Beheerdershandleiding

Mobile Threat Defense (MTD)

Datum	01/05/2022
Onze referentie	**MTD_Beheerdershandleiding**
Contact	**Bart Callens**
E-mail	**b.callens@proximus.com**

Inhoud

Overzicht

De scope van dit document is om u als beheerder te ondersteunen bij de belangrijkste stappen bij de aanvraag van de MTD-optie (Mobile Threat Defense) op de Proximus mobiele tariefplannen en het gebruik van het MTD-portaal om deze te beheren.
Een uitgebreidere handleiding is beschikbaar in het Engels op https://proximus.be/mtd.
Een handleiding voor uw eindgebruikers van de MTD optie is beschikbaar op https://proximus.be/mtduser.

1. Beschrijving van de dienst

Om bedreigingen op mobiele toestellen tegen te gaan, biedt Proximus een beveiligingsoptie aan op haar mobiele contracten voor bedrijfsklanten: MTD (Mobile Threat Defense). Deze beveiligingsoptie beschermt het mobiele toestel van uw medewerkers, door middel van installatie van een app (beschikbaar voor iOS en Android). Deze app beveiligt de smartphone tegen aanvallen die netwerk-, systeem- of applicatiegericht kunnen zijn.

U als beheerder hebt toegang tot een beveiligd portaal waar u uw bedrijfsbeveiligingsbeleid kan configureren en bedreigingen kan beheren.

Deze gebruikershandleiding beschrijft voor u, als beheerder, hoe u toegang krijgt tot het MTD-portaal en hoe U daar de MTD-optie voor uw eindgebruikers kan beheren.

2. Aanvraag MTD-optie

2.1 Voorafgaand

U dient de MTD-optie te laten opnemen in uw mobiele contract met Proximus. Contacteer hiervoor uw commerciële contactpersoon bij Proximus.

2.2 Technisch bestelformulier

Nadat de MTD-optie toegevoegd is aan uw contract, gelieve uw commerciële contactpersoon bij Proximus te contacteren. Hij zal u een technisch bestelformulier bezorgen. Met dit technisch bestelformulier kan u aangeven op welke mobiele nummers van uw organisatie, u de MTD-optie wenst te activeren. Op dit technisch formulier geeft u eveneens aan of u gebruik wenst te maken van de optionele initiële configuratiedienst van Proximus om de configuratie af te stemmen op uw beveiligingsbeleid.

Voor ieder mobiel nummer waarop u de MTD-optie wenst te activeren vult u het e-mailadres in van de medewerker alsook het gewenste profiel (eindgebruiker of beheerder). Merk op dat u in totaal over minimaal 1 en maximaal 5 beheerderaccounts dient te beschikken.

In het technisch bestelformulier hebt u de mogelijkheid om de activatie van de MTD optie op mobiele nummers op te splitsen in een initiële fase en een roll-outfase om u als beheerder de mogelijkheid te geven tijdens deze initiële fase om de configuratie aan te passen aan uw veiligheidsbeleid en deze af te toetsen bij een beperkt aantal gebruikers.

Indien U voor deze opsplitsing kiest, verwittigt u uw contactpersoon bij Proximus bij Proximus wanneer u klaar bent met de initiële configuratie en u wenst dat de mobiele nummers uit de roll-outfase geactiveerd worden met de MTD-optie.

Naam entiteit	Btw/KBO-nummer	Klantnummer Proximus	Mobiel nummer	E-mailadres	Profiel
Bedrijf	BE0123456789	12345678	32475727335	jan.jansen@bedrijf.be	End-user

Facturatie van de MTD-optie voor een specifiek mobiel nummer start wanneer de activatie-e-mail verzonden is voor dat nummer.

3. Activering

Nadat u het ingevulde technisch bestelformulier hebt bezorgd aan uw contactpersoon bij Proximus , zal Proximus de activeringen uitvoeren op de gevraagde mobiele nummers.

Als gevolg van deze activeringen wordt er een welkom e-mail verstuurd, naar zowel de eindgebruikers als de beheerders van de MTD optie op het mobiele contract.

3.1 Installatie van de MTD app voor eindgebruikers via MDM (optioneel)

Indien uw organisatie over een MDM (Mobile Device Management) omgeving beschikt kan u de installatie van de MTD-app (zIPS) op de mobiele toestellen van uw eindgebruikers automatisch laten gebeuren via uw MDM-oplossing. U vindt de MTD-app (zIPS) op de publieke Google Play Store and Apple Store.

3.2 Activering van Eindgebruikers

Eindgebruikers met de MTD-optie ontvangen een verwelkomingsmail, waarmee ze de MTD-app kunnen installeren en activeren op hun mobiele toestel (Android of iOS). In het geval dat de MTD-app reeds via uw MDM oplossing geïnstalleerd is, is enkel de activatie nog nodig.

Gelieve de gebruikershandleiding voor MTD eindgebruikers te raadplegen op https://proximus.be/mtduser voor meer informatie over de activering van de eindgebruikers.

3.3 Activering van de beheerder

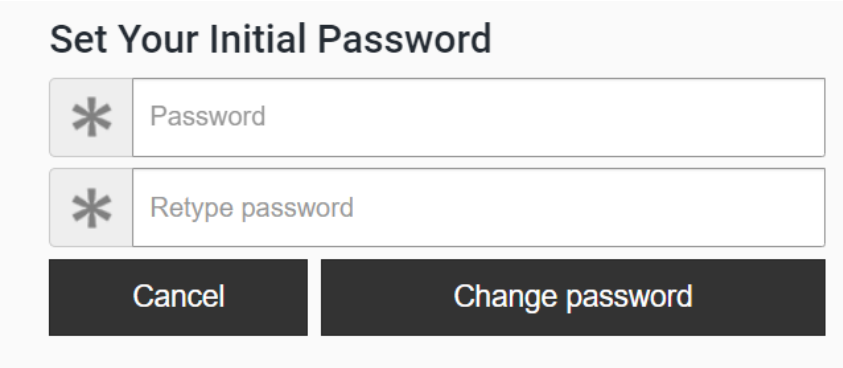
U ontvangt als beheerder van de MTD-optie een verwelkomingsmail, waarmee u de MTD-app kan installeren en activeren voor uw eigen toestel enerzijds en u uw account op het MTD-portaal kan activeren anderzijds.

Om uw account op het MTD-portaal te activeren, klikt u op de link in de ontvangen e-mail om een nieuw wachtwoord aan te vragen.

Uw toegang tot het MTD-portaal :

MTD Portal link	Userid	Wachtwoord
Portaal Link	john.doe@company.be	Klik hier en vraag een reset van uw wachtwoord om uw wachtwoord in te stellen voor uw toegang tot de MTD portaal. U dient deze reset van uw wachtwoord te doen binnen de 24 uur. Na de reset van uw wachtwoord, zal u toegang hebben tot de MTD Portaal

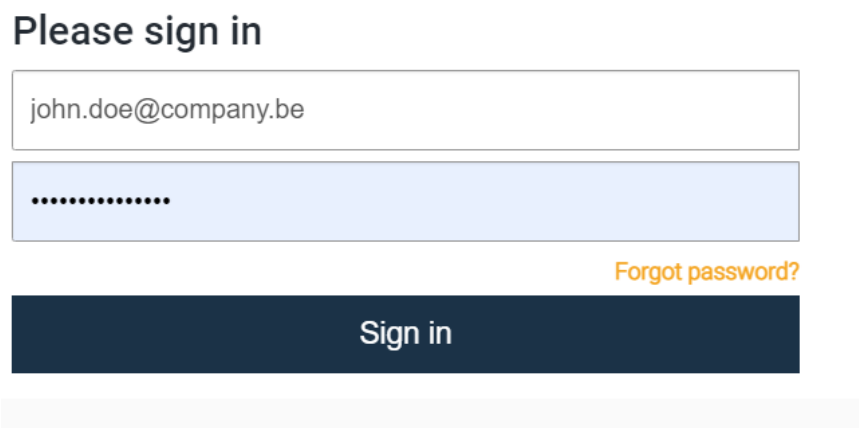
Vervolgens geeft u uw gewenste wachtwoord op het MTD-portaal en bevestigt u dit wachtwoord :



U hebt nu toegang tot het MTD-portaal via de link, het ontvangen user-id in uw verwelkomingsmail (uw e-mail adres opgegeven op het technisch bestelformulier en het zelf gekozen wachtwoord :

Uw toegang tot het MTD-portaal :

MTD Portal link	Userid	Wachtwoord
Portaal Link	john.doe@company.be	Klik hier en vraag een reset van uw wachtwoord om uw wachtwoord in te stellen voor uw toegang tot de MTD portaal. U dient deze reset van uw wachtwoord te doen binnen de 24 uur. Na de reset van uw wachtwoord, zal u toegang hebben tot de MTD Portaal



4. Beheer van de MTD-optie

4.1 MTD-app

Als beheerder hebt u zelf ook de MTD-optie actief op uw mobiele nummer. Dit betekent dat u op uw mobiele toestel de MTD-app kunt installeren en activeren.

