# Vodafone Mobiele Beveiliging Beheerhandleiding

jamf

Together we can
vodafone
business

# Aan de slag met Vodafone Mobiele Beveiliging

Veilig Toestel en Veilig Internet in samenwerking met Jamf

Deze handleiding laat u als beheerder zien hoe u de smartphones en tablets in uw netwerk beschermt tegen malware, phishing en andere hack-praktijken. We leggen uit hoe u Vodafone Mobiele Beveiliging activeert en beheert. Dit omvat zowel de functionaliteiten van de Jamf Mobile Threat Defense app en het bijbehorende beheerportaal. Daarnaast biedt het een snelle start voor de uitrol van de dienst aan eindgebruikers en aanpassingen in het beveiligingsprofiel van uw organisatie.

Voor verdere vragen en ondersteuning gaat u naar www.vodafone.nl/mb of neem contact op met de Zakelijke klantenservice van Vodafonevia 1200 (mobiel), 0800-0094 (vast) of +31654500100 (buitenland). Meer informatie over het Mobiele Beveiliging beheerportaal en de app kunt u vinden op de Jamf knowledgebase, zie achterin deze handleiding.

**Together we can**

## Vodafone Mobiele Beveiliging en Jamf

Vodafone heeft een wereldwijd beveiligingsteam dat samenwerkt met Jamf, onze partner in het beveiligen van mobiele apparaten in het MKB. Samen zorgen we voor een veilige apparaten en veilig internet. De Jamf mobiele app is makkelijk in gebruik en scant automatisch de nieuwste online gevaren voor u. Jamf is marktleider in mobiele beveiliging. Jamf's geavanceerde servernetwerk scant en analyseert non-stop verdachte activiteiten op het internet. Wereldwijd. Zo identificeren en elimineren we samen talloze bekende én onbekende bedreigingen. De gerenommeerde onderzoeksinstituut Gartner en IDC plaatst Jamf in de top op het gebied van mobile threatdefense.

**Goed om te weten:** Nadat u Vodafone Mobiele Beveiliging heeft aangevraagd, ontvangt u ook mails en berichten van Jamf. De beveiliging op uw apparaten activeert u via de app van Jamf.

| Veilig Toestel | |
|---|---|
| Systeem-beveiliging | Beveilig kwetsbare OS-versies, jailbreaks, riskante profielen en gekraakte toestellen |
| Applicatie-beveiliging | Scan en beveiliging van miljoenen apps, voorkom datalekken |
| Anti-malware | Scan en blokkeer kwaadaardige apps en content met malware |

| Veilig Internet | |
|---|---|
| Anti-phishing | Realtime phishing detectie en blokkade via o.m. sms, mail en Whatsapp |
| Internet-beveiliging | Scan en blokkeer schadelijke websites, downloads, domeinen |
| WiFi-bescherming | Beveilig gegevens op riskante WiFi netwerken (SSL-stripping, MITM) |
| Privacy mode | Extra encryptie van webaanvragen |

## Waarom wilt u uw moieltjes ook al weer beveiligen?

**Veilig Toestel (endpointprotection)** De Jamf app scant non-stop op malware, onveilige apps en systeemrisico's voor iOS en Android. Het systeem herkent en reageert op alle bedreigingen.

**Veilig Internet (secure access)** Elke internetverbinding wordt gecheckt op onveilige inhoud, ook via wifi. De app blokkeert preventief toegang tot onveilige websites (phishing, malware), blokkeert of waarschuwt voor onveilige apps en beschermt onveilige wifi-verbindingen (via dynamische vpn).

**Privacy** Wachtwoorden, contacten, berichten of foto's worden extra beschermd: u voorkomt diefstal van persoonlijke gegevens, ook voor uw klanten.

**Ook goed om te weten:** Beheerders zien alleen het gebruik van de Jamf app en de risico's. Zij hebben geen inzage in bezochte websites, gebruikte apps of andere gebruikersgegevens.

## En nu: echt aan de slag!

U heeft gekozen voor Vodafone Mobiele Beveiliging. Als beheerder (administrator) krijgt u op uw bij Vodafone bekende e-mailadres twee e-mails: één met bevestiging van uw aanmelding en informatie over uw account en één (van Jamf) met uw **inloggegevens** voor het beheerportaal. Normaalgesproken krijgt deze mails rond het moment dat uw nieuwe abonnementen daadwerkelijk worden aangesloten of verlengd.

