



Gebruikershandleiding

Mobile Threat Defense (MTD)

Datum	26/04/2023
Onze referentie	Gebruikershandleiding MTD
Contact	Bart Callens
E-mail	b.callens@proximus.com

Inhoud

Inhoud	1
Overzicht	2
1. Beschrijving van de dienst	3
2. Installatie en activering	4
2.1 Voor u aan de slag gaat	4
2.2 Installatie en activering van de MTD-app op uw smartphone.....	4
2.2.1 Stap 1: de MTD-app downloaden	5
2.2.2 Stap 2: de MTD-app activeren.....	7
2.2.3 Stap 3: machtigingen verlenen aan de MTD-app	9
3. Gebruik van de MTD-app.....	17
3.1 Dashboard	17
3.1.1 Apps beveiliging	17
3.1.2 Web beveiliging	19
3.1.3 Apparaat beveiliging	20
3.1.4 Netwerk beveiliging	21
3.1.5 Bedreigingszones	21
3.2 Instellingen.....	22
3.2.1 Volle gebeurtenislog	23
3.2.2 Instellingen.....	24
4. Vaak gestelde vragen	25
4.1 Ik scan de QR-code in mijn activeringsmail en krijg een leeg browserscherm.	25
4.2 Kan ik de MTD-app activeren op meerdere toestellen tegelijk?	25
4.3 Ik verander van mobiel toestel. Wat moet ik doen?	25
4.4 Ik ga weg bij mijn huidige werkgever. Vervalt mijn MTD-optie?	25
4.5 Welke controle heeft mijn beheerder over mijn toestel?	26
4.6 Wat met mijn privacy? Tot welke gegevens heeft mijn beheerder toegang?	26
4.7 Ik krijg in mijn MTD-app de melding ‘Serververificatie onvolledig’	27

Overzicht

De bedoeling van dit document is om u als eindgebruiker ondersteuning te bieden bij de belangrijkste stappen van de installatie en het gebruik van de MTD-optie bij de mobiele tariefplannen van Proximus.

Merk op dat de beschikbaarheid van bepaalde functies die hier beschreven worden, afhangt van de configuratie van de MTD-optie door uw beheerder.

Eventuele verschillen tussen types toestellen (Android vs. iOS) worden vermeld.

Een uitgebreidere handleiding voor Android en iOS is in het Engels beschikbaar op <https://proximus.be/mtduser>.

1. Beschrijving van de dienst

Om bedreigingen tegen te gaan, stelt Proximus de beveiligingsoptie MTD (Mobile Threat Defense) voor bij zijn mobiele tariefplannen voor bedrijfsklanten. Deze beveiligingsoptie is een app (beschikbaar voor iOS en Android) die uw mobiel toestel (smartphone of tablet) beschermt tegen aanvallen die netwerk-, systeem-, web- of applicatiegericht kunnen zijn.

Uw beheerder heeft toegang tot een beveiligd portaal voor de configuratie van het bedrijfsbeleid en het beheer van eventuele bedreigingen.

Deze gebruikershandleiding beschrijft hoe de eindgebruiker de app kan installeren, activeren en gebruiken op iOS- en Android-smartphones of -tablets.

2. Installatie en activering

2.1 Voor u aan de slag gaat

Check de versie van uw Android- of iOS-smartphone. Deze dient minimaal Android 5.1 of iOS 11 te zijn op een 64 bit-toestel.

Uw beheerder dient de optie 'Mobile Threat Defense' voor zijn of haar medewerkers aan te vragen bij Proximus. Wenst u als werknemer deze optie te activeren, wend u dan tot de beheerder binnen uw bedrijf.

Uw beheerder zal contact opnemen met Proximus of een erkende Proximus-partner om de MTD-optie toe te voegen aan het mobiele contract tussen uw organisatie en Proximus.

2.2 Installatie en activering van de MTD-app op uw smartphone

Na de toevoeging van de MTD-optie aan het mobiele contract tussen uw organisatie en Proximus ontvangt u een e-mail om de MTD-app te installeren en te activeren op uw mobiel toestel.

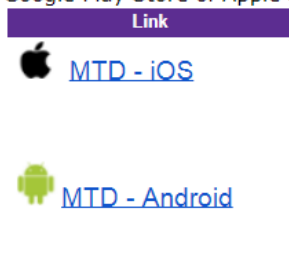
U ontvangt deze e-mail op het door uw beheerder opgegeven e-mailadres. Ontvangt u geen e-mail, check dan de spam- of junkfolder van uw e-mail client.

Nederlands


Geachte,

wij zijn verheugd u te kunnen bevestigen dat de MTD-optie voor uw mobiele apparaat beschikbaar is en vanaf nu zal gefactureerd worden op het mobiele contract van uw organisatie. Ga verder met de onderstaande stappen om uw mobiele apparaat te beschermen. U kunt [hier](#) verdere ondersteuning vinden of contact opnemen met de beheerder van uw organisatie.

1. Download de MTD app in de Google Play Store of Apple Store op uw mobiele apparaat:



2. Activeer de MTD app op uw mobiele apparaat door op de onderstaande link op uw mobiele apparaat te klikken of scan de QR-code met uw mobiele apparaat met de MTD app :

Link	QR Code
Activeer de MTD app	

Met vriendelijke groeten,

Proximus

Indien uw organisatie over een MDM-omgeving (Mobile Device Management) beschikt, kan de eerste stap (de MTD-app downloaden op uw toestel) automatisch gebeuren. In dat geval kunt u onmiddellijk naar de tweede stap gaan (de MTD-app activeren).

2.2.1 Stap 1: de MTD-app downloaden

Klik in de ontvangen e-mail op de voor u relevante link (afhankelijk van uw smartphone: Android of iOS). Hiermee opent u de Google Play of Apple App Store. Klik op de knop 'Installeren'.



