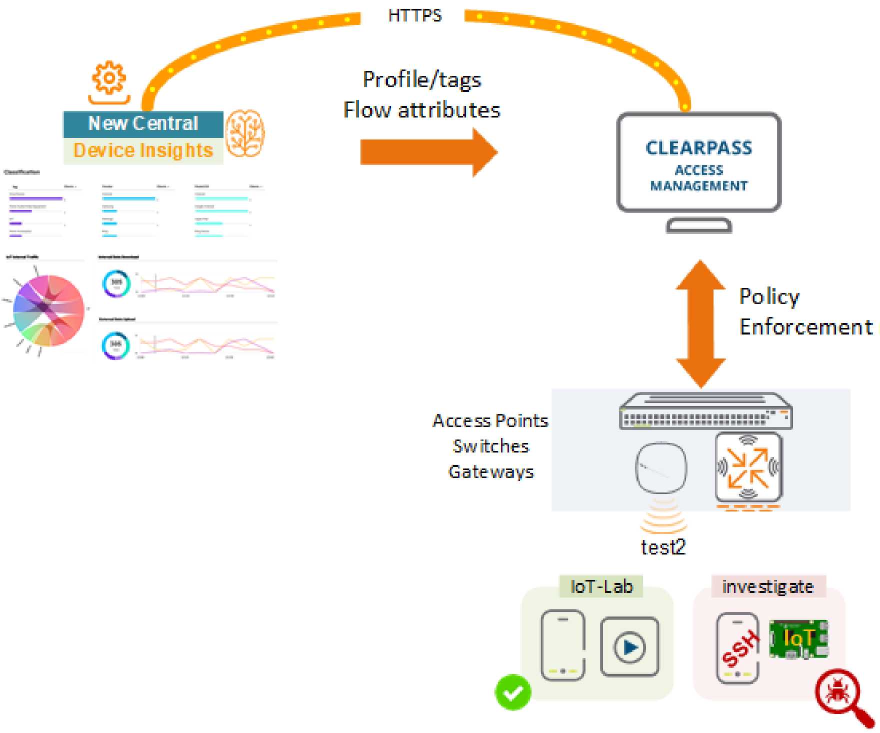
1 Table of Contents

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
14 Apr 2025	0.1	Ariya Parsamanesh	Initial creation
27 Apr 2025	0.2	Ariya Parsamanesh	Added the site view section

2 Aruba New Central Device Insights and ClearPass

This short technote covers integrating **Aruba New Central** with ClearPass Policy Manager. With this integration Aruba Central sends the device profiling information and insights to ClearPass. Device Insight (DI) is part of the Aruba Central Platform and uses data collectors (APs, CX switches and gateways) that are on your network to continuously gather metadata. You can then setup device tags based on **location, application categories/types, device type/OS attributes** used in ClearPass enforcement policies. It also provides much richer device profiling information and visibility.



In this scenario RPi device connect to a Bridged PSK SSID and it is classified as "Computing Systems" and it is put into IoT-Lab user role. However, when this device starts a SSH session to an internal server. DI identifies this flow and automatically notifies ClearPass that puts the device in a "investigate" restricted user role.

With this integration, ClearPass uses New Central DI instead of its profiler for all device discovery and classification. A much richer meta data is automatically sent in both directions between ClearPass and Aruba Central. DI also updates ClearPass in real time if it detects a change in device classification which could be an indication of a security threat.

2.1 Things you need

We need the following.

- 1x AP that is managed by Aruba Central. (I am using AP-615 AOS8.12.0.5), you can also use AOS10 firmware. Note that I am using Instant AP to show that various flow attribute are available without using a gateway. This is also true for AOS10 bridge mode WLANs.
- ClearPass Policy Manager 6.11.x

2.2 Assumptions

- Aruba AP is visible and online in Aruba New Central and have a valid subscription.

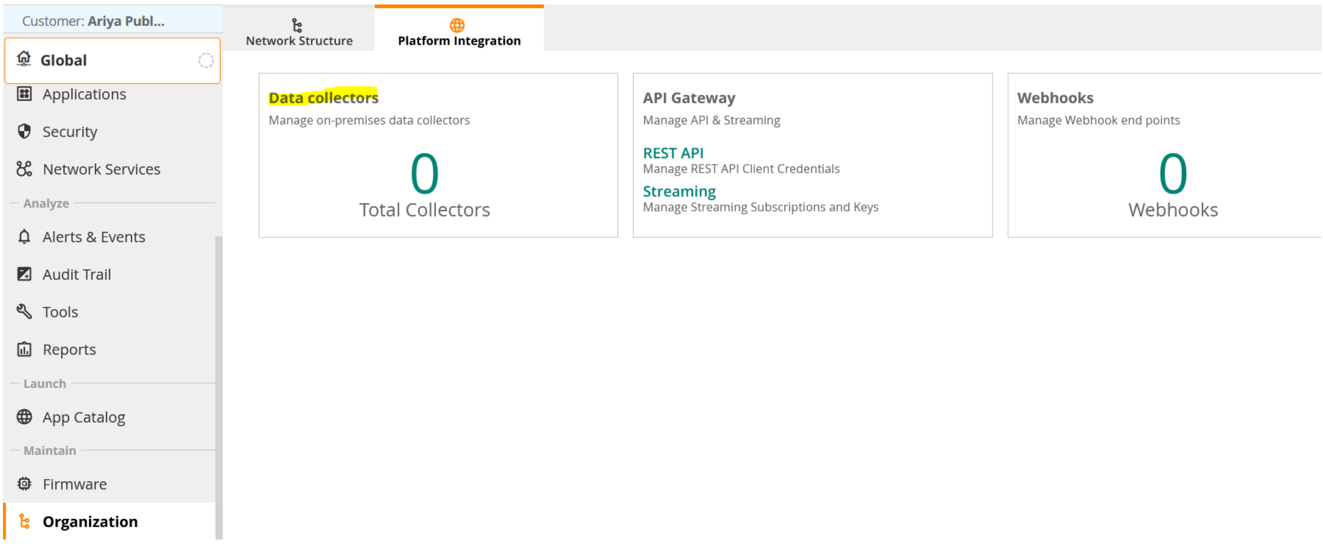
3 Aruba Central Integration with ClearPass

Here we'll cover the configurations steps that are needed for this integration.

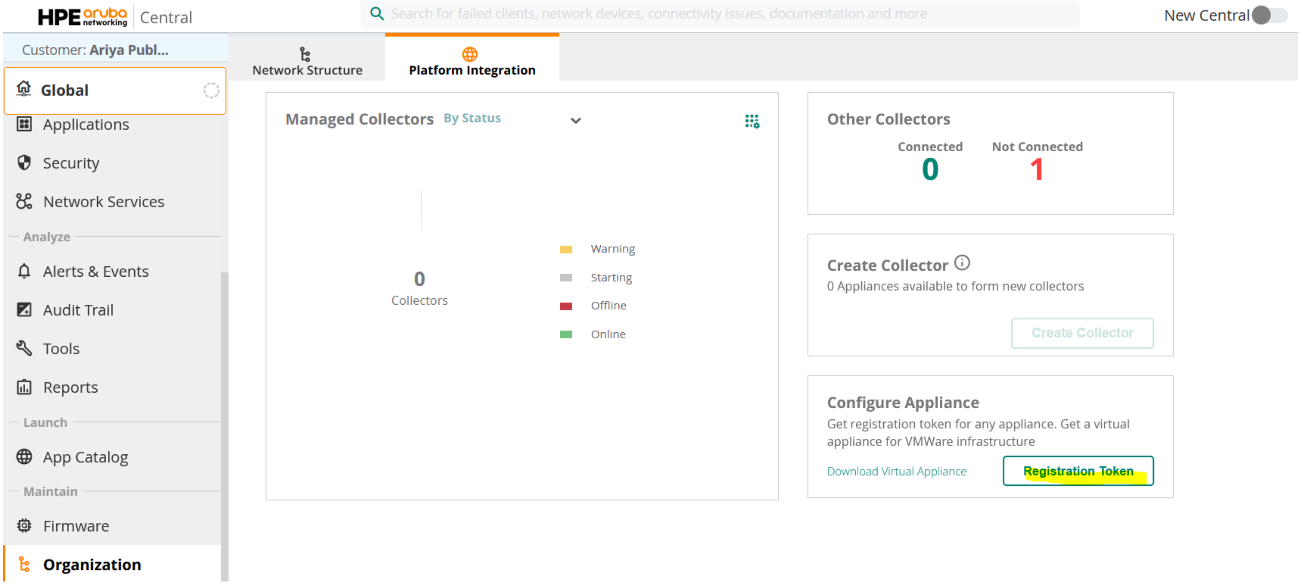
3.1 Aruba Central Configuration

This configuration is the same whether you are using classic or New Central.

Start at the "global" context, go to Organisation >> Platform Integration and then click on "Data Collectors"



The integration between ClearPass and Aruba Central need registration token. This is where we generate a token to be used when configuring ClearPass.



Click on the "Registration Token" and copy it. The registration token will last for 2 days. Then go to ClearPass.

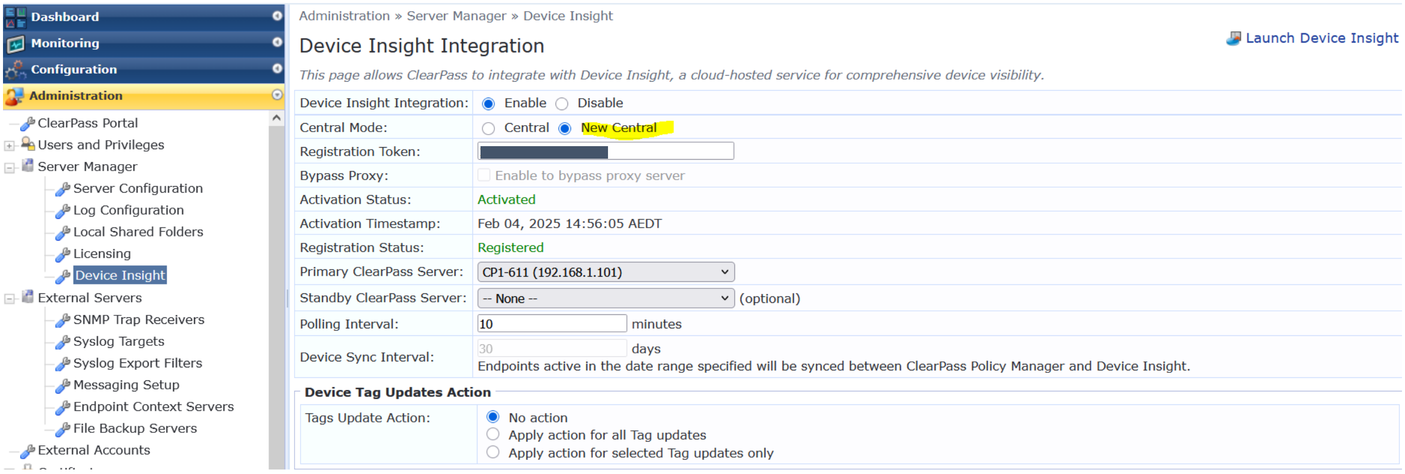
Note that these are the same steps that you need to do for New Central as well.

3.2 ClearPass Integration

On the ClearPass side we need to configure it in two places. But first, we need to enable communication with **New Central** which is done through CLI. So SSH to your ClearPass and run this command.

```
[appadmin@CP1-611]# configure central-communication 1
Central Communication Mode is now Enabled.
[appadmin@CP1-611]#
```

Once this is done, we should see the “New Central” option in “Device Insight” integration. This is where we use our Aruba Central token that we copied earlier.



Administration » Server Manager » Device Insight

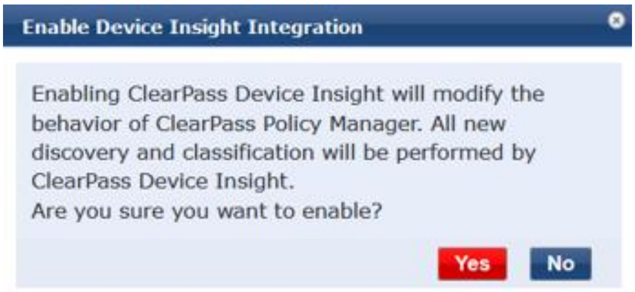
Device Insight Integration

This page allows ClearPass to integrate with Device Insight, a cloud-hosted service for comprehensive device visibility.

Device Insight Integration: ● Enable ○ Disable
Central Mode: ○ Central ● New Central
Registration Token: [redacted]
Bypass Proxy: □ Enable to bypass proxy server
Activation Status: Activated
Activation Timestamp: Feb 04, 2025 14:56:05 AEDT
Registration Status: Registered
Primary ClearPass Server: CP1-611 (192.168.1.101)
Standby ClearPass Server: -- None -- (optional)
Polling Interval: 10 minutes
Device Sync Interval: 30 days
Endpoints active in the date range specified will be synced between ClearPass Policy Manager and Device Insight.

Device Tag Updates Action
Tags Update Action: ● No action
○ Apply action for all Tag updates
○ Apply action for selected Tag updates only

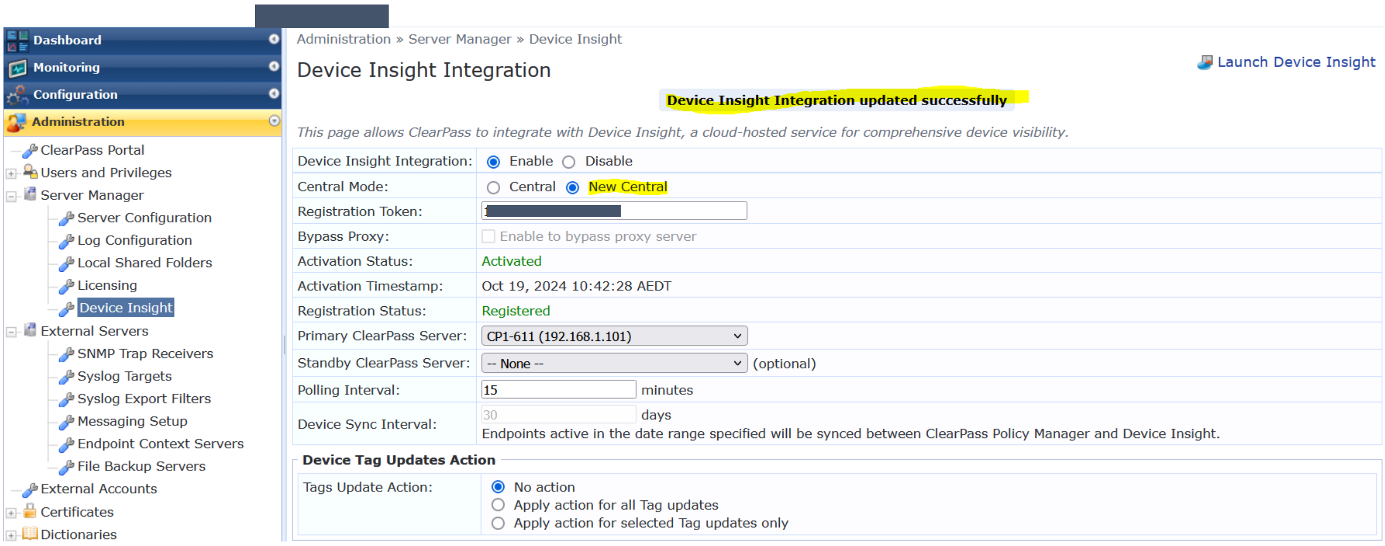
When you add this integration for the first time you also get this notice



Enable Device Insight Integration

Enabling ClearPass Device Insight will modify the behavior of ClearPass Policy Manager. All new discovery and classification will be performed by ClearPass Device Insight.
Are you sure you want to enable?

Note that the profiling behaviour will change as stated above.



Administration » Server Manager » Device Insight

Device Insight Integration

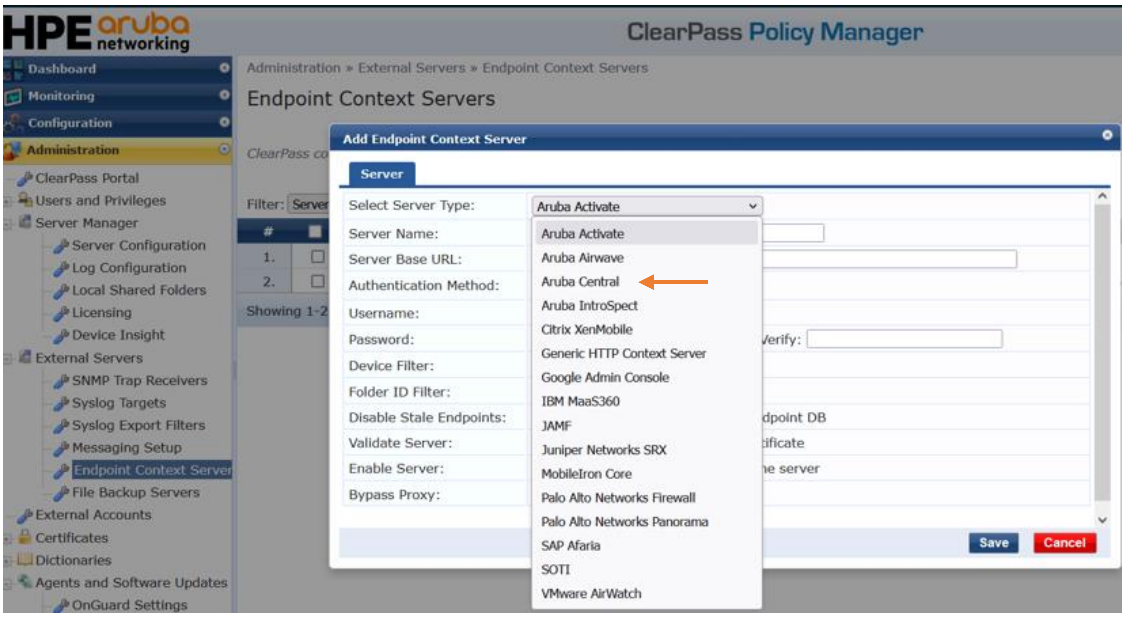
Device Insight Integration updated successfully

This page allows ClearPass to integrate with Device Insight, a cloud-hosted service for comprehensive device visibility.

