunt gemakkelijk schakelen van het ene Bitdefender 2013-product naar een ander product.

Dit zijn de drie Bitdefender 2013-producten die u op uw systeem kunt installeren:

- Bitdefender Antivirus Plus 2013
- Bitdefender Internet Security 2013
- Bitdefender Total Security 2013

Als u een ander Bitdefender 2013-product dan het product dat u hebt aangeschaft, wilt installeren op uw systeem, volgt u deze stappen:

1. Het **Bitdefender-venster** openen.
2. Een link die het aantal resterende dagen van uw licentie weergeeft, verschijnt onderaan het Bitdefender-venster. Klik op deze link om het registratievenster te openen.
3. Voer de licentiesleutel in en klik op **Nu registreren**.
4. Bitdefender zal u laten weten dat de licentiesleutel voor een ander product is en u de mogelijkheid bieden dit te installeren. Klik op de overeenkomende koppeling en volg de procedure om de installatie uit te voeren.

## 11. Registratie

### 11.1. Welk Bitdefender-product gebruik ik?

Volg deze stappen om uit te zoeken welk Bitdefender-programma u hebt geïnstalleerd:

1. Het **Bitdefender-venster** openen.
2. Bovenaan het venster zou u een van de volgende items moeten zien:
  - Bitdefender Antivirus Plus 2013
  - Bitdefender Internet Security 2013
  - Bitdefender Total Security 2013

### 11.2. Een evaluatieversie registreren

Als u een evaluatieversie hebt geïnstalleerd, kunt u deze slechts voor een beperkte periode gebruiken. Om Bitdefender verder te blijven gebruiken na het verlopen van de evaluatieperiode, moet u het registreren met een licentiesleutel.

Volg deze stappen om Bitdefender uit te schakelen:

1. Het **Bitdefender-venster** openen.
2. Een link die het aantal resterende dagen van uw licentie weergeeft, verschijnt onderaan het Bitdefender-venster. Klik op deze link om het registratievenster te openen.
3. Voer de licentiesleutel in en klik op **Nu registreren**.

Als u geen licentiesleutel hebt, klikt u op de koppeling die in het venster is voorzien om naar een webpagina te gaan waar u een sleutel kunt aanschaffen.

4. Wacht tot het registratieproces is voltooid en sluit het venster.

### 11.3. Wanneer verloopt mijn Bitdefender-bescherming?

Volg deze stappen om uit te zoeken hoeveel dagen uw licentiesleutel nog geldig is:

1. Het **Bitdefender-venster** openen.
2. Een link die het aantal resterende dagen van uw licentie weergeeft, verschijnt onderaan het Bitdefender-venster.
3. Klik voor extra informatie op de koppeling om het registratievenster te openen.
4. In het venster **Uw product registreren** kunt u het volgende:
  - De huidige licentiesleutel weergeven
  - Registreren met een andere licentiesleutel

- Licentiesleutels aanschaffen

## 11.4. Hoe kan ik Bitdefender registreren zonder internetverbinding?

Als u net Bitdefender hebt aangeschaft en geen internetverbinding hebt, kunt u Bitdefender nog steeds offline registreren.

Volg deze stappen om Bitdefender te registreren met uw licentiesleutel:

1. Ga naar een pc die verbonden is met internet. U kunt bijvoorbeeld de computer van een vriend of een pc vanaf een openbare plaats gebruiken.
2. Ga naar <https://my.bitdefender.com> om een MyBitdefender-account te maken.
3. Log in op uw account.
4. Klik bovenaan op uw gebruikersnaam en selecteer **Producten** in het vervolgkeuzemenu.
5. Klik op **Offline registratie**.
6. Voer de licentiesleutel in die u hebt aangeschaft.
7. Klik op **Verzenden** om een bevestigingscode te verkrijgen.



**Belangrijk**  
Noteer de bevestigingscode.

8. Terugkeren naar uw pc met de bevestigingscode.
9. Het **Bitdefender-venster** openen.
10. Een link die het aantal resterende dagen van uw licentie weergeeft, verschijnt onderaan het Bitdefender-venster. Klik op deze link om het registratievenster te openen.
11. Voer de machtigingscode in het overeenkomende veld in en klik op **Nu registreren**.
12. Wacht tot het registratieproces is voltooid.

## 11.5. Hoe kan ik mijn Bitdefender-beveiliging vernieuwen?

Wanneer de beveiliging van Bitdefender op het punt staat te vervallen, moet u uw licentiesleutel vernieuwen.

- Volg deze stappen om een website te bezoeken waar u uw Bitdefender-licentiesleutel kunt verlengen:

1. Het **Bitdefender-venster** openen.



2. Een link die het aantal resterende dagen van uw licentie weergeeft, verschijnt onderaan het Bitdefender-venster. Klik op deze link om het registratievenster te openen.
3. Klik op **Geen licentiesleutel? Nu kopen.**
4. Er wordt een webpagina geopend op uw webbrowser waar u een Bitdefender-licentiesleutel kunt aanschaffen.



## Opmerking

Als alternatief kunt u contact opnemen met de kleinhandelaar bij wie u het Bitdefender-product hebt gekocht.

- Volg deze stappen om uw Bitdefender te registreren met de nieuwe licentiesleutel:
  1. Het **Bitdefender-venster** openen.
  2. Een link die het aantal resterende dagen van uw licentie weergeeft, verschijnt onderaan het Bitdefender-venster. Klik op deze link om het registratievenster te openen.
  3. Voer de licentiesleutel in en klik op **Nu registreren.**
  4. Wacht tot het registratieproces is voltooid en sluit het venster.

Voor meer informatie kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in sectie "*Hulp vragen*" (p. 192).

## 12. Scannen met Bitdefender

### 12.1. Een bestand of map scannen

De eenvoudigste en aanbevolen manier om een bestand of map te scannen is klikken met de rechtermuisknop op het object dat u wilt scannen, Bitdefender aanwijzen en **Scannen met Bitdefender** te selecteren in het menu. Volg de Antivirusscanwizard om de scan te voltooien. Bitdefender zal automatisch de aanbevolen acties ondernemen op de gedetecteerde bestanden.

Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen.

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.

### 12.2. Hoe kan ik mijn systeem scannen?

Volg deze stappen om een volledige scan op het systeem uit te voeren:

1. Het **Bitdefender-venster** openen.
2. Klik in het **Antivirus**-paneel op **Nu scannen** en selecteer **Systeemsan** in het uitklapbaar keuzemenu.
3. Volg de Antivirusscanwizard om de scan te voltooien. Bitdefender zal automatisch de aanbevolen acties ondernemen op de gedetecteerde bestanden. Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen. Meer informatie vindt u onder "**Antivirusscanwizard**" (p. 82).

### 12.3. Een aangepaste scantaak maken

Als u specifieke locaties wilt scannen op uw computer of de scanopties wilt configureren, kunt u een aangepaste scantaak configureren en uitvoeren.

Ga als volgt te werk om een aangepaste scantaak te maken:

1. Het **Bitdefender-venster** openen.
2. Klik in het **Antivirus**-paneel op **Nu scannen** en selecteer **Aangepaste scan** in het uitklapbaar keuzemenu.
3. Klik op **Doel toevoegen** om de te scannen bestanden of mappen te selecteren.

4. Klik op **Scanopties** als u de scanopties in detail wilt configureren.  
U kunt de scanopties gemakkelijk configureren door het scanniveau aan te passen. Sleep de schuifregelaar langs de schaal om het gewenste scanniveau in te stellen.  
U kunt er ook voor kiezen de computer uit te schakelen wanneer de scan is voltooid en er geen bedreigingen zijn gevonden. Denk eraan dat dit, telkens wanneer u deze taak uitvoert, het standaard gedrag zal zijn.
5. Klik op **Scannen starten** en volg de **Antivirusscanwizard** om het scannen te voltooien. Aan het einde van de scan wordt u gevraagd te kiezen welke acties moeten worden ondernemen op de gedetecteerde bestanden, als die er zijn.
6. Als u de scantask wilt opslaan voor toekomstig gebruik, opent u het venster voor de aangepaste scanconfiguratie opnieuw.
7. Zoek de scan die u net hebt uitgevoerd in de lijst **Recente scans**.
8. Beweeg met de muiscursor over de naam van de scan en klik op het pictogram  om de scan toe te voegen aan de lijst met favoriete scans.
9. Voer een gemakkelijk te onthouden naam in voor de scan.

## 12.4. Een map uitsluiten van de scan

Met Bitdefender kunt u specifieke bestanden, mappen of bestandsextensies uitsluiten van het scannen.

Uitsluitingen zijn bedoeld voor gebruikers met een gevorderde computerkennis en alleen in de volgende situaties:

- U hebt een grote map op uw systeem waarin u films en muziek bewaart.
- U hebt een groot archief op uw systeem waarin u verschillende gegevens bewaart.
- U bewaart een map waarin u verschillende types software en toepassingen installeert voor testdoeleinden. Het scannen van de map kan resulteren in het verlies van bepaalde gegevens.

Volg deze stappen om de map toe te voegen aan de lijst Uitsluitingen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Antivirus**.
4. Selecteer in het venster met **Antivirustellingen** de tab **Uitsluitingen**.
5. Zorg dat **Uitsluitingen voor bestanden** is ingeschakeld door op de schakelaar te klikken.
6. Klik op de koppeling **Uitgesloten bestanden en mappen**.
7. Klik bovenaan in de tabel met uitsluitingen op de knop **Toevoegen**.

8. Klik op **Bladeren**, selecteer het bestand of de map die u wilt uitsluiten van de scan en klik vervolgens op **OK**.
9. Klik op **Toevoegen** en klik vervolgens op **OK** om de wijzigingen op te slaan en het venster te sluiten.

## 12.5. Wat moet ik doen wanneer Bitdefender een schoon bestand als geïnficeerd beschouwt?

Er zijn gevallen waarbij Bitdefender een rechtmatig bestand verkeerdelijk markeert als een bedreiging (vals positief). Om deze fout te corrigeren, voegt u het bestand toe aan het gebied Uitsluitingen van Bitdefender:

1. Schakel de real time-antivirusbeveiliging van Bitdefender uit.
  - a. Het **Bitdefender-venster** openen.
  - b. Klik op de knop **Instellingen** in de werkbalk bovenaan.
  - c. Selecteer in het venster met het **Instellingenoverzicht Antivirus**.
  - d. Selecteer in het venster met **Antivirusinstellingen** de tab **Beveiliging**.
  - e. Klik op de schakelaar om **Scannen bij toegang** uit te schakelen.
2. Verborgen objecten weergeven in Windows. Raadpleeg "*Verborgen objecten weergeven in Windows*" (p. 67) voor meer informatie hierover.
3. Het bestand herstellen vanaf het quarantainegebied:
  - a. Het **Bitdefender-venster** openen.
  - b. Klik op de knop **Instellingen** in de werkbalk bovenaan.
  - c. Selecteer in het venster met het **Instellingenoverzicht Antivirus**.
  - d. Selecteer in het venster met **Antivirusinstellingen** de tab **Quarantaine**.
  - e. Selecteer het bestand en klik op **Herstel**.
4. Het bestand toevoegen aan de lijst Uitsluitingen. Raadpleeg "*Een map uitsluiten van de scan*" (p. 50) voor meer informatie hierover.
5. Schakel de real time antivirusbeveiliging van Bitdefender in.
6. Neem contact op met de medewerkers van onze ondersteuningsdienst zodat wij de detectiehandtekening kunnen verwijderen. Raadpleeg "*Hulp vragen*" (p. 192) voor meer informatie hierover.

## 12.6. Hoe kan ik controleren welke virussen Bitdefender heeft gedetecteerd?

Telkens wanneer een scan wordt uitgevoerd, wordt een scanlogboek gemaakt en registreert Bitdefender de verwijderde problemen.

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

Zodra het scannen is voltooid, kunt u het scanlogboek direct vanaf de scanwizard openen door op **Logboek weergeven** te klikken.

Om een scanverslag of een willekeurige gedetecteerde infectie op een later tijdstip te controleren, volgt u deze stappen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Gebeurtenissen** in de werkbalk bovenaan.
3. Selecteer in het venster **GebeurtenissenoverzichtAntivirus**.
4. Selecteer in het venster met **Antivirusgebeurtenissen** de tab **Virusscan**. Hier vindt u alle gebeurtenissen van scans op malware, inclusief bedreigingen die zijn gedetecteerd door Scannen bij toegang, door gebruiker gestarte scans en statuswijzigingen voor automatische scans.
5. In de gebeurtenissenlijst kunt u controleren welke scans onlangs werden uitgevoerd. Klik op een gebeurtenis om details erover weer te geven.
6. Klik op **Logboek weergeven** om het scanlogboek te openen. Het scanlogboek wordt geopend in een nieuw venster.

## 13. Ouderlijk Toezicht

### 13.1. Mijn kinderen beschermen tegen online bedreigingen

Met Ouderlijk toezicht van Bitdefender kunt u de toegang tot internet en specifieke toepassingen beperken en voorkomen dat uw kinderen ongepaste inhoud bekijken wanneer u niet in de buurt bent.

Volg deze stappen om Ouderlijk toezicht te configureren:

1. Creëer beperkte (standaard) Windows gebruikersaccounts voor uw kinderen. Meer informatie vindt u onder "*Windows-gebruikersaccounts maken*" (p. 55).
2. Zorg dat u bij de computer bent aangemeld met een beheerdersaccount. Alleen gebruikers met beheerdersrechten (administrators) op het systeem kunnen Ouderlijk Toezicht openen en configureren.
3. Configureer Ouderlijk Toezicht voor de Windows gebruikersaccounts van uw kinderen.
  - a. Het **Bitdefender-venster** openen.
  - b. Klik bovenaan in het venster op de knop **MyBitdefender** en selecteer **Ouderlijk toezicht** in het vervolgkeuzemenu.
  - c. Het dashboard Ouderlijk toezicht wordt geopend in een nieuw venster. Hier kunt u de instellingen voor Ouderlijk toezicht controleren en configureren.
  - d. Klik in het menu aan de linkerzijde op **Kind toevoegen**.
  - e. Voer de naam en leeftijd van het kind in op het tabblad **Profiel**. Wanneer u de leeftijd van het kind instelt, worden de instellingen die voor die leeftijdscategorie als geschikt worden beschouwd, automatisch geladen volgens de ontwikkelingsnormen van het kind.

Controleer de activiteiten van uw kinderen en wijzig de instellingen voor Ouderlijk toezicht via MyBitdefender vanaf elke computer of elk mobiel apparaat met internetverbinding.

Meer gedetailleerde informatie over het gebruik van Ouderlijk toezicht, vindt u onder "*Ouderlijk Toezicht*" (p. 138).

### 13.2. Hoe kan ik de internettoegang beperken voor mijn kind?

Nadat u Ouderlijk toezicht hebt geconfigureerd, kunt u gemakkelijk de internettoegang blokkeren voor specifieke perioden.

Via Ouderlijk toezicht van Bitdefender kunt u het gebruik van uw kinderen controleren, zelfs als u niet thuis bent.

Volg deze stappen om de internettoegang te beperken voor bepaalde perioden van de dag:

1. Open een webbrowser op een willekeurig apparaat met internettoegang.
2. Ga naar:<https://my.bitdefender.com>
3. Meld u aan bij uw account met uw gebruikersnaam en wachtwoord.
4. Klik op **Ouderlijk toezicht** om het dashboard te openen.
5. Selecteer het profiel van uw kind in het menu aan de linkerzijde.
6. Klik op  in het paneel **Web** om het venster **Webactiviteit** te openen.
7. Klik op **Planning**.
8. Selecteer de tijdsintervallen in het rooster voor het blokkeren van de internettoegang. U kunt op individuele cellen klikken of klikken en slepen om langere perioden te dekken. Klik op **Opnieuw instellen** om een nieuwe selectie te starten.
9. Klik op **OK**.



#### Opmerking

Bitdefender zal elk uur een update uitvoeren, ongeacht of de webtoegang is geblokkeerd.

## 13.3. Hoe blokkeer ik de toegang van mijn kind tot een website?

Met Ouderlijk toezicht van Bitdefender kunt u de inhoud die door uw kind bekeken tijdens het gebruik van de computer, controleren. U kunt ook de toegang tot een website blokkeren, zelfs wanneer u niet thuis bent.

Via Ouderlijk toezicht van Bitdefender kunt u het gebruik van uw kinderen controleren, zelfs als u niet thuis bent.

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

1. Open een webbrowser op een willekeurig apparaat met internettoegang.
2. Ga naar:<https://my.bitdefender.com>
3. Meld u aan bij uw account met uw gebruikersnaam en wachtwoord.
4. Klik op **Ouderlijk toezicht** om het dashboard te openen.
5. Selecteer het profiel van uw kind in het menu aan de linkerzijde.
6. Klik op  in het paneel **Web** om het venster **Webactiviteit** te openen.
7. Klik op **Zwarte lijst**.

8. Voer het websiteadres in het overeenkomende veld in en klik op **Toevoegen**.
9. De website is toegevoegd aan de lijst van geblokkeerde websites.

## 13.4. Hoe verhinder ik dat mijn kind een spel speelt?

Met Bitdefender Ouderlijk toezicht hebt u het beheer over de inhoud waarvoor uw kind toegang hebben wanneer ze de computer gebruiken.

Als u de toegang tot een spel of toepassing moet beperken, kunt u Ouderlijk toezicht van Bitdefender gebruiken, zelfs als u niet thuis bent.

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

1. Open een webbrowser op een willekeurig apparaat met internettoegang.
2. Ga naar:<https://my.bitdefender.com>
3. Meld u aan bij uw account met uw gebruikersnaam en wachtwoord.
4. Klik op **Ouderlijk toezicht** om het dashboard te openen.
5. Selecteer het profiel van uw kind in het menu aan de linkerzijde.
6. Klik op  in het paneel **Toepassingen** om het venster **Activiteit toepassingen** te openen.
7. Klik op **Zwarte lijst**.
8. Typ (of kopieer en plak) het pad naar het uitvoerbaar bestand in het overeenkomende veld.
9. Klik op **Toevoegen** om de toepassing toe te voegen aan de **Zwarte lijst toepassingen**.

## 13.5. Windows-gebruikersaccounts maken

Een Windows-gebruikersaccount is een uniek profiel dat alle instellingen, privileges en persoonlijke bestanden voor elke gebruiker bevat. Via de Windows-accounts kan de beheerder van de thuis-pc de toegang voor elke gebruiker beheren.

Het instellen van gebruikersaccounts is handig wanneer de pc zowel door ouders als door kinderen wordt gebruikt. Ouders kunnen accounts instellen voor elk kind.

Selecteer uw besturingssysteem voor meer informatie over het maken van Windows-accounts.

### ● Windows XP:

1. Meld u als beheerder aan op uw computer.
2. Klik op Start, Configuratiescherm en daarna op Gebruikersaccounts.
3. Klik op Een nieuwe account maken.



4. Voer de naam in voor de gebruiker. U kunt de volledige naam, de voornaam of een bijnaam van de persoon gebruiken. Klik daarna op Volgende.
  5. Kies voor het accounttype de optie Beperkt en vervolgens Account maken. Beperkte accounts zijn geschikt voor kinderen omdat ze dan geen wijzigingen aan het systeem kunnen aanbrengen of bepaalde toepassingen kunnen installeren.
  6. Uw nieuwe account wordt gemaakt en weergegeven in het scherm Accounts beheren.
- Windows Vista of Windows 7:
1. Meld u als beheerder aan op uw computer.
  2. Klik op Start, Configuratiescherm en daarna op Gebruikersaccounts.
  3. Klik op Een nieuwe account maken.
  4. Voer de naam in voor de gebruiker. U kunt de volledige naam, de voornaam of een bijnaam van de persoon gebruiken. Klik daarna op Volgende.
  5. Klik voor het accounttype op Standaard en vervolgens op Account maken. Beperkte accounts zijn geschikt voor kinderen omdat ze dan geen wijzigingen aan het systeem kunnen aanbrengen of bepaalde toepassingen kunnen installeren.
  6. Uw nieuwe account wordt gemaakt en weergegeven in het scherm Accounts beheren.



## Opmerking

Nu u nieuwe gebruikersaccounts hebt toegevoegd, kunt u wachtwoorden maken voor de accounts.

## 14. Privacybeheer

### 14.1. Hoe kan ik controleren of mij online transactie beveiligd is?


Als u wilt controleren of uw online bewerkingen privé blijven, kunt u de browser die door Bitdefender is geleverd, gebruiken voor het beschermen van uw transacties en toepassingen voor thuisbankieren.

Bitdefender Safepay is een beveiligde browser die is ontwikkeld om uw creditcardgegevens, accountnummer of andere vertrouwelijke gegevens die u mogelijk invoert bij toegang tot verschillende online locaties, te beschermen.

Volg deze stappen om uw online activiteit veilig en privé te houden:

1. Dubbelklik op het Bitdefender Safepay-pictogram op uw bureaublad.

De Bitdefender Safepay-browser verschijnt.

2. Klik op de knop  om toegang te krijgen tot het **virtuele toetsenbord**.
3. Gebruik het **virtuele toetsenbord** wanneer u vertrouwelijke informatie, zoals uw wachtwoorden, invoert.

### 14.2. Wat kan ik doen als mijn systeem gestolen wordt?

Laptopdiefstal is een van de grootste problemen vandaag die individuele personen en organisaties in de hele wereld beïnvloedt.

Met Bitdefender Antidiefstal kunt u niet alleen de gestolen laptop zoeken en vergrendelen, maar kunt u ook alle gegevens wissen om zeker te zijn dat ze niet worden gebruikt door de dief.

Om naar de antidiefstalfuncties te gaan vanuit uw account, volgt u deze stappen:

1. Ga naar <https://my.bitdefender.com> en log in op uw account.
2. Klik op **Antidiefstal**.
3. Selecteer uw computer in de lijst met apparaten.
4. Selecteer de functie die u wilt gebruiken:



- **Localiseren** - geef de locatie van uw apparaat weer op Google Maps.



- **Wissen** - verwijder alle gegevens van uw computer.



**Belangrijk**

Nadat u een apparaat hebt gewist, stoppen de functies van Antidiefstal.



- **Vergrendelen** - Vergrendel uw computer en stel een numerieke PINcode in om hem te ontgrendelen.

## 14.3. Hoe kan ik mijn Facebook-account beschermen?

Safego is een Facebook-toepassing die is ontwikkeld door Bitdefender om uw sociale netwerkaccount veilig te houden.

Deze module heeft de taak de koppelingen die u ontvangt van uw Facebook-vrienden te scannen en de privacy-instellingen van uw account te bewaken.

Volg deze stappen om Safego te openen vanaf uw Bitdefender-product:

1. Het **Bitdefender-venster** openen.
2. Op het **Safego**-paneel klikt u op **Beheren** en selecteert u **Activeren voor Facebook** op het uitklapbaar keuzemenu. U wordt naar uw account gebracht.

Als u Safego for Facebook al hebt geactiveerd, zult u de statistieken met betrekking tot de activiteiten ervan kunnen openen door op de knop **Rapporten voor Facebook weergeven** te klikken.

3. Gebruik uw Facebook-aanmeldingsgegevens om een verbinding te maken met de Safego-toepassing.
4. Safego-toegang tot uw Facebook-account toestaan.

## 14.4. Bestandskluizen gebruiken

Met Bitdefender Bestandskluis kunt u gecodeerde, door een wachtwoord beveiligde logische schijven (of kluizen) op uw computer maken waar u uw confidentiële en gevoelige documenten veilig kunt opslaan. De kluis is in werkelijkheid een bestand dat op de lokale harde schijf is opgeslagen met de extensie .bvd.

Wanneer u een bestandskluis maakt, zijn twee aspecten belangrijk: de grootte en het wachtwoord. De standaardgrootte van 50 MB zou moeten voldoende zijn voor uw persoonlijke documenten, Excel-bestanden en dergelijke. Voor video's of andere grote bestanden kunt u echter meer ruimte nodig hebben.

Volg de onderstaande stappen om uw vertrouwelijke of gevoelige bestanden of mappen veilig op te slaan in Bitdefender-bestandskluizen:

- **Maak een bestandskluis en stel er een sterk wachtwoord voor in.**

Om een kluis te maken en te openen, klikt u met de rechtermuisknop in een leeg gebied op het bureaublad of in een map op uw computer. Wijs vervolgens Bitdefender Bestandskluis aan en selecteer **Kluis maken**.

Een nieuw venster wordt weergegeven. Ga als volgt te werk:

1. Klik op **Bladeren**, selecteer de plaats van de kluis en sla het kluisbestand op met de door u gewenste naam.

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 wachtwoord voor de kluis in de velden **Wachtwoord** en **Bevestigen** in.
4. Als u de standaardgrootte (50 MB) van de kluis wilt veranderen, typt u de gewenste waarde in het **Kluisgrootte** veld.
5. 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 en Openen**.



## Opmerking

Als u de kluis opent, verschijnt een virtuele schijf in **Deze computer**. De schijf heeft de schijfletter die is toegewezen aan de kluis.

### ● **Voeg de bestanden of mappen die u wilt beveiligen toe aan de kluis.**

Om een bestand aan een kluis toe te voegen, moet u eerst de kluis openen.

1. Blader naar het bvd-kluisbestand.
2. Klik met de rechtermuisknop op het kluisbestand, selecteer Bitdefender Bestandskluis en selecteer **Openen**.
3. Selecteer in het venster dat verschijnt een stationsletter die u aan de kluis wilt toewijzen, voer het wachtwoord in en klik op **Openen**.

U kunt nu via Windows Verkenner bewerkingen uitvoeren op het station dat overeenkomt met de gewenste bestandskluis, net zoals bij een gewoon station. Om een bestand aan een open kluis toe te voegen, kunt u ook met de rechtermuisknop op een bestand klikken, Bitdefender bestandskluis aanwijzen en **Toevoegen aan bestandskluis** selecteren.

### ● **Houd de kluis op elk ogenblik vergrendeld.**

Open alleen kluizen als de toegang vereist is of als u hun inhoud moet beheren. Om een kluis te vergrendelen, klikt u met de rechtermuisknop op het overeenkomende virtuele schijfstation onder **Deze computer**. Wijs vervolgens **Bitdefender Bestandskluis** aan en selecteer **Vergrendelen**.

### ● **Zorg dat u het bvd-kluisbestand niet verwijdert.**

Wanneer u het bestand verwijdert, wordt ook de inhoud van de kluis verwijderd.

Raadpleeg "**Bestandscodering**" (p. 113) voor meer informatie over het werken met bestandskluizen.

## 14.5. Hoe kan ik een bestand definitief verwijderen met Bitdefender?

Als u een bestand definitief van uw systeem wilt verwijderen, moet u de gegevens fysiek verwijderen van uw harde schijf.

De Bestandsvernietiging van Bitdefender zal u helpen om bestanden of mappen snel permanent te verwijderen van uw computer via het contextmenu van Windows:

1. Klik met de rechtermuisknop op het bestand of de map die u definitief wilt verwijderen, wijs Bitdefender aan en selecteer **Bestandsvernietiging**.
2. Er wordt een bevestigingsvenster weergegeven. Klik op **Ja** om de wizard Bestandsvernietiging te starten.
3. Wacht tot Bitdefender het vernietigen van de bestanden heeft voltooid.
4. De resultaten worden weergegeven. Klik op **Sluiten** om de wizard af te sluiten.

## 15. Tune-up

### 15.1. Mijn systeemprestaties verbeteren

De systeemprestaties zijn niet alleen afhankelijk van hardwareconfiguratie, zoals de CPU-belasting, het geheugengebruik en de harde schijfruimte. Deze is ook gekoppeld aan uw softwareconfiguratie en uw gegevensbeheer.

Dit zijn de belangrijkste acties die u kunt ondernemen met Bitdefender om de snelheid en prestaties van uw systeem te verbeteren:

- *“Uw harde schijf defragmenteren”* (p. 61)
- *“Uw pc opruimen”* (p. 61)
- *“Windows-register opruimen”* (p. 62)
- *“Scan uw systeem periodiek”* (p. 62)

#### 15.1.1. Uw harde schijf defragmenteren

Het is aanbevolen de harde schijf te defragmenteren om sneller toegang te krijgen tot uw bestanden en de algemene systeemprestaties te verbeteren. Schijfdefragmentatie helpt u bij het beperken van de bestandsfragmentatie en verbetert de prestaties van uw systeem.

Volg deze stappen om de Schijfdefragmentatie te starten:

1. Het **Bitdefender-venster** openen.
2. Klik op het **Tune-Up**-paneel op **Optimaliseren** en selecteer **Schijfdefragmentatie** vanuit het uitklapbaar keuzemenu.
3. Volg de stappen van de wizard.

#### 15.1.2. Uw pc opruimen

Pc-opruiming verbetert de systeemprestaties door de bestanden te verwijderen die niet langer nuttig zijn, zoals: tijdelijke internetbestanden, cookies en tijdelijke systeembestanden.

Volg deze stappen om de pc-opruiming te starten:

1. Het **Bitdefender-venster** openen.
2. Klik op het **Tune-Up**-paneel op **Optimaliseren** en selecteer **PC-opruiming** vanuit het uitklapbaar keuzemenu.
3. Volg de stappen van de wizard.

## 15.1.3. Windows-register opruimen

U kunt de prestaties van uw systeem verbeteren door het Windows-register op te ruimen. Gebruik hiervoor de Registeropruiming. Registeropruiming scant het Windows-register en verwijdert ongeldige registersleutels.

Volg deze stappen om de Registeropruiming te starten:

1. Het **Bitdefender-venster** openen.
2. Klik op het **Tune-Up**-paneel op **Optimaliseren** en selecteer **Registeropruiming** vanuit het uitklapbaar keuzemenu.
3. Volg de stappen van de wizard.

## 15.1.4. Scan uw systeem periodiek

De snelheid en het algemene gedrag van uw systeem kan ook worden beïnvloed door malware.

Zorg dat u uw systeem periodiek scant, maar minstens eenmaal per week.

Het is aanbevolen de Volledige systeemscan te gebruiken omdat hiermee wordt gescand op alle types malware die de beveiliging van uw systeem bedreigen en dit type scan ook binnen de archieven scant.

Volg deze stappen om de Volledige systeemscan te starten:

1. Het **Bitdefender-venster** openen.
2. Klik in het **Antivirus**-paneel op **Nu scannen** en selecteer **Systeemsan** in het uitklapbaar keuzemenu.
3. Volg de stappen van de wizard.

## 16. Online back-up Safebox

### 16.1. Hoe kan ik vanaf een andere computer toegang krijgen tot mijn back-upbestanden?

Met Bitdefender kunt u vanaf elke locatie toegang krijgen tot de bestanden waarvan u een back-up hebt gemaakt met Safebox, zelfs wanneer u niet thuis bent.

U hebt alleen een computer met internettoegang en een webbrowser nodig.

Om toegang te krijgen tot uw bestanden, moet u zich aanmelden bij MyBitdefender:

1. Open een webbrowser op een willekeurig apparaat met internettoegang.
2. Ga naar:<https://my.bitdefender.com>
3. Meld u aan bij uw account met uw gebruikersnaam en wachtwoord.
4. Klik op **Safebox** om toegang te krijgen tot het Safebox-dashboard.

### 16.2. Hoe kan ik bestanden delen met mijn vrienden?

Bitdefender Total Security 2013 is de oplossing waarmee u foto's, muziekbestanden, video's of documenten kunt delen met uw vrienden.

Om een bestand te delen met Bitdefender Total Security 2013, kiest u een van de volgende opties:

1. Het **Bitdefender-venster** openen.
2. Klik op het paneel **Safebox** op **Beheren** en selecteer **Beheer gedeelde bestanden** in het vervolgkeuzemenu.
3. Sleep het bestand en zet het neer in het venster **Delen beheren**.
4. Selecteer het bestand en klik op **Link delen**.
5. Klik op de opgegeven koppeling om deze te kopiëren naar het klembord.
6. Om toegang te krijgen tot het gedeelde bestand, stuurt u de koppeling naar de persoon met wie u het bestand wilt delen.

