

Bitdefender[®] MOBILE SECURITY



HANDLEIDING





Bitdefender Mobile Security Handleiding

Publication date 09/09/2019

Copyright© 2019 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. Webbescherming | 10 |
| 5. VPN | 12 |
| 6. Antidiefstalfuncties | 15 |
| 7. Accountprivacy | 19 |
| 8. App Lock | 21 |
| 9. Rapporten | 26 |
| 10. WearON | 27 |
| 11. Info | 28 |
| 12. Bitdefender Central | 29 |
| 13. Veelgestelde vragen | 36 |
| 14. Hulp vragen | 42 |



1. BESCHERMINGSFUNCTIES

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

- Malwarescanner
- Webbescherming
- VPN
- Antidiefstal, met:
 - Lokalisering op afstand
 - Apparaatvergrendeling op afstand
 - Gegevens wissen op afstand
 - Apparaatwaarschuwingen op afstand
- Accountprivacy
- 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 4.1 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  en selecteer vervolgens **Mijn apparaten**.
4. Tik op **BESCHERMING INSTALLEREN** en tik vervolgens op **Dit apparaat beschermen**.
5. Selecteer de eigenaar van het apparaat. Als het apparaat toebehoort aan iemand anders, druk dan op de overeenstemmende knop.
6. U wordt doorgestuurd naar **Google Play**. In het scherm van Google Play tikt u op de installatie-optie.

● Windows, macOS, iOS

1. Ga naar <https://central.bitdefender.com>.
2. Aanmelden bij uw Bitdefender-account.
3. Druk op  in de linkerbovenhoek van het scherm en klik dan op **Mijn Apparaten**.
4. Druk op **BESCHERMING INSTALLEREN** en druk vervolgens op **Andere apparaten beschermen**.
5. Selecteer de eigenaar van het apparaat. Als het apparaat toebehoort aan iemand anders, druk dan op de overeenstemmende knop.
6. Druk op **DOWNLOADLINK VERSTUREN**.
7. Voer in het overeenstemmende veld een e-mailadres in en druk op **E-MAIL VERSTUREN**. De gegenereerde downloadlink is slechts 24



uur geldig. Indien de link vervalst, dient u aan de hand van dezelfde stappen een nieuwe te genereren.

8. Controleer op het apparaat waarop u Bitdefender wilt installeren, het e-mailadres dat u ingevoerd hebt en druk op de overeenstemmende downloadknop.

● Vanuit Google Play

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

Als alternatief kunt u de QR-code scannen:



Voordat u de valideringsstappen kunt volgen, 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. 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.
2. 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.

Bescherming configureren

Eens u ingelogd bent op de toepassing verschijnt het venster **Bescherming configureren**. Om uw apparaat te beveiligen, raden we aan dat u de volgende stappen doorloopt:

- **Status abonnement.** Om te worden beschermd door Bitdefender Mobile Security, moet u uw product activeren met behulp van een abonnement, dat aangeeft hoelang u het product mag gebruiken. Wanneer het abonnement verlopen is, zal de toepassing niet meer werken en is uw apparaat niet langer beschermd.

Tik op **IK HEB EEN CODE** en vervolgens op **ACTIVEREN** indien u een activeringscode hebt.

Indien u ingelogd bent met een nieuwe Bitdefender-account en geen activeringscode hebt, kunt u het product 14 dagen lang gratis gebruiken.

- **Webbescherming.** Tik op **ACTIVEREN** indien uw apparaat Toegankelijkheid vereist om Webbescherming te activeren. U wordt dan doorgestuurd naar het menu Toegankelijkheid. Tik op Bitdefender Mobile Security en schakel de overeenkomstige schakelaar in.
- **Malware scanner.** Voer een eenmalige scan uit om te verzekeren dat uw apparaat geen bedreigingen bevat. Tik op **NU SCANNEN** om het scanproces op te starten.

Het dashboard verschijnt zodra het scanproces begint. Hier ziet u de beveiligingsstatus van uw apparaat.