Voor meer informatie in verband met het gebruik van de MTD-app, gelieve de MTD-gebruikershandleiding voor eindgebruikers te raadplegen die u kan downloaden via https://proximus.be/mtduser.

4.2 MTD-portaal

Via het MTD-portaal kan u dashboards en rapporten raadplegen met betrekking tot de beveiliging van de mobiele toestellen van uw organisatie waarvan de MTD-optie geactiveerd is. Het MTD-portaal laat eveneens toe om het beveiligingsbeleid van uw organisatie te configureren.

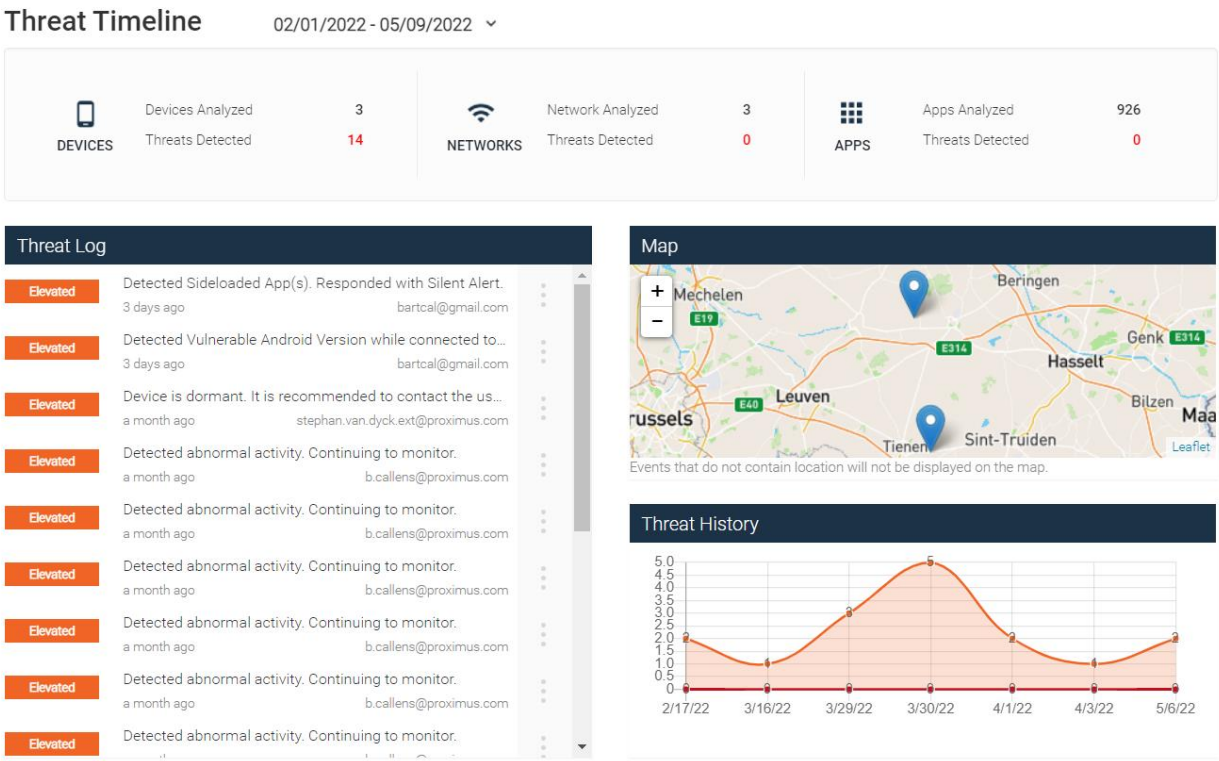
Hieronder vindt u de voornaamste functionaliteiten van het MTD-portaal. Een volledige (uitgebreidere) handleiding in het Engels kan u downloaden via https://proximus.be/mtd

4.2.1 Dashboard

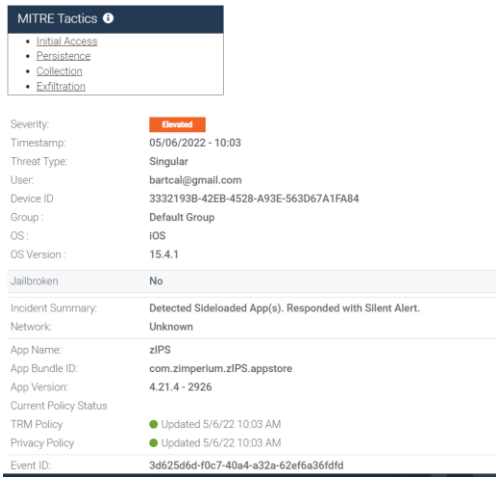
Nadat u hebt ingelogd op het MTD-portaal, komt u in een dashboard waarbij u in een oogopslag de belangrijkste informatie ziet met betrekking tot de beveiliging van de mobiele toestellen met de MTD-optie geactiveerd.

De tijdslijn bedraagt standaard 7 dagen, maar kan indien gewenst worden aangepast in het dashboard.

In het dashboard krijgt u een overzicht van het aantal toestellen, netwerken en apps die geanalyseerd zijn en hoeveel bedreigingen er zijn aangetroffen.

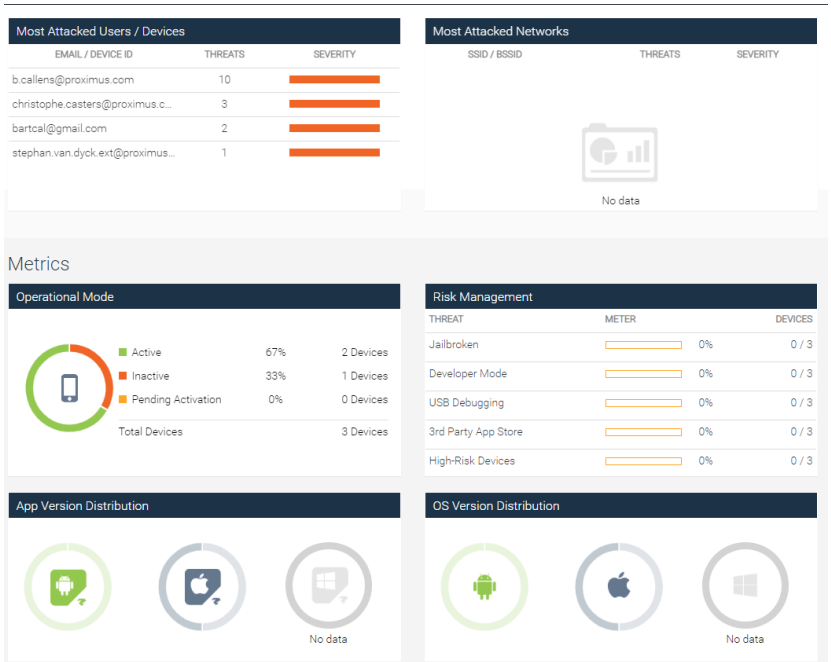


U ziet eveneens een overzicht van alle bedreigingen die tijdens de tijdslijn voorgekomen zijn. Als u op een bedreiging klikt, ziet u verdere details met betrekking tot deze bedreiging. De details die u ziet, zijn afhankelijk van de privacyinstellingen die u hebt ingesteld.



Afhankelijk van de privacyinstellingen die u hebt ingesteld, ziet u ook de locaties van de toestellen wanneer deze bedreiging zich heeft voorgedaan op een kaart gepresenteerd, evenals een trend van het aantal bedreigingen gedurende de opgegeven tijdslijn.