### 16.3. Waar kan ik de resterende ruimte op mijn Safebox zien?

Volg deze stappen om de resterende ruimte op uw Safebox te controleren:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Safebox**.
4. In het gedeelte **Gebruikte ruimte** ziet u de resterende ruimte.



Als u een grote hoeveelheid gegevens hebt met muziek, films of belangrijke bestanden, volstaat de gratis online ruimte mogelijk niet.

Klik op **Safebox upgraden** om uw online ruimte te upgraden.

De MyBitdefender-pagina wordt geopend in uw webbrowser. Volg de instructies om de aankoop te voltooien.

## 16.4. Hoe maak ik ruimte vrij op mijn Safebox?

Bitdefender biedt u 2GB vrije online ruimte voor uw gegevens.

Als u een grote hoeveelheid gegevens hebt met muziek, films of belangrijke bestanden, volstaat de gratis online ruimte mogelijk niet.

Volg deze stappen om ruimte vrij te maken op uw Safebox:

1. Open een webbrowser op een willekeurig apparaat met internettoegang.
2. Ga naar:<https://my.bitdefender.com>
3. Meld u aan bij uw account met uw gebruikersnaam en wachtwoord.
4. Klik op **Safebox** om toegang te krijgen tot het Safebox-dashboard.
5. Selecteer het tabblad **Prullenbak**.
6. Schakel het overeenkomende selectievakje in om het bestand dat u wilt verwijderen, te selecteren.
7. Klik op **Acties** en selecteer **Verwijderen** in het vervolgkeuzemenu.
8. Er wordt een bevestigingsvenster weergegeven. Klik op **OK** om te bevestigen.

## 17. Nuttige informatie

### 17.1. Hoe kan ik de computer automatisch afsluiten nadat het scannen is voltooid?

Bitdefender biedt meerdere scantaken die u kunt gebruiken om zeker te zijn dat uw systeem niet is geïnfecteerd door malware. Het scannen van de volledige computer kan langer duren, afhankelijk van de hardware- en softwareconfiguratie van uw systeem.

Omwille van deze reden biedt Bitdefender u de mogelijkheid Bitdefender te configureren om uw systeem af te sluiten zodra het scannen is voltooid.

Overweeg dit voorbeeld: u bent klaar met uw werk op de computer en wilt naar bed. U wilt dat Bitdefender uw volledige systeem controleert op malware.

In dat geval kunt u Bitdefender op de volgende manier instellen om het systeem uit te schakelen nadat de scan is voltooid.

1. Het **Bitdefender-venster** openen.
2. Klik in het **Antivirus**-paneel op **Nu scannen** en selecteer **Aangepaste scan** in het uitklapbaar keuzemenu.
3. Klik op **Doel toevoegen** om de te scannen bestanden of mappen te selecteren.
4. Klik op **Scanopties** als u de scanopties in detail wilt configureren.
5. Kies om de computer uit te schakelen wanneer de scan is voltooid en er geen bedreigingen zijn gevonden.
6. Klik op **Scannen starten**.

Als er geen bedreigingen zijn gevonden, wordt de computer uitgeschakeld.

Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen. Meer informatie vindt u onder "*Antivirusscanwizard*" (p. 82).

### 17.2. Bitdefender configureren voor het gebruik van een proxy-internetverbinding

Als uw computer een internetverbinding maakt via een proxyserver, moet u Bitdefender configureren met de proxy-instellingen. Bitdefender zal standaard de proxy-instellingen van uw systeem automatisch detecteren en importeren.



#### Belangrijk

Internetverbindingen bij u thuis gebruiken doorgaans geen proxyserver. Als vuistregel is het aanbevolen de proxyverbindinginstellingen van uw Bitdefender-programma te controleren en te configureren wanneer de updates niet werken. Als Bitdefender

een update kan uitvoeren, dan is de toepassing correct geconfigureerd voor het maken van een internetverbinding.

Volg de onderstaande stappen om de proxy-instellingen te beheren:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Algemeen**.
4. Selecteer in het venster met **Algemene instellingen** de tab **Geavanceerd**.
5. Schakel het proxygebruik in door op de schakelaar te klikken.
6. Klik op de koppeling **Proxy's beheren**.
7. Er zijn twee opties voor het instellen van de proxy-instellingen:
  - **Proxy-instellingen van de standaardbrowser importeren** - 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

Bitdefender kan proxy-instellingen van de populairste browsers importeren, inclusief de nieuwste versies van Internet Explorer, Mozilla Firefox en Opera.

- **Proxy-instellingen aanpassen** - proxy-instellingen die u zelf kunt configureren. 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** - typ een gebruikersnaam die door de proxy wordt herkend.
    - ▶ **Wachtwoord** - voer het geldige wachtwoord voor de eerder opgegeven gebruiker in.
8. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.
- Bitdefender gebruikt de beschikbare proxy-instellingen tot er een internetverbinding kan worden gemaakt.

## 17.3. Gebruik ik een 32- of 64-bits versie van Windows?

Volg de onderstaande stappen om uit te zoeken of u een 32-bits of 64-bits besturingssysteem hebt:

- Voor **Windows XP**:
  1. Klik op **Start**.

2. Zoek **Deze computer** in het menu **Start**.
3. Klik met de rechtermuisknop op **Deze computer** en selecteer **Eigenschappen**.
4. Als u **x64 Edition** vindt onder **Systeem**, betekent dit dat u werkt met de 64-bits versie van Windows XP.  
Als **x64 Edition** niet in de lijst staat, betekent dit dat u werkt met de 32-bits versie van Windows XP.

● Voor **Windows Vista** en **Windows 7**:

1. Klik op **Start**.
2. Zoek **Computer** in het menu **Start**.
3. Klik met de rechtermuisknop op **Deze computer** en selecteer **Eigenschappen**.
4. Kijk onder **Systeem** om de informatie over uw systeem te controleren.

## 17.4. Verborgene objecten weergeven in Windows

Deze stappen zijn nuttig in de gevallen waarin u te maken krijgt met een malware en u de geïnfecteerde bestanden die kunnen verborgen zijn, te vinden en te verwijderen.

Volg deze stappen om verborgen objecten weer te geven in Windows.

1. Klik op **Start**, ga naar **Configuratiescherm** en selecteer **Mapopties**.
2. Ga naar het tabblad **Weergave**.
3. Selecteer **Inhoud systeemmappen weergeven** (alleen voor Windows XP).
4. Selecteer **Verborgene bestanden en mappen weergeven**.
5. Schakel het selectievakje **Extensies voor bekende bestandstypen verbergen** uit.
6. Schakel het selectievakje **Beveiligde besturingssysteembestanden verbergen** in.
7. Klik op **Toepassen** en vervolgens op **OK**.

## 17.5. Andere beveiligingsoplossingen verwijderen

De hoofdreden voor het gebruik van een beveiligingsoplossing is het bieden van bescherming en veiligheid voor uw gegevens. Maar wat gebeurt er als er meerdere beveiligingsproducten aanwezig zijn op hetzelfde systeem?

Wanneer u meer dan één beveiligingsoplossing op dezelfde computer gebruikt, wordt het systeem onstabiel. Het installatieprogramma van Bitdefender Total Security 2013 detecteert automatisch andere beveiligingsprogramma's en biedt u de mogelijkheid om ze te verwijderen.

Volg de onderstaande stappen als u de andere beveiligingsoplossingen niet hebt verwijderd tijdens de eerste installatie:

● Voor **Windows XP**:

1. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Software**.
2. Wacht enkele ogenblikken tot de lijst met geïnstalleerde software wordt weergegeven.
3. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
4. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

● Voor **Windows Vista** en **Windows 7**:

1. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
2. Wacht enkele ogenblikken tot de lijst met geïnstalleerde software wordt weergegeven.
3. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
4. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.

Als u de andere beveiligingsoplossing niet van uw systeem kunt verwijderen, kunt u het hulpprogramma voor het verwijderen ophalen van de website van de verkoper of direct met hem contact opnemen voor richtlijnen betreffende het verwijderen.

## 17.6. Systeemherstel gebruiken in Windows

Als u de computer niet in de normale modus kunt starten, kunt u opstarten in Veilige modus en Systeemherstel gebruiken om te herstellen naar een tijdstip waarop de computer kon starten zonder fouten.

Om Systeemherstel uit te voeren, moet u als beheerder zijn aangemeld bij Windows.

Volg deze stappen om Systeemherstel te gebruiken:

● In Windows XP:

1. Bij Windows aanmelden in Veilige modus.
2. Volg het pad vanaf het menu van Windows: **Start** → **Alle programma's** → **Systeemwerkset** → **Systeemherstel**.
3. Klik op de pagina **Welkom bij Systeemherstel** om de optie **Mijn computer herstellen naar een eerder tijdstip** te selecteren en klik daarna op Volgende.

4. Volg de stappen van de wizard en u zou in staat moeten zijn het systeem op te starten in normale modus.
- In Windows Vista en Windows 7:
  1. Bij Windows aanmelden in Veilige modus.
  2. Volg het pad vanaf het menu Start van Windows: **Alle programma's** → **Bureau-accessoires** → **Systeemwerkset** → **Systeemherstel**.
  3. Volg de stappen van de wizard en u zou in staat moeten zijn het systeem op te starten in normale modus.

## 17.7. Opnieuw opstarten in Veilige modus

De Veilige modus is een diagnostische gebruiksmodus die hoofdzakelijk wordt gebruikt om problemen op te lossen die de normale werking van Windows beïnvloeden. Dergelijke problemen kunnen lopen van conflicterende stuurprogramma's tot virussen die verhinderen dat Windows normaal wordt gestart. In de Veilige modus werken slechts enkele toepassingen en laadt Windows alleen de basisbesturingsprogramma's en een minimum aan componenten van het besturingssysteem. Daarom zijn de meeste virussen inactief wanneer Windows in de Veilige modus wordt gebruikt en kunnen ze gemakkelijk worden verwijderd.

Windows in Veilige modus starten:

1. Start de computer opnieuw.
2. Druk meerdere keren op de **F8**-toets voordat Windows wordt gestart om toegang te krijgen tot het opstartmenu.
3. Selecteer **Veilige modus** in het opstartmenu of **Veilige modus met netwerkmogelijkheden** als u internettoegang wenst.
4. Druk op **Enter** en wacht terwijl Windows wordt geladen in Veilige modus.
5. Dit proces eindigt met een bevestigingsbericht. Klik op **OK** om te bevestigen.
6. Om Windows normaal te starten, hoeft u alleen het systeem opnieuw op te starten.

## Uw beveiliging beheren

## 18. Antivirusbeveiliging

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

- **Scannen bij toegang** - verhindert dat nieuwe malware-bedreigingen uw systeem binnenkomen. Bitdefender zal bijvoorbeeld een Worddocument scannen op bekende gevaren wanneer u het opent, en een e-mailbericht wanneer u het ontvangt.

Met Scannen bij toegang bent u zeker van bescherming in real time tegen malware, een essentieel onderdeel van elk computerbeveiligingsprogramma.



### Belangrijk

Houd **Scannen bij toegang** ingeschakeld om te verhinderen dat virussen uw computer infecteren.

- **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.

Wanneer **Autoscan** is ingeschakeld, is het zelden nodig malwarescans handmatig uit te voeren. Autoscan zal uw computer voortdurend opnieuw scannen en de geschikte acties ondernemen wanneer er malware is gedetecteerd. Autoscan werkt alleen wanneer er voldoende systeembronnen beschikbaar zijn, zodat de computer niet wordt vertraagd.

Bitdefender scant automatisch alle verwisselbare media die op de computer zijn aangesloten om zeker te zijn dat ze veilig kunnen worden geopend. Meer informatie vindt u onder "*Automatisch scannen van verwisselbare media*" (p. 86).

Geavanceerde gebruikers kunnen scanuitsluitingen configureren als ze niet willen dat er specifieke bestanden of bestandstypes worden gescand. Meer informatie vindt u onder "*Scanuitsluitingen configureren*" (p. 88).

Wanneer een virus of andere malware wordt gedetecteerd, zal Bitdefender automatisch proberen de malwarecode te verwijderen uit het geïnfecteerde bestand en het originele bestand reconstrueren. Deze bewerking wordt een desinfectie genoemd. Bestanden die niet kunnen worden gedesinfecteerd, worden naar quarantaine verplaatst om de infectie in te dammen. Meer informatie vindt u onder "*Bestanden in quarantaine beheren*" (p. 90).

Als uw computer werd geïnfecteerd door malware, moet u "*Malware van uw systeem verwijderen*" (p. 182) raadplegen. Om u te helpen bij het opruimen van de malware die niet kan worden verwijderd van het Windows-besturingssysteem op uw computer, biedt Bitdefender u de **Helpmodus**. Dit is een vertrouwde omgeving, vooral ontworpen voor het verwijderen van malware, waarmee u uw computer onafhankelijk van



Windows kunt opstarten. Wanneer de computer start in de Helpmodus, is de Windows-malware inactief zodat deze gemakkelijk kan worden verwijderd.

Om u te beschermen tegen onbekende boosaardige toepassingen, gebruikt Bitdefender Actief virusbeheer, een geavanceerde heuristische technologie die de toepassingen die op uw systeem worden uitgevoerd, doorlopend bewaakt. Actief virusbeheer blokkeert automatisch toepassingen die een malware-achtig gedrag vertonen om te voorkomen dat ze uw computer beschadigen. In sommige gevallen kunnen rechtmatige toepassingen worden geblokkeerd. In dergelijke situaties kunt u Actief virusbeheer configureren om die toepassingen niet opnieuw te blokkeren door uitsluitingsregels te maken. Raadpleeg "*Actief virusbeheer*" (p. 91) voor meer informatie.

Heel wat vormen van malware zijn ontwikkeld voor het infecteren van systemen door gebruik te maken van hun kwetsbaarheden, zoals ontbrekende updates van besturingssystemen of verouderde toepassingen. Bitdefender helpt u bij de systeemkwetsbaarheden gemakkelijk te identificeren en op te lossen om uw computer veiliger te stellen tegen malware en hackers. Meer informatie vindt u onder "*Systeemkwetsbaarheden oplossen*" (p. 94).

## 18.1. Scannen bij toegang (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.

De standaardinstellingen voor de real time-beveiliging, garanderen een goede beveiliging tegen malware, met een minimale impact op de systeemprestaties. U kunt de instellingen voor de real time-beveiliging gemakkelijk wijzigen volgens uw behoeften door naar een van de vooraf gedefinieerde beveiligingsniveaus te schakelen. Als u een geavanceerde gebruiker bent, kunt u de scaninstellingen in detail configureren door een aangepast beveiligingsniveau te maken.

### 18.1.1. De real time-beveiliging in- of uitschakelen

Volg deze stappen om real time malwarebeveiliging in of uit te schakelen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Antivirus**.
4. Selecteer in het venster met **Antivirusinstellingen** de tab **Beveiliging**.
5. Klik op de schakelaar om Scannen bij toegang in of uit te schakelen.
6. 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.

## 18.1.2. Het real time-beveiligingsniveau aanpassen

Het real time-beveiligingsniveau definieert de scaninstellingen voor real time-beveiliging. U kunt de instellingen voor de real time-beveiliging gemakkelijk wijzigen volgens uw behoeften door naar een van de vooraf gedefinieerde beveiligingsniveaus te schakelen.

Volg deze stappen om de standaard real time-beveiligingsinstellingen te herstellen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Antivirus**.
4. Selecteer in het venster met **Antivirusinstellingen** de tab **Beveiliging**.
5. Sleep de schuifregelaar langs de schaal om het gewenste beveiligingsniveau in te stellen. Gebruik de beschrijving aan de rechterzijde van de schaal om het beveiligingsniveau te kiezen dat beter beantwoordt aan uw beveiligingsbehoeften.

## 18.1.3. De instellingen voor de realtime beveiliging configureren

Gevorderde gebruikers willen wellicht voordeel halen uit de scaninstellingen die door Bitdefender worden aangeboden. U kunt de instellingen voor de real time-beveiliging in detail configureren door een aangepast beschermingsniveau te maken.

Volg deze stappen om de instellingen voor realtime beveiliging te configureren:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Antivirus**.
4. Selecteer in het venster met **Antivirusinstellingen** de tab **Beveiliging**.
5. Klik op **Aangepast**.
6. Configureer de scaninstellingen zoals dat nodig is.
7. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

## Informatie over de scanopties

Deze informatie kan nuttig zijn:

- Als u bepaalde termen niet kent, kunt u ze opzoeken in de [woordenlijst](#). U kunt ook nuttige informatie vinden door op het internet te zoeken.
- **Scanopties voor geopende bestanden.** U kunt Bitdefender instellen om alleen alle geopende bestanden of toepassingen (programmabestanden) te scannen. Het scannen van alle geopende bestanden biedt de beste beveiliging, terwijl het scannen van toepassingen alleen kan worden gebruikt voor betere systeemprestaties.

Standaard komen zowel lokale mappen als zaken die via het netwerk worden gedeeld in aanmerking voor scannen bij toegang. Voor betere systeemprestaties kunt u netwerklocaties uitsluiten van scannen bij toegang.

Toepassingen (of programmabestanden) zijn veel kwetsbaarder voor malwareaanvallen dan andere bestandstypen. Deze categorie bevat de volgende bestandsextensies:

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Binnen archieven scannen.** Het scannen binnenin de archieven verloopt langzaam en is een veeleisend proces, waardoor het niet aanbevolen is voor de real time-beveiliging. Archieven die geïnfecteerde bestanden bevatten, zijn geen onmiddellijke bedreiging voor de beveiliging van uw systeem. De malware kan uw systeem alleen beïnvloeden als het geïnfecteerde bestand wordt uitgepakt uit het archief en uitgevoerd zonder dat de real time-beveiliging is ingeschakeld.

Als u beslist deze optie te gebruiken, kunt u een maximaal geaccepteerde grootte instellen voor archieven die bij toegang moeten worden

gescand.Schakel het overeenkomende selectievakje in en typ de maximale archiefgrootte (in MB).

- **Scanopties voor verkeer via e-mail, web en expresberichten.** Om te verhinderen dat er malware wordt gedownload naar uw computer, scant Bitdefender automatische de volgende ingangspunten van malware:

- ▶ binnenkomende en uitgaande e-mails
- ▶ webverkeer
- ▶ bestanden ontvangen via Yahoo! Messenger

Het scannen van het webverkeer kan het surfen op het weg iets vertragen, maar het zal malware blokkeren die afkomstig is van internet, inclusief downloads tijdens het passeren.

Hoewel dit niet aanbevolen is, kunt u de antivirusscan van e-mails, internet of expresberichten uitschakelen om de systeemprestaties te verbeteren. Als u de overeenkomende scanopties uitschakelt, worden de e-mails en bestanden die zijn ontvangen of gedownload via internet niet gescand, waardoor geïnfecteerde bestanden op uw computer moeten worden opgeslagen. Dit is geen belangrijke bedreiging omdat de real time-beveiliging de malware zal blokkeren wanneer u probeert toegang te krijgen tot de geïnfecteerde bestanden (openen, verplaatsen, kopiëren of uitvoeren).

- **Opstartsectoren scannen.** U kunt Bitdefender instellen om de startgebieden van uw harde schijf te scannen. Dit deel van de harde schijf bevat de vereiste computercode om het opstartproces te starten. Als een virus het opstartgebied besmet, kan de toegang tot de schijf geblokkeerd worden en het is mogelijk dat u dan uw systeem niet meer kunt starten en geen toegang meer hebt tot uw gegevens.
- **Alleen nieuwe en gewijzigde bestanden scannen.** Door alleen nieuwe en gewijzigde bestanden te scannen, kunt u de algemene reactiviteit van uw systeem aanzienlijk verbeteren met een minimale inlevering op het vlak van beveiliging.
- **Scannen op keyloggers.** Selecteer deze optie om uw systeem te scannen op keyloggers. Keyloggers slaan op wat u op uw toetsenbord intypt en zenden via internet verslagen 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.

## Acties die worden ondernomen op gedetecteerde malware

U kunt de acties die door de realtime beveiliging worden genomen configureren.

Om deze acties te configureren, volgt u deze stappen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Antivirus**.

4. Selecteer in het venster met **Antivirusinstellingen** de tab **Beveiliging**.
5. Klik op **Aangepast**.
6. Configureer de scaninstellingen zoals dat nodig is.
7. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

De volgende acties kunnen worden ondernomen door de realtime beveiliging in Bitdefender:

## Neem gepaste acties

Bitdefender zal de aanbevolen acties ondernemen op basis van het type van het gedetecteerde bestand:

- **Geïnfecteerde bestanden.** Bestanden die als geïnfecteerd zijn gedetecteerd, komen overeen met een malwarehandtekening in de database van malwarehandtekeningen van Bitdefender. Bitdefender zal automatisch proberen de malwarecode van een geïnfecteerd bestand te verwijderen en het originele bestand te reconstrueren. Deze bewerking wordt een desinfectie genoemd.

Bestanden die niet kunnen worden gedesinfecteerd, worden naar quarantaine verplaatst om de infectie in te dammen. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer. Meer informatie vindt u onder "*Bestanden in quarantaine beheren*" (p. 90).



### Belangrijk

Voor specifieke types malware is desinfectie niet mogelijk omdat het gedetecteerde bestand volledig boosaardig is. In dergelijke gevallen wordt het geïnfecteerde bestand verwijderd van de schijf.

- **Verdachte bestanden.** De bestanden worden gedetecteerd als verdacht door de heuristische analyse. Verdachte bestanden kunnen niet worden gedesinfecteerd omdat er geen desinfectieroutine beschikbaar is. Ze worden verplaatst naar quarantaine om een mogelijke infectie te voorkomen.

Bestanden in quarantaine worden standaard automatisch verzonden naar Bitdefender Labs voor analyse door de malwareonderzoekers van Bitdefender. Als de aanwezigheid van malware is bevestigd, wordt een handtekening uitgegeven waarmee de malware kan worden verwijderd.

- **Archieven die geïnfecteerde bestanden bevatten.**

- ▶ Archieven die alleen geïnfecteerde bestanden bevatten, worden automatisch verwijderd.
- ▶ Als een archief zowel geïnfecteerde als schone bestanden bevat, zal Bitdefender proberen de geïnfecteerde bestanden te verwijderen op voorwaarde dat het programma het archief met de schone bestanden

opnieuw kan opbouwen. Als het niet mogelijk is het archief te reconstrueren, wordt u op de hoogte gebracht dat er geen actie kan worden ondernomen om zo te vermijden dat schone bestanden verloren gaan.

## Naar quarantaine

Verplaatst gedetecteerde bestanden naar de quarantaine. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer. Meer informatie vindt u onder "*Bestanden in quarantaine beheren*" (p. 90).

## Toegang weigeren

Wanneer een geïnfecteerd bestand is gedetecteerd, zal de toegang tot dit bestand worden geweigerd.

## 18.1.4. De standaardinstellingen herstellen

De standaardinstellingen voor de real time-beveiliging, garanderen een goede beveiliging tegen malware, met een minimale impact op de systeemprestaties.

Volg deze stappen om de standaard real time-beveiligingsinstellingen te herstellen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Klik in het menu aan de linkerkant op **Antivirus** en klik vervolgens op het tabblad **Shield**.
4. Klik op **Standaard**.

## 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 absoluut een goed idee om uw computer regelmatig te scannen op virussen.

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. Als u specifieke locaties wilt scannen op uw computer of de scanopties wilt configureren, kunt u een aangepaste scantaak configureren en uitvoeren.

## 18.2.1. Autoscan

Autoscan is een lichte scan op aanvraag die op de achtergrond al uw gegevens scant op malware en de geschikte acties onderneemt voor eventuele opgespoorde infecties. Autoscan zoekt en gebruikt tijdsegmenten wanneer het gebruik van de systeembronnen daalt onder een bepaalde drempel om terugkerende scans van het volledige systeem uit te voeren.

Voordelen van het gebruik van Autoscan:

- Dit heeft nagenoeg geen invloed op het systeem.
- Door de volledige harde schijf vooraf te scannen, worden toekomstige taken op aanvraag bijzonder snel.
- Scannen bij toegang zal eveneens veel minder tijd in beslag nemen.

Volg deze stappen om Autoscan in of uit te schakelen:

1. Het **Bitdefender-venster** openen.
2. Klik op het **Antivirus**-paneel op de schakelaar om **Autoscan** in of uit te schakelen.

## 18.2.2. Een bestand of map scannen op malware

U moet bestanden en mappen scannen wanneer u vermoedt dat ze geïnfecteerd zijn. Klik met de rechtermuisknop op het bestand of de map die u wilt scannen, kies **Bitdefender** en selecteer **Scannen met Bitdefender**. De **Antivirusscanwizard** wordt weergegeven en begeleidt u doorheen het scanproces. Aan het einde van de scan wordt u gevraagd te kiezen welke acties moeten worden ondernemen op de gedetecteerde bestanden, als die er zijn.

## 18.2.3. Een snelle scan uitvoeren

Quick Scan gebruikt in-the-cloud scanning om malware die op uw pc wordt uitgevoerd, te detecteren. Het uitvoeren van een Snelle scan duurt doorgaans minder dan één minuut en gebruikt slechts een fractie van de systeembronnen die nodig zijn door een regelmatig virusscan.

Volg deze stappen om een Snelle scan uit te voeren:

1. Het **Bitdefender-venster** openen.
2. Klik op het **Antivirus**-paneel op **Nu scannen** en selecteer **Snelle scan** in het uitklapbaar keuzemenu.
3. Volg de **Antivirusscanwizard** om de scan te voltooien. Bitdefender zal automatisch de aanbevolen acties ondernemen op de gedetecteerde bestanden. Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen.

## 18.2.4. Een systeemscan uitvoeren

De systeemscan scant de volledige computer op alle types malware die de beveiliging bedreigen, zoals virussen, spyware, adware, rootkits en andere. Als u **Autoscan** hebt uitgeschakeld, is het aanbevolen minstens een keer per week een systeemscan uit te voeren.



### Opmerking

Omdat **Systeemscan** een grondige scan van het complete systeem uitvoert, kan de scan even duren. Het is daarom aanbevolen deze taak uit te voeren wanneer u de computer niet gebruikt.

Voordat u een systeemscan uitvoert, wordt het volgende aanbevolen:

- Controleer of de malwarehandtekeningen van Bitdefender up-to-date zijn. Het scannen van uw computer met een oude handtekeningendatabase kan verhinderen dat Bitdefender nieuwe malware die sinds de laatste update is gevonden, detecteert. Meer informatie vindt u onder *“Bitdefender up-to-date houden”* (p. 39).
- Alle open programma's afsluiten

Als u specifieke locaties wilt scannen op uw computer of de scanopties wilt configureren, kunt u een aangepaste scantaak configureren en uitvoeren. Meer informatie vindt u onder *“Een aangepaste scan configureren”* (p. 79).

Volg deze stappen om een systeemscan uit te voeren:

1. Het **Bitdefender-venster** openen.
2. Klik in het **Antivirus**-paneel op **Nu scannen** en selecteer **Systeemscan** in het uitklapbaar keuzemenu.
3. Volg de **Antivirusscanwizard** om de scan te voltooien. Bitdefender zal automatisch de aanbevolen acties ondernemen op de gedetecteerde bestanden. Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen.

## 18.2.5. Een aangepaste scan configureren

Volg deze stappen om het scannen op malware gedetailleerd te configureren en uit te voeren:

1. Het **Bitdefender-venster** openen.
2. Klik in het **Antivirus**-paneel op **Nu scannen** en selecteer **Aangepaste scan** in het uitklapbaar keuzemenu.
3. Als u dat wenst, kunt u snel een eerdere aangepaste scan opnieuw uitvoeren door in de lijst **Recente scans** of **Favoriete scans** op het overeenkomende item te klikken.



4. Klik op **Doel toevoegen**, schakel de selectievakjes in die overeenkomen met de locatie die u wilt scannen op malware en klik vervolgens op **OK**.
5. Klik op **Scanopties** als u de scanopties wilt configureren. Een nieuw venster wordt weergegeven. Volg deze stappen:
  - a. U kunt de scanopties gemakkelijk configureren door het scanniveau aan te passen. Sleep de schuifregelaar langs de schaal om het gewenste scanniveau in te stellen. Gebruik de beschrijving aan de rechterzijde van de schaal om het scanniveau te identificeren dat beter beantwoordt aan uw behoeften.

Gevorderde gebruikers willen wellicht voordeel halen uit de scaninstellingen die door Bitdefender worden aangeboden. Klik op **Aangepast** om de scanopties in detail te configureren. Aan het einde van dit gedeelte vindt u informatie over deze opties.
  - b. U kunt ook deze algemene opties configureren:
    - **De taak uitvoeren met lage prioriteit** . Verlaagt de prioriteit van het geselecteerde scanproces. U zult andere programma's sneller kunnen uitvoeren en de tijd die nodig is om het scanproces te voltooien, verlengen.
    - **Scanwizard minimaliseren naar systeemvak** . Minimaliseert het scanvenster naar het **stysteemvak**. Dubbelklik op het pictogram Bitdefender om het programma te openen.
    - Geef de actie op die moet worden ondernomen als er geen bedreigingen zijn gevonden.
  - c. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.
6. Klik op **Scannen starten** en volg de **Antivirusscanwizard** om het scannen te voltooien. Afhankelijk van de locaties die moeten worden gescand, kan het scannen even duren. Aan het einde van de scan wordt u gevraagd te kiezen welke acties moeten worden ondernemen op de gedetecteerde bestanden, als die er zijn.


## Een aangepaste scan opslaan naar favorieten

Wanneer u een aangepaste scan configureert en uitvoert, wordt deze automatisch toegevoegd aan een beperkte lijst van recente scans. Als u een aangepaste scan in de toekomst opnieuw wilt gebruiken, kunt u deze opslaan in de lijst met favoriete scans.

Volg deze stappen om een recent uitgevoerde aangepaste scan op te slaan in de lijst met favoriete scans.

1. Open het venster voor het configureren van een aangepaste scan.
  - a. Het **Bitdefender-venster** openen.
  - b. Klik in het **Antivirus**-paneel op **Nu scannen** en selecteer **Aangepaste scan** in het uitklapbaar keuzemenu.

2. Zoek de gewenste scan in de lijst **Recente scans**.
3. Beweeg met de muiscursor over de naam van de scan en klik op het pictogram  om de scan toe te voegen aan de lijst met favoriete scans.

Scans die zijn opgeslagen in de favorieten, zijn gemarkeerd met het pictogram . Als u op dit pictogram klikt, wordt de scan verwijderd uit de lijst met favoriete scans.

## Informatie over de scanopties

Deze informatie kan nuttig zijn:

- Als u bepaalde termen niet kent, kunt u ze opzoeken in de [woordenlijst](#). U kunt ook nuttige informatie vinden door op het internet te zoeken.
- **Bestanden scannen.** U kunt Bitdefender instellen om alleen alle types bestanden of toepassingen (programmabestanden) te scannen. Het scannen van alle bestanden biedt de beste beveiliging, terwijl het scannen van toepassingen alleen kan worden gebruikt om een snellere scan uit te voeren.

Toepassingen (of programmabestanden) zijn veel kwetsbaarder voor malwareaanvallen dan andere bestandstypen. Deze categorie bevat de volgende bestandsextensies: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Scanopties voor archieven.** Archieven die geïnfecteerde bestanden bevatten, zijn geen onmiddellijke bedreiging voor de beveiliging van uw systeem. De malware kan uw systeem alleen beïnvloeden als het geïnfecteerde bestand wordt uitgepakt uit het archief en uitgevoerd zonder dat de real time-beveiliging is ingeschakeld. Het is echter aanbevolen deze optie te gebruiken om eventuele

potentiële bedreigingen te detecteren en te verwijderen, zelfs als het niet om een onmiddellijke bedreiging gaat.



## Opmerking

Het scannen van de gearchiveerde bestanden verlengt de algemene scanduur en vereist meer systeembronnen.