Device Insight Integration: ● Enable ○ Disable
Central Mode: ○ Central ● New Central
Registration Token: [redacted]
Bypass Proxy: □ Enable to bypass proxy server
Activation Status: Activated
Activation Timestamp: Oct 19, 2024 10:42:28 AEDT
Registration Status: Registered
Primary ClearPass Server: CP1-611 (192.168.1.101)
Standby ClearPass Server: -- None -- (optional)
Polling Interval: 15 minutes
Device Sync Interval: 30 days
Endpoints active in the date range specified will be synced between ClearPass Policy Manager and Device Insight.

Device Tag Updates Action
Tags Update Action: ● No action
○ Apply action for all Tag updates
○ Apply action for selected Tag updates only

Next you need to add Aruba Central as an Endpoint Context server. As you know, ClearPass can collect endpoint information from various of sources. The screenshot below provides some of the predefined context servers.

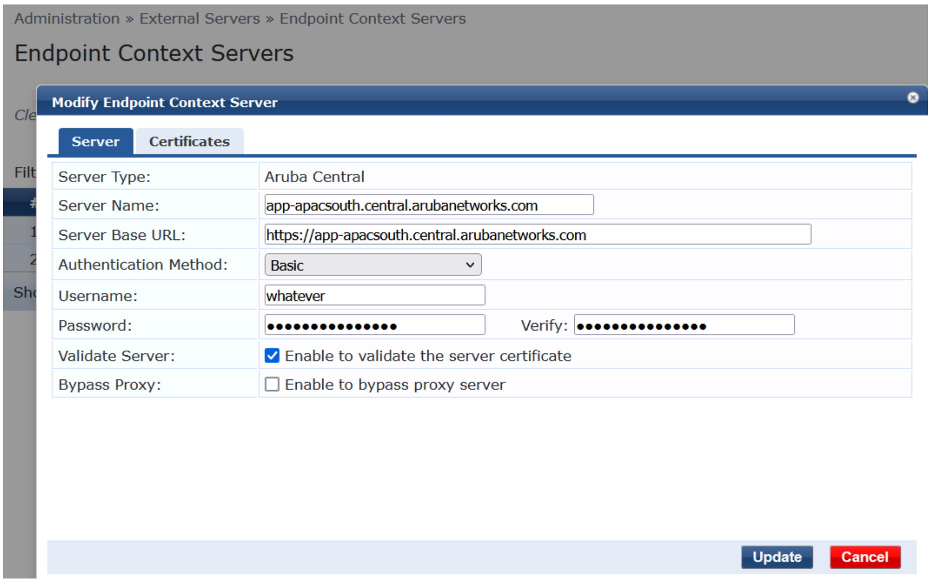


Select Server Type: Aruba Activate
Server Name:
Server Base URL:
Authentication Method:
Username:
Password:
Device Filter:
Folder ID Filter:
Disable Stale Endpoints:
Validate Server:
Enable Server:
Bypass Proxy:

Here we'll choose Aruba Central from the dropdown list and then use the appropriate server Base URL for your Aruba Central region. For example, the base URL I am using is for APAC southeast, you can get the list from here by referring to Table-2.

https://arubanetworking.hpe.com/techdocs/central/latest/content/nms/device-mgmt/communication_ports.htm#Domain2

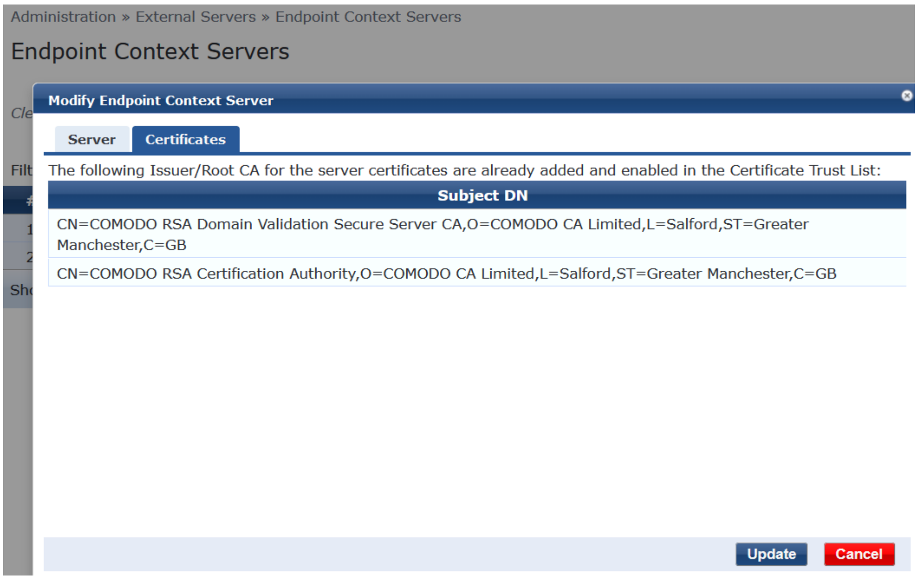
Region	HPE Aruba Networking Central URL	Region	HPE Aruba Networking Central URL
US-1	app.central.arubanetworks.com	CA Central	app-ca.central.arubanetworks.com
US-2	app-prod2.central.arubanetworks.com	CN North	app.central.arubanetworks.com.cn
US West	app-uswest4.central.arubanetworks.com	CN-2	app-china2.central.arubanetworks.com.cn
US West 5	app-uswest5.central.arubanetworks.com	AP South	app2-ap.central.arubanetworks.com
EU-1	app2-eu.central.arubanetworks.com	AP NorthEast	app-apaceast.central.arubanetworks.com
EU-2	app-eucentral2.central.arubanetworks.com	AP SouthEast	app-apacsouth.central.arubanetworks.com
EU-3	app-eucentral3.central.arubanetworks.com	UAE North	app-uaenorth1.central.arubanetworks.com



Administration » External Servers » Endpoint Context Servers
Endpoint Context Servers
Modify Endpoint Context Server
Server
Certificates
Update
Cancel

Server Type:	Aruba Central
Server Name:	app-apacsouth.central.arubanetworks.com
Server Base URL:	https://app-apacsouth.central.arubanetworks.com
Authentication Method:	Basic
Username:	whatever
Password:	••••••••••••••• Verify: •••••••••••••••
Validate Server:	☑ Enable to validate the server certificate
Bypass Proxy:	☐ Enable to bypass proxy server

Note that username and password are not used, you can put anything. Also ensure that the issuer certificate is enabled.



Administration » External Servers » Endpoint Context Servers

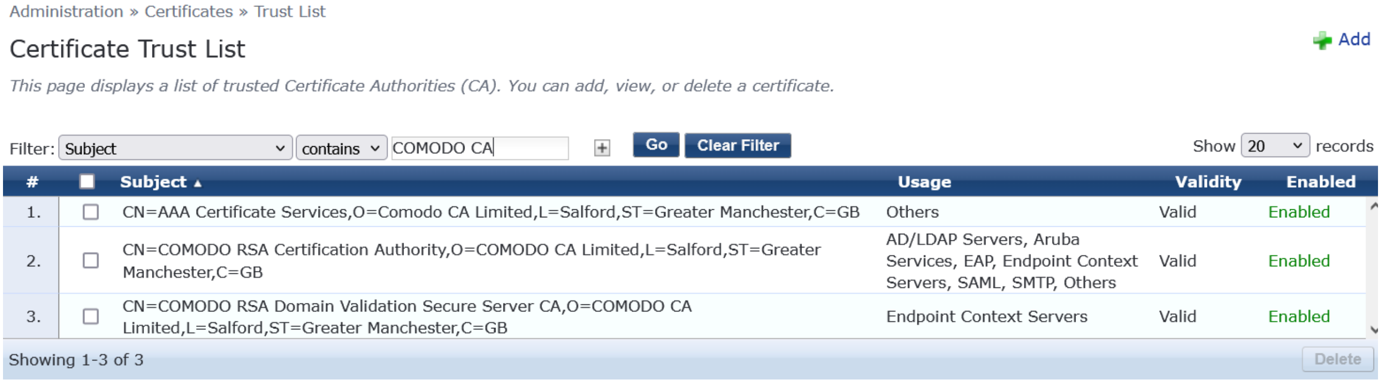
Endpoint Context Servers

Modify Endpoint Context Server

The following Issuer/Root CA for the server certificates are already added and enabled in the Certificate Trust List:

Subject DN
CN=COMODO RSA Domain Validation Secure Server CA,O=COMODO CA Limited,L=Salford,ST=Greater Manchester,C=GB
CN=COMODO RSA Certification Authority,O=COMODO CA Limited,L=Salford,ST=Greater Manchester,C=GB

You don’t need to enable anything in the Certificate trust list as it should already be enabled by default. I am showing this here just for clarity.



Administration » Certificates » Trust List

Certificate Trust List

This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.

Filter: Subject contains COMODO CA

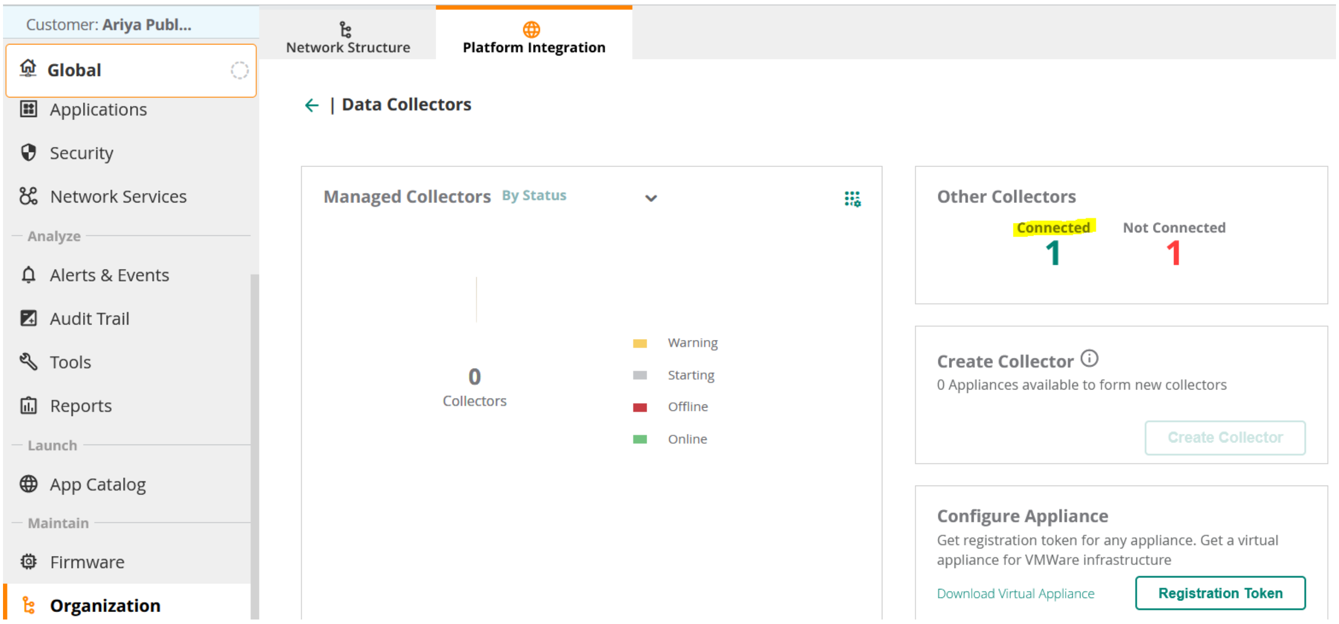
Show 20 records

#	□	Subject ▴	Usage	Validity	Enabled
1.	□	CN=AAA Certificate Services,O=Comodo CA Limited,L=Salford,ST=Greater Manchester,C=GB	Others	Valid	Enabled
2.	□	CN=COMODO RSA Certification Authority,O=COMODO CA Limited,L=Salford,ST=Greater Manchester,C=GB	AD/LDAP Servers, Aruba Services, EAP, Endpoint Context Servers, SAML, SMTP, Others	Valid	Enabled
3.	□	CN=COMODO RSA Domain Validation Secure Server CA,O=COMODO CA Limited,L=Salford,ST=Greater Manchester,C=GB	Endpoint Context Servers	Valid	Enabled

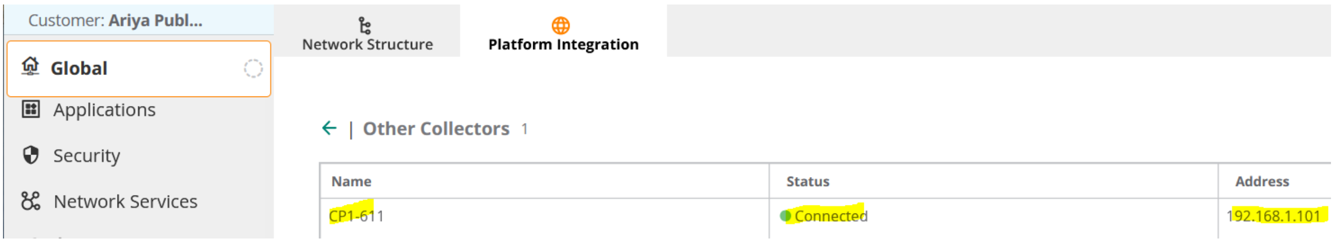
Showing 1-3 of 3

3.3 Integration Status

Let’s check the status of our integration starting with Aruba Central. We see that there is one that is connected.



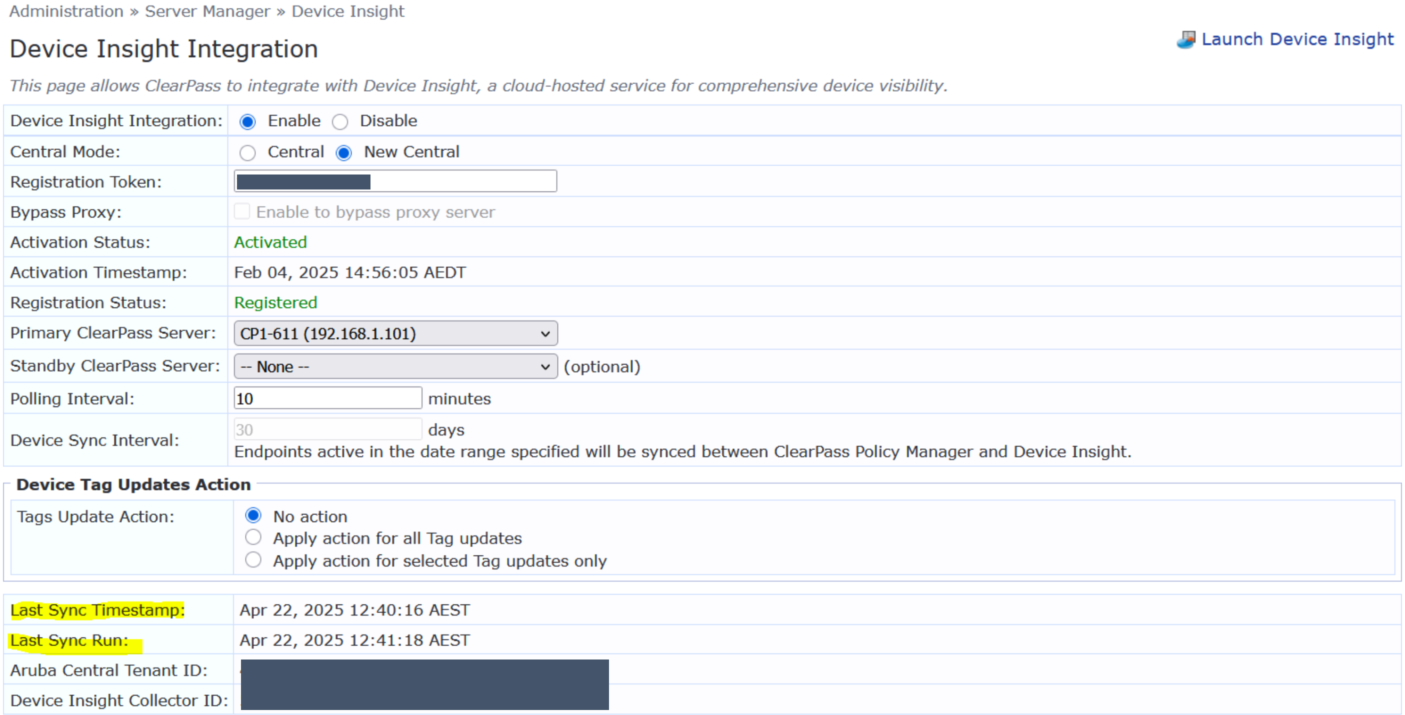
After clicking on it we get more details about the ClearPass node.



← | Other Collectors 1

Name	Status	Address
CP1-611	● Connected	192.168.1.101

Now check the Device Insight section on ClearPass and look for the last time it was synced



Device Insight Integration

This page allows ClearPass to integrate with Device Insight, a cloud-hosted service for comprehensive device visibility.