Dashboard

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

Het Dashboard biedt u informatie over de beveiligingsstatus van uw apparaat en helpt u aan de hand van Autopilot de beveiliging van uw apparaat te verbeteren, door u aanbevelingen te doen over de functies.

De statuskaart bovenaan het venster informeert u aan de hand van expliciete berichten en suggestieve kleuren over de beveiligingsstatus van het apparaat. Indien Bitdefender Mobile Security geen waarschuwingen bevat, is de statuskaart groen. Wanneer er een beveiligingsprobleem werd gedetecteerd, verandert de kleur van de statuskaart naar rood.

Bitdefender Autopilot is uw persoonlijke beveiligingsadviseur om u bij al uw activiteiten een effectieve werking en verhoogde bescherming te bieden. Naargelang de activiteiten die u uitvoert, biedt Bitdefender Autopilot contextuele aanbevelingen op basis van het gebruik en de noden van uw apparaat. Hiermee kunt u de voordelen van de functies die in de toepassing van Bitdefender Mobile Security inbegrepen zijn, ontdekken, en ervan genieten.

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.

Vanuit de onderste navigatiebalk hebt u toegang tot de Bitdefender Mobile Security-functies en kunt u eenvoudig navigeren:

Malwarescanner

Hiermee kunt u een scan starten en de optie Opslag scannen inschakelen. Zie "[Malwarescanner](#)" (p. 7) voor meer informatie.

Webbescherming

Garandeert een veilige surfervaring door u te waarschuwen over mogelijke schadelijke websites. Zie "[Webbescherming](#)" (p. 10) voor meer informatie.

VPN

Versleutelt internetcommunicatie, om uw privacy te verzekeren ongeacht welk netwerk u gebruikt. Zie "[VPN](#)" (p. 12) voor meer informatie.

Antidiefstal

Hiermee kunt u de Antidiefstalfuncties in- of uitschakelen en instellingen configureren. Zie "[Antidiefstalfuncties](#)" (p. 15) voor meer informatie.



Accountprivacy

Controleert of er een gegevenslek was in uw online accounts. Zie "[Accountprivacy](#)" (p. 19) voor meer informatie.

App Lock

Hiermee kunt u de geïnstalleerde apps beveiligen door een pincode in te stellen. Zie "[App Lock](#)" (p. 21) 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. 26) voor meer informatie.

WearON

Deze functie communiceert met uw smartwatch om uw telefoon terug te vinden als deze is zoekgeraakt. Zie "[WearON](#)" (p. 27) 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.

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 de scan op verzoek te starten:

1. Tik op de onderste navigatiebalk op  **Malwarescanner**.
2. Tik op **Scan starten**.

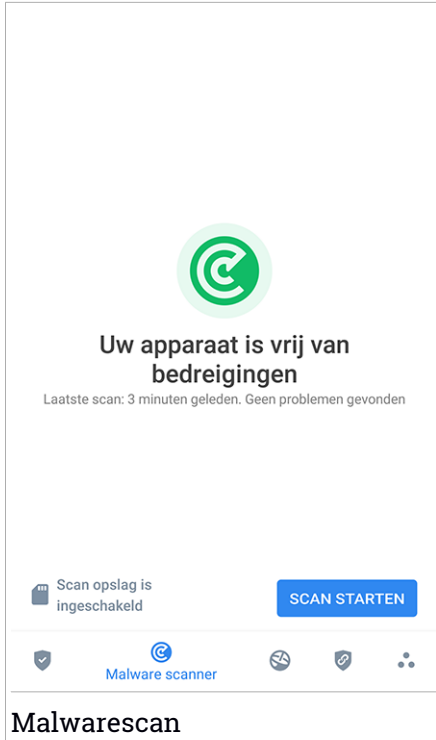


Opmerking

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.


Om de instelling Opslag scannen uit te schakelen:

1. Tik in de navigatiebalk op  **Meer**.
2. Tik op  **Instellingen**.
3. Schakel de schakelaar **Opslag scannen** in het gebied Malwarescanner uit.

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.