Klik op de knop 'Openen':



U ziet het volgende scherm. Indien u meer informatie wenst over de functionaliteiten van de app kan u naar rechts swipen, indien niet, klik u op “Aan de slag”



U ziet het volgende scherm :



Uw MTD-app is geïnstalleerd. Ga nu naar Stap 2 om uw MTD-app te activeren.

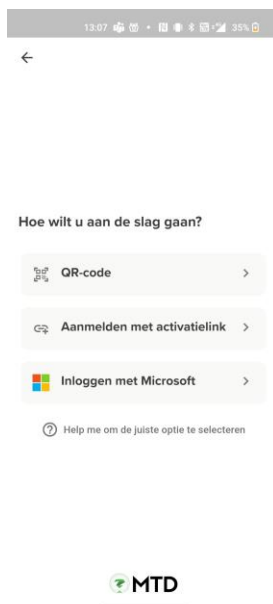
2.2.2 Stap 2: de MTD-app activeren

U kunt de MTD-app activeren via een van de volgende twee methodes. Kies de voor u eenvoudigste.

2.2.2.1 Activering via QR-code

Open de ontvangen e-mail op uw laptop of pc.

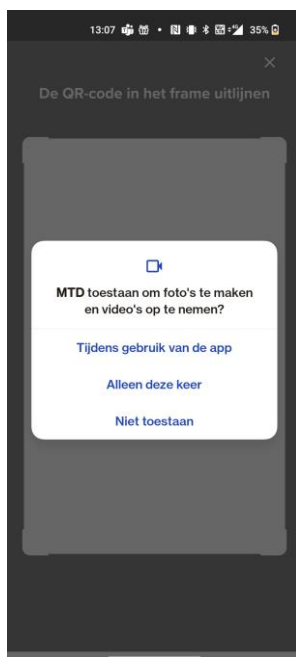
Klik in het welkomstscherf van de MTD-app op uw smartphone (zie Stap 1) op de knop 'QR Code'.



Mocht u de MTD-app ondertussen gesloten hebben, open hem dan opnieuw. De QR-code moet gescand worden met de MTD-app.

Opmerking: de knop 'Inloggen met Microsoft' is **niet relevant** en hoeft dus niet gebruikt te worden.

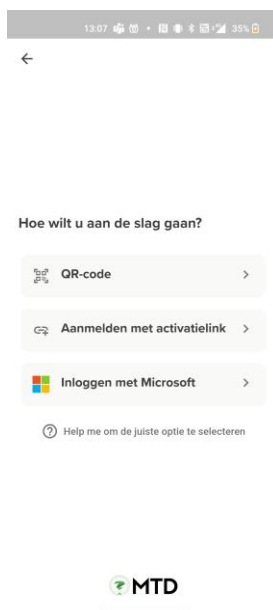
U moet de MTD-app toestaan om foto's te maken en video's op te nemen om de QR-code te kunnen scannen. Klik 'Tijdens gebruik van deze app'.



Scan de QR-code in de ontvangen welkomstmail. Ga naar [Stap 3](#).

2.2.2 Activering via URL


Open de ontvangen e-mail op uw smartphone en klik op de link '**Activeer de MTD app**'. Als alternatief kan u ook klikken op "**Aanmelden met activatielink**" in de MTD app en de activatielink uit uw e-mail copy/pasten in de MTD app :




Ga naar [Stap 3](#).

2.2.3 Stap 3: machtigingen verlenen aan de MTD-app

U krijgt eerst een overzicht van de gegevens van uw smartphone of tablet die via het MTD beheerdersplatform voor uw beheerder wel of niet zichtbaar gemaakt worden. Dit overzicht is afhankelijk van het privacy beleid dat uw beheerder heeft ingesteld.


13:09  35%





Wij vinden uw privacy belangrijk


Niet verzamelen


Mag verzamelen


 Apparaatmodel


 Besturingssysteem

 Locatie van uw apparaat

 wifinetwerk

 Geïnstalleerde apps


13:09  35%





Wij vinden uw privacy belangrijk


Niet verzamelen


Mag verzamelen

 Browsegeschiedenis


 Afbeeldingen, video's en andere mediabestanden

 Wachtwoorden

 Persoonlijke e-mails, documenten, contactpersonen of agenda

 Bekijk ons volledige privacybeleid

Doorgaan

 Bekijk ons volledige privacybeleid

Doorgaan

Klik op 'Doorgaan':

Proximus NV van publiek recht, Koning Albert II-laan 27, B-1030 Brussel, België
BTW BE 0202.239.951, RPR Brussel, BE50 0001 7100 3118 BPOTBEB1