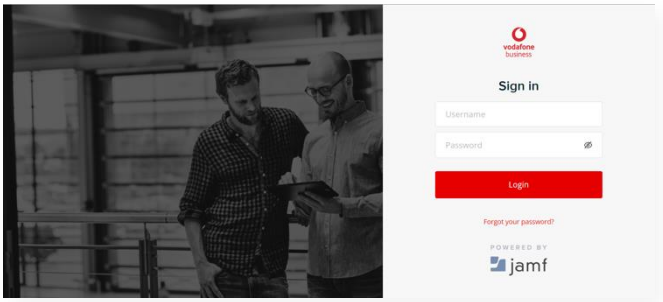
Het beheerportaal geeft u de volgende mogelijkheden:
1. Creëren van een Activation Profile, waarmee u eenvoudig uzelf en uw medewerkers kunt activeren (en activeren) met de Jamf beveiligingsapp*.
2. Inzicht verkrijgen in de beveiligingsstatus van al uw medewerkers: wie gebruikt de Jamf app, welke bedreigingen zijn er geweest en hoe zijn die onschadelijk gemaakt.
3. Aanpassen van het standaard beveiligingsprofiel, bijvoorbeeld door extra blokkades van ongewenste websites (blacklisting).

**Let op.** Maakt u gebruik van Vodafone Mobiele Beveiliging in combinatie met Red Pro of Business Mobile, dan krijgen uw medewerkers helemaal automatisch twee sms-berichten gestuurd op hun mobiele nummer. Die eerste sms ontvangt de gebruiker op het moment dat u toegang heeft gekregen tot het beheer-portaal, de tweede circa twee dagen later met de activatielink. U hoeft hen dus niet zelf uit te rollen.

# Zo werkt het beheerportaal

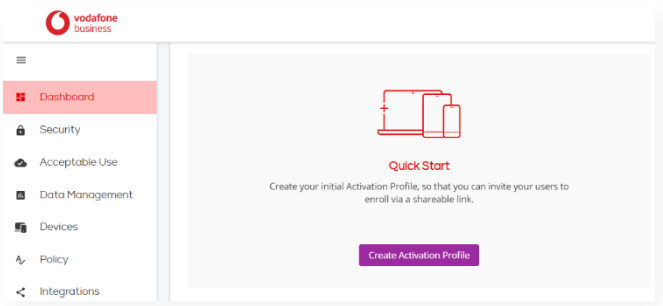
## Zo logt u in op het beheerportaal

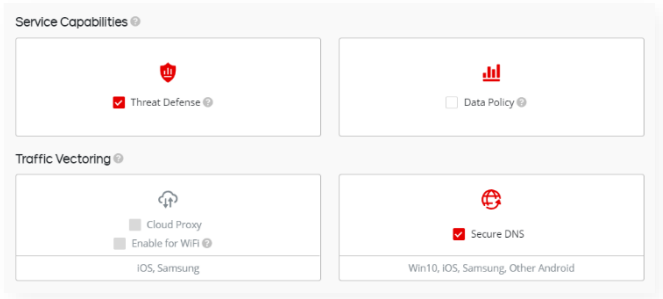
1. Ga naar vodafone-radar.jamf.com
2. Log in met uw e-mailadres en uw wachtwoord dat u per mail heeft ontvangen in de activatiemail van Jamf. U gebruikt het e-mailadres dat bij Vodafone bekend is als loginnaam voor My Vodafone Zakelijk.
3. U komt nu automatisch op het Dashboard in het portaal terecht (of ga hier naar toe).



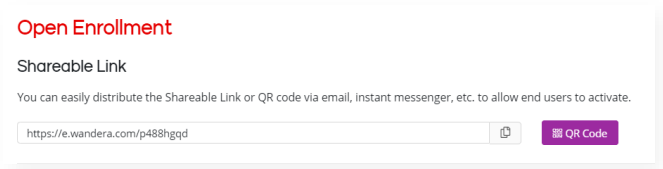

## Zo activeert u uzelf en uw medewerkers*

1. Ga naar het Dashboard in het beheerportaal. Hier ziet u Quick Start om een initieel Activation Profile (een activatielink) te creëren waarmee u uw gebruikers kunt activeren met de Jamf beveiligingsapp.
2. Stel het Configuration Profile goed in:
   - Vul de Service in: normaalgesproken is dat (a) Threat Defenseen (b) Secure DNS.
   - Vul in hoe vaak en/of tot wanneer met deze activatiecode gebruikers geactiveerd mogen worden.
3. Druk op Save en bevestig Profile Creation. Een nieuw venster verschijnt met de activatielink. Kopieer en plak de activatielink (Shareable Link) in een e-mail of ander bericht en verstuur die naar uzelf en uw medewerkers.
4. Als medewerkers op de link klinken dan worden zij automatisch geleid naar de appstore van Apple of Android om de Jamf app te downloaden en te activeren met de juiste instellingen.








* Deze stap kunt u overslaan als u en uw medewerkers al automatisch uitgerold zijn omdat u gebruik maakt van een Red Pro of Business Mobile bundel.