Als uw Android-versie 7.1 of recenter is, kunt u een snelkoppeling gebruiken naar Malware Scanner zodat u scans sneller kunt uitvoeren, zonder de Bitdefender Mobile Security interface te openen. Om dit te doen het Bitdefender icoon op uw startscherm of apps drawer ingedrukt houden, en dan het  icoon selecteren.



4. 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.

Telkens u een website voor internetbankieren gebruikt, vraagt Bitdefender-Webbescherming u om Bitdefender VPN te gebruiken. De notificatie verschijnt in de statusbalk. We raden aan dat u Bitdefender VPN gebruikt wanneer u ingelogd bent op uw bankrekening, zodat u beveiligd blijft tegen mogelijke beveiligingsinbreuken.

Om de notificatie Webbescherming uit te schakelen:

1. Tik in de navigatiebalk op **Meer**.
2. Tik op **Instellingen**.
3. Schakel de overeenstemmende schakelaar in het gebied Webbescherming uit.








Webbescherming is AAN






U bent beschermd tegen gevaarlijke pagina's

[UITZETTEN](#)

Beschermde browsers

Gebruik een van deze browsers om veilig te zijn

| | | |
|---|--------------------------------|------------------------|
|  | Chrome Geïnstalleerd | OPENEN |
|  | Dolphin | |
|  | Firefox | |

   **Webbescherming**  

Webbescherming



5. 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 in de VPN-kaart op het Dashboard op **VERBINDEN**.

De status van Bitdefender VPN wordt weergegeven.

- Tik op  **VPN** op de onderste navigatiebalk en tik dan op **VERBINDEN**.

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.

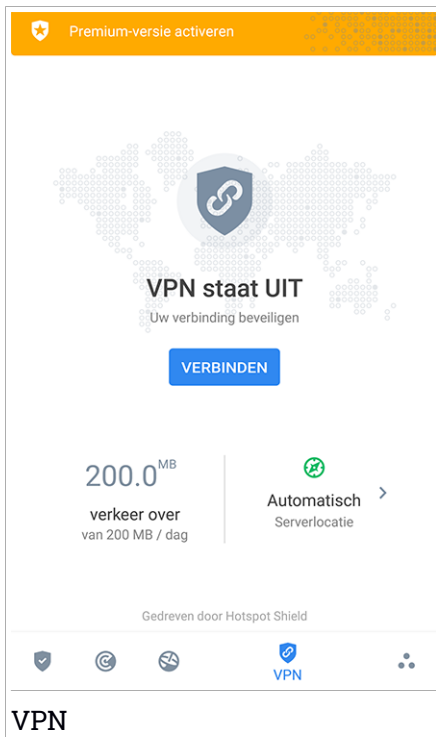


Als uw Android-versie 7.1 of recenter is, kunt u een snelkoppeling gebruiken naar Bitdefender VPN, zonder de Bitdefender Mobile Security interface te openen. Om dit te doen het Bitdefender icoon op uw startscherm of apps drawer ingedrukt houden, en dan het  icoon selecteren.

Het icoon  verschijnt in de statusbalk wanneer Bitdefender VPN actief is.

Om uw batterij te sparen, raden we aan de VPN-functie uit te schakelen wanneer u dit niet gebruikt.



Indien u een premium-abonnement hebt en u de server naar wens wilt veranderen, tik op **Serverlocatie** in de VPN-functie en selecteer vervolgens de locatie die u wenst. Voor meer info over VPN-abonnementen, raadpleeg **“Abonnementen”** (p. 14).





VPN Instellingen

Voor een geavanceerde configuratie van uw VPN:

1. Tik in de navigatiebalk op  **Meer**.
2. Tik op  **Instellingen**.

In het VPN-gebied kunt u de volgende opties configureren:

- Snelle toegang VPN - er verschijnt een notificatie in de statusbalk van uw apparaat waarmee u VPN snel kunt inschakelen.
- Open wifinetwerk - telkens u een verbinding maakt met een open wifinetwerk, wordt u via de statusbalk van uw apparaat gevraagd 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 **PREMIUM ACTIVEREN** beschikbaar in het Dashboard, of **Premium-versie activeren** 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 beschermingsabonnement. 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.



