

Harmony Mobile

4.2

Release Notes



© 2023 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(iii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page <http://www.checkpoint.com/copyright.html> for a list of our trademarks.

Refer to the Third-Party copyright notices http://www.checkpoint.com/3rd_party_copyright.html for a list of relevant copyrights and third-party licenses.

Important Information



Latest Software

We recommend that you install the most recent software release to stay up to date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.



Check Point Harmony Mobile 4.2

For more about this product, see the Harmony Mobile Product Page <https://www.checkpoint.com/harmony/mobile-security/mobile/>



More Information

Visit the Check Point Support Center <http://supportcenter.checkpoint.com>.

Revision History

Date	Description
July 4 th , 2023	First release of this document

Contents

Harmony Mobile.....	1
Important Information.....	3
Contents.....	3
Mobile Client Supported Platforms	4
Version 4.2 Updates.....	5
Phishing SMS prevention.....	5
On iOS	5
On Android.....	5
One-Click Integration with MS-Intune UEM.....	6
Protection against AI threats.....	7
Network Protection for browsers	9
Protection against unsecure WiFi.....	10
Most vulnerable mobile devices	11
Alert when Network Protection suspended	12
New Live Demo.....	13
Improved link scanning in Harmony Mobile app.....	14
Various UI Improvements	15

References

- [1]: [Harmony Mobile Administration Guide](#)
- [2]: [Harmony Mobile Integration Guide](#)
- [3a]: [Harmony Mobile Users' Guide for iOS](#)
- [3b]: [Harmony Mobile Users' Guide for Android](#)
- [4]: [Harmony Mobile Home Page SK](#)

Mobile Client Supported Platforms

Minimum mobile OS versions

- iOS: 13.x and later
- Android: 8.x and later

Version 4.2 Updates

Phishing SMS prevention

Researches show that Phishing campaigns are much easier to handle, and chances of success are by far higher when conducted over mobile users with small screens and with a general mindset that everything in mobile needs to go fast. Therefore, pure mobile attack surfaces like SMSs are by nature more vulnerable and require additional protection against Phishing and Zero-day Phishing threats.

In Harmony Mobile from 4.2, we introduced the ability to protect mobiles users against any phishing attempts and malicious URL sent over SMS.

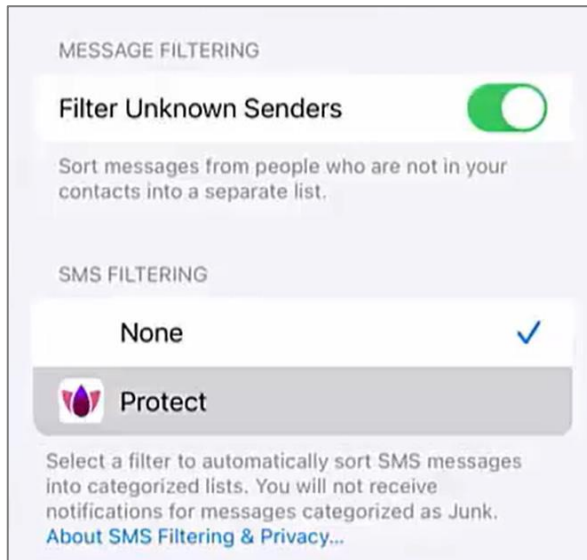


Figure 1 : SMS Phishing Activation on iOS

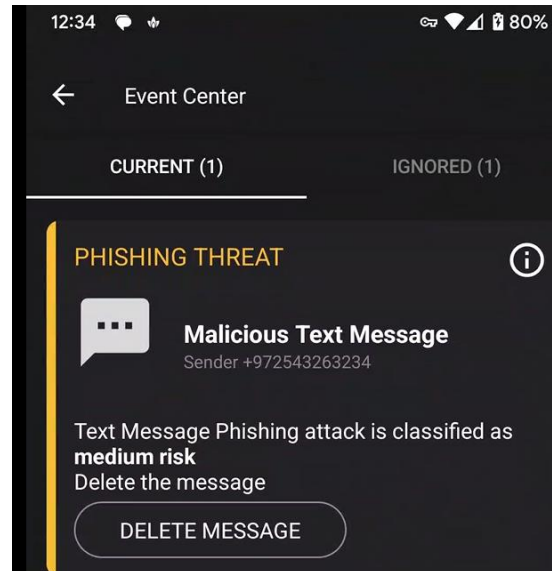


Figure 2 : Malicious Text Message on Android

On iOS

This feature can be enabled on the iOS device as follows:

1. Open the settings → Messages → Under Message Filtering, click the “Unknown & Spam”
2. Under the SMS FILTERING section, enable “Protect”
3. Confirm the selection by clicking “ENABLE”

Those instructions can also be found in the Harmony Mobile client app under Settings → SMS Phishing Protection.

On Android

This feature is enabled on the Android device by the user granting the READ_SMS permissions.

Note that, because Apple and Google have very different approaches of the features, the implementation, design and look-and-feel of the feature are radically different on iOS and Android.

The table below lists the main differences in the feature implementation on iOS and Android:

	iOS	Android
Alert	Device's owner/User only	Device's owner/User and Alert to admin
Actions available	Malicious messages are silently quarantined as a Junk	Notification so malicious SMS is removed manually
SMS Source	Only from unknown senders	SMS from any phone number
Pre-requisite	Feature activation in iOS settings	READ_SMS Permission by the end-user
Availability	iOS version: iOS 16.x+ Harmony Mobile version: 4.2.x+	Harmony Mobile version: 4.2.x+

A video clip is available [here](#) to understand the feature on iOS and Android.

One-Click Integration with MS-Intune UEM

Moving to the new Intune MS-Graph API

Microsoft recently announced that they deprecate their legacy Intune API and that integration with Mobile Threat Defense solutions should be migrated to the newest MS Graph API.

This move has been successfully conducted and completed for all Harmony Mobile tenants and customers in Harmony Mobile 4.2.

Microsoft Intune One-Click Integration

With the introduction of these new Intune API calls, in Harmony Mobile 4.2, we fully redesigned the integration with Microsoft Intune, so all configurations required for the Harmony Mobile/Intune integration are fully automated and conducted only from the Harmony Mobile console in a few clicks (via API calls).