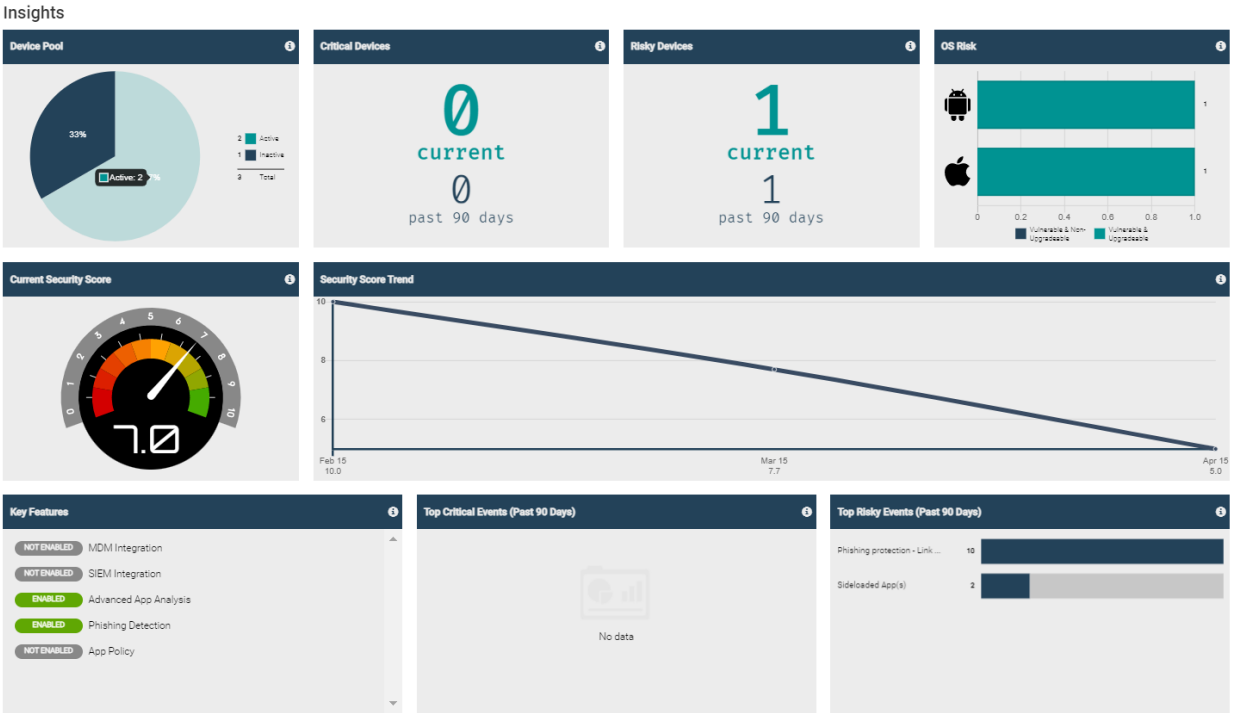
Verder ziet u bijkomende statistieken met betrekking tot de meest aangevallen gebruikers, toestellen en netwerk en bijkomende metrics met betrekking tot de mobiele toestellen waar de MTD-optie geactiveerd is.



4.2.2 Insights

De Insights tab geeft U verdere sleutelinformatie met betrekking tot de beveiliging van uw mobiele toestellen.

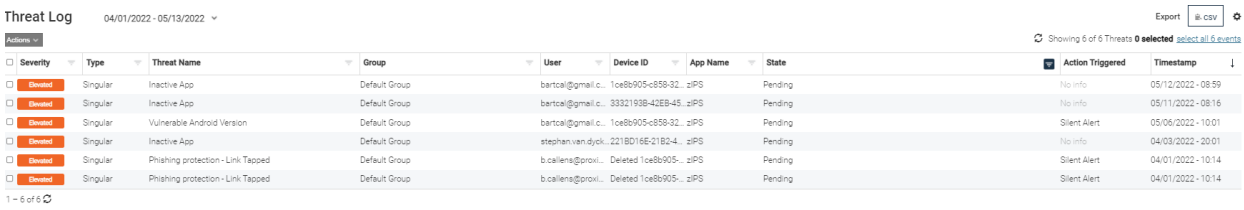
Door middel van de security score krijgt U een globaal beeld van uw beveiligingsstatus van uw mobiele toestellen, evenals de evolutie van deze beveiligingsstatus.



4.3 Threat Log

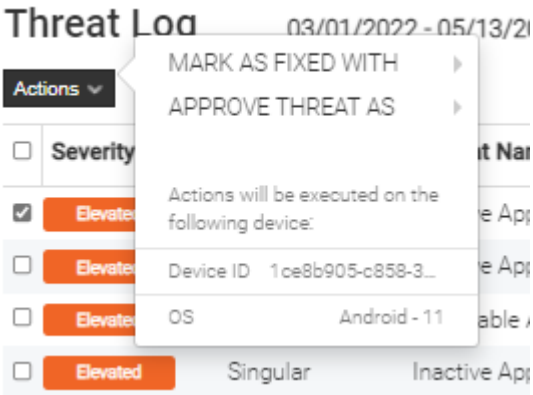
De Threat Log-tab geeft details met betrekking tot de gedetecteerde bedreigingen op uw toestel. De belangrijkste details die per bedreiging worden weergegeven, zijn :

- **Severity** :
  - **Critical** : Er heeft een echte aanval plaatsgevonden op het mobiele toestel en die vereist onmiddellijke aandacht van u als beheerder
  - **Elevated** : Er is een verhoogd risico geweest voor uw mobiele toestel, wat kan leiden tot een succesvolle aanval op het mobiele toestel
  - **Low** : Er heeft een gebeurtenis plaatsgevonden op het mobiele toestel, welke een indicatie is van een risico wat mogelijks kan leiden tot een aanval op het mobiele toestel door een kwetsbaarheid uit te buiten.
  - **Normal** : Er heeft een normale gebeurtenis plaatsgevonden op het toestel. Er is geen indicatie van een aanval, maar dit kan een aanleiding zijn om de mogelijkheid van een bedreiging te analyseren (bv. wijziging van DNS, proxy,…)
- **Type** :
  - **Singular** : er heeft een individuele bedreiging plaatsgevonden op het mobiele toestel
  - **Composite** : er hebben verschillende individuele bedreigingen samen plaatsgevonden tijdens een bepaalde tijdspanne op het mobiele toestel
- **Threat Name** : De naam van de bedreiging
- **User** : Het e-mailadres van de gebruiker gelinkt aan het mobiele toestel waarop de bedreiging zich heeft voorgedaan
- **Group** : Groep waarbinnen het mobiele toestel zich bevindt. Standaard is dit “default”.
- **DeviceID** : Uniek ID van het mobiele toestel waarop de bedreiging zich heeft voorgedaan
- **State :** De staat waarin de mitigatie van de bedreiging zich bevindt (standaard is deze “pending”)
- **Action** : Welke actie deze bedreiging getriggerd heeft
- **Timestamp** : Wanneer deze bedreiging zich voorgedaan heeft



Door op een bedreiging te klikken, kunnen verdere forensische details bekomen worden.

Een specifieke bedreiging kan worden geselecteerd en volgende mitigatie-acties kunnen worden ondernomen op deze bedreiging :

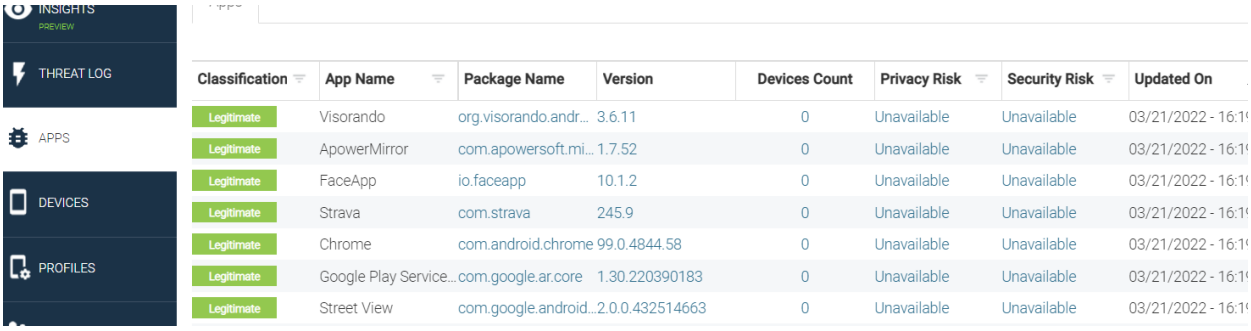


De beheerder kan de bedreiging als opgelost markeren of de bedreiging goedkeuren. De status van de bedreiging in de Threat Log zal dan gewijzigd worden.