6. ANTIDIEFSTALFUNCTIES

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

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

Bitdefender Mobile Security biedt de volgende Antidiefstalfuncties:

Lokaliseren 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.

Vergrendelen op afstand

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

Wissen op afstand

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

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.

Antidiefstal activeren

Om de Antidiefstalfuncties te activeren, voltooit u de configuratieprocedure vanaf de Antidiefstalkaart in het Dashboard.

In plaats hiervan kunt u Antidiefstal ook op deze manier activeren:

1. Tik in de navigatiebalk op  **Meer**.
2. Tik op  **Antidiefstal**.
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. Volg deze stappen om dit in te schakelen:

- a. Tik op **Antidiefstal activeren** en tik vervolgens op **Aanzetten**.
- b. Geef **Antivirus** toestemming om de locatie van uw apparaat te kennen.

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

Stel een pincode in om ongeoorloofde toegang tot uw apparaat te vermijden. Telkens er een poging wordt gedaan om uw apparaat te gebruiken, moet een pincode worden ingegeven. Voor apparaten die authenticatie via vingerafdruk ondersteunen, kan een bevestiging via vingerafdruk worden ingesteld in plaats van de pincode.



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

c. Snapshot activeren

Telkens iemand het apparaat probeert te ontgrendelen terwijl Snapshot ingeschakeld is, en hier niet in slaagt, neemt Bitdefender een foto van die persoon.

Meer in detail: telkens wanneer de door u ingestelde pincode, het wachtwoord of de vingerafdruk drie keer na 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 door Bitdefender Mobile Security te openen en naar het scherm Antidiefstal te gaan. Of u kunt de foto bekijken in uw Bitdefender-account.

- i. Ga naar <https://central.bitdefender.com>.
- ii. Inloggen op uw account.
- iii. Tik linksboven in het venster op  en selecteer vervolgens **Mijn apparaten**.
- iv. Selecteer uw Android-apparaat en vervolgens het tabblad **Antidiefstal**.
- v. Tik op  naast **Uw snapshots controleren** om de meest recente foto's weer te geven.

Alleen de twee recentste foto's worden opgeslagen.

Eens de functie Antidiefstal geactiveerd is, kunt u de Webbeheer-opdrachten vanuit het scherm Antidiefstal individueel in- of uitschakelen door op de bijbehorende opties te tikken.

De Antidiefstalfuncties gebruiken vanuit Bitdefender Central



Opmerking

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



Zo opent u de Antidiefstalfuncties vanuit uw Bitdefender-account:

1. Ga naar **Bitdefender Central**.
2. Tik linksboven in het venster op  en selecteer vervolgens **Mijn apparaten**.
3. Selecteer de gewenste apparaatkaart in het venster **Mijn apparaten**.
4. Selecteer het tabblad **Antidiefstal**.
5. Tik in het onderste veld van het venster op  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 weergeven 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.

Antidiefstalinstellingen.

Als u de opdrachten vanop afstand wilt in- of uitschakelen:

1. Tik in de navigatiebalk op  **Meer**.
2. Tik op  **Antidiefstal**.
3. Schakel de gewenste opties in of uit.



7. ACCOUNTPRIVACY

Bitdefender-accountprivacy gaat na of er gegevensinbreuken hebben plaatsgevonden in de accounts die u gebruikt om online betalingen te verrichten, te winkelen of u aan te melden bij verschillende toepassingen of websites. De gegevens die in een account opgeslagen zijn, kunnen wachtwoorden, kredietkaartinformatie of bankrekeninginformatie betreffen en, indien niet goed beveiligd, kan er sprake zijn van identiteitsdiefstal of inbreuk op uw 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 inbreuken worden ontdekt op gevalideerde e-mailaccounts, worden meldingen weergegeven.

Om vanaf nu persoonlijke informatie veilig te houden:

1. Tik in de navigatiebalk op  **Meer**.
2. Tik op  **Accountprivacy**.
3. Tik op **AAN DE SLAG**.
4. Het e-mailadres dat u gebruikt hebt om uw Bitdefender-account aan te maken, verschijnt.

