



HARMONY IoT
Cyber Of Things

Harmony IoT Release Notes

Release Version: 6.4.2

Release Date: 1/12/2021

Copyright

Copyright ©2021 by Orchestra Group Ltd. All Rights Reserved.

The “original instructions” of this manual are published in the English language.

The information conveyed in this document has been carefully checked and is believed to be reliable at the time of printing. However, Orchestra Group Ltd makes no warranty regarding the information set forth in this document and assumes no responsibility for any errors or inaccuracies contained herein. Orchestra Group Ltd is not obligated to update or correct any information contained in this document. Orchestra Group Ltd reserves the right to change products or specifications at any time without notice.

No part of this document may be reproduced in any form for any purpose without the prior written permission of Orchestra Group Ltd.

The Orchestra Group Ltd logo and all Orchestra Group Ltd product and service names listed herein are either registered trademarks or trademarks of Orchestra Group Ltd or its subsidiaries. All other marks are the property of their respective owners.

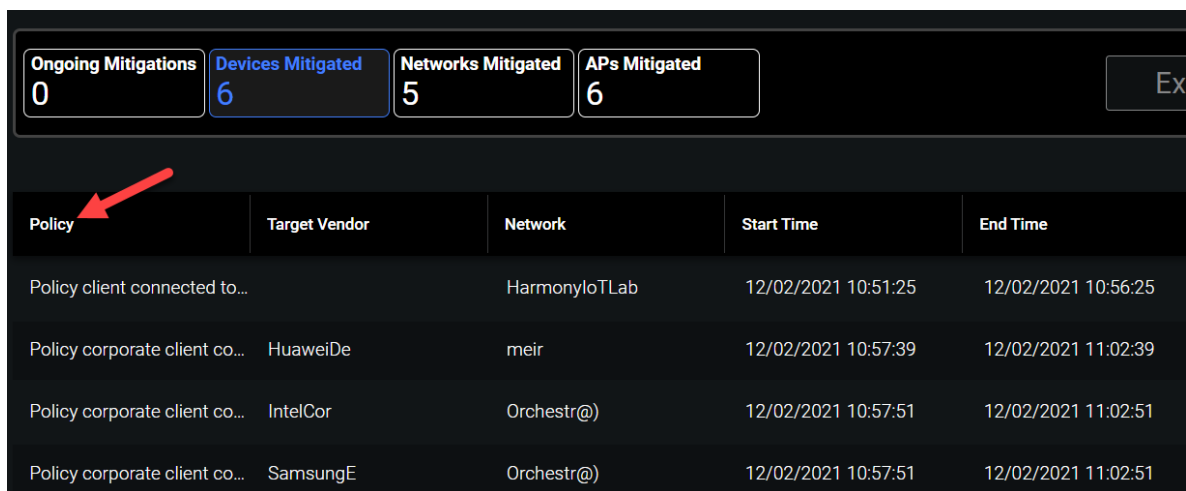
Mention of third-party products or services is for informational purposes only and does not constitute an endorsement or recommendation.

Harmony IoT Release Notes 6.4.2

The following new features are available in Harmony IoT Version 6.4.2.

Mitigations Page Changes

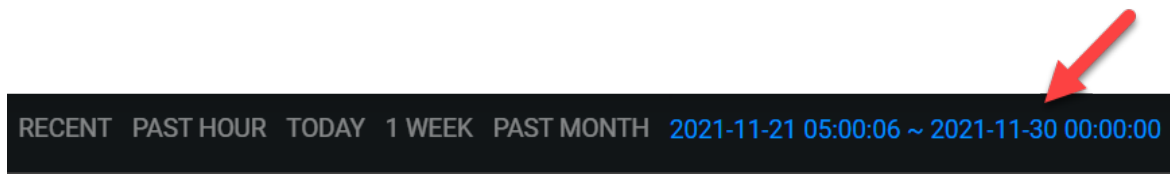
- The Mitigations page has a new column—**Policy**. This is the Rule that generated the mitigation.



The screenshot shows a summary bar at the top with four metrics: Ongoing Mitigations (0), Devices Mitigated (6), Networks Mitigated (5), and APs Mitigated (6). Below this is a table with five columns: Policy, Target Vendor, Network, Start Time, and End Time. A red arrow points to the 'Policy' column header. The table contains four rows of mitigation data.

Policy	Target Vendor	Network	Start Time	End Time
Policy client connected to...		HarmonyIoTLab	12/02/2021 10:51:25	12/02/2021 10:56:25
Policy corporate client co...	HuaweiDe	meir	12/02/2021 10:57:39	12/02/2021 11:02:39
Policy corporate client co...	IntelCor	Orchestr@)	12/02/2021 10:57:51	12/02/2021 11:02:51
Policy corporate client co...	SamsungE	Orchestr@)	12/02/2021 10:57:51	12/02/2021 11:02:51

- You may also filter the mitigations by a specific date and **time**.



Audit Trail: Filter by Date & Time

You may also filter the Audit Trail by a specific date and **time**.

RECENT PAST HOUR TODAY 1 WEEK PAST MONTH 2021-11-14 05:00:00 ~ 2021-11-23 06:00:00

AUDIT TRAIL Export

Action type	User	Page	Data	Created At
LOG_OUT	amir.test@gmail.com	/visibility/devices	{'message':'Logged Out'}	11/22/2021 20:05:59
LOG_IN:	amir.test@gmail.com	/login	{'message':'Logged In'}	11/22/2021 19:42:23

Incident Page Enhancements

The Incidents page now displays detailed information on the risk, best practices, and the incident itself to better allow you to mitigate the risk.

SECURITY VISIBILITY OPERATIONS GENERATE REPORT

Suspicious AP Detected

Start Time: 11/05/2021 12:19:18 End Time: 11/05/2021 12:27:14

, Our system detected the following suspicious AP with network SSID: , **AndroidAP8BDB** , Vendor: , **SamsungE** , MAC: **d4:e6:b7:55:bb:db** , which is similar to the , **Corporate network: AndroidAP** ,

Risk Critical

- Sensitive data theft from devices through network sniffing
- Privileged credentials theft through phishing and man-in-the-middle network attacks to be used to access high priority assets
- Malware infection of devices through network exploits for complete remote control over the device

Recommendations

- Block all devices from connecting to Evil Twin networks
- Locate the Evil Twin AP
- Refrain from using network names that give away the organization's name

What is Suspicious AP Detected?

The diagram illustrates a man-in-the-middle attack. A Hacker is shown on the left, connected to a Corporate User on the right. The Corporate User is connected to a Corporate Network Name (Pied_Piper). The Hacker is also connected to the Corporate Network Name, leading to Data Leakage. The Corporate User is also connected to the Corporate Network Name, leading to Data Leakage.

Suspicious AP Detected

, Similar SSIDs were detected being broadcasted. The presence of an access point with a similar SSID to yours could indicate an attempt to fool unsuspecting users into connecting to a malicious access point instead of the original one. Once connected, users are susceptible to data leakage of sensitive information such as their banking credentials and even malware injection through man-in-the-middle attacks.

Harmony IoT by Orchestra

Report Enhancements

The generated report is more detailed with a friendlier design.