

# Bitdefender<sup>®</sup> Mobile Security



HANDLEIDING



## Bitdefender Mobile Security Handleiding

Publication date 05/28/2018

Copyright© 2018 Bitdefender

### Kennisgevingen

**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 is alleen mogelijk als de bron van het citaat wordt vermeld. De inhoud mag op geen enkele manier worden gewijzigd.

**Waarschuwing en voorbehoud.** Dit product en de bijhorende documentatie zijn auteursrechtelijk beschermd. De informatie in dit document wordt geleverd "zoals hij is", zonder enige garantie. Dit document is met de grootste zorgvuldigheid samengesteld, maar de auteurs kunnen niet aansprakelijk worden gesteld door personen of organisaties voor eventuele verliezen of schade die (beweerdelijk) rechtstreeks of indirect zijn veroorzaakt door informatie in dit document.

Dit document bevat koppelingen naar externe websites die niet onder controle staan van Bitdefender. Bitdefender is niet verantwoordelijk voor de inhoud van dergelijke websites. Als u een externe website bezoekt die in dit document wordt genoemd, doet u dit geheel op eigen risico. Bitdefender vermeldt deze koppelingen uitsluitend bij wijze van dienstverlening. De vermelding van een koppeling betekent niet dat Bitdefender de inhoud van de externe website onderschrijft of hiervoor verantwoordelijkheid aanvaardt.

**Handelsmerken.** Dit document bevat mogelijk namen van handelsmerken. Alle geregistreerde en niet-geregistreerde handelsmerken in dit document zijn de exclusieve eigendom van hun respectievelijke eigenaars en worden nadrukkelijk gerespecteerd.



## Inhoudsopgave

|                               |    |
|-------------------------------|----|
| 1. Beschermingsfuncties ..... | 1  |
| 2. Aan de slag .....          | 2  |
| 3. Malwarescanner .....       | 7  |
| 4. Accountprivacy .....       | 10 |
| 5. Webbescherming .....       | 12 |
| 6. VPN .....                  | 14 |
| 7. Anti-Theft-functies .....  | 18 |
| 8. App Lock .....             | 24 |
| 9. Rapporten .....            | 29 |
| 10. WearON .....              | 30 |
| 11. Instellingen .....        | 31 |
| 12. Info .....                | 32 |
| 13. Bitdefender Central ..... | 33 |
| 14. Veelgestelde vragen ..... | 37 |
| 15. Hulp vragen .....         | 43 |



## 1. BESCHERMINGSFUNCTIES

Bitdefender Mobile Security beschermt uw Android-apparaat door middel van de volgende functies:

- Malwarescanner
- Accountprivacy
- Webbescherming
- VPN
- Anti-Theft, met:
  - Lokalisering op afstand
  - Apparaatvergrendeling op afstand
  - Gegevens wissen op afstand
  - Apparaatwaarschuwingen op afstand
- App Lock
- Rapporten
- WearON

U kunt gedurende 14 dagen gratis gebruikmaken van de functies van het product. Na afloop van deze periode dient u de volledige versie aan te schaffen voor blijvende bescherming van uw mobiele apparaat.



## 2. AAN DE SLAG

### Apparaatvereisten

Bitdefender Mobile Security werkt op alle apparaten met Android 4.0.3 of hoger. Voor bedreiging-scans via de cloud is een actieve internetverbinding nodig.

### Bitdefender Mobile Security installeren

#### ● Vanuit Bitdefender Central

##### ● Android

1. Ga naar <https://central.bitdefender.com>.
2. Aanmelden bij uw Bitdefender-account.
3. Tik linksboven in het venster op het pictogram  en selecteer vervolgens **Mijn apparaten**.
4. Tik op **LOKALE BESCHERMING INSTALLEREN**.
5. Selecteer **Bitdefender Mobile Security** in de lijst en tik op **Ga naar Google Play**.
6. Tik in het scherm van Google Play op **Installeren**.

##### ● Windows, macOS, iOS

1. Ga naar <https://central.bitdefender.com>.
2. Aanmelden bij uw Bitdefender-account.
3. Druk op de icoon  in de linkerbovenhoek van het scherm en klik dan op **Mijn Apparaten**.
4. Druk op **LOKALE BESCHERMING INSTALLEREN**.
5. Klik voor Windows en macOS op de link **Op een ander apparaat**.  
Tik op iOS op **Wilt u andere apparaten beschermen?**
6. Kies **Android**.
7. Selecteer **Bitdefender Mobile Security** uit de lijst en klik dan op **DOORGAAN**.



8. Voer een e-mailadres in het passende veld in en klik daarna op **VERZENDEN**.
9. Open uw e-mailaccount op uw Android-apparaat en tik op de knop **Kopen bij Google Play**.  
U wordt doorgestuurd naar de **Google Play**-app.
- 10 Tik in het scherm van Google Play op **Installeren**.

## ● Vanuit Google Play

Zoek naar Bitdefender Mobile Security om de app te vinden en te installeren.

Als alternatief kunt u de QR-code scannen:



Om de installatieprocedure te vervolledigen, dient u in te stemmen met de Abonnementsovereenkomst. Lees de Abonnementsovereenkomst grondig door: deze bevat de algemene voorwaarden voor uw gebruik van Bitdefender Mobile Security.

Tik op **VERDERGAAN** om verder te gaan naar het volgende venster.

## Log in op uw Bitdefender-account

Om Bitdefender Mobile Security te gebruiken, moet u uw apparaat aan een Bitdefender-, Facebook-, Google- of Microsoft-account koppelen door vanuit de app in te loggen op uw account. De eerste keer dat u de app opent, wordt u gevraagd in te loggen op een account.

Als u Bitdefender Mobile Security vanaf uw Bitdefender-account hebt geïnstalleerd, zal de app proberen om automatisch op deze account in te loggen.



Zo koppelt u uw apparaat aan een Bitdefender-account:

1. Open Bitdefender Mobile Security.
2. Geef in de overeenkomstige velden het e-mailadres en wachtwoord in van uw Bitdefender-account. Hebt u geen Bitdefender-account en wenst u er een aan te maken, klik op de daartoe bestemde link.
3. Tik op **Inloggen**.

Om in te loggen via een Facebook-, Google- of Microsoft-account, geeft u de dienst die u wilt gebruiken in bij **OF LOG IN MET**. U wordt doorgestuurd naar de inlogpagina van de gewenste dienst. Volg de instructies om uw account te linken met Bitdefender Mobile Security.



## 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.

## Bitdefender Mobile Security activeren

U moet Bitdefender Mobile Security activeren met behulp van een abonnement, dat aangeeft hoe lang u dit product mag gebruiken. Wanneer het abonnement verlopen is, zal de app niet meer werken en is uw apparaat niet langer beschermd.

Zo activeert u Bitdefender Mobile Security:

1. Open Bitdefender Mobile Security.
2. De app toont informatie over de huidige status van uw abonnement.  
Tik op **Ik heb een code**.
3. Typ een activeringscode in het desbetreffende veld en tik op **Activeren**.

Zo verlengt u uw huidige abonnement:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **Mijn account** uit de lijst.
3. Voer onder **Abonnement verlengen** een activeringscode in en tik op **Activeren**.

U kunt uw huidige abonnement ook verlengen door gebruik te maken van een van de aanbiedingen.



## Dashboard

Tik op het pictogram van Bitdefender Mobile Security in de App Drawer van uw apparaat, zodat de applicatie-interface wordt geopend.

Het Dashboard toont informatie over de beveiligingsstatus van uw apparaat en stelt u in staat alle beveiligingsfuncties gemakkelijk te beheren.

Als er een procedure actief is of als u actie moet ondernemen, wordt er in het Dashboard een kaart weergegeven met meer informatie en mogelijke acties.