- **Opstartsectoren scannen.** U kunt Bitdefender instellen om de startgebieden van uw harde schijf te scannen. Dit deel van de harde schijf bevat de vereiste computercode om het opstartproces te starten. Als een virus het opstartgebied besmet, kan de toegang tot de schijf geblokkeerd worden en het is mogelijk dat u dan uw systeem niet meer kunt starten en geen toegang meer hebt tot uw gegevens.
- **Geheugen scannen.** Selecteer deze optie om programma's te scannen die worden uitgevoerd in uw systeemgeheugen.
- **Register scannen.** Selecteer deze optie voor het scannen van registersleutels. Het Windows-register is een database die de configuratie-instellingen en opties opslaat voor de componenten van het Windows-besturingssysteem, evenals voor geïnstalleerde toepassingen.
- **Cookies scannen.** Selecteer deze opties om de cookies te scannen die via browsers op uw computers zijn opgeslagen.
- **Alleen nieuwe en gewijzigde bestanden scannen.** Door alleen nieuwe en gewijzigde bestanden te scannen, kunt u de algemene reactiviteit van uw systeem aanzienlijk verbeteren met een minimale inlevering op het vlak van beveiliging.
- **Commerciële keyloggers negeren.** Selecteer deze opties als u commerciële keylogger-software op uw computer hebt geïnstalleerd en deze software gebruikt. Commerciële keyloggers zijn rechtmatige computerbewakingsprogramma's waarvan de basisfunctie eruit bestaat alles wat op het toetsenbord wordt getypt, te registreren.
- **Scannen op rootkits.** Selecteer deze optie om te scannen op **rootkits** en verborgen objecten die dergelijke software gebruiken.

## 18.2.6. Antivirusscanwizard

Telkens wanneer u een scan op aanvraag start (bijvoorbeeld klik met de rechtermuisknop op een map, kies Bitdefender en selecteer **Scannen met Bitdefender** ), verschijnt de Antivirusscanwizard van Bitdefender. Volg de wizard om het scannen 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 - Scan uitvoeren

Bitdefender start het scannen van de geselecteerde objecten. U ziet real time-informatie over de scanstatus en statistieken (inclusief de verstreken tijd, een schatting van de resterende tijd en het aantal gedetecteerde bedreigingen). Klik op de koppeling **Meer tonen** om meer details te zien.

Wacht tot Bitdefender het scannen beëindigt. Afhankelijk van de complexiteit van de scan, kan het scanproces enige tijd in beslag nemen.

**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**.

**Wachtwoordbeveiligde archieven.** Wanneer een met een wachtwoord beschermd archief wordt gedetecteerd, kunt u afhankelijk van de scaninstellingen worden gevraagd het wachtwoord op te geven. 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.

Kies de gewenste optie en klik op **OK** om door te gaan met scannen.

## Stap 2 - Acties kiezen

Aan het einde van de scan wordt u gevraagd te kiezen welke acties moeten worden ondernemen op de gedetecteerde bestanden, als die er zijn.



### Opmerking

Wanneer u een snelle scan of een volledige systeemscan uitvoert, neemt Bitdefender automatisch de aanbevolen acties op bestanden die zijn gedetecteerd tijdens de scan. Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen.

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.

## Neem gepaste acties

Bitdefender zal de aanbevolen acties ondernemen op basis van het type van het gedetecteerde bestand:

- **Geïnfecteerde bestanden.** Bestanden die als geïnfecteerd zijn gedetecteerd, komen overeen met een malwarehandtekening in de database van malwarehandtekeningen van Bitdefender. Bitdefender zal automatisch proberen de malwarecode van een geïnfecteerd bestand te verwijderen en het originele bestand te reconstrueren. Deze bewerking wordt een desinfectie genoemd.

Bestanden die niet kunnen worden gedesinfecteerd, worden naar quarantaine verplaatst om de infectie in te dammen. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer. Meer informatie vindt u onder "*Bestanden in quarantaine beheren*" (p. 90).



### Belangrijk

Voor specifieke types malware is desinfectie niet mogelijk omdat het gedetecteerde bestand volledig boosaardig is. In dergelijke gevallen wordt het geïnfecteerde bestand verwijderd van de schijf.

- **Verdachte bestanden.** De bestanden worden gedetecteerd als verdacht door de heuristische analyse. Verdachte bestanden kunnen niet worden gedesinfecteerd omdat er geen desinfectieroutine beschikbaar is. Ze worden verplaatst naar quarantaine om een mogelijke infectie te voorkomen.

Bestanden in quarantaine worden standaard automatisch verzonden naar Bitdefender Labs voor analyse door de malwareonderzoekers van Bitdefender. Als de aanwezigheid van malware is bevestigd, wordt een handtekening uitgegeven waarmee de malware kan worden verwijderd.

- **Archieven die geïnfecteerde bestanden bevatten.**

- ▶ Archieven die alleen geïnfecteerde bestanden bevatten, worden automatisch verwijderd.
- ▶ Als een archief zowel geïnfecteerde als schone bestanden bevat, zal Bitdefender proberen de geïnfecteerde bestanden te verwijderen op voorwaarde dat het programma het archief met de schone bestanden opnieuw kan opbouwen. Als het niet mogelijk is het archief te reconstrueren,

wordt u op de hoogte gebracht dat er geen actie kan worden ondernomen om zo te vermijden dat schone bestanden verloren gaan.

## Wissen

Verwijdert gedetecteerde bestanden van de schijf.

Als er geïnfecteerde bestanden samen met schone bestanden in een archief zijn opgeslagen, zal Bitdefender proberen de geïnfecteerde bestanden te verwijderen en het archief opnieuw op te bouwen met de schone bestanden. Als het niet mogelijk is het archief te reconstrueren, wordt u op de hoogte gebracht dat er geen actie kan worden ondernomen om zo te vermijden dat schone bestanden verloren gaan.

## 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.

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

## Stap 3 - Overzicht

Wanneer Bitdefender het oplossen van de problemen heeft voltooid, verschijnen de scanresultaten in een nieuw venster. Als u uitgebreide informatie over het scanproces wenst, klikt u op **Logboek weergeven** om het scanlogboek weer te geven.

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



### Belangrijk

In de meeste gevallen desinfecteert Bitdefender met succes de geïnfecteerde bestanden die het detecteert of isoleert het de infectie. Er zijn echter problemen die niet automatisch kunnen worden opgelost. Start indien nodig uw systeem opnieuw, zodat het installatieprogramma de installatie kan voltooien. Meer informatie en instructies over het handmatig verwijderen van malware, vindt u onder "*Malware van uw systeem verwijderen*" (p. 182).

## 18.2.7. Scanlogboeken controleren

Telkens wanneer er een scan wordt uitgevoerd, wordt er een scanverslag aangemaakt en Bitdefender slaat de gedetecteerde problemen op in het venster 'Antivirusoverzicht'. Het scanlog bevat gedetailleerde informatie over het gevolgde scanproces, zoals de scanopties, het scandoel, de gevonden bedreigingen en de hierop uitgevoerde acties.

Zodra het scannen is voltooid, kunt u het scanlogboek direct vanaf de scanwizard openen door op **Logboek weergeven** te klikken.

Om een scanverslag of een willekeurige gedetecteerde infectie op een later tijdstip te controleren, volgt u deze stappen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Gebeurtenissen** in de werkbalk bovenaan.
3. Selecteer in het venster **GebeurtenissenoverzichtAntivirus**.
4. Selecteer in het venster met **Antivirusgebeurtenissen** de tab **Virusscan**. Hier vindt u alle gebeurtenissen van scans op malware, inclusief bedreigingen die zijn gedetecteerd door Scannen bij toegang, door gebruiker gestarte scans en statuswijzigingen voor automatische scans.
5. In de gebeurtenissenlijst kunt u controleren welke scans onlangs werden uitgevoerd. Klik op een gebeurtenis om details erover weer te geven.
6. Klik op **Logboek weergeven** om het scanlogboek te openen. Het scanlog wordt geopend in uw standaard webbrowser.

## 18.3. Automatisch scannen van verwisselbare media


Bitdefender detecteert automatisch wanneer u een verwisselbaar opslagapparaat aansluit op uw computer en scant dit op de achtergrond. 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

U kunt het automatisch scannen afzonderlijk configureren voor elke categorie opslagapparaten. Automatisch scannen van toegewezen netwerkstations is standaard uitgeschakeld.

### 18.3.1. Hoe werkt het?

Wanneer Bitdefender een verwisselbaar opslagapparaat detecteert, start het programma met scannen op malware op de achtergrond (op voorwaarde dat de automatische scan is ingeschakeld voor dat type apparaat). Een Bitdefender-scanpictogram  verschijnt in het **systeemvak**. U kunt op dit pictogram klikken om het scanvenster te openen en de scanvoortgang te bekijken.

Als Auto Pilot is ingeschakeld, wordt u niet gehinderd door herinnering aan de scan. De scan wordt alleen geregistreerd en de informatie over de scan zal beschikbaar zijn in het venster **Gebeurtenissen**.

Als Auto Pilot is uitgeschakeld:

1. U wordt via een pop-upvenster gemeld dat een nieuw apparaat is gedetecteerd en dat het wordt gescand.

2. In de meeste gevallen verwijdert Bitdefender automatisch de gedetecteerde malware of isoleert het programma geïnfekteerde bestanden in quarantaine. Als er na de scan niet opgeloste bedreigingen zijn, wordt u gevraagd de acties te kiezen die moeten worden ondernomen.



## Opmerking

Houd ermee rekening dat er geen actie kan worden ondernomen op geïnfekteerde of verdachte bestanden die op cd's/dvd's zijn gevonden. Zo kan er ook geen actie worden ondernomen op geïnfekteerde of verdachte bestanden die zijn gedetecteerd op toegewezen netwerkstations als u niet over de geschikte privileges beschikt.

3. Nadat de scan is voltooid, wordt het venster met de scanresultaten weergegeven om u te laten weten of u de bestanden op de verwisselbare media veilig kunt openen.

Deze informatie kan nuttig zijn voor u:

- Wees voorzichtig wanneer u een door malware geïnfekteerde cd/dvd gebruikt. De malware kan niet van de schijf worden verwijderd (het medium is alleen-lezen). Zorg dat de real time-beveiliging is ingeschakeld om te verhinderen dat malware zich over uw systeem verspreidt. De beste werkwijze is het kopiëren van alle waardevolle gegevens van de schijf naar uw systeem en ze daarna verwijderen van de schijf.
- In sommige gevallen zal Bitdefender niet in staat zijn malware te verwijderen uit specifieke bestanden vanwege wettelijke of technische beperkingen. Een voorbeeld hiervan zijn bestanden die gearchiveerd zijn met een eigen technologie (dit is te wijten aan het feit dat het archief niet correct opnieuw kan worden gemaakt).

Raadpleeg "*Malware van uw systeem verwijderen*" (p. 182) voor meer informatie over het omgaan met malware.

## 18.3.2. Scan verwisselbare media beheren

Volg deze stappen om het automatisch scannen van verwisselbare media te beheren:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Antivirus**.
4. Selecteer in het venster met **Antivirusinstellingen** de tab **Uitsluitingen**.

Voor de beste beveiliging is het aanbevolen het automatisch scannen in te schakelen voor alle types verwisselbare opslagapparaten.

De scanopties zijn vooraf geconfigureerd voor de beste detectieresultaten. Als er geïnfekteerde bestanden wordt gedetecteerd, probeert Bitdefender ze te desinfecteren (de malwarecode verwijderen) of ze naar quarantaine te verplaatsen. Als beide acties mislukken, kunt u met de Antivirusscanwizzard andere acties opgeven



die moeten worden ondernemen op geïnfekteerde bestanden. De scanopties zijn standaard en u kunt ze niet wijzigen.

## 18.4. Scanuitsluitingen configureren

Met Bitdefender kunt u specifieke bestanden, mappen of bestandsextensies uitsluiten van het scannen. Deze functie is bedoeld om te vermijden dat u in uw werk wordt gestoord en kan ook helpen de systeemprestaties te verbeteren. Uitsluitingen zijn voorzien voor gebruikers die over een gevorderde computerkennis beschikken. Als u deze kennis niet hebt, kunt u de aanbevelingen van een expert van Bitdefender volgen.

U kunt uitsluitingen configureren die u wilt toepassen op Scannen bij toegang of Scannen op aanvraag afzonderlijk, of op beide scantypes tegelijk. De objecten die zijn uitgesloten van scannen bij toegang, worden niet gescand, ongeacht of ze door u of door een toepassing worden geopend.



### Opmerking

Uitsluitingen komen NIET in aanmerking 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**.

### 18.4.1. Bestanden of mappen uitsluiten van het scannen

Volg deze stappen om specifieke bestanden of mappen uit te sluiten van het scannen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Antivirus**.
4. Selecteer in het venster met **Antivirusinstellingen** de tab **Uitsluitingen**.
5. Schakel scanuitsluitingen voor bestanden in met de overeenkomende schakelaar.
6. Klik op de koppeling **Uitgesloten bestanden en mappen**. In het venster dat verschijnt, kunt u de bestanden en mappen die van het scannen zijn uitgesloten, beheren.
7. Volg deze stappen om uitsluitingen toe te voegen:
  - a. Klik bovenaan in de tabel met uitsluitingen op de knop **Toevoegen**.
  - b. Klik op **Bladeren**, selecteer het bestand of de map die u wilt uitsluiten van de scan en klik vervolgens op **OK**. Daarnaast kunt u ook het pad naar het bestand of de map in het bewerkingsveld typen (of kopiëren en plakken).

c. Het geselecteerde bestand of de geselecteerde map wordt standaard uitgesloten van Scannen bij toegang en Scannen bij aanvraag. Selecteer een van de andere opties om het toepassen van de uitsluiting te wijzigen.

d. Klik op **Toevoegen**.

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

## 18.4.2. Bestandsextensies uitsluiten van het scannen

Wanneer u een bestandsextensie uitsluit van de scan, zal Bitdefender niet langer bestanden met die extensie scannen, ongeacht hun locatie op uw computer. De uitsluiting is ook van toepassing op bestanden op verwisselbare media, zoals cd's, dvd's, USB-opslagapparaten of netwerkstations.



### Belangrijk

Ga voorzichtig te werk wanneer u extensies uitsluit van het scannen, want dergelijke uitsluitingen kunnen uw computer kwetsbaar maken voor malware.

Volg deze stappen om bestandsextensies uit te sluiten van het scannen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Antivirus**.
4. Selecteer in het venster met **Antivirusinstellingen** de tab **Uitsluitingen**.
5. Schakel scanuitsluitingen voor bestanden in met de overeenkomende schakelaar.
6. Klik op de koppeling **Uitgesloten extensies**. In het venster dat verschijnt, kunt u de bestandsextensies die van het scannen zijn uitgesloten, beheren.
7. Volg deze stappen om uitsluitingen toe te voegen:
  - a. Klik bovenaan in de tabel met uitsluitingen op de knop **Toevoegen**.
  - b. Voer de extensies in die u wilt uitsluiten van het scannen en scheid ze van elkaar met puntkomma's (;). Hier is een voorbeeld:  
`txt;avi;jpg`
  - c. Alle bestanden met de opgegeven extensies worden standaard uitgesloten van Scannen bij toegang en Scannen op aanvraag. Selecteer een van de andere opties om het toepassen van de uitsluiting te wijzigen.
  - d. Klik op **Toevoegen**.
8. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

## 18.4.3. Scanuitsluitingen beheren

Als de geconfigureerde scanuitsluitingen niet langer nodig zijn, is het aanbevolen dat u ze verwijdert of dat u scanuitsluitingen uitschakelt.

Volg deze stappen om de scanuitsluitingen te beheren:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Antivirus**.
4. Selecteer in het venster met **Antivirusinstellingen** de tab **Uitsluitingen**. Gebruik de opties in het gedeelte **Bestanden en mappen** om scanuitsluitingen te beheren.
5. Klik op een van de beschikbare koppelingen om scanuitsluitingen te verwijderen of te bewerken. Ga als volgt te werk:
  - 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, dubbelklikt u op dit item (of selecteert u het en klikt u op de knop **Bewerken**). Er verschijnt een nieuw venster. Hierin kunt u de extensie van het pad dat moet worden uitgesloten en het type scan waarvoor u het wilt uitsluiten wijzigen volgens uw voorkeur. Breng de nodige wijzigingen aan en klik daarna op **Wijzigen**.
6. Gebruik de overeenkomende schakelaar voor het uitschakelen van scanuitsluitingen.

## 18.5. Bestanden in quarantaine beheren

Bitdefender isoleert de door malware geïnfecteerde bestanden die het niet kan desinfecteren en de verdachte bestanden in een beveiligd gebied dat de quarantaine wordt genoemd. Wanneer het virus in quarantaine is, kan het geen schade berokkenen, aangezien het niet kan worden uitgevoerd of gelezen.

Bestanden in quarantaine worden standaard automatisch verzonden naar Bitdefender Labs voor analyse door de malwareonderzoekers van Bitdefender. Als de aanwezigheid van malware is bevestigd, wordt een handtekening uitgegeven waarmee de malware kan worden verwijderd.

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

Volg deze stappen om de bestanden in quarantaine te controleren en te beheren:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.

3. Selecteer in het venster met het **Instellingenoverzicht Antivirus**.
4. Selecteer in het venster met **Antivirusinstellingen** de tab **Quarantaine**.
5. Bestanden in quarantaine worden automatisch beheerd door Bitdefender op basis van de standaard quarantaine-instellingen. Hoewel dit niet aanbevolen is, kunt u de quarantaine-instellingen aanpassen volgens uw voorkeur.

### **Quarantaine opnieuw scannen na updaten van virusdefinities**

Houd deze optie ingeschakeld om bestanden in quarantaine automatisch te scannen na elke update van de virusdefinities. Opgeruimde bestanden worden automatisch terug naar hun originele locatie verplaatst.

### **Voeg verdachte bestanden die in quarantaine staan toe voor verdere analyses**

Houd deze optie ingeschakeld om bestanden in quarantaine automatisch naar Bitdefender te verzenden. De voorbeeldbestanden worden geanalyseerd door de malwareonderzoekers van Bitdefender. Als de aanwezigheid van malware is bevestigd, wordt een handtekening uitgegeven waarmee de malware kan worden verwijderd.

### **Inhoud ouder dan {30} dagen verwijderen**

Standaard worden bestanden in quarantaine die ouder zijn dan 30 dagen, automatisch verwijderd. Als u dit interval wilt wijzigen, geeft u een nieuwe waarde op in het overeenkomende veld. Typ 0 om het automatisch verwijderen van oude bestanden in quarantaine uit te schakelen.

6. Om een bestand in quarantaine te verwijderen, selecteert u het en klikt u op de knop **Verwijderen**. Als u een bestand uit quarantaine wilt terugzetten op zijn oorspronkelijke locatie, selecteert u het en klikt u op **Herstellen**.

## 18.6. Actief virusbeheer

Bitdefender Actief virusbeheer is een innovatieve proactieve detectietechnologie die geavanceerde heuristische methoden gebruikt voor het in real time detecteren van nieuwe potentiële bedreigingen.

Actief virusbeheer bewaakt voortdurend de toepassingen die op de computer worden uitgevoerd en zoekt naar acties die op malware lijken. Elk van deze acties krijgt een score en voor elk proces wordt een algemene score berekend. Wanneer de algemene score voor een proces een bepaalde drempel bereikt, wordt het proces beschouwd als schadelijk en wordt het automatisch geblokkeerd.

Als Auto Pilot uit is, wordt u op de hoogte gebracht via een pop-upvenster over de geblokkeerde toepassing. Anders wordt de toepassing geblokkeerd zonder enige melding. U kunt controleren welke toepassingen zijn gedetecteerd door Actief virusbeheer in het venster **Gebeurtenissen**.

## 18.6.1. Gedetecteerde toepassingen controleren

Volg deze stappen om de toepassingen die zijn gedetecteerd door Actief virusbeheer, te controleren:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Gebeurtenissen** in de werkbalk bovenaan.
3. Selecteer in het venster **Gebeurtenissenoverzicht Antivirus**.
4. Selecteer in het venster met **Antivirusgebeurtenissen** de tab **Actief Virusbeheer**.
5. Klik op een gebeurtenis om details erover weer te geven.
6. Als u de toepassing vertrouwt, kunt u Actief virusbeheer configureren om deze niet meer te blokkeren door op **Toestaan en bewaken** te klikken. Actief virusbeheer blijft de uitgesloten toepassingen bewaken. Als voor een uitgesloten toepassing wordt gedetecteerd dat deze verdachte activiteiten uitvoert, wordt de gebeurtenis eenvoudigweg gemeld en gerapporteerd aan Bitdefender Cloud als detectiefout.

## 18.6.2. Actief virusbeheer in- of uitschakelen

Volg deze stappen om Actief virusbeheer in of uit te schakelen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Antivirus**.
4. Selecteer in het venster met **Antivirusinstellingen** de tab **Beveiliging**.
5. Klik op de schakelaars om deze optie in of uit te schakelen.

## 18.6.3. De bescherming van Antivirusbeheer aanpassen

Als u merkt dat Actief virusbeheer vaak rechtmatige toepassingen detecteert, moet u een toegeeflijker beveiligingsniveau instellen.

Volg deze stappen om de bescherming door Actief virusbeheer aan te passen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Antivirus**.
4. Selecteer in het venster met **Antivirusinstellingen** de tab **Beveiliging**.
5. Controleer of Actief virusbeheer is ingeschakeld.

6. Sleep de schuifregelaar langs de schaal om het gewenste beveiligingsniveau in te stellen. Gebruik de beschrijving aan de rechterzijde van de schaal om het beveiligingsniveau te kiezen dat beter beantwoordt aan uw beveiligingsbehoeften.



## Opmerking

Wanneer u het beveiligingsniveau hoger instelt, zal Actief virusbeheer minder tekenen van malware-achtig gedrag nodig hebben om een proces te rapporteren. Dit zal leiden tot een hoger aantal gerapporteerde toepassingen en tegelijkertijd tot een grotere waarschijnlijkheid van fout-positieven (veilige toepassingen die worden gedetecteerd als kwaadaardig).

## 18.6.4. Uitgesloten processen beheren

U kunt de uitsluitingsregels configureren voor vertrouwde toepassingen zodat Actief virusbeheer ze niet blokkeert als ze acties uitvoeren die op malware lijken. Actief virusbeheer blijft de uitgesloten toepassingen bewaken. Als voor een uitgesloten toepassing wordt gedetecteerd dat deze verdachte activiteiten uitvoert, wordt de gebeurtenis eenvoudigweg gemeld en gerapporteerd aan Bitdefender Cloud als detectiefout.

Volg deze stappen om de uitsluitingen voor het proces van Actief virusbeheer te beheren:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Antivirus**.
4. Selecteer in het venster met **Antivirusinstellingen** de tab **Uitsluitingen**.
5. Klik op de koppeling **Uitgesloten processen**. In het venster dat verschijnt, kunt u de uitsluitingen voor het proces Actief virusbeheer beheren.



## Opmerking

Procesuitsluitingen zijn ook van toepassing op het **inbraakdetectiesysteem** dat in de Bitdefender-firewall is inbegrepen.

6. Volg deze stappen om uitsluitingen toe te voegen:
  - a. Klik bovenaan in de tabel met uitsluitingen op de knop **Toevoegen**.
  - b. Klik op **Bladeren**, zoek en selecteer de toepassing die u wilt uitsluiten en klik vervolgens op **OK**.
  - c. Houd de optie **Toestaan** geselecteerd om te verhinderen dat Actief virusbeheer de toepassing blokkeert.
  - d. Klik op **Toevoegen**.
7. Ga als volgt te werk om uitsluitingen te verwijderen of te bewerken:

- 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, dubbelklikt u op dit item (of selecteert het) en klikt op de knop **Wijzigen**. Breng de nodige wijzigingen aan en klik daarna op **Wijzigen**.

8. De wijzigingen opslaan en het venster sluiten.

## 18.7. Systeemkwetsbaarheden oplossen

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. Wij raden u ook aan te overwegen om de Windows-instellingen die het systeem kwetsbaarder maken voor malware, uit te schakelen. 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 biedt twee eenvoudige manieren om de kwetsbaarheden van uw systeem op te lossen:

- U kunt uw systeem scannen op kwetsbaarheden en ze stapsgewijs repareren met de wizard **Kwetsbaarheidsscan**.
- Met de automatische kwetsbaarheidsbewaking kunt u de gedetecteerde kwetsbaarheden controleren en oplossen in het venster **Gebeurtenissen**.

Het is aanbevolen de systeemkwetsbaarheden om de week of twee weken te controleren en op te lossen.

### 18.7.1. Uw systeem scannen op kwetsbaarheden

Volg deze stappen om systeemkwetsbaarheden op te lossen met de wizard Kwetsbaarheidsscan:

1. Het **Bitdefender-venster** openen.
2. Klik op het **Antivirus**-paneel op **Nu scannen** en selecteer **Kwetsbaarheidsscan** in het uitklapbaar keuzemenu.
3. Volg de begeleide procedure van zes stappen om kwetsbaarheden van uw systeem te verwijderen. Gebruik de knop **Volgende** om te navigeren door de wizard. Klik op **Annuleren** om de wizard af te sluiten.
  - a. **Uw pc beveiligen**  
Selecteer de kwetsbaarheden die u wilt controleren.
  - b. **Controleren op problemen**

Wacht tot Bitdefender om de controle van uw systeem op kwetsbaarheden, te voltooien.

## c. **Windows updates**

U ziet de lijst van kritieke en niet-kritieke Windows updates die niet zijn geïnstalleerd op uw computer. Selecteer de updates die u wilt installeren.

Klik op **Volgende** om de installatie van de geselecteerde updates te starten. De installatie van de updates kan even duren en voor sommige updates zal het nodig zijn het systeem opnieuw op te starten om de installatie te voltooien. Start, indien nodig, het systeem zo snel mogelijk opnieuw op.

## d. **Toepassingsupdates**

Als een applicatie niet up-to-date is, klik dan op de getoonde link om de laatste versie te downloaden.

## e. **Zwakke wachtwoorden**

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

Klik op **Herstellen** om de zwakke wachtwoorden te wijzigen. U kunt kiezen om de gebruiker te vragen het wachtwoord te wijzigen bij de volgende aanmelding of u kunt het wachtwoord zelf onmiddellijk wijzigen. Voor een sterk wachtwoord gebruikt u een combinatie van hoofdletters en kleine letters, getallen en speciale tekens (zoals #, \$ of @).

## f. **Summary**

Hier kunt u het resultaat van de bewerking bekijken.

## 18.7.2. De automatische kwetsbaarheidsbewaking gebruiken

Bitdefender scant uw systeem regelmatig op de achtergrond op kwetsbaarheden en houdt gegevens bij van de gevonden problemen in het venster **Gebeurtenissen**.

Volg deze stappen om de gedetecteerde problemen te controleren en op te lossen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Gebeurtenissen** in de werkbalk bovenaan.
3. Selecteer in het venster **Gebeurtenissenoverzicht** **Antivirus**.
4. Selecteer in het venster met **Antivirusgebeurtenissen** de tab **Kwetsbaarheid**.
5. U kunt gedetailleerde informatie betreffende de gedetecteerde kwetsbaarheden van het systeem zien. 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 **Nu bijwerken** om de wizard Kwetsbaarheidsscan te openen en de updates te installeren.



- Als een toepassing verouderd is, klikt u op **Nu bijwerken** om een koppeling te zoeken naar de webpagina van de verkoper vanaf waar u de nieuwste versie van die toepassing kunt installeren.
- Als een Windows-gebruikersaccount een zwak wachtwoord heeft, klikt u op **Wachtwoord 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 @).
- Als de Windows-functie Autorun is ingeschakeld, klikt u op **Uitschakelen** om de functie uit te schakelen.

Volg deze stappen om de instellingen voor de kwetsbaarheidsbewaking te configureren:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Antivirus**.
4. Selecteer in het venster met **Antivirusgebeurtenissen** de tab **Kwetsbaarheid**.
5. Klik op de schakelaar om Automatische kwetsbaarheidsscan in of uit te schakelen.



### Belangrijk

Om automatisch op de hoogte te worden gebracht over kwetsbaarheden van het systeem of de toepassing, moet u **Automatische kwetsbaarheidsscan** ingeschakeld houden.

6. Kies de systeemkwetsbaarheden die u regelmatig wilt controleren met de overeenkomende schakelaars.

### Kritieke Windows updates

Controleer of uw Windows-besturingssysteem over de laatste kritieke beveiligingsupdates van Microsoft beschikt.

### Normale Microsoft updates

Controleer of uw Windows-besturingssysteem over de laatste gewone beveiligingsupdates van Microsoft beschikt.

### Toepassingsupdates

Controleer of cruciale webverwante toepassingen die op uw systeem zijn geïnstalleerd, up-tot-date zijn. Verouderde toepassingen kunnen door kwaadaardige software worden misbruikt, waardoor uw pc kwetsbaar wordt voor aanvallen van buitenaf.

### Zwakke wachtwoorden

Controleer of de wachtwoorden van de Windows-accounts die op het systeem zijn geconfigureerd, gemakkelijk te raden zijn. Het instellen van moeilijk te

raden wachtwoorden (sterke wachtwoorden) maakt het bijzonder moeilijk voor hackers om in uw systeem in te breken. Een sterk wachtwoord bevat hoofdletters en kleine letters, cijfers en speciale tekens (zoals #, \$ of @).

## **Autorun media**

Controleer de status van de Windows-functie Autorun. Met deze functie kunnen toepassingen automatisch worden gestart vanaf cd's, dvd's, USB-stations of andere externe apparaten.

Sommige malwaretypes gebruiken Autorun om zich automatisch te verspreiden van de verwisselbare media naar de pc. Daarom is het aanbevolen deze Windows-functie uit te schakelen.



## **Opmerking**

Als u de bewaking van een specifieke kwetsbaarheid uitschakelt, worden verwante problemen niet langer opgenomen in het venster Gebeurtenissen.

## 19. Antispam

Spam is een term die wordt gebruikt voor het beschrijven van ongewenste e-mail. Spam is een groeiend probleem voor zowel individuele gebruikers als bedrijven. 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 op zakelijke e-mailadres) 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.

Bitdefender Antispam gebruikt opmerkelijke technologische innovaties en industriestandaard antispamfilters om spam op te sporen voordat deze het Postvak IN van de gebruiker bereikt. Meer informatie vindt u onder "*Antispam-begrippen*" (p. 99).

De antispambeveiliging van Bitdefender is alleen beschikbaar voor e-mailclients die geconfigureerd zijn om e-mailberichten te ontvangen via het POP3-protocol. POP3 is een van de op grootste schaal gebruikte protocollen voor het downloaden van e-mailberichten van een e-mailserver.



### Opmerking

Bitdefender biedt geen antispambeveiliging voor e-mailaccounts die u aanspreekt via een e-mailservice op internet.

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.

## 19.1. Antispam-begrippen

### 19.1.1. Antispam-filters

De Bitdefender Antispam-engine bevat meerdere filters die garanderen dat uw Postvak IN vrij blijft van SPAM: **Vriendenlijst**, **Spammerslijst**, **Tekensetfilter**, **Verbindingsfilter**, **Handtekeningenfilter**, **NeuNet-filter** (heuristisch) en **in-the-cloud-detectie**.

#### Vriendenlijst / Spammerslijst

De meeste mensen communiceren regelmatig met een groep mensen of ontvangen zelfs berichten van bedrijven of organisaties op hetzelfde domein. Wanneer u gebruik maakt van **vrienden- of spammerslijsten**, kunt 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).



#### 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

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

#### Link filter

Bijna alle spamberichten bevatten links 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 Linkfilter kijkt elke URL-link in een bericht na in zijn database. Als een treffer is gevonden, wordt het bericht gelabeld als SPAM.

#### Handtekeningenfilter

De spamonderzoekers van Bitdefender analyseren voortdurend de spam-e-mails in het wild en geven spamhandtekeningen vrij waarmee deze e-mails kunnen worden gedetecteerd.

De Handtekeningenfilter controleert e-mails ten opzichte van de spamhandtekeningen in de lokale database. Als een treffer is gevonden, wordt het bericht gelabeld als SPAM.