4.4 Apps

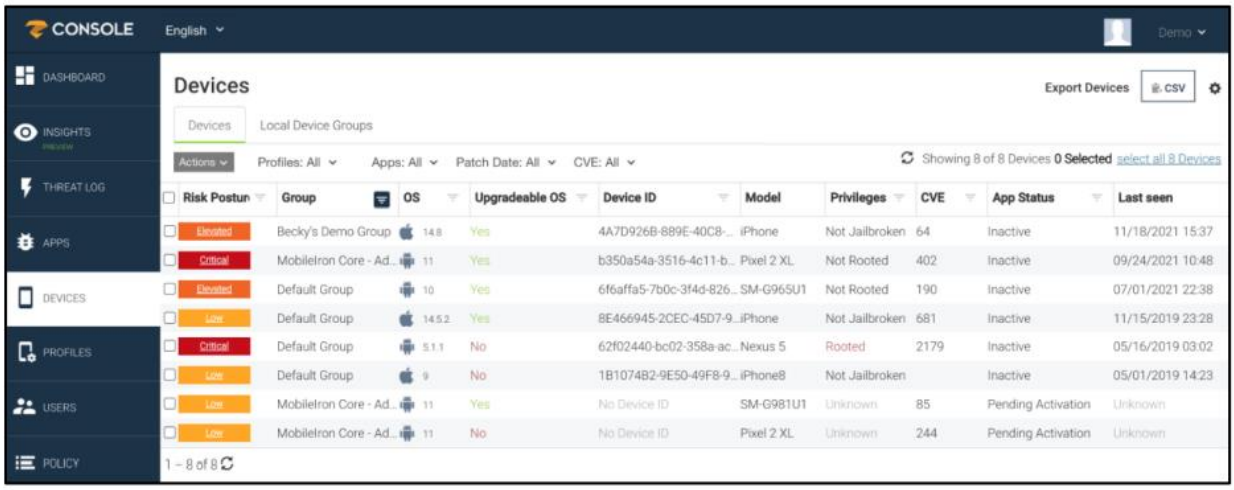
De Apps tab geeft de beheerder een overzicht van de apps geïnstalleerd op de mobiele toestellen van zijn organisatie met de MTD-optie (zIPS app) actief. Voor iedere app wordt de classificatie ("legitimate" of "malicious"), de naam van de app, de naam van de app package, de versie, op hoeveel toestellen de app geïnstalleerd is en wanneer de informatie over de app de laatste maal geüpdatet is in het MTD-portaal.

Privacy en security risk worden niet getoond vermits deze een bijkomende licentie vereisen die niet inbegrepen is in uw MTD-optie. Gelieve uw contactpersoon bij Proximus te contacteren indien u wenst deze bijkomende functionaliteit te activeren.



Classification	App Name	Package Name	Version	Devices Count	Privacy Risk	Security Risk	Updated On
Legitimate	Visorando	org.visorando.andr...	3.6.11	0	Unavailable	Unavailable	03/21/2022 - 16:1
Legitimate	ApowerMirror	com.apowersoft.mi...	1.7.52	0	Unavailable	Unavailable	03/21/2022 - 16:1
Legitimate	FaceApp	io.faceapp	10.1.2	0	Unavailable	Unavailable	03/21/2022 - 16:1
Legitimate	Strava	com.strava	245.9	0	Unavailable	Unavailable	03/21/2022 - 16:1
Legitimate	Chrome	com.android.chrome	99.0.4844.58	0	Unavailable	Unavailable	03/21/2022 - 16:1
Legitimate	Google Play Service...	com.google.ar.core	1.30.220390183	0	Unavailable	Unavailable	03/21/2022 - 16:1
Legitimate	Street View	com.google.android...	2.0.0.432514663	0	Unavailable	Unavailable	03/21/2022 - 16:1

4.5 Devices



De devices-tab geeft de beheerder een overzicht van alle mobiele toestellen binnen zijn organisatie met de MTD-optie geactiveerd. Hieronder vindt u de belangrijkste informatie die weergegeven wordt :

- **Risk Posture** : Dit veld geeft het hoogste risiconiveau aan van een bepaalde gebeurtenis voor dit mobiele toestel. Indien bijvoorbeeld het risiconiveau van een bepaald mobiele toestel "Elevated" is en er wordt een "Critical" event gedetecteerd, zal dit mobiele toestel een nieuw risiconiveau krijgen van "Critical".

- **Group :** De groep waartoe het mobiele toestel behoort. Standaard is dit de default group

- **OS :** Besturingssysteem, inclusief de versie

- **Upgradeable OS :** indicatie of het huidige besturingssysteem kan worden geüpgraded.

- **Device ID :** Identifier van het mobiele toestel

- **Model :** Model van het mobiele toestel (bv. iPhone, Nexus 5, …)

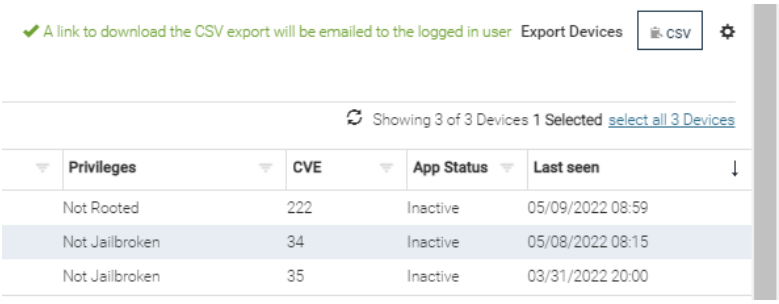
- **Privileges :** privileges van het mobiele toestel (bijvoorbeeld jailbroken of rooted)

- **CVE's** : het aantal CVE's (Common Vulnerabilities and Exposures) van de versie van het besturingssysteem van het mobiele toestel

- **App status** : Status van de MTD-app (zIPS) op het mobiele toestel

- **Last seen** : Laatste tijdstip waarop er synchronisatie geweest is tussen het mobiele toestel en het MTD-platform.

U kan dit overzicht eveneens naar een csv-bestand exporteren. Wanneer u op CSV klikt wordt een e-mail verzonden met dit csv-bestand in een attachment naar de beheerder die ingelogd is.



4.6 Profiles

Niet van toepassing

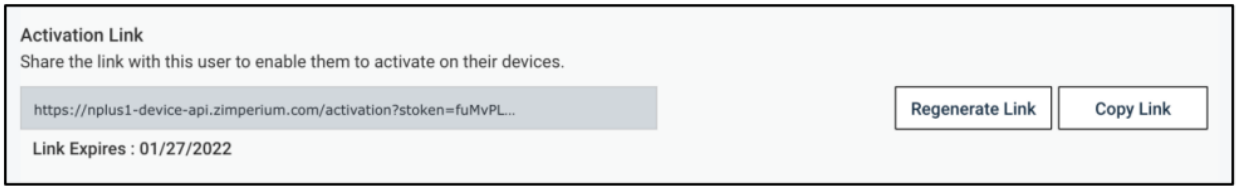
4.7 Users

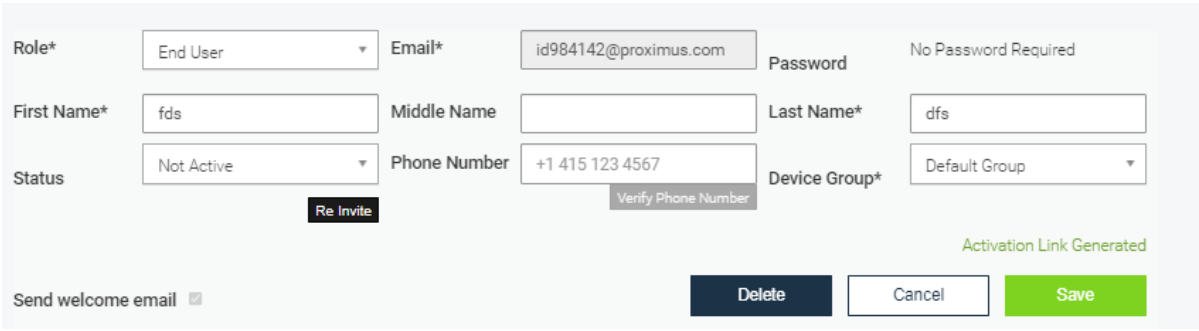
Indien een gebruiker zijn activatielink verloren heeft of de geldigheid van zijn activatielink is verlopen, kan u de bestaande activatie-link opnieuw sturen naar de gebruiker of een nieuwe activatielink genereren voor de gebruiker via de User-tab.