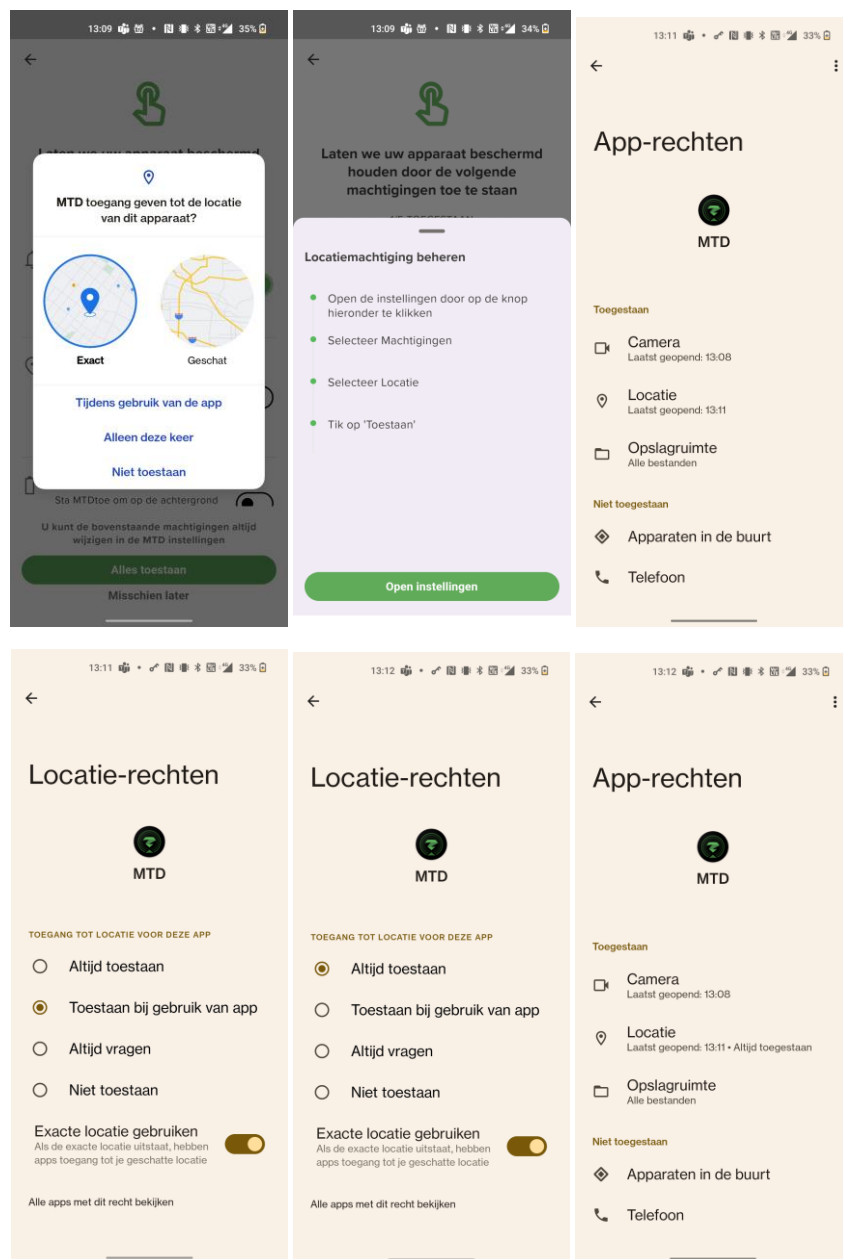
Pagina 10 van 27



Om uw toestel optimaal te beveiligen is het nodig om bepaalde machtigingen toe te staan op uw toestel. Klik op **“Alles toestaan”**.

Pas de verschillende machtigingen aan op uw toestel :

Locatiemachtiging : hiermee geeft U de toestemming aan de app om de locatie van uw toestel door te geven aan het MTD beheersplatform waar uw beheerder toegang toe heeft :

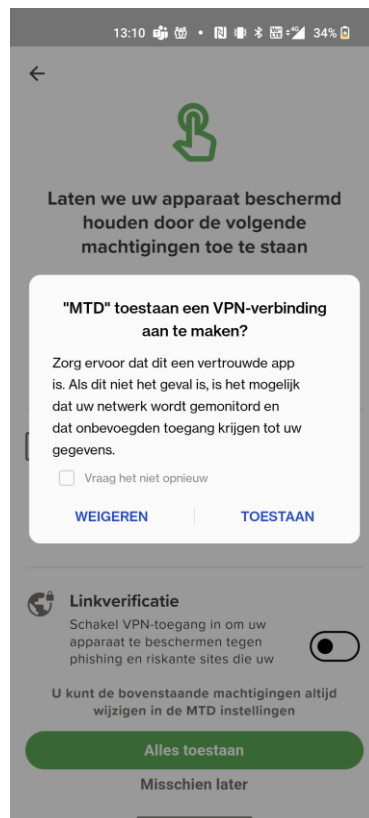


Batterij optimalisatie :

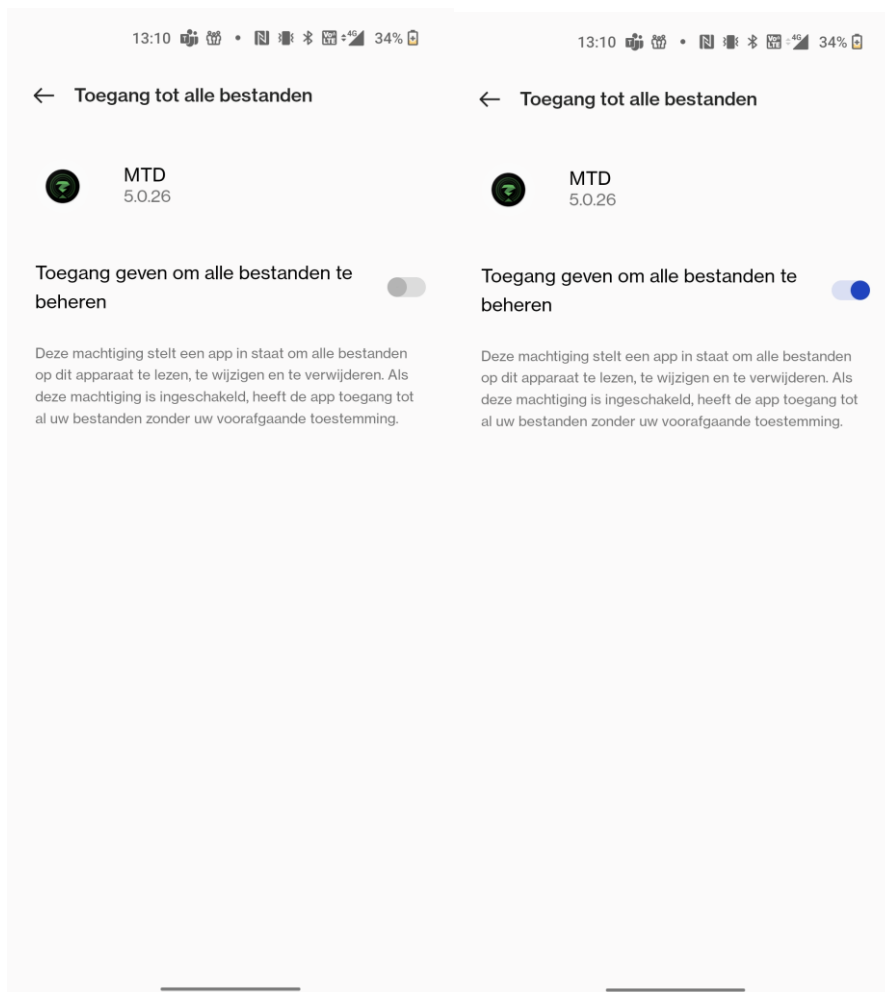
Om optimale bescherming te bieden wordt aangeraden om de MTD app toestemming te geven om in de achtergrond actief te zijn :