Tik op **TOEVOEGEN** om verder te gaan.

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.

Om andere accounts toe te voegen, tikt u in het venster Accountprivacy op **ACCOUNT TOEVOEGEN** en volgt u de nodige stappen.

Indien er in een van uw accounts inbreuken 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 privacyschending beveiligd hebt, kunt u de wijzigingen bevestigen door de geïdentificeerde inbreuken aan te duiden als **Opgelost**. Om dit te doen:

1. Tik in de navigatiebalk op  **Meer**.
2. Tik op  **Accountprivacy**.
3. Tik op de account die u net beveiligd hebt.
4. Tik op de inbreuk waarvoor u de account beveiligd hebt.
5. Tik op **OPGELOST** om te bevestigen dat de account beveiligd is.

Wanneer alle gedetecteerde inbreuken aangeduid zijn als **Opgelost**, wordt de account niet langer gemarkeerd als geschonden, tot er een nieuwe inbreuk wordt ontdekt.

Om geen notificaties meer te ontvangen telkens een automatische scan wordt uitgevoerd:

1. Tik in de navigatiebalk op  **Meer**.
2. Tik op  **Instellingen**.
3. Schakel de bijbehorende schakelaar in het gebied Accountprivacy uit.



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 Antidiefstal is geactiveerd.

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

1. Tik in de navigatiebalk op  **Meer**.
2. Tik op  **App Lock**.
3. Tik op **Aanzetten**.
4. Verleen toegang tot gebruiksgegevens voor Bitdefender.



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.

5. 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 Antidiefstal hebt ingesteld.



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

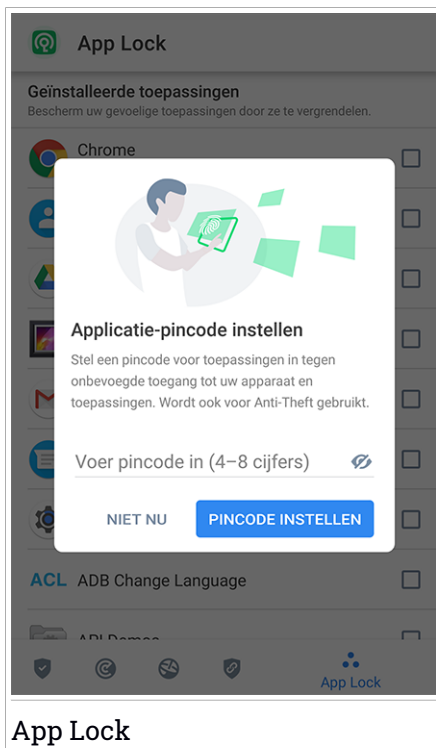
7. Selecteer welke toepassingen u wilt beschermen.

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 Antidiefstal gebruikt.



App Lock

Vergrendelmodus



De eerste keer dat u een toepassing aan App Lock toevoegt, verschijnt het venster App Lock Mode. Hier kunt u kiezen wanneer de functie App Lock de toepassingen op uw apparaat moet beschermen.



U kunt kiezen uit deze opties:



- **Telkens ontgrendelen** - telkens wanneer de vergrendelde toepassingen worden gebruikt, moet de pincode of vingerafdruk die u hebt ingesteld, worden gebruikt.
- **Ontgrendeld houden tot scherm uit** - de toepassingen zijn toegankelijk totdat het scherm wordt uitgeschakeld.
- **Vergrendelen na 30 seconden** - u kunt uw niet-vergrendelde toepassingen verlaten en binnen 30 seconden terug openen.

Als u de geselecteerde instelling wilt wijzigen:

1. Tik in de navigatiebalk op  **Meer**.
2. Tik op  **Instellingen**.
3. Tik in het gebied App Lock op **Telkens ontgrendelen**.
4. Kies de gewenste optie.