Via de **Menu**-knop linksboven in het scherm kunt u de functies van Bitdefender Mobile Security gebruiken en van de ene sectie naar de andere navigeren:

### Malwarescanner

Hiermee kunt u zelf een scan starten en de optie Opslag scannen in- of uitschakelen. Zie "*Malwarescanner*" (p. 7) voor meer informatie.

### Accountprivacy

Controleer of er data gelekt werd in uw online accounts. Zie "*Accountprivacy*" (p. 10) voor meer informatie.

### Webbescherming

Hiermee kunt u de functie voor Webbescherming in- of uitschakelen. Zie "*Webbescherming*" (p. 12) voor meer informatie.

### VPN

Versleutelt internetcommunicatie, om uw privacy te verzekeren ongeacht welk netwerk u gebruikt. Zie "*VPN*" (p. 14) voor meer informatie.

### Anti-Theft

Hiermee kunt u de Anti-Theft-functies in- of uitschakelen en instellingen configureren. Zie "*Anti-Theft-functies*" (p. 18) voor meer informatie.

### App Lock

Hiermee kunt u de geïnstalleerde apps beveiligen door een pincode in te stellen. Zie "*App Lock*" (p. 24) voor meer informatie.

### Rapporten

Hier wordt een logboek bijgehouden van alle belangrijke acties, statuswijzigingen en andere kritieke berichten over de activiteiten op uw apparaat. Zie "*Rapporten*" (p. 29) voor meer informatie.



## **WearON**

Deze functie communiceert met uw smartwatch om uw telefoon terug te vinden als deze is zoekgeraakt. Zie "*WearON*" (p. 30) voor meer informatie.



## 3. MALWARESCANNER

Bitdefender beschermt uw apparaat en uw gegevens tegen schadelijke apps, door scans uit te voeren tijdens de installatie van nieuwe apps. U kunt ook handmatig een scan starten.



### Opmerking

Zorg dat uw mobiele apparaat verbonden is met internet. Als uw apparaat geen internetverbinding heeft, kan de scan niet worden gestart.

### ● Scannen bij installatie

Zodra u een nieuwe app installeert, wordt deze automatisch door Bitdefender Mobile Security gescand met behulp van cloud-technologie. Deze scanprocedure wordt herhaald wanneer u een update van de geïnstalleerde apps uitvoert.

Dit type scan wordt uitgevoerd via de Autopilot-functie. Autopilot is een intelligente scanner die alle geïnstalleerde of bijgewerkte apps scant en bedreigingen elimineert.

Als een geïnstalleerde app schadelijk blijkt te zijn, verschijnt er een waarschuwing met het advies de app te verwijderen. Tik dan op **Verwijderen** om naar het verwijderingsscherm voor de app te gaan.

### ● Scannen op aanvraag

Wanneer u wilt controleren of u alle apps op uw apparaat veilig kunt gebruiken, kunt u een scan op aanvraag uitvoeren.

Om een scan te starten, tikt u in de Malwarescanner-kaart van het Dashboard op de knop **Scan starten**.

In plaats hiervan kunt u ook op deze manier een scan starten:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **Malwarescanner** uit de lijst.
3. Tik op **Scan starten**.



### Opmerking

In Android 6 zijn extra machtigingen vereist voor de Malware Scanner-functie. Nadat u de knop **Scan starten** hebt ingedrukt, selecteert u **Toestaan** voor de volgende items:



- **Antivirus** toestaan om telefoongesprekken te starten en te beheren?
- **Antivirus** toegang geven tot foto's, media en bestanden op uw apparaat?

De voortgang van de scan wordt weergegeven. U kunt de scan op elk gewenst moment afbreken.



Malwarescan

Bitdefender Mobile Security scant normaal gesproken het interne geheugen van uw apparaat met inbegrip van een eventueel aanwezige SD-kaart (de "opslag"). Hierdoor worden ook schadelijke apps op de geheugenkaart opgespoord voordat ze schade kunnen aanrichten.

Zo kunt u Opslag scannen in- of uitschakelen:

1. Open Bitdefender Mobile Security.



2. Tik op de **Menu**-knop en selecteer **Malwarescanner** uit de lijst.
3. Tik op de bijbehorende schakelaar.

U kunt Opslag scannen ook vanuit **Instellingen** in- of uitschakelen door eerst op de knop  en daarna op de bijbehorende schakelaar te tikken.

Als er schadelijke apps worden aangetroffen, krijgt u hier bericht over. U kunt deze apps dan verwijderen via de knop **Verwijderen**.

De Malwarescanner-kaart geeft de status van uw apparaat weer. Zolang het apparaat veilig is, is de kaart groen. Wanneer er een scan moet worden uitgevoerd of als u actie moet ondernemen, wordt de kaart rood.



## 4. ACCOUNTPRIVACY

Bitdefender-accountprivacy gaat na of er data werd gelekt in de accounts die u gebruikt om online betalingen te verrichten, te winkelen of u aan te melden bij verschillende apps of websites. De data die in een account opgeslagen is, kan gaan om wachtwoorden, credit card-informatie of bankrekeninginformatie en, indien niet goed beveiligd, kan er sprake zijn van identiteitsdiefstal of inbreuk op privacy.

De privacystatus van een account wordt weergegeven na de validering.

Automatische nieuwe controles zijn geprogrammeerd om in de achtergrond uitgevoerd te worden, maar u kunt ook dagelijks manuele scans lanceren.

Telkens wanneer er nieuwe lekken werden ontdekt in verband met de gevalideerde e-mailaccounts, worden meldingen weergegeven.

Om vanaf nu persoonlijke informatie veilig te houden:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **Accountprivacy** uit de lijst.
3. Tik op de blauwe cirkel onderaan rechts op het scherm.
4. Typ uw e-mailadres in het daarvoor bestemde veld en tik daarna op **VOLGENDE**.

Bitdefender moet deze account valideren voordat persoonlijke informatie wordt weergegeven. Daarom werd een e-mailbericht met valideringscode verzonden naar het opgegeven e-mailadres.

5. Controleer uw Postvak IN en tik vervolgens de ontvangen code in het vakje **Accountprivacy** van uw app in. Indien u de bevestigingse-mail niet in uw Postvak IN vindt, controleer uw Ongewenste mail.

De privacystatus van de gevalideerde account wordt weergegeven.

Indien er in een van uw accounts worden gevonden, bevelen we u aan het wachtwoord zo snel mogelijk te wijzigen. Om een sterk en veilig wachtwoord te creëren, kunt u deze tips in gedachten houden:

- Zorg ervoor dat het minstens acht karakters lang is.
- Gebruik kleine letters en hoofdletters.
- Voeg ten minste een cijfer of symbool toe, zoals #, @, % of !.



Eens u een account die deel uitmaakte van een privacy-schending beveiligd hebt, kunt u de wijzigingen bevestigen door de geïdentificeerde lekken aan te duiden als **Opgelost**. Om dit te doen:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **Accountprivacy** uit de lijst.
3. Tik op de account die u net beveiligd hebt.
4. In het gebied **Lekken**, sleep naar links op de lek waarvoor u de account beveiligd hebt.
5. Tik op de icoon .
6. De kaart **Aanduiden als opgelost** verschijnt.

Tik op **BEVESTIGEN** om te bevestigen dat de account beveiligd is.

Wanneer alle gedetecteerde lekken aangeduid zijn als **Opgelost**, wordt de account niet langer gemarkeerd als gelekt, tot er een nieuw lek wordt ontdekt.



## 5. WEBBESCHERMING

Web Protection gebruikt de cloudservices van Bitdefender om de webpagina's te controleren die u bezoekt met de standaard Android-browser, Google Chrome, Firefox, Opera, Opera Mini en/of Dolphin. Een volledig overzicht van ondersteunde webbrowsers is te vinden in het gedeelte Web Protection.