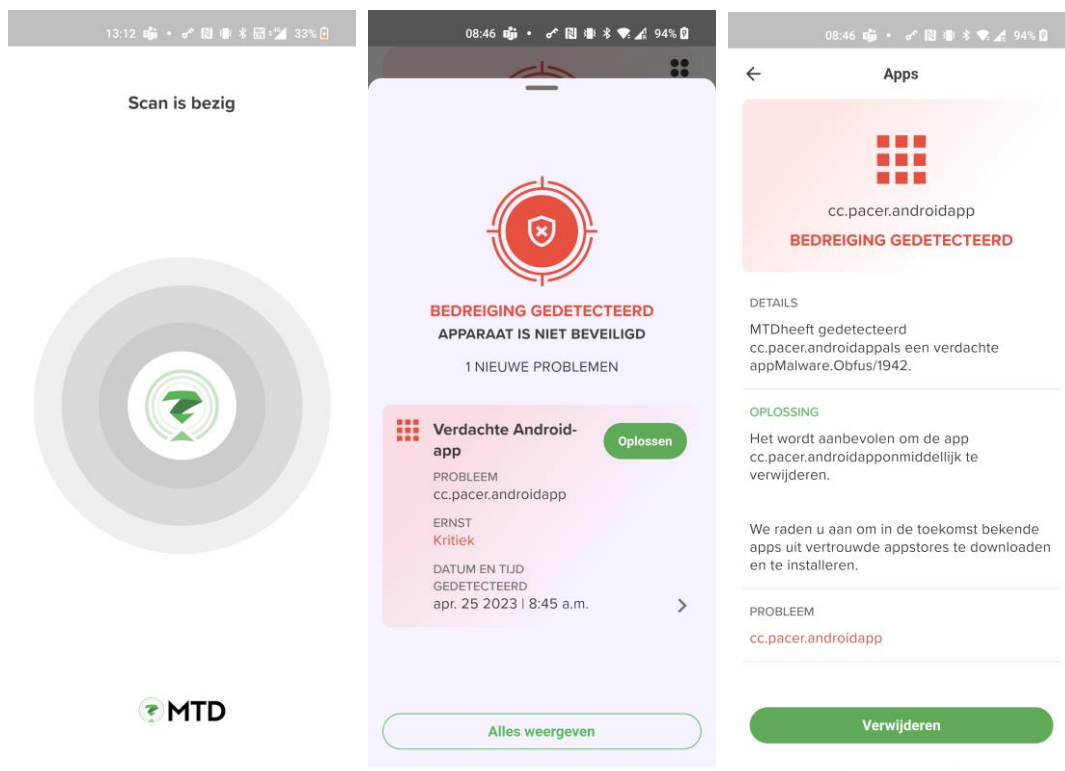
VPN toegang: Om uw toestel te beveiligen tegen phishing en riskante sites is het nodig om de MTD app VPN toegang te verlenen.



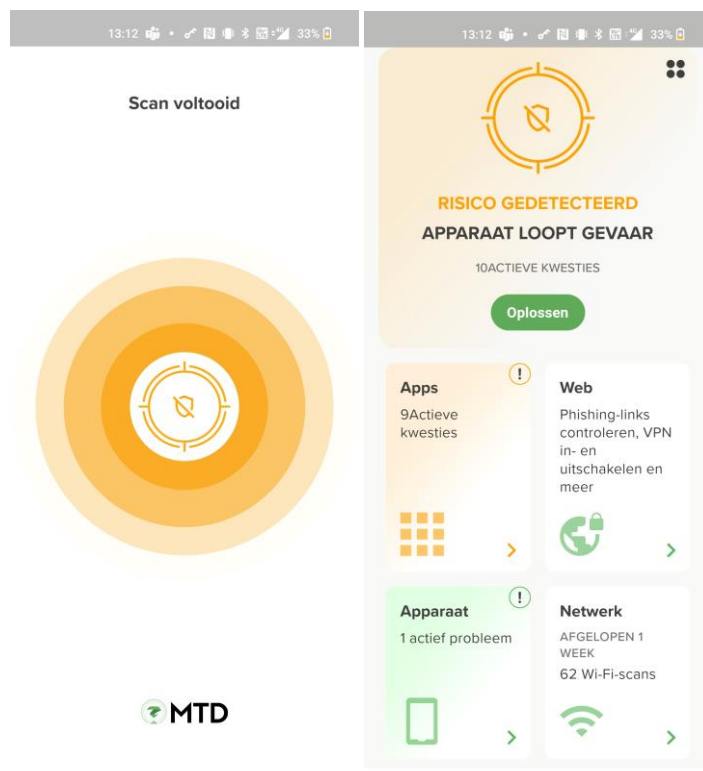
Toegang tot alle bestanden : Om kwaadaardige gedragingen op uw mobiel toestel te kunnen detecteren heeft de MTD app toegang nodig tot de bestanden op uw toestel :



Als alle machtigingen verleend zijn, zal de MTD-app een eerste scan uitvoeren van uw mobiele toestel. Indien er bedreigingen gevonden worden, zoals een kwaadaardige app, wordt dit getoond en kan U deze bedreigingen oplossen, door bijvoorbeeld de kwaadaardige app in kwestie te verwijderen.