Belangrijk : Creëer geen nieuwe gebruikers, verwijder geen gebruikers of verander geen profiel van bestaande gebruikers via het MTD-portaal. Indien U nieuwe gebruikers wenst toe te voegen, te verwijderen of profielen te wijzigen , gelieve uw contactpersoon bij Proximus te contacteren!

Indien gebruikers veranderen van mobiel toestel of de MTD-app gedesinstalleerd hebben op hun huidige toestel en dit terug wensen te installeren, dient de MTD-optie opnieuw geactiveerd te worden.

Indien de oorspronkelijke link vervallen is (standaard is er een geldigheidsperiode van 7 dagen), dient u als beheerder deze link opnieuw te genereren via het portaal. U kan dan de nieuwe link kopiëren en deze aan de gebruiker bezorgen of u kan ervoor kiezen om de gebruiker opnieuw uit te nodigen (re-invite). De gebruiker krijgt dan een e-mail met de nieuwe activatielink.





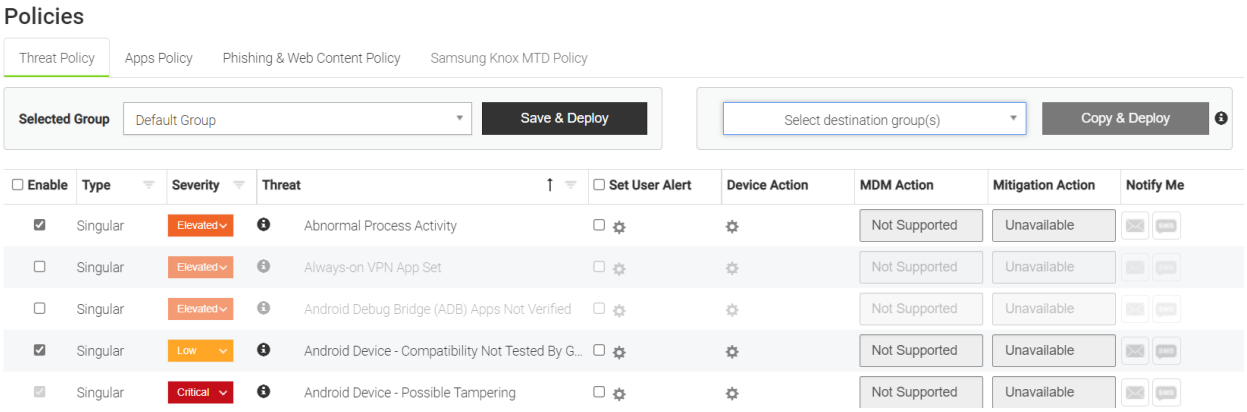
4.8 Policy

In de Policy-tab kan u als beheerder de security policy instellen met betrekking tot beveiligingsbedreigingen.

Merk op dat de Apps Policy en Samsung Knox Policy niet van toepassing zijn.

4.8.1 Threat Policy

In de Threat Policy-tab kan u definiëren welke detecties u wenst te activeren voor verschillende bedreigingen. Dit doet u door het vakje in de kolom “Enable” naast de desbetreffende bedreiging aan te vinken.



Verder kan u indien gewenst, het risiconiveau van een bedreiging aanpassen, een alarm voor de eindgebruiker instellen, een gewenste actie van het mobiele toestel definiëren of een notificatie naar u als beheerder via e-mail of sms laten sturen wanneer deze bedreiging zich voordoet op een mobiel toestel van uw gebruikers.

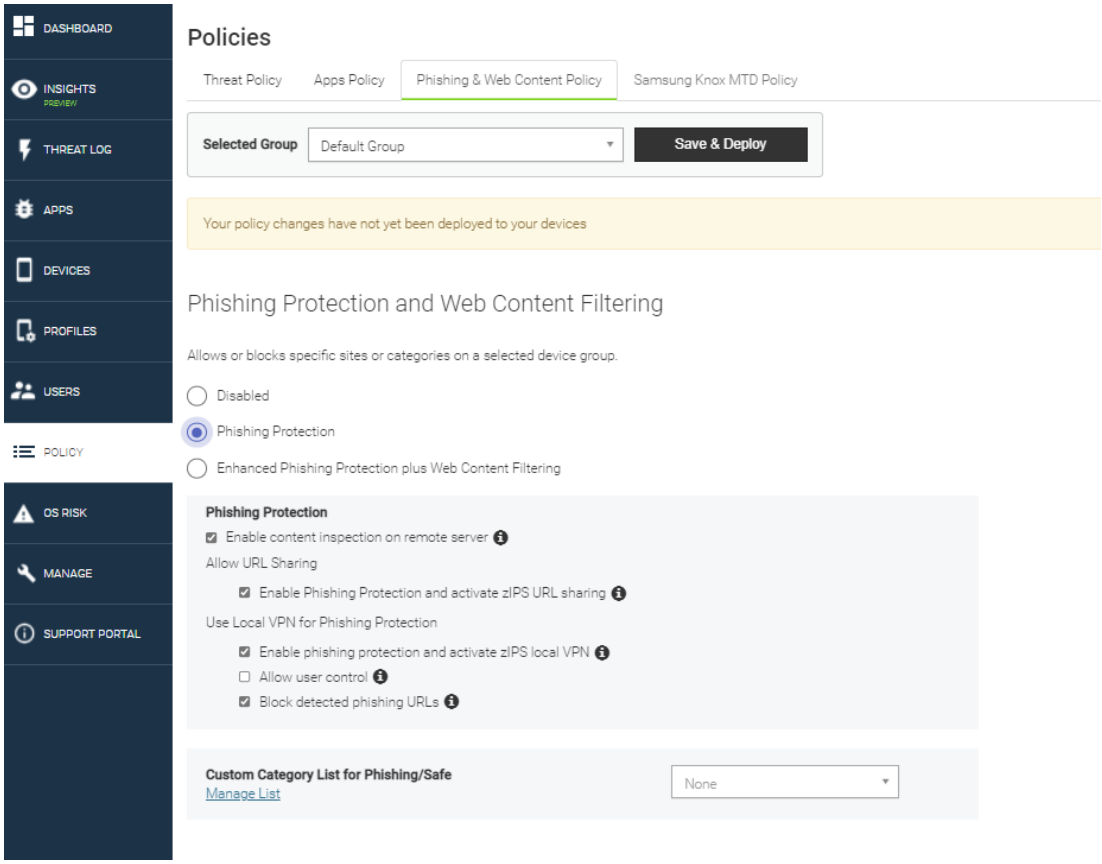
4.8.2 Phishing & Web Content Policy

In de Phishing & Web Content Policy tab kan u als beheerder configureren of u uw gebruikers wenst te beveiligen tegen phishing en/of filtering wenst toe te passen met betrekking tot de webinhoud die geraadpleegd wordt door uw gebruikers via hun mobiele toestel. Indien u meerdere groepen gedefinieerd heeft, kunt u deze instellingen per groep aanpassen.