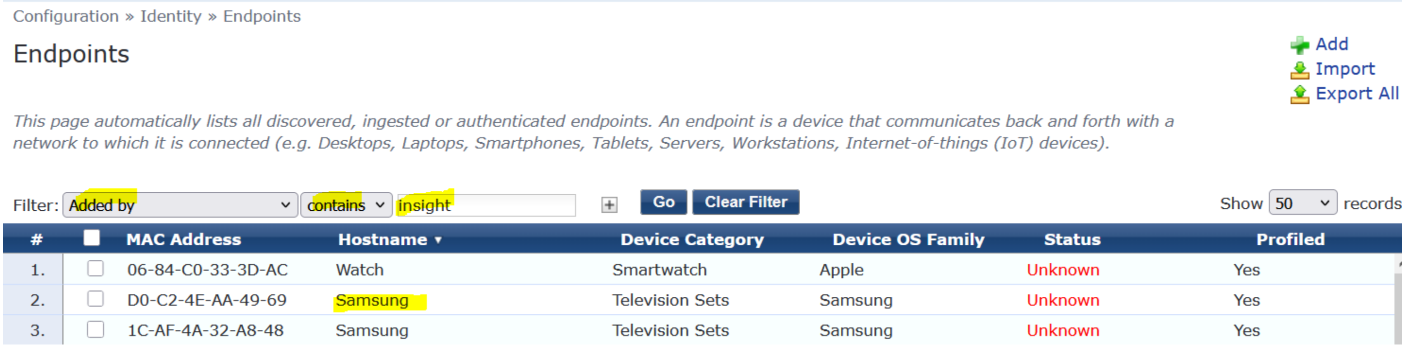
Device Insight Integration:	● Enable ○ Disable
Central Mode:	○ Central ● New Central
Registration Token:	[redacted]
Bypass Proxy:	□ Enable to bypass proxy server
Activation Status:	Activated
Activation Timestamp:	Feb 04, 2025 14:56:05 AEDT
Registration Status:	Registered
Primary ClearPass Server:	CP1-611 (192.168.1.101)
Standby ClearPass Server:	-- None -- (optional)
Polling Interval:	10 minutes
Device Sync Interval:	30 days Endpoints active in the date range specified will be synced between ClearPass Policy Manager and Device Insight.

Device Tag Updates Action

Tags Update Action:	● No action ○ Apply action for all Tag updates ○ Apply action for selected Tag updates only

Last Sync Timestamp:	Apr 22, 2025 12:40:16 AEST
Last Sync Run:	Apr 22, 2025 12:41:18 AEST
Aruba Central Tenant ID:	[redacted]
Device Insight Collector ID:	[redacted]

Since it was synced, we'll be able to see some of endpoints that was pushed by Aruba Central. For that we'll check the endpoint repository on ClearPass. Note the filter I am using.



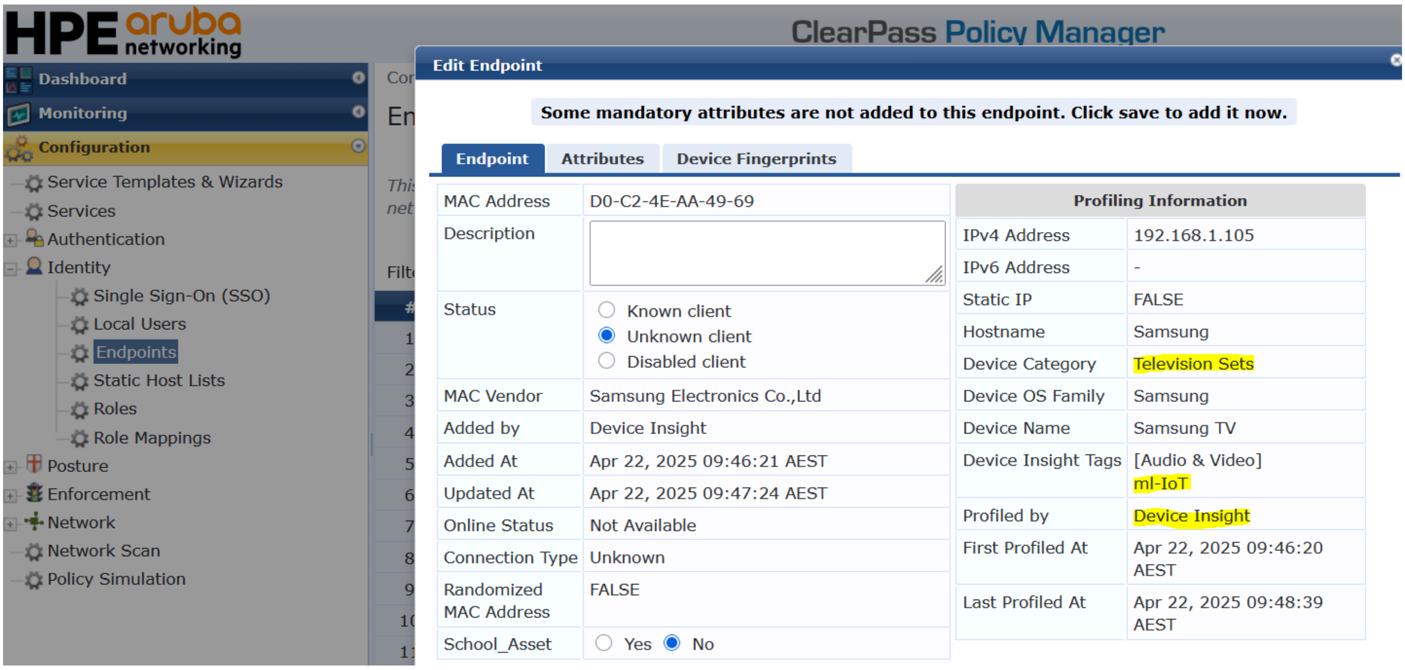
Endpoints

This page automatically lists all discovered, ingested or authenticated endpoints. An endpoint is a device that communicates back and forth with a network to which it is connected (e.g. Desktops, Laptops, Smartphones, Tablets, Servers, Workstations, Internet-of-things (IoT) devices).

Filter: Added by | contains | insight

Show 50 records

#	□	MAC Address	Hostname ▾	Device Category	Device OS Family	Status	Profiled
1.	□	06-84-C0-33-3D-AC	Watch	Smartwatch	Apple	Unknown	Yes
2.	□	D0-C2-4E-AA-49-69	Samsung	Television Sets	Samsung	Unknown	Yes
3.	□	1C-AF-4A-32-A8-48	Samsung	Television Sets	Samsung	Unknown	Yes



Some mandatory attributes are not added to this endpoint. Click save to add it now.

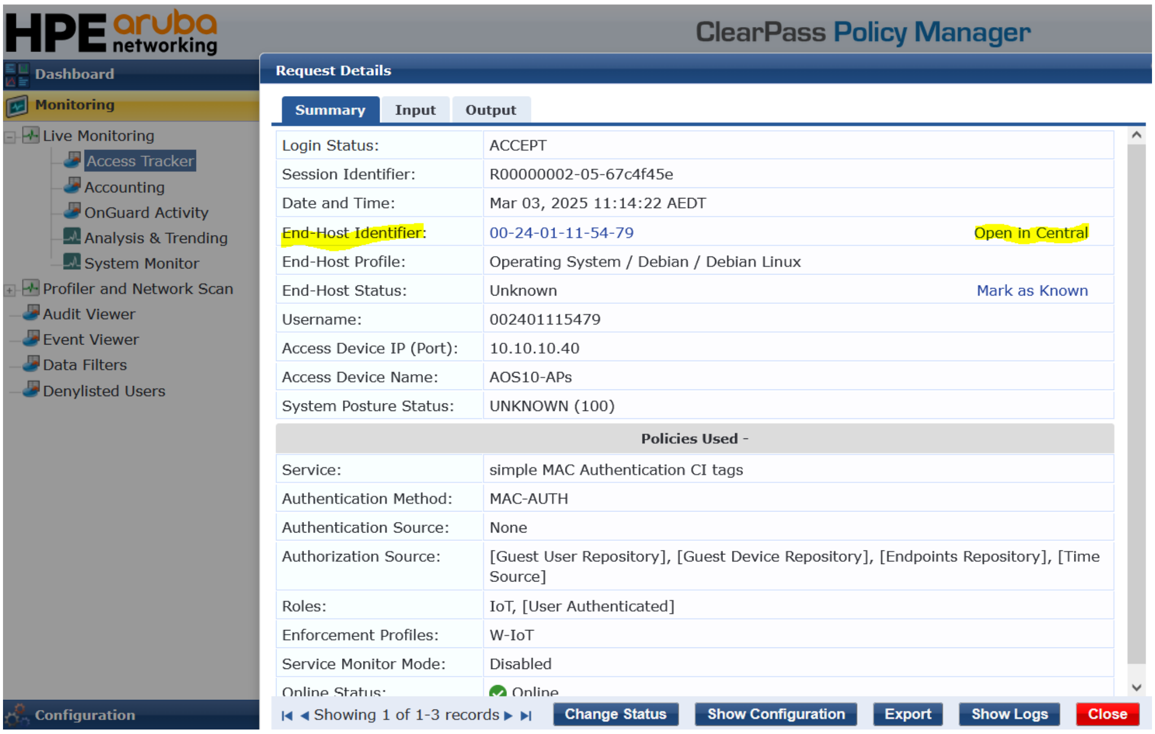
MAC Address	D0-C2-4E-AA-49-69
Description	
Status	○ Known client ● Unknown client ○ Disabled client
MAC Vendor	Samsung Electronics Co.,Ltd
Added by	Device Insight
Added At	Apr 22, 2025 09:46:21 AEST
Updated At	Apr 22, 2025 09:47:24 AEST
Online Status	Not Available
Connection Type	Unknown
Randomized MAC Address	FALSE
School_Asset	○ Yes ● No

Profiling Information	
IPv4 Address	192.168.1.105
IPv6 Address	-
Static IP	FALSE
Hostname	Samsung
Device Category	Television Sets
Device OS Family	Samsung
Device Name	Samsung TV
Device Insight Tags	[Audio & Video] ml-IoT
Profiled by	Device Insight
First Profiled At	Apr 22, 2025 09:46:20 AEST
Last Profiled At	Apr 22, 2025 09:48:39 AEST

Here in the above screenshot, Aruba Central used machine learning (ML) to categories the device as indicated by “ml-IoT”.

3.4 Access Tracker

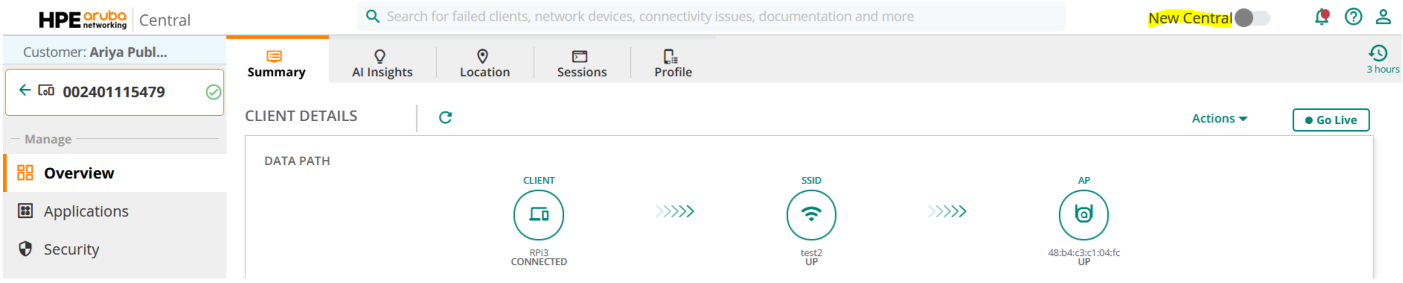
Here I’ll just check the access tracker for an authentication session, and we can simply click on the “open in Central” to get the Aruba Central view of it. This is handy as it goes to the client’s page in Aruba Central.



Login Status:	ACCEPT	
Session Identifier:	R00000002-05-67c4f45e	
Date and Time:	Mar 03, 2025 11:14:22 AEDT	
End-Host Identifier:	00-24-01-11-54-79	Open in Central
End-Host Profile:	Operating System / Debian / Debian Linux	
End-Host Status:	Unknown	Mark as Known
Username:	002401115479	
Access Device IP (Port):	10.10.10.40	
Access Device Name:	AOS10-APs	
System Posture Status:	UNKNOWN (100)	

Policies Used -	
Service:	simple MAC Authentication CI tags
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Time Source]
Roles:	IoT, [User Authenticated]
Enforcement Profiles:	W-IoT
Service Monitor Mode:	Disabled
Online Status:	✓ Online

Note that currently it will first open in Classic Central but later when you use only New Central, then it will open it in New Central directly. You should also change the base URL in “Endpoint Context server”.


HPE aruba networking | Central
Search for failed clients, network devices, connectivity issues, documentation and more
New Central
3 hours
Summary
AI Insights
Location
Sessions
Profile
Manage
Overview
Applications
Security
Actions
Go Live

Customer: Ariya Publ...

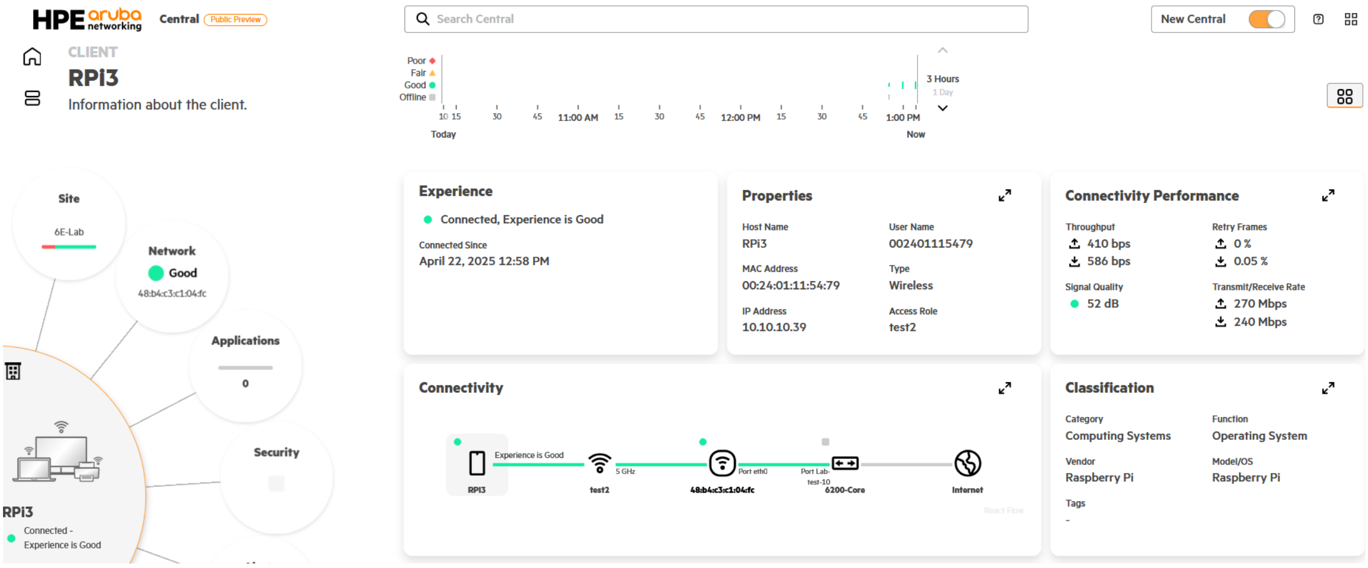
002401115479

CLIENT DETAILS

DATA PATH

CLIENT	SSID	AP
RPi3 CONNECTED	test2 UP	48:b4:c3:c1:04:fc UP

This is view in New Central.



CLIENT

RPI3

Information about the client.

Experience

● Connected, Experience is Good

Connected Since
April 22, 2025 12:58 PM

Properties

Host Name	User Name
RPi3	002401115479
MAC Address	**Type**
00:24:01:11:54:79	Wireless
IP Address	**Access Role**
10.10.10.39	test2

Connectivity Performance

Throughput	Retry Frames
↑ 410 bps	↑ 0 %
↓ 586 bps	↓ 0.05 %
Signal Quality	**Transmit/Receive Rate**
● 52 dB	↑ 270 Mbps
	↓ 240 Mbps

Connectivity

Classification

Category	Function
Computing Systems	Operating System
Vendor	**Model/OS**
Raspberry Pi	Raspberry Pi
Tags	
-	

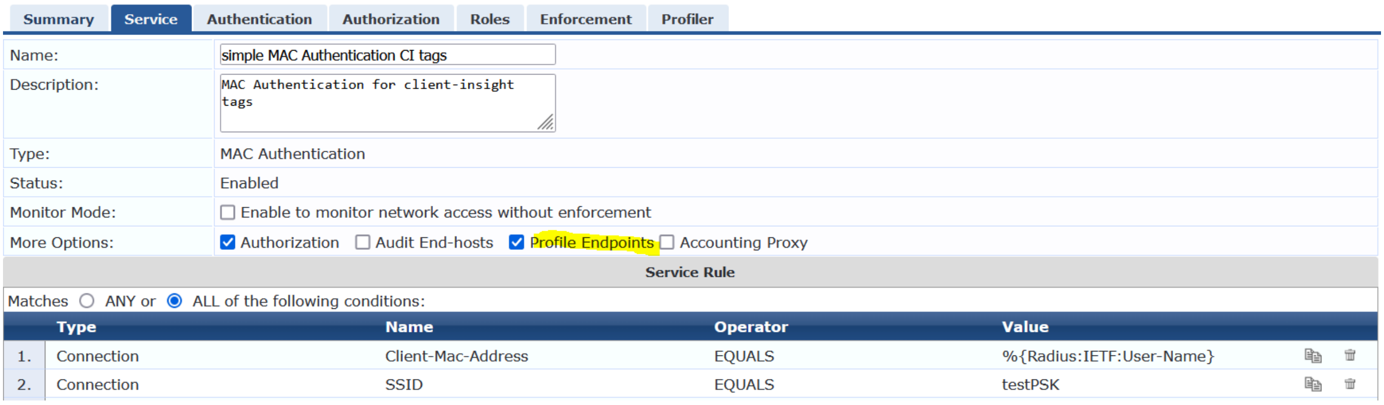
4 New Central Device Insight Tag

The lab setup uses clients that connects to AP-615 broadcasting “test2” PSK based WLAN with MAC authentication.

I won’t be covering the Instant AP 8.12.x configuration as it is same as the previous technote with classic central (look that up). But remember to enable AppRF and as a re-cap there are two user roles that ClearPass will be sending back to the Instant AP. And they are user roles “IoT-Lab” mapped to VLAN 31 and “investigate” mapped to VLAN 32. So, these user-roles needs to be configured in IAP side.