With the introduction of this new feature, the complexity of the integration with Intune so propitious to errors and mistakes is no more a problem. All the integration process, configuration and settings are fully automated and run from a single Harmony Mobile screen.

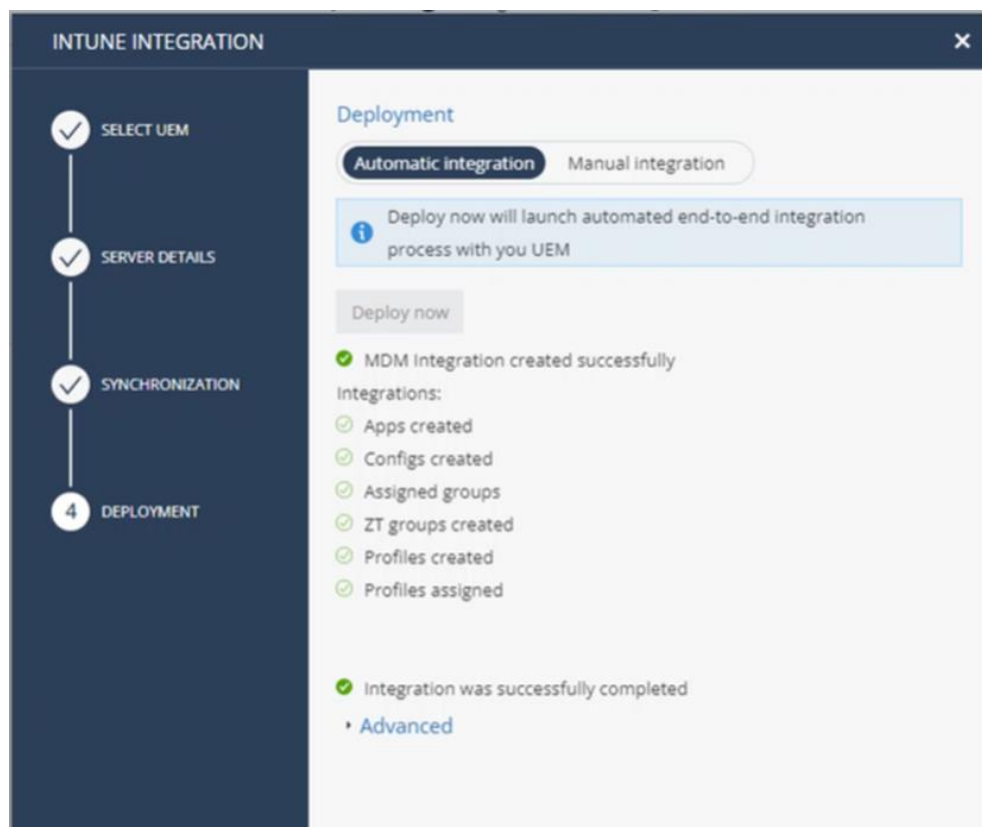


Figure 3 : One-Click Intune Integration

A video clip is available [here](#) to understand the simplicity of this new integration procedure.

Protection against AI threats

Recent surveys and security research have revealed that employees are more opened to share personal information or to disclose sensitive corporate data in their conversations with Generative AI dialogs. Since this information is consumed by the machine learning model, it might be shared with unexpected audiences.

Therefore, many companies and countries have decided to restrict, limit or block access to AI services.

From Harmony Mobile 4.2 onwards, security admins can configure policies:

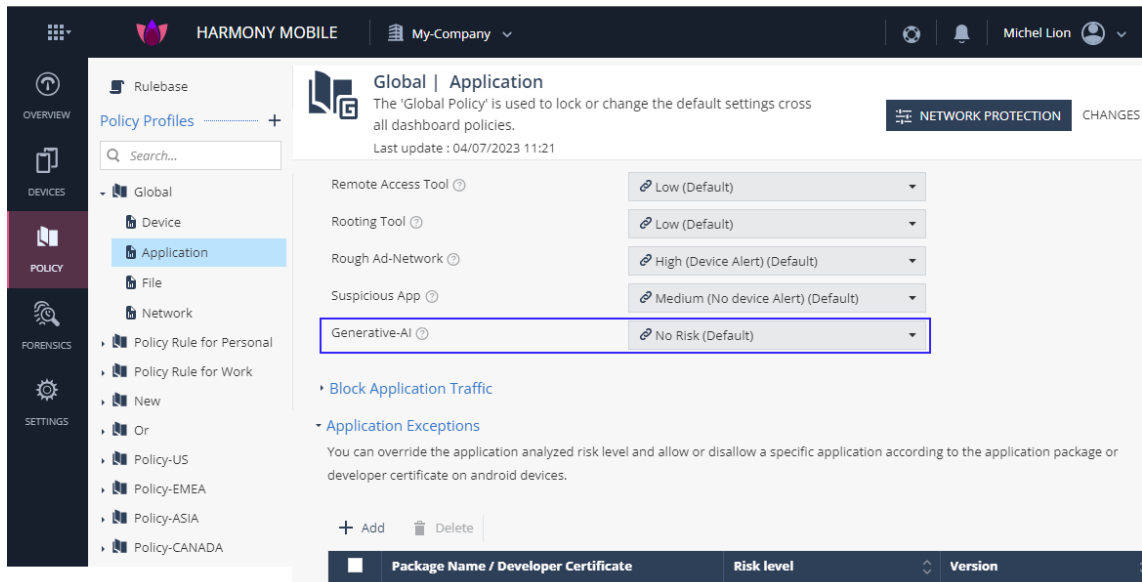
- 1- to raise the risk-level of mobile installed with **apps** using AI technologies
- 2- to block access to AI **web sites** whether from mobile apps and/or from web browsers.

Consequently, once those policy items configured,

- If a conditional access is in place, devices installed with Apps using AI services will not be able to access the corporate resources.
- On Android, traffic from those mobile apps will also be blocked if ONP enabled in full inspection mode.
- Access to AI web sites will be blocked.