App Lock-instellingen

Voor een geavanceerde configuratie van App Lock:

1. Tik in de navigatiebalk op  **Meer**.
2. Tik op  **Instellingen**.

In het gebied App Lock kunt u de volgende opties configureren:

- **Suggestie gevoelige toepassing** - ontvang een lock-notificatie telkens u een gevoelige toepassing installeert.
- **Telkens ontgrendelen** - kies een van de beschikbare vergrendelings- en ontgrendelingsopties.
- **Smart Unlock** - houdt toepassingen ontgrendeld wanneer u verbonden bent met vertrouwde wifinetwerken.
- **VWillekeurig toetsenbord** - voorkom PIN-aflezing door de posities van de getallen te randomiseren.



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.

Om de functie Snapshot voor App Lock te configureren:

1. Tik in de navigatiebalk op  **Meer**.
2. Tik op  **Instellingen**.
3. Schakel de bijbehorende schakelaar in het gebied Snapshot in.

De foto's die tijdens het invoeren van een incorrecte pincode worden gemaakt, worden in het venster App Lock 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  en selecteer vervolgens **Mijn apparaten**.
4. Selecteer uw Android-apparaat en vervolgens het tabblad **Antidiefstal**.
5. Tik op  naast **Uw snapshots controleren** om de meest recente foto's weer te geven.

Alleen de twee recentste foto's worden opgeslagen.

Om de genomen foto's niet langer naar uw Bitdefender-account te uploaden:

1. Tik in de navigatiebalk op  **Meer**.



2. Tik op  **Instellingen**.
3. Schakel **Foto's uploaden** in het gebied Snapshot uit.

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 configureert u de functie Smart Unlock:

1. Tik in de navigatiebalk op  **Meer**.
2. Tik op  **App Lock**.
3. Tik op **TOEVOEGEN** om de wifiverbinding die u momenteel gebruikt, als vertrouwd in te stellen.



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. Tik in de navigatiebalk op  **Meer**.
2. Tik op  **Rapporten**.

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.

Om geen notificaties meer te ontvangen telkens een rapport werd gegenereerd:

1. Tik in de navigatiebalk op  **Meer**.
 2. Tik op  **Instellingen**.
 3. Schakel de schakelaar **Notificatie nieuw rapport** uit in het gebied Rapporten.
- **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 beschikbare activiteitenlogboek te verwijderen:

1. Tik in de navigatiebalk op  **Meer**.
2. Tik op  **Instellingen**.
3. Tik op **Activiteitenlogboek wissen**, en vervolgens op **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.

Indien u uw smartwatch bij zich hebt, detecteert deze automatisch de toepassing op uw telefoon en trilt wanneer u te ver verwijderd bent van uw telefoon, en in het bijzonder wanneer de Bluetooth-verbinding wordt verbroken.

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. INFO

Voor meer informatie over de Bitdefender Mobile Security-versie die u geïnstalleerd hebt, raadpleeg de Abonnementsovereenkomst en het Privacybeleid en bekijk de Open source-licenties.

1. Tik in de navigatiebalk op  **Meer**.
2. Tik op  **Instellingen**.
3. Tik op de gewenste optie in het gebied Over.



12. BITDEFENDER CENTRAL

Bitdefender Central is een webplatform dat u toegang geeft tot de online functies en diensten van het product. Vanuit dit platform kunt u vanop afstand belangrijke taken 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 of rechtstreeks vanuit de Bitdefender Central-toepassing op Android- en iOS-apparaten.

Om de Bitdefender Central-toepassing op uw apparaten te installeren:

- **Op Android** - zoek Bitdefender Central op Google Play en download en installeer de toepassing. Volg de nodige stappen om de installatie te voltooien.
- **Op iOS** - zoek Bitdefender Central in de App Store en download en installeer de toepassing. Volg de nodige stappen om de installatie te voltooien.

Zodra u aangemeld bent, kunt u beginnen met het volgende:

- 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.
- Bescherm de netwerktoestellen en hun gegevens tegen diefstal of verlies met **Antidiefstal**.

Inloggen op uw Bitdefender-account

Er bestaan twee manieren om naar Bitdefender Central te gaan

- Vanuit uw webbrowser:



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.
- Vanaf uw Android- of iOS-apparaat:
Open de Bitdefender Central-toepassing die u geïnstalleerd hebt.