4.1 ClearPass Service

Now we need a ClearPass authentication service for this WLAN that we have called “simple MAC Authentication CI tags”. Remember that we enable MAC authentication for the PSK SSID, that why we need a MAC auth service in ClearPass.

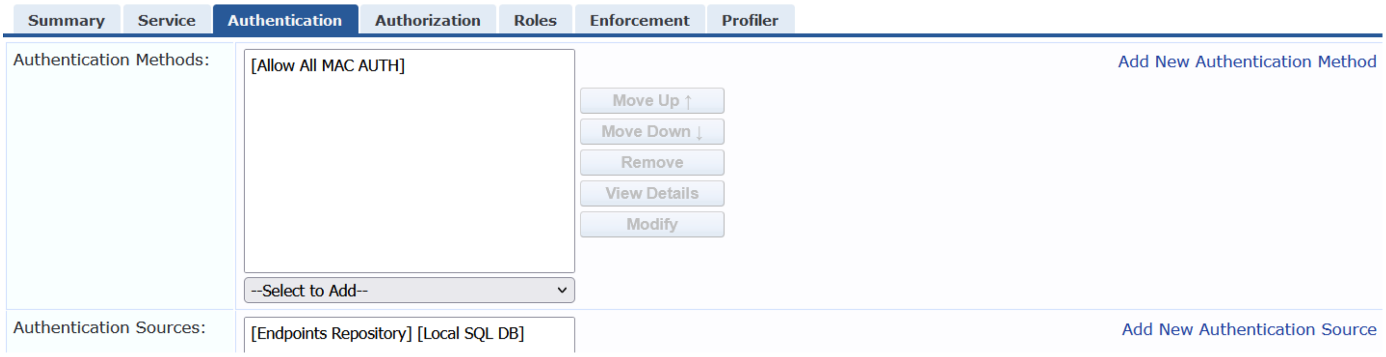


Name:	simple MAC Authentication CI tags
Description:	MAC Authentication for client-insight tags
Type:	MAC Authentication
Status:	Enabled
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	☑ Authorization □ Audit End-hosts ☑ Profile Endpoints □ Accounting Proxy

Service Rule

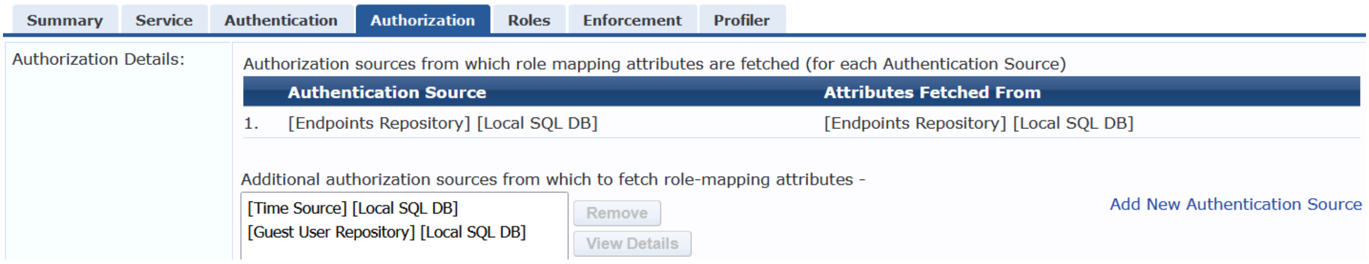
Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
2.	Connection	SSID	EQUALS	testPSK



Authentication Methods: [Allow All MAC AUTH]

Authentication Sources: [Endpoints Repository] [Local SQL DB]



Authorization Details:

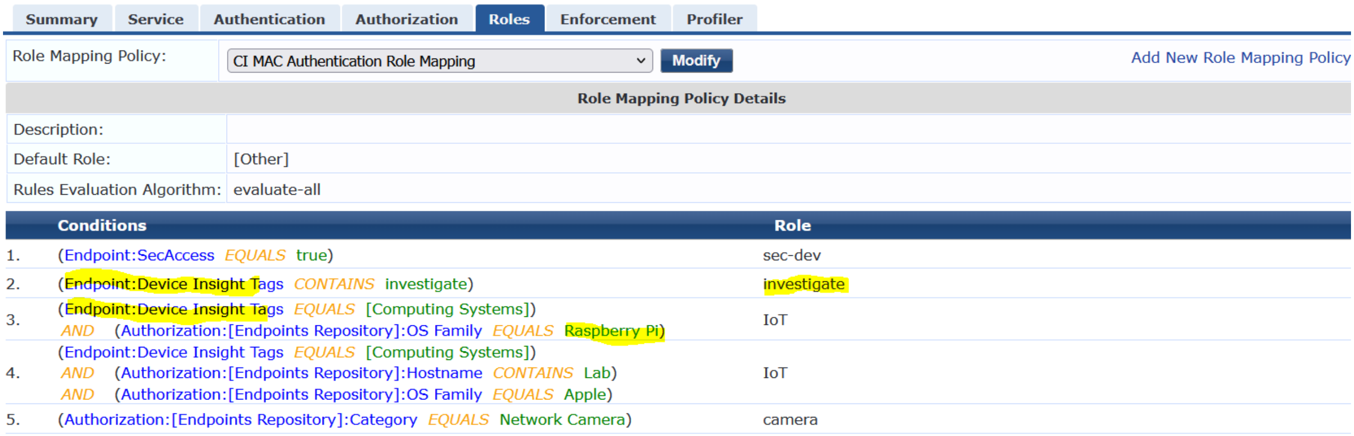
Authorization sources from which role mapping attributes are fetched (for each Authentication Source)

	Authentication Source	Attributes Fetched From
1.	[Endpoints Repository] [Local SQL DB]	[Endpoints Repository] [Local SQL DB]

Additional authorization sources from which to fetch role-mapping attributes -

[Time Source] [Local SQL DB]
[Guest User Repository] [Local SQL DB]

In our use case, IoT devices should not be running SSH and hence we can catch them with this role mapping.

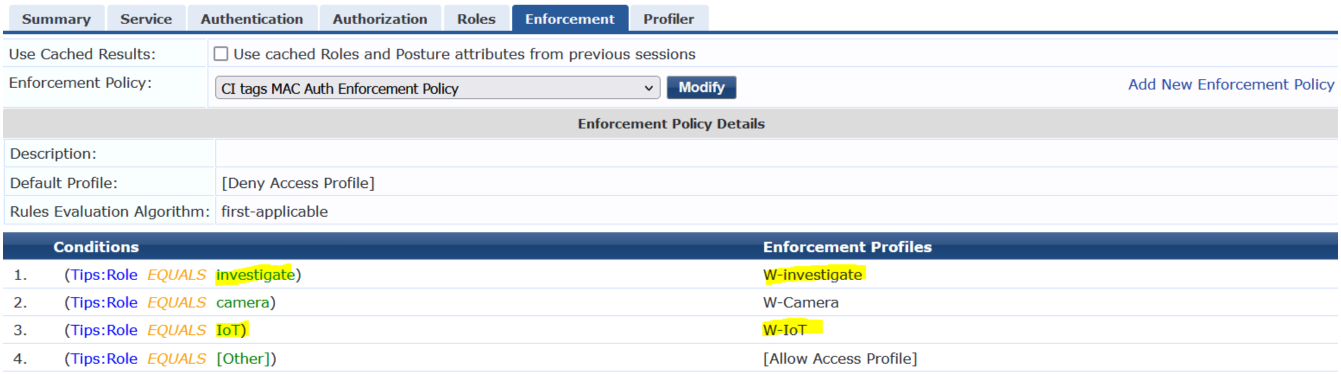


Role Mapping Policy:	CI MAC Authentication Role Mapping

Role Mapping Policy Details

Description:	
Default Role:	[Other]
Rules Evaluation Algorithm:	evaluate-all

	Conditions	Role
1.	(Endpoint:SecAccess EQUALS true)	sec-dev
2.	(Endpoint:Device Insight Tags CONTAINS investigate)	investigate
3.	(Endpoint:Device Insight Tags EQUALS [Computing Systems]) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Raspberry Pi)	IoT
4.	(Endpoint:Device Insight Tags EQUALS [Computing Systems]) AND (Authorization:[Endpoints Repository]:Hostname CONTAINS Lab) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Apple)	IoT
5.	(Authorization:[Endpoints Repository]:Category EQUALS Network Camera)	camera

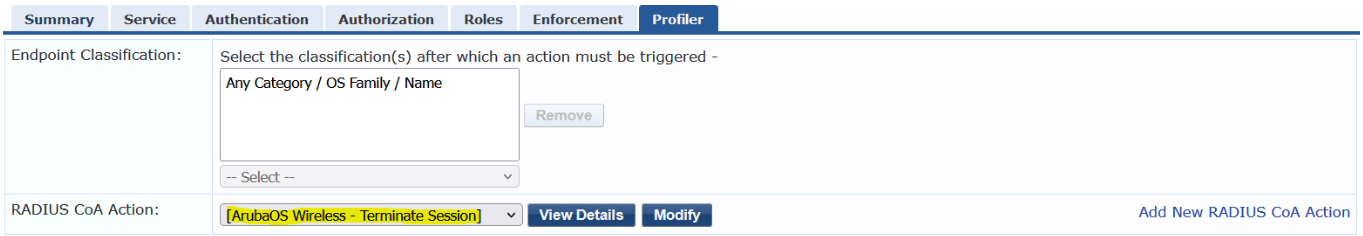


Use Cached Results:	☐ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	CI tags MAC Auth Enforcement Policy

Enforcement Policy Details

Description:	
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Role EQUALS investigate)	W-investigate
2.	(Tips:Role EQUALS camera)	W-Camera
3.	(Tips:Role EQUALS IoT)	W-IoT
4.	(Tips:Role EQUALS [Other])	[Allow Access Profile]



Endpoint Classification:	Select the classification(s) after which an action must be triggered - Any Category / OS Family / Name
RADIUS CoA Action:	[ArubaOS Wireless - Terminate Session]

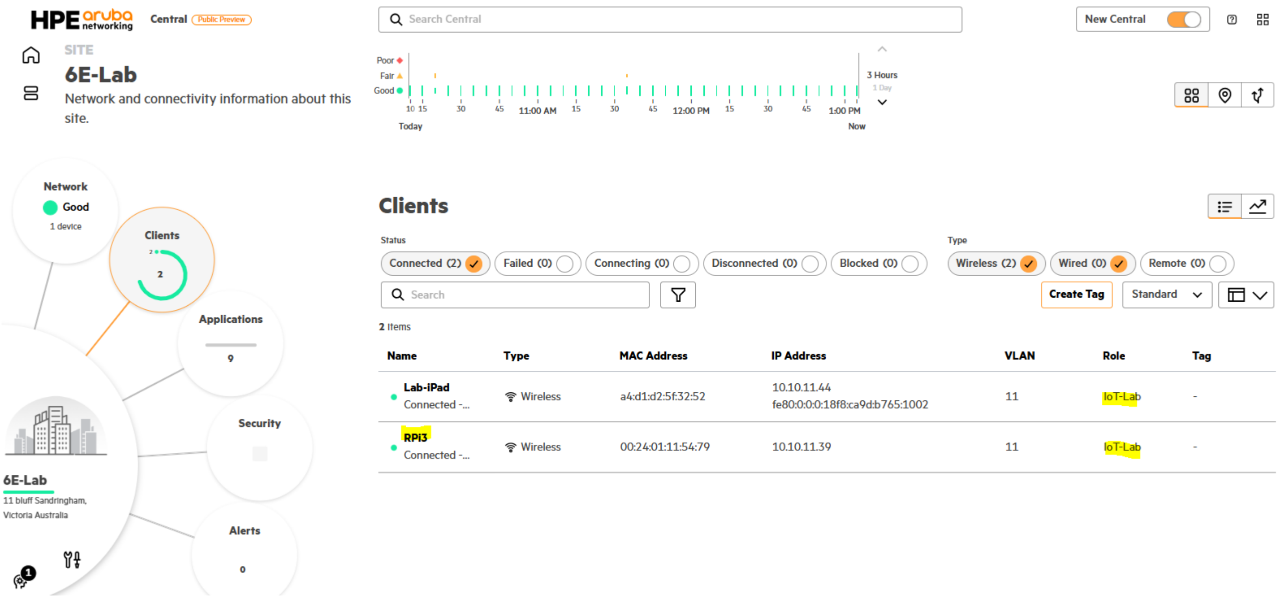
The two enforcement profiles are

- W-IoT that is sending Aruba-user-role = IoT-Lab
- W-investigate that is sending Aruba-user-role = investigate

5 Device Attribute Testing

5.1 Initial Device Attribute Testing

Now we get couple of clients connect to the “test2”. It shows up in Aruba Central client list . We see that it has the correct user-role = IoT-Lab and they are in VLAN 11. Note that one is RPi and the other an iPad.



SITE

6E-Lab

Network and connectivity information about this site.

Clients

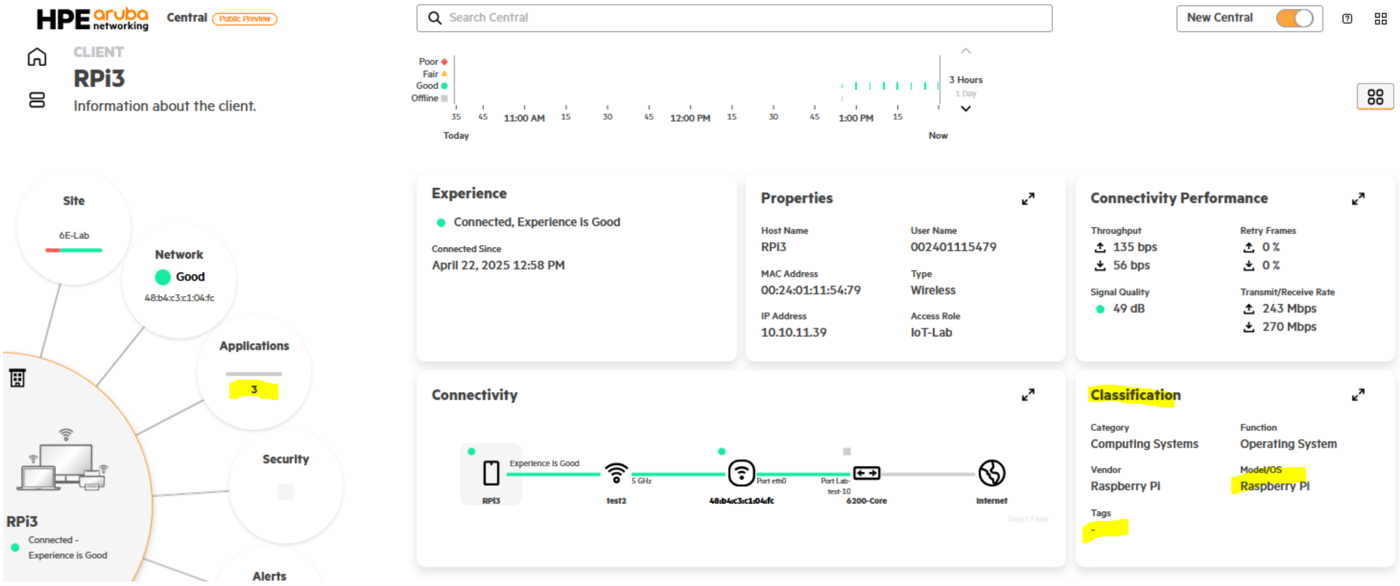
Status: Connected (2) ✓ · Failed (0) ○ · Connecting (0) ○ · Disconnected (0) ○ · Blocked (0) ○

Type: Wireless (2) ✓ · Wired (0) ✓ · Remote (0) ○

2 Items

Name	Type	MAC Address	IP Address	VLAN	Role	Tag
Lab-iPad Connected -...	Wireless	a4:d1:d2:5f:32:52	10.10.11.44 fe80:0:0:0:18f8:ca9d:b765:1002	11	IoT-Lab	-
RPi3 Connected -...	Wireless	00:24:01:11:54:79	10.10.11.39	11	IoT-Lab	-

Next, we’ll click on a client to see the details. The context changes and the client becomes the sun in Solaris view.



CLIENT

RPi3

Information about the client.

Experience

Connected, Experience Is Good

Connected Since: April 22, 2025 12:58 PM

Properties

Host Name	User Name
RPI3	002401115479
MAC Address	**Type**
00:24:01:11:54:79	Wireless
IP Address	**Access Role**
10.10.11.39	IoT-Lab

Connectivity Performance

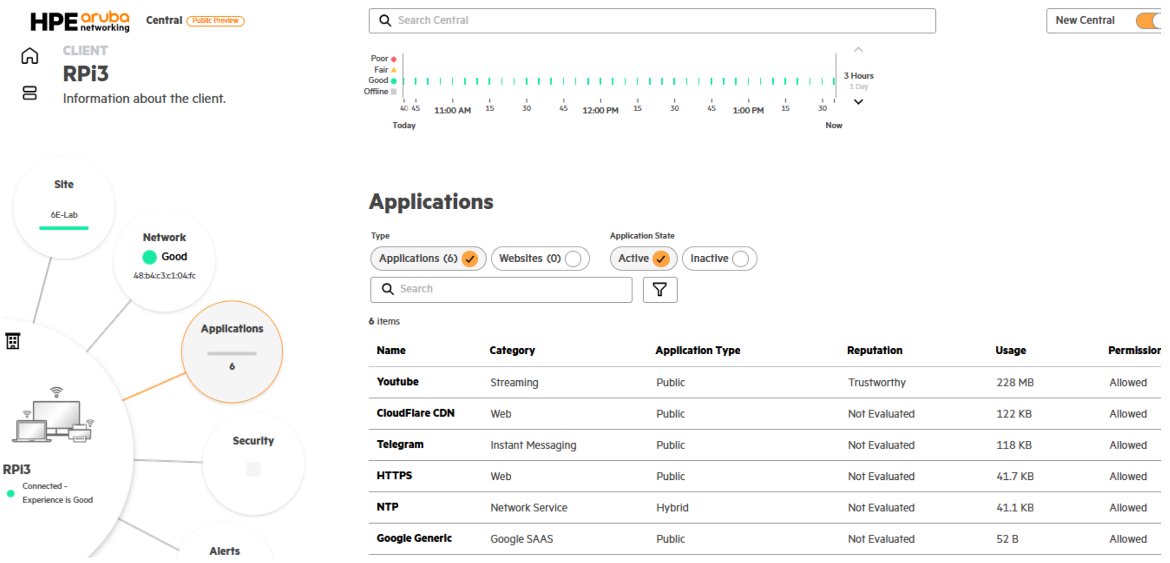
Throughput	Retry Frames
↑ 135 bps ↓ 56 bps	↑ 0 % ↓ 0 %
Signal Quality	**Transmit/Receive Rate**
49 dB	↑ 243 Mbps ↓ 270 Mbps

Classification

Category	Function
Computing Systems	Operating System
Vendor	**Model/OS**
Raspberry Pi	Raspberry Pi

Tags: -

As you can see in the above screenshot, that are no tags that are assigned to it. Next we need to check if the applications are being identified as we have enabled AppRF. So click on the Application planet to see the application that are used by RPi client.