## Opmerking

In tegenstelling tot de andere filters, kan de Handtekeningenfilter niet onafhankelijk van de antispambescherming worden uitgeschakeld.

## 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, zal de e-mail een spamscore ontvangen.

Als de spamscore het drempelniveau overschrijdt, wordt de e-mail beschouwd als SPAM. Het drempelniveau wordt bepaald door het antispamgevoeligheidsniveau. Meer informatie vindt u onder *"Het gevoeligheidsniveau aanpassen"* (p. 106).

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.

## In-the-cloud detectie

"In-the cloud"-detectie maakt gebruik van de Bitdefender Cloud-services om u efficiënte antispambeveiliging te bieden die altijd up-to-date is.

E-mails worden alleen "in the cloud" gecontroleerd als de lokale antispamfilters geen afdoend resultaat bieden.

## 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.

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

In het andere geval zal de filter **Spammerslijst** de e-mail overnemen om het adres van de afzender te controleren in zijn lijst. Als er een treffer wordt gevonden, wordt de e-mail gelabeld als SPAM en naar de map **Spam** verplaatst.

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**.

De **Linkfilter** zal de links die in de e-mail zijn gevonden, vergelijken met de links van de Bitdefender-database van bekende spamlinks. In geval van overeenkomst, wordt de e-mail als SPAM beschouwd.

Vervolgens controleert de **Handtekeningenfilter** de e-mail ten opzichte van de spamhandtekeningen in de lokale database. Als een treffer is gevonden, wordt het bericht gelabeld als SPAM.

De **NeuNet-filter (heuristisch)** 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. Op basis van de resultaten van de analyse, zal de e-mail een spamscore ontvangen.



## Opmerking

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

Als de spamscore het drempelniveau overschrijdt, wordt de e-mail beschouwd als SPAM. Het drempelniveau wordt bepaald door het antispambeveiligingsniveau. Meer informatie vindt u onder *“Het gevoeligheidsniveau aanpassen”* (p. 106).

Als de lokale antispamfilters geen afdoend resultaat bieden, wordt de e-mail gecontroleerd met “in-the-cloud” detectie die uiteindelijk beslist of de e-mail spam of rechtmatig is.

## 19.1.3. Antispam-updates

Telkens wanneer een update wordt uitgevoerd, worden nieuwe handtekeningen voor bekende spam-e-mails en koppelingen toegevoegd aan de databases. Dit zal de doeltreffendheid van uw Antispam-engine verbeteren.

Bitdefender kan automatische updates uitvoeren om u te beschermen tegen spammers. Zorg dat de optie voor **Automatische Update** ingeschakeld blijft.

## 19.1.4. Ondersteunde e-mailclients en protocollen

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

- Microsoft Outlook 2007 / 2010
- Microsoft Outlook Express en Windows Mail (op 32-bits systemen)
- Mozilla Thunderbird 3.0.4

## 19.2. De antispambeveiliging in- of uitschakelen

Antispambeveiliging is standaard niet ingeschakeld. Om de antispammodule in te schakelen, volgt u deze stappen:

1. Het **Bitdefender-venster** openen.

2. Klik op het **Antispam**-paneel op de schakelaar om **Antispam** in of uit te schakelen.
3. Wacht tot Bitdefender de onderdelen van de module installeert.

## 19.3. De antispam-werkbalk in het venster van uw e-mailclient gebruiken


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.




### Belangrijk

Bitdefender wordt geïntegreerd in de vaakst gebruikte e-mailclients via een gemakkelijk te gebruiken antispamwerkbalk. Raadpleeg "*Ondersteunde e-mailclients en protocollen*" (p. 101) voor een complete lijst van ondersteunde e-mailclients.


Elke knop van de Bitdefender-werkbalk wordt hieronder uitgelegd.


 **Is spam** - geeft aan dat de geselecteerde e-mail spam is. De e-mail wordt onmiddellijk naar de map **Spam** verplaatst. Als de antispam-cloud-services zijn geactiveerd, wordt het bericht verzonden naar Bitdefender Cloud voor verdere analyse.


 **Geen spam** - geeft aan dat de geselecteerde e-mail geen spam is en dat Bitdefender het niet als dusdanig mocht labelen. De e-mail wordt van de map **Spam** verplaatst naar de map van uw **Postvak IN**. Als de antispam-cloud-services zijn geactiveerd, wordt het bericht verzonden naar Bitdefender Cloud voor verdere analyse.





### 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. U zult mogelijk op **OK** moeten klikken om te bevestigen. De e-mailberichten die zijn ontvangen van adressen in de spammerslijst, worden automatisch gemarkeerd als [spam].

 **Vriend toevoegen** - voegt de afzender van de geselecteerde e-mail toe aan de vriendenlijst. U zult mogelijk op **OK** moeten klikken om te bevestigen. U ontvangt alle e-mailberichten van dit adres, ongeacht hun inhoud.

 **Spammers** - opent de **Spammerslijst** die alle e-mailadressen bevatten waarvan u geen berichten wilt ontvangen, ongeacht hun inhoud. Meer informatie vindt u onder "*Spammerslijst configureren*" (p. 105).

 **Vrienden** - opent de **Vriendenlijst** die alle e-mailadressen bevatten waarvan u altijd e-mailberichten wilt ontvangen, ongeacht hun inhoud. Meer informatie vindt u onder "*De Vriendenlijst configureren*" (p. 104).

 **Instellingen** - opent een venster waarin u de antispamfilters en de werkbalkinstellingen kunt configureren.


## 19.3.1. Detectiefouten aangeven

Als u een ondersteunde e-mailclient gebruikt, kunt u de antispamfilter gemakkelijk corrigeren (door aan te geven welke e-mailberichten niet als [spam] aangemerkt moeten worden). Hierdoor helpt u de efficiëntie van de antispamfilter te 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 antispam-werkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient). Het e-mailbericht wordt verplaatst naar de map Postvak IN.


## 19.3.2. Niet-gedetectedeerde spamberichten aangeven

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

1. Open uw e-mailclient.
2. Ga naar de map Postvak IN.
3. Selecteer de niet-gedetectedeerde spamberichten.
4. Klik op de knop  **Niet als spam** in de antispam-werkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient). Ze worden onmiddellijk als [spam] gemarkeerd en naar de map met ongewenste e-mail verplaatst.



## 19.3.3. Werkbalkinstellingen configureren

Om de instellingen voor antispam-werkbalk te configureren, klikt u op de knop  **Instellingen** op de werkbalk en vervolgens op het tabblad **Instellingen werkbalk**.

De instellingen zijn gegroepeerd in twee categorieën:

- In de categorie **E-mailregels** kunt u de verwerkingsregels configureren voor de spam-e-mails die door Bitdefender zijn gedetecteerd.
  - ▶ **Bericht verplaatsen naar Verwijderde items** (alleen voor Microsoft Outlook Express / Windows Mail)



### Opmerking

In Microsoft Outlook /Mozilla Thunderbird worden gedetecteerde spamberichten automatisch verplaatst naar een Spam-map die zich in de map Verwijderde items / Trash bevindt.

- ▶ **Markeer e-mailberichten met spam als 'gelezen'** - markeert spamberichten automatisch als gelezen, zodat u er niet door wordt gestoord als ze aankomen.
- In de categorie **Meldingen** kunt u kiezen of u bevestigingsvensters wilt weergeven wanneer u in de antispam-werkbalk op de knoppen  **Spammer toevoegen** en  **Vriend toevoegen** klikt. Bevestigingsvensters kunnen verhinderen dat u e-mailafzenders per ongeluk toevoegt aan een Vrienden-/Spammerslijst.

## 19.4. 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 worden niet als spam gelabeld, zelfs niet 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.

De Vriendenlijst configureren en beheren:

- Als u Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird gebruikt, klikt u op de knop  **Vrienden** in de antispam-werkbalk van **Bitdefender** die in uw e-mailclient is geïntegreerd.
- U kunt ook deze stappen volgen:
  1. Het **Bitdefender-venster** openen.
  2. Op het **Antispam**-paneel klikt u op **Beheren** en selecteert u **Vrienden beheren** op het uitklapbaar keuzemenu.

Om een e-mailadres toe te voegen, selecteert u de optie **E-mailadres**, voert u het adres in en klikt u op de knop **Toevoegen**. Syntaxis: naam@domein.com.

Om alle e-mailadressen van een specifiek domein toe te voegen, selecteert u de optie **Domeinnaam**, voert u de domeinnaam in en klikt u op **Toevoegen**. 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;

Het is aanbevolen het toevoegen van volledige domeinen toe te vermijden, maar in sommige situaties kan dit nuttig zijn. U kunt bijvoorbeeld het e-maildomein toevoegen van het bedrijf waarvoor u werkt of de domeinen van uw vertrouwde partners toevoegen.

Om een item uit de lijst te verwijderen, klikt u op de overeenkomende koppeling **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 .bw1 hebben.

Om een eerder opgeslagen vriendenlijst te laden, klikt u op de knop **Laden** en opent u het overeenkomende bw1-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 **OK** om de wijzigingen op te slaan en het venster te sluiten.

## 19.5. Spammerslijst configureren

De **Spammerslijst** is een lijst van alle e-mailadressen waarvan u geen berichten wilt ontvangen, ongeacht hun inhoud. Alle e-mailberichten die worden ontvangen van een adres van de **Spammerslijst**, worden automatisch en zonder verdere verwerking als SPAM gelabeld.

De Spammerslijst configureren en beheren:

- Als u Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird gebruikt, klikt u op de knop **Spammers** in de antispamwerkbalk van **Bitdefender** die in uw e-mailclient is geïntegreerd.
- U kunt ook deze stappen volgen:
  1. Het **Bitdefender-venster** openen.
  2. Op het **Antispam**-paneel klikt u op **Beheren** en selecteert u **Spammers beheren** op het uitklapbaar keuzemenu.
  3. Ga naar het deelvenster **Antispam**.
  4. Klik op **Beheren** en kies **Spammers** in het menu.

Om een e-mailadres toe te voegen, selecteert u de optie **E-mailadres**, voert u het adres in en klikt u op de knop **Toevoegen**. Syntaxis: naam@domein.com.

Om alle e-mailadressen van een specifiek domein toe te voegen, selecteert u de optie **Domeinnaam**, voert u de domeinnaam in en klikt u op **Toevoegen**. 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 domeinachtersvoegsels) worden als SPAM gelabeld;
- \*com\* - alle ontvangen e-mailberichten met het domeinachtersvoegsel com worden als SPAM gelabeld.

Het is aanbevolen het toevoegen van volledige domeinen toe te vermijden, maar in sommige situaties kan dit nuttig zijn.



## Waarschuwing

Voeg geen domein van rechtmatige webgebaseerde e-mailservices (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, klikt u op de overeenkomende koppeling **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 **OK** om de wijzigingen op te slaan en het venster te sluiten.

## 19.6. Het gevoeligheidsniveau aanpassen

Als u merkt dat sommige rechtmatige e-mails als spam zijn gemarkeerd of dat heel wat spam-e-mails niet gedetecteerd worden, kunt u proberen het niveau voor de antispamgevoeligheid aan te passen om het probleem op te lossen. In plaats van het gevoeligheidsniveau onafhankelijk te wijzigen, is het echter aanbevolen dat u eerst "*De antispamfilter werkt niet goed*" (p. 174) leest en de instructies volgt om het probleem te corrigeren.

Volg deze stappen om het antispamgevoelighedsniveau aan te passen:

1. Bitdefender openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Antispam**.
4. Selecteer in het venster met **Antispaminstellingen** de tab **Instellingen**.
5. Gebruik de beschrijving aan de rechterzijde van de schaal om het gevoelighedsniveau te kiezen dat beter beantwoordt aan uw beveiligingsbehoeften. De beschrijving informeert u ook over alle extra acties die u moet ondernemen om potentiële problemen te vermijden of de efficiëntie van de antispamdetectie te verhogen.

## 19.7. De lokale antispamfilters configureren

Zoals beschreven in "*Antispam-begrippen*" (p. 99), gebruikt Bitdefender een combinatie van verschillende antispamfilters voor het identificeren van spam. De antispamfilters zijn vooraf geconfigureerd voor een efficiënte bescherming.



### Belangrijk

Afhankelijk van het feit of rechtmatige e-mails ontvangt in Aziatische of Cyrillische tekens, kunt u de instelling die dergelijke e-mails blokkeert, in- of uitschakelen. De overeenkomende instelling is uitgeschakeld in de gelocaliseerde versies van het programma die dergelijke tekensets gebruiken (bijvoorbeeld in de Russische of Chinese versie).

Volg deze stappen om de lokale antispamfilters te configureren:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Antispam**.
4. Selecteer in het venster met **Antispaminstellingen** de tab **Instellingen**.
5. Klik op de schakelaars om de lokale antispamfilters in of uit te schakelen.


Als u Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird gebruikt, kunt u de lokale antispamfilters direct vanaf uw e-mailclient configureren. Klik op de knop **Instellingen** in de antispamwerkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient) en klik vervolgens op het tabblad **Antispamfilters**.

## 19.8. In-the-cloud detectie configureren

"In-the cloud"-detectie maakt gebruik van de Bitdefender Cloud-services om u efficiënte antispambeveiliging te bieden die altijd up-to-date is.

Volg deze stappen om een “in the cloud”-detectie te configureren:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Antispam**.
4. Selecteer in het venster met **Antispaminstellingen** de tab **Cloud**.
5. Klik op de schakelaar om de “in-the-cloud”-detectie in of uit te schakelen.
6. Voorbeelden van rechtmatige e-mails of spam-e-mails kunnen worden verzonden naar Bitdefender Cloud wanneer u detectiefouten of niet-gedetecteerde spam-e-mails aanduidt. Hiermee kan de antispam-detectie van Bitdefender worden verbeterd. Configureer het verzenden van e-mailvoorbeelden naar Bitdefender Cloud door de gewenste opties te selecteren.

Als u Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird gebruikt, kunt u “in-the-cloud”-detectie direct vanaf uw e-mailclient configureren. Klik op de knop  **Instellingen** in de antispamwerkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient) en klik vervolgens op het tabblad **Cloud-instellingen**.

## 20. Privacybeheer

Uw persoonlijke informatie is een constant doelwit voor cybercriminelen. Als de bedreigingen zich hebben uitgebreid tot nagenoeg het volledige spectrum van uw online activiteiten, kan onvoldoende beschermde e-mail, Instant messaging en surfen op het web leiden tot informatielekken die uw privacy in gevaar brengen.

Daarnaast kunnen belangrijke bestanden die u op uw computer opslaat, ooit in de verkeerde handen terechtkomen.

Bitdefender Privacybeheer gaat al deze bedreigingen te lijf met meerdere componenten.

- **Antiphishing-beveiliging** - biedt een uitgebreide reeks functies waarmee uw systeem wordt beschermd terwijl u surft op internet. Deze optie verhindert dat u persoonlijke informatie bekendmaakt aan frauduleuze websites die zich voordoen als rechtmatig.
- **Chat encryptie** - codeert uw IM-conversaties zodat u zeker bent dat de inhoud vertrouwelijk blijft tussen u en uw chatpartner.
- **Bestands codering** - hiermee kunt u gecodeerde, door een wachtwoord beveiligde logische schijven (of kluizen) op uw computer maken waar u uw vertrouwelijke en gevoelige documenten veilig kunt opslaan.
- **Bestandsvernietiging** - wist de bestanden en hun sporen permanent van uw computer.

### 20.1. Antiphishing-beveiliging

Bitdefender Antiphishing dat persoonlijke informatie over u wordt onthuld, als u over het Internet surft, door u te waarschuwen voor potentiële phishing webpagina's.

Bitdefender biedt real-time antiphishing bescherming voor:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera
- Yahoo! Messenger

Volg deze stappen om de Antiphishing-instellingen te configureren:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster **Overzicht instellingen** de optie **Privacybeheer**.
4. Selecteer in het venster **Instellingen privacybeheer** het tabblad **Antiphishing**.

Klik op de schakelaars om deze optie in of uit te schakelen.

- De **Bitdefender-werkbalk** in de webbrowser weergeven.



## Opmerking

De werkbalk van de Bitdefender-browser is niet standaard ingeschakeld.

- Search advisor is een component die de resultaten van uw zoekopdrachten en de koppelingen die op websites van sociale netwerken zijn geplaatst, beoordeelt door naast elk resultaat een pictogram te plaatsen.

● U mag deze webpagina niet bezoeken.

⚠ Deze webpagina kan gevaarlijke inhoud bevatten. Ga voorzichtig te werk als u beslist om deze pagina te bezoeken.

● Dit is een pagina die u veilig kunt bezoeken.

Search Advisor beoordeelt de zoekresultaten van de volgende zoekmachines op internet:

- ▶ Google
- ▶ Yahoo!
- ▶ Bing
- ▶ Baidu

Search Advisor beoordeelt de koppelingen die zijn geplaatst op de volgende online sociale netwerkservices:

- ▶ Facebook
- ▶ Twitter

- SSL-webverkeer scannen.

Meer verfijnde aanvallen kunnen gebruik maken van beveiligd webverkeer om hun slachtoffers te misleiden. Het is daarom aanbevolen SSL scannen in te schakelen.

- Bescherming tegen fraude.
- Bescherming tegen phishing.
- Bescherming voor instant messaging.

U kunt een lijst opmaken van websites die niet zullen worden gescand door de Antiphishing-engines van Bitdefender. De lijst mag websites bevatten die u volledig vertrouwt. Voeg bijvoorbeeld de websites toe waar u regelmatig online winkelt.

Klik op de koppeling **Witte lijst** om de witte lijst voor antiphishing te configureren en te beheren. Een nieuw venster wordt weergegeven.

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**.

Om een website uit de lijst te verwijderen, selecteert u de site in de lijst en klikt u op de overeenkomende koppeling **Verwijderen**.

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

## 20.1.1. Bitdefender-bescherming in de webbrowser

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

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera

De Bitdefender-werkbalk is niet uw standaard browserwerkbalk. Hiermee wordt alleen een kleine sleper  bovenaan elke webpagina toegevoegd. Klik om de werkbalk weer te geven.


De werkbalk van Bitdefender bevat de volgende elementen:

### Paginaclassificatie

Afhankelijk van de manier waarop Bitdefender de webpagina die u momenteel bekijkt classificeert, wordt een van de volgende classificaties weergegeven aan de linkerkant van de werkbalk:

- Het bericht "Pagina is niet veilig" verschijnt op een rode achtergrond - u moet de webpagina onmiddellijk verlaten. Als u meer informatie wilt over deze bedreiging, klikt u op het symbool + op de paginaclassificatie.
- Het bericht "Opgelet" verschijnt op een oranje achtergrond - deze webpagina kan gevaarlijke inhoud bevatten. Ga voorzichtig te werk als u beslist om deze pagina te bezoeken.
- Het bericht "Deze pagina is veilig" verschijnt op een groen achtergrond - dit is een veilige pagina om te bezoeken.

### Sandbox

Klik op  om de browser te starten in een door Bitdefender geleverde omgeving, waarbij deze wordt geïsoleerd van het besturingssysteem. Hiermee wordt verhinderd dat op browsers gebaseerde bedreigingen kwetsbaarheden van de browser benutten om de controle over het systeem te krijgen. Gebruik Sandbox wanneer u webpagina's bezoekt waarvan u vermoedt dat ze malware bevatten.

Browservensters die in Sandbox worden geopend, zullen gemakkelijk herkenbaar zijn aan hun gewijzigde omtreklijn en het Sandbox-pictogram dat in het midden van de titelbalk is toegevoegd.





## Opmerking


Sandbox is niet beschikbaar op computers met Windows XP.

### Instellingen

Klik op  om individuele functies in of uit te schakelen:

- Antiphishing Filter
- Antimalware Webfilter
- Search Advisor

### Voedingsschakelaar

Om de werkbalkfuncties volledig in of uit te schakelen, klikt u rechts op de werkbalk op .

## 20.1.2. Bitdefender waarschuwt in de browser

Telkens wanneer u een website bezoekt die als onveilig is geclassificeerd, wordt de website geblokkeerd en wordt een waarschuwingpagina weergegeven in uw browser.

De pagina bevat informatie, zoals de URL van de website en de gedetecteerde bedreiging.

U moet beslissen wat u vervolgens wilt doen. De volgende opties zijn beschikbaar:

- Navigeer weg van de webpagina door te klikken op **Breng me terug naar de veiligheid**.
- Schakel blokkerende pagina's die phishing bevatten, uit door op **Antiphishingfilter uitschakelen** te klikken.
- Schakel blokkerende pagina's die malware bevatten uit door op **Antimalwarefilter uitschakelen** te klikken.
- Voeg de pagina toe aan de witte lijst voor Antiphishing door op **Toevoegen aan witte lijst** te klikken. De pagina wordt niet langer gescand door de antiphishing-engines van Bitdefender.
- U kunt ondanks de waarschuwing naar de webpagina gaan door op **Ik begrijp het risico, laat me er toch heengaan** te klikken.

## 20.2. IM encryptie

De inhoud van uw expresberichten zou alleen mogen bekend zijn voor u en uw chatpartner. Door uw conversaties te coderen, kunt u verhinderen dat iemand die ze probeert te onderscheppen naar en van uw contactpersonen, de inhoud kan lezen.

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

- Uw chatpartner heeft een Bitdefender-product geïnstalleerd dat Chat Encryptie ondersteunt en Chat Encryptie is ingeschakeld voor de toepassing voor instant messaging die voor het chatten wordt gebruikt.
- U en uw chatpartner gebruiken Yahoo! Messenger.



## Belangrijk

Bitdefender zal een conversatie niet coderen als een van de chatpartners een op het web gebaseerde chattoepassing gebruikt, zoals Meebo.

Zodra er aan de minimale vereisten is voldaan, brengt Bitdefender u op de hoogte van de codeerstatus van uw chatsessie via berichten die in het chatvenster worden weergegeven.

Volg deze stappen om de codering van expresberichten in of uit te schakelen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster **Overzicht instellingen** de optie **Privacybeheer**.
4. Klik in het venster **Instellingen privacybeheer** op de schakelaar om de codering van expresberichten in of uit te schakelen. Encryptie is standaard ingeschakeld.

## 20.3. Bestandscodering

Met Bestandscodering van Bitdefender kunt u gecodeerde, door een wachtwoord beveiligde logische schijven (of kluisen) op uw computer maken waar u uw confidentiële en gevoelige documenten veilig kunt opslaan. De in de kluisen 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 kluis schijven vormen, geopend kunnen worden door een ander besturingssysteem (zoals Linux), kan de informatie erop niet gelezen worden doordat deze is gecrypteerd.

Bestandskluisen kunnen worden beheerd vanaf het Bitdefender-venster of via het Windows-snelmenu en het logische station dat aan de kluis is gekoppeld.

### 20.3.1. Bestandskluisen beheren vanaf de Bitdefender-interface

Volg deze stappen om uw bestandskluisen te beheren vanaf de Bitdefender-interface:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.

3. Selecteer in het venster **Overzicht instellingen** de optie **Bestandscodering**.
4. Selecteer in het venster **Bestandscodering** het tabblad **Codering**.

De bestaande bestandskluisen verschijnen in de tabel in het onderste gedeelte van het venster. Om de lijst te vernieuwen, klikt u met de rechtermuisknop in de tabel en selecteert u **Kluisen vernieuwen** in het menu dat wordt weergegeven.

## Bestandskluisen maken

Om een nieuwe kluis te maken, klikt u met de rechtermuisknop in de koptekst van de kluisentabel en selecteert u **Creër bestandskluis**.

Een nieuw venster wordt weergegeven.

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.
  - Voer de naam en het pad van het kluisbestand op de schijf in de overeenkomende velden in.
2. Kies een schijfletter in het menu. Als u de kluis opent, verschijnt een virtuele schijf met de geselecteerde schijfletter in Deze computer.
3. Als u de standaardgrootte (50 MB) van de kluis wilt veranderen, typt u de gewenste waarde in het **Kluisgrootte** veld.
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. 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.

## Bestandskluisen 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. Klik op de kluis in de tabel en selecteer **Kluis openen** in het menu dat wordt weergegeven.



## Opmerking

Als een eerder gemaakte kluis niet in de tabel verschijnt, klikt u met de rechtermuisknop in de koptekst van de kluisentabel, selecteert u **Bestaande kluis toevoegen** en bladert u naar die locatie.

2. Een nieuw venster wordt weergegeven.

De kluisnaam en pad op de schijf worden weergegeven. Kies een schijfletter in het menu.

3. Typ het wachtwoord van de kluis in het **Wachtwoord** veld.

4. 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.

## Bestanden toevoegen aan kluisen

Volg deze stappen om een wizard te starten waarmee u bestanden kunt toevoegen aan een kluis:

1. Het **Bitdefender-venster** openen.
2. Klik op het paneel **Bestands codering** op **Coderen** en selecteer **Bestanden toevoegen aan kluisen** in het vervolkeuzemenu.

Gebruik de knoppen **Volgende** en **Vorige** om te navigeren door de wizard. Klik op **Annuleren** om de wizard af te sluiten.

1. **Bestanden & mappen selecteren**

Klik op **Doel toevoegen** om de bestanden/mappen te selecteren die aan de kluis zullen worden toegevoegd.

2. **Selecteren**

U kunt een bestaande kluis selecteren, een eerder gemaakte kluis zoeken of een nieuwe maken voor het toevoegen van de bestanden.

3. **Maken**

Als u hebt gekozen om een nieuwe kluis te maken, voert u hier de benodigde informatie over de kluis in. Meer informatie vindt u onder "**Bestandskluisen maken**" (p. 114)

4. **Wachtwoord invoeren**

Als u een vergrendelde kluis hebt geselecteerd, moet u het wachtwoord invoeren om deze te openen.

## 5. Bevestigen

Hier kan u de gekozen acties controleren.



### Opmerking

Als u ervoor hebt gekozen om een nieuwe bestandskluis te maken, vraagt Bitdefender u het station dat ermee gekoppeld is, te formatteren. Selecteer de formatteeropties en klik op **Start** om het station te formatteren.

## 6. Inhoud

Hier kan u de inhoud van de kluis zien.

## Kluizen 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.

Om een kluis te vergrendelen; klikt u in de tabel en selecteert u **Kluis vergrendelen** in het menu dat wordt weergegeven.

Volg deze stappen om een wizard te starten waarmee u een bestandskluis kunt vergrendelen:

1. Het **Bitdefender-venster** openen.
2. Klik op het paneel **Bestandscodering** op **Coderen** en selecteer **Kluis vergrendelen** in het vervolgkeuzemenu.

Gebruik de knoppen **Volgende** en **Vorige** om te navigeren door de wizard. Klik op **Annuleren** om de wizard af te sluiten.

### 1. Selecteren

Hier kan u de te vergrendelen kluis opgeven.

### 2. Bevestigen

Hier kan u de gekozen acties controleren.

### 3. Voltoeien

Hier kan u het resultaat van de actie zien.

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.

## Bestanden verwijderen uit kluisen

Volg deze stappen om een wizard te starten waarmee u bestanden kunt verwijderen uit een kluis:

1. Het **Bitdefender-venster** openen.
2. Klik op het paneel **Bestandscodering** op **Coderen** en selecteer **Bestanden uit kluis verwijderen** in het vervolgkeuzemenu.

Gebruik de knoppen **Volgende** en **Vorige** om te navigeren door de wizard. Klik op **Annuleren** om de wizard af te sluiten.

### 1. Selecteren

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

### 2. Wachtwoord invoeren

Als u een vergrendelde kluis hebt geselecteerd, moet u het wachtwoord invoeren om deze te openen.

### 3. Inhoud

Selecteer de bestanden/mappen die zullen worden verwijderd uit de kluis.

### 4. Bevestigen

Hier kan u de gekozen acties controleren.

### 5. Voltooien

Hier kunt u het resultaat van de bewerking bekijken.

## De inhoud van kluisen weergeven

Volg deze stappen om een wizard te starten waarmee u de inhoud van een bestandskluis kunt weergeven:

1. Het **Bitdefender-venster** openen.
2. Klik op het paneel **Bestandscodering** op **Coderen** en selecteer **Kluisbestanden tonen** in het vervolgkeuzemenu.

Gebruik de knoppen **Volgende** en **Vorige** om te navigeren door de wizard. Klik op **Annuleren** om de wizard af te sluiten.

### 1. Selecteren

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

### 2. Wachtwoord invoeren

Als u een vergrendelde kluis hebt geselecteerd, moet u het wachtwoord invoeren om deze te openen.

### 3. Bevestigen

Hier kan u de gekozen acties controleren.

#### 4. Inhoud

Hier kunt u het resultaat van de bewerking bekijken.

## Het kluiswachtwoord wijzigen

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

1. Klik op de kluis in de tabel en selecteer **Wachtwoord wijzigen** in het menu dat wordt weergegeven.

Een nieuw venster wordt weergegeven.

2. Typ het huidige wachtwoord in het veld **Oud wachtwoord**.
3. 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 @).

4. 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.

## 20.3.2. Bestandskluisen beheren vanaf Windows

Bitdefender wordt in Windows geïntegreerd om u te helpen uw bestandskluisen gemakkelijker te beheren.

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. Om toegang te krijgen tot alle beschikbare kluisbewerkingen, hoeft u in dit menu alleen Bitdefender Bestandskluis aan te wijzen.

Wanneer u daarnaast een kluis opent (monteert), verschijnt een nieuwe logische partitie (een nieuw station). Open Deze computer en u ziet een nieuwe schijf: uw bestandskluis. Hierop kunt u bestandsbewerkingen uitvoeren (kopiëren, verwijderen, wijzigen, 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.

## Kluizen maken

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** > **Bitdefender Bestandskluis** aan en selecteer **Bestandskluis maken**. Een nieuw venster wordt weergegeven.
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.
  - Voer de naam en het pad van het kluisbestand op de schijf in de overeenkomende velden in.
3. Kies een schijfletter in het menu. Als u de kluis opent, verschijnt een virtuele schijf met de geselecteerde schijfletter in Deze computer.
4. Als u de standaardgrootte (50 MB) van de kluis wilt veranderen, typt u de gewenste waarde in het **Kluisgrootte** veld.
5. 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.
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.



## Kluizen 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. Een nieuw venster wordt weergegeven.
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.

## Bestanden toevoegen aan kluizen

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 in het menu Start van Windows op **Computer** (op Windows Vista en 7) of op **Deze computer** (op Windows XP).
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.

## Kluizen 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 in het menu Start van Windows op **Computer** (op Windows Vista en 7) of op **Deze computer** (op Windows XP).
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 Bestandskluis** en klik op **Vergrendelen**.

U kunt ook met de rechtermuisknop klikken op het bestand .bvd dat de kluis voorstelt. Selecteer **Bitdefender Bestandskluis** en klik op **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.

## Bestanden verwijderen uit kluizen

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 in het menu Start van Windows op **Computer** (op Windows Vista en 7) of op **Deze computer** (op Windows XP).
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**).

## Het kluiswachtwoord wijzigen

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**. Een nieuw venster wordt weergegeven.
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.

## 20.4. Bestanden definitief verwijderen

Wanneer u een bestand verwijdert, is het niet langer toegankelijk met de normale middelen. Het bestand blijft echter opgeslagen op de harde schijf tot het wordt overschreven wanneer nieuwe bestanden worden gekopieerd.

Bitdefender Bestandsvernietiging zal u helpen gegevens permanent te verwijderen door ze fysisch te wissen van uw harde schijf.

Volg deze stappen om bestanden of mappen snel permanent te verwijderen van uw computer via het contextmenu van Windows:

1. Klik met de rechtermuisknop op het bestand of de map die u permanent wilt verwijderen.
2. Selecteer **Bitdefender** > **Bestandsvernietiging** in het contextmenu dat verschijnt.
3. Er wordt een bevestigingsvenster weergegeven. Klik op **Ja** om de wizard Bestandsvernietiging te starten.
4. Wacht tot Bitdefender het vernietigen van de bestanden heeft voltooid.
5. De resultaten worden weergegeven. Klik op **Sluiten** om de wizard af te sluiten.