Opmerking

In dit materiaal leest u de opties en instructies die op het webplatform beschikbaar zijn.


Twee-factorenauthenticatie

De 2-Factor authenticatiemethode voegt een extra veiligheidslaag toe aan uw Bitdefender account, door een authenticatiecode te vragen bovenop uw aanmeldgegevens. Op deze manier voorkomt u dat uw account wordt overgenomen en houdt u types cyberaanvallen, zoals keyloggers, bruteforce- of woordenlijstaanvallen, af.

Twee-factorenauthenticatie activeren

Door de tweefactorenauthenticatie te activeren, maakt u uw Bitdefender account veel veiliger. Uw identiteit zal gecontroleerd worden telkens u zich aanmeldt via verschillende apparaten, hetzij om één van de Bitdefender producten te installeren, hetzij om de status van uw abonnement te controleren of vanop afstand taken uit te voeren op uw apparaten.

Om de twee-factorenauthenticatie te activeren:

1. Ga naar **Bitdefender Central**.
2. Tik rechtsboven op het scherm op de icoon .
3. Tik op **Bitdefender Account** in het schuifmenu.
4. Selecteer het tabblad **Wachtwoord en beveiliging**.
5. Tik op **Twee-factorenauthenticatie**.
6. Tik op **AAN DE SLAG**.

Kies een van de volgende methodes:



- **Authenticator App** - gebruik een authenticator app om een code te genereren telkens u zich wilt aanmelden op uw Bitdefender account.

Als u een authenticator app zou willen, gebruiken, maar u niet zeker weet welke te kiezen, is er een lijst beschikbaar van de authentication apps die we aanbevelen.

- a. Tik op **AUTHENTICATOR APP GEBRUIKEN** om te starten.
- b. Om u aan te melden op een op Android of iOS gebaseerd apparaat, gebruik dat dan om de QR code te scannen.

Om u aan te melden op een laptop of computer, kunt u de getoonde code manueel toevoegen.

Tik op **Verdergaan**.

- c. Voer de code in die de app geeft of deze die weergegeven wordt in de vorige stap, en tik dan op **ACTIVEREN**.

- **E-mail** - telkens u zich aanmeldt in uw Bitdefender account, zal er een verificatiecode naar het Postvak-IN van uw e-mail worden gestuurd. Controleer uw e-mailaccount, en tik dan de code in die u hebt ontvangen.

- a. Tik op **E-MAIL GEBRUIKEN** om te starten.
- b. Controleer uw e-mailaccount en tik de verstrekte code in.

Let erop dat u vijf minuten hebt om uw e-mailaccount te controleren en tik de gegenereerde code in. Als de tijd verstreken is, zult u een nieuwe code moeten genereren volgens dezelfde stappen.

- c. Tik op **ACTIVATEREN**.
- d. U krijgt tien activeringscodes. U kunt de lijst kopiëren, downloaden of afdrukken en deze gebruiken in het geval u uw e-mailadres verliest of u zich niet meer kunt aanmelden. Elke code kan slechts één keer gebruikt worden.
- e. Tik op **GEREED**.

In het geval u wilt stoppen met het gebruik van de twee-factorenauthenticatie:

1. Tik op **TWEE-FACTORENAUTHENTICATIE UITSCHAKELEN**.
2. Controleer uw app of e-mailaccount en tik de code in die u hebt ontvangen.

In het geval u ervoor hebt gekozen om de authenticatiecode te ontvangen via e-mail, hebt u vijf minuten om uw e-mailaccount te controleren en de




gegenereerde code in te tikken. Als de tijd verstreken is, zult u een nieuwe code moeten genereren volgens dezelfde stappen.

3. Bevestig uw keuze.

Betrouwbare apparaten toevoegen

Om ervoor te zorgen dat alleen u toegang hebt tot uw Bitdefender account, is het mogelijk dat we eerst een veiligheidscode vragen. Als u deze stap zou willen overslaan telkens u verbinding maakt vanaf hetzelfde apparaat, raden we u aan dit te benoemen als een betrouwbaar apparaat.

