

# Beheerdershandleiding

# Mobile Threat Defense (MTD)

Datum Onze referentie Contact E-mail

#### 01/05/2022

MTD\_Beheerdershandleiding Bart Callens b.callens@proximus.com



# Inhoud

Inł	noud	1
O٧	verzicht	3
1.	Beschrijving van de dienst	4
2.	Aanvraag MTD-optie	5
	2.1 Voorafgaand	5
	2.2 Technisch bestelformulier	5
З.	Activering	6
	3.1 Installatie van de MTD app voor eindgebruikers via MDM (optioneel)	6
	3.2 Activering van Eindgebruikers	6
	3.3 Activering van de beheerder	6
4.	Beheer van de MTD-optie	8
	4.1 MTD-app	8
	4.2 MTD-portaal	8
	4.2.1 Dashboard	8
	4.2.2 Insights	10
	4.3 Threat Log	11
	4.4 Apps	12
	4.5 Devices	12
	4.6 Profiles	14
	4.7 Users	14
	4.8 Policy	15
	4.8.1 Threat Policy	15
	4.8.2 Phishing & Web Content Policy	15
	4.9 OS Risk	17
	4.10Manage	18
	4.10.1General	18
	4.10.2 Privacy	19
	4.10.3 Integrations	20
	4.10.4 VPN Settings	20

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



	4.10.	5 Network Sinkhole settings	20
	4.10.	5 Audit Logs	21
	4.10.	7 Roles	21
	4.10.	8 Message Templates	21
	4.10.	9 Whitelisting	21
	4.10.	10 Access Control List	22
	4.11 Sup	port Portal	22
5.	Veel v	oorkomende vragen	.23
	5.1 Initi	ele link van uw beheerdersaccount is vervallen	23
	5.1 Initi 5.2 Aar	ële link van uw beheerdersaccount is vervallen passen van het profiel van gebruikers	23 23
	<ul><li>5.1 Initi</li><li>5.2 Aar</li><li>5.3 Hoe</li></ul>	ële link van uw beheerdersaccount is vervallen passen van het profiel van gebruikers veel mobiele toestellen kan ik beveiligen met de MTD-optie?	23 23 23



# 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 <u>https://proximus.be/mtd</u>.

Een handleiding voor uw eindgebruikers van de MTD optie is beschikbaar op <u>https://proximus.be/mtduser</u>.



# 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.

		Klantnummer	Mobiel		
<u>Naam entiteit</u>	Btw/KBO-nummer	<b>Proximus</b>	nummer	E-mailadres	<b>Profiel</b>
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 <u>https://proximus.be/mtduser</u> 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
<u>Portaal Link</u>	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 <u>MTD Portaal</u>

Proximus NV van publiek recht, Koning Albert II-laan 27, B-1030 Brussel, België BTW BE 0202.239.951, RPR Brussel, BE50 00017100 3118 BP0TBEB1



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

#### Set Your Initial Password



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
		Klik hier en vraag een reset van uw wachtwoord om uw wachtwoord in te stellen voor uw toegang tot de
<u>Portaal Link</u>	john.doe@company.be	van uw wachtwoord te doen binnen de 24 uur. Na de reset van uw wachtwoord, zal u toegang hebben tot de <u>MTD Portaal</u>

#### Please sign in

john.doe@company.be		
•••••		
		Forgot password?
	Sign in	



# 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 <u>https://proximus.be/mtduser</u>.

#### 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 <u>https://proximus.be/mtd</u>

#### 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 MTDoptie 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 <u>privacyinstellingen</u> die u hebt ingesteld.

MITRE Tactics ()	
Initial Access     Persistence     Collection     Exfiltration	
Severity:	Elevated
Timestamp:	05/06/2022 - 10:03
Threat Type:	Singular
User:	bartcal@gmail.com
Device ID	3332193B-42EB-4528-A93E-563D67A1FA84
Group :	Default Group
OS:	iOS
OS Version :	15.4.1
Jailbroken	No
Incident Summary:	Detected Sideloaded App(s). Responded with Silent Alert.
Network:	Unknown
App Name:	zIPS
App Bundle ID:	com.zimperium.zIPS.appstore
App Version:	4.21.4 - 2926
Current Policy Status	
TRM Policy	Updated 5/6/22 10:03 AM
Privacy Policy	Updated 5/6/22 10:03 AM
Event ID:	3d625d6d-f0c7-40a4-a32a-62ef6a36fdfd

Afhankelijk van de <u>privacyinstellingen</u> 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.



Most Attacked Us	ers / Devices			Most Attacked Netwo	rks		
EMAIL / DEVIC	E ID THREATS		SEVERITY	SSID / BSSID	THREATS	SEVERIT	γ
b.callens@proximus.	com 10						
christophe.casters@p	proximus.c 3	-					
bartcal@gmail.com	2						
stephan.van.dyck.ext	@proximus 1				<b>G</b> II		
					No data		
Metrics							
Operational Mode				Risk Management			
				THREAT	METER		DEVICES
	Active	67%	2 Devices	Jailbroken		0%	0/3
	Inactive	33%	1 Devices	Developer Mode		0%	0/3
	Pending Activation	0%	0 Devices	USB Debugging		0%	0/3
	Total Devices		3 Devices	3rd Party App Store		0%	0/3
				High-Risk Devices		0%	0/3
App Version Distri	bution			OS Version Distributio	n		
0,		(	No data	۰	Ű	No data	

#### 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.

Device Pool 6	Critical Devices	Ð F	Risky Devices	6	OS Risk		0
33% 2 1 2 104 2 104	Current O past 90 days		<b>1</b> past 90 days			0.4 00 0.0 Uneversit L	1
Current Security Score	Security Score Trend						0
	8 6 Feb 15 10.0		Mar 15 7.7				Apr 15 5.0
Key Features	🔁 Top Cr	itical Events (Past 90 Days)	6	Top Risky Events (Pa	st 90 Days)		0
INTENSED         MOM Integration           INTENSED         SEM Integration           BNAD         Advanced App Analysis           BNAD         Philping Detection           INTENSED         App Policy	*	No data		Phishing protection - Lini Sideloaded App(s)	c 10 2		

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



#### 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

Threat Actions ~	Threat Log         04/01/2022-05/13/2022 v           Automs v         C Showing 6 of 6 Treess 0 cells							Export R.csv ¢		
Sever	ty –	Туре	Threat Name	Group		- Device ID -	App Name	State	Triggered	Timestamp ↓
C Bee	ted	Singular	Inactive App	Default Group	bartcal@gma	I.c 1ce8b905-c858-32	ziPS	Pending		05/12/2022 - 08:59
🗆 🛛 🖬 🖬	ted	Singular	Inactive App	Default Group	bartcal@gma	il.c 33321938-42EB-45	5zIPS	Pending		05/11/2022 - 08:16
C Bee	ted	Singular	Vulnerable Android Version	Default Group	bartcal@gma	I.c 1ce8b905-c858-32	zIPS	Pending	Silent Alert	05/06/2022 - 10:01
- Bee	ted	Singular	Inactive App	Default Group	stephan.van.e	lyck221BD16E-21B2-4	zIPS	Pending	No info	04/03/2022 - 20:01
🗆 🛛 Bee	ted	Singular	Phishing protection - Link Tapped	Default Group	b.callens@pr	xi Deleted 1ce8b905-	zIPS	Pending	Silent Alert	04/01/2022 - 10:14
O Bee	ted	Singular	Phishing protection - Link Tapped	Default Group	b.callens@pr	xi Deleted 1ce8b905-	zIPS	Pending	Silent Alert	04/01/2022 - 10:14

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 :



Τŀ	Threat Loa 03/01/2022 - 05/13/20							
		MARK AS FIXE	D WITH	•				
Act	ions	APPROVE THR	EAT AS	•				
	Severity			ıt Nar				
	Elevater	Actions will be ex following device:	ecuted on the	e Ap;				
	Elevated	Device ID 1 ce8	o905-c858-3	e App				
	Elevater	OS	Android - 11	able /				
	Elevated	Singular	Ina	active App				

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.

Image: THREAT LOG       Classification       App Name       Package Name       Version       Devices Count       Privacy Risk       Security Risk       Updated On         # APPS       Legitimate       Visorando       org visorando.andr       3.6.11       0       Unavailable       Unavailable       03/21/2022-16.11         Legitimate       Apower/Mirror       com.apowersoft.mi17.52       0       Unavailable       Unavailable       03/21/2022-16.11         Devices       Legitimate       FaceApp       io.faceapp       10.1.2       0       Unavailable       Unavailable       03/21/2022-16.11         Legitimate       Strava       com.strava       245.9       0       Unavailable       Unavailable       03/21/2022-16.11         Legitimate       Chrome       com.android.chrome 99.0.4844.58       0       Unavailable       03/21/2022-16.11         Legitimate       Google Play Servicecom.google.ar.core       1.30.220390183       0       Unavailable       03/21/2022-16.11         Legitimate       Street View       com.google.android2.0.0432514663       0       Unavailable       Unavailable       03/21/2022-16.11	U	PREVIEW								
Legitimate       Visorando       org.visorando.andr       3.6.11       0       Unavailable       Unavailable       03/21/2022 - 16.7         Legitimate       ApowerMirror       com.apowersoft.mi 1.7.52       0       Unavailable       Unavailable       03/21/2022 - 16.7         Detvices       Legitimate       FaceApp       io.faceapp       10.1.2       0       Unavailable       Unavailable       03/21/2022 - 16.7         Legitimate       Strava       com.strava       245.9       0       Unavailable       Unavailable       03/21/2022 - 16.7         Legitimate       Chrome       com.android.chrome 99.0.4844.58       0       Unavailable       Unavailable       03/21/2022 - 16.7         Legitimate       Google Play Servicecom.google.ar.core       1.30.220390183       0       Unavailable       Unavailable       03/21/2022 - 16.7         Legitimate       Street View       com.google.ar.core       1.30.220390183       0       Unavailable       03/21/2022 - 16.7	¥	THREAT LOG	Classification =	App Name 📼	Package Name	Version	Devices Count	Privacy Risk 📼	Security Risk =	Updated On
Image: AppS       Legitimate       Apower/Mirror       com.apowersoft.mi 1.7.52       0       Unavailable       Unavailable       03/21/2022-16:7         Image: Devices       Legitimate       FaceApp       io.faceapp       10.1.2       0       Unavailable       Unavailable       03/21/2022-16:7         Legitimate       Strava       com.strava       245.9       0       Unavailable       Unavailable       03/21/2022-16:7         Legitimate       Chrome       com.android.chrome 99.0.4844.58       0       Unavailable       Unavailable       03/21/2022-16:7         Legitimate       Google Play Servicecom.google.ar.core       1.30.220390183       0       Unavailable       Unavailable       03/21/2022-16:7         Legitimate       Street View       com.google.android2.0.0.432514663       0       Unavailable       Unavailable       03/21/2022-16:7			Legitimate	Visorando	org.visorando.andr	3.6.11	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 Servicecom.google.ar.core       1.30.220390183       0       Unavailable       Unavailable       03/21/2022-16:1         Legitimate       Street View       com.google.android2.0.0.432514663       0       Unavailable       Unavailable       03/21/2022-16:1	9	APPS	Legitimate	ApowerMirror	com.apowersoft.mi	. 1.7.52	0	Unavailable	Unavailable	03/21/2022 - 16:19
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 Servicecom.google.ar.core       1.30.220390183       0       Unavailable       Unavailable       03/21/2022 - 16:1         Legitimate       Street View       com.google.android2.0.0.432514663       0       Unavailable       Unavailable       03/21/2022 - 16:1			Legitimate	FaceApp	io.faceapp	10.1.2	0	Unavailable	Unavailable	03/21/2022 - 16:19
Legitimate         Chrome         com.android.chrome 99.0.4844.58         0         Unavailable         Unavailable         03/21/2022-16:1           Legitimate         Google Play Servicecom.google.ar.core         1.30.220390183         0         Unavailable         Unavailable         03/21/2022-16:1           Legitimate         Street View         com.google.android2.0.0.432514663         0         Unavailable         Unavailable         03/21/2022-16:1		DEVICES	Legitimate	Strava	com.strava	245.9	0	Unavailable	Unavailable	03/21/2022 - 16:19
Legitimate         Google Play Servicecom.google.ar.core         1.30.220390183         0         Unavailable         Unavailable         03/21/2022 - 16:1           Legitimate         Street View         com.google.android2.0.0.432514663         0         Unavailable         Unavailable         03/21/2022 - 16:1	_		Legitimate	Chrome	com.android.chrome	99.0.4844.58	0	Unavailable	Unavailable	03/21/2022 - 16:19
Legitimate         Street View         com.google.android2.0.0.432514663         0         Unavailable         Unavailable         03/21/2022 - 16:10	Ľ	PROFILES	Legitimate	Google Play Service.	com.google.ar.core	1.30.220390183	0	Unavailable	Unavailable	03/21/2022 - 16:19
			Legitimate	Street View	com.google.android.	2.0.0.432514663	0	Unavailable	Unavailable	03/21/2022 - 16:19

## 4.5 Devices



CONSOLE	English 🛩											Demo 🛩
DASHBOARD	Devices	ł	Export Devices 🔐 CSV 🛛 💠									
	Devices	Local Device Groups										
Ave. and W	Actions > Profiles: All > Apps: All > Patch Date: All > CVE: All >							0	C Showing 8 of 8 Devices 0 Selected select all 8 Devices			
THREAT LOG	Risk Postur	👻 Group	os	Ŧ	Upgradeable OS	Device ID	Model	Privileges =	CVE	Ŧ	App Status	Last seen
# ADDS	Elected	Becky's Demo Group	<b>14</b>	8		4A7D926B-889E-40C8	iPhone	Not Jailbroken	64		Inactive	11/18/2021 15:37
	Critical	MobileIron Core - Ad.	-			b350a54a-3516-4c11-b.	Pixel 2 XL	Not Rooted	402		Inactive	09/24/2021 10:48
DEVICES	Elevated	Default Group	<b>-</b> 10		Yes	6f6affa5-7b0c-3f4d-826.	.SM-G965U1	Not Rooted	190		Inactive	07/01/2021 22:38
-	Law Law	Default Group	14	5.2		8E466945-2CEC-45D7-9	iPhone	Not Jailbroken	681		Inactive	11/15/2019 23:28
	Citical	Default Group	i .	1	No	62f02440-bc02-358a-ac	Nexus 5	Rooted	2179		Inactive	05/16/2019 03:02
	C Late	Default Group	<b>ei</b> *		No	1B1074B2-9E50-49F8-9.	iPhone8	Not Jailbroken			Inactive	05/01/2019 14:23
	Low	MobileIron Core - Ad.	-		Yes	No Device ID	SM-G981U1	Unknown	85		Pending Activation	Unknown
	Low	MobileIron Core - Ad.	-		No	No Device ID	Pixel 2 XL	Unknown	244		Pending Activation	Unknown
E POLICY	1 - 8 of 8 🕽											

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.



A link to download the CSV export will be emailed to the logged in user Export Devices												
	Showing 3 of 3 Devices 1 Selected select all 3 Devices											
$\overline{\gamma}$	Privileges	Ŧ	CVE	App Status 👳	Last seen	Ţ						
	Not Rooted		222	Inactive	05/09/2022 08:59							
	Not Jailbroken		34	Inactive	05/08/2022 08:15							
	Not Jailbroken		35	Inactive	03/31/2022 20:00							

#### 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 : Creër 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.

tps://nplus1-de	evice-api.zimperium.con	n/activation?	stoken=fuMvPL		R	egenerate Link Copy Link
nk Expires : 0	1/27/2022					
ole*	End User	Ŧ	Email*	id984142@proximus.com	Password	No Password Required
			1	·		
rst Name*	fds		Middle Name		Last Name*	dfs
	Not Active	Ŧ	Phone Number	+1 415 123 4567	Davias Orevert	Default Group 🔹
atus				Verify Phone Numbe	Device Group*	

Proximus NV van publiek recht, Koning Albert II-laan 27, B-1030 Brussel, België BTW BE 0202.239.951, RPR Brussel, BE50 00017100 3118 BP0TBEB1



#### 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.

#### Policies

Threat Po	Threat Policy Apps Policy Phishing & Web Content Policy Samsung Knox MTD Policy												
Selected	Group	Defau	ult Group		▼ Save & De	ploy	Select de	estination group(s)	Copy & Deploy				
Enable	Туре	Ŧ	Severity 👻	Threa	t † =	Set User Alert	Device Action	MDM Action	Mitigation Action	Notify Me			
	Singular		Elevated ~	0	Abnormal Process Activity	□ ‡	¢	Not Supported	Unavailable				
	Singular		Elevated ~	0	Always-on VPN App Set	0 🌣	¢	Not Supported	Unavailable				
	Singular		Elevated ~	0	Android Debug Bridge (ADB) Apps Not Verified	0 \$	\$	Not Supported	Unavailable				
	Singular		Low 🗸	0	Android Device - Compatibility Not Tested By G	□ ‡	¢	Not Supported	Unavailable				
	Singular		Critical 🗸	0	Android Device - Possible Tampering	□ ‡	¢	Not Supported	Unavailable				

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.

DASHBOARD	Policies									
	Threat Policy Apps Policy Phishing & Web Content Policy Samsung Knox MTD Policy									
THREAT LOG	Selected Group									
DPS	Your policy changes have not yet been deployed to your devices									
DEVICES	Dhicking Destantion and Mick Constant Filturian									
	PRISENT PROTECTION AND WED CONTENT FITERING									
USERS	O Disabled									
E POLICY	Phishing Protection     Enhanced Phishing Protection plus Web Content Filtering									
▲ OS RISK	Phishing Protection									
A MANAGE	Allow URL Sharing C Enable Phishing Protection and activate zIPS URL sharing ①									
SUPPORT PORTAL	Use Local VPN for Phishing Protection  C Enable phishing protection and activate zIPS local VPN  Allow user control  Block detected phishing URLs									
	Custom Category List for Phishing/Safe None									

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 <u>Access Control List</u> aanmaken met domeinen en deze als veilig categoriseren.

DASHBOARD	Manage
	General Privacy Integrations VPN Settings Network Snihola Settings Audit Log Roles Message Templates Whitelating Access Control
👎 THREAT LOG	Access Control Lists Create custom lass of sites (domain names or ful UPLs) with their associated categories to use with the Phishing and Web Contert Filtering Festure. Site Category Checker
🗃 apps	Sites are evaluated from the top of the last to the bottom. New entries are added to the top. To re-order an entrie last export the CSV, make your changes and import it.
	Select List to edit testist phalmage * Create New List Delete List
	Add Site to List O Category * Add Groups using this List
2 USERS	Rename List         Export CSV         Import CSV         Download Sample CSV         Default Group
E POLICY	Site
🛕 OS RISK	www.test.be Business Safe 🗊
A MANAGE	
SUPPORT PORTAL	

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 BP0TBEB1



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.

Cat Def	Category Policy Define the access control action for each content category below.										
0	Copy from group Use Recommended Settings	Block & Create Threat									
	Category	- Action									
$\sim$	Security/Risk	Multiple									
	Anonymizers Botnets Cryptocurrency Mining Hacking Illegal Software Malware Phishing Spam Suspected Domain	Block & Create Threat Alert Block & Create Threat Block with No Alert Block & Create Threat									
>	Adult Content	Multiple									
>	Business	Allow									
>	Crime/Fraud	Multiple									
>	Drugs	Multiple									
>	General	Allow									
>	🗆 Lifestyle	Multiple									
>	Mature/Violence	Multiple									
>	Technology/Communications	Multiple									
>	□ System Categories	Allow									

# 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.



OS R	lisk				-	-	-
Devices With Vulnerable OS		5 Total	4 🗯 🔲 u	ogradeable 3 evices Total	2 🗯 💽 Non-U 1 🖷 Device	pgradeable d is d To	2 2 <b>*</b> 0 <b>*</b>
CVEs	OS Version:	S					
							780 CVEs S
CVE	↓ ÷	CVE Severity	CVE Type	Operating Systems	OS Version Count	Device Count	Upgradeable
CVE-2020	-9996	Critical	remote code execution	Ś.	4	4	2
CVE-2020	-9994	Medium	arbitrary file write	ć.	4	4	2
CVE-2020	-9993	Critical	ui spoofing	é.	4	4	2
CVE-2020	-9992	Critical	remote code execution	É	4		2
CVE-2020	-9991	Medium	denial of service	é	4	4	2
CVE-2020	-9989	Critical	code signing bypass	é	4	4	2
CVE-2020	-9988	Critical	code signing bypass	é	4	4	2
CVE-2020	-9983	Critical	remote code execution	É	4	4	2
CVE-2020	-9981	Critical	remote code execution	é	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 MTDpPortaal, 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.



CONSOLE 🤝	English 🗸						
DASHBOARD	General Privacy Integ	grations VPN Settings Network Sinkhole Settings Audit Log	Roles Message Templates Whitelisting Access Control				
	💼 Company Informatio	n	🗙 Preferred Language				
THREAT LOG	Name	Proximus	Select the preferred language for the customer.				
,	Tenant ID	proximus	Lignoi				
APPS	Contact email	raise proximus support@zimperium com					
	Country	be	🙆 Danger Zone				
DEVICES	Activated	02/08/2022 - 10:31	Enable the Danger Zone feature in zIPS 6				
_	Zip code	None	🗸 App Risk Lookup				
PROFILES	Plan	Advanced					
•-	Default Channel	https://proximus-acceptor.zimperium.com/srx	Enable the App Risk Lookup reactire in ZiPS				
USERS			Android Battery Optimization				
	▲ Logged in user		$\ensuremath{\mathbbm Z}$ Add zIPS to the Android battery optimization exemption list. $\ensuremath{\mathfrak{O}}$				
	Email	b.callens@proximus.com	Privacy Summary				
A OS RISK	First Name	Bart	Enable the Privacy Summary feature in zIPS 1				
MANACE	Last Name	Callens	Save				
WIANAGE	Role	System Admin					
SUPPORT PORTAL	Password	Change password	Samsung Knox KPE License				
			Save				
		S Device Inactivity Configuration					
		Enable Policy					
		Allowed Inactivity Time					
		4320 Minutes ~	ence (wmminin suce - o mmiles)				
		Warning Interval					
		1440 Minutes V	ures)				
		Max Warnings					
		The maximum number of warnings that can be sent to the device (0 = Disable Dormanc	y Notifications)				
		0					
		Warning Message Types Configure these warning message types when the Max Warnings field is greater than ze	ero.				
		Send iOS Notification to Devices (1)					
		<ul> <li>Send email to user ( iOS Devices ) (1)</li> <li>Send email to user ( Android Devices ) (1)</li> </ul>					
		Enforce zIPS Install on Both Work and Personal Profiles of Android Enterg	prise				
		This option should only be used if all Android devices have both work and personal prof Trigger a threat when only one of the Android Enterprise profiles has zIP the Allowed Inactivity Time value.	les configured. 19 Installed for a time greater than				
		Save					

#### 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 <u>Threat Policy</u>.



General	Privacy	Integrations	VPN Settings	Network Sinkhole Sett	ings	Audit l	og Roles	Message Templates	Whitelisting	Access Contro
Netwo	ork Sinkl	hole Settir	ngs							
Block ne	etwork acces	s except ALLOW1	the IP Address ran	nes/Domains below						
Allow ne	etwork acces	s except BLOCK t	he IP Address rand	es/Domains below						
' Addr	esses		ID 1 (							
P Address	5		IP Mask			_	Allowed IP Add	esses		
(e.g. 19	2.168.10.1)		(e.g. 255.255.2	(55.0)		<b>~</b>				
omair	ıs									
Domain A	ddress						Allowed Domai	IS		
(e.g. wv	ww.example.c	om)				0				
ountri	60									
	00						lowed Countr	ec		
• • • • • •							aonea obana			
Search	for									
Search 1	for istan				0	<u> </u>				
Search i Afghani Aland Is	for istan slands				0					
Search f Afghani Aland Is Albania	for istan slands				0000					
Search 1 Afghani Aland Is Albania Algeria	for istan slands				00000					

#### 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 <u>Threat Policy</u> zal dan onderdrukt worden.



💝 CONSOLE	English 🗸											
DASHBOARD	General Privacy	Integrations VPN Settings	Network Sinkhole Settings	Audit Log Roles	Message Templates	Whitelisting	Access Control					
	Certificate Wi-	Fi Access Points App Develo										
THREAT LOG	Upload a CSV file of Wr-Fi Access Points to whitelist. BSSID, SSID, and Access Point IP address are all possible values to specify or any combination of the three. At least one value is required. Download example file.											
🍎 APPS	Unsecureu wrrt, Gapure Fortal and Dangel Zone uneata wil de suppresseu wrien a dence la connecueu to a willellisted Access Point.											
DEVICES	+ Upload CSV											
	Actions ~		SSID	-	RSSID			Access Point IP Address				
			esid4		00.00.00.00.00.02			10.0.0.4				
JE USERS	U Whiteliste	ed	esid4		00.00.00.00.00.03			10.0.0.3				
	Whiteliste	ed	ssid2		00.00.00.00.00.01			10.0.0.2				
E POLICY	Whiteliste	ed .	ssid1		00:00:00:00:00:00			10.0.0.1				
🛕 OS RISK	1 – 4 of 4 🕽											
🔧 MANAGE												
SUPPORT PORTAL												

#### 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 <u>https://proximus.be/mtd</u>. 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 MTDoptie?

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 <u>Users</u>.

# 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 <u>Threat Policy</u> 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