U kunt bestanden ook vernietigen via de Bitdefender-interface.

1. Het **Bitdefender-venster** openen.
2. Klik op het paneel **Privacy** op **Beveiligen** en selecteer **Bestandsvernietiging** in het vervolkeuzemenu.

3. Volg de wizard Bestandsvernietiging:

a. **Map/bestand selecteren**

Voeg de bestanden of mappen toe die u definitief wilt verwijderen.

b. **Bestanden vernietigen**

Wacht tot Bitdefender het vernietigen van de bestanden heeft voltooid.

c. **Resultaten**

De resultaten worden weergegeven. Klik op **Sluiten** om de wizard af te sluiten.

## 21. Firewall

De Firewall beschermt uw computer tegen inkomende en uitgaande onrechtmatige verbindingspogingen, zowel op lokale netwerken als op internet. Dit kan worden vergeleken met een wachter bij uw poort - de toepassing traceert verbindingspogingen en beslist welke moeten worden toegestaan en welke moeten worden geblokkeerd.

De Bitdefender-firewall gebruikt een reeks regels om gegevens te filteren die naar en van uw systeem zijn overgedragen. De regels zijn gegroepeerd in 3 categorieën:

### Algemene regels

Regels die vastleggen via welke protocollen communicatie is toegelaten.

Er wordt een standaard set met regels gebruikt die een optimale bescherming biedt. U kunt de regels bewerken door verbindingen via bepaalde protocollen toe te staan of te weigeren.

### Toepassingsregels

Regel die bepalen hoe elk toepassing toegang krijgt tot de netwerkbronnen en internet.

In normale omstandigheden maakt Bitdefender automatisch een regel wanneer een toepassing toegang probeert te krijgen via internet. U kunt regels voor toepassingen ook handmatig toevoegen of bewerken.

### Adapterregels

Regels die bepalen of uw computer kan communiceren met andere computers verbonden met hetzelfde netwerk.

U dient regels aan te maken om verkeer tussen uw computer en andere computers duidelijk toe te staan of te weigeren.

Als uw computer werkt met Windows Vista of Windows 7, wijst Bitdefender automatisch een netwerktype toe aan elke netwerkverbinding die het detecteert. Afhankelijk van het netwerktype is de firewall-beveiliging ingesteld op het geschikte niveau voor elke aansluiting.

Meer informatie over de firewall-instellingen voor elk netwerktype en de manier waarop u de netwerkinstellingen kunt bewerken, vindt u onder "*Verbindingsinstellingen beheren*" (p. 125).

Er wordt aanvullende bescherming geboden door het **Inbraakdetectiesysteem** (IDS). Het inbraakdetectiesysteem bewaakt de netwerk- en systeemactiviteiten en beschermt ze tegen boosaardige activiteiten of overtredingen van het beleid. Niet alleen pogingen tot het wijzigen van kritieke systeembestanden, Bitdefender-bestanden of registergegevens, worden hiermee gedetecteerd en geblokkeerd, maar ook pogingen om malwarestuurprogramma's te installeren en aanvallen door de injectie van codes (DLL-injectie) worden verhinderd.

Bitdefender is standaard geconfigureerd om de aanbevolen acties voor uw bescherming automatisch te ondernemen, zonder u lastig te vallen. Als u op de hoogte wilt worden gebracht en wilt beslissen welke actie de beste is wanneer een toepassing internettoegang vraagt of verdacht gedrag vertoont, moet u de **Paranoïde-modus** inschakelen.

## 21.1. De firewall-beveiliging in- of uitschakelen

Volg deze stappen om de firewallbescherming in of uit te schakelen:

1. Het **Bitdefender-venster** openen.
2. Klik op het **Firewall**-paneel, op de Firewall-schakelaar.



### Waarschuwing

Omdat het uw computer blootstelt voor onbevoegde verbindingen, mag het uitschakelen van de firewall slechts een tijdelijke maatregel zijn. Schakel de firewall zo snel mogelijk opnieuw in.

## 21.2. Verbindingsinstellingen beheren

Volg deze stappen om de netwerkverbindinginstellingen weer te geven en te bewerken:

1. Het **Bitdefender-venster** openen.
2. Klik op het **Firewall**-paneel, op **Adapters beheren**.

Een nieuw venster wordt weergegeven. De grafiek bovenaan in het venster toont real time informatie over binnenkomend en uitgaand verkeer.

Onder de grafiek wordt de volgende informatie weergegeven voor elke netwerkverbinding.

● **Netwerktipe** - het type netwerk waarmee de computer verbonden is. Bitdefender is van toepassing op een basisset firewall-instellingen, afhankelijk van het type netwerk waarmee u verbonden bent.

U kunt het type wijzigen door het vervolkeuzemenu **Netwerktipe** te openen en een van de beschikbare types in de lijst te selecteren.

Netwerktipe	Beschrijving
<b>Vertrouwd</b>	De firewall voor de betreffende adapter uitschakelen.
<b>Thuis/Bureau</b>	Alle verkeer tussen uw computer en computers in het netwerk toestaan.
<b>Openbaar</b>	Alle verkeer blokkeren is uitgeschakeld.

Netwerktype	Beschrijving
<b>Niet-vertrouwd</b>	Netwerk- en internetverkeer door de betreffende adapter compleet blokkeren.

- **Stealth-modus** - hiermee kunt u instellen of u door andere computers kunt worden gedetecteerd.

Om de Stealth-modus te configureren, selecteert u de gewenste optie vanuit het overeenkomstige uitklapbare keuzemenu.

Stealth-optie	Beschrijving
<b>Aan</b>	Stealth-modus is aan.Uw computer is zowel onzichtbaar vanaf het lokale netwerk als vanaf internet.
<b>Uit</b>	Stealth-modus is uit.Iemand op het lokale netwerk of het internet kan pingen en uw computer detecteren.
<b>Remote</b>	Uw computer kan niet gedetecteerd worden vanaf het internet.Lokale netwerk gebruikers kunnen pingen en uw computer detecteren.

- **Algemeen** - hiermee kunt u instellen of er generieke regels moeten worden toegepast op deze verbinding.

Als het IP-adres van een netwerkadapter wordt gewijzigd, zal Bitdefender het netwerktype overeenkomstig wijzigen.Indien u hetzelfde type wilt behouden, selecteert u **Ja** in het overeenkomstige uitklapbare keuzemenu.

## 21.3. Firewall-regels beheren

### 21.3.1. Algemene regels

Telkens wanneer gegevens via internet worden verzonden, worden bepaalde protocollen gebruikt.

Via de algemene regels kunt u configureren via welke protocollen verkeer is toegestaan.Volg deze stappen om de regels te bewerken:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Firewall**.
4. Selecteer in het venster met **Firewallinstellingen** de tab **Instellingen**.

5. Klik onder Firewallregels op **Algemene regels**.

Een nieuw venster wordt weergegeven. De huidige regels worden weergegeven.

Om een regel te bewerken, klikt u op de overeenkomende pijl in de kolom **Actie** en selecteert u **Toestaan** of **Weigeren**.

## **DNS via UDP/TCP**

DNS via UDP en TCP toestaan of weigeren.

Dit type verbinding is standaard toegestaan.

## **Binnenkomende ICMP/ICMPv6**

ICMP-/ ICMPv6-berichten toestaan of weigeren.

ICMP-berichten worden vaak gebruikt door hackers om aanvallen op computernetwerken uit te voeren. Dit type verbinding wordt standaard geweigerd.

## **E-mails verzenden**

Het verzenden van e-mails via SMTP toestaan of weigeren.

Dit type verbinding is standaard toegestaan.

## **HTTP webbrowsing**

HTTP surfen op het web toestaan of weigeren.

Dit type verbinding is standaard toegestaan.

## **Inkomende desktopverbindingen op afstand**

Toegang van andere computers via verbindingen met extern bureaublad toestaan of weigeren.

Dit type verbinding is standaard toegestaan.

## **Windows Verkenner-verkeer op HTTP/FTP**

HTTP- en FTP-verkeer van Windows Verkenner toestaan of weigeren.

Dit type verbinding wordt standaard geweigerd.

## 21.3.2. Toepassingsregels

Klik op **Toepassingsregels** om de firewallregels die de toegang bepalen van de toepassingen tot netwerkbronnen en internet, te beheren.

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Firewall**.
4. Selecteer in het venster met **Firewallinstellingen** de tab **Instellingen**.
5. Klik onder Firewallregels op **Toepassingsregels**.



U kunt de programma's (processen) zien waarvoor er firewallregels zijn gemaakt in de tabel. Om de regels voor een specifieke toepassing te zien, klikt u op het vakje + naast de betreffende toepassing of dubbelklikt u erop.

Voor elke regel wordt de volgende informatie weergegeven:

- **Proces/Netwerktypen** - het proces en de netwerkadaptertypes waarop de regel van toepassing is. 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)
- **Protocol** - het IP-protocol waarvoor de regel geldt. U kan een van de volgende dingen zien:

Protocol	Beschrijving
<b>Alle</b>	Omvat alle IP-protocollen.
<b>TCP</b>	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.
<b>UDP</b>	User Datagram Protocol - UDP is een IP-gebaseerd transport ontwikkeld voor hoge prestaties. Games en andere op video gebaseerde toepassingen gebruiken vaak UDP.
<b>Een getal</b>	Geeft een specifiek IP-protocol aan (ander dan TCP en UDP). U vindt de complete lijst van toegewezen IP-protocolnummers op <a href="http://www.iana.org/assignments/protocol-numbers">http://www.iana.org/assignments/protocol-numbers</a> .

- **Actie** - of de toepassing al dan niet netwerk- of internettoegang krijgt onder de opgegeven omstandigheden.

Gebruik de knoppen in het onderste deel van het venster voor het beheren van de regels.

- **Regel toevoegen** - opent het venster **Toepassingsregel toevoegen** waarin u een nieuwe regel kunt maken.
- **Regel bewerken** - opent het venster **Toepassingsregel bewerken** waar u de instellingen van een geselecteerde regel kunt wijzigen.
- **Regel verwijderen** - verwijdert de geselecteerde regel.

## Toepassingsregels toevoegen/bewerken

Klik op de overeenkomende knop om een regel toe te voegen of te bewerken. Een nieuw venster wordt weergegeven. Ga als volgt te werk:

- **Programmapad.** Klik op **Bladeren** en selecteer de applicatie waarvoor de regel geldt.
- **Lokaal adres.** Geef het lokale IP-adres en poort waarvoor de regel geldt, op. Als u meer dan een netwerkadapter hebt, kunt u het selectievakje **Elke** uitschakelen en een specifiek IP-adres invoeren.
- **Adres op afstand.** Geef het externe IP-adres en poort waarvoor de regel geldt, 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.
- **Netwerktipe.** Selecteer het type netwerk waarvoor de regel geldt.
- **Gebeurtenissen.** Afhankelijk van het geselecteerde protocol, selecteert u de netwerkgebeurtenissen waarop de regel geldt. De volgende gebeurtenissen kunnen verwerkt worden:

Gebeurtenis	Beschrijving
<b>Verbinden</b>	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.
<b>Verkeer</b>	Datastroom tussen twee computers.
<b>Luisteren</b>	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.

- **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 <http://www.iana.org/assignments/protocol-numbers>.

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

Richting	Beschrijving
<b>Uitgaand</b>	De regel zal alleen voor uitgaand verkeer worden toegepast.
<b>Inkomend</b>	De regel zal alleen voor inkomend verkeer worden toegepast.
<b>Beide</b>	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.
- **Machtiging.** Selecteer een van de beschikbare machtigingen:

Machtiging	Beschrijving
<b>Toestaan</b>	De opgegeven toepassing zal netwerk-/internettoegang krijgen onder de opgegeven omstandigheden.
<b>Weigeren</b>	De opgegeven toepassing zal geen netwerk-/internettoegang krijgen onder de opgegeven omstandigheden.

### 21.3.3. Adapterregels

Voor elke netwerkverbinding kunt u speciale vertrouwde of niet-vertrouwde zones configureren.

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

Een niet-vertrouwde zone is een apparaat dat u helemaal niet met uw computer wilt laten communiceren.

Volg deze stappen om gebieden op uw netwerkadapters weer te geven en te beheren:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.

3. Selecteer in het venster met het **Instellingenoverzicht Firewall**.
4. Selecteer in het venster met **Firewallinstellingen** de tab **Instellingen**.
5. Klik onder Firewallregels op **Adapterregels**.

Er verschijnt een nieuw venster met de netwerkadapters met actieve verbindingen en met de huidige zones, als die er zijn.

Gebruik de knoppen in het onderste deel van het venster voor het beheren van de zones.

- **Zone toevoegen** - opent het venster **IP-adres toevoegen** waarin u een nieuwe zone voor een geselecteerde adapter kunt maken.
- **Zone bewerken** - opent het venster **Regel bewerken** waar u de instellingen van een geselecteerde zone kunt wijzigen.
- **Zone verwijderen** - verwijdert de geselecteerde zone.

## Zones toevoegen / bewerken

Klik op de overeenkomende knop om een zone toe te voegen of te bewerken. Er wordt een nieuw venster weergegeven met de IP-adressen van de apparaten die met het netwerk zijn verbonden. Ga als volgt te werk:

1. Selecteer het IP-adres van de computer die u wilt toevoegen of voer een adres of adresbereik in het opgegeven tekstvak in.
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** om de wijzigingen op te slaan en het venster te sluiten.




## 21.4. De netwerkactiviteit bewaken

Om de huidige netwerk-/internetactiviteit (via TCP en UDP) gesorteerd op toepassing te bewaken en het Bitdefender Firewall-logboek te openen, volgt u de onderstaande stappen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Firewall**.
4. Selecteer in het venster met **Firewallinstellingen** de tab **Geavanceerd**.
5. Klik onder Netwerkactiviteit op **Netwerk-activiteit**.

Een nieuw venster wordt weergegeven. 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.

Naast elke verbinding wordt een pictogram weergegeven. 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 realtime. 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 verbindingsoogingen of verkeer volgens de regels), kunt u het Firewall-logboek van Bitdefender weergeven door op **Logboek weergeven** te klikken. Het logboekbestand kunt u vinden onder `?\Program Files\Common Files\Bitdefender\Bitdefender Firewall\bdfirewall.txt`.

## 21.5. Intensiteit waarschuwingen configureren

Bitdefender Total Security 2013 is ontworpen met zo weinig mogelijk opdringerigheid. In normale omstandigheden hoeft u geen beslissingen te nemen over het toestaan of weigeren van verbindingen of acties die toepassingen op uw systeem hebben proberen uit te voeren. Bitdefender neemt alle beslissingen voor u.

Volg deze stappen als u de volledige controle over de beslissingen wilt hebben:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Firewall**.
4. Selecteer in het venster met **Firewallinstellingen** de tab **Instellingen**.
5. Schakel de **Paranoïde-modus** in of uit door op de overeenkomende schakelaar te klikken.



### Opmerking

Als de Paranoïdemodus is ingeschakeld, wordt **Autopilot** automatisch uitgeschakeld.

Zolang de Paranoïde-modus ingeschakeld blijft, wordt een waarschuwing weergegeven waarin u, telkens wanneer een van de volgende situaties optreedt, wordt gevraagd actie te ondernemen:

- Een toepassing probeert een verbinding te maken met internet.
- Een toepassing probeert een actie uit te voeren die door het **inbraakdetectiesysteem** of het **Actief virusbeheer** als verdacht wordt beschouwd.

De waarschuwing bevat gedetailleerde informatie betreffende de toepassing en het gedetecteerde gedrag. Selecteer **Toestaan** of **Weigeren** om de actie toe te staan of te weigeren.

## 21.6. Geavanceerde instellingen configureren

Volg deze stappen om geavanceerde firewallinstellingen te configureren:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Firewall**.
4. Selecteer in het venster met **Firewallinstellingen** de tab **Geavanceerd**.

### 21.6.1. Inbraakdetectiesysteem

Volg deze stappen om het inbraakdetectiesysteem te configureren:

1. Om het inbraakdetectiesysteem in te schakelen, klikt u op de overeenkomende schakelaar.
2. Sleep de schuifregelaar langs de schaal om het gewenste agressiviteitsniveau in te stellen. Gebruik de beschrijving aan de rechterzijde van de schaal om het niveau te kiezen dat beter beantwoordt aan uw beveiligingsbehoeften.

U kunt controleren welke toepassingen zijn gedetecteerd door het inbraakdetectiesysteem in het venster **Gebeurtenissen**.

Als er toepassingen zijn die u vertrouwt en niet wilt dat het inbraakdetectiesysteem scant, kunt u uitsluitingsregels toevoegen voor deze toepassingen. Volg de stappen beschreven in "*Uitgesloten processen beheren*" (p. 93) om een toepassing uit te sluiten van de scan.



#### Opmerking

De werking van de inbraakdetectiesysteem is verwant met deze van **Actief virusbeheer**. Regels voor de uitsluiting van processen zijn van toepassing op beide systemen.

### 21.6.2. Overige instellingen

De volgende functies kunnen worden in- of uitgeschakeld.

- **Internetverbinding delen** - schakelt ondersteuning voor Internetverbinding delen in.



## Opmerking

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

- **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.

- **Meer logboekinformatie** - vermeerdert de informatie van het firewall-logboek.

Bitdefender houdt een logboek bij 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). Het logboek is toegankelijk vanaf het venster **Firewall-activiteit** door op **Logboek weergeven** te klikken.

- **WiFi-verbindingen bewaken** - als u verbonden bent met draadloze netwerken, wordt informatie weergegeven met betrekking tot specifieke netwerkgebeurtenissen (bijvoorbeeld, wanneer een nieuwe computer bij het netwerk is gekomen).

## 22. Safepay veilige online transacties

De computer wordt in snel tempo hét hulpmiddel voor winkelen en bankieren. Facturen betalen, geld overmaken, bijna alles wat u zich maar voor kunt stellen kopen, dat alles is nooit sneller en gemakkelijker geweest.

Dit houdt in het verzenden via internet van persoonlijke gegevens, account- en creditcardgegevens, wachtwoorden en andere soorten privégegevens, met andere woorden, precies het soort gegevensstroom waar cybercriminelen graag gebruik van maken. Hackers zijn meedogenloos in hun pogingen deze gegevens te stelen, dus u kunt nooit voorzichtig genoeg zijn als het om het beveiligen van online transacties gaat.

Bitdefender Safepay biedt een samengebundelde oplossing voor de verschillende manieren waarop uw privégegevens kunnen worden geschaad. Het is een beveiligde browser, een verzegelde omgeving, die is bestemd voor het privé en veilig houden van online bankieren, e-shopping en andere soorten online transacties. U kunt Bitdefender Safepay starten op elk moment dat u gevoelige gegevens via internet wilt verzenden, of het zo instellen dat het automatisch wordt gestart wanneer u bepaalde websites bezoekt.

Bitdefender Safepay biedt de volgende functies:

- Het blokkeert de toegang tot uw desktop en elke poging snapshots van uw scherm te maken.
- Het verschaft een virtueel toetsenbord dat het, als het wordt gebruikt, onmogelijk maakt voor hackers uw aanslagen te lezen.
- Het is volledig onafhankelijk van uw andere browsers.
- Het biedt een ingebouwde hotspotbeveiliging die kan worden gebruikt wanneer uw computer is verbonden met onbeveiligde Wi-Fi-netwerken.
- Het ondersteunt bookmarks en stelt u in staat om te surfen tussen uw favoriete bank/winkelsites.
- Het is niet beperkt tot bankieren en online winkelen. Elke website kan worden geopend in Bitdefender Safepay.

### 22.1. Bitdefender Safepay gebruiken

Standaard detecteert Bitdefender wanneer u naar een online banksite of online winkel in een willekeurige browser op uw computer surft en het vraagt u deze site te starten in Bitdefender Safepay.


Volg dit pad om Bitdefender Safepay handmatig te openen: **Start** → **Alle programma's** → **Bitdefender 2013** → **Bitdefender Safepay**. U kunt dit ook sneller doen door te dubbelklikken op de Bitdefender Safepay-snelkoppeling op uw bureaublad.



Indien u gewend bent aan webbrowsers, zult u geen moeite hebben Bitdefender Safepay te gebruiken - het ziet eruit en gedraagt zich als een gewone browser:

- geef de URL's op in de adresbalk van de sites waar u heen wilt gaan.
- voeg tabs toe om meerdere websites te bezoeken in het Bitdefender Safepay-venster door te klikken op .
- surf terug en vooruit en vernieuw pagina's met gebruikmaking van respectievelijk .
- ga naar de Bitdefender Safepay **instellingen** door te klikken op .
- beheer uw **favorieten** door te klikken op  naast de adresbalk.
- het virtuele toetsenbord openen door te klikken op .

## 22.2. Instellingen configureren

Klik op  om de volgende instellingen te configureren:

### **Algemeen gedrag van Bitdefender Safepay**

Kies wat u wilt dat er gebeurt als u naar een online winkel of site voor online bankieren gaat in uw gewone webbrowser:

- Automatisch openen in Bitdefender Safepay.
- Bitdefender u elke keer laten vragen wat u wilt doen.
- Bitdefender Safepay nooit gebruiken voor pagina's bezocht in een gewone browser.

### **Domeinenlijst**

Kies hoe Bitdefender Safepay zich gedraagt als u websites van specifieke domeinen bezoekt in uw gewone webbrowser door ze toe te voegen aan de domeinenlijst en het gedrag voor elk van hen te selecteren:

- Automatisch openen in Bitdefender Safepay.
- Bitdefender u elke keer laten vragen wat u wilt doen.
- Bitdefender Safepay nooit gebruiken wanneer er een pagina van het domein wordt bezocht in een gewone browser.

## 22.3. Favorieten beheren

Indien u de automatische detectie van sommige of alle websites hebt uitgeschakeld, of Bitdefender detecteert bepaalde websites eenvoudigweg niet, dan kunt u favorieten toevoegen aan Bitdefender Safepay zodat u favoriete websites in de toekomst eenvoudig kunt starten.

Volg deze stappen om een URL toe te voegen aan Bitdefender Safepay-favorieten:

1. Klik op  naast de adresbalk om de pagina met favorieten te openen.



#### Opmerking

De pagina met favorieten is standaard geopend als u Bitdefender Safepay start.

2. Klik op de knop **+** om een nieuwe favoriete pagina toe te voegen.
3. Voer de URL en de titel van de favoriete pagina in en klik op **Aanmaken**. De URL wordt ook toegevoegd aan de Domeinenlijst op de **instellingen**-pagina.


## 22.4. Hotspotbeveiliging voor onbeveiligde netwerken

Als u Bitdefender Safepay gebruikt terwijl u bent verbonden met onbeveiligde Wi-Fi-netwerken (bijvoorbeeld een openbare hotspot), dan wordt er een extra beveiligingslaag geboden door de functie 'Hotspotbeveiliging'. Deze service versleutelt internetcommunicatie via onbeveiligde verbindingen en helpt u daarmee om uw privacy te bewaren, via welk netwerk u ook bent verbonden.

Er moet aan de volgende minimale vereisten worden voldaan voordat Hotspotbeveiliging kan werken:

- U bent ingelogd op een MyBitdefender-account van Bitdefender Total Security 2013.
- Uw computer is verbonden met een onbeveiligd netwerk.

Zodra er aan de minimale vereisten is voldaan, zal Bitdefender u automatisch vragen de beveiligde verbinding te gebruiken wanneer u Bitdefender Safepay opent. U hoeft alleen uw MyBitdefender-gegevens in te voeren wanneer u dat wordt gevraagd.

De beveiligde verbinding wordt geïnitieerd en er wordt een bericht weergegeven in het Bitdefender Safepay-venster wanneer de verbinding tot stand is gebracht. Het symbool  verschijnt voor de URL in de adresbalk om u te helpen beveiligde verbindingen gemakkelijk te herkennen.

## 23. Ouderlijk Toezicht

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

Zodra u Ouderlijk toezicht hebt geconfigureerd, kunt u gemakkelijk zien wat uw kind op de computer doet.

U hebt alleen een computer met internettoegang en een webbrowser nodig.

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).
- applicaties zoals spelletjes, chatten, programma's die bestanden uitwisselen en dergelijke.
- instant messages van andere dan de toegelaten IM contacten.

Controleer de activiteiten van uw kinderen en wijzig de instellingen voor Ouderlijk toezicht via MyBitdefender vanaf elke computer of elk mobiel apparaat met internetverbinding.

### 23.1. Het dashboard van Ouderlijk toezicht openen

Het dashboard van Ouderlijk toezicht is geordend in modules vanaf waar u de activiteiten op de computer van uw kind kunt bewaken.

Met Bitdefender kunt u de toegang tot internet en specifieke toepassingen beheren voor uw kinderen. U kunt ook tegelijkertijd hun activiteiten op hun Facebook-account bewaken.

Met Bitdefender krijgt u toegang tot de instellingen voor Ouderlijk toezicht vanaf uw MyBitdefender-account op elke computer of elk mobiel apparaat met een internetverbinding.

Uw online account openen:

- Op elk apparaat met internettoegang:
  1. Open een webbrowser.
  2. Ga naar: <https://my.bitdefender.com>
  3. Meld u aan bij uw account met uw gebruikersnaam en wachtwoord.
  4. Klik op **Ouderlijk toezicht** om het dashboard te openen.
- Vanaf uw Bitdefender 2013-interface:

1. Zorg dat u bij de computer bent aangemeld met een beheerdersaccount. Alleen gebruikers met beheerdersrechten (administrators) op het systeem kunnen Ouderlijk Toezicht openen en configureren.
2. Het **Bitdefender-venster** openen.
3. Klik bovenaan in het venster op de knop **MyBitdefender** en selecteer **Ouderlijk toezicht** in het vervolgkeuzemenu.
4. Het dashboard Ouderlijk toezicht wordt geopend in een nieuw venster. Hier kunt u de instellingen voor Ouderlijk toezicht van elke Windows-gebruikersaccount controleren en configureren.

## 23.2. Het profiel van uw kind toevoegen

Voordat u Ouderlijk toezicht configureert, moet u afzonderlijke Windows-gebruikersaccounts maken voor uw kinderen. Hiermee weet u precies wat uw kinderen doen op de computer. U moet beperkte (standaard) gebruikersaccounts maken zodat ze de instellingen voor Ouderlijk toezicht niet kunnen wijzigen. Meer informatie vindt u onder *"Windows-gebruikersaccounts maken"* (p. 55).

Het profiel van uw kind toevoegen aan Ouderlijk toezicht:

1. Open het dashboard van Ouderlijk toezicht vanaf uw MyBitdefender-account.
  2. Klik in het menu aan de linkerzijde op **Kind toevoegen**.
  3. Voer de naam en leeftijd van het kind in op het tabblad **Profiel**. Wanneer u de leeftijd van het kind instelt, worden de instellingen die voor die leeftijdscategorie als geschikt worden beschouwd, automatisch geladen volgens de ontwikkelingsnormen van het kind.
  4. Klik op het tabblad **Apparaten**.
- Op het tabblad Apparaten ziet u de computers en mobiele apparaten die gekoppeld zijn met uw MyBitdefender-account.
5. Selecteer de computer en de Windows-account voor uw kind.
  6. Klik op **Opslaan**.

De computer en de Windows-account van uw kind zijn nu gekoppeld aan uw MyBitdefender-account.

### 23.2.1. De activiteit van de kind bewaken


Met Bitdefender kunt u volgen wat uw kinderen op de computer doen.

Zo kunt u altijd exact uitvinden welke websites ze hebben bezocht, welke toepassingen ze hebben gebruikt of welke activiteiten door Ouderlijk toezicht werden geblokkeerd.

De rapporten bevatten gedetailleerde informatie voor elke gebeurtenis, zoals:

- De status van de gebeurtenis.
- De naam van de geblokkeerde website.
- De naam van de geblokkeerde toepassing.
- De apparaatnaam.
- De datum en het tijdstip waarop de gebeurtenis is opgetreden.
- De acties die zijn ondernomen door Bitdefender.

Volg deze stappen voor het bewaken van het internetverkeer, de geopende toepassingen of de Facebook-activiteit voor uw kind:

1. Open het dashboard van Ouderlijk toezicht vanaf uw MyBitdefender-account.
2. Klik op  om het activiteitenvenster te openen voor de overeenkomende module.

## 23.2.2. E-mailmeldingen configureren


Wanneer Ouderlijk toezicht is ingeschakeld, worden de activiteiten van uw kinderen standaard geregistreerd.

Volg deze stappen om e-mailmeldingen te ontvangen:

1. Open het dashboard van Ouderlijk toezicht vanaf uw MyBitdefender-account.
2. Klik bovenaan rechts op het pictogram **Algemene instellingen** .
3. Voer het e-mailadres in waarnaar de e-mailmeldingen moeten worden verzonden.
4. Klik op de knop naast **Update** om de frequentie aan te passen: Dagelijks, wekelijks of maandelijks.

## 23.3. Ouderlijk toezicht configureren

Via het dashboard Ouderlijk toezicht kunt u de modules van Ouderlijk toezicht direct beheren.

Elke module bevat de volgende elementen: de naam van de module, een statusbericht, het pictogram van de module en een knop  waarmee u belangrijke taken met betrekking tot de module kunt uitvoeren.

Klik op een tabblad om de overeenkomende functie van Ouderlijk toezicht te configureren voor de computer:

- **Web** - hiermee kunt u de webnavigatie filteren en tijdbeperkingen op internettoegang.
- **Toepassingen** - hiermee kunt u de toegang tot specifieke toepassingen blokkeren of beperken.

- **Facebook** - hiermee kunt u de Facebook-account van uw kind beschermen.
- **Instant Messaging** - hiermee kunt u het chatten met specifieke IM-contactpersonen toestaan of blokkeren.

De volgende modules zijn toegankelijk voor het bewaken van de activiteit van het kind op het mobiele apparaat:

- **Locatie** - hiermee kunt u de huidige locatie van het apparaat van uw kind op Google Maps.
- **SMS** - hiermee kunt u tekstberichten van een telefoonnummer blokkeren.
- **Oproepen** - hiermee kunt u oproepen van een telefoonnummer blokkeren.

Ga naar uw MyBitdefender-account voor meer informatie over deze modules.

## 23.3.1. Webbeheer

Webbeheer helpt u bij het blokkeren van websites met ongepaste inhoud en het instellen van tijdbeperkingen voor internettoegang.

Webbeheer configureren voor een specifieke gebruikersaccount:

1. Klik op  in het paneel **Web** om het venster **Webactiviteit** te openen.
2. Gebruik de schakelaar om **Webactiviteit** in te schakelen.

### Een website blokkeren

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

1. Klik op de knop **Zwarte lijst**.
2. Geef de website op in het overeenkomende veld.
3. Klik op **Toevoegen**. De website wordt toegevoegd aan de lijst van geblokkeerde websites. Als u uw mening verandert, klikt u op de overeenkomende knop **Verwijderen**.

### Beheer trefwoorden

Trefwoordenbeheer helpt u bij het blokkeren van de toegang tot expresberichten en webpagina's die specifieke woorden bevatten. Met Trefwoordenbeheer kunt u voorkomen dat kinderen ongepaste woorden en zinnen zien wanneer ze online zijn. Bovendien kunt u er zeker van zijn dat ze geen persoonlijke gegevens (zoals het thuisadres of het telefoonnummer) aan mensen die ze op internet ontmoeten geven.

Volg de onderstaande stappen om Trefwoordenbeheer te configureren voor een specifieke gebruikersaccount:

1. Klik op de knop **Trefwoorden**.
2. Geef het trefwoord op in het overeenkomende veld.

3. Klik op **Toevoegen**. Als u uw mening verandert, klikt u op de overeenkomende knop **Verwijderen**.

## Categoriefilter

De Categoriefilter filtert de toegang tot websites op dynamische wijze volgens hun inhoud. Wanneer u de leeftijd van uw kind instelt, wordt de filter automatisch geconfigureerd om websitecategorieën te blokkeren die als ongeschikt worden beschouwd voor de leeftijd van uw kind. Deze configuratie is geschikt in de meeste gevallen.