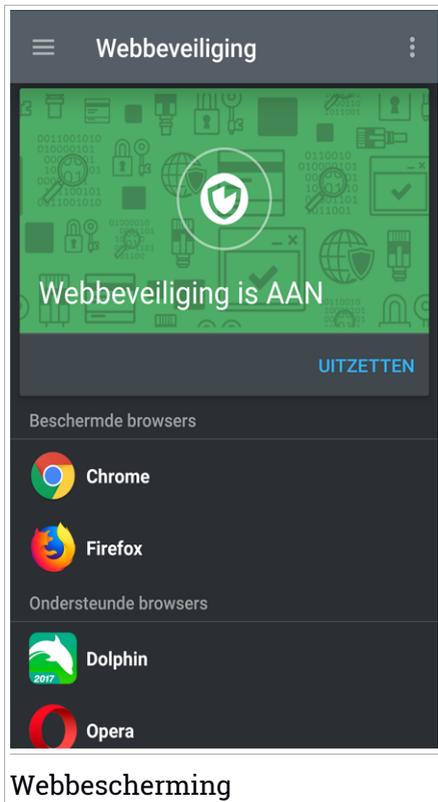
Als een URL verwijst naar een website waarvan bekend is dat deze spyware of virussen bevat of voor phishing of fraude wordt gebruikt, wordt de webpagina tijdelijk geblokkeerd en verschijnt er een waarschuwing.

U kunt dan zelf beslissen of u de webpagina toch wilt bezoeken of wilt terugkeren naar een veilige pagina.



### Opmerking

In Android 6 zijn extra machtigingen vereist voor de functie Webbeveiliging. Geef de functie toestemming om zich te registreren als een Toegankelijkheid-service en tik op **Aanzetten** wanneer hierom wordt gevraagd. Tik op **Antivirus** en zet de schakelaar aan. Bevestig vervolgens dat u toestemming geeft voor de toegang.





## 6. VPN

Met Bitdefender VPN houdt u uw data privé telkens u verbindt met onbeveiligde draadloze netwerken in luchthavens, winkelcentra, cafés of hotels. Zo vermijdt u onfortuinlijke situaties, bijvoorbeeld diefstal van persoonlijke gegevens of pogingen om het IP-adres van uw apparaat toegankelijk te maken voor hackers.

De VPN werkt zoals een tunnel tussen uw apparaat en het netwerk waarmee u verbindt: de VPN beveilgt die verbinding, door aan de hand van versleuteling volgens bankrichtlijnen de gegevens te versleutelen en door uw IP-adres te verbergen, waar u ook bent. Uw dataverkeer wordt omgeleid via een andere server, waardoor het praktisch onmogelijk wordt om uw apparaat te identificeren tussen de talloze andere toestellen die gebruikmaken van onze diensten. Wanneer u via Bitdefender VPN verbonden bent met het internet kunt u bovendien inhoud bekijken die normaal afgeschermd wordt in bepaalde gebieden.



### Opmerking

Bepaalde landen doen aan internetcensuur, waardoor het gebruik van VPN's op hun grondgebied bij wet verboden is. Om wettelijke gevolgen te vermijden, is het mogelijk dat er een waarschuwingsboodschap verschijnt wanneer u de Bitdefender VPN-functie voor het eerst probeert te gebruiken. Door deze functie te blijven gebruiken, bevestigt u dat u op de hoogte bent van de toepasselijke regels van dat land en van de risico's die u zou kunnen lopen.

Er zijn twee manieren om Bitdefender VPN in of uit te schakelen:

- Tik op de knop aan/uit in de VPN-kaart op het Dashboard.

De status van Bitdefender VPN wordt weergegeven.

- Tik op de **Menu**-knop en selecteer **VPN** uit de lijst.

Tik op **VERBINDEN** telkens u bescherming wenst wanneer u verbonden bent met een onbeveiligd draadloos netwerk.

Tik op **VERBREKEN** wanneer u de verbinding wilt verbreken.



### Opmerking

De eerste keer dat u VPN opstart, zal u worden gevraagd Bitdefender toe te laten een VPN verbinding op te zetten die het netwerkverkeer zal monitoren. Tik op **OK** om verder te gaan.





- Kies de server waarmee u wilt verbinden en bekijk hoelang uw abonnement nog geldig is - Info beschikbaar in de Premium VPN-versie.

## VPN Instellingen

Tik op de knop  in het menu van de VPN functie, selecteer vervolgens **Instellingen** voor de geavanceerde configuratie-opties van uw VPN.

In VPN **Instellingen** kunt u de volgende opties configureren:

- Snelle toegang VPN notificatie - u krijgt een notificatie in de statusbalk waarmee u VPN snel kunt inschakelen.
- Notificatie bij verbinding met een open Wi-Fi - u krijgt, in de statusbalk, een notificatie om VPN te gebruiken telkens u verbindt met een open Wi-Fi netwerk.
- Notificatie bij het bezoeken van een website voor internetbankieren - telkens u een website voor internetbankieren bezoekt, krijgt u in de statusbalk een notificatie om VPN te gebruiken.

## Abonnementen

Bitdefender VPN biedt dagelijks gratis 200 MB dataverkeer per apparaat om uw verbinding te beveiligen telkens u dit nodig hebt, en verbindt bovendien automatisch met de beste serverlocatie.

Upgrade naar de premium-versie voor onbeperkt dataverkeer en toegang tot afgeschermd inhoud overal ter wereld, doordat u de serverlocatie naar wens kunt selecteren.

U kunt op elk ogenblik upgraden naar de Bitdefender Premium VPN-versie door te tikken op de knop **PREMIUM VPN ACTIVEREN** die beschikbaar is het Dashboard of in het VPN-venster.

Het Bitdefender Premium VPN-abonnement is onafhankelijk van het abonnement voor Bitdefender Mobile Security: u kunt het dus gedurende de hele geldigheid ervan gebruiken, onafhankelijk van de status van het beschermingabonnement. Indien het Bitdefender Premium VPN-abonnement vervalt, maar als het abonnement voor Bitdefender Mobile Security nog actief is, gaat u terug naar de gratis versie.

Bitdefender VPN is een cross-platform product en is beschikbaar in de Bitdefender-producten die compatibel zijn met Windows, macOS, Android



en iOS. Eens u upgradet naar de premium-versie, kunt u uw abonnement op alle producten gebruiken, op voorwaarde dat u inlogt met dezelfde Bitdefender-account.



## 7. ANTI-THEFT-FUNCTIES

Bitdefender helpt u bij het terugvinden van uw apparaat en kan verhinderen dat uw gegevens in verkeerde handen vallen.

Hiervoor hoeft u alleen maar Anti-Theft te activeren op het apparaat. Als het nodig blijkt te zijn, kunt u vervolgens vanuit elke webbrowser toegang krijgen tot **Bitdefender Central**.

Zelfs als u geen internettoegang hebt, kunt u uw apparaat en uw gegevens beschermen door vanaf een mobiele telefoon **sms-opdrachten** naar uw apparaat te sturen.

Bitdefender Mobile Security biedt de volgende Anti-Theft-functies:

### Lokalisering op afstand

Bekijk de huidige locatie van uw apparaat in Google Maps. De locatie wordt elke 5 seconden vernieuwt, dus u kunt deze volgen indien hij in beweging is.

De nauwkeurigheid van de locatie hangt af van hoe Bitdefender deze kan bepalen:

- Als de GPS is ingeschakeld op het apparaat, kan de locatie worden bepaald tot op enkele meters, zolang deze binnen bereik van GPS-satellieten is (dus niet in een gebouw).
- Indien het apparaat binnenshuis is, kan de locatie worden bepaald tot binnen tientallen meters als Wi-Fi is ingeschakeld en er beschikbare draadloze netwerken in de omtrek zijn.
- Anders wordt de locatie bepaald met gebruikmaking van alleen gegevens van het mobiele netwerk, dat geen betere nauwkeurigheid dan enkele honderden meters kan bieden.

### IP tonen

Toont het laatste IP-adres van het geselecteerde apparaat. Tik op **IP tonen** om deze informatie zichtbaar te maken.