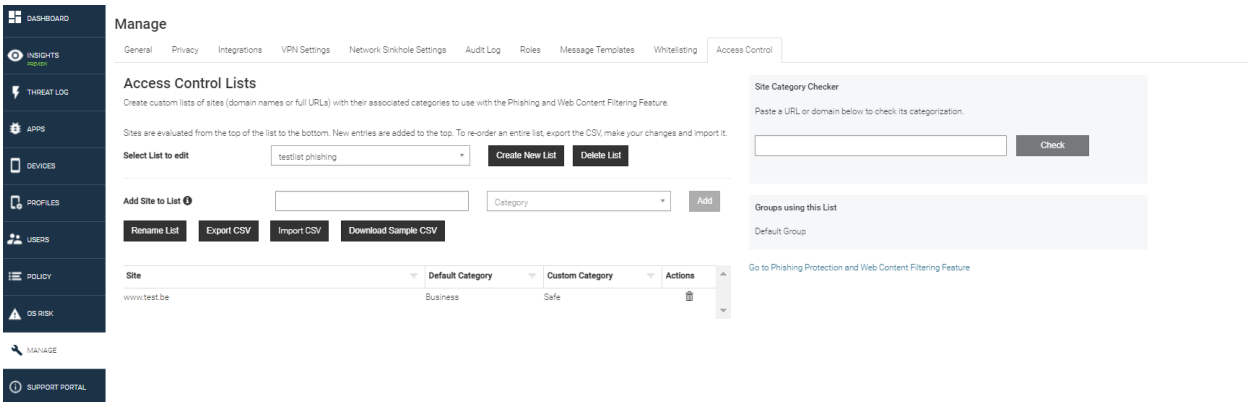
Indien u “**Phishing Protection**” aanvinkt, hebt u verder de mogelijkheid om aan te geven op welke manier u uw gebruikers wenst te beveiligen tegen phishing.

- **Enable content inspection on remote server :** Als u deze optie aanvinkt, zal, bovenop de lokale on-device analyse, er een remote analyse gebeuren van mogelijke phishing-URL’s.
- **Enable Phishing Protection and activate zIPS URL sharing** : Als u deze optie aanvinkt, zullen uw gebruikers de mogelijkheid hebben om d.m.v. lang op een URL te klikken op hun mobiele toestel, deze te laten analyseren op phishing.
- **Enable Phishing Protection and activate zIPS local VPN :** Als u deze optie aanvinkt, zal op de toestellen van uw gebruikers een lokale VPN gestart worden om de analyse te maken van mogelijke phishing-URL’s.

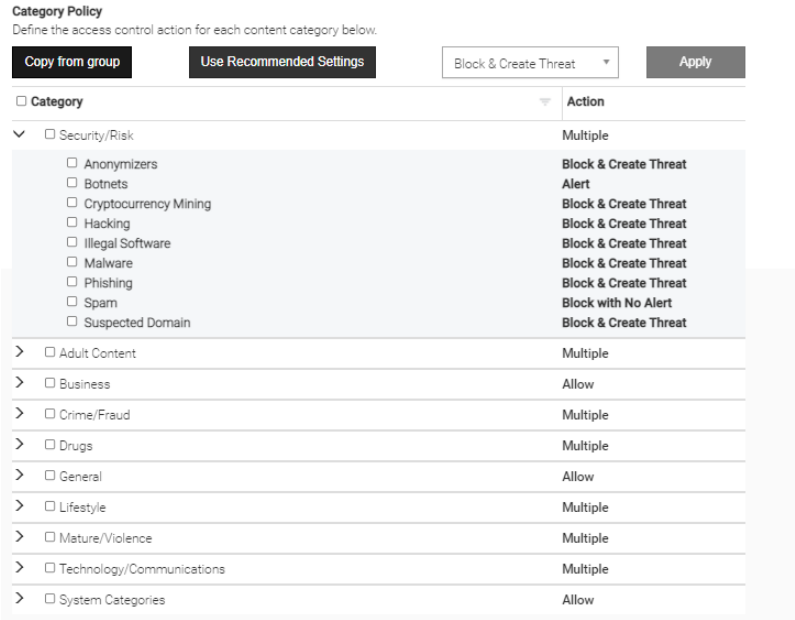
- **Allow User Control** : Als u deze optie aanvinkt, zullen uw gebruikers de mogelijkheid hebben om zelf de beveiliging tegen phishing te activeren en desactiveren op hun mobiele toestel.
- **Block Deteted phishing URL's** : Als u deze optie aanvinkt, zullen gedecteerde phishing URL's, geblokkeerd worden op de mobiele toestellen van uw gebruikers.



Indien u bepaalde URL's een aangepaste categorisatie wenst mee te geven (bv. om deze uit te sluiten van een phishing-categorisatie), klikt u op Manage List. Hierbij kunt u een Access Control List aanmaken met domeinen en deze als veilig categoriseren.

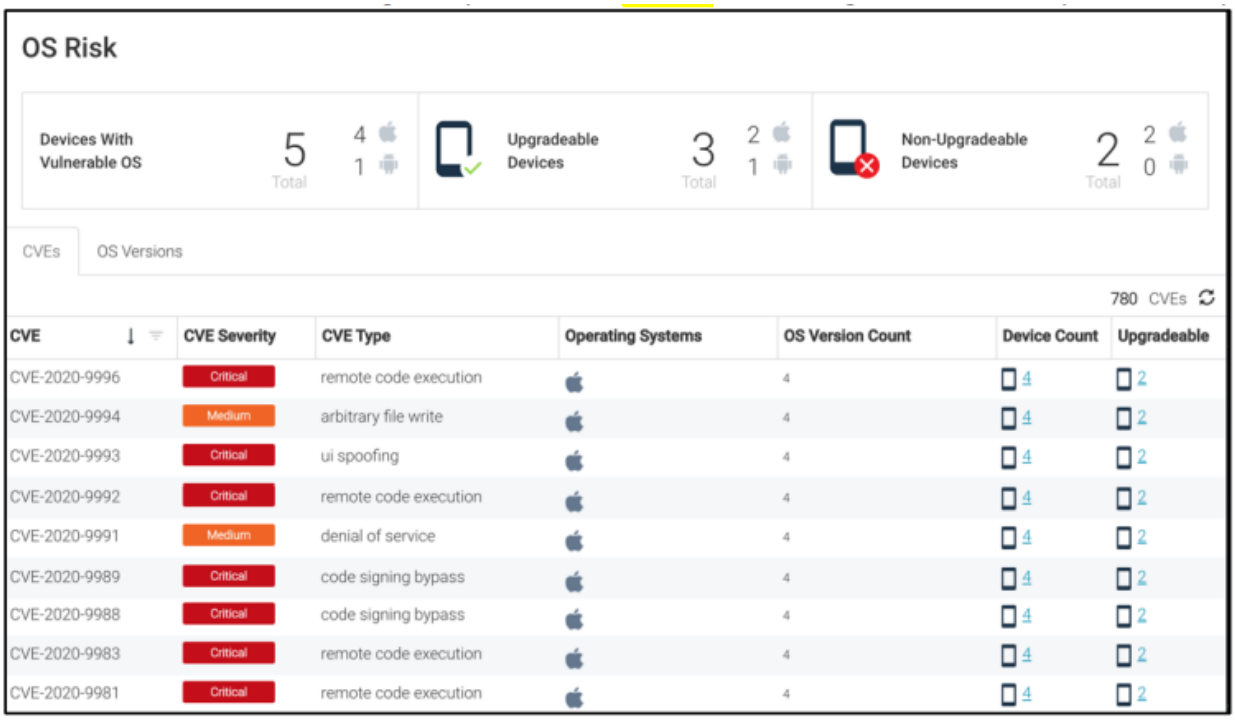


Indien u **Enhanced Phishing Protection and Web Content Filtering** aanvinkt kan u bijkomend bij de beveiliging tegen phishing, per categorie van webinhoud bepalen welke actie er ondernomen dient te worden, wanneer uw gebruikers op hun mobiele toestel deze webinhoud wensen op te vragen.



4.9 OS Risk

In de OS Risk-tab hebt u als beheerder een overzicht van alle kwetsbaarheden (CVE's) van de verschillende versies van de besturingssystemen op de mobiele toestellen van uw gebruikers. U ziet eveneens hoeveel toestellen kwetsbaar zijn en hoeveel daarvan geüpgradet kunnen worden.