Als u meer controle wilt over de internetinhoud waaraan uw kind wordt blootgesteld, kunt u de specifieke websitecategorieën kiezen die moeten worden geblokkeerd door de Categoriefilter.

Volg deze stappen om de instellingen voor Categoriefilter voor een specifieke gebruikersaccount te controleren en te configureren:

1. Klik op de knop **Categorieën**.
2. U kunt controleren welke webcategorieën automatisch worden geblokkeerd/beperkt voor de momenteel geselecteerde leeftijdsgroep. Als u niet tevreden bent met de standaardinstellingen, kunt u ze configureren zoals dat nodig is.
3. Klik op **Opslaan**.

## Internettoegang beperken op tijd

U kunt bepalen wanneer uw kind internettoegang krijgt via de opties van **Webplanning** in het venster **Webactiviteit**.


Volg deze stappen om de internettoegang voor een specifieke gebruikersaccount te controleren en te configureren:

1. Klik op de knop **Planning**.
2. Selecteer de tijdsintervallen in het rooster voor het blokkeren van de internettoegang.
3. Klik op **OK**.

## 23.3.2. Toepassings- beheer

Met Toepassingsbeheer kunt u elke toepassing blokkeren. Games, media en messaging software, maar ook andere categorieën van software en malware kunnen op deze manier worden geblokkeerd.

Volg de onderstaande stappen om Toepassingsbeheer te configureren voor een specifieke gebruikersaccount:

1. Klik op  in het paneel **Toepassingen** om het venster **Activiteit toepassingen** te openen.
2. Gebruik de schakelaar om **Activiteit toepassingen** in te schakelen.
3. Klik op de knop **Zwarte lijst**.
4. Klik op **Toevoegen** om de toepassing toe te voegen aan de **Witte lijst toepassingen** of **Zwarte lijst toepassingen**.

## 23.3.3. Facebook-beveiliging

Ouderlijk toezicht bewaakt de Facebook-account van uw kind en rapporteert de hoofdactiviteiten die plaatsvinden.

Deze online activiteiten worden gecontroleerd en uw wordt gewaarschuwd als ze een bedreiging lijken voor uw accountprivacy.

De bewaakte elementen van de online account omvatten:

- het aantal vrienden
- opmerkingen van het kind of zijn vrienden over deze foto's of publicaties
- berichten
- profielpublicaties
- geüploade foto's en video's
- accountprivacy-instellingen

De Facebook-beveiliging configureren voor een specifieke gebruikersaccount:

1. Ga naar het tabblad **Facebook**.
2. Klik op **Profiel kind verbinden** in het paneel **Facebook**.
3. Om de Facebook-account van een kind te beveiligen, installeert u de toepassing met de overeenkomende koppeling.

## 23.3.4. Instant Messaging beheer

Met IM-beheer (Instant Messaging) kunt u de IM-contactpersonen opgeven waarmee uw kinderen mogen chatten of kunt u de toegang blokkeren tot expresberichten die specifieke woorden bevatten.



### Opmerking

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

Volg de onderstaande stappen om Instant Messaging beheer te configureren voor een specifieke gebruikersaccount:



1. Ga naar het tabblad **Instant Messaging**.
2. Klik op  in het paneel **Instant Messaging** om het venster **Activiteit Instant Messaging** te openen.
3. Gebruik de schakelaar om **Activiteit Instant Messaging** in te schakelen.  
Beperk de toegang tot **Instant Messaging** met een van de beschikbare opties:
  - Knop **Zwarte lijst** om een instant messaging-ID in te voeren.
  - De knop **Trefwoorden** om de toegang tot expresberichten die specifieke woorden bevatten, te blokkeren.

## 24. Safego-beveiliging voor sociale netwerken

U vertrouwt uw online vrienden, maar vertrouwt u hun computers? Gebruik de Safego-beveiliging voor sociale netwerken om uw account en uw vrienden te beschermen tegen van online bedreigingen.

Safego is een Bitdefender-toepassing die is ontwikkeld om uw Facebook- en Twitteraccounts veilig te houden. De taak ervan is het scannen van de links die u ontvangt van uw vrienden en het bewaken van de privacy-instellingen van uw account.



### Opmerking

Er is een MyBitdefender-account vereist om deze functie te gebruiken. Meer informatie vindt u onder "*MyBitdefender-account*" (p. 36).

## Safego beveiliging voor Facebook

Dit zijn de hoofdfuncties die beschikbaar zijn voor uw Facebook-account:

- scant automatisch de publicaties in uw newsfeed op boosaardige koppelingen.
- beschermt uw account tegen online bedreigingen.  
Wanneer een publicatie of opmerking die spam, phishing of malware is, wordt gedetecteerd, ontvangt u een waarschuwingsbericht.
- waarschuwt uw vrienden voor verdachte koppelingen die op hun newsfeed zijn gepubliceerd.
- helpt u bij het opbouwen van een veilig netwerk van vrienden met de functie **FriendOMeter**.
- voert een controle uit van de status van de systeemveiligheid, geleverd door Bitdefender QuickScan.

Volg deze stappen om Safego for Facebook te openen vanaf uw Bitdefender-product:

1. Het **Bitdefender-venster** openen.
2. Op het **Safego**-paneel klikt u op **Beheren** en selecteert u **Activeren voor Facebook** op het uitklapbaar keuzemenu. U wordt naar uw account gebracht.  
Als u Safego for Facebook al hebt geactiveerd, zult u de statistieken met betrekking tot de activiteiten ervan kunnen openen door op de knop **Rapporten voor Facebook weergeven** te klikken.
3. Gebruik uw Facebook-aanmeldingsgegevens om een verbinding te maken met de Safego-toepassing.
4. Safego-toegang tot uw Facebook-account toestaan.

## Safego beveiliging voor Twitter

Dit zijn de hoofdfuncties die beschikbaar zijn voor uw Twitter-account:

- scant uw account voortdurend op de achtergrond.
- wanneer er een bedreiging wordt gedetecteerd, wordt u via een rechtstreeks bericht gewaarschuwd, zodat u de nodige acties kunt ondernemen op de bedreiging te neutraliseren.
- zendt een rechtstreeks bericht vanuit uw account naar de volgers op uw lijst waarbij problemen in de accounts zijn gedetecteerd.
- scant uw privéberichten op spam, phishing en malware.
- post automatisch wekelijkse beveiligingsstatistieken over de activiteit in uw account.

Volg deze stappen om Safego for Twitter te openen vanaf uw Bitdefender-product:

1. Het **Bitdefender-venster** openen.
2. Op het **Safego**-paneel klikt u op **Beheren** en selecteert u **Activeren voor Twitter** op het uitklapbaar keuzemenu. U wordt naar uw account gebracht.  
Als u Safego for Twitter al hebt geactiveerd, zult u de statistieken met betrekking tot de activiteiten ervan kunnen openen door op de knop **Rapporten voor Twitter weergeven** te klikken.
3. Gebruik uw Twitter-aanmeldingsgegevens om een verbinding te maken met de Safego-toepassing.
4. Safego-toegang tot uw Twitter-account toestaan.

## 25. Antidiefstalinstrument

Diefstal van laptops is een belangrijk probleem dat individuele personen en bedrijven evenzeer schaaft. De gegevens die men verliest kan zelfs voor nog meer schade zorgen dan het verliezen van de hardware zelf en kan op zowel financieel als emotioneel gebied belangrijk zijn.

Er zijn maar weinig mensen die de juiste stappen nemen om hun belangrijke persoonlijke, zakelijke en financiële gegevens te beveiligen voor het geval ze gestolen of verloren worden.

Bitdefender Antidiefstal helpt u om beter voorbereid te zijn op een dergelijk gebeuren en stelt u in staat om op afstand uw computer te lokaliseren of te vergrendelen en om zelfs alle gegevens ervan te wissen, mocht uw computer ooit tegen uw wil worden meegenomen.

Om de Antidiefstalfuncties te gebruiken, moet er worden voldaan aan de volgende minimale vereisten:

- U moet uw computer linken aan een MyBitdefender-account door in te loggen op een account van Bitdefender Total Security 2013.
- De opdrachten kunnen uitsluitend worden verzonden vanuit de MyBitdefender-account waaraan uw computer is gelinkt.
- De computer moet zijn verbonden met internet om de opdrachten te kunnen ontvangen.

Antidiefstalfuncties werken op de volgende manier:

### **Lokaliseren op afstand**

Bekijk de locatie van uw apparaat op Google Maps.

De nauwkeurigheid van de locatie hangt af van hoe Bitdefender deze kan bepalen. De locatie wordt tot op enkele tientallen meters nauwkeurig bepaald als Wi-Fi is ingeschakeld op uw computer en er draadloze netwerken in de omgeving zijn.

Als de computer is verbonden met een LAN-kabel zonder dat er een Wi-Fi-locatie beschikbaar is, wordt de locatie bepaald op basis van het IP-adres, en dat is veel minder nauwkeurig.

### **Vergrendelen op afstand**

Uw computer vergrendelen en een PIN van 4 cijfers instellen om hem te ontgrendelen. Wanneer u de opdracht Vergrendelen verzendt, start de computer opnieuw op en opnieuw inloggen op Windows is alleen mogelijk als de juiste PIN die u hebt ingesteld wordt ingevoerd.

## Wissen op afstand

Alle gegevens van uw computer verwijderen. Wanneer u de opdracht Wissen verzendt, start de computer opnieuw op en de gegevens op alle delen van de harde schijf worden gewist.

Antidiefstal wordt geactiveerd na de installatie en is uitsluitend toegankelijk via uw MyBitdefender-account vanaf elk apparaat met een internetverbinding, waar u ook bent.

## De Antidiefstalfuncties gebruiken vanuit MyBitdefender

Om naar de antidiefstalfuncties te gaan vanuit uw account, volgt u deze stappen:

1. Ga naar <https://my.bitdefender.com> en log in op uw account.
2. Klik op **Antidiefstal**.
3. Selecteer uw computer in de lijst met apparaten.
4. Selecteer de functie die u wilt gebruiken:



**Localiseren** - geef de locatie van uw apparaat weer op Google Maps.



**Wissen** - verwijder alle gegevens van uw computer.



**Belangrijk**

Nadat u een apparaat hebt gewist, stoppen de functies van Antidiefstal.



**Vergrendelen** - Vergrendel uw computer en stel een PINcode in om hem te ontgrendelen.

## 26. Bitdefender USB Immunizer

De Autorun-functie die is ingebouwd in Windows-besturingssystemen is een heel handig hulpmiddel waardoor computers automatisch een bestand kunnen uitvoeren vanaf media die zijn verbonden met deze computers. Software-installaties bijvoorbeeld kunnen automatisch starten als er een cd in de cd-lezer wordt geschoven.

Helaas kan deze functie ook worden gebruikt door malware om automatisch te starten en zo in uw computer te infiltreren vanaf media die beschreven kunnen worden, zoals USB-sticks en geheugenkaarten die via kaartlezers worden verbonden. De afgelopen jaren zijn er talloze op Autorun gebaseerde aanvallen aangemaakt.

Met USB Immunizer kunt u voorkomen dat een willekeurige NTFS, FAT32 of FAT-geformatteerde USB-stick ooit nog automatisch malware uitvoert. Zodra een USB-apparaat immuun is gemaakt, kan malware het niet langer configureren om een bepaalde toepassing uit te voeren wanneer het apparaat wordt verbonden met een Windows-computer.

Om een USB-apparaat immuun te maken, volgt u deze stappen:

1. Verbind de USB-stick met uw computer.
2. Blader op uw computer naar de locatie van het verwijderbare opslagapparaat en rechterklik op het pictogram ervan.
3. Ga in het contextuele menu naar **Bitdefender** en selecteer **Deze schijf immuniseren**.



### Opmerking

Als het station al immuun is gemaakt, verschijnt het bericht **Het USB-apparaat wordt beveiligd tegen op autorun gebaseerde malware** in plaats van de optie Immuniseren.

Om te voorkomen dat uw computer malware start vanaf USB-apparaten die niet immuun zijn gemaakt, kunt u de media autorun-functie uitschakelen. Meer informatie vindt u onder "*De automatische kwetsbaarheidsbewaking gebruiken*" (p. 95).

## 27. Uw computer op afstand beheren

Met uw MyBitdefender-account kunt u de Bitdefender-producten die op uw computers zijn geïnstalleerd, op afstand beheren.

Gebruik MyBitdefender om taken voor uw computers te maken en toe te passen vanaf een externe locatie.

Elke computer wordt beheerd vanaf de MyBitdefender-account als deze voldoet aan de volgende voorwaarden:

- U hebt een Bitdefender 2013-product op de computer geïnstalleerd
- U hebt het Bitdefender-product gekoppeld aan de MyBitdefender-account.
- Ga naar een pc die verbonden is met internet.

### 27.1. MyBitdefender openen

Met Bitdefender kunt u de beveiliging van uw computers beheren door taken toe te voegen aan uw Bitdefender-producten.

Met Bitdefender krijgt u toegang tot uw MyBitdefender-account op elke computer of elk mobiel apparaat met een internetverbinding.

MyBitdefender openen:

- Op elk apparaat met internettoegang:
  1. Open een webbrowser.
  2. Ga naar: <https://my.bitdefender.com>
  3. Meld u aan bij uw account met uw gebruikersnaam en wachtwoord.
- Vanaf uw Bitdefender 2013-interface:
  1. Het **Bitdefender-venster** openen.
  2. Klik bovenaan in het venster op de knop **MyBitdefender** en selecteer vervolgens **Dashboard** in het vervolgkeuzemenu.

### 27.2. Taken uitvoeren op de computers

Om een taak op een van uw computer uit te voeren, opent u uw MyBitdefender-account.

Als u onderaan in het venster op een computerpictogram klikt, ziet u alle administratieve taken die u op de externe computer kunt uitvoeren.

#### **Productregistratie**

Hiermee kunt u Bitdefender op de externe computer registreren door een licentiesleutel in te voeren.

**Een volledige scan van de pc uitvoeren**

Hiermee kunt u een complete scan uitvoeren op de externe computer.

**Kritieke gebieden scannen om actieve malware te detecteren**

Hiermee kunt u een snelle scan uitvoeren op de externe computer.

**Kritieke problemen oplossen**

Hiermee kunt u de problemen oplossen die beveiliging van de externe computer beïnvloeden.

**Productupdate**

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



Tune-up en back-up

## 28. Tune-up

Bitdefender wordt geleverd met een Tune-upmodule die u helpt de integriteit van uw systeem te behouden. De aangeboden hulpmiddelen voor het onderhoud zijn van cruciaal belang voor de verbetering van de reactiviteit van uw systeem en het efficiënte beheer van de harde schijfruimte.

Bitdefender stelt u de volgende hulpmiddelen voor optimalisering van pc's voor:

- **Opruiming van de pc** verwijdert tijdelijke internetbestanden en cookies, ongebruikte systeembestanden en snelkoppelingen naar recente documenten.
- **Defragmentatie** reorganiseert feitelijk de gegevens op de harde schijf, zodat de verschillende gedeelten van een bestand achter elkaar worden opgeslagen op doorgaande wijze.
- **Kopiezoeker** vindt en verwijdert dubbele bestanden op uw systeem.
- **Opruiming register** identificeert en verwijdert de ongeldige of verlopen referenties in het register van Windows. Om het Windows-register zuiver en geoptimaliseerd te houden, adviseren wij om maandelijks een registeropruiming uit te voeren.
- **Registerherstel** kan registersleutels herstellen die eerder door Bitdefender Registeropruiming zijn verwijderd uit het Windows-register.
- **Prestatiebewaking** bewaakt de hardware- en softwareconfiguratie van uw systeem zodat u volledig beschermd bent tegen malware.

### 28.1. Uw PC opruimen

Telkens wanneer u een webpagina bezoekt, worden tijdelijke internetbestanden gemaakt zodat u de volgende keer sneller toegang krijgt tot deze pagina.

Wanneer u een webpagina bezoekt, worden ook cookies opgeslagen op uw computer.

De wizard Pc-opruiming helpt u schijfruimte vrij te maken en uw privacy te beschermen door bestanden te verwijderen die niet langer nuttig zijn.

- Internet Explorer tijdelijke internetbestanden en cookies.
- Mozilla Firefox tijdelijke internetbestanden en cookies.
- tijdelijke bestanden die Windows creëert tijdens de werking.
- recente document snelkoppelingen die Windows creëert als u een bestand opent.

Volg deze stappen om de wizard PC opruimen te starten:

1. Het **Bitdefender-venster** openen.
2. Klik op het **Tune-Up**-paneel op **Optimaliseren** en selecteer **PC-opruiming** vanuit het uitklapbaar keuzemenu.

3. Volg de begeleide procedure van drie stappen om het opruimen uit te voeren. Gebruik de knop **Volgende** om te navigeren door de wizard. Klik op **Annuleren** om de wizard af te sluiten.

- a. **Welkom**

Schakel de opties voor pc-opruiming in of uit door te klikken op **Opruimen aanpassen**:

- Internet Explorer cache opruimen
- Mozilla Firefox cache opruimen
- Recente documenten en tijdelijke systeembestanden opruimen

- b. **Opruiming uitvoeren**

- c. **Resultaten**

## 28.2. Harde schijven defragmenteren

Wanneer u een bestand kopieert dat groter is dan het grootste blok vrije ruimte op de harde schijf, treedt een bestandsfragmentatie op. Omdat er onvoldoende vrije ruimte is om het volledige bestand doorlopend op te slaan, wordt het opgeslagen in verschillende blokken. Wanneer het gefragmenteerde bestand wordt geopend, moeten de gegevens ervan vanaf meerdere verschillende locaties worden gelezen.

Het is aanbevolen een defragmentatie van de harde schijf uit te voeren om:

- sneller toegang te krijgen tot de bestanden.
- de algemene systeemprestaties te verbeteren.
- de levensduur van de harde schijf te verlengen.

Volg deze stappen om de wizard Schijfdefragmentatie te starten:

1. Het **Bitdefender-venster** openen.
2. Klik op het **Tune-Up**-paneel op **Optimaliseren** en selecteer **Schijfdefragmentatie** vanuit het uitklapbaar keuzemenu.
3. Volg de begeleide procedure in vijf stappen om de defragmentatie uit te voeren. Gebruik de knop **Volgende** om te navigeren door de wizard. Klik op **Annuleren** om de wizard af te sluiten.

- a. **Kies de te analyseren schijven**

Selecteer de partities die u wilt controleren voor de fragmentatie.

- b. **Analyseren van geselecteerde partities bezig**

Wacht tot Bitdefender het analyseren van de partities heeft voltooid.

- c. **Schijf selecteren**

de fragmentatiestatus van de geanalyseerde partities wordt weergegeven. Selecteer de partities die u wilt defragmenteren.

#### d. Defragmenteren

Wacht tot Bitdefender het defragmenteren van de partities heeft voltooid.

#### e. Resultaten



#### Opmerking

De defragmentatie kan enige tijd in beslag nemen omdat hierbij delen van opgeslagen gegevens van de ene plaats op de harde schijf naar de andere worden verplaatst. Wij raden u aan de defragmentatie uit te voeren wanneer u de computer niet gebruikt.

## 28.3. Dubbele bestanden zoeken

Dubbele bestanden nemen ruimte in op uw harde schijf. Denk maar eens aan de situatie waarbij hetzelfde .mp3-bestand op drie verschillende locaties is opgeslagen.

De wizard Kopiezoeker helpt u bij het detecteren en verwijderen van dubbele bestanden op uw computer.

Volg deze stappen om de wizard Kopiezoeker te starten:

1. Het **Bitdefender-venster** openen.
2. Klik op het **Tune-Up**-paneel op **Optimaliseren** en selecteer **Kopiezoeker** vanuit het uitklapbaar keuzemenu.
3. Volg de begeleide procedure in vier stappen om duplicaten te identificeren en te verwijderen. Gebruik de knop **Volgende** om te navigeren door de wizard. Klik op **Annuleren** om de wizard af te sluiten.

#### a. Doel selecteren

Voeg de mappen toe waarin dubbele bestanden moeten worden gezocht.

#### b. Zoeken naar kopieën

Wacht tot Bitdefender het zoeken naar duplicaten heeft voltooid.

#### c. Selecteer te verwijderen bestanden

Identieke bestanden worden weergegeven in groepen. U kunt een actie kiezen die op alle groepen of op elke afzonderlijke groep moet worden ondernomen. nieuwste houden, oudste houden of geen actie ondernemen. U kunt ook acties selecteren voor elk individueel bestand.



#### Opmerking

Deze stap wordt overgeslagen als er geen dubbele bestanden zijn gevonden.

#### d. Resultaten

## 28.4. Windows-register opruimen

Heel wat toepassingen schrijven tijdens de installatie sleutels in het Windows-register. Wanneer u dergelijke toepassingen verwijdert, zullen sommige van de gekoppelde registersleutels mogelijk niet worden verwijderd en in het Windows-register blijven. Dit kan uw systeem vertragen en zelfs systeeminstabiliteit veroorzaken. Hetzelfde gebeurt wanneer u snelkoppelingen of bepaalde bestanden van toepassingen die op uw systeem zijn geïnstalleerd verwijdert en in het geval van beschadigde stuurprogramma's.

Volg deze stappen om de wizard Registeropruiming te starten:

1. Het **Bitdefender-venster** openen.
2. Klik op het **Tune-Up**-paneel op **Optimaliseren** en selecteer **Registeropruiming** vanuit het uitklapbaar keuzemenu.
3. Volg de begeleide procedure in vier stappen om het register op te ruimen. Gebruik de knop **Volgende** om te navigeren door de wizard. Klik op **Annuleren** om de wizard af te sluiten.

### a. **Welkom**

### b. **Scan uitvoeren**

Wacht tot Bitdefender het scannen van het register heeft voltooid.

### c. **Selecteer sleutels**

U ziet alle detecteerde ongeldige of verweesde registersleutels. Er wordt gedetailleerde informatie over elke registersleutel verschaft (naam, waarde, prioriteit, categorie).

De registersleutels zijn gegroepeerd op basis van hun plaats in het Windows-register:

- **Software locaties.** Registersleutels die informatie bevatten over het pad naar de op uw computer geïnstalleerde applicaties.

De ongeldige sleutels hebben een lage prioriteit gekregen, waardoor u ze bijna zonder enig risico kan verwijderen.

- **Bedieningselementen.** Registersleutels die informatie bevatten over de op uw computer geregistreerde bestandsextensies. Deze registersleutels worden meestal gebruikt om de associaties te behouden (die ervoor zorgen dat het juiste programma wordt geopend als u een bestand opent vanuit de Windows verkenner). Bijvoorbeeld, zo'n registersleutel laat Windows een .doc bestand openen in Microsoft Word.

De ongeldige sleutels hebben een lage prioriteit gekregen, waardoor u ze bijna zonder enig risico kan verwijderen.

- **Gedeelde DLLs.** Registersleutels die informatie bevatten over de locatie van gedeelde DLL's (Dynamic Link Libraries). In DLL's zijn functies opgeslagen die worden gebruikt door geïnstalleerde toepassingen voor het uitvoeren van bepaalde taken. Zij kunnen worden gedeeld door meerdere toepassingen om geheugen en vereiste schijfruimte te sparen.

Deze registersleutels worden ongeldig als de DLL waarnaar zij verwijzen, is verplaatst naar een andere locatie of geheel is verwijderd (dit gebeurt meestal als u een programma verwijderd).

De ongeldige sleutel heeft een gemiddelde prioriteit gekregen, zodat het verwijderen ervan het systeem negatief kan beïnvloeden.

Standaard zijn alle sleutels gemarkeerd voor het verwijderen. U kunt ervoor kiezen om individuele ongeldige sleutels te verwijderen uit een geselecteerde categorie.

#### d. Resultaten

## 28.5. Opperuimd register herstellen

Na het opruimen van het register, kunt u soms merken dat uw systeem niet goed werkt of dat sommige toepassingen niet correct werken vanwege ontbrekende registersleutels. Dit kan worden veroorzaakt door gedeelde registersleutels die werden verwijderd tijdens de registeropruiming of door andere verwijderde sleutels. Om dit probleem op te lossen, moet u het opperuimde register herstellen.

Volg deze stappen om de wizard Registerherstel te starten:

1. Het **Bitdefender-venster** openen.
2. Klik op het **Tune-Up**-paneel op **Optimaliseren** en selecteer **Registerherstel** vanuit het uitklapbaar keuzemenu.
3. Volg de begeleide procedure in twee stappen om het opperuimde register te herstellen. Gebruik de knop **Volgende** om te navigeren door de wizard. Klik op **Annuleren** om de wizard af te sluiten.

#### a. Controlepunt selecteren

U ziet een lijst met tijdstippen waarop het Windows-register werd opperuimd. Selecteer het tijdstip waarnaar u het Windows-register wilt herstellen.



#### Waarschuwing

Het herstellen van het opperuimde register kan de registersleutels overschrijven die sinds de laatste registeropruiming werden bewerkt.

#### b. Taakresultaten

## 28.6. Prestatiebewaking

De module Prestatiebewaking bewaakt de systeembelasting voortdurend zodat u de lopende toepassingen kunt zien, evenals hun impact op het algemene gedrag van het systeem.

Dit zijn de hoofdfuncties:

- Het CPU- en geheugengebruik van het systeem voorstellen met een reeks indicators
- Het gebruik van de toepassingsbronnen bepalen
- Hulp voor het sluiten van een toepassing die veel systeembronnen in beslag neemt waardoor het systeem slecht presteert

Volg deze stappen om toegang te krijgen tot de opties voor Prestatiebewaking:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Tune-up**.
4. Als u ondervindt dat het systeem vertraagt, kan het probleem worden veroorzaakt door bepaalde toepassingen die op uw systeem worden uitgevoerd. Volg deze stappen om het probleem op te lossen:
  - a. Identificeer de toepassing die het probleem veroorzaakt.
  - b. Klik op de naam van de toepassing om een geschiedenis van het CPU- en geheugengebruik weer te geven en om het installatiepad te tonen.
  - c. Sluit de toepassing met de hiervoor voorziene knop.



### Waarschuwing

Als u vermoedt dat de toepassing (of het proces) die u wilt sluiten, deel uitmaakt van het Windows-besturingssysteem en uw actie het systeem zou kunnen beïnvloeden, moet u contact opnemen met Bitdefender voor ondersteuning zoals beschreven in deel "*Hulp vragen*" (p. 192).

## 29. Online back-up en synchronisatie Safebox

Safebox is de Bitdefender-service waarmee u een back-up kunt maken van belangrijke gegevens op beveiligde online servers, ze kunt delen met uw vrienden en ze kunt synchroniseren tussen uw apparaten.



### Opmerking

Er is een MyBitdefender-account vereist om deze functie te gebruiken. Meer informatie vindt u onder "*MyBitdefender-account*" (p. 36).

Met Safebox:

- U krijgt 2GB vrije free online ruimte voor uw back-ups.
- U kunt uw back-ups direct vanaf Windows Verkenner beheren. Raadpleeg **Back-ups van Safebox beheren vanaf Windows** voor meer informatie.
- U kunt eerdere back-upbestanden die werden verwijderd, herstellen.
- Wijzigingen aan uw bestanden worden opgeslagen zodat u eerdere versies kunt herstellen.
- U kunt bestanden synchroniseren tussen meerdere apparaten waarop Bitdefender Total Security 2013 of de zelfstandige Safebox-toepassing wordt uitgevoerd. Safebox-toepassingen zijn beschikbaar voor Windows PC, iOS en Android. Bezoek <http://www.bitdefender.nl/solutions/safebox.html> voor meer informatie.
- U kunt de bestanden zelf openen op apparaten waarop Bitdefender Total Security 2013 of Bitdefender Safebox niet zijn geïnstalleerd. In dat geval gaat u direct vanaf de browser van elke computer of elk mobiel apparaat met internetverbinding naar uw MyBitdefender-account.

### 29.1. Safebox activeren

Volg deze stappen om Safebox te activeren:

1. Het **Bitdefender-venster** openen.
2. Op het **Safebox**-paneel klikt u op de schakelaar **Auto Sync**.

Er is een snelkoppeling naar de standaardmap voor Safebox op uw bureaublad geplaatst.

Houd de automatische synchronisatie ingeschakeld voor een naadloze back-up van uw gegevens op de Bitdefender-servers.

Safebox-back-ups kunnen worden beheerd vanaf het Bitdefender-venster van Windows Verkenner en andere programma's voor bestandsbeheer via het contextmenu van Windows, of online vanaf de MyBitdefender-account.



## 29.2. SafeBox beheren vanaf het Bitdefender-venster

Volg deze stappen om uw Safebox-back-ups te beheren vanaf Bitdefender:

1. Het **Bitdefender-venster** openen.
2. Klik op het paneel **Safebox** op **Beheren** en selecteer een optie in het vervolgkeuzemenu.

### Mappen beheren

Een nieuw venster zal verschijnen met de mappen die aan Safebox zijn toegevoegd vanaf deze computer en van andere computers of vanaf MyBitdefender.

- Om een nieuwe map toe te voegen aan de Safebox-synchronisatie, bladert u naar de map op uw computer en sleept u deze naar het venster Mappen beheren.


Voeg mappen toe aan de Safebox-synchronisatie om hun inhoud automatisch te synchroniseren met de online servers van Safebox die beschikbaar zijn van MyBitdefender.

- Om een map te verwijderen uit de Safebox-synchronisatie, selecteert u de map en klikt u op de knop **Unsync**.



### Opmerking

Door het verwijderen van een map uit de SafeBox-synchronisatie, wordt de online map niet verwijderd, maar wordt alleen de koppeling tussen de lokale map en de online map verwijderd.

- De Safebox-mappen die zijn toegevoegd van andere computers of van MyBitdefender, verschijnen in de lijst, maar worden niet standaard gesynchroniseerd (het pictogram  verschijnt ernaast).

Om een dergelijke map toe te voegen aan de gesynchroniseerde mappen op deze computer, selecteert u deze en klikt u op **Sync**. Een nieuw venster verschijnt met de vraag de locatie van de lokale map te selecteren. Klik op **Ja** om de standaardlocatie te gebruiken, of op **Nee** om een andere locatie te selecteren.

Om een niet-gesynchroniseerde map die is toegevoegd vanaf een andere computer in de lijst te verwijderen, selecteert u de map en klikt u op **Verwijderen**.

### Beheer gedeelde bestanden

Een nieuw venster zal verschijnen met de bestanden die aan Safebox delen zijn toegevoegd vanaf deze computer en van andere computers of vanaf MyBitdefender.


- Om een nieuw bestand toe te voegen aan Safebox delen, bladert u naar de map op uw computer en sleept u deze naar het venster Mappen beheren. Een nieuw venster verschijnt en toont de voortgang van het uploaden. Zodra het uploaden is voltooid, kopieert u de openbare koppeling naar het klembord door te klikken op het overeenkomende bericht.
- Om de koppeling van een bestand te kopiëren van de lijst naar het klembord, klikt u op de knop **Link delen** en vervolgens op het overeenkomende bericht.
- Om een bestand uit Safebox delen te verwijderen, selecteert u het bestand en klikt u op **Link verwijderen**.

## 29.3. Safebox beheren vanaf Windows




Telkens wanneer u met de rechtermuisknop op of binnen een map klikt, biedt het contextmenu van Windows u snel toegang tot alle beschikbare Safebox-bewerkingen.

### 29.3.1. Mappen toevoegen aan Safebox

Om een map toe te voegen aan Safebox, klikt u met de rechtermuisknop op het pictogram of ergens anders binnen de map en selecteert u **Toevoegen aan Safebox**.

Er wordt een externe map gemaakt op de Bitdefender-servers en de volledige mapinhoud wordt geüpload. Wanneer de mapsynchronisatie is voltooid, verschijnt het Bitdefender-pictogram  over het mappictogram.

De pictogrammen van de bestanden en mappen in een Safebox-map zullen veranderen volgens de status van hun synchronisatie met de externe map:

-  Het bestand / de map wordt gesynchroniseerd.
-  Het bestand / de map wordt niet gesynchroniseerd.
-  Het bestand / de map wordt gesynchroniseerd.

Zodra een map wordt toegevoegd aan Safebox en zolang Auto Sync is ingeschakeld, wordt de inhoud van de map automatisch gesynchroniseerd met de online (externe) map.

### 29.3.2. Mappen uit Safebox verwijderen

Om een map uit Safebox sync te verwijderen, klikt u met de rechtermuisknop op zijn pictogram. Selecteer vervolgens **Bitdefender Safebox** en klik op **Verwijderen van Bitdefender Safebox**. Er wordt een bevestigingsvenster weergegeven. Klik op **Ja** om te verhinderen dat SafeBox de map synchroniseert.

## 29.3.3. Bestanden die uit Safebox zijn verwijderd, herstellen

Zodra een map wordt toegevoegd aan Safebox, houdt Bitdefender alle wijzigingen bij die in die map zijn aangebracht. Hiermee kunt u bestanden herstellen die uit een lokale Safebox-map zijn verwijderd en eerdere versies van bestanden die u in de loop van de tijd hebt gewijzigd, terugzetten.

Om de bestanden die uit een Safebox-map zijn verwijderd, te herstellen, klikt u met de rechtermuisknop op het mappictogram of een andere plaats binnen de map. Selecteer **Bitdefender Safebox** en vervolgens **Verwijderde bestanden herstellen**. Dit zal de nieuwste versies van alle bestanden die uit de map zijn verwijderd, herstellen.

Volg deze stappen om een individueel bestand te herstellen naar een bepaalde versie:

1. Klik met de rechtermuisknop op het bestand.
2. Selecteer **Bitdefender Safebox** en vervolgens **Vorige versies bekijken**.
3. Er wordt een lijst weergegeven met de tijdstippen waarop het bestand werd gewijzigd. Selecteer de versie die u wilt herstellen.
4. Klik op **Herstellen naar...**
5. Selecteer de map waar u het bestand wilt herstellen en klik op **OK**.

## 29.4. Safebox beheren vanaf MyBitdefender

U kunt uw Safebox-mappen openen via uw MyBitdefender-account vanaf elke computer of elk mobiel apparaat met internetverbinding. Dezelfde bewerkingen kunnen zowel vanaf uw account als van Bitdefender Total Security 2013 worden uitgevoerd.

Safebox openen vanaf MyBitdefender:

- Meld u aan bij <https://my.bitdefender.com> vanaf elke computer of elk mobiel apparaat en klik vervolgens op het Safebox-pictogram.
- Van Bitdefender Total Security 2013:
  1. Het **Bitdefender-venster** openen.
  2. Klik op het paneel **Safebox** op **Beheren** en selecteer **Ga naar dashboard** in het vervolgkeuzemenu.

## 29.5. Bestanden synchroniseren tussen uw computers

De bestandssynchronisatie tussen twee of meer computers werkt wanneer aan de volgende voorwaarden is voldaan:

- Bitdefender Total Security 2013 of de zelfstandige Safebox-toepassing wordt geïnstalleerd op de computers waartussen u bestanden wilt synchroniseren.

- U bent met dezelfde MyBitdefender-account aangemeld op elke computer.
- Lokale mappen die met dezelfde online map zijn gekoppeld, zijn op elke computer toegevoegd aan de Safebox-synchronisatie.
- Controleer voor de automatische synchronisatie of Safebox **Auto Sync** is ingeschakeld op elke computer.

Als aan de voorwaarden wordt voldaan, wordt de inhoud van mappen die aan Safebox zijn toegevoegd op de ene computer, gesynchroniseerd met de inhoud van dezelfde externe mappen op de andere computers.

## 29.6. Uw online ruimte upgraden

Safebox biedt u 2GB vrije online ruimte voor uw back-ups.

Als u een grote hoeveelheid gegevens hebt met gegevens zoals muziek, films of belangrijke bestanden die moeten worden beschermd, volstaat de gratis online ruimte van 2 GB mogelijk niet.

Volg deze stappen om uw Safebox-ruimte te upgraden:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Safebox**.
4. Klik in het venster **Safebox-instellingen** op **Safebox upgraden**.
5. De MyBitdefender-pagina wordt geopend in uw webbrowser. Volg de instructies om extra ruimte aan te kopen.

## 29.7. Bestanden permanent verwijderen

Om een bestand volledig te verwijderen van Safebox, moet u het niet alleen uit de Safebox-map op uw computer verwijderen, maar ook uit de online map. Volg deze stappen:

1. Ga naar <https://my.bitdefender.com> en log in op uw account.
2. Klik op het Safebox-pictogram.
3. Selecteer het bestand op het tabblad **Bestanden en mappen** en selecteer vervolgens **Verwijderen** in het vervolgkeuzemenu Acties. Het bestand wordt verplaatst naar de Prullenbak van Safebox.
4. Selecteer het bestand op het tabblad **Prullenbak** en selecteer vervolgens **Verwijderen** in het vervolgkeuzemenu Acties. Klik op **Ja** in het bevestigingsvenster om het bestand volledig te verwijderen.

Zodra een bestand volledig is verwijderd uit Safebox, kunt u niet langer oudere versies herstellen of terugzetten.

## 29.8. Limiet bandbreedte toewijzing

Wanneer u een back-up maakt van uw bestanden, kan dit uw internetverbinding belasten, vooral wanneer het gaat om de overdracht van grote hoeveelheden gegevens.

Om uw andere online activiteiten niet te storen, kunt u de hoeveelheid bandbreedte die is toegewezen aan Safebox-overdrachten, beperken.

Volg deze stappen om de bandbreedte van Safebox te beperken tot 50 kB/s.

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Safebox**.
4. Klik in het venster **Safebox-instellingen** op de schakelaar **Bandbreedte beperken**.

## Problemen oplossen

## 30. Algemene 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.

- *"Mijn systeem lijkt traag"* (p. 166)
- *"Het scannen start niet"* (p. 167)
- *"Ik kan de toepassing niet meer gebruiken"* (p. 168)
- *"Ik kan geen verbinding maken met internet"* (p. 169)
- *"Ik kan geen toegang krijgen tot een apparaat op mijn netwerk."* (p. 170)
- *"Mijn internetverbinding is langzaam"* (p. 171)
- *"Bitdefender updaten bij een langzame internetverbinding"* (p. 172)
- *"Mijn computer is niet verbonden met internet. Hoe kan ik Bitdefender updaten?"* (p. 173)
- *"De Bitdefender-services reageren niet"* (p. 173)
- *"De antispamfilter werkt niet goed"* (p. 174)
- *"Het verwijderen van Bitdefender is mislukt"* (p. 179)
- *"Mijn systeem start niet op na het installeren van Bitdefender"* (p. 179)

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 *"Hulp vragen"* (p. 192).

### 30.1. Mijn systeem lijkt traag

Na het installeren van beveiligingssoftware kan er doorgaans een lichte vertraging van het systeem merkbaar zijn. Dit is normaal tot in zekere mate.

Als u een aanzienlijke vertraging opmerkt, kan dit probleem verschijnen door de volgende redenen:

- **Bitdefender is niet het enige beveiligingsprogramma dat op uw systeem is geïnstalleerd.**

Hoewel Bitdefender de beveiligingsprogramma's verwijdert die tijdens de installatie zijn gevonden, is het aanbevolen elk ander antivirusprogramma dat u mogelijk gebruikt voordat u Bitdefender installeert, te verwijderen. Meer informatie vindt u onder *"Andere beveiligingsoplossingen verwijderen"* (p. 67).

- **Er is niet voldaan aan de minimale systeemvereisten voor het uitvoeren van Bitdefender.**

Als uw apparaat niet voldoet aan de minimale systeemvereisten, wordt de computer trager, vooral wanneer er meerdere toepassingen tegelijk actief zijn. Meer informatie vindt u onder "*Minimale systeemvereisten*" (p. 3).

- **Er zijn nog teveel ongeldige registersleutels in het Windows-register.**

U kunt de prestaties van uw systeem verbeteren door het Windows-register op te ruimen. Meer informatie vindt u onder "*Windows-register opruimen*" (p. 156).

- **Uw harde schijven zijn te gefragmenteerd.**

Bestandsfragmentatie vertraagt de bestandstoegang en verlaagt de systeemprestaties.

U kunt de prestaties van uw systeem verbeteren door Schijfdefragmentatie uit te voeren. Meer informatie vindt u onder "*Harde schijven defragmenteren*" (p. 154).

- **De toepassingen die op uw systeem worden uitgevoerd, gebruiken teveel bronnen.**

Met Prestatiebewaking van Bitdefender kunt u de impact vaststellen van de toepassingen die op uw systeem worden uitgevoerd op uw systeem aan de hand van de CPU-belasting, het geheugengebruik en het gebruik van de harde schijf.

U moet de toepassingen kunnen bepalen waardoor het systeem zwak presteert en ze sluiten of bewaken. Meer informatie vindt u onder "*Prestatiebewaking*" (p. 158).

## 30.2. Het scannen start niet

Dit probleemtype kan twee hoofdoorzaken hebben:

- **Een eerder installatie van Bitdefender die niet volledig werd verwijderd of een ongeldige Bitdefender-installatie.**

Volg in dat geval de onderstaande stappen:

1. Bitdefender volledig van het systeem verwijderen:
  - a. Ga naar <http://www.bitdefender.nl/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. Bitdefender opnieuw installeren op het systeem.



## ● **Bitdefender is niet de enige beveiligingsoplossing die op uw systeem is geïnstalleerd.**

Volg in dat geval de onderstaande stappen:

1. Verwijder de andere beveiligingsoplossing. Meer informatie vindt u onder *"Andere beveiligingsoplossingen verwijderen"* (p. 67).
2. Bitdefender volledig van het systeem verwijderen:
  - a. Ga naar <http://www.bitdefender.nl/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.
3. Bitdefender opnieuw installeren op het systeem.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie *"Hulp vragen"* (p. 192).

## 30.3. Ik kan de toepassing niet meer gebruiken

Dit probleem doet zich voor wanneer u probeert een programma te gebruiken dat normaal werkte vóór de installatie van Bitdefender.

Er kan zich een van de volgende situaties voordoen:

- U kunt van Bitdefender een bericht ontvangen met de melding dat het programma probeert een wijziging aan te brengen aan het systeem.
- U kunt een foutbericht ontvangen van het programma dat u probeert te gebruiken.

Dit soort situatie doet zich voor wanneer de module Actief virusbeheer sommige toepassingen verkeerdelijk identificeert als kwaadaardig.

Actief virusbeheer is een Bitdefender-module die de toepassingen op uw systeem voortdurend bewaakt en programma's met een potentieel boosaardig gedrag rapporteert. Omdat deze functie op een heuristisch systeem is gebaseerd, kunnen er gevallen zijn waarbij rechtmatige toepassingen worden gerapporteerd door Actief virusbeheer.

Wanneer deze situatie zich voordoet, kunt u de respectieve toepassing uitsluiten van de bewaking door Actief virusbeheer.

Volg deze stappen om het programma toe te voegen aan de lijst met uitsluitingen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Antivirus**.

4. Selecteer in het venster met **Antivirusinstellingen** de tab **Uitsluitingen**.
5. Klik op de koppeling **Uitgesloten processen**. In het venster dat verschijnt, kunt u de uitsluitingen voor het proces Actief virusbeheer beheren.
6. Volg deze stappen om uitsluitingen toe te voegen:
  - a. Klik bovenaan in de tabel met uitsluitingen op de knop **Toevoegen**.
  - b. Klik op **Bladeren**, zoek en selecteer de toepassing die u wilt uitsluiten en klik vervolgens op **OK**.
  - c. Houd de optie **Toestaan** geselecteerd om te verhinderen dat Actief virusbeheer de toepassing blokkeert.
  - d. Klik op **Toevoegen**.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 192).

## 30.4. Ik kan geen verbinding maken met internet

Het is mogelijk dat een programma of een webbrowser, na het installeren van Bitdefender, geen verbinding meer kan maken met internet of geen toegang meer krijgt tot de netwerkdiensten.

In dat geval is de beste oplossing het configureren van Bitdefender om verbindingen naar en van de respectieve softwaretoepassing automatisch toe te staan.

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Firewall**.
4. Selecteer in het venster met **Firewallinstellingen** de tab **Instellingen**.
5. Klik onder Firewallregels op **Toepassingsregels**.
6. Klik op de overeenkomende knop om een toepassingsregel toe te voegen.
7. Klik op **Bladeren** en selecteer de applicatie waarvoor de regel geldt.
8. Selecteer alle beschikbare netwerktypes.
9. Ga naar **Machtiging** en selecteer **Toestaan**.

Sluit Bitdefender, open de softwaretoepassing en probeert opnieuw een verbinding te maken met internet.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 192).

## 30.5. Ik kan geen toegang krijgen tot een apparaat op mijn netwerk.

Afhankelijk van het netwerk waarmee u verbonden bent, kan de Bitdefender-firewall de verbinding tussen uw systeem en een ander apparaat (zoals een andere computer of printer) blokkeren. Hierdoor zult u mogelijk niet langer bestanden kunnen delen of afdrucken.

In dat geval is de beste oplossing het configureren van Bitdefender om verbindingen naar en van het respectieve apparaat automatisch toe te staan. Voor elke netwerkverbinding kunt u een speciale vertrouwde zone configureren.

Een vertrouwde zone is een apparaat dat u volledig vertrouwt. Al het verkeer tussen uw computer en het vertrouwde apparaat is toegestaan. Om bronnen met specifieke apparaten, zoals computers of printers te delen, voegt u ze toe als vertrouwde zones.

Volg deze stappen om een vertrouwde zone toe te voegen aan uw netwerkadapters:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Firewall**.
4. Selecteer in het venster met **Firewallinstellingen** de tab **Instellingen**.
5. Klik onder Firewallregels op **Adapterregels**.
6. Klik op de overeenkomende knop om een zone toe te voegen. Er wordt een nieuw venster weergegeven met de IP-adressen van de apparaten die met het netwerk zijn verbonden.
7. Selecteer het IP-adres van de computer of de printer die u wilt toevoegen of voer een adres of adresbereik in het opgegeven tekstvak in.
8. Ga naar **Machtiging** en selecteer **Toestaan**.

Als u nog steeds geen verbinding kunt maken met het apparaat, wordt het probleem mogelijk niet veroorzaakt door Bitdefender.

Controleer op andere potentiële oorzaken, zoals hieronder:

- De firewall op de andere computer kan het delen van bestanden en printers met uw computer blokkeren.
  - ▶ 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**).

- De toegang tot de netwerkprinter is mogelijk beperkt tot specifieke computers of gebruikers. Raadpleeg de netwerkbeheerder om uit te vinden of u de machtiging hebt om een verbinding te maken met die printer.


Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie *"Hulp vragen"* (p. 192).

## 30.6. Mijn internetverbinding is langzaam

Deze situatie kan zich voordoen nadat u Bitdefender hebt geïnstalleerd. Het probleem kan zijn veroorzaakt door fouten in de Bitdefender-firewallconfiguratie.

Volg de onderstaande stappen om deze probleemsituatie op te lossen:

1. Het **Bitdefender-venster** openen.
2. Klik op het paneel **Firewall** op de schakelaar om **Firewall** uit te schakelen.
3. Controleer of uw internetverbinding verbetert wanneer de Bitdefender-firewall is uitgeschakeld.

- Als u nog steeds een langzame internetverbinding kunt maken, wordt het probleem mogelijk niet veroorzaakt door Bitdefender. Neem contact op met uw internet-provider om te controleren of de verbinding werkt aan hun kant.  
Als u van uw internet-provider de bevestiging ontvangt dat de verbinding aan hun zijde werkt en het probleem zich blijft voordoen, neemt u contact op met Bitdefender zoals beschreven in sectie "*Hulp vragen*" (p. 192).
- Volg deze stappen als de internetverbinding is verbeterd naar het uitschakelen van de Bitdefender-firewall:
  - a. Het **Bitdefender-venster** openen.
  - b. Klik op het paneel **Firewall** op de schakelaar om **Firewall** in te schakelen.
  - c. Klik op de knop **Instellingen** in de werkbalk bovenaan.
  - d. Selecteer in het venster met het **Instellingenoverzicht Firewall**.
  - e. Selecteer in het venster met **Firewallinstellingen** de tab **Geavanceerd**.
  - f. Ga naar **Internetverbinding delen** en klik op de schakelaar om deze optie in te schakelen.
  - g. Ga naar **Poortscans blokkeren** en klik op de schakelaar om deze optie uit te schakelen.
  - h. Klik op  om terug te keren naar het hoofdvenster.
  - i. Klik op het **Firewall**-paneel, op **Adapters beheren**.
  - j. Ga naar **Netwerktipe** en selecteer **Thuis/Bureau**.
  - k. Ga naar **Stealth-modus** en stel deze in op **Extern**. Stel **Algemeen** in op **Ja**.
  - l. Sluit Bitdefender, start het systeem opnieuw op en controleer de snelheid van de internetverbinding.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 192).

## 30.7. Bitdefender updaten bij een langzame internetverbinding

Als u een langzame internetverbinding hebt (zoals een inbelverbinding), kunnen er fouten optreden tijdens het updaten.

Volg deze stappen om uw systeem up-to-date te houden met de recentste Bitdefender-malwarehandtekeningen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Update**.

4. Selecteer in het venster **Update-instellingen** het tabblad **Update**.
5. Selecteer onder **Regels voor behandelen updates** de optie **Herinneren voor het downloaden**.
6. Klik op  om terug te keren naar het hoofdvenster.
7. Open het venster **Update** en klik op **Nu bijwerken**.
8. Selecteer alleen **Updates handtekeningen** en klik vervolgens op **OK**.
9. Bitdefender zal alleen de updates van de malwarehandtekeningen downloaden en installeren.

## 30.8. Mijn computer is niet verbonden met internet. Hoe kan ik Bitdefender updaten?

Als uw computer niet is verbonden met internet, moet u de updates handmatig downloaden naar een computer met internettoegang en ze vervolgens overdragen naar uw computer met een verwisselbaar apparaat, zoals een flashstation.

Volg deze stappen:

1. Open een webbrowser op een computer met internettoegang en ga naar:  
<http://www.bitdefender.nl/site/view/Desktop-Products-Updates.html>
2. Klik in de kolom **Handmatige update** op de koppeling die overeenkomt met uw product en systeemarchitectuur. Raadpleeg "*Gebruik ik een 32- of 64-bits versie van Windows?*" (p. 66) als u niet weet of Windows op 32- of 64-bits wordt uitgevoerd.
3. Sla het bestand met de naam `weekly.exe` op het systeem op.
4. Draag het gedownloade bestand over naar een verwisselbaar apparaat, zoals een flashstation, en vervolgens naar uw computer.
5. Dubbelklik op het bestand en volg de stappen van de wizard.

## 30.9. 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 u krijgt een melding 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.

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.

Meer informatie vindt u onder *"Andere beveiligingsoplossingen verwijderen"* (p. 67).

Als de fout zich blijft voordoen, moet u contact opnemen met onze experts voor hulp, zoals beschreven in deel *"Hulp vragen"* (p. 192).

## 30.10. 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.

### 30.10.1. 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.
  1. Als u een van de e-mailclients gebruikt waarin Bitdefender wordt geïntegreerd, **worden de detectiefouten aangegeven.**



## Opmerking

Bitdefender wordt geïntegreerd in de vaakst gebruikte e-mailclients via een gemakkelijk te gebruiken antispam-werkbalk. Raadpleeg "**Ondersteunde e-mailclients en protocollen**" (p. 101) voor een complete lijst van ondersteunde e-mailclients.

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.

## 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. Het **Bitdefender-venster** openen.
2. Op het **Antispam**-paneel klikt u op **Beheren** en selecteert u **Vrienden** op het uitklapbaar keuzemenu.

Een configuratievenster wordt weergegeven.
3. Voer het e-mailadres in waarop u e-mailberichten wilt ontvangen en klik daarna op **Toevoegen**. U kunt zoveel e-mailadressen toevoegen als u wilt.



4. 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 als [spam] aangemerkt moeten worden). Hierdoor helpt u de efficiëntie van de antispamfilter te 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 antispam-werkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient). Het e-mailbericht wordt verplaatst naar de map Postvak IN.

## Het antispambeschermingsniveau verlagen

Volg deze stappen om het antispambeschermingsniveau te verlagen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Antispam**.
4. Selecteer in het venster met **Antispaminstellingen** de tab **Instellingen**.
5. Verplaats de schuifregelaar omlaag op de schaal.

## 30.10.2. Veel spamberichten worden 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.

Probeer de volgende oplossingen:

1. Als u een van de e-mailclients gebruikt waarin Bitdefender wordt geïntegreerd, **worden niet-gedetecteerde spamberichten aangegeven**.



## Opmerking

Bitdefender wordt geïntegreerd in de vaakst gebruikte e-mailclients via een gemakkelijk te gebruiken antispamwerkbalk. Raadpleeg "*Ondersteunde e-mailclients en protocollen*" (p. 101) voor een complete lijst van ondersteunde e-mailclients.

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.

## 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 helpt u de efficiëntie van de antispamfilter te 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 **Als spam** in de antispamwerkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient). Ze worden onmiddellijk als [ spam ] gemarkeerd en naar de map met ongewenste e-mail verplaatst.

## 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. Het **Bitdefender-venster** openen.

2. Op het **Antispam**-paneel klikt u op **Beheren** en selecteert u **Spammers** op het uitklapbaar keuzemenu.  
Een configuratievenster wordt weergegeven.
3. Voer het e-mailadres van de scanner in en klik daarna op **Toevoegen**. U kunt zoveel e-mailadressen toevoegen als u wilt.
4. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

## Het antispambeveiligingsniveau verhogen

Volg deze stappen om het antispambeschermingsniveau te verhogen:

1. Het **Bitdefender-venster** openen.
2. Klik op de knop **Instellingen** in de werkbalk bovenaan.
3. Selecteer in het venster met het **Instellingenoverzicht Antispam**.
4. Selecteer in het venster met **Antispaminstellingen** de tab **Instellingen**.
5. Verplaats de schuifregelaar omhoog op de schaal.

### 30.10.3. De antispamfilter detecteert geen enkel spambericht

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 wordt mogelijk uitgeschakeld. Om de antispam-beveiligingsstatus te controleren, opent u het Bitdefender-venster en schakelt u het selectievakje in het paneel **Antispam** in.

Als Antispam is uitgeschakeld, is dit de oorzaak van uw probleem. Klik op de schakelaar om de antispambeveiliging in te schakelen.

- 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 Total Security 2013 scant geen POP3-verkeer van Lotus Notes.

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 *"Hulp vragen"* (p. 192).

## 30.11. 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.

Volg deze stappen om Bitdefender volledig te verwijderen van uw systeem:

1. Ga naar <http://www.bitdefender.nl/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.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie *"Hulp vragen"* (p. 192).

## 30.12. Mijn systeem start niet op na het installeren van Bitdefender

Als u Bitdefender net hebt geïnstalleerd en het systeem niet langer opnieuw kunt opstarten in de normale modus, kunnen er verschillende redenen zijn voor dit probleem.

Dit wordt zee waarschijnlijk veroorzaakt door een eerdere installatie van Bitdefender die niet goed werd verwijderd of door een andere beveiligingsoplossing die nog steeds op het systeem aanwezig is.

U kunt elke situatie op de volgende manier aanpakken:

● **U had eerder een versie van Bitdefender en hebt deze niet correct verwijderd.**

Volg deze stappen om dit op te lossen:

1. Start uw systeem opnieuw op en ga naar de Veilige modus. Raadpleeg "*Opnieuw opstarten in Veilige modus*" (p. 69) voor meer informatie hierover.
2. Bitdefender verwijderen van uw systeem:
  - a. Ga naar <http://www.bitdefender.nl/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.
3. Start uw systeem opnieuw op in de normale modus en installeer Bitdefender opnieuw.

● **U had eerder een andere beveiligingsoplossing en u hebt deze niet correct verwijderd.**

Volg deze stappen om dit op te lossen:

1. Start uw systeem opnieuw op en ga naar de Veilige modus. Raadpleeg "*Opnieuw opstarten in Veilige modus*" (p. 69) voor meer informatie hierover.
2. Bitdefender verwijderen van uw systeem:
  - a. Ga naar <http://www.bitdefender.nl/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.
3. Om andere software correct te verwijderen, gaat u naar de betreffende website en voert u het hulpprogramma voor het verwijderen uit of neemt u contact op met ons voor de richtlijnen voor het verwijderen.
4. Start uw systeem opnieuw op in de normale modus en installeer Bitdefender opnieuw.

**U hebt de bovenstaande stappen al gevolgd en de situatie is niet opgelost.**

Volg deze stappen om dit op te lossen:

1. Start uw systeem opnieuw op en ga naar de Veilige modus. Raadpleeg "*Opnieuw opstarten in Veilige modus*" (p. 69) voor meer informatie hierover.
2. Gebruik de optie Systeemherstel van Windows om de computer te herstellen naar een eerdere datum voordat u het product Bitdefender installeert. Raadpleeg "*Systeemherstel gebruiken in Windows*" (p. 68) voor meer informatie hierover.

3. Start het systeem opnieuw op in de normale modus en neem contact op met onze experts voor hulp, zoals beschreven in deel "*Hulp vragen*" (p. 192).

## 31. Malware van uw systeem verwijderen

Malware kan uw systeem op heel wat verschillende manieren beïnvloeden en de benadering van Bitdefender is afhankelijk van het type malware-aanval. Omdat virussen vaak hun gedrag veranderen, is het moeilijk een patroon vast te stellen voor hun gedrag en hun acties.

Er zijn situaties wanneer Bitdefender de malwareinfectie niet automatisch kan verwijderen van uw systeem. In dergelijke gevallen is uw tussenkomst vereist.

- *"Helpmodus Bitdefender"* (p. 182)
- *"Wat moet er gebeuren wanneer Bitdefender virussen op uw computer vindt?"* (p. 184)
- *"Een virus in een archief opruimen"* (p. 185)
- *"Een virus in een e-mailarchief opruimen"* (p. 186)
- *"Wat moet ik doen als ik vermoed dat een bestand gevaarlijk is?"* (p. 187)
- *"De geïnfecteerde bestanden van de Systeemvolume-informatie opruimen"* (p. 187)
- *"Wat zijn de wachtwoordbeveiligde bestanden in het scanlogboek?"* (p. 189)
- *"Wat zijn de overgeslagen items in het scanlogboek?"* (p. 189)
- *"Wat zijn de overgecomprimeerde bestanden in het scanlogboek?"* (p. 190)
- *"Waarom heeft Bitdefender een geïnfecteerd bestand automatisch verwijderd?"* (p. 190)

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 *"Hulp vragen"* (p. 192).

### 31.1. Helpmodus Bitdefender

**Helpmodus** is een Bitdefender-functie waarmee u alle bestaande harde schijfpartities buiten uw besturingssysteem kunt scannen en desinfecteren.

Zodra Bitdefender Total Security 2013 is geïnstalleerd, kan de Helpmodus worden gebruikt, zelfs als u niet langer kunt opstarten in Windows.

### Uw systeem starten in de Helpmodus

U kunt de Helpmodus op één of twee manieren openen:

Vanaf het Bitdefender-venster

Volg deze stappen om de Helpmodus direct vanaf Bitdefender te openen:

1. Het **Bitdefender-venster** openen.
2. Klik op het paneel **Antivirus** op **Nu scannen** en selecteer **Helpmodus** in het vervolgkeuzemenu.  
Er wordt een bevestigingsvenster weergegeven. Klik **Yes** om uw computer nu opnieuw op te starten.
3. Nadat de computer opnieuw is opgestart, verschijnt een menu waarin u wordt gevraagd een besturingssysteem te selecteren. Kies **Bitdefender Rescue Image** en druk op de **Enter**-toets om op te starten in een Bitdefender-omgeving waar u uw Windows-partitie kunt opruimen.
4. Druk op **Enter** wanneer u dit wordt gevraagd en selecteer de schermresolutie die het nauwst aanleunt bij de resolutie die u normaal gebruikt. Druk vervolgens opnieuw op **Enter**.

Bitdefender Helpmodus wordt binnen enkele ogenblikken geladen.

Start uw computer direct op in de Helpmodus

Als Windows niet langer start, kunt u met de onderstaande stappen uw computer direct opstarten in de Helpmodus van Bitdefender.



#### Opmerking

Deze methode is niet beschikbaar op computers met Windows XP.

1. Start / herstart uw computer en druk op uw toetsenbord op de **spatiebalk** voordat het Windows-logo verschijnt.
2. Er verschijnt een menu waarin u wordt gevraagd een besturingssysteem voor het opstarten te selecteren. Druk op **TAB** om naar het gebied Tools. Kies **Bitdefender Rescue Image** en druk op de **Enter**-toets om op te starten in een Bitdefender-omgeving waar u uw Windows-partitie kunt opruimen.
3. Druk op **Enter** wanneer u dit wordt gevraagd en selecteer de schermresolutie die het nauwst aanleunt bij de resolutie die u normaal gebruikt. Druk vervolgens opnieuw op **Enter**.

Bitdefender Helpmodus wordt binnen enkele ogenblikken geladen.

## Uw systeem scannen in de Helpmodus

Volg deze stappen om uw systeem te scannen in de Helpmodus:

1. Open de Helpmodus zoals beschreven in "[Uw systeem starten in de Helpmodus](#)" (p. 182).
2. Het Bitdefender-logo verschijnt en het kopiëren van de antivirus-engines wordt gestart.
3. Een welkomstvenster wordt weergegeven. Klik op **Doorgaan**.



4. Er is een update van de antivirushandtekeningen gestart.
5. Nadat de update is voltooid, verschijnt het venster van de antivirusscanner van Bitdefender voor scannen op aanvraag.
6. Klik op **Nu scannen**, selecteer het scandoel in het venster dat verschijnt en klik op **Openen** om het scannen te starten.  
Het is aanbevolen de volledige Windows-partitie te scannen.



## Opmerking

Wanneer u in de Helpmodus werkt, krijgt u te maken met partitienamen van het Linux-type. Schijfpartities zullen verschijnen als `sda1` die waarschijnlijk overeenstemmen met het station (C:) Partitie van het Windows-type, `sda2` overeenkomend met (D:) enz.

7. Wacht tot de scan is voltooid. Volg de instructies als er malware is gedetecteerd, om de bedreiging te verwijderen.
8. Om de Helpmodus af te sluiten, klikt u met de rechtermuisknop in een leeg gebied op het bureaublad. Selecteer vervolgens **Afmelden** in het menu dat verschijnt en kies vervolgens of u de computer opnieuw wilt opstarten of uitschakelen.

## 31.2. Wat moet er gebeuren wanneer Bitdefender virussen op uw computer vindt?

U kunt op een van de volgende manieren controleren of er een virus op uw computer aanwezig is:

- U hebt uw computer gescand en Bitdefender heeft geïnfecteerde items gevonden.
- Een viruswaarschuwing laat u weten dat Bitdefender een of meerdere virussen op uw computer heeft geblokkeerd.

Voer in dergelijke gevallen een update uit van Bitdefender om zeker te zijn dat u over de laatste malwarehandtekeningen beschikt en voer een Volledige systeemscaan uit om het systeem te analyseren.

Selecteer de gewenste actie (desinfecteren, verwijderen, naar quarantaine verplaatsen) voor de geïnfecteerde items zodra de volledige scan is voltooid.



## Waarschuwing

Als u vermoedt dat het bestand deel uitmaakt van het Windows-besturingssysteem of dat het geen geïnfecteerd bestand is, volgt u deze stappen niet en neemt u zo snel mogelijk contact op met de klantendienst van Bitdefender.

Als de geselecteerde actie niet kan worden ondernemen en het scanlogboek een infectie meldt die niet kan worden verwijderd, moet u de bestanden handmatig verwijderen.

## De eerste methode kan worden gebruikt in de normale modus:

1. Schakel de real time-antivirusbeveiliging van Bitdefender uit.
  - a. Het **Bitdefender-venster** openen.
  - b. Klik op de knop **Instellingen** in de werkbalk bovenaan.
  - c. Selecteer **Antivirus**.
  - d. Klik op het tabblad **Shield** in het venster **Antivirusinstellingen**.
  - e. Klik op de schakelaar om **Scannen bij toegang** uit te schakelen.
2. Verborgen objecten weergeven in Windows. Raadpleeg "*Verborgen objecten weergeven in Windows*" (p. 67) voor meer informatie hierover.
3. Blader naar de locatie van het geïnfecteerde bestand (controleer het scanlogboek) en verwijder het.
4. Schakel de real time antivirusbeveiliging van Bitdefender in.

## Volg deze stappen in het geval de infectie niet kan worden verwijderd met de eerste methode:

1. Start uw systeem opnieuw op en ga naar de Veilige modus. Raadpleeg "*Opnieuw opstarten in Veilige modus*" (p. 69) voor meer informatie hierover.
2. Verborgen objecten weergeven in Windows.
3. Blader naar de locatie van het geïnfecteerde bestand (controleer het scanlogboek) en verwijder het.
4. Start uw systeem opnieuw op en ga naar de normale modus.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 192).

## 31.3. Een virus in een archief opruimen

Een archief is een bestand of een verzameling van bestanden dat is gecomprimeerd onder een speciale indeling om de benodigde schijfruimte voor het opslaan van de bestanden te beperken.

Sommige van deze formaten zijn open formaten. Hierdoor kan Bitdefender binnen deze formaten scannen en de geschikte acties ondernemen om ze te verwijderen.

Andere archiefformaten worden gedeeltelijk of volledig gesloten. Bitdefender kan alleen de aanwezigheid van virussen detecteren, maar kan geen andere acties ondernemen.

Als Bitdefender u meldt dat er een virus is gedetecteerd binnen een archief en er geen actie beschikbaar is, betekent dit dat het niet mogelijk is het virus te verwijderen vanwege beperkingen op de machtigingsinstellingen voor het archief.

Een virus dat in een archief is opgeslagen, wordt op de volgende manier opgeruimd:

1. Identificeer het archief dat het virus bevat door een systeemscan uit te voeren.
2. Schakel de real time-antivirusbeveiliging van Bitdefender uit.
  - a. Het **Bitdefender-venster** openen.
  - b. Klik op de knop **Instellingen** in de werkbalk bovenaan.
  - c. Selecteer **Antivirus**.
  - d. Klik op het tabblad **Shield** in het venster **Antivirusinstellingen**.
  - e. Klik op de schakelaar om **Scannen bij toegang** uit te schakelen.
3. Ga naar de locatie van het archief en decomprimeer het met een archiveringstoepassing, zoals WinZip.
4. Identificeer het geïnfecteerde bestand en verwijder het.
5. Verwijder het originele archief zodat u zeker bent dat de infectie volledig is verwijderd.
6. Comprimeer de bestanden in een nieuw archief met een archiveringstoepassing zoals WinZip.
7. Schakel de real time antivirusbescherming van Bitdefender in en voer een Volledige systeemscan uit om zeker te zijn dat er geen andere infecties op het systeem aanwezig zijn.



## Opmerking

Het is belangrijk dat u weet dat een virus dat is opgeslagen in een archief, geen onmiddellijke bedreiging is voor uw systeem, omdat het virus moet worden gedecomprimeerd en uitgevoerd om uw systeem te kunnen infecteren.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie *“Hulp vragen”* (p. 192).

## 31.4. Een virus in een e-mailarchief opruimen

Bitdefender kan ook virussen identificeren in e-maildatabases en e-mailarchieven die op de schijf zijn opgeslagen.

Het is soms nodig het geïnfecteerde bestand te identificeren met de informatie die is opgegeven in het scanrapport en het handmatig te verwijderen.

Een virus dat in een e-mailarchief is opgeslagen, wordt op de volgende manier opgeruimd:

1. Scan de e-maildatabase met Bitdefender.
2. Schakel de real time-antivirusbeveiliging van Bitdefender uit.
  - a. Het **Bitdefender-venster** openen.

- b. Klik op de knop **Instellingen** in de werkbalk bovenaan.
  - c. Selecteer **Antivirus**.
  - d. Klik op het tabblad **Shield** in het venster **Antivirusinstellingen**.
  - e. Klik op de schakelaar om **Scannen bij toegang** uit te schakelen.
3. Open het scanrapport en gebruik de identificatiegegevens (Onderwerp, Van, Aan) van de geïnfecteerde berichten om ze te zoeken in de e-mailclient.
  4. De geïnfecteerde bestanden verwijderen. De meeste e-mailclients verplaatsen het verwijderde bericht ook naar een herstelmap van waar het kan worden hersteld. U moet controleren of dit bericht ook uit deze herstelmap is verwijderd.
  5. Comprimeer de map die het geïnfecteerde bericht bevat.
    - In Outlook Express: Klik in het menu Bestand op Map en vervolgens op Alle mappen comprimeren.
    - In Microsoft Outlook: Klik in het menu Bestand op Gegevensbestandsbeheer. Selecteer de bestanden van de persoonlijke mappen (.pst) die u wilt comprimeren en klik op Instellingen. Klik op Compact.
  6. Schakel de real time antivirusbeveiliging van Bitdefender in.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie "*Hulp vragen*" (p. 192).

## 31.5. Wat moet ik doen als ik vermoed dat een bestand gevaarlijk is?

U kunt vermoeden dat een bestand in uw systeem gevaarlijk is, ondanks het feit dat uw Bitdefender-product het niet heeft gedetecteerd.

Volg deze stappen om te controleren of uw systeem beschermd is:

1. Voer een **Systeemsan** uit met Bitdefender. Raadpleeg "*Hoe kan ik mijn systeem scannen?*" (p. 49) voor meer informatie hierover.
2. Als het scanresultaat schoon lijkt, maar u nog steeds twijfels hebt en wilt zeker zijn over het bestand, moet u contact opnemen met onze experts zodat wij u kunnen helpen.

Raadpleeg "*Hulp vragen*" (p. 192) voor meer informatie hierover.

## 31.6. De geïnfecteerde bestanden van de Systemvolume-informatie opruimen

De map met informatie over systeemvolumes is een zone op uw harde schijf die door het besturingssysteem is gemaakt en door Windows wordt gebruikt voor het opslaan van belangrijke informatie met betrekking tot de systeemconfiguratie.

De Bitdefender-engines kunnen alle geïnfecteerde bestanden die door Systeemvolume-informatie zijn opgeslagen detecteren, maar omdat het om een beschermd gebied gaat is het mogelijk dat ze niet kunnen worden verwijderd.

De geïnfecteerde bestanden die worden gedetecteerd in de mappen Systeemherstel, verschijnen als volgt in het scanlogboek:

```
?:\System Volume Information\_restore{B36120B2-BA0A-4E5D-...
```

Om de geïnfecteerde bestanden in de gegevensopslag volledig en onmiddellijk te verwijderen, schakelt u de functie Systeemherstel uit en opnieuw in.

Wanneer Systeemherstel wordt uitgeschakeld, worden alle herstelpunten verwijderd.

Wanneer Systeemherstel opnieuw wordt ingeschakeld, worden nieuwe herstelpunten gemaakt zoals dat vereist wordt door de planning en de gebeurtenissen.

Volg de onderstaande stappen om Systeemherstel uit te schakelen:

## ● Voor Windows XP:

1. Volg dit pad. **Start** → **Alle programma's** → **Bureau-accessoires** → **Systeemwerkset** → **Systeemherstel**.
2. Klik op **Instellingen Systeemherstel** aan de linkerzijde van het venster.
3. Schakel het selectievakje **Systeemherstel uitschakelen** in voor alle stations en klik op **Toepassen**.
4. Wanneer u wordt gewaarschuwd dat alle bestaande herstelpunten worden verwijderd, klikt u op **Ja** om door te gaan.
5. Om Systeemherstel in te schakelen, schakelt u het selectievakje **Systeemherstel uitschakelen** uit voor alle stations en klikt u op **Toepassen**.

## ● Voor Windows Vista:

1. Volg dit pad. **Start** → **Configuratiescherm** → **Systeem en onderhoud** → **Systeem**
2. Klik in het linkerpaneel op **Systeembeveiliging**.  
Als u wordt gevraagd naar een beheerderswachtwoord of bevestiging, voert u het wachtwoord in of antwoordt u bevestigend.
3. Om Systeemherstel uit te schakelen, schakelt u de selectievakjes uit die overeenkomen met elk station en klikt u op **OK**.
4. Om Systeemherstel in te schakelen, schakelt u de selectievakjes in die overeenkomen met elk station en klikt u op **OK**.

## ● Voor Windows 7:

1. Klik op **Start**, klik met de rechtermuisknop op **Deze computer** en klik op **Eigenschappen**.

2. Klik op de koppeling **Systeembeveiliging** in het linkerdeelvenster.
3. Selecteer elke stationsletter in de opties van **Systeembeveiliging** en klik op **Configureren**.
4. Selecteer **Systeembeveiliging uitschakelen** en klik op **Toepassen**.
5. Klik op **Verwijderen**, klik op **Doorgaan** wanneer u dat wordt gevraagd en klik daarna op **OK**.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in de sectie *"Hulp vragen"* (p. 192).

## 31.7. Wat zijn de wachtwoordbeveiligde bestanden in het scanlogboek?

Dit is slechts een melding die aangeeft dat Bitdefender heeft gedetecteerd dat deze bestanden ofwel door een wachtwoord ofwel door een vorm van codering zijn beveiligd.

De meest gebruikelijke items die door een wachtwoord zijn beveiligd, zijn:

- Bestanden die bij een andere beveiligingsoplossing horen.
- Bestanden die bij het besturingssysteem horen.

Om de inhoud ook daadwerkelijk te scannen, moeten deze bestanden zijn opgehaald of op een andere manier zijn gedecodeerd.

Als deze inhoud zou worden uitgepakt, zou de real time scanner van Bitdefender ze automatisch scannen om uw computer beschermd te houden. Als u die bestanden wilt scannen met Bitdefender, moet u contact opnemen met de productfabrikant voor meer informatie over die bestanden.

Wij raden u aan deze bestanden te negeren omdat ze geen bedreiging vormen voor uw systeem.

## 31.8. Wat zijn de overgeslagen items in het scanlogboek?

Alle bestanden die in het scanrapport als Overgeslagen worden weergegeven, zijn zuiver.

Voor betere prestaties scant Bitdefender geen bestanden die niet werden gewijzigd sinds de laatste scan.

## 31.9. Wat zijn de overgecomprimeerde bestanden in het scanlogboek?

Overgecomprimeerde items zijn elementen die niet kunnen worden opgehaald door de scanengine of elementen waarvoor de decoderingstijd te lang zou zijn waardoor het systeem onstabiel zou kunnen worden.

Overgecomprimeerd betekent dat het Bitdefender het scannen binnen dat archief heeft overgeslagen omdat het uitpakken ervan teveel systeembronnen zou in beslag nemen. De inhoud zal bij real time toegang worden gescand indien dat nodig is.

## 31.10. Waarom heeft Bitdefender een geïnfecteerd bestand automatisch verwijderd?

Als er een geïnfecteerd bestand wordt gedetecteerd, zal Bitdefender automatisch proberen dit te desinfecteren. Als de desinfectie mislukt, wordt het bestand naar quarantaine verplaatst om de infectie in te dammen.

Voor specifieke types malware is desinfectie niet mogelijk omdat het gedetecteerde bestand volledig boosaardig is. In dergelijke gevallen wordt het geïnfecteerde bestand verwijderd van de schijf.

Dit is doorgaans het geval met installatiebestanden die zijn gedownload vanaf onbetrouwbare websites. Als u zelf in een dergelijke situatie terechtkomt, downloadt u het installatiebestand vanaf de website van de fabrikant of een andere vertrouwde website.

Contact opnemen met ons



## 32. Hulp vragen

Bitdefender streeft ernaar haar klanten een ongeëvenaard niveau van snelle en nauwkeurige ondersteuning te bieden. Als u problemen ondervindt met of vragen hebt over uw Bitdefender-product, kunt u meerdere online bronnen gebruiken om snel een oplossing of antwoord te vinden. Als u dat wenst, kunt u ook contact opnemen met de Bitdefender-klantenservice. Onze medewerkers van de ondersteuningsdienst zullen uw vragen snel beantwoorden en u alle hulp bieden die u nodig hebt.

De *“Algemene problemen oplossen”* (p. 166) sectie biedt u de nodige informatie betreffende de vaakst voorkomende problemen tijdens het gebruik van dit product.

Als u de oplossing voor uw probleem niet in de geleverde middelen hebt gevonden, kunt u direct met ons contact opnemen:

- *“Neem direct met ons contact op vanaf uw Bitdefender-product”* (p. 192)
- *“Neem contact op met ons via ons online Ondersteuningscentrum”* (p. 193)



### Belangrijk

Om contact op te nemen met de klantendienst van Bitdefender, moet u uw Bitdefender-product registreren. Meer informatie vindt u onder *“Bitdefender registreren”* (p. 34).

## Neem direct met ons contact op vanaf uw Bitdefender-product

Als u een actieve internetverbinding hebt, kunt u direct vanaf de productinterface contact opnemen met Bitdefender voor hulp.

Volg deze stappen:

1. Het **Bitdefender-venster** openen.
2. Klik onderaan rechts in het venster op de koppeling **Help en ondersteuning**.
3. U hebt de volgende opties:
  - **Help-bestand Bitdefender.**  
Blader door de Bitdefender-documentatie en probeer de voorgestelde oplossingen.
  - **Ondersteuningscentrum**  
Ga naar onze database en zoek de benodigde informatie.
  - **Contact Ondersteuning**  
Gebruik de knop **Contact opnemen met ondersteuning** om het ondersteuningshulpprogramma te starten en contact op te nemen met de

klantendienst. Gebruik de knop **Volgende** om te navigeren door de wizard. Klik op **Annuleren** om de wizard af te sluiten.

- a. Schakel het selectievakje voor de overeenkomst en klik op **Volgende**.
- b. Vul het verzendformulier in met de nodige gegevens:
  - i. Voer uw e-mailadres in.
  - ii. Voer uw volledige naam in.
  - iii. Kies uw land in het overeenkomende menu.
  - iv. Voer een beschrijving in van het probleem dat zich heeft voorgedaan.
- c. Wacht enkele minuten terwijl Bitdefender met het product verwante informatie verzamelt. Deze informatie zal onze technici helpen een oplossing voor uw probleem te vinden.
- d. Klik op **Voltoeien** om de informatie te verzenden naar de klantendienst van Bitdefender. Wij nemen zo snel mogelijk contact op met u.

## Neem contact op met ons via ons online Ondersteuningscentrum

Als u de benodigde informatie niet kunt openen met het Bitdefender-product, kunt u ons online ondersteuningscentrum raadplegen:

1. Ga naar <http://www.bitdefender.nl/support/consumer.html>. Het Ondersteuningscentrum van Bitdefender bevat talrijke artikelen met oplossingen voor problemen met betrekking tot Bitdefender.
2. Selecteer uw product en zoek het Bitdefender-ondersteuningscentrum voor artikels die een oplossing voor uw probleem kunnen bieden.
3. Lees de relevante artikels of documenten en probeer de voorgestelde oplossingen.
4. Als uw probleem hiermee niet is opgelost, gaat u naar <http://www.bitdefender.nl/support/contact-us.html> en neemt u contact op met onze experts.

### 32.1. 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/getSupport>
  - 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/getSupport>
- 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 licentienummer 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 mogelijkerwijze 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.nl> voor upgrades, of onze site met veelgestelde vragen (FAQ) op <http://www.bitdefender.nl/site/Main/contactus/>.

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.

## 33. Online bronnen

Er zijn meerdere online bronnen beschikbaar om u te helpen bij het oplossen van uw problemen en vragen met betrekking tot Bitdefender.

- Bitdefender-ondersteuningscentrum: <http://www.bitdefender.nl/support/consumer.html>
- Bitdefender-ondersteuningsforum: <http://forum.bitdefender.com>
- h e t                    H O T f o r S e c u r i t y - p o r t a a l                    v o o r  
computerbeveiliging: <http://www.hotforsecurity.com>

U kunt ook uw favoriete zoekmachine gebruiken om meer informatie te zoeken over computerbeveiliging, de Bitdefender-producten en het bedrijf.

### 33.1. Bitdefender-ondersteuningscentrum

Het Bitdefender-ondersteuningscentrum is een online opslagplaats van informatie over Bitdefender-producten. Hier worden rapporten bijgehouden in een gemakkelijk toegankelijk formaat over de doorlopende technische ondersteuning en activiteiten voor foutoplossingen van de ondersteunings- en ontwikkelingsteams van Bitdefender. Daarnaast vindt u hier ook meer algemene artikels over viruspreventie, het beheer van Bitdefender-oplossingen met gedetailleerde uitleg en talrijke andere artikels.

Het Bitdefender-ondersteuningscentrum is toegankelijk voor het publiek en kan vrij worden doorzocht. De uitgebreide informatie die de database bevat is nog een middel om Bitdefender-klanten de technische kennis en het inzicht te bieden die ze nodig hebben. Alle geldige aanvragen voor informatie of foutrapporten die van Bitdefender-klanten komen, vinden uiteindelijk hun weg naar het Bitdefender-ondersteuningscentrum, als rapporten over het oplossen van problemen, “spiekbriefjes” om een probleem te omzeilen of informatieve artikels om de helpbestanden van het product aan te vullen.

Het Bitdefender-ondersteuningscentrum is op elk ogenblik beschikbaar op <http://www.bitdefender.nl/support/consumer.html>.

### 33.2. Bitdefender-ondersteuningsforum

Het Bitdefender-ondersteuningsforum biedt Bitdefender-gebruikers een eenvoudige manier om hulp te krijgen en anderen te helpen.

Als uw Bitdefender-product niet goed werkt, als het specifieke virussen niet van uw computer kan verwijderen of als u vragen hebt over de manier waarop het werkt, kunt u uw probleem of vraag op het forum plaatsen.

Bitdefender-ondersteuningstechnici controleren het forum en plaatsen nieuwe informatie om u te helpen. U kunt ook een antwoord of oplossing krijgen van een meer ervaren Bitdefender-gebruiker.

Voordat u uw probleem of vraag verzendt, moet u op het forum zoeken of er geen soortgelijk of verwant onderwerp is.

Het Bitdefender-ondersteuningsforum is beschikbaar op <http://forum.bitdefender.com> in 5 verschillende talen: Engels, Duits, Frans, Spaans en Roemeens. Klik op de koppeling **Home & Home Office Protection** om toegang te krijgen tot het gebied voor verbruiksproducten.

## 33.3. HOTforSecurity-portaal

Het HOTforSecurity-portaal is een rijke bron aan informatie over de computerbeveiliging. Hier leert u meer over de verschillende bedreigingen waaraan uw computer wordt blootgesteld wanneer u een verbinding met internet maakt (malware, phishing, spam, cybercriminelen). Via een nuttig woordenboek leer u de termen kennen met betrekking tot de computerbeveiliging.

Er worden regelmatig nieuwe artikels gepubliceerd om u op de hoogte te houden van de recentst opgespoorde bedreigingen, de huidige beveiligingstrends en andere informatie over de sector van computerbeveiliging.

De webpagina van HOTforSecurity is <http://www.hotforsecurity.com>.

## 34. Contactinformatie

Efficiënte communicatie is de sleutel naar het succes. Gedurende de laatste 10 jaar heeft BITDEFENDER een onberispelijke reputatie opgebouwd door voortdurend te streven naar een betere communicatie om de verwachtingen van onze klanten en partners steeds opnieuw te overtreffen. Aarzel niet contact op te nemen met ons als u eventuele vragen hebt.

### 34.1. Webadressen

Verkoopsafdeling: [sales@bitdefender.com](mailto:sales@bitdefender.com)  
Ondersteuningscentrum: <http://www.bitdefender.com/help>  
Documentatie: [documentation@bitdefender.com](mailto:documentation@bitdefender.com)  
Lokale verdelers: <http://www.bitdefender.nl/partners>  
Partnerprogramma: [partners@bitdefender.com](mailto:partners@bitdefender.com)  
Perscontact: [pr@bitdefender.com](mailto:pr@bitdefender.com)  
Jobs: [jobs@bitdefender.com](mailto:jobs@bitdefender.com)  
Virusverzoeken: [virus\\_submission@bitdefender.com](mailto:virus_submission@bitdefender.com)  
Spamverzoeken: [spam\\_submission@bitdefender.com](mailto:spam_submission@bitdefender.com)  
Misbruikmeldingen: [abuse@bitdefender.com](mailto:abuse@bitdefender.com)  
Website: <http://www.bitdefender.nl>

### 34.2. Lokale verdelers

De lokale Bitdefender-verdelers zijn altijd paraat om te reageren op aanvragen met betrekking tot hun bedrijfsgebied, zowel op commercieel als algemeen vlak.

Een Bitdefender-verdeler in uw land zoeken:

1. Ga naar <http://www.bitdefender.nl/partners/#PartnerLocator/>.
2. De contactgegevens van de lokale Bitdefender-verdelers zouden automatisch moeten verschijnen. Als dat niet gebeurt, selecteert u het land waarin u zich bevindt om de informatie weer te geven.
3. Als u geen Bitdefender-verdeler in uw land vindt, kunt u met ons contact opnemen via e-mail op [sales@bitdefender.com](mailto:sales@bitdefender.com). Noteer uw e-mail in het Engels zodat wij u onmiddellijk kunnen helpen.

### 34.3. Bitdefender-kantoren

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

## France - Nederland

### **Editions Profil**

49, Rue de la Vanne

92120 Montrouge

Telefoon: (0)20.788.61.50

Verkoopsafdeling: [bitdefender@editions-profil.eu](mailto:bitdefender@editions-profil.eu)

Technische ondersteuning: <http://www.bitdefender.com/nl/Main/nousContacter/>

Website product: <http://www.bitdefender.com/nl>

## V.S.

### **Bitdefender, LLC**

PO Box 667588

Pompano Beach, Fl 33066

Telefoon (kantoor&verkoop): 1-954-776-6262

Verkoop: [sales@bitdefender.com](mailto:sales@bitdefender.com)

Technische ondersteuning: <http://www.bitdefender.com/help>

Web: <http://www.bitdefender.com>

## VK en Ierland

Genesis Centre Innovation Way

Stoke-on-Trent, Staffordshire

ST6 4BF

E-mail: [info@bitdefender.co.uk](mailto:info@bitdefender.co.uk)

Telefoon: +44 (0) 8451-305096

Verkoop: [sales@bitdefender.co.uk](mailto:sales@bitdefender.co.uk)

Technische ondersteuning: <http://www.bitdefender.com/help>

Web: <http://www.bitdefender.co.uk>

## Duitsland

### **Bitdefender GmbH**

Airport Office Center

Robert-Bosch-Straße 2

59439 Holzwickede

Deutschland

Kantoor: +49 2301 91 84 0

Verkoop: [vertrieb@bitdefender.de](mailto:vertrieb@bitdefender.de)

Technische ondersteuning: <http://kb.bitdefender.de>

Web: <http://www.bitdefender.de>

## Spanje

### **Bitdefender España, S.L.U.**



Avda. Diagonal, 357, 1<sup>o</sup> 1<sup>a</sup>

08037 Barcelona

Fax: +34 93 217 91 28

Telefoon: +34 902 19 07 65

Verkoop: [comercial@bitdefender.es](mailto:comercial@bitdefender.es)

Technische ondersteuning: <http://www.bitdefender.es/ayuda>

Website: <http://www.bitdefender.es>

## Roemenië

### **BITDEFENDER SRL**

West Gate Park, Building H2, 24 Preciziei Street

Bucharest

Fax: +40 21 2641799

Telefoon verkoop: +40 21 2063470

E-mail verkoop: [sales@bitdefender.ro](mailto:sales@bitdefender.ro)

Technische ondersteuning: <http://www.bitdefender.ro/suport>

Website: <http://www.bitdefender.ro>

## Verenigde Arabische Emiraten

### **Dubai Internet City**

Building 17, Office # 160

Dubai, UAE

Telefoon verkoop: 00971-4-4588935 / 00971-4-4589186

E-mail verkoop: [sales@bitdefender.com](mailto:sales@bitdefender.com)

Technische ondersteuning: <http://www.bitdefender.com/suport>

Website: <http://www.bitdefender.com/world>

## Woordenlijst

### **Achterdeur**

Een gat in de beveiliging van een systeem, dat opzettelijk werd achtergelaten door ontwikkelaars of beheerders. De motivatie voor dergelijke gaten is niet altijd boosaardig. Sommige besturingssystemen worden bijvoorbeeld geleverd met bevoegde accounts die bedoeld zijn voor gebruik door technici voor service ter plaatse of onderhoudsprogrammeurs van verkopers.

### **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.

### **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 bestandsextensies. Ze gebruiken doorgaans één tot drie letters (sommige betreuwenswaardige oude besturingssystemen ondersteunen niet meer dan drie letters). Voorbeelden hiervan zijn "c" voor C-broncode, "ps" voor PostScript, "txt" voor tekst zonder opmaak.

## **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. Beide zijn grafische browsers. Dit betekent dat ze zowel grafische beelden als tekst kunnen weergeven. Bovendien kunnen de meeste moderne browsers ook multimedia-informatie voorstellen met geluid en video, hoewel voor sommige formaten plug-ins vereist zijn.

## **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 vaak een bijzonder nauwkeurige omschrijving.

## **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 online-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.

## **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.

## **Heuristisch**

Een methode voor het identificeren van nieuwe virussen op basis van regels. Deze scanmethode steunt niet op specifieke virushandtekeningen. 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.

## **Ingepakte programma's**

Een bestand in een gecomprimeerd formaat. Talrijke besturingssystemen en toepassingen beschikken over opdrachten waarmee u bestanden kunt inpakken, zodat ze minder geheugen in beslag nemen. Veronderstel bijvoorbeeld dat u een tekstbestand hebt dat tien opeenvolgende spatietekens bevat. Normaal zou dit tien bytes opslagruimte vereisen.

Een programma dat bestanden inpakt zou echter de spatietekens vervangen door een speciaal spatiereeks-teken, gevolgd door het aantal spaties dat wordt vervangen. In dit geval zouden de tien spaties slechts twee bytes nodig hebben. Dit is slechts één inpaktechniek, maar er zijn er veel meer.

## **IP**

Internet Protocol - Een routeerbaar protocol in de TCP/OP-protocolreeks die verantwoordelijk is voor de IP-adressering, routing en de fragmentatie en defragmentatie van IP-pakketten.

## **Java-applet**

Een Java-programma dat is ontwikkeld om alleen op een webpagina te worden uitgevoerd. Om een applet op een webpagina te gebruiken, zou u de naam van het applet opgeven en de grootte (lengte en breedte in pixels) die het applet kan gebruiken. Wanneer de webpagina wordt geopend, downloadt de browser het applet van een server en voert hij het uit op de computer van de gebruiker (de client). Applets onderscheiden zich van toepassingen omdat ze worden beheerd door een streng beveiligingsprotocol.

Zelfs wanneer applets bijvoorbeeld op de client worden uitgevoerd, kunnen ze geen gegevens lezen van of schrijven naar de computer van de client. Bovendien worden applets verder beperkt zodat ze alleen gegevens kunnen lezen van en schrijven naar hetzelfde domein waarvan ze worden bediend.

## **Keylogger**

Een keylogger is een toepassing die alles wat u typt registreert.

Keyloggers zijn in wezen niet kwaadaardig. Ze kunnen worden gebruikt voor rechtmatige doeleinden, zoals het bewaken van de activiteiten van werknemers of kinderen. Ze worden echter steeds meer gebruikt door cybercriminele voor boosaardige doeleinden (bijv. voor het verzamelen van persoonlijke gegevens, zoals aanmeldingsgegevens en nummer van de sociale zekerheid).

## **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.

## **Niet-heuristisch**

Deze scanmethode steunt op specifieke virushandtekeningen. 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.

## **Opdrachtregel**

In een opdrachtregelinterface typt de gebruiker opdrachten in opdrachttaal rechtstreeks op het scherm in de ruimte die hiervoor wordt geboden.

## **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.

## **Opstartsector**

Een sector aan het begin van elke schijf die de architectuur van de schijf identificeert (sectorgrootte, clustergrootte, enz). Bij opstartdiskettes bevat de opstartsector ook een programma dat het besturingssysteem laadt.

## **Opstartsectorvirus**

Een virus dat de opstartsector van een vaste schijf of een diskette infecteert. Wanneer u probeert op te starten vanaf een diskette die geïnfecteerd is met een opstartsectorvirus, zal het virus actief worden in het geheugen. Wanneer u vanaf dat ogenblik uw systeem opstart, zal het virus telkens in het geheugen geactiveerd zijn.

## **Pad**

De exacte weg naar een bestand op een computer. Deze weg wordt doorgaans beschreven door middel van het hiërarchische archiveringssysteem vanaf het begin.

De route tussen twee willekeurige punten, zoals het communicatiekanaal tussen twee computers.

## **Phishing**

Het onder valse voorwendselen verzenden van een e-mail aan een gebruiker, waarbij de indruk wordt gewekt dat het bericht afkomstig is van een bestaande onderneming, in een poging de gebruiker persoonlijke gegevens te ontfutselen die zullen worden gebruikt voor identiteitsroof. In het e-mailbericht wordt de gebruiker doorverwezen naar een website waar persoonlijke gegevens kunnen worden bijgewerkt, zoals wachtwoorden en creditcard-, sofi- en bankrekeningnummers, die reeds in het bezit zijn van de rechtmatige organisatie. De website is echter nep en alleen opgezet om de gebruikersgegevens te stelen.

## **Polymorf virus**

Een virus dat zijn vorm wijzigt bij elk bestand dat hij infecteert. Aangezien ze geen consequent binair patroon hebben, zijn dergelijke virussen moeilijk te identificeren.

## **Poort**

Een interface op een computer waarop u een apparaat kunt aansluiten. PC's hebben verschillende types poorten. Intern zijn er verschillende poorten voorzien voor het aansluiten van schijfstations, beeldschermen en toetsenborden. Extern beschikken PC's over poorten voor het aansluiten van modems, printers, muizen en andere randapparatuur.

Bij TCP/IP- en UDP-netwerken, zijn ze een eindpunt voor een logische verbinding. Het poortnummer duidt aan over welk type poort het gaat. Poort 80 wordt bijvoorbeeld gebruikt voor HTTP-verkeer.

## Rapportbestand

Een bestand dat de acties weergeeft die zich hebben voorgedaan. Bitdefender houdt een rapportbestand bij met het gescande pad, het aantal gescande mappen, archieven en bestanden, en het aantal gevonden geïnfecteerde en verdachte bestanden.

## Rootkit

Een rootkit is een set softwarehulpprogramma's die toegang biedt tot een systeem op beheerniveau. Deze term werd voor het eerst gebruikt voor UNIX-besturingssystemen en verwees naar opnieuw gecompileerde hulpprogramma's die indringers beheerrechten verleende, zodat ze hun aanwezigheid konden verbergen zodat ze onzichtbaar bleven voor systeembeheerders.

De belangrijkste rol van rootkits is het verbergen van processen, bestanden, aanmeldingen en logboeken. Ze kunnen ook gegevens onderscheppen van terminals, netwerkverbindingen of randapparaten als ze de geschikte software bevatten.

Rootkits zijn in wezen niet kwaadaardig. Systemen en zelfs sommige toepassingen verbergen kritieke bestanden met de hulp van rootkits. Ze worden echter het vaakst gebruikt om malware of de aanwezigheid van een indringer op het systeem te verbergen. In combinatie met malware, vormen rootkits een ernstige bedreiging voor de integriteit en beveiliging van een systeem. Ze kunnen het verkeer controleren, achterpoortjes in het systeem maken, bestanden en logboeken wijzigen en detectie vermijden.

## 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).

## 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 reclaimedoeleinden. 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.

## **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.

## **Vals positief**

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

## **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. Een nog gevaarlijker type is een virus dat in staat is zichzelf te verzenden via netwerken en beveiligingssystemen te omzeilen.

## **Virushandtekening**

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.