Op het einde van de scan wordt het dashboard van de MTD app getoond. Uw MTD-app is nu succesvol geïnstalleerd en geactiveerd :

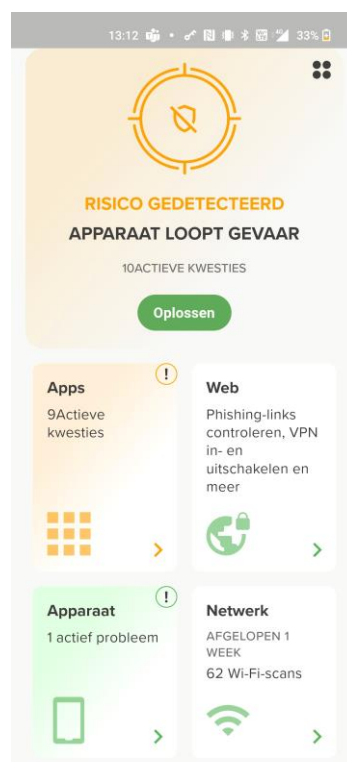


3. Gebruik van de MTD-app

De MTD-app beveiligt uw smartphone tegen bedreigingen. Afhankelijk van de instellingen door uw beheerder zult u een melding krijgen van bepaalde bedreigingen en de mogelijkheid om hierop te reageren. U kunt ook manueel een beveiligingsscan uitvoeren van uw toestel. De meest voorkomende interacties worden hieronder beschreven.


3.1 Dashboard

In het dashboard ziet u voor elk van de bedreigingscategorieën (Apps, Web, Apparaat en Netwerk) de beveiligingsstatus, evenals een algemene beveiligingsstatus. Via een kleurencode wordt aangegeven of er geen bedreigingen gevonden zijn (groen), niet kritische bedreigingen (oranje), of kritische bedreigingen (rood)




3.1.1 Apps beveiliging






De Apps beveiliging-tab geeft u een overzicht van de beveiliging van alle geïnstalleerde apps op uw toestel.




APP RAPPORT
Geïnstalleerde apps
Bekijk het beveiligingsoverzicht van uw apps

ONTDEKKEN
App opzoeken
Zoek in de Play Store om het gedetailleerde beveiligingsrapport van een app te bekijken voordat u de app downloadt.



	TikTok Geen risico gedetecteerd	>
	Instagram Risico gedetecteerd	>
	SHEIN-Shopping Online Risico gedetecteerd	>
	WhatsApp Messenger Risico gedetecteerd	>
	Local News: Breaking & Latest Geen rapport beschikbaar	>

Bijkomend kan u een beveiligingsrapport krijgen van een app uit de publieke app stores om deze app te evalueren alvorens u deze downloadt :




DETAILS

App verzamelt verschillende soorten gegevens die uw privacy in gevaar kunnen brengen en uw informatie aan hackers kunnen blootstellen.

OPLOSSING

Wees voorzichtig met het gebruik van deze app, het delen van informatie met deze app en het openen van links in deze app.

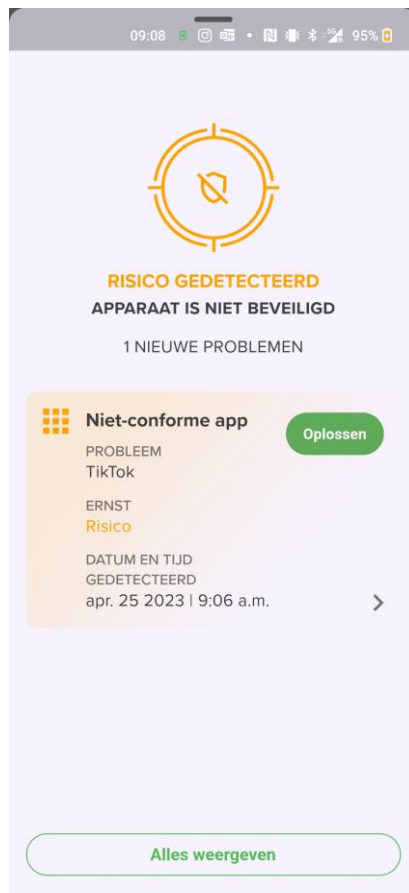


App permissions:

- Cryptografie**: Deze categorie bevat alle aspecten van toegang tot de cryptografische gegevens, zoals de sleutelhanger en wachtwoorden.
- Media**: De mediacategorie omvat alle media waar de app toegang tot heeft, zoals audio, video en de camera.
- Netwerk**: Deze categorie behandelt alle aspecten van networking waartoe de app toegang heeft, zoals VPN-, Bluetooth- en clouddiensten.
- Persoonsgegevens (PII)**: Deze categorie bevat persoonlijk identificeerbare informatie (PII) die de app opent of toegang tot heeft, zoals e-mail en locatie.