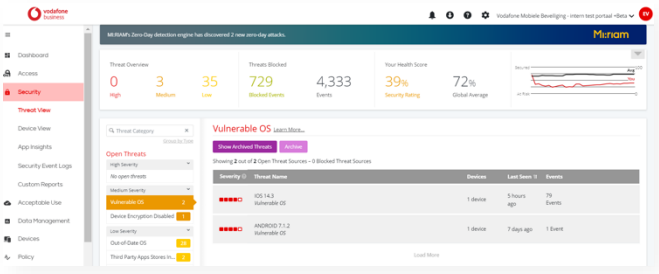

## Zo activeren uw medewerkers de Jamf app

1. Uw medewerkers ontvangen het bericht met de activatielink. Wanneer zij hierop klikken wordt de Jamf app geïnstalleerd en geactiveerd op hun mobiele apparaat.
2. Uw medewerkers dienen een aantal instellingen te accepteren tijdens het activatieproces.
3. De app is nu actief op het mobiele apparaat en uw medewerkers zijn beschermd.

# Zo werkt het beheerportaal

## Zo heeft u inzicht en behoudt u overzicht

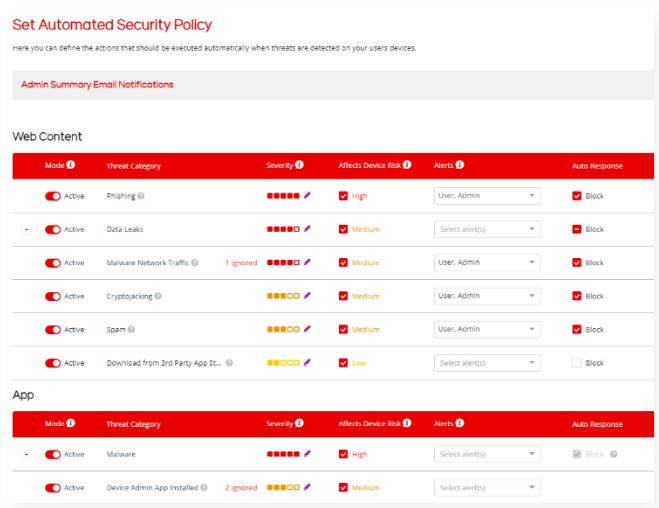
Op het Security Threat View overzicht ziet u wat er gebeurt: tegen welke risico's lopen uw gebruikers aan en hoe worden ze beveiligd. Het meeste gaat volledig automatisch. U hoeft daar niets voor te doen. Mocht u toch graag zelf ingrijpen, dan vindt u hier alle informatie om verder actie te ondernemen.

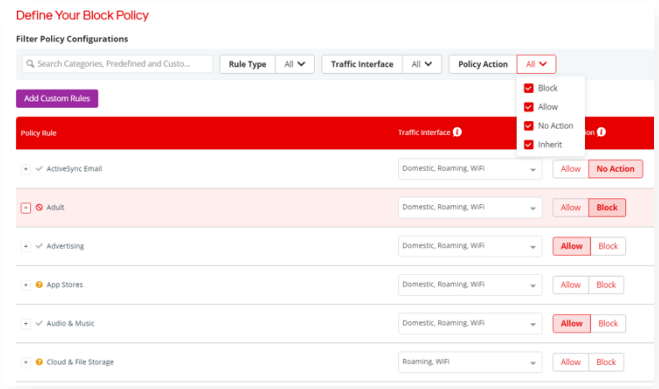


## Zo past u uw beveiligingsprofiel aan

Vodafone en Jamf hebben voor uw organisatie een standaard beveiligingsprofiel ingesteld, gebaseerd op de gemiddelde behoeften van onze klanten. In het beheerportaal kunt u dit profiel aanpassen aan de behoeften van uw organisatie. Klik hier voor in het linkermenu op Policy. U ziet nu meerdere opties die u kunt aanpassen, bijvoorbeeld:

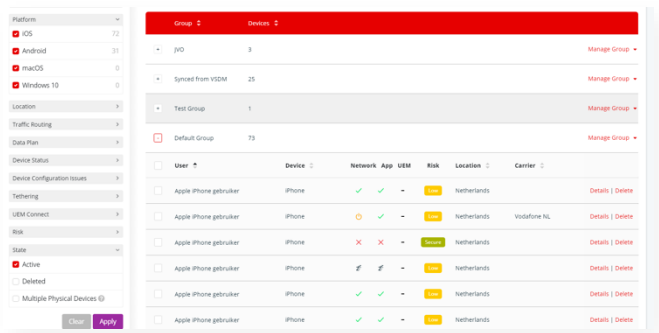
- Security Policy: Hier stelt u in hoe er met dreigingen wordt omgegaan op de apparaten van u en uw medewerkers. U kiest hier ook of u notificaties wilt ontvangen. Tot slot u bepaalt hier onder Exceptions of bepaalde dreigingen juist genegeerd moeten worden.
- Block Policy (niet voor alle abonnementen beschikbaar): Hier beheert u het internetgebruik. Zo kunt u bepaalde sites blokkeren. Hier stelt u whitelists op: sites die altijd toegankelijk moeten zijn. En blacklists: geblokkeerde sites. En u stelt hier het mobiel internet binnen Nederland, dataroaming in het buitenland en wifi-gebruik in. Let op: dit werkt alleen als u Cloud Proxy Traffic Vectoring hebt geselecteerd in het Activation Profile.
- Notifications: Hier stelt u de tekst in van de notificaties. Bijvoorbeeld als er een internet-verbinding van een gebruiker geblokkeerd wordt.




## Zo monitort u al uw gebruikers

In het linkermenubij Devices List ziet u het aantal aangeschafte licenties en het aantal licenties dat u in gebruik heeft. Ook heeft u hier het overzicht over alle actieve (en inactieve) gebruikers. Mocht er een gebruiker onterecht inactief zijn, dan kunt u hem of haar hier opnieuw activeren.



# Zo werkt het beheerportaal

## Zo heractiveertof deactiveert u gebruikers

Alle Red Pro of Business Mobile gebruikers ontvangen automatisch een sms met daarin een link. Hiermee activeren ze zelf Mobiele Beveiliging. Voor andere gebruikers of bij aanpassingen in uw gebruikersbase, dient u zelf gebruikers te heractiveren of deactiveren via het beheerportaal. Wil een eindgebruiker de app zelf verwijderen, bijvoorbeeld om van apparaat te wisselen, dan kan die dat zelf doen. U ziet dan in uw beheerportaal dat deze gebruiker niet meer actief is. Ook deze gebruiker kunt u zelf opnieuw activeren voor Mobiele Beveiliging via het portaal (zie ook eerder in deze handleiding).

1. Klik in het linkermenu van het portaal op Devices en daarna Activations
2. Klik op Create Profile. Vul de velden en selecteer Save.
3. U kunt dit profiel (activatielink) eenvoudig kopiëren en versturen (bivoorbeel per mail) naar uw medewerkers die geactiveerd moeten worden voor Mobiele Beveiliging.

Wilt u zelf een gebruiker verwijderen dan kan dat door op het mobiele apparaat van de gebruiker te klikken en te kiezen voor Delete.

**Tip:** Heeft een eindgebruiker per ongeluk een verkeerde profiel op z'n apparaat geactiveerd gekregen? Of werkt de Jamf app niet goed. Vraag uw collega dan om op zijn mobiele apparaat naar reset.jamf.com te surfen. Hier kan hij de app volledig resetten. Activeer de eindgebruiker dan opnieuw, zoals hierboven beschreven.

## Zo maakt u nieuwe beheerders aan

Wilt u collega's activeren als extra portaal-beheerder dan kunt u dit eenvoudig zelf doen:

1. Klik op het tandwiel-icoontje (bovenmenu).
2. Kies Administration.
3. Rechtsboven ziet u de knop New Admin. Klik hierop en maak de nieuwe beheerder aan.
4. U kunt met deze knop meerdere beheerders aanmaken, zodat meerdere mensen in uw organisatie toegang tot het portaal hebben.

## Zo wijzigt u geavanceerde instellingen

- Onder Settings in het linkermenu vindt u geavanceerde instellingen om bijvoorbeeld aangepaste rapporten te maken, of om aanpassingen te maken van pincodes, APNsen privacy.
- Onder Integrations vindt u onder meer UEM Integrations om de koppeling met uw bestaande Endpoint Management/MDM-software aan te passen en andere tools om te koppelen aan uw bedrijfssoftware.
- In de meeste gevallen zult u deze instellingen niet nodig hebben.

## Zo vindt u meer informatie

Bent u op zoek naar meer informatie of andere functies, kijk op Jamf Knowledge Base. Klik hiervoor naar het vraagteken(?)-icoon in de bovenbalk van het portaal. Naast toegang naar de knowledge base kunt u in de bovenbalk rapporten downloaden en de instellingen van het portaal zelf beheren.

**Nog vragen?**
**Zo neemt u contact met ons op...**

Voor verdere vragen en ondersteuning gaat u naar www.vodafone.nl/zakelijk/beveiliging/mobiele-beveiliging of neem contact op met de Zakelijke klantenservice van Vodafone via 1200 (mobiel), 0800-0094 (vast) of +31654500100 (buitenland).

We wensen u een Veilig Toestel en
Veilig Internet met Vodafone Mobiele Beveiliging.

**Together we can**

vodafone
business

Together we can