CLIENT

RPi3

Information about the client.

Applications

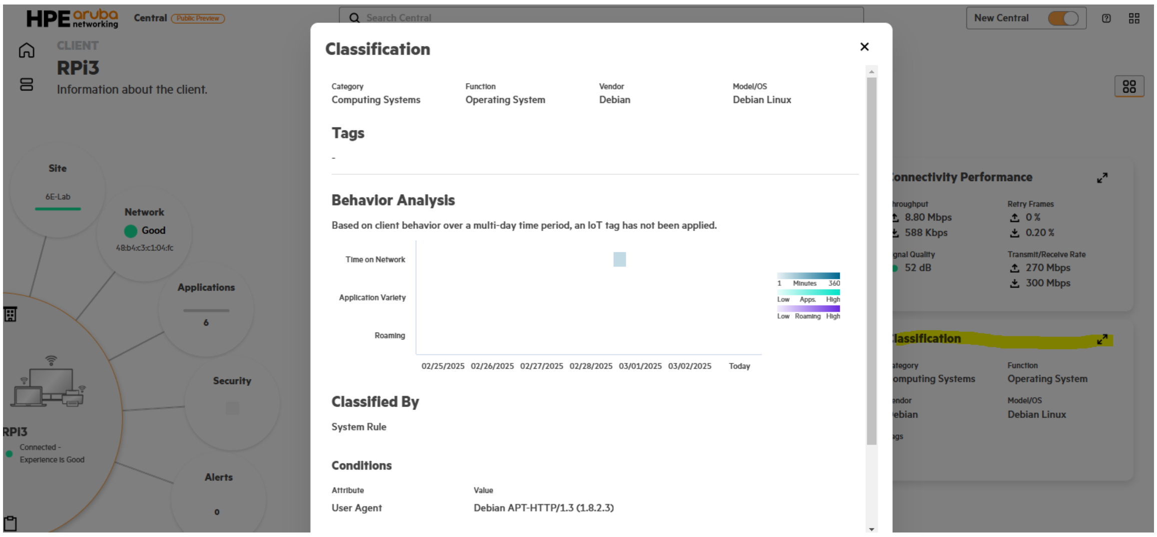
Type: Applications (6) ✓ Websites (0) ○

Application State: Active ✓ Inactive ○

6 items

Name	Category	Application Type	Reputation	Usage	Permissior
Youtube	Streaming	Public	Trustworthy	228 MB	Allowed
CloudFlare CDN	Web	Public	Not Evaluated	122 KB	Allowed
Telegram	Instant Messaging	Public	Not Evaluated	118 KB	Allowed
HTTPS	Web	Public	Not Evaluated	41.7 KB	Allowed
NTP	Network Service	Hybrid	Not Evaluated	41.1 KB	Allowed
Google Generic	Google SAAS	Public	Not Evaluated	52 B	Allowed

We'll go back to the previous page and we'll check the Classification card by expanding it to see some details.



Classification

Category	Function	Vendor	Model/OS
Computing Systems	Operating System	Debian	Debian Linux

Tags

-

Behavior Analysis

Based on client behavior over a multi-day time period, an IoT tag has not been applied.

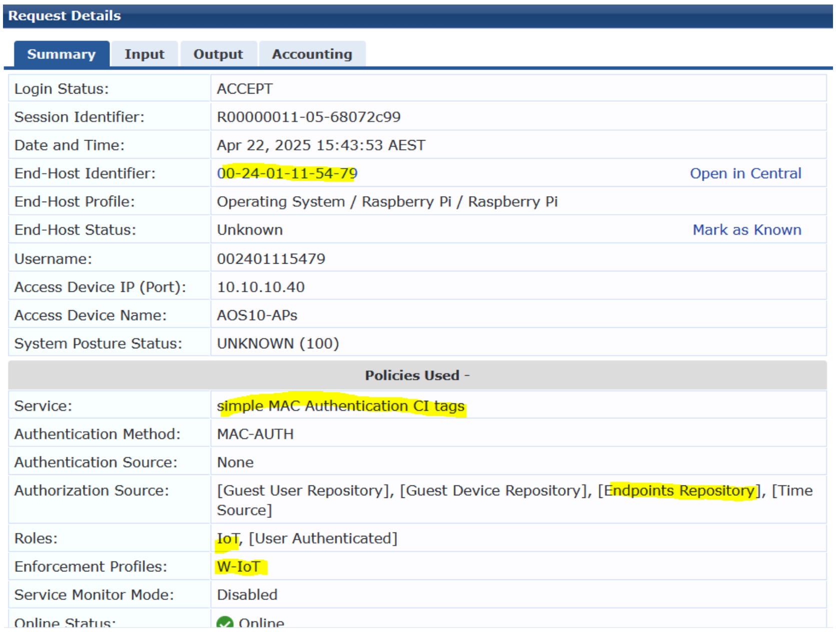
Classified By

System Rule

Conditions

Attribute	Value
User Agent	Debian APT-HTTP/1.3 (1.8.2.3)

Note that New Central does not show the "Flow Attributes" like in classic Central. Looking at the Access Tracker we see how roles were assigned to this client. Remember in our service it allows all MAC authentication, however it uses role-mapping policy to assign the roles based on the various attributes. Then those gets referenced in the enforcement policy.

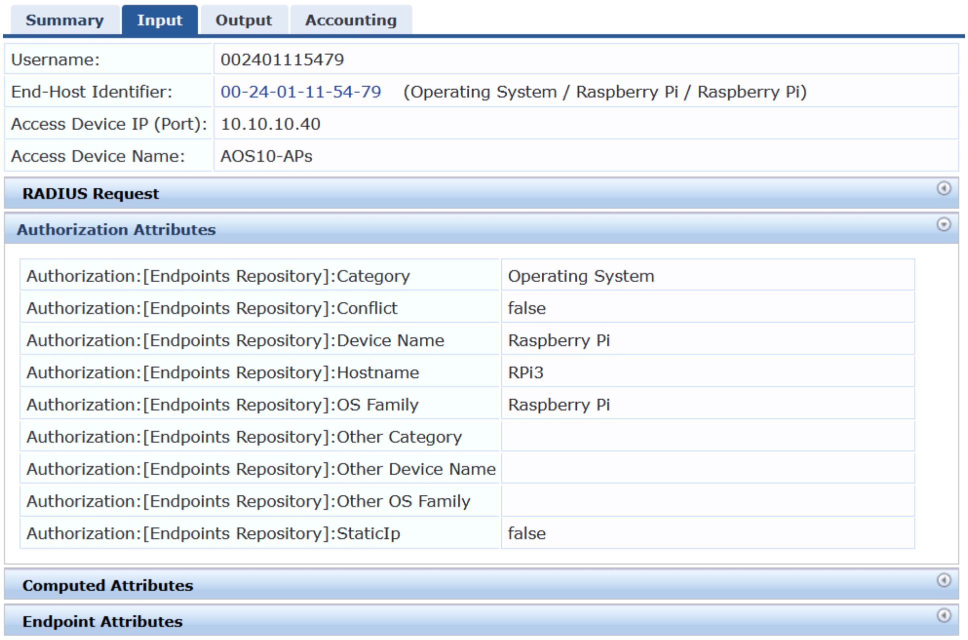


Request Details

Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R00000011-05-68072c99
Date and Time:	Apr 22, 2025 15:43:53 AEST
End-Host Identifier:	00-24-01-11-54-79 Open in Central
End-Host Profile:	Operating System / Raspberry Pi / Raspberry Pi
End-Host Status:	Unknown Mark as Known
Username:	002401115479
Access Device IP (Port):	10.10.10.40
Access Device Name:	AOS10-APs
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	simple MAC Authentication CI tags
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Time Source]
Roles:	IoT, [User Authenticated]
Enforcement Profiles:	W-IoT
Service Monitor Mode:	Disabled
Online Status:	✓ Online

The authorisation section shows the various Endpoints Repository attributes that we can match.



Username:	002401115479
End-Host Identifier:	00-24-01-11-54-79 (Operating System / Raspberry Pi / Raspberry Pi)
Access Device IP (Port):	10.10.10.40
Access Device Name:	AOS10-APs

RADIUS Request

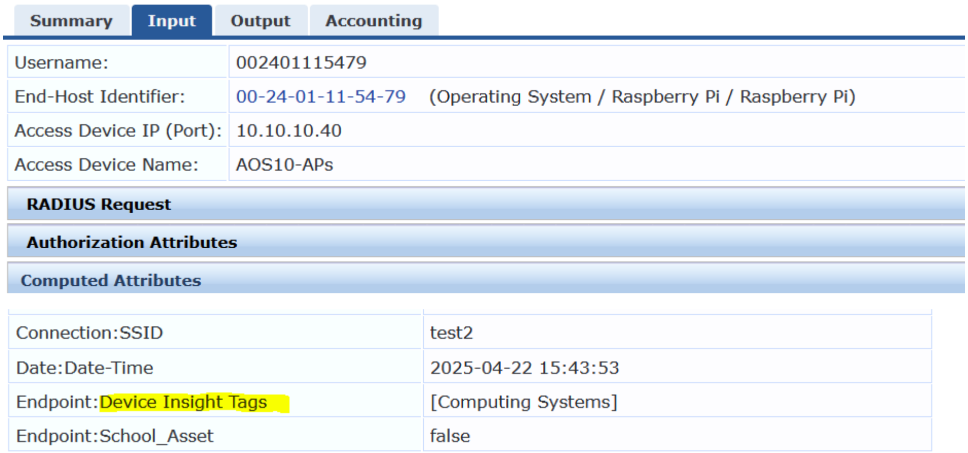
Authorization Attributes

Authorization:[Endpoints Repository]:Category	Operating System
Authorization:[Endpoints Repository]:Conflict	false
Authorization:[Endpoints Repository]:Device Name	Raspberry Pi
Authorization:[Endpoints Repository]:Hostname	RPi3
Authorization:[Endpoints Repository]:OS Family	Raspberry Pi
Authorization:[Endpoints Repository]:Other Category	
Authorization:[Endpoints Repository]:Other Device Name	
Authorization:[Endpoints Repository]:Other OS Family	
Authorization:[Endpoints Repository]:StaticIp	false

Computed Attributes

Endpoint Attributes

When we click on the “Computed attributes”, we see that it was profiles by Aruba central as indicated b yDevice Insight Tags = [Computing Systems]



Username:	002401115479
End-Host Identifier:	00-24-01-11-54-79 (Operating System / Raspberry Pi / Raspberry Pi)
Access Device IP (Port):	10.10.10.40
Access Device Name:	AOS10-APs

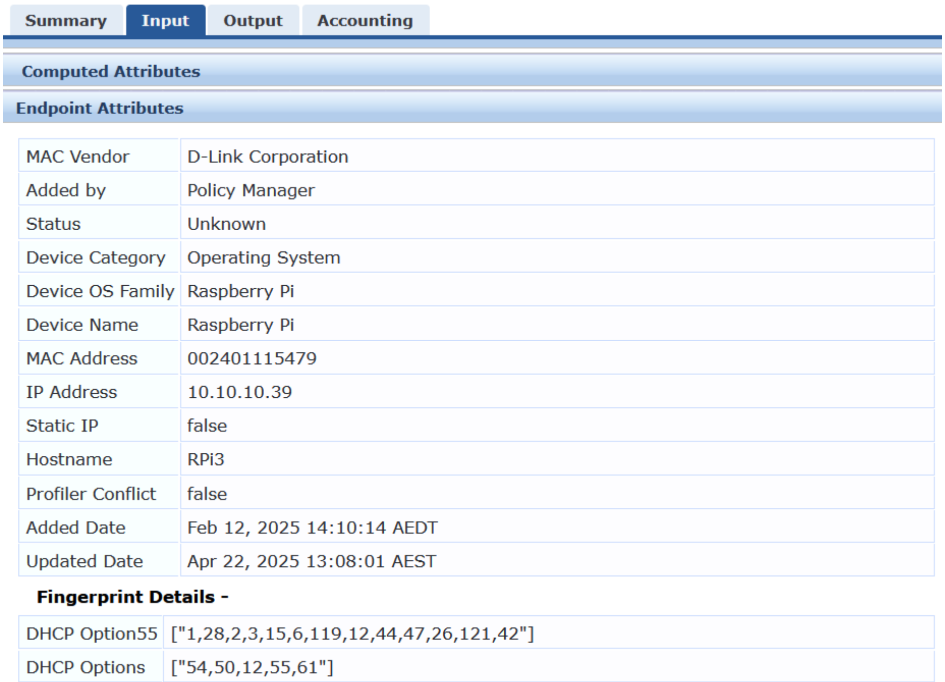
RADIUS Request

Authorization Attributes

Computed Attributes

Connection:SSID	test2
Date:Date-Time	2025-04-22 15:43:53
Endpoint:Device Insight Tags	[Computing Systems]
Endpoint:School_Asset	false

Next, we’ll look at the Endpoint Attributes.



Computed Attributes

Endpoint Attributes

MAC Vendor	D-Link Corporation
Added by	Policy Manager
Status	Unknown
Device Category	Operating System
Device OS Family	Raspberry Pi
Device Name	Raspberry Pi
MAC Address	002401115479
IP Address	10.10.10.39
Static IP	false
Hostname	RPi3
Profiler Conflict	false
Added Date	Feb 12, 2025 14:10:14 AEDT
Updated Date	Apr 22, 2025 13:08:01 AEST

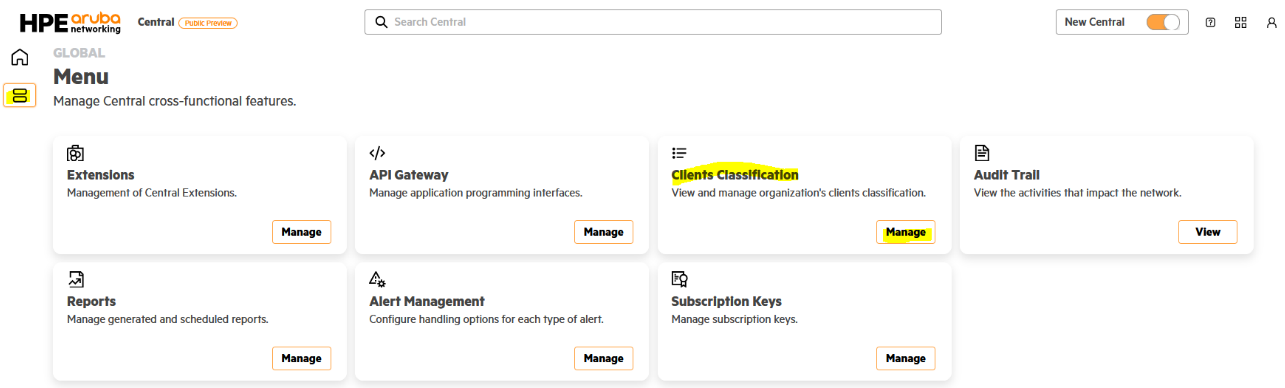
Fingerprint Details -

DHCP Option55	["1,28,2,3,15,6,119,12,44,47,26,121,42"]
DHCP Options	["54,50,12,55,61"]

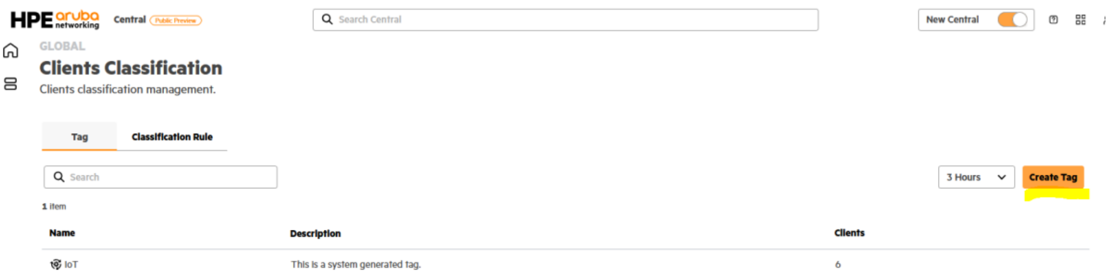
So, currently, we establish the baseline.

5.2 Creating Device Tags

Here we'll create a new tag to catch the IoT devices that are initiating SSH. You can create a new Tag in several ways. One way is to go to the main menu and then click on the "Manage" Client Classification as shown below.