Downloaden

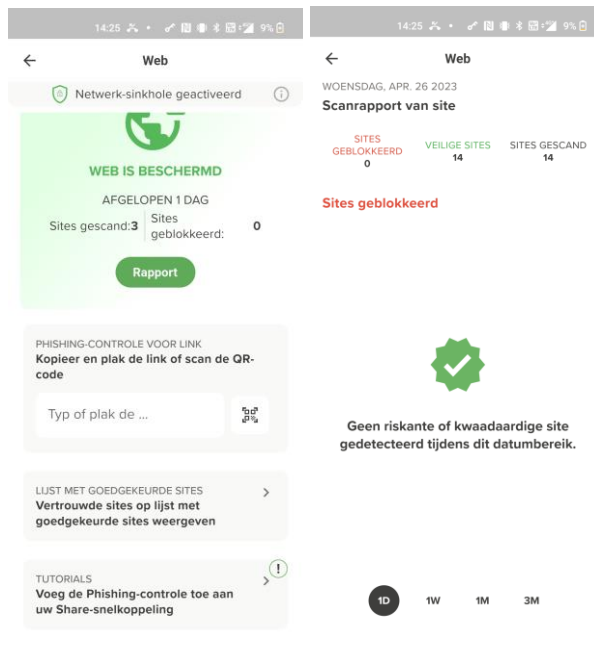
Inderdaad er bepaalde apps (zoals bvb TikTok) door uw beheerder als niet compliant gedefinieerd zijn zullen deze apps, wanneer geïnstalleerd op uw mobiele toestel, hier ook getoond worden. U kan uw toestel compliant maken door de betreffende app te verwijderen van uw toestel.



3.1.2 Web beveiliging

Via de Web beveiliging-tab kan u zien welke sites er door u vertrouwd geweest zijn. Indien ingesteld door uw beheerder zal u eveneens een boodschap krijgen dat de “netwerk sinkhole” geactiveerd is. Hiermee wordt uw toestel actief beveiligd tegen kwaadaardige web inhoud. U kan een rapport vragen van de sites die afgelopen periode door uw toestel geblokkeerd geweest zijn.

Afhankelijk van de instellingen door uw beheerder, zal u eveneens de mogelijkheid hebben om bepaalde URL's en QR'codes te verifiëren op kwaadaardige inhoud door deze te knippen en te plakken in de MTD app of door de QR code te scannen.



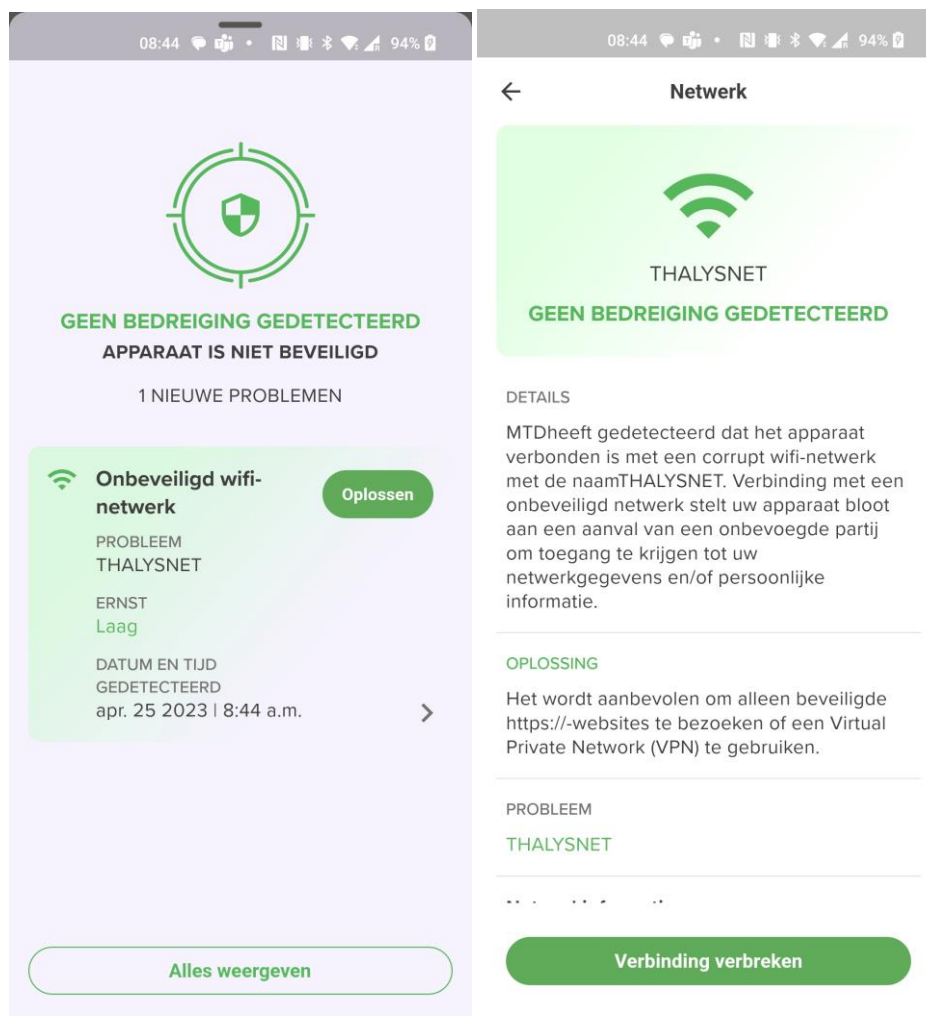
3.1.3 Apparaat beveiliging

De Apparaat beveiliging-tab geeft een overzicht van toestelgerelateerde bedreigingen, zoals een kwetsbare Android-versie of een rooted device. Wanneer een bedreiging gedetecteerd werd, kunt U deze oplossen door op “oplossen” te klikken.