Om toestellen toe te voegen als betrouwbare apparaten:

1. Ga naar **Bitdefender Central**.
2. Tik rechtsboven op het scherm op de icoon .
3. Tik op **Bitdefender Account** in het schuifmenu.
4. Selecteer het tabblad **Wachtwoord en beveiliging**.
5. Tik op **Betrouwbare apparaten**.
6. De lijst van de apparaten waar Bitdefender op geïnstalleerd is, wordt weergegeven. Tik op het gewenste apparaat.

U kunt zo veel apparaten toevoegen als u wilt, op voorwaarde dat Bitdefender erop geïnstalleerd is en uw abonnement geldig is.


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  en selecteer vervolgens **Mijn apparaten**.



3. Tik op de gewenste apparaatkaart en vervolgens op  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  en selecteer vervolgens **Mijn apparaten**.
3. Tik op de gewenste apparaatkaart en vervolgens op  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. Klik 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.

- **Antidiefstal.** Als uw apparaat is zoekgeraakt of gestolen, kunt u het met de Antidiefstalfunctie 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 "**Antidiefstalfuncties**" (p. 15) 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 in de linkerbovenhoek van het scherm op  en selecteer **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 in de linkerbovenhoek van het scherm op  en selecteer **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.



13. 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 Antidiefstalfuncties 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.
- Locatie -> nodig voor lokalisatie op afstand.
- Camera -> nodig voor Snapshot.
- Opslag -> nodig om de Malwarescanner ook de SD-kaart te laten scannen.

Hoe dien ik niet langer informatie in bij Bitdefender over verdachte toepassingen?

Bitdefender Mobile Security stuurt standaard rapporten naar de Bitdefender-servers over verdachte toepassingen die u installeert. Deze informatie is van essentieel belang voor de verbetering van de detectie van bedreigingen en kan ons helpen om u in de toekomst een betere ervaring te bieden. Als u ons geen informatie meer wilt sturen over verdachte toepassingen:

1. Tik in de navigatiebalk op  **Meer**.
2. Tik op  **Instellingen**.
3. Schakel **In-de-cloud-detectie** in het gebied Malwarescanner uit.

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 kritische boodschappen die gelinkt zijn aan de activiteiten. Om de activiteiten van de toepassing te bekijken:

1. Tik in de navigatiebalk op  **Meer**.
2. Tik op  **Rapporten**.



In het venster WEKELIJKSE RAPPORTEN kunt u de rapporten bekijken die wekelijks worden opgesteld en in het venster ACTIVITEITENLOGBOEK ziet u de informatie over de activiteiten van uw Bitdefender-toepassing.

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

Hoe kan ik de pincode die ik heb ingesteld voor App Lock en Antidiefstal wijzigen?

Als u de pincode die u ingesteld hebt voor App Lock of Antidiefstal wilt wijzigen:

1. Tik in de navigatiebalk op  **Meer**.
2. Tik op  **Instellingen**.
3. Tik in het gebied Antidiefstal op Beveiliging **PINCODE**.
4. Voer de huidige pincode in.
5. Voer de nieuwe pincode in die u wilt configureren.



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?

Eerst moet u uw apparaat verbinden met het draadloze netwerk dat u als vertrouwd hebt ingesteld. Volg vervolgens deze stappen:

1. Tik in de navigatiebalk op  **Meer**.
2. Tik op  **App Lock**.
3. Tik in de rechterbovenhoek op .
4. Tik naast het netwerk dat u als vertrouwd wilt instellen, op **TOEVOEGEN**.

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 aan de rechterbovenkant van het scherm op .
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 dicht bij 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. Tik in de navigatiebalk op  **Meer**.
2. Tik op uw e-mailadres.
3. Tik op **Uitloggen van account**. Is er een pincode geconfigureerd, wordt u gevraagd deze in te voeren.



4. Bevestig uw keuze.
5. Voer het e-mailadres en wachtwoord van uw account in de overeenkomende velden in en tik dan op **AANMELDEN**.

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.

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**.

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
- Zweeds
- 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.



14. 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/>.