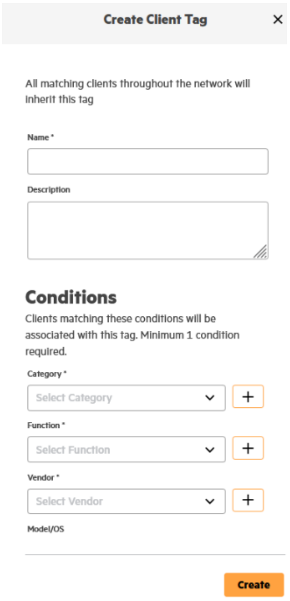

HPE aruba networking
Central Public Preview
Search Central
New Central
GLOBAL
Menu
Manage Central cross-functional features.
Extensions
Management of Central Extensions.
Manage
API Gateway
Manage application programming interfaces.
Manage
Clients Classification
View and manage organization's clients classification.
Manage
Audit Trail
View the activities that impact the network.
View
Reports
Manage generated and scheduled reports.
Manage
Alert Management
Configure handling options for each type of alert.
Manage
Subscription Keys
Manage subscription keys.
Manage

And then clicking on the "Create Tag" button.



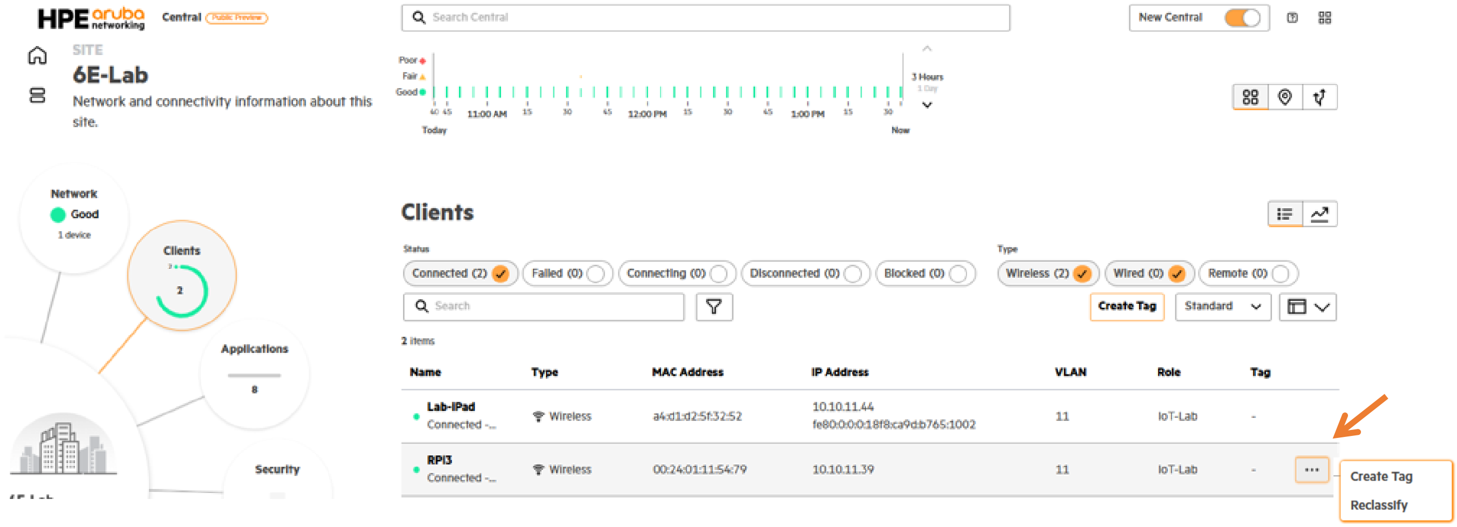
1 item

Name	Description	Clients
IoT	This is a system generated tag.	6


Create Client Tag
All matching clients throughout the network will inherit this tag
Name *
Description
Conditions
Clients matching these conditions will be associated with this tag. Minimum 1 condition required.
Category *
Select Category
Function *
Select Function
Vendor *
Select Vendor
Model/OS
Create

Here you need to remember the category and function type, etc. For me, the other easier way that does not require you to remember that information is by going to the client section and hover over the client you want to add a tag and click on the ⋯. Here we are looking at the RPi3.

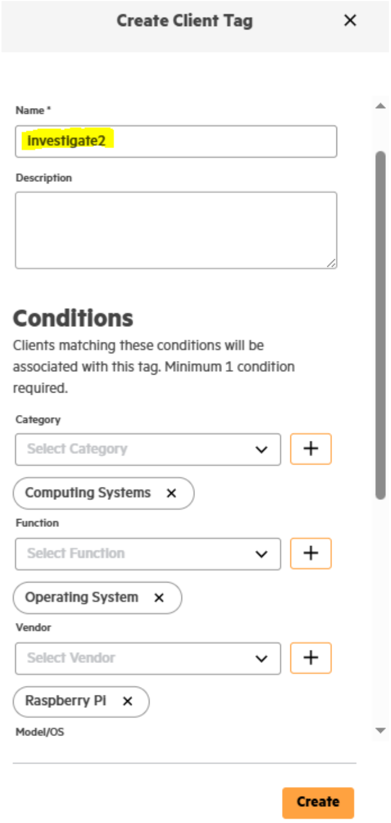
This is shown below.



2 items

Name	Type	MAC Address	IP Address	VLAN	Role	Tag
Lab-IPad Connected -...	Wireless	a4:d1:d2:5f:32:52	10.10.11.44 fe80:0:0:0:18f8:ca9d:b765:1002	11	IoT-Lab	-
RPI3 Connected -...	Wireless	00:24:01:11:54:79	10.10.11.39	11	IoT-Lab	-

The “Create Client Tag” card provides various conditions that can be used while creating a tag. It has already used the conditions known for that client like category, operating system, etc.



Create Client Tag

Name * investigate2

Description

Conditions

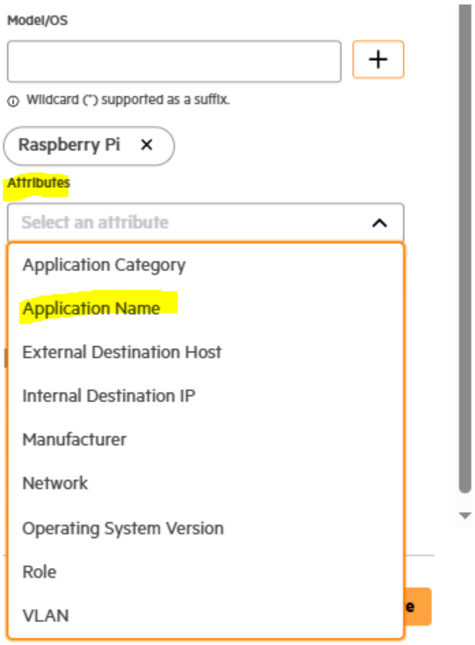
Clients matching these conditions will be associated with this tag. Minimum 1 condition required.

Category: Select Category — Computing Systems ×

Function: Select Function — Operating System ×

Vendor: Select Vendor — Raspberry Pi ×

Model/OS



Model/OS

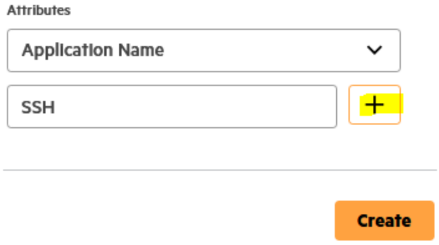
Wildcard (*) supported as a suffix.

Raspberry Pi ×

Attributes: Select an attribute

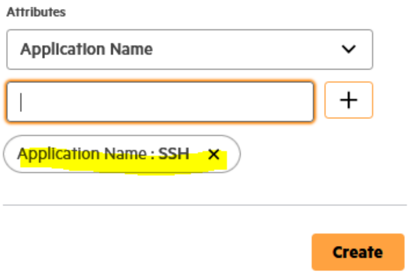
- Application Category
- Application Name
- External Destination Host
- Internal Destination IP
- Manufacturer
- Network
- Operating System Version
- Role
- VLAN

We’ll keep it simple and add an attribute of Application Name = SSH. Remember to click on the + sign to add it in



Attributes: Application Name

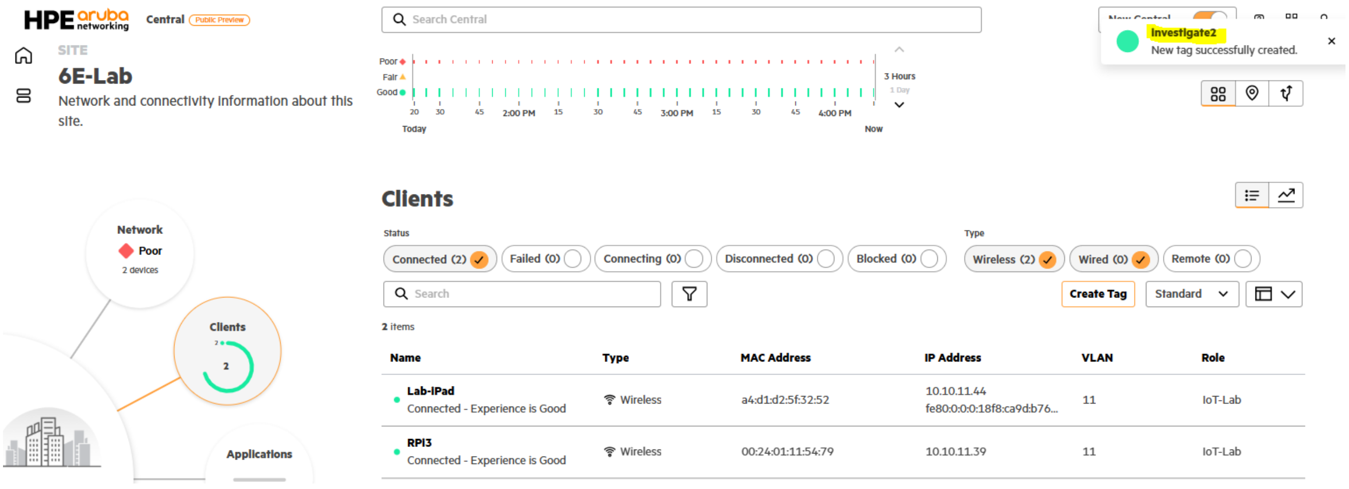
SSH +



Attributes: Application Name

Application Name : SSH ×

Once you click on the “Create” button, the tag gets created and saved as shown below.



investigate2 — New tag successfully created.

SITE

6E-Lab

Network and connectivity information about this site.

Clients

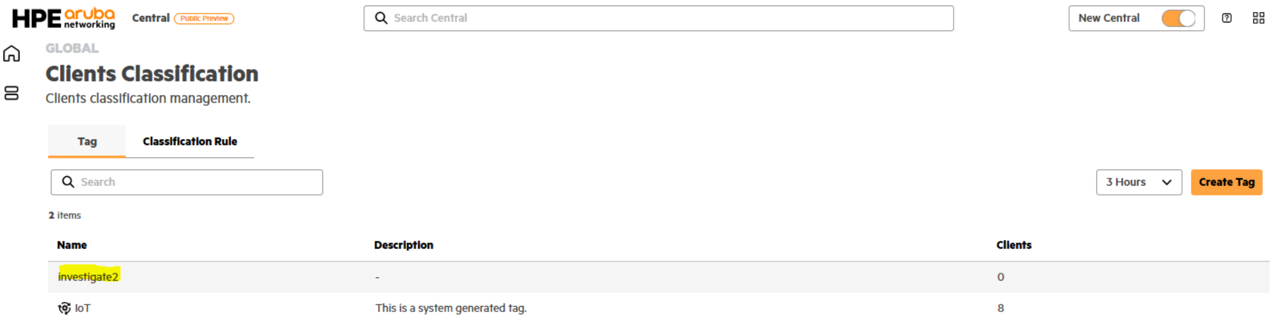
Status: Connected (2) ✓ | Failed (0) ○ | Connecting (0) ○ | Disconnected (0) ○ | Blocked (0) ○

Type: Wireless (2) ✓ | Wired (0) ✓ | Remote (0) ○

2 items

Name	Type	MAC Address	IP Address	VLAN	Role
Lab-IPad Connected - Experience is Good	Wireless	a4:d1:d2:5f:32:52	10.10.11.44 fe80:0:0:0:18f8:ca9d:b76...	11	IoT-Lab
RPI3 Connected - Experience is Good	Wireless	00:24:01:11:54:79	10.10.11.39	11	IoT-Lab

So now when we navigate to “Clients Classification”, we should see our new tag.



Clients Classification

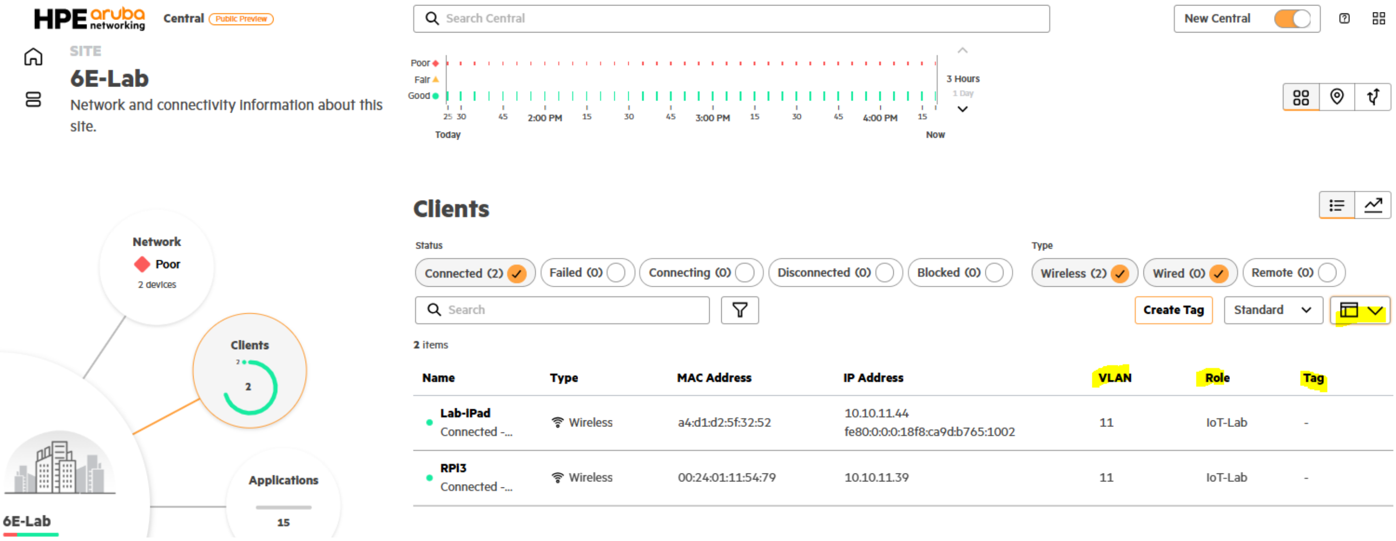
Clients classification management.

2 items

Name	Description	Clients
investigate2	-	0
IoT	This is a system generated tag.	8

5.3 Device Insight Tag Testing

We are now ready to perform our testing. I have reconnected both our clients to the same “test2” WLAN and they are both on VLAN 11. Note that I had added “Role” and “Tag” column using the customisation table feature.

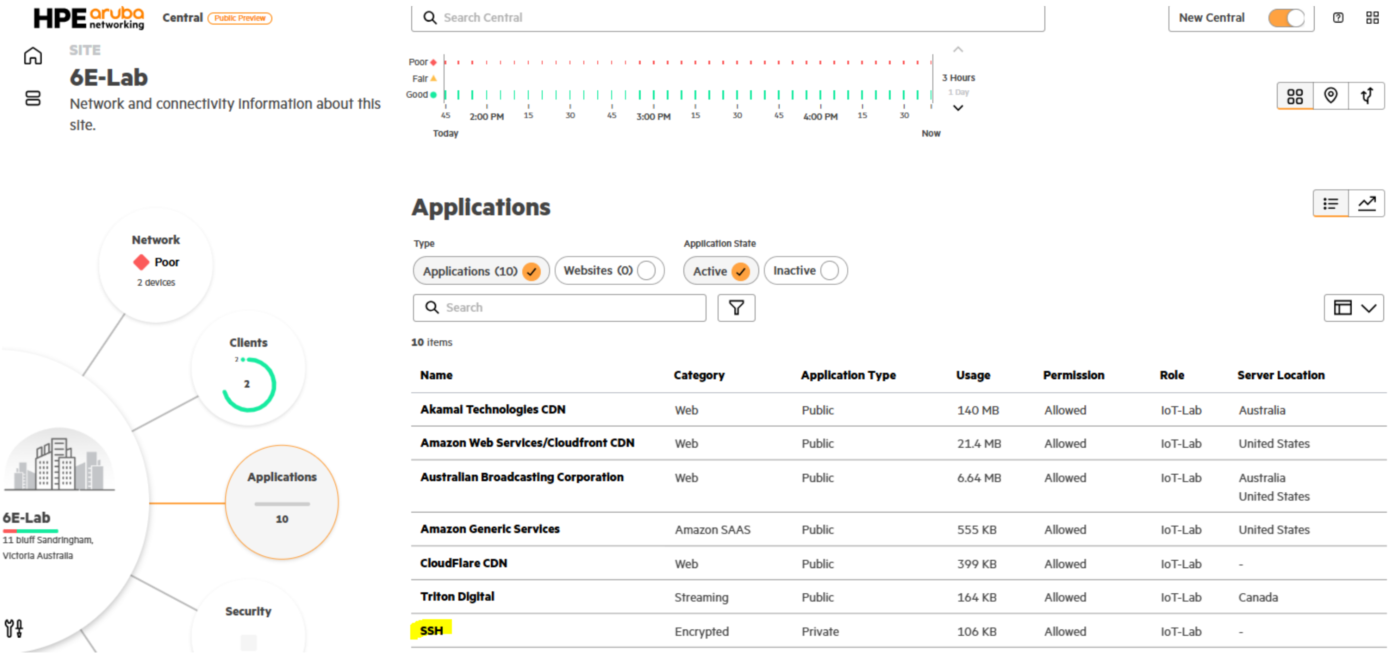


Clients

2 items

Name	Type	MAC Address	IP Address	VLAN	Role	Tag
Lab-iPad Connected -...	Wireless	a4:d1:d2:5f:32:52	10.10.11.44 fe80:0:0:0:18f8:ca9d:b765:1002	11	IoT-Lab	-
RPI3 Connected -...	Wireless	00:24:01:11:54:79	10.10.11.39	11	IoT-Lab	-

Next, I have started a SSH session from the RPi3 to 192.168.1.249 and I’ll wait for the SSH to show up under application list, this could take 5-10 minutes.