3.1.4 Netwerk beveiliging

De Netwerk beveiliging-tab geeft de huidige beveiligingsstatus van de mobiele netwerk- of wifiverbinding weer. Voorbeelden van kritieke bedreigingen in deze categorie zijn MITM-aanvallen (Man-in-the-Middle), valse SSL-certificaten en valse wifitoegangspunten. U krijgt verdere details over bedreigingen en kunt deze desgevallend oplossen, bijvoorbeeld door een connectie naar een vals wifitoegangspunt te verbreken



3.1.5 Bedreigingszones

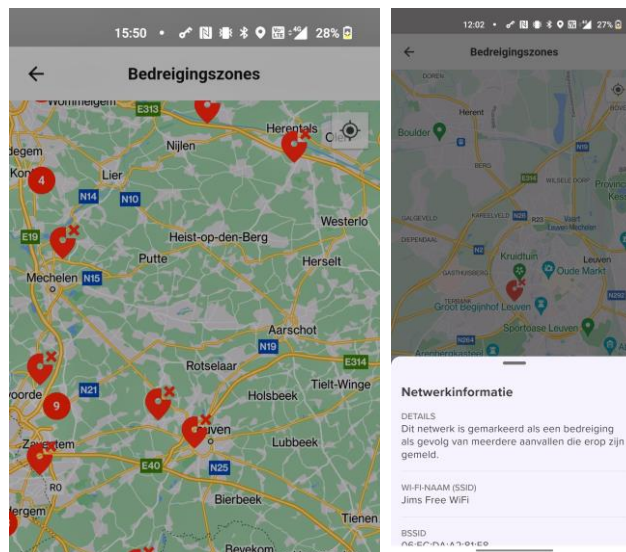
De beschikbaarheid van deze functionaliteit is afhankelijk van de configuratie door uw beheerder.

Op reis of onderweg logt u soms in op beschikbare open wifinetwerken. Veel van deze open wifinetwerken zijn echter vals, waarbij aanvallers met slechte bedoelingen hun slachtoffers in de val trachten te lokken door hen te laten inloggen op hun wifitoegangspunt.

De bedreigingszones pagina vertelt u welke beschikbare netwerken in de buurt u het best vermijdt omdat ze een hoog beveiligingsrisico inhouden.

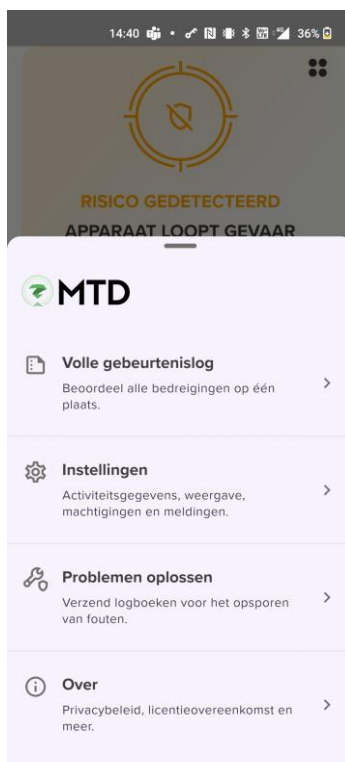
Raadpleeg vóór u op een netwerk inlogt via uw MTD-app de Bedreigingszones-kaart. Daarop worden risiconetwerken in uw omgeving met een rood icoon aangegeven.

Logt u in op een risiconetwerk zonder de MTD-app te raadplegen, dan stuurt de MTD-app u een waarschuwing met aanbevelingen, bijvoorbeeld om de verbinding met dit toegangspunt te verbreken.



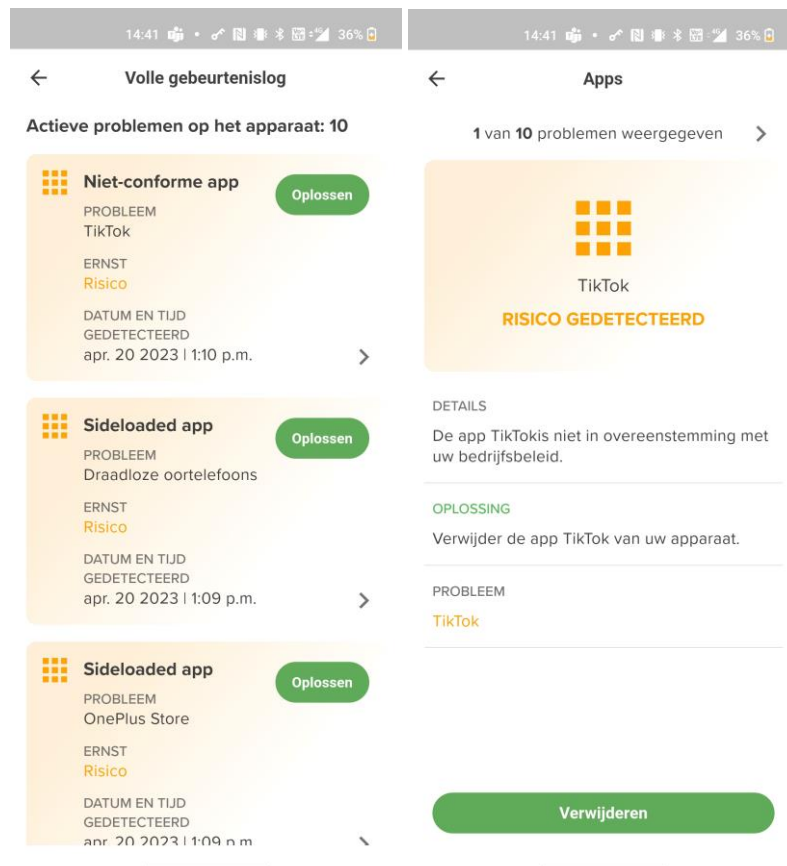
3.2 Instellingen

Als u in het dashboard op de 4 punten rechtsboven in het scherm klikt, krijgt U het volgende scherm :