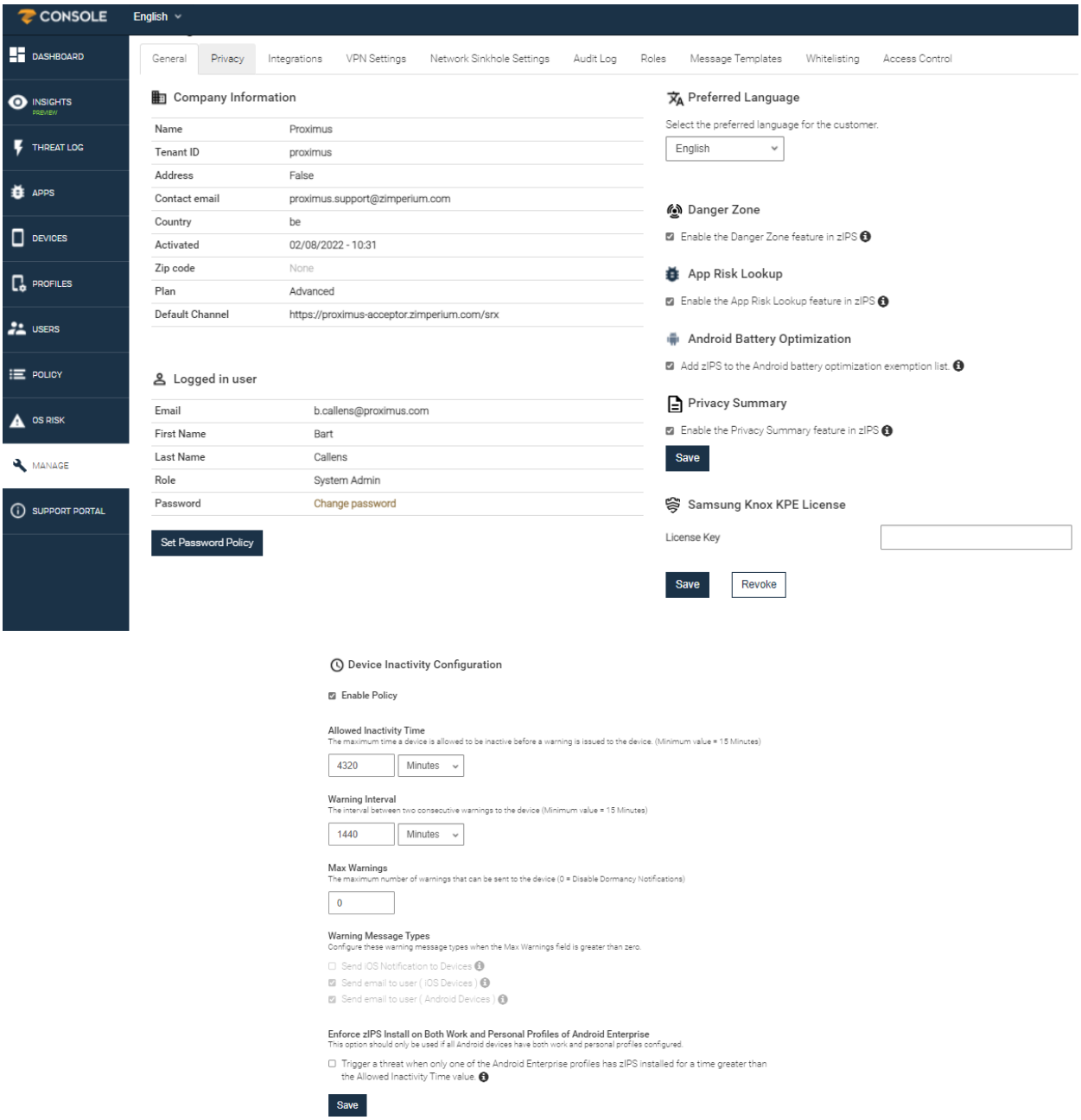
CVE	CVE Severity	CVE Type	Operating Systems	OS Version Count	Device Count	Upgradeable
CVE-2020-9996	Critical	remote code execution		4	4	2
CVE-2020-9994	Medium	arbitrary file write		4	4	2
CVE-2020-9993	Critical	ui spoofing		4	4	2
CVE-2020-9992	Critical	remote code execution		4	4	2
CVE-2020-9991	Medium	denial of service		4	4	2
CVE-2020-9989	Critical	code signing bypass		4	4	2
CVE-2020-9988	Critical	code signing bypass		4	4	2
CVE-2020-9983	Critical	remote code execution		4	4	2
CVE-2020-9981	Critical	remote code execution		4	4	2

4.10 Manage

In de Manage-tab kan de beheerder verschillende settings aanpassen. De belangrijkste settings worden hieronder weergegeven.

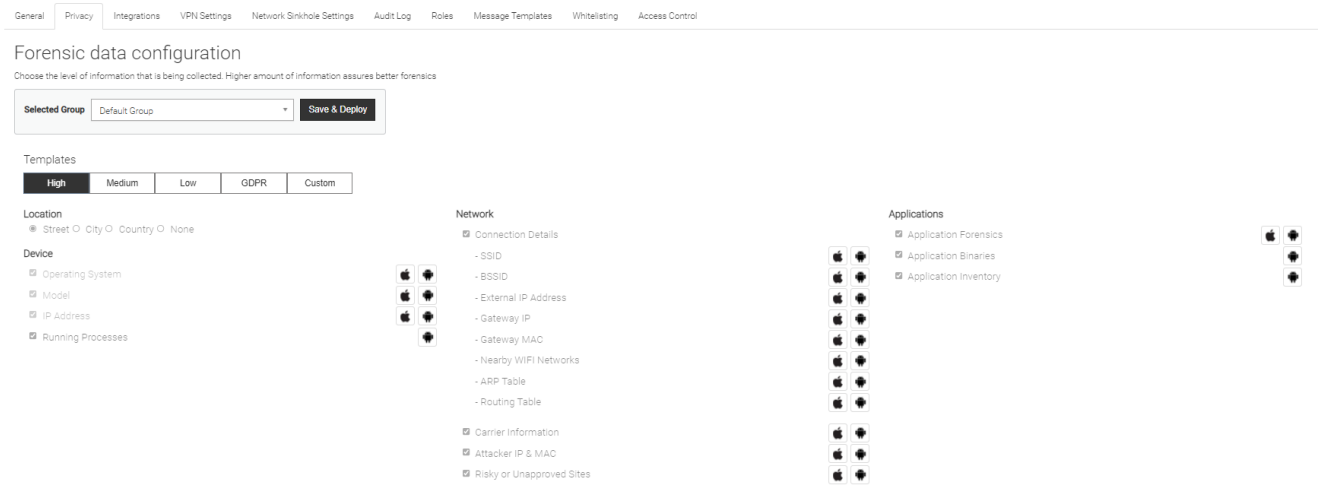
4.10.1 General

Hier kunt u algemene settings aanpassen, zoals het wachtwoordbeleid om aan te loggen op het MTD-pPortaal, uw voorkeur van taal van het MTD-portaal, de visualisatie van bepaalde items in de MTD-aApp (Danger Zone, App Risk Lookup, Pricacy Summary) en de policy m.b.t. inactiviteit van de MTD-app op de mobiele toestellen van uw gebruikers.



4.10.2 Privacy

Hier kunt u privacy-settings aanpassen met betrekking tot welke gegevens er vanuit de MTD-app (zIPS) met het MTD-platform gedeeld worden voor forensische doeleinden.



4.10.3 Integrations

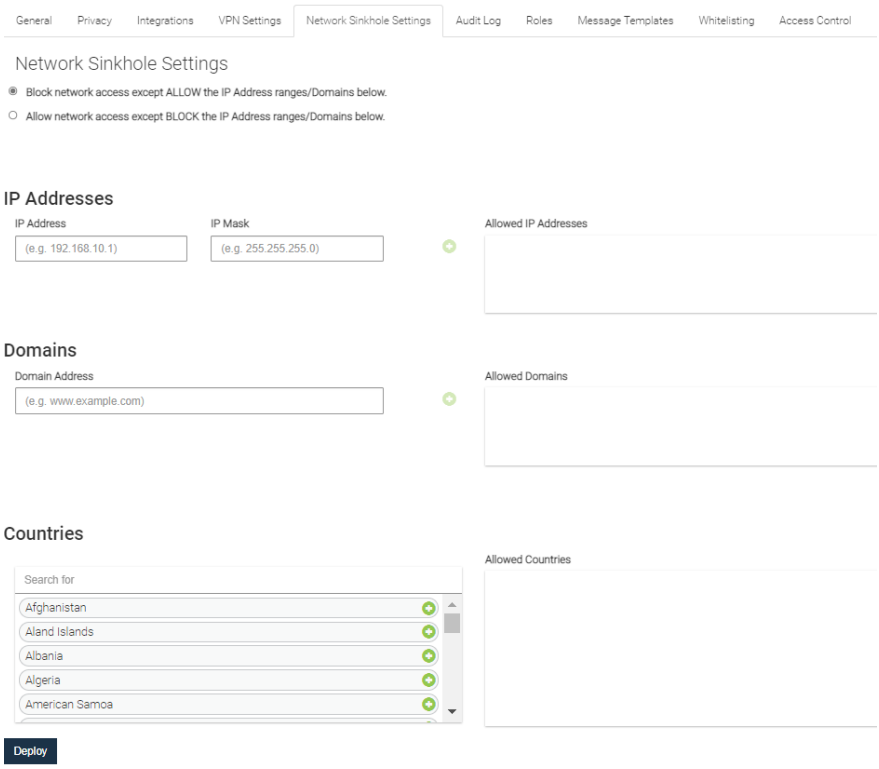
Niet van toepassing

4.10.4 VPN Settings

Niet van toepassing

4.10.5 Network Sinkhole settings

Hier kan U definiëren welke IP-adressen, domeinen of landen dienen toegestaan of geblokkeerd te worden vanaf de mobiele toestellen van uw gebruikers wanneer bepaalde bedreigingen zich voordoen, zoals gedefinieerd in de Threat Policy.