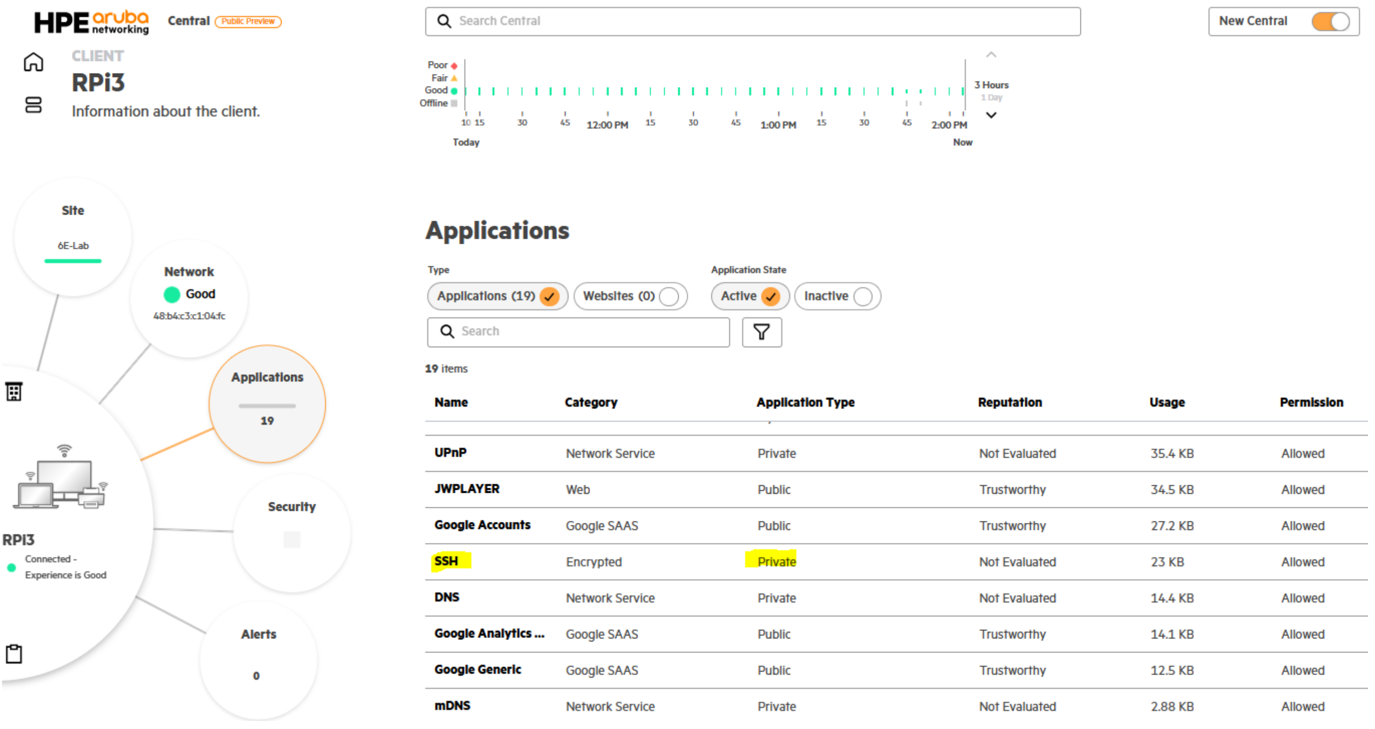


Applications

10 items

Name	Category	Application Type	Usage	Permission	Role	Server Location
Akamai Technologies CDN	Web	Public	140 MB	Allowed	IoT-Lab	Australia
Amazon Web Services/Cloudfront CDN	Web	Public	21.4 MB	Allowed	IoT-Lab	United States
Australian Broadcasting Corporation	Web	Public	6.64 MB	Allowed	IoT-Lab	Australia United States
Amazon Generic Services	Amazon SAAS	Public	555 KB	Allowed	IoT-Lab	United States
CloudFlare CDN	Web	Public	399 KB	Allowed	IoT-Lab	-
Triton Digital	Streaming	Public	164 KB	Allowed	IoT-Lab	Canada
SSH	Encrypted	Private	106 KB	Allowed	IoT-Lab	-

We'll check the application specific to RPi client and see the SSH application listed as well.



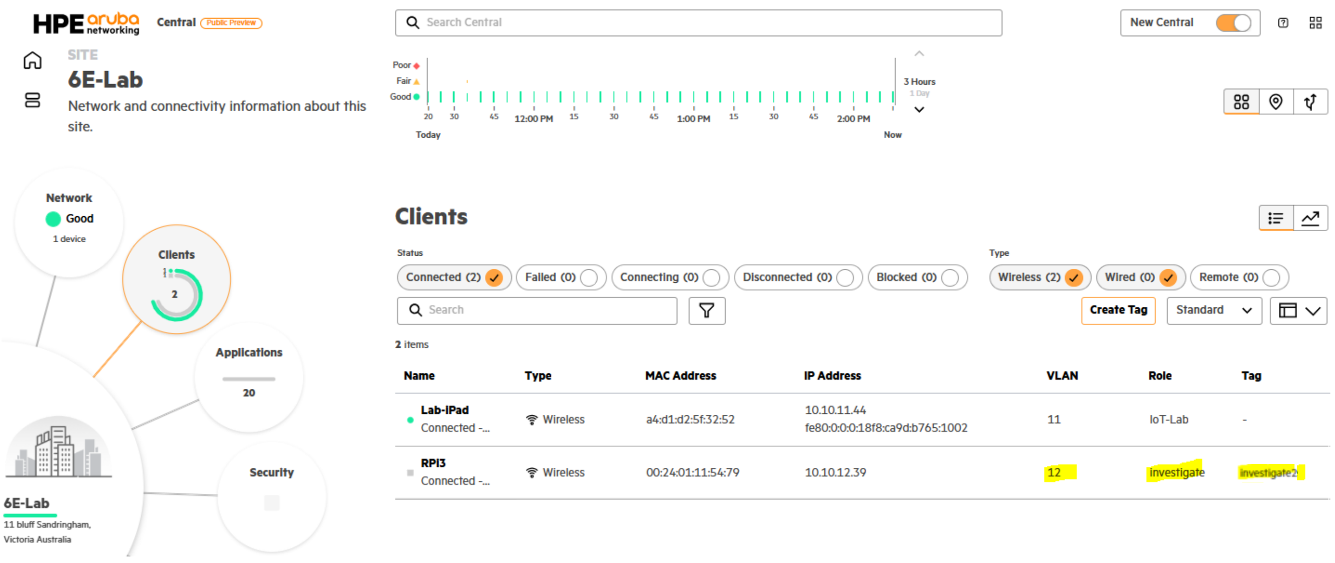
Applications

Type: Applications (19) ✓ Websites (0) ○ Application State: Active ✓ Inactive ○

19 items

Name	Category	Application Type	Reputation	Usage	Permission
UPnP	Network Service	Private	Not Evaluated	35.4 KB	Allowed
JWPLAYER	Web	Public	Trustworthy	34.5 KB	Allowed
Google Accounts	Google SAAS	Public	Trustworthy	27.2 KB	Allowed
SSH	Encrypted	Private	Not Evaluated	23 KB	Allowed
DNS	Network Service	Private	Not Evaluated	14.4 KB	Allowed
Google Analytics ...	Google SAAS	Public	Trustworthy	14.1 KB	Allowed
Google Generic	Google SAAS	Public	Trustworthy	12.5 KB	Allowed
mDNS	Network Service	Private	Not Evaluated	2.88 KB	Allowed

So now that we see the SSH application listed for the client, we expect for it to be automatically tagged with "investigate2". After a while we'll check the unified client page to see if the investigate2 tag has been applied.



Clients

Status: Connected (2) ✓ Failed (0) ○ Connecting (0) ○ Disconnected (0) ○ Blocked (0) ○

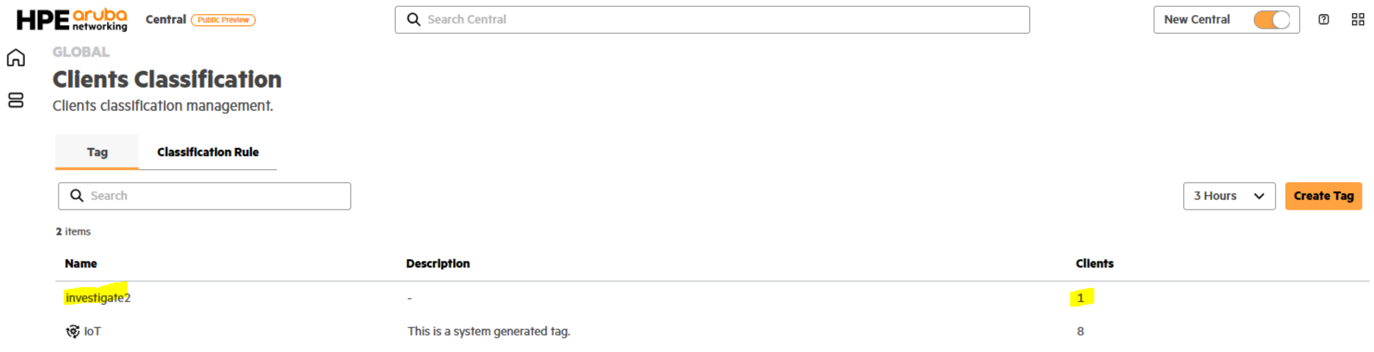
Type: Wireless (2) ✓ Wired (0) ✓ Remote (0) ○

Create Tag Standard

2 items

Name	Type	MAC Address	IP Address	VLAN	Role	Tag
Lab-iPad Connected -...	Wireless	a4:d1:d2:5f:32:52	10.10.11.44 fe80:0:0:0:18f8:ca9d:b765:1002	11	IoT-Lab	-
RPI3 Connected -...	Wireless	00:24:01:11:54:79	10.10.12.39	12	investigate	investigate2

We can also check the global client classification where we see one client is matched with "investigate2" tag.



Clients Classification

Clients classification management.

Tag | Classification Rule

3 Hours Create Tag

2 items

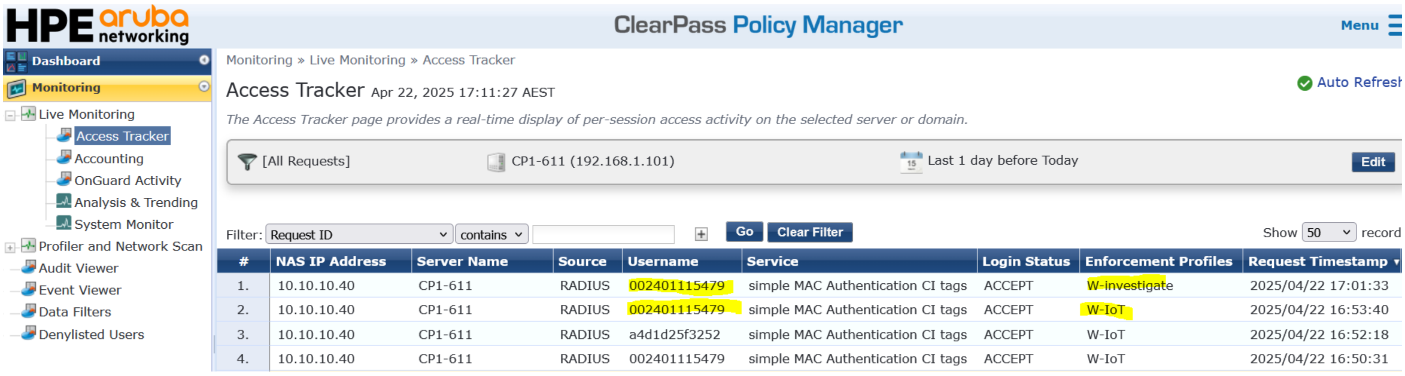
Name	Description	Clients
investigate2	-	1
IoT	This is a system generated tag.	8

5.4 ClearPass Access Monitor Check

Now let’s check the access tracker in ClearPass to see what just happened. Remember that username “002401115479” is our RPi3 client.

Here we see that RPi3 client first connected to the network, and it was matched with W-IoT enforcement profile. This is shown in session #2 below.

And then when RPi3 client was running SSH application, it got matched with “W-investigate” enforcement profile and this is shown in session #1



Access Tracker Apr 22, 2025 17:11:27 AEST

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[All Requests]   CP1-611 (192.168.1.101)   Last 1 day before Today

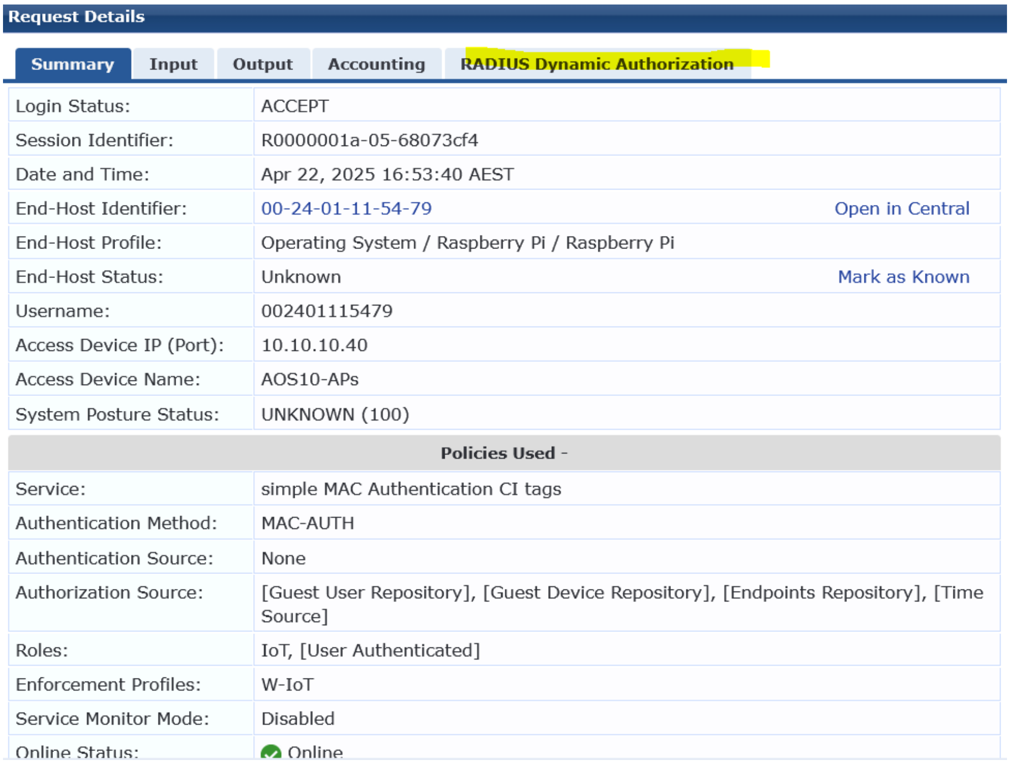
Filter: Request ID contains

Show 50 record

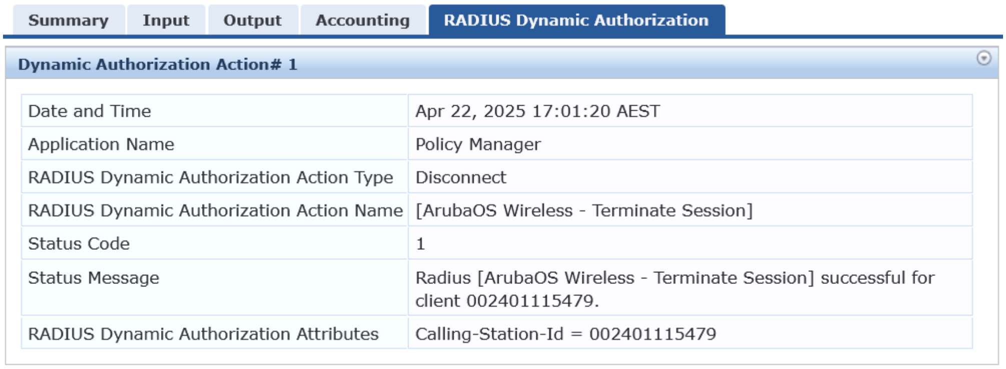
#	NAS IP Address	Server Name	Source	Username	Service	Login Status	Enforcement Profiles	Request Timestamp
1.	10.10.10.40	CP1-611	RADIUS	002401115479	simple MAC Authentication CI tags	ACCEPT	W-investigate	2025/04/22 17:01:33
2.	10.10.10.40	CP1-611	RADIUS	002401115479	simple MAC Authentication CI tags	ACCEPT	W-IoT	2025/04/22 16:53:40
3.	10.10.10.40	CP1-611	RADIUS	a4d1d25f3252	simple MAC Authentication CI tags	ACCEPT	W-IoT	2025/04/22 16:52:18
4.	10.10.10.40	CP1-611	RADIUS	002401115479	simple MAC Authentication CI tags	ACCEPT	W-IoT	2025/04/22 16:50:31

Let’s take a close look. As seen above we see that in the session #2 the first authentication requests comes in and the enforcement profile of W-IoT is sent. And soon after when the SSH application was executed on that client, the second authentication request comes in and this time the W-investigate enforcement profile was used.

We’ll first open session #2 and here we see that indeed a CoA was sent. We see this by looking at “RADIUS Dynamic Authorization” tab.