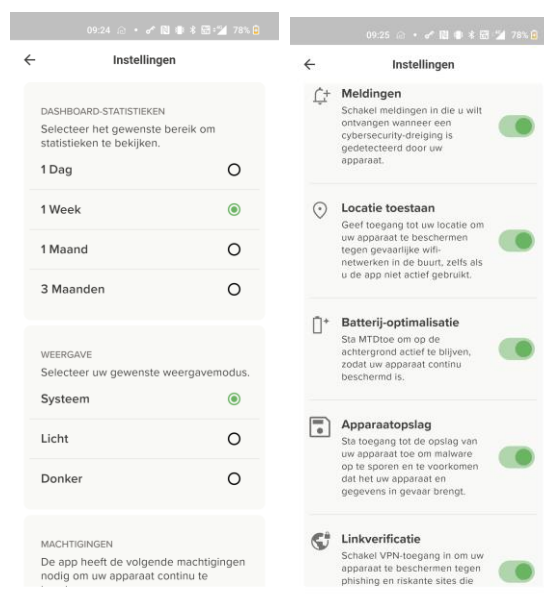
3.2.1 Volle gebeurtenislog

Hier krijgt u een volledig overzicht van alle gebeurtenissen op uw mobiele toestel. Door op **“oplossen”** te klikken kan u details van iedere gebeurtenis bekijken en deze oplossen, bijvoorbeeld het verwijderen van een app die niet conform is met het bedrijfsbeleid.



3.2.2 Instellingen

Onder instellingen kan u de tijdsperiode van de getoonde rapportering in de MTD app, de weergave modus van de MTD app aanpassen en de bij de installatie van de app geconfigureerde machtigingen van de app aanpassen.



4. Vaak gestelde vragen

4.1 Ik scan de QR-code in mijn activeringsmail en krijg een leeg browserscherm.

Check of de MTD-app al geïnstalleerd is op uw smartphone (zie [Stap 1](#) in de welkomstmail). Is dat het geval, neem dan contact op met uw beheerder voor verdere ondersteuning.

4.2 Kan ik de MTD-app activeren op meerdere toestellen tegelijk?

Neen, u kunt de MTD-app slechts activeren op één toestel. Zie ook '[Ik verander van mobiel toestel. Wat moet ik doen?](#)' hieronder.

4.3 Ik verander van mobiel toestel. Wat moet ik doen?

- De-installeer de MTD-app op uw oud mobiel toestel.
- Installeer de MTD-app op uw nieuw mobiel toestel (vanuit de Google Play Store of Apple Store of gepusht via een MDM-oplossing van de werkgever).
- Activeer de MTD-app op uw nieuw mobiel toestel. Gebruik hiervoor de originele link of de QR-code die u initieel ontvangen hebt. Hebt u deze link of QR-code niet meer, neem dan contact op met uw beheerder, die u deze link of QR-code opnieuw zal bezorgen.

4.4 Ik ga weg bij mijn huidige werkgever. Vervalt mijn MTD-optie?

Als uw huidige werkgever uw gsm-abonnement stopzet, vervalt automatisch ook de MTD-optie. Als uw nieuwe werkgever uw gsm-abonnement overneemt, kan deze beslissen om de MTD-optie weer te activeren. U ontvangt dan een nieuwe welkomstmail. Klik op "Opnieuw activeren MTD".

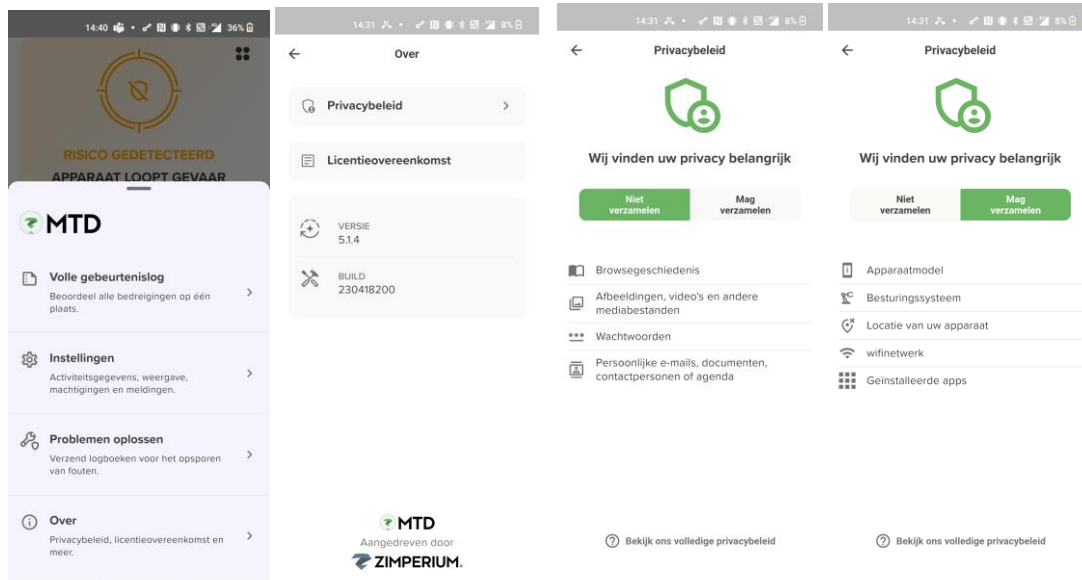


4.5 Welke controle heeft mijn beheerder over mijn toestel?

Afhankelijk van de door uw beheerder ingestelde policy kan de wifitoegang of Bluetooth afgesloten worden of de toegang tot de bedrijfsomgeving (bv. e-mail) geblokkeerd worden wanneer zich bepaalde bedreigingen voordoen op uw mobiel toestel.

4.6 Wat met mijn privacy? Tot welke gegevens heeft mijn beheerder toegang?

Welke data op uw toestel uw beheerder al dan niet kan zien, hangt af van de privacy instellingen van de oplossing, ingesteld door uw beheerder. U kunt dit raadplegen via de Instellingen in de MTD-app:



4.7 Ik krijg in mijn MTD-app de melding ‘Serververificatie onvolledig’.

Indien U deze boodschap krijgt, dient u uw beheerder te contacteren. Hij dient de configuratie aan te passen via het MTD portaal.