### Wissen op afstand

U kunt alle persoonlijke gegevens op uw apparaat op afstand wissen als het apparaat niet langer in uw bezit is.

### Vergrendelen op afstand

Vergrendel het scherm van uw apparaat en stel een numerieke pincode in, die moet worden ingevoerd om het scherm te ontgrendelen.



## Waarschuwing naar apparaat sturen (Scream-functie)

U kunt op afstand een bericht op het scherm van het apparaat laten weergeven, of een luid geluidssignaal laten afspelen via de luidspreker van het apparaat.

Als het apparaat is zoekgeraakt, kunt u een bericht op het scherm van het apparaat weergeven, zodat de eerlijke vinder weet hoe hij of zij u kan bereiken.

En als u het apparaat niet kunt vinden, terwijl het misschien vlakbij is (bijvoorbeeld ergens in huis of op kantoor), kunt u een luid geluidssignaal laten klinken via de Scream-functie. Dit werkt ook als het apparaat in de stille modus staat.

## Anti-Theft activeren

Om de Anti-Theft-functies te activeren, voltooit u de configuratieprocedure vanaf de Anti-Theft-kaart in het Dashboard.

In plaats hiervan kunt u Anti-Theft ook op deze manier activeren:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **Anti-Theft** uit de lijst.
3. Tik op **Aanzetten**.
4. U kunt deze functie nu als volgt activeren:



### Opmerking

In Android 6 zijn extra machtigingen vereist voor de functie Anti-Theft. Voer de onderstaande stappen uit om deze functie in te schakelen:

- Tik op **Anti-Theft activeren** en tik vervolgens op **Aanzetten**.
- Ken de volgende machtigingen toe:
  - a. **Antivirus** toestaan om sms-berichten te sturen en te bekijken?
  - b. **Antivirus** toegang geven tot de locatie van dit apparaat?
  - c. **Antivirus** toegang geven tot uw contacten?

### a. Beheerdersmachtigingen toekennen

Deze bevoegdheden zijn absoluut noodzakelijk om de Anti-Theft-module te kunnen gebruiken. U moet daarom beheerdersbevoegdheden toekennen voordat u verder kunt gaan.



## b. Applicatie-pincode instellen

Om er zeker van te zijn dat wijzigingen in de instellingen van Anti-Theft door u zijn geautoriseerd, moet u een pincode instellen. Bij elke poging de instellingen van Anti-Theft te wijzigen, moet eerst deze pincode worden ingevoerd. Op apparaten met ondersteuning voor vingerafdrukherkenning kan ook een vingerafdrukscan worden gebruikt in plaats van de ingestelde pincode.



### Opmerking

Dezelfde pincode wordt ook door App Lock gebruikt om uw geïnstalleerde apps te beschermen.

## c. Snapshot activeren

Telkens wanneer iemand probeert uw geïnstalleerde applicaties te gebruiken terwijl de optie Snapshot ingeschakeld is, maakt Bitdefender een foto van deze persoon. Zie "[Snapshot](#)" (p. 26) voor meer informatie over deze functie.

## d. Vertrouwd nummer instellen voor Anti-Theft

Selecteer het tabblad **Sms-beheer**, type een vertrouwd telefoonnummer of selecteer een telefoonnummer uit de lijst, en tik op **Nummer opslaan**. Het vertrouwde telefoonnummer moet ook een landcode bevatten, en kan het nummer zijn van iemand die u kent of van een andere telefoon die u gebruikt.

Wanneer een andere simkaart in uw apparaat wordt geplaatst, stuurt Bitdefender Mobile Security automatisch een sms-bericht met informatie over het telefoonnummer van de nieuwe simkaart. Dit sms-bericht wordt verzonden naar het door u van tevoren ingestelde 'vertrouwde nummer'.

Op deze manier kunt u nog steeds sms-opdrachten naar uw telefoon sturen, ook als de simkaart is vervangen en de telefoon een nieuw nummer heeft.



### Belangrijk

Dit is geen verplichte stap, maar het is wel aan te raden om tijdens de eerste configuratie een vertrouwd nummer in te stellen. De opdracht voor wissen op afstand werkt alleen wanneer deze wordt verzonden vanaf het ingestelde vertrouwde nummer.



Nadat Anti-Theft is geactiveerd, kunt u de functies Webbeheer en Sms-beheer afzonderlijk in- of uitschakelen met behulp van de desbetreffende knoppen in het Anti-Theft-scherm.

## Webbeheer: Anti-Theft-functies gebruiken vanuit Bitdefender Central



### Opmerking

Voor alle Anti-Theft-functies is het noodzakelijk dat de optie **Achtergrondgegevens** bij de gegevensgebruik-instellingen van uw apparaat is ingeschakeld.

Zo opent u de Anti-Theft-functies vanuit uw Bitdefender-account:

1. Ga naar **Bitdefender Central**.
2. Tik linksboven in het venster op het pictogram  en selecteer vervolgens **Mijn apparaten**.
3. Selecteer de gewenste apparaatkaart in het venster **Mijn apparaten**.
4. Selecteer het tabblad **Anti-Theft**.
5. Tik in het onderste veld van het venster op het pictogram  en tik vervolgens op de knop voor de functie die u wilt gebruiken:

**Lokaliseren** - geef de lokatie van uw apparaat weer op Google Maps.



**Waarschuwing** - typ een bericht om op het scherm van uw apparaat te laten weergegeven en/of laat het apparaat een geluidssignaal afspelen.



**Vergrendelen** - vergrendel uw apparaat en stel een pincode in die moet worden ingevoerd voordat het apparaat kan worden ontgrendeld.



**Wissen** - wis alle gegevens van uw apparaat.



### Belangrijk

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

**IP tonen** - geeft het laatste IP-adres voor het geselecteerde apparaat weer.



## Sms-beheer: Anti-Theft-functies gebruiken via sms-opdrachten

Als sms-opdrachten zijn ingeschakeld, kunt u vanaf elke gewenste mobiele telefoon sms-berichten met de volgende opdrachten naar uw smartphone sturen:

- **LOCATE** - stuur een bericht met informatie over de locatie van het apparaat naar het telefoonnummer waarvandaan deze sms-opdracht is verzonden. Het bericht bevat een Google Maps-link, die kan worden geopend in de browser van de mobiele telefoon.
- **SCREAM** - speel een luid geluidssignaal af via de luidspreker van het apparaat.
- **LOCK** - vergrendel het scherm van het apparaat met de door u ingestelde pincode.
- **WIPE** - wis alle gegevens op het apparaat.



### Belangrijk

Deze opdracht werkt alleen als deze is verzonden vanaf het van tevoren ingestelde vertrouwde nummer.

- **CALLME** - bel het telefoonnummer waarvandaan deze sms-opdracht is verzonden, met de luidspreker ingeschakeld. Op deze manier kunt u meeluisteren met de persoon die uw telefoon in handen heeft.
- **HELP** - stuur een bericht met een overzicht van alle beschikbare opdrachten naar het telefoonnummer waarvandaan deze sms-opdracht is verzonden.
- **SIM Change** - het vertrouwde nummer ontvangt een sms-bericht met het nieuwe telefoonnummer, zodra uw simkaart wordt vervangen door een andere. Om het telefoonnummer van uw vriend of kennis in te stellen, tikt u op **Vertrouwd nummer**. Typ het telefoonnummer inclusief de landcode, of kies de desbetreffende kaart uit de contactenlijst.

Alle sms-opdrachten moeten in deze vorm worden ingevoerd:

`bd-<pincode> <opdracht>`



### Opmerking

De spitse haakjes dienen alleen om een variabele aan te geven en moeten zelf niet worden ingevoerd.