4.10.6 Audit Logs

Hier ziet u een overzicht van verschillende activiteiten op het MTD-platform, zoals bv. het creëren en inloggen van beheerderaccounts en het wijzigen van policy's.

4.10.7 Roles

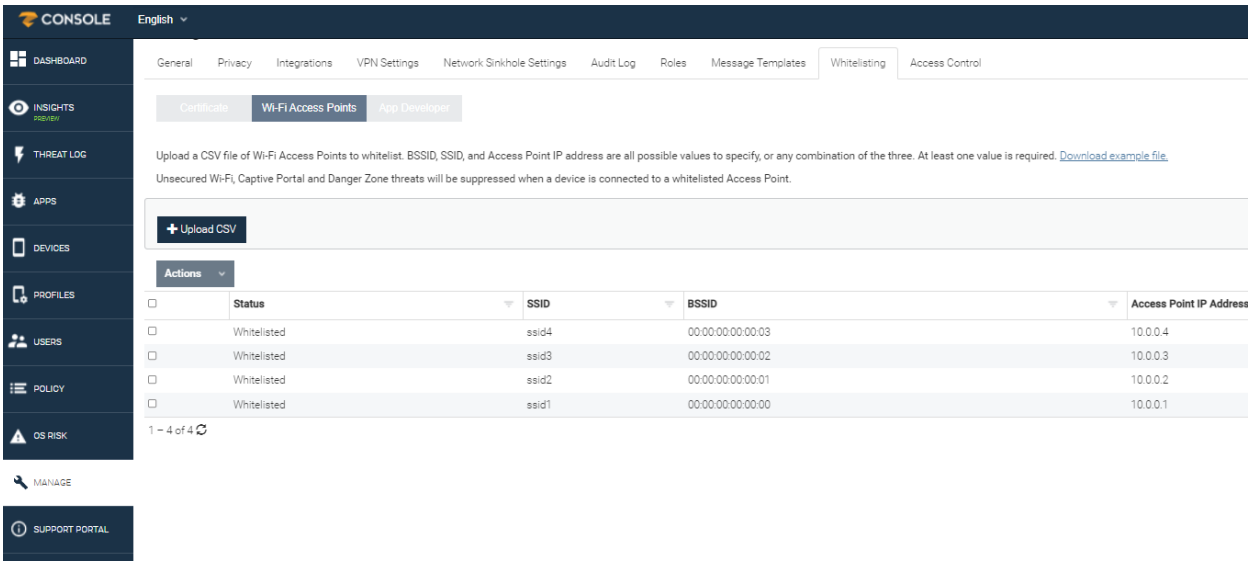
Gelieve de roles niet aan te passen. Aanpassen van de Roles kan als gevolg hebben dat bepaalde toegangen tot het platform niet meer correct werken.

4.10.8 Message Templates

Gelieve de Message Templates niet aan te passen. Aanpassen van deze Message Templates kan als gevolg hebben dat bepaalde funtionaliteiten (bv. re-invite van gebruikers) niet meer correct werken.

4.10.9 Whitelisting

In deze sectie kan u digitale certificaten, Wi-Fi Access points of Apps whitelisten. Detectie van gerelateerde bedreigingen gedefinieerd in de Threat Policy zal dan onderdrukt worden.



4.10.10 Access Control List

Hier kan u lijsten definiëren die gebruikt kunnen worden in de Phishing & Web Content Policy.

4.11 Support Portal

Wanneer u hier op klikt komt u op de Proximus MTD-supportpagina terecht.

Wanneer u als beheerder ondersteuning nodig heeft, kan u de nodige ondersteuningsinformatie raadplegen op https://proximus.be/mtd . Indien u daar de nodige informatie niet vindt kan u, als beheerder, contact opnemen met uw contactpersoon bij Proximus .

Merk op dat Proximus geen ondersteuning biedt met betrekking tot mobiele toestellen die “rooted“ of “jailbroken” zijn.

5. Veel voorkomende vragen

5.1 Initiële link van uw beheerdersaccount is vervallen

Bij het aanmaken van uw account op het MTD-portaal, krijgt u bij de reset van uw wachtwoord een boodschap dat de link vervallen is *(your link has expired. Please obtain a new reset password link)*. Dit kan voorvallen vermits deze link wegens veiligheidsredenen slechts 24 uur geldig is.

Gelieve in dat geval een andere beheerder binnen uw organisatie te contacteren om u een nieuwe link te bezorgen.
Indien u de enige actieve beheerder bent binnen uw organisatie, gelieve Proximus te contacteren om u een nieuwe link te bezorgen.

5.2 Aanpassen van het profiel van gebruikers

U wenst één of meer eindgebruikers beheerrechten te geven of de beheerrechten van één of meer beheerders te verwijderen.

Gelieve in dat geval uw contactpersoon bij Proximus te contacteren. Deze zal de bestaande MTD-optie voor deze gebruiker verwijderen en een nieuwe MTD-optie activeren voor deze gebruiker met de aangepaste rechten.

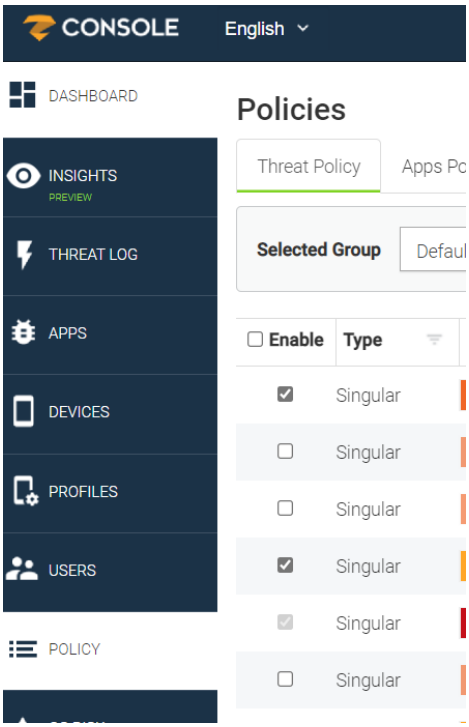
5.3 Hoeveel mobiele toestellen kan ik beveiligen met de MTD-optie?

De MTD optie is gekoppeld aan een mobiel nummer. U kan enkel het mobiel toestel beveiligen gekoppeld aan dit mobiele nummer. Indien uw gebruiker verandert van mobiele toestel, dient u de gebruiker een nieuwe activatielink te bezorgen, zoals beschreven in Users.

5.4 Een eindgebruiker contacteert mij met volgende boodschap in zijn MTD-app : 'Server verification incomplete'.

Dit betekent dat u de phishing policy geactiveerd heeft, maar niet de overeenkomstige detecties.
Ga hiervoor naar de Threat Policy en vink de volgende bedreigingsdetecties aan :

- Risky Site - Link Tapped
- Risky Site - Link Visited
- Risky Site - Blocked
- Site Blocked
- Site Blocked - Link Tapped
- Site Blocked - Link Visited


CONSOLE
English
DASHBOARD
INSIGHTS
PREVIEW
THREAT LOG
APPS
DEVICES
PROFILES
USERS
POLICY
Policies
Threat Policy
Apps Pc
Selected Group
Defaul
Enable
Type
Singular
Singular
Singular
Singular
Singular
Singular