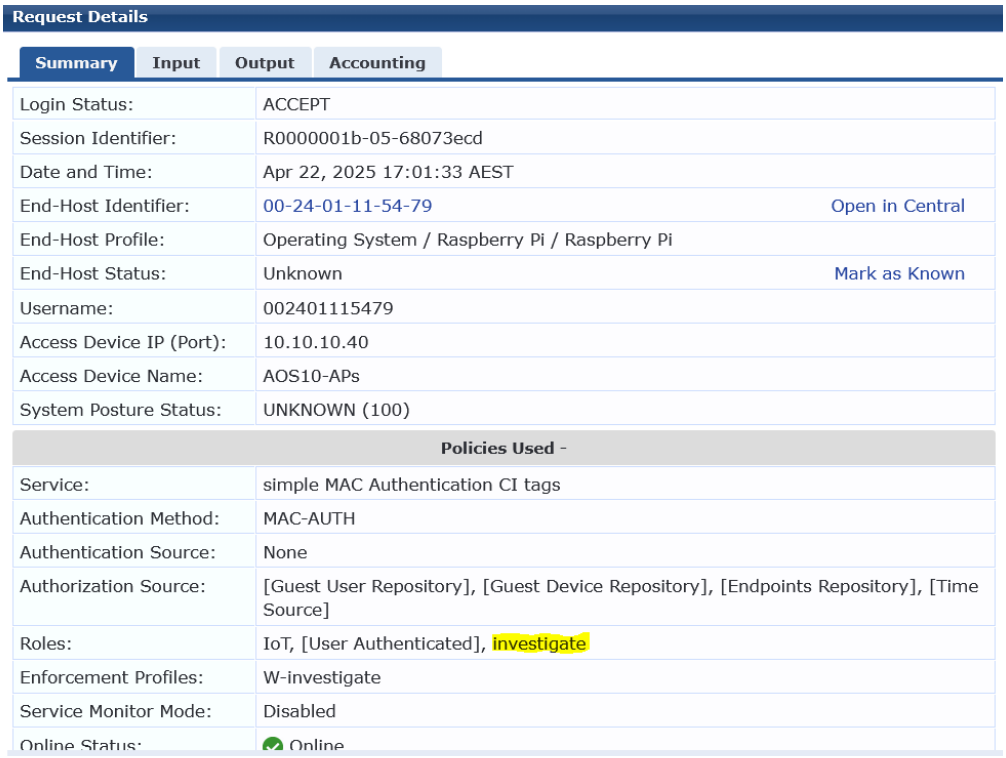
Login Status:	ACCEPT
Session Identifier:	R0000001a-05-68073cf4
Date and Time:	Apr 22, 2025 16:53:40 AEST
End-Host Identifier:	00-24-01-11-54-79
End-Host Profile:	Operating System / Raspberry Pi / Raspberry Pi
End-Host Status:	Unknown
Username:	002401115479
Access Device IP (Port):	10.10.10.40
Access Device Name:	AOS10-APs
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	simple MAC Authentication CI tags
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Time Source]
Roles:	IoT, [User Authenticated]
Enforcement Profiles:	W-IoT
Service Monitor Mode:	Disabled
Online Status:	Online



Dynamic Authorization Action# 1

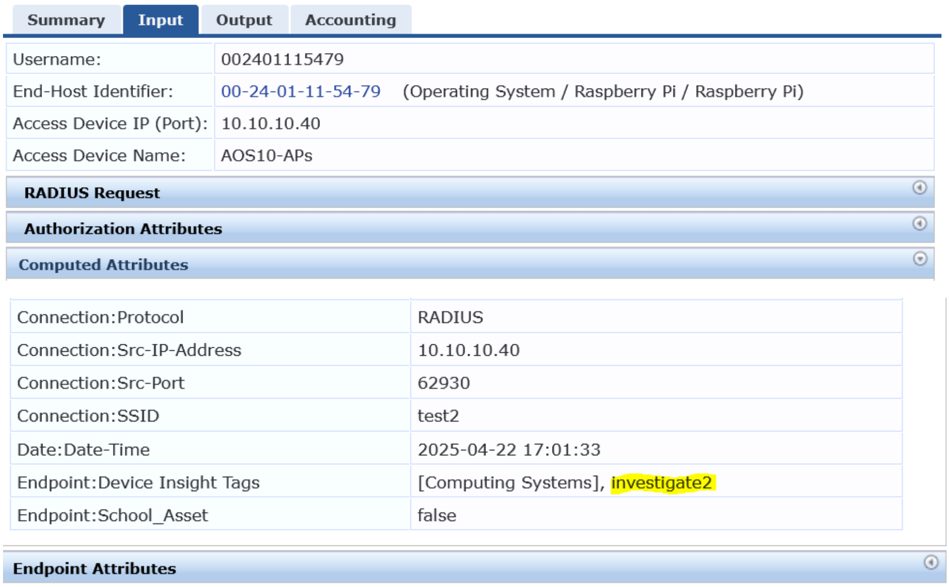
Date and Time	Apr 22, 2025 17:01:20 AEST
Application Name	Policy Manager
RADIUS Dynamic Authorization Action Type	Disconnect
RADIUS Dynamic Authorization Action Name	[ArubaOS Wireless - Terminate Session]
Status Code	1
Status Message	Radius [ArubaOS Wireless - Terminate Session] successful for client 002401115479.
RADIUS Dynamic Authorization Attributes	Calling-Station-Id = 002401115479

This was the result of the change we made in the “Device Tag Updates Action” to send a CoA. Now when we look at the session #1, we see the role is now “investigate”



Login Status:	ACCEPT
Session Identifier:	R0000001b-05-68073ecd
Date and Time:	Apr 22, 2025 17:01:33 AEST
End-Host Identifier:	00-24-01-11-54-79 Open in Central
End-Host Profile:	Operating System / Raspberry Pi / Raspberry Pi
End-Host Status:	Unknown Mark as Known
Username:	002401115479
Access Device IP (Port):	10.10.10.40
Access Device Name:	AOS10-APs
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	simple MAC Authentication CI tags
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Time Source]
Roles:	IoT, [User Authenticated], investigate
Enforcement Profiles:	W-investigate
Service Monitor Mode:	Disabled
Online Status:	✓ Online

Checking the computed attributes we see “investigate2” tag that was sent by Aruba Central device insight.

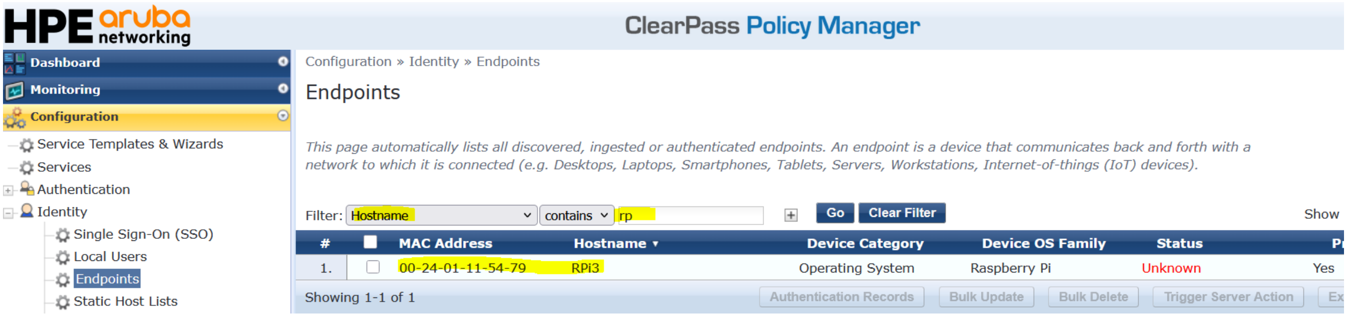


Username:	002401115479
End-Host Identifier:	00-24-01-11-54-79 (Operating System / Raspberry Pi / Raspberry Pi)
Access Device IP (Port):	10.10.10.40
Access Device Name:	AOS10-APs

Computed Attributes

Connection:Protocol	RADIUS
Connection:Src-IP-Address	10.10.10.40
Connection:Src-Port	62930
Connection:SSID	test2
Date:Date-Time	2025-04-22 17:01:33
Endpoint:Device Insight Tags	[Computing Systems], investigate2
Endpoint:School_Asset	false

Now when we also check the Endpoint database in ClearPass for this client we see the new attributes and tags.



Configuration » Identity » Endpoints

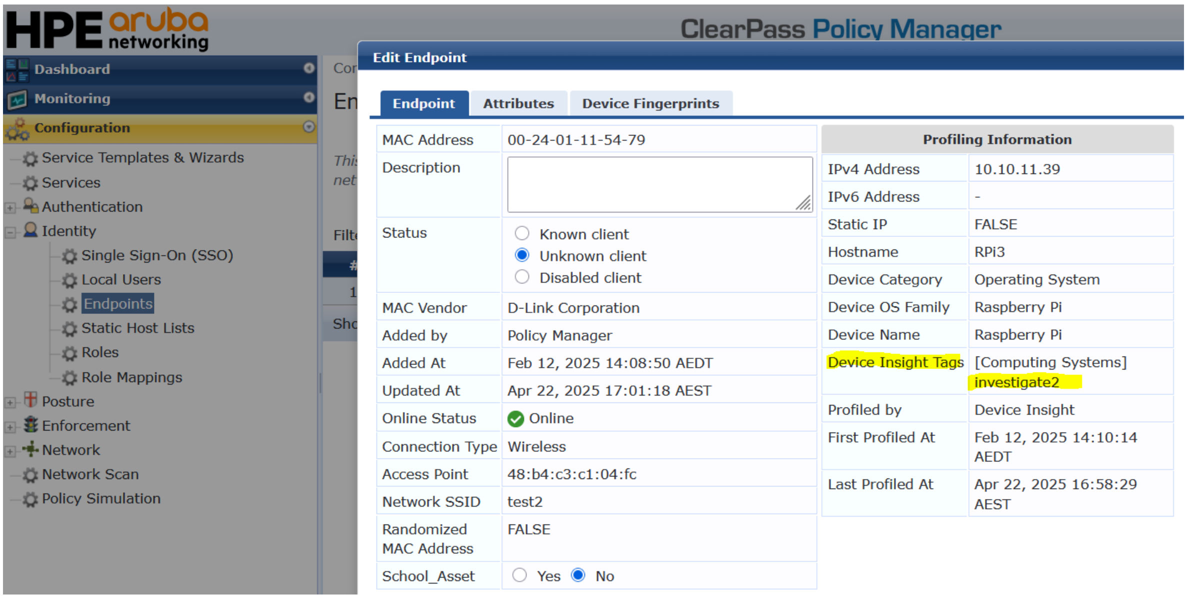
Endpoints

This page automatically lists all discovered, ingested or authenticated endpoints. An endpoint is a device that communicates back and forth with a network to which it is connected (e.g. Desktops, Laptops, Smartphones, Tablets, Servers, Workstations, Internet-of-things (IoT) devices).

Filter: Hostname contains rp

#	□	MAC Address	Hostname ▾	Device Category	Device OS Family	Status	P
1.	□	00-24-01-11-54-79	RPi3	Operating System	Raspberry Pi	Unknown	Yes

Showing 1-1 of 1

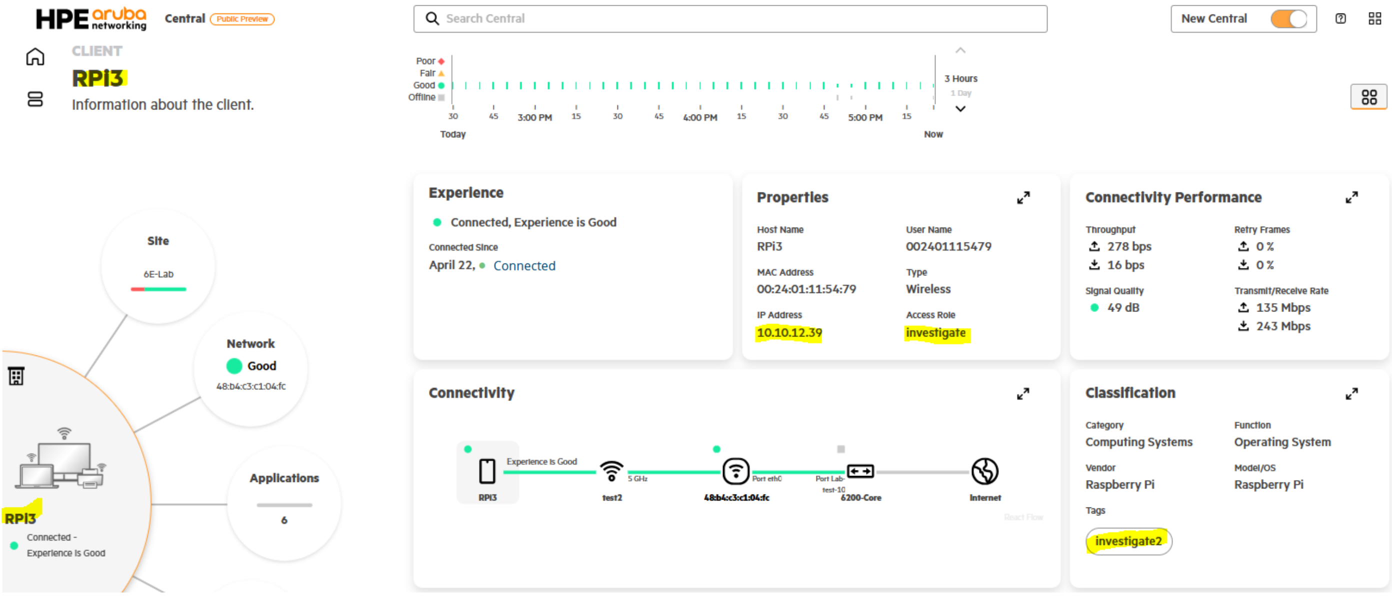


Edit Endpoint

MAC Address	00-24-01-11-54-79
Description	
Status	○ Known client ● Unknown client ○ Disabled client
MAC Vendor	D-Link Corporation
Added by	Policy Manager
Added At	Feb 12, 2025 14:08:50 AEDT
Updated At	Apr 22, 2025 17:01:18 AEST
Online Status	✓ Online
Connection Type	Wireless
Access Point	48:b4:c3:c1:04:fc
Network SSID	test2
Randomized MAC Address	FALSE
School_Asset	○ Yes ● No

Profiling Information	
IPv4 Address	10.10.11.39
IPv6 Address	-
Static IP	FALSE
Hostname	RPi3
Device Category	Operating System
Device OS Family	Raspberry Pi
Device Name	Raspberry Pi
Device Insight Tags	[Computing Systems] investigate2
Profiled by	Device Insight
First Profiled At	Feb 12, 2025 14:10:14 AEDT
Last Profiled At	Apr 22, 2025 16:58:29 AEST

Remember with New Central, the application attributes are not sent to ClearPass. Going back to the client view in Aruba Central we'll see the correct user role and VLAN assignment.



CLIENT

RPi3

Information about the client.

Experience

Connected, Experience is Good

Connected Since
April 22, Connected

Properties

Host Name RPi3	User Name 002401115479
MAC Address 00:24:01:11:54:79	Type Wireless
IP Address 10.10.12.39	Access Role investigate

Connectivity Performance

Throughput 278 bps 16 bps	Retry Frames 0 % 0 %
Signal Quality 49 dB	Transmit/Receive Rate 135 Mbps 243 Mbps

Connectivity

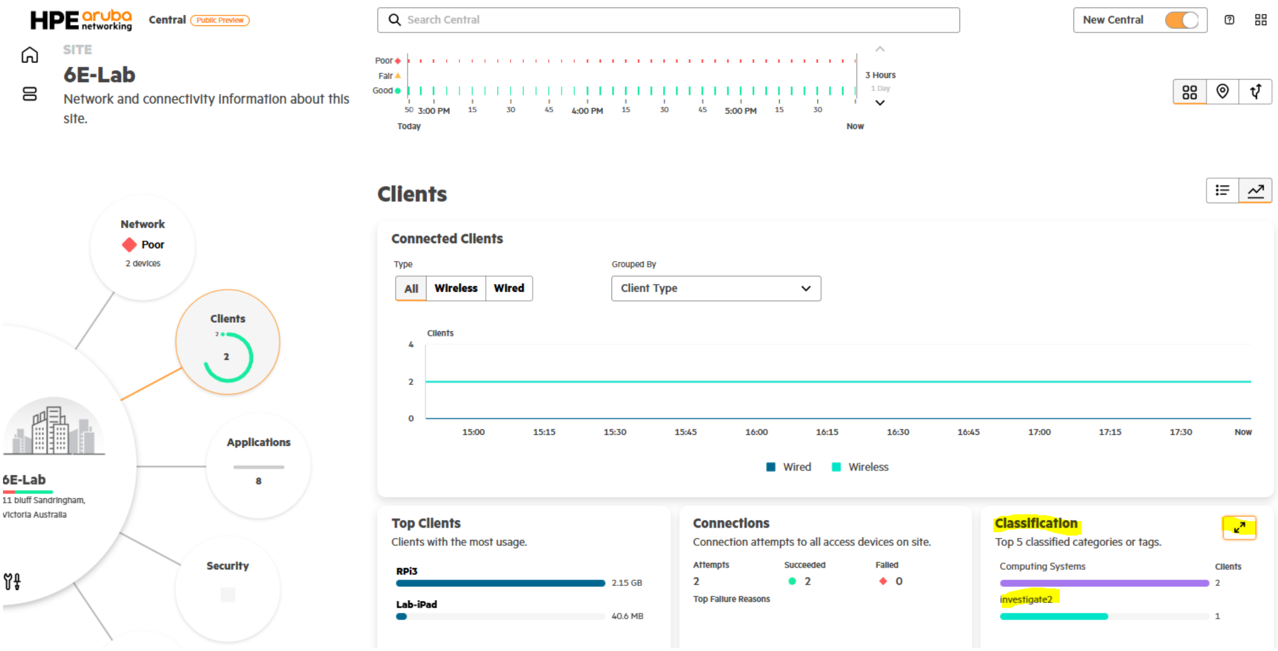
Classification

Category Computing Systems	Function Operating System
Vendor Raspberry Pi	Model/OS Raspberry Pi
Tags investigate2	