To activate the protection against mobile apps using AI,

From your Harmony Mobile management console, set the desired risk-level under POLICY → Policy Name → Application → Classification – Generative-AI.

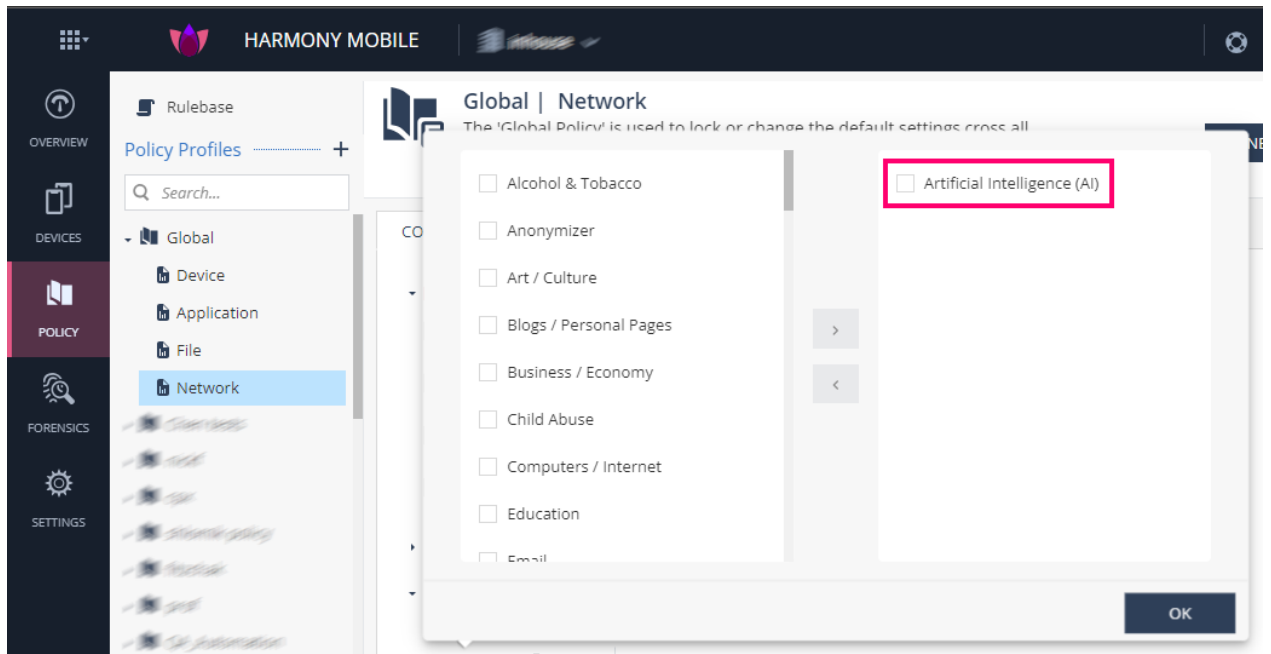


: Setting the risk-level of mobile apps using AI services

Note that security admins can still define application exceptions to set the desired risk level for specific mobile apps under POLICY → Policy Name → Application → Application Exceptions.

To block access to AI sites,

From your Harmony Mobile management console, select the Artificial Intelligence (AI) category in the categories to block in the URL Filtering policy – POLICY → Policy Name → Network → URL Filtering Categories – Add the Artificial Intelligence (AI) category.



: Blocking access to AI web sites

Note: Blocking access to AI web sites requires the activation of the On-Device Network Protection.

Network Protection for browsers

In Harmony Mobile 4.2, we introduce a new mode of Network Protection which consists in sending browser traffic to the On-Device Network Protection (ONP), while mobile apps' traffic is directly sent to the Internet.

This option offers an intermediate level of protection for customers who do not want to use Network Protection in the full inspection mode. It is a good balance between security and customer experience as mobile applications are already assumed to be safe based on the ThreatCloud™ Behavioral Risk Engine module, which runs an extensive behavioral analysis of the mobile application tenant's ecosystem.

For this feature to operate,

- In Android, Harmony Mobile instructs the mobile OS to send only traffic from browser to the ONP inspection module.
- In iOS,
 - For protecting traffic generated by Safari, the user should install a plugin to allow network protection.
 - For all other browsers, an MDM/UEM is required to enable a per-app VPN configuration.

With this option, security admins have also the ability to configure exceptions so traffic from specific browsers are not inspected by the On-Device Network Protection module.

This option can be enabled via the Network Protection Settings → Network Protection Working Mode.

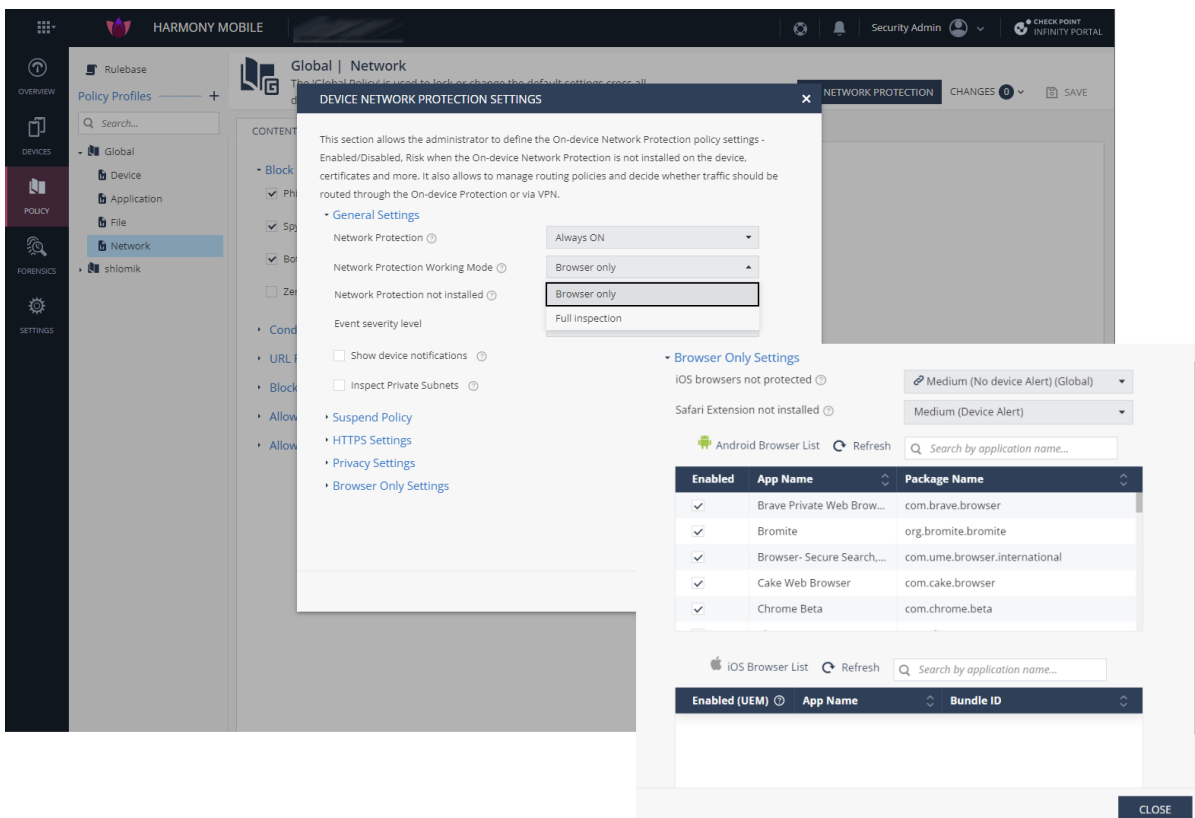


Figure 6: ONP for Browsers

Note that the following features are not available when mobiles devices' policy is set to "Network Protection for Browsers":

- Anti-bot
- Protected DNS
- Ability to block traffic from specific mobile apps
- Port scan detection.

Protection against unsecure WiFi

By essence, mobile users are roaming and connect to public hotspots and other networks offering weak security. These networks offer poor security which might allow malicious actors to intercept or intersect the end-users' traffic data posing a huge risk for personal information and corporate data.

Because of the ease of conducting attacks in such environments, in Harmony Mobile 4.2, we introduced the ability for security admins to detect and raise the risk-level of devices connected to unencrypted WiFi networks.

This new feature can be enabled in the Harmony Mobile Management console by setting the desired risk-level under POLICY → <Policy name> → Network → WIFI NETWORK tab → Unsecure WIFI.

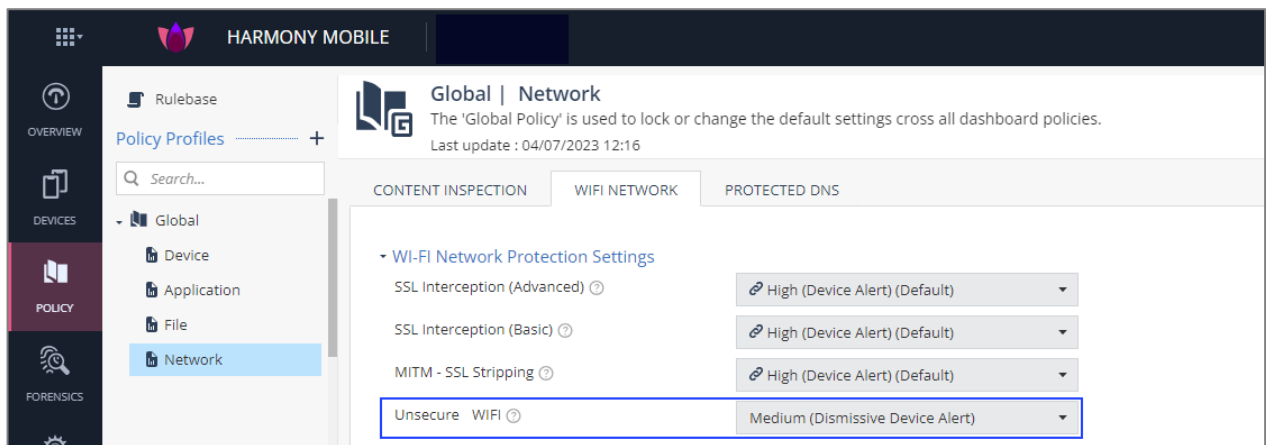


Figure 7: Enabling Unsecure WIFI Protection

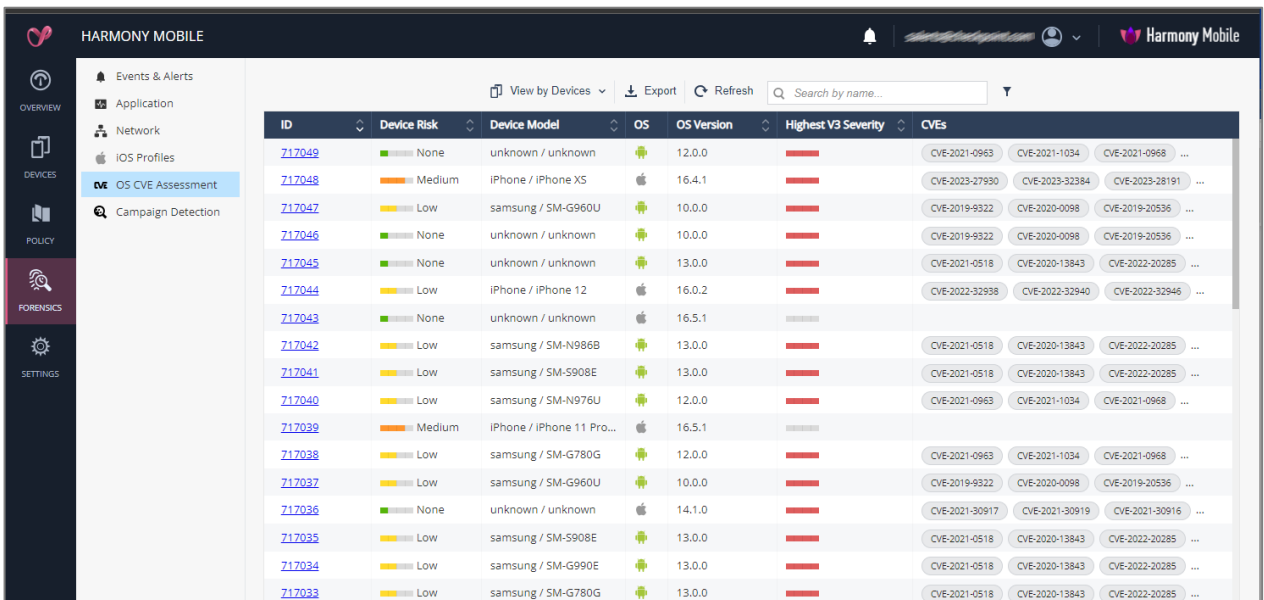
Most vulnerable mobile devices

Harmony Mobile runs a full OS vulnerability assessment and reporting of the mobile fleet.

In the previous Harmony Mobile version, security admins could check:

- 1- the list of the OS installed in the mobile fleet with their respective CVEs
- 2- the list of the CVEs detected in the mobile fleet with the number of devices affected by those OS vulnerabilities.

In Harmony Mobile 4.2, a new screen is added, so security admins can list the most vulnerable devices in the mobile fleet.



The screenshot shows the Harmony Mobile dashboard with a table titled 'OS CVE Assessment'. The table lists various mobile devices with their IDs, risk levels, models, OS versions, and highest vulnerability severity. The 'Device Risk' column uses color-coded bars to indicate risk levels: None (green), Low (yellow), and Medium (orange). The 'Highest V3 Severity' column uses red bars to indicate severity levels. The 'CVEs' column lists specific CVE identifiers for each device.

ID	Device Risk	Device Model	OS	OS Version	Highest V3 Severity	CVEs
717049	None	unknown / unknown	Android	12.0.0	High	CVE-2021-0963 CVE-2021-1034 CVE-2021-0968 ...
717048	Medium	iPhone / iPhone XS	iOS	16.4.1	High	CVE-2023-27930 CVE-2023-32384 CVE-2023-28191 ...
717047	Low	samsung / SM-G960U	Android	10.0.0	High	CVE-2019-9322 CVE-2020-0098 CVE-2019-20536 ...
717046	None	unknown / unknown	Android	10.0.0	High	CVE-2019-9322 CVE-2020-0098 CVE-2019-20536 ...
717045	None	unknown / unknown	Android	13.0.0	High	CVE-2021-0518 CVE-2020-13843 CVE-2022-20285 ...
717044	Low	iPhone / iPhone 12	iOS	16.0.2	High	CVE-2022-32998 CVE-2022-32940 CVE-2022-32946 ...
717043	None	unknown / unknown	iOS	16.5.1	Medium	
717042	Low	samsung / SM-N986B	Android	13.0.0	High	CVE-2021-0518 CVE-2020-13843 CVE-2022-20285 ...
717041	Low	samsung / SM-S908E	Android	13.0.0	High	CVE-2021-0518 CVE-2020-13843 CVE-2022-20285 ...
717040	Low	samsung / SM-N976U	Android	12.0.0	High	CVE-2021-0963 CVE-2021-1034 CVE-2021-0968 ...
717039	Medium	iPhone / iPhone 11 Pro...	iOS	16.5.1	Medium	
717038	Low	samsung / SM-G780G	Android	12.0.0	High	CVE-2021-0963 CVE-2021-1034 CVE-2021-0968 ...
717037	Low	samsung / SM-G960U	Android	10.0.0	High	CVE-2019-9322 CVE-2020-0098 CVE-2019-20536 ...
717036	None	unknown / unknown	iOS	14.1.0	High	CVE-2021-30917 CVE-2021-30919 CVE-2021-30916 ...
717035	Low	samsung / SM-S908E	Android	13.0.0	High	CVE-2021-0518 CVE-2020-13843 CVE-2022-20285 ...
717034	Low	samsung / SM-G990E	Android	13.0.0	High	CVE-2021-0518 CVE-2020-13843 CVE-2022-20285 ...
717033	Low	samsung / SM-G780G	Android	13.0.0	High	CVE-2021-0518 CVE-2020-13843 CVE-2022-20285 ...

Figure 8: Most vulnerable mobile devices

Alert when Network Protection suspended

Based on the policy configuration, security admins might want to allow end-users to momentarily suspend the On-device Network Protection (ONP) on their mobile devices.

In such scenario, mobile devices are temporarily not protected against Network threats, admins might want to be notified and/or raise the risk-level of such devices.

In Harmony Mobile 4.2, we introduced the ability to report on ONP suspension in the Dashboard under the Events and Alerts screen.

This option is available in the Harmony Mobile management console under Policy > Network > Network Protection > Suspend Policy > Suspend Severity Level.

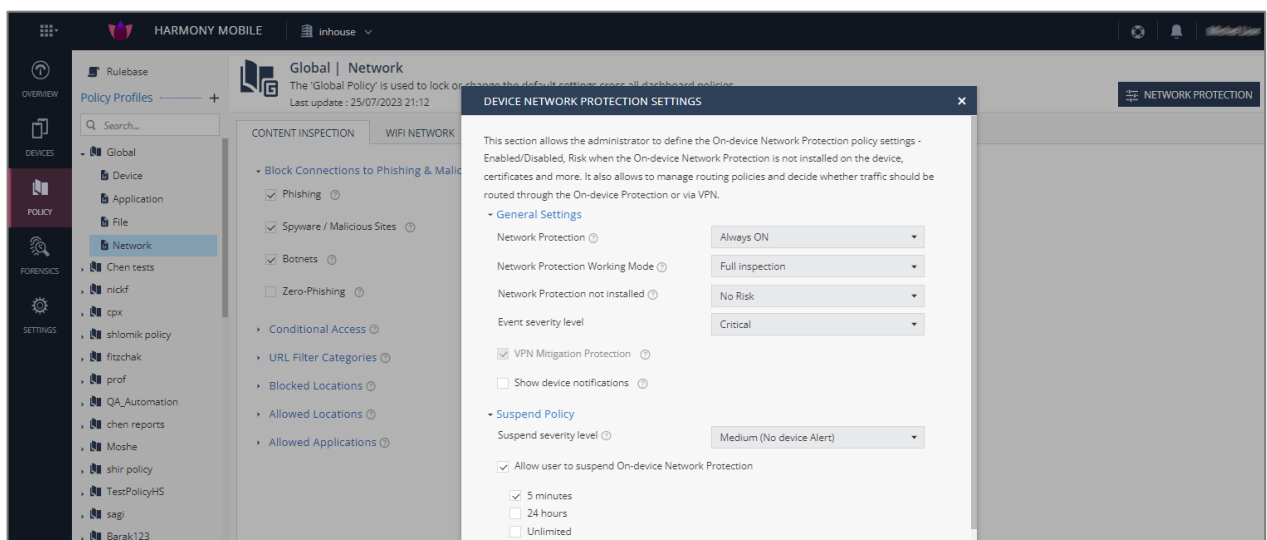


Figure 9 : Alerting when Network Protection is Suspended

Date/Time	Severity Level	Attack Vector	Threat Factors	Event	Event Details	OS	Device ID	User Email
07/09/2023 08:48:49	Information	Device	Network Protection	Resumed	Duration (minutes): 5	iOS	50	View Details
07/09/2023 08:45:10	Warning	Device	Network Protection	Suspended	Duration (minutes): 5	iOS	50	View Details
07/09/2023 08:42:25	Information	Device	Network Protection	Resumed	Duration (minutes): 5	iOS	50	View Details
07/09/2023 08:38:08	Warning	Device	Network Protection	Suspended	Duration (minutes): 5	iOS	50	View Details
09/08/2023 20:37:41	Warning	Device	Local Network Permission	Noncompliant		iOS	50	View Details
09/08/2023 20:37:41	Information	Device	Local Network Permission	Compliant		iOS	50	View Details

Figure 10 : Alert in the dashboard when Network Protection suspended

New Live Demo

Whether you are a security operational, admin or manager or a partner who want to quickly evaluate or demonstrate the Harmony Mobile solution, smooth end-to-end device on-boarding process and rolling-on most popular security use cases are crucial.

In Harmony Mobile 4.2, the Live Demo has been enriched with a wealth of new features from our latest Harmony Mobile capability additions – File Protection, Phishing and Zero-day phishing, MiTM attack detection scenarios, URL Filtering based on categories, SSL/TLS certificate checks and many more...

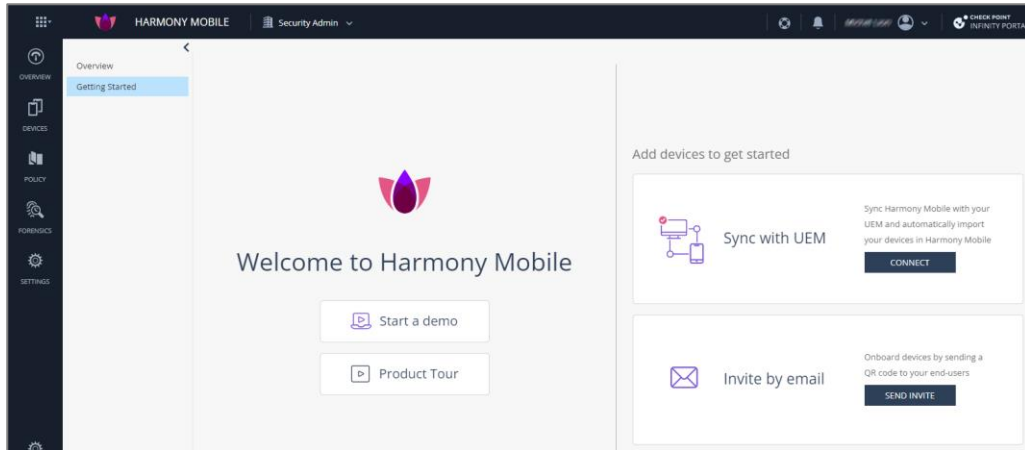


Figure 11: Getting Started

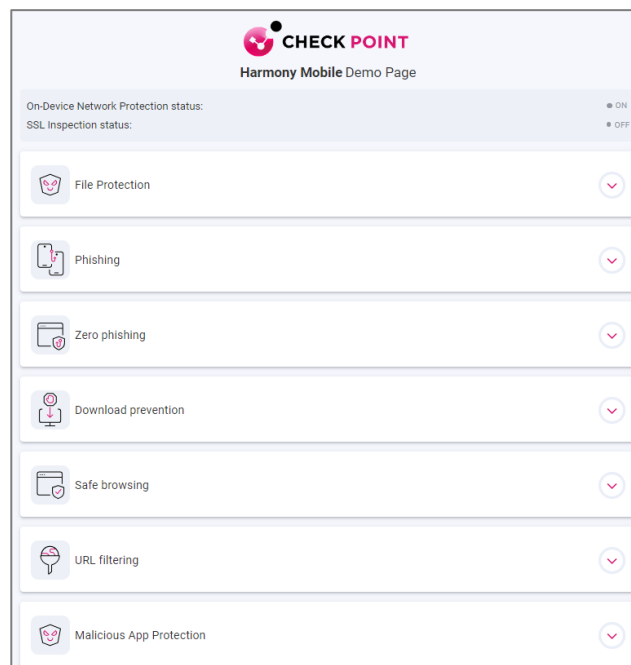


Figure 12: New Live Demo Page

A video clip is available [here](#) to walk you through the new Harmony Mobile Live Demo.

Note: The live demo policy does not include the on-board traffic SSL inspection so on-boarding is yet easier. For evaluation of use cases including SSL/TLS inspection, a separate full demo page is available for full SSL/TLS inspection policies under <http://main.sbm-demo.xyz/>.

Improved link scanning in Harmony Mobile app

End-users can submit suspicious links for analysis in their Harmony Mobile client application to receive a full and detailed security verdict and site categorization.

Since sites with invalid SSL/TLS certificates are de facto unsafe, in Harmony Mobile 4.2, the existing Link Scan verdict has been enriched with information about the SSL certificate validity.

The scan link option can be accessed

- By clicking a link if a default app has not been selected
- By opening the Harmony Mobile app --> 3 dots --> Scan Link

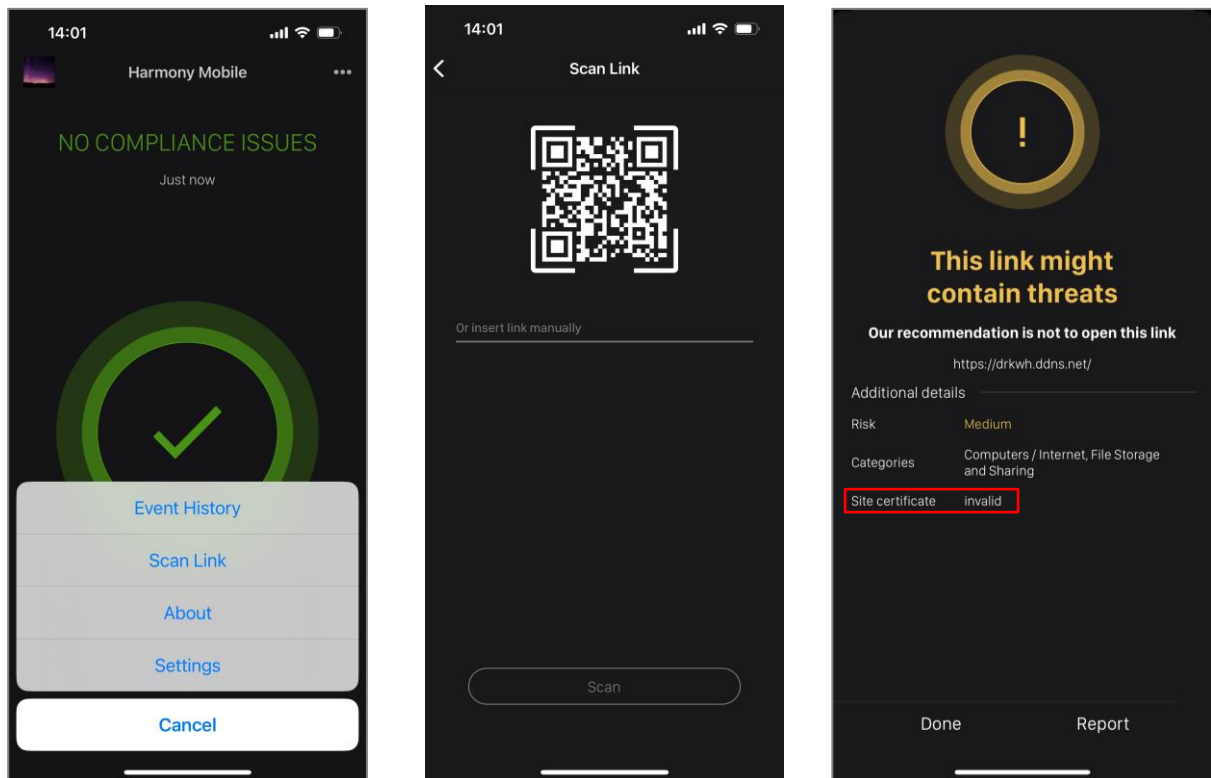


Figure 13: Site certificate is now part of the "Scan link" verdict

Note:

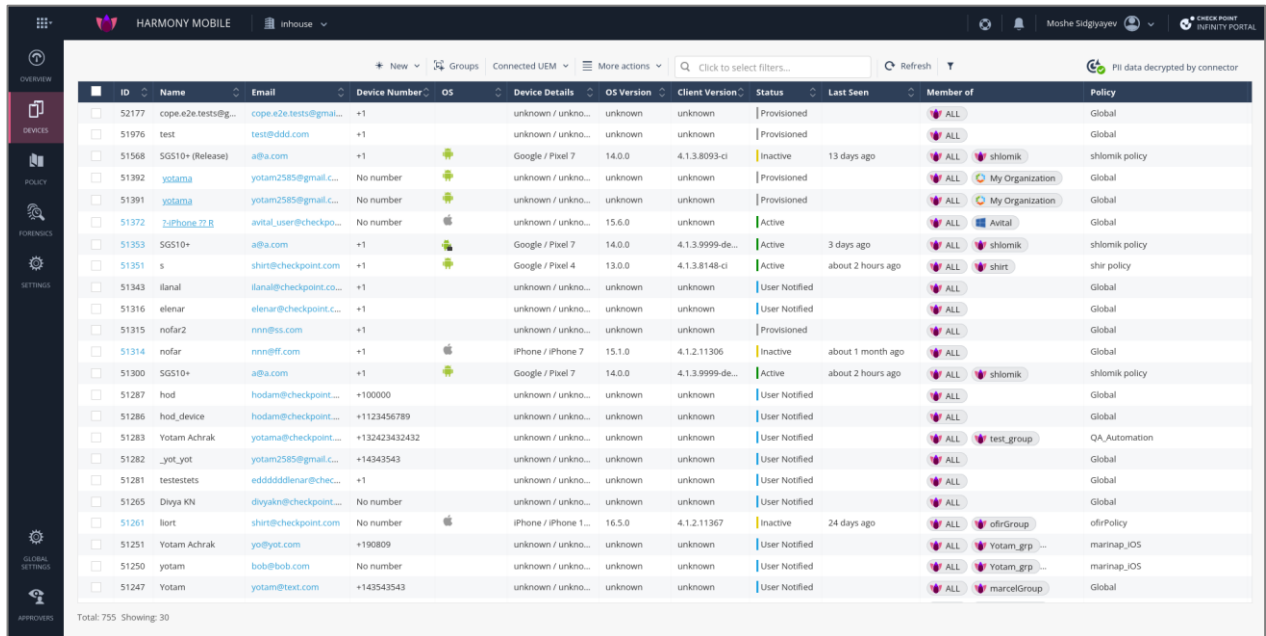
This feature is available for iOS only for now.
This feature will be supported soon on Android.

Various UI Improvements

UEM Group icons

Device groups might be defined locally in Harmony Mobile but can also be imported from an external system when integrated with a UEM. This creates situations where Harmony Mobile is expected to manage different groups from different UEM with same names.

For that reason, we added an icon in the UI next to the group name so security admin and operators can easily and immediately understand the group they belong to in their policy settings and configuration.

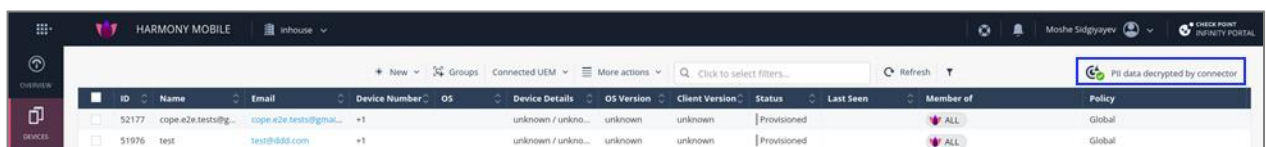


ID	Name	Email	Device Number	OS	Device Details	OS Version	Client Version	Status	Last Seen	Member of	Policy
52177	cope.e2e.tests@...	cope.e2e.tests@gmail...	+1		unknown / unkno...	unknown	unknown	Provisioned		ALL	Global
51976	test	test@ddd.com	+1		unknown / unkno...	unknown	unknown	Provisioned		ALL	Global
51568	SGS10+ (Release)	a@a.com	+1		Google / Pixel 7	14.0.0	4.1.3.8093-ci	Inactive	13 days ago	ALL, shlomik	shlomik policy
51392	yotama	yotam2585@gmail.c...	No number		unknown / unkno...	unknown	unknown	Provisioned		ALL, My Organization	Global
51391	yotama	yotam2585@gmail.c...	No number		unknown / unkno...	unknown	unknown	Provisioned		ALL, My Organization	Global
51372	2iPhone 72.0	avital_user@checkpo...	No number		unknown / unkno...	15.6.0	unknown	Active		ALL, Avital	Global
51353	SGS10+	a@a.com	+1		Google / Pixel 7	14.0.0	4.1.3.9999-de...	Active	3 days ago	ALL, shlomik	shlomik policy
51351	s	shirt@checkpoint.com	+1		Google / Pixel 4	13.0.0	4.1.3.8148-ci	Active	about 2 hours ago	ALL, shirt	shir policy
51343	ilanal	ilanal@checkpoint.co...	+1		unknown / unkno...	unknown	unknown	User Notified		ALL	Global
51316	elenar	elenar@checkpoint.c...	+1		unknown / unkno...	unknown	unknown	User Notified		ALL	Global
51315	nofar2	nnn@ss.com	+1		unknown / unkno...	unknown	unknown	Provisioned		ALL	Global
51314	nofar	nnn@f.com	+1		iPhone / iPhone 7	15.1.0	4.1.2.11306	Inactive	about 1 month ago	ALL	Global
51300	SGS10+	a@a.com	+1		Google / Pixel 7	14.0.0	4.1.3.9999-de...	Active	about 2 hours ago	ALL, shlomik	shlomik policy
51287	hod	hodam@checkpoint...	+100000		unknown / unkno...	unknown	unknown	User Notified		ALL	Global
51286	hod_device	hodam@checkpoint...	+1123456789		unknown / unkno...	unknown	unknown	User Notified		ALL	Global
51283	Yotam Achrak	yotama@checkpoint...	+132423432432		unknown / unkno...	unknown	unknown	User Notified		ALL, test_group	QA_Automation
51282	yot_yot	yotam2585@gmail.c...	+14943543		unknown / unkno...	unknown	unknown	User Notified		ALL	Global
51281	testestets	eddddienar@chec...	+1		unknown / unkno...	unknown	unknown	User Notified		ALL	Global
51265	Divya KN	divyakn@checkpoint...	No number		unknown / unkno...	unknown	unknown	User Notified		ALL	Global
51261	liort	shirt@checkpoint.com	No number		iPhone / iPhone 1...	16.5.0	4.1.2.11367	Inactive	24 days ago	ALL, ofirGroup	ofirPolicy
51251	Yotam Achrak	yo@yot.com	+190809		unknown / unkno...	unknown	unknown	User Notified		ALL, Yotam_grp ...	marinap_iOS
51250	yotam	bob@bob.com	No number		unknown / unkno...	unknown	unknown	User Notified		ALL, Yotam_grp ...	marinap_iOS
51247	Yotam	yotam@text.com	+143543543		unknown / unkno...	unknown	unknown	User Notified		ALL, marcelGroup	Global

Figure 14: Group names are now prefixed by an icon indicating the provenance of those groups

PII Data Decryption Connector indication

In Harmony Mobile setups including a Harmony Mobile Connector component, all Personal Identifiable Information (PII) data is decrypted by the Connector only from consoles having direct access to the Connector.



ID	Name	Email	Device Number	OS	Device Details	OS Version	Client Version	Status	Last Seen	Member of	Policy
52177	cope.e2e.tests@...	cope.e2e.tests@gmail...	+1		unknown / unkno...	unknown	unknown	Provisioned		ALL	Global
51976	test	test@ddd.com	+1		unknown / unkno...	unknown	unknown	Provisioned		ALL	Global

Figure 15: PII data is decrypted by the Harmony Mobile Connector

Security admins connecting from outside of their organization might not be able to view the PII data in the various screens of the Harmony Mobile Management console.

To avoid confusion and help security admins to better understand why and when they cannot view the users' PII data, an indication that the "PII data is decrypted by the Connector" was added on the top right corner of the screens where PII data is supposed to appear.

When the admin's console cannot access the Harmony Mobile Connector, an icon indicating that the Connector is unreachable is presented as follows:

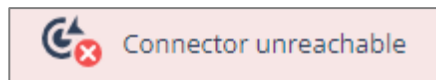


Figure 16: The Harmony Mobile Connector is unreachable