Een voorbeeld: als de pincode is ingesteld op 368711 en u een bericht wilt ontvangen met informatie over de locatie van uw telefoon, stuurt u deze sms-opdracht naar het telefoonnummer van uw telefoon:

**BD-123456 LOCATE**



## 8. APP LOCK

Bepaalde apps, bijvoorbeeld voor e-mail, foto's of berichten, bevatten persoonlijke informatie die u waarschijnlijk graag privé wilt houden. U kunt deze informatie beschermen door de toegang tot deze apps te beperken.

Via App Lock kunt u apps beveiligen met een speciale pincode, zodat onbevoegden deze apps niet meer kunnen gebruiken. U moet hiervoor een pincode van minimaal 4 en maximaal 8 cijfers instellen. Elke keer dat u een van de beveiligde apps wilt gebruiken, moet u deze pincode invoeren.

Op apparaten met ondersteuning voor vingerafdrukherkenning kan ook een vingerafdrukscan worden gebruikt in plaats van de ingestelde pincode.

### App Lock activeren

Om de toegang tot bepaalde apps te beperken, configureert u App Lock vanaf de kaart die in het Dashboard wordt weergegeven nadat Anti-Theft is geactiveerd.

In plaats hiervan kunt u App Lock ook op deze manier activeren:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **App Lock** uit de lijst.
3. Tik op **Aanzetten** en geef Bitdefender toegang tot de gebruiksgegevens door het desbetreffende selectievakje in te schakelen.



#### Opmerking

In Android 6 zijn extra machtigingen vereist voor de functie Snapshot. Om deze functie in te schakelen, moet u **Antivirus** toestemming geven om foto's te maken en video's op te nemen.

4. Ga terug naar de app, configureer de toegangscode en tik op **Pincode instellen**.



#### Opmerking

Deze stap is alleen beschikbaar als u nog geen pincode voor Anti-Theft hebt ingesteld.

5. Gebruik de optie Snapshot om indringers te betrappen die proberen toegang te krijgen tot uw persoonlijke gegevens.



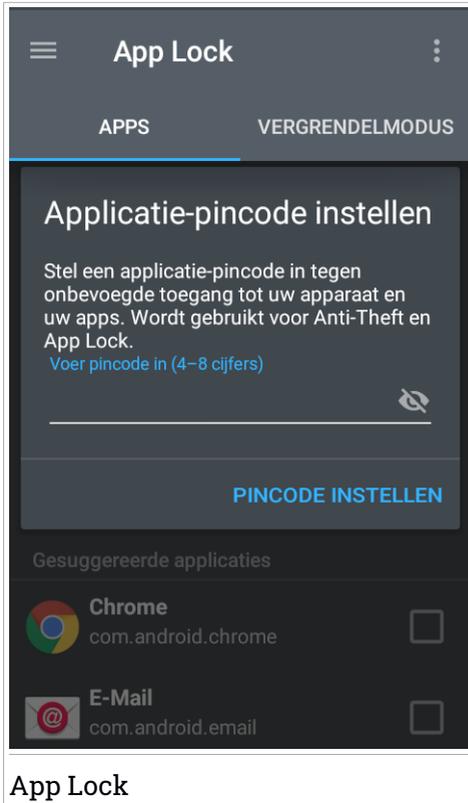
6. Selecteer welke toepassingen u wilt beschermen.

Als vijf keer achter elkaar een verkeerde pincode of vingerafdruk wordt gebruikt, wordt een time-out van 30 seconden gestart. Hierdoor wordt het vrijwel onmogelijk om in de beveiligde apps in te breken.



## Opmerking

Dezelfde pincode wordt ook door Anti-Theft gebruikt.



## Vergrendelmodus

Hier kunt u instellen wanneer de App Lock-functie de applicaties op uw apparaat moet beveiligen.

U kunt kiezen uit deze opties:



- **Telkens vergrendelen** - de door u geconfigureerde pincode of vingerafdruk moet bij elk gebruik van de beveiligde apps worden gebruikt.
- **Ontgrendelen tot scherm uit** - de apps zijn toegankelijk totdat het scherm wordt uitgeschakeld.
- **Korte onderbreking toestaan** - u kunt een ontgrendelde app verlaten en binnen 30 seconden weer activeren.
- **Smart Unlock activeren** - als deze optie is ingeschakeld en er verbinding is met een netwerk dat als vertrouwd is ingesteld, zijn de overige opties niet beschikbaar. Bevestiging met een pincode of vingerafdruk is dan niet nodig om toegang te krijgen tot de apps.

## App Lock-instellingen

Tik op de knop  in het App Lock-menu en selecteer **Instellingen** om geavanceerde configuratieopties voor App Lock weer te geven.

Met de **App Lock-instellingen** kunt u het volgende doen:

- Een snapshot laten maken na drie mislukte pogingen om de pincode in te voeren.
- Vergrendelingsberichten voor nieuw geïnstalleerde apps.
- Uw pincode wijzigen.

## Snapshot

Met Bitdefender Snapshot kunt u uw vrienden of familie op heterdaad betrappen. Zo kunt u hen een lesje leren, zodat ze niet langer nieuwsgierig uw persoonlijke bestanden doorlopen of de apps bekijken die u gebruikt.

Deze functie werkt heel eenvoudig: telkens wanneer de pincode of vingerafdruk drie keer achter elkaar verkeerd wordt ingevoerd, wordt er een foto gemaakt met de camera aan de voorkant. Deze foto wordt samen met het tijdstempel en de reden opgeslagen. U kunt deze informatie opvragen via de App Lock-functie van Bitdefender Mobile Security.



### Opmerking

Deze functie is alleen beschikbaar op apparaten die aan de voorkant beschikken over een camera.



Zo configureert u de Snapshot-functie:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **App Lock** uit de lijst.
3. Tik op de knop  in het App Lock-menu en selecteer **Instellingen**.
4. Activeer de schakelaar **Snapshot maken na 3 mislukte pincodepogingen**.

De foto's die tijdens het invoeren van een incorrecte pincode worden gemaakt, worden in het App Lock-menu weergegeven en kunnen in het volledige scherm worden bekeken.

U kunt de foto's ook bekijken in uw Bitdefender-account:

1. Ga naar <https://central.bitdefender.com>.
2. Inloggen op uw account.
3. Tik linksboven in het venster op het pictogram  en selecteer vervolgens **Mijn apparaten**.
4. Selecteer uw apparaat in het venster **Mijn apparaten** en selecteer vervolgens het tabblad **Anti-Theft**.

De foto's worden weergegeven.

Alleen de 3 meest recente foto's worden opgeslagen.

## Smart Unlock

Met Smart Unlock kunt u heel eenvoudig voorkomen dat u elke keer een pincode of vingerafdrukscan nodig hebt voor de beveiligde apps.

U kunt bepaalde Wi-Fi-netwerken als 'vertrouwd' aanmerken, zodat de App Lock-blokkeringsinstellingen worden uitgeschakeld zolang u via een van deze netwerken verbonden bent met internet.

Zo activeert u de functie Smart Unlock:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **App Lock** uit de lijst.
3. Open het tabblad **Vergrendelmodus** en kies de gewenste optie.

Het draadloze netwerk waarmee u verbonden bent, wordt weergegeven.



Als u het momenteel gebruikte Wi-Fi-netwerk als vertrouwd netwerk wilt aanmerken, tikt u op het pictogram .



## Opmerking

Deze instelling is alleen beschikbaar indien Smart Unlock is ingeschakeld.

Als u later van mening verandert, kunt u de functie weer uitschakelen. De vertrouwde Wi-Fi-netwerken worden dan niet langer vertrouwd.



## 9. RAPPORTEN

De Rapporten-functie houdt een uitgebreid logboek bij van gebeurtenissen met betrekking tot de scanactiviteiten op uw apparaat.

Elke keer dat er iets gebeurt dat van belang is voor de beveiliging van het apparaat, wordt een nieuw bericht toegevoegd aan de rapporten.

Zo opent u de Rapporten:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **Rapporten** uit de lijst.

Het venster Rapporten bevat de volgende tabbladen:

- **Weekrapporten** - hier kunt u de beveiligingsstatus en de uitgevoerde taken van de huidige en de vorige week bekijken. Elke zondag wordt het rapport van de afgelopen week gegenereerd. U krijgt bericht wanneer het weekrapport beschikbaar is.

Elke week wordt hier een nieuwe tip weergegeven, dus kom hier regelmatig terug om uw app zo goed mogelijk te leren gebruiken.

- **Activiteitenlogboek** - hier kunt u gedetailleerde informatie bekijken over de activiteiten van uw Bitdefender Mobile Security-app vanaf het moment van installatie op uw Android-apparaat.

Om het huidige activiteitenlogboek te wissen, tikt u rechtsboven in het scherm op  en vervolgens selecteert u **Activiteitenlogboek wissen**.



## 10. WEARON

Met Bitdefender WearON kunt u uw smartphone heel gemakkelijk terugvinden als u deze bent kwijtgeraakt, bijvoorbeeld op kantoor of thuis. Deze functie werkt ook als de stille modus van de telefoon actief is.

Zorg dat deze functie altijd ingeschakeld is, zodat u uw smartphone zo nodig gemakkelijk kunt terugvinden.



### Opmerking

Deze functie werkt met Android 4.3 en Android Wear.

## WearON activeren

Om WearON te gebruiken, koppelt u uw smartwatch aan Bitdefender Mobile Security en activeert u de WearON-functie met deze spraakopdracht:

**Start:**<Where is my phone>

**Bitdefender WearON** ondersteunt twee opdrachten:

### 1. Phone Alert

De functie Phone Alert waarschuwt u als u te ver van uw smartphone verwijderd bent.

Wanneer u uw smartwatch bij u hebt, detecteert deze automatisch de app op uw telefoon. Uw smartwatch gaat trillen wanneer u meer dan tien meter van de telefoon verwijderd bent.

U kunt deze functie als volgt inschakelen: open Bitdefender Mobile Security, tik in het menu op **Algemene instellingen** en activeer de schakelaar in het gedeelte WearON.

### 2. Scream

Als uw telefoon toch is zoekgeraakt, kunt u vanaf uw smartwatch een Scream-opdracht naar de telefoon sturen om een luid geluidssignaal op de telefoon te laten klinken.



## 11. INSTELLINGEN

Onder Instellingen kunt u de volgende opties wijzigen:

- **Pincode Beveiliging** - u kunt de pincode wijzigen die u hebt ingesteld om toepassingen of Antidiefstal-opdrachten te ontgrendelen.
- **Malware-scanner** - u kunt beslissen of de opslag moet worden gescand.
- **In-de-cloud-detectie** - u kunt beslissen of u ons rapporten stuurt die ons kunnen helpen de cloud-detectie te verbeteren.
- **Accountprivacy** - u kunt beslissen of u op de hoogte wilt blijven wanneer uw accounts niet betrokken zijn in lekken.
- **App Lock** - u kunt beslissen of u notificaties voor nieuwe toepassingen vergrendelt.
- **Snapshot** - u kunt beslissen of er een schermafdruck moet worden genomen na drie mislukte pogingen om uw toepassingen te gebruiken.
- **Antidiefstal** - u kunt het nummer dat u ingesteld hebt als vertrouwd, wijzigen, voor het geval uw toestel in vreemde handen valt.
- **Rapporten** - u kunt beslissen of u notificaties voor rapporten ontvangt.
- **Anonieme rapporten sturen** - u kunt beslissen of u ons rapporten stuurt met informatie over hoe u het product gebruikt. Deze informatie is essentieel voor productverbeteringen en helpt ons een betere ervaring aan te bieden in de toekomst.



## 12. INFO

Om informatie te vinden over de Bitdefender Mobile Security-versie die u hebt geïnstalleerd, gaat u naar **Over**. Daar kunt u ons ook contacteren voor ondersteuning en vindt u de Abonnementsovereenkomst, het Privacybeleid en de Open source-licenties.



## 13. BITDEFENDER CENTRAL

Bitdefender Central is een webplatform dat u toegang geeft tot de online functies en services van het product. Vanuit dit platform kunt u op afstand belangrijke handelingen uitvoeren op de apparaten waarop Bitdefender is geïnstalleerd. U kunt vanaf elke computer en elk mobiel apparaat met een internetverbinding inloggen op uw Bitdefender-account door naar <https://central.bitdefender.com> te gaan. Wanneer u bent ingelogd, kunt u het volgende doen:

- Bitdefender downloaden en installeren op besturingssystemen Windows, macOS, iOS en Android. De producten die beschikbaar zijn om te downloaden, zijn:
  - Bitdefender Mobile Security
  - Bitdefender Mobile Security voor iOS
  - Bitdefender Antivirus voor Mac
  - De Bitdefender-productlijn voor Windows
- Uw Bitdefender-abonnementen beheren en vernieuwen.
- Nieuwe apparaten aan uw netwerk toevoegen en deze apparaten beheren, waar u op dat moment ook bent.

## Inloggen op uw Bitdefender-account

Zo kunt u op uw Bitdefender-account inloggen:

1. Open een webbrowser op een computer of mobiel apparaat met internettoegang.
2. Ga naar <https://central.bitdefender.com>.
3. Log in op uw account met uw e-mailadres en wachtwoord.

## Mijn apparaten

Vanaf het paneel **Mijn apparaten** van uw Bitdefender-account kunt u uw Bitdefender-product installeren, beheren en op afstand gebruiken op al uw apparaten die zijn ingeschakeld en verbinding hebben met het internet. De apparaatkaarten geven de naam en de beveiligingsstatus van het apparaat weer en geven weer of er beveiligingsrisico's zijn die de bescherming van uw apparaten beïnvloeden.



Om uw apparaten beter te kunnen herkennen, kunt u de apparaatnaam aanpassen:

1. Ga naar **Bitdefender Central**.
2. Tik linksboven in het venster op het pictogram  en selecteer vervolgens **Mijn apparaten**.
3. Tik op de gewenste apparaatkaart en vervolgens op de icoon  in de rechterbovenhoek van het scherm.
4. Selecteer **Instellingen**.
5. Voer een nieuwe naam in het veld **Naam Apparaat** in en selecteer **OPSLAAN**.

Om het beheer van uw apparaten te vereenvoudigen, kunt u eigenaren instellen en aan de apparaten toewijzen:

1. Ga naar **Bitdefender Central**.
2. Tik linksboven in het venster op het pictogram  en selecteer vervolgens **Mijn apparaten**.
3. Tik op de gewenste apparaatkaart en vervolgens op de icoon  in de rechterbovenhoek van het scherm.
4. Selecteer **Profiel**.
5. Tik op **Eigenaar toevoegen**, vul de bijbehorende velden in, stel het geslacht en de geboortedatum in en voeg eventueel een profielafbeelding toe.
6. Tik op **Toevoegen** om het profiel op te slaan.
7. Selecteer de gewenste eigenaar uit de lijst **Apparaateigenaar** en tik op **Toewijzen**.

Voor meer bewerkingen op afstand en voor meer informatie over uw Bitdefender-product op een specifiek apparaat, selecteert u de desbetreffende apparaatkaart.

Wanneer u een apparaatkaart selecteert, komen de volgende tabbladen beschikbaar:

- **Dashboard**. In dit venster kunt u de gegevens van het geselecteerde apparaat bekijken, de beschermingsstatus en de Bitdefender VPN-status controleren en nakijken hoeveel bedreigingen de voorbije zeven dagen werden geblokkeerd. De beschermingsstatus is altijd groen (dan zijn er



geen problemen voor uw apparaat), geel (dan moet u het apparaat controleren) of rood (dan loopt uw apparaat een risico). Wanneer er problemen zijn met uw apparaat, tik dan op het uitklappijtje in het bovenste statusgebied voor meer details. Hier kunt u de problemen die de beveiliging van uw apparaat beïnvloeden handmatig herstellen.

- **Bescherming.** In dit tabblad kunt u op afstand een scan uitvoeren op uw apparaat. Tik op de knop **Scan** om de scan te starten. U kunt ook zien wanneer de laatste scan op het apparaat is uitgevoerd en er is een rapport beschikbaar met de belangrijkste gegevens van de laatste scan.
- **Anti-Theft.** Als uw apparaat is zoekgeraakt of gestolen, kunt u het met de Anti-Theft-functie terugvinden en op afstand opdrachten uitvoeren. Tik op **Lokaliseren** om de locatie van het apparaat te achterhalen. Er wordt dan informatie weergegeven over de laatst bekende locatie van het apparaat, samen met de datum en de tijd. Zie "**Anti-Theft-functies**" (p. 18) voor meer informatie over deze functie.

## Mijn abonnementen

Via Bitdefender Central beheert u heel eenvoudig de abonnementen die u voor uw apparaten hebt aangeschaft.

## Controleer beschikbare abonnementen

Om uw beschikbare abonnementen te controleren:

1. Ga naar **Bitdefender Central**.
2. Tik linksboven in het venster op het symbool  en selecteer vervolgens **Mijn abonnementen**.

Hier hebt u informatie over de beschikbaarheid van de abonnementen die u hebt en het aantal toestellen dat elk daarvan gebruikt.

U kunt een nieuw toestel aan een abonnement toevoegen of het vernieuwen door een abonnementenkaart te selecteren.

## Een nieuw toestel toevoegen

Als uw abonnement voor meerdere apparaten geldt, kunt u een nieuw apparaat toevoegen en uw versie van Bitdefender Mobile Security op dit apparaat installeren, zoals wordt beschreven in "**Bitdefender Mobile Security installeren**" (p. 2).



## Abonnement verlengen

Als uw abonnement nog minder dan 30 dagen geldig is en u niet voor automatische verlenging hebt gekozen, kunt u het abonnement als volgt handmatig verlengen:

1. Ga naar **Bitdefender Central**.
2. Tik linksboven in het venster op het symbool  en selecteer vervolgens **Mijn abonnementen**.
3. Selecteer de gewenste abonnementenkaart.
4. Klik op **Verlengen** om door te gaan.

In uw webbrowser wordt een webpagina geopend waar u uw Bitdefender-abonnement kunt verlengen.



## 14. VEELGESTELDE VRAGEN

### Waarom heeft Bitdefender Mobile Security een internetverbinding nodig?

De applicatie moet met Bitdefender-servers communiceren om te kunnen bepalen of de geïnstalleerde applicaties en de bezochte webpagina's wel veilig zijn, en ook om opdrachten vanaf uw Bitdefender-account te kunnen ontvangen wanneer u de Anti-Theft-functies gebruikt.

### Waarom heeft Bitdefender Mobile Security deze bevoegdheden nodig?

- Internettoegang -> nodig voor communicatie met de cloud.
- Telefoonstatus en -identiteit lezen -> wordt gebruikt om te bepalen of het apparaat verbonden is met internet en om bepaalde apparaatinformatie op te vragen, waarmee een unieke ID kan worden samengesteld voor de communicatie met de Bitdefender-cloud.
- Browserfavorieten lezen en schrijven -> de module Webbeveiliging verwijdert schadelijke websites uit uw browsergeschiedenis.
- Loggegevens lezen -> Bitdefender Mobile Security detecteert sporen van bedreigingsactiviteiten in de Android-logboeken.
- Sms, contacten, accountgegevens en externe opslag lezen en schrijven -> nodig om op afstand gegevens te kunnen wissen.
- Locatie -> nodig voor lokalisatie op afstand.
- Camera -> nodig voor Snapshot.
- Opslag -> nodig om de Malwarescanner ook de SD-kaart te laten scannen.

### Waar zie ik de details over de activiteit van de toepassing?

Bitdefender Mobile Security houdt een logboek bij van alle belangrijke acties, statuswijzigingen en andere kritieke berichten over de activiteiten van de applicatie. Om deze informatie weer te geven, opent u Bitdefender Mobile Security, tikt u op de **Menu**-knop en selecteert u **Rapporten** uit de lijst.

### Ik ben de pincode vergeten waarmee ik mijn app heb beveiligd. Wat moet ik doen?

1. Ga naar **Bitdefender Central**.
2. Tik linksboven in het venster op het pictogram  en selecteer vervolgens **Mijn apparaten**.



3. Tik op de gewenste apparaatkaart en vervolgens op de icoon  in de rechterbovenhoek van het scherm.
4. Selecteer **Instellingen**.
5. De pincode wordt weergegeven in het veld **Applicatiepincode**.

## **Welk effect heeft Bitdefender Mobile Security op de prestaties en de batterij van mijn apparaat?**

We houden de impact heel laag. De toepassing wordt enkel uitgevoerd wanneer dit van essentieel belang is - nadat u een toepassing installeert, wanneer u de interface van de toepassing gebruikt of wanneer u een beveiligingscontrole wenst. Bitdefender Mobile Security is niet op de achtergrond actief wanneer u telefoongesprekken voert, een sms-bericht invoert of een spel speelt.

## **Hoe kan ik App Lock uitzetten?**

U kunt de App Lock-functie als zodanig niet uitzetten, maar u kunt de functie wel heel eenvoudig uitschakelen door de selectievakjes naast alle geselecteerde apps leeg te maken. (Hiervoor hebt u uw pincode of vingerafdruk nodig.)

## **Hoe kan ik een ander draadloos netwerk instellen als vertrouwd netwerk?**

Als u een ander draadloos netwerk als vertrouwd wilt instellen:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **App Lock** uit de lijst.
3. Open het tabblad **Vergrendelmodus** en selecteer het pictogram .
4. Gebruik uw pincode of vingerafdruk om de actie te bevestigen.
5. Tik op het pictogram  naast het netwerk dat u als vertrouwd wilt instellen.

## **Hoe kan ik de snapshots die op mijn apparaten genomen zijn, niet meer zien?**

Om de op uw apparaten gemaakte fotosnaps niet langer zichtbaar te maken:

1. Ga naar **Bitdefender Central**.
2. Tik rechtsboven op het scherm op de icoon .
3. Tik op **Mijn Account** in het schuifmenu.



4. Selecteer het tabblad **Instellingen**.
5. Deactiveer de optie **Snapshots die met uw toestellen zijn gemaakt, tonen/niet tonen**.

## **Hoe kan ik veilig online blijven winkelen?**

Online winkelen gaat gepaard met hoge risico's als u enkele details over het hoofd ziet. Om niet het slachtoffer te worden van fraude, bevelen wij u het volgende aan:

- Houd uw beveiligingsapp up to date.
- Voer enkel online betalingen met kopersbescherming uit.
- Gebruik een VPN wanneer u een verbinding maakt met het internet via openbare en onbeveiligde draadloze netwerken.
- Wees aandachtig voor de wachtwoorden die u hebt toegekend aan uw online accounts. Ze moeten sterk zijn, met hoofdletters en kleine letters, cijfers en symbolen (@, !, %, #, etc.).
- Zorg ervoor dat de informatie die u verzendt, via veilige verbindingen gaat. De online website-extensies moet HTTPS://, zijn, niet HTTP://.

## **Wanneer moet ik Bitdefender VPN gebruiken?**

U dient voorzichtig te zijn wanneer u inhoud van het internet bekijkt, downloadt of uploadt. Om ervoor te zorgen dat u beveiligd bent wanneer u surft op het internet, raden we aan dat u Bitdefender VPN gebruikt wanneer u:

- wilt verbinden met publieke draadloze netwerken
- inhoud wilt bekijken die normaal afgeschermd wordt in specifieke gebieden, ongeacht u thuis of in het buitenland bent
- uw persoonlijke gegevens privé wilt houden (gebruikersnamen, wachtwoorden, kredietkaartgegevens enz.)
- uw IP-adres wilt verbergen

## **Zal Bitdefender VPN een negatief effect hebben op de batterij van mijn apparaat?**

Bitdefender VPN werd ontworpen om uw persoonlijke gegevens te beschermen, om uw IP-adres te verbergen wanneer u verbonden bent met onbeveiligde draadloze netwerken en om afgeschermd inhoud te bekijken in bepaalde landen. Om onnodig verbruik van uw batterij te vermijden, raden



we u aan VPN enkel te gebruiken indien nodig, en de verbinding te verbreken wanneer u offline bent.

## **Waarom is het internet soms trager wanneer ik verbonden ben met Bitdefender VPN?**

Bitdefender VPN is ontworpen om u een aangename ervaring te bieden tijdens het surfen. Uw internetconnectiviteit of de afstand met de server waarmee u verbonden bent, kan echter zorgen voor vertraging. In dat geval, indien het niet noodzakelijk is om te verbinden met een server die veraf gehost wordt (bijv. van China naar de VS), raden we aan Bitdefender VPN toe te staan om u automatisch te verbinden met de dichtstbijzijnde server, of een server te vinden die dichterbij uw huidige locatie gelegen is.

## **Kan ik een andere Bitdefender-account aan mijn apparaat koppelen?**

Ja, u kunt als volgt wijzigen welke Bitdefender-account aan uw apparaat is gekoppeld:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **Mijn account** uit de lijst.
3. Tik op **Uitloggen** en bevestig uw keuze.
4. Tik op **Central-account gebruiken** en typ het e-mailadres en het wachtwoord voor uw nieuwe Bitdefender-account.

## **Wat is Apparaatbeheer?**

Apparaatbeheer is een Android-functie die Bitdefender Mobile Security de benodigde bevoegdheden geeft om bepaalde taken op afstand te kunnen uitvoeren. Zonder deze bevoegdheden zou vergrendeling op afstand niet werken en zouden niet alle gegevens op afstand kunnen worden gewist. Als u de app wilt verwijderen, moet u eerst deze machtigingen intrekken via **Instellingen > Beveiliging > Apparaatbeheerders kiezen**.

## **Waarvoor dient het vertrouwde nummer?**

Als uw telefoon in handen komt van iemand die niet van plan is de telefoon aan de rechtmatige eigenaar terug te geven, is de kans groot dat deze persoon al snel de simkaart zal vervangen. Zodra Bitdefender Mobile Security merkt dat de simkaart in uw telefoon is vervangen, wordt automatisch een sms-bericht met informatie over het telefoonnummer van de nieuwe simkaart verzonden naar het vertrouwde nummer dat u van tevoren hebt ingesteld. Het vertrouwde nummer is bijvoorbeeld het telefoonnummer van iemand die



u goed kent en vertrouwt, of het nummer van een andere telefoon die in uw bezit is.

## Kan het vertrouwde nummer nog worden gewijzigd nadat ik het heb ingesteld?

Ja, dat kan:

1. Open Bitdefender Mobile Security.
2. Tik op de **Menu**-knop en selecteer **Instellingen** uit de lijst.
3. Tik in het gedeelte **Anti-Theft** op **Vertrouwd nummer**.

U moet eerst een pincode invoeren, voordat u het vertrouwde nummer kunt wijzigen.

## Hoeveel kost het versturen van sms-opdrachten?

Sms-opdrachten worden verzonden als gewone sms-berichten, waarvoor u de gebruikelijke kosten van uw telefoonmaatschappij verschuldigd bent. Bitdefender brengt hiervoor verder geen kosten in rekening.

## Hoe kan ik de fout "Geen Google-token" verhelpen, die zich voordoet wanneer ik inlog op Bitdefender Mobile Security?

Deze fout treedt op als het apparaat niet aan een Google-account is gekoppeld of als het apparaat wel aan een account is gekoppeld, maar er vanwege een tijdelijk probleem geen verbinding met Google gemaakt kan worden. Probeer een van de volgende oplossingen:

- Ga naar Android Instellingen > Applicaties > Applicatiebeheer > Bitdefender Mobile Security en tik op **Gegevens wissen**. Probeer vervolgens opnieuw in te loggen.
- Controleer of uw apparaat is gekoppeld aan een Google-account.  
Dit kunt u als volgt controleren: ga naar Instellingen > Accounts & synchronisatie en kijk of er een Google-account wordt weergegeven onder **Accounts beheren**. Voeg uw account toe als er geen account wordt weergegeven, start het apparaat opnieuw op en probeer opnieuw in te loggen op Bitdefender Mobile Security.
- Start het apparaat opnieuw op en probeer opnieuw in te loggen.

## In welke talen is Bitdefender Mobile Security leverbaar?

Bitdefender Mobile Security is momenteel beschikbaar in deze talen:



- Braziliaans
- Tsjechisch
- Nederlands
- Engels
- Frans
- Duits
- Grieks
- Hongaars
- Italiaans
- Japans
- Koreaans
- Pools
- Portugees
- Roemeens
- Russisch
- Spaans
- Thais
- Turks
- Vietnamees

In de toekomst worden hieraan nog meer talen toegevoegd. Om de taal voor de interface van Bitdefender Mobile Security te wijzigen, gaat u naar de **Taal & toetsenbord**-instellingen van uw apparaat en stelt u het apparaat in op de gewenste taal.



## 15. HULP VRAGEN

Er zijn meerdere online informatiebronnen beschikbaar om u te helpen bij het oplossen van problemen en vragen met betrekking tot Bitdefender.

- Bitdefender-ondersteuningscentrum:  
<https://www.bitdefender.com/support/consumer.html>
- Bitdefender-ondersteuningsforum:<https://forum.bitdefender.com>
- Het HOTforSecurity-portaal over computerbeveiliging:  
<https://www.hotforsecurity.com>

U kunt ook uw favoriete zoekmachine gebruiken om meer informatie te zoeken over computerbeveiliging, de Bitdefender-producten en het bedrijf.

### 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 preventie tegen bedreigingen, 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 informatieverzoeken en probleemmeldingen van klanten van Bitdefender komen uiteindelijk in het Bitdefender-ondersteuningscentrum terecht in de vorm van bugfix-rapporten, oplossingen of informatieve artikelen, die een aanvulling vormen op de Help-bestanden van onze producten.

Het Bitdefender-ondersteuningscentrum is op elk ogenblik beschikbaar op <http://www.bitdefender.com/support/>.

### 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 bepaalde bedreigingen niet van uw apparaat worden verwijderd of als u iets wilt vragen over de werking van het product, kunt u dit melden of vragen op het forum.

Supportmedewerkers van Bitdefender 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.

Zoek altijd eerst op het forum om te zien of een vergelijkbare vraag of kwestie al eerder is besproken.

Het Bitdefender-ondersteuningsforum is beschikbaar op <https://forum.bitdefender.com> in 5 verschillende talen: Engels, Duits, Frans, Spaans en Roemeens. Tik op **Home & Home Office Protection** om toegang te krijgen tot het gedeelte voor consumentenproducten.

## HOTforSecurity-portaal

Het HOTforSecurity-portaal is een rijke bron van informatie over computerbeveiliging. Hier leert u meer over de verschillende dreigingen waaraan uw computer wordt blootgesteld wanneer u verbinding met internet maakt (malware, phishing, spam, cybercriminelen). Een handige woordenlijst helpt u om bepaalde vaktermen uit de computerbeveiliging beter te begrijpen.

Er worden regelmatig nieuwe artikelen gepubliceerd om u op de hoogte te houden van de meest recent ontdekte bedreigingen, actuele beveiligingstrends en andere informatie over de beveiligingssector.

De webpagina van HOTforSecurity is <https://hotforsecurity.bitdefender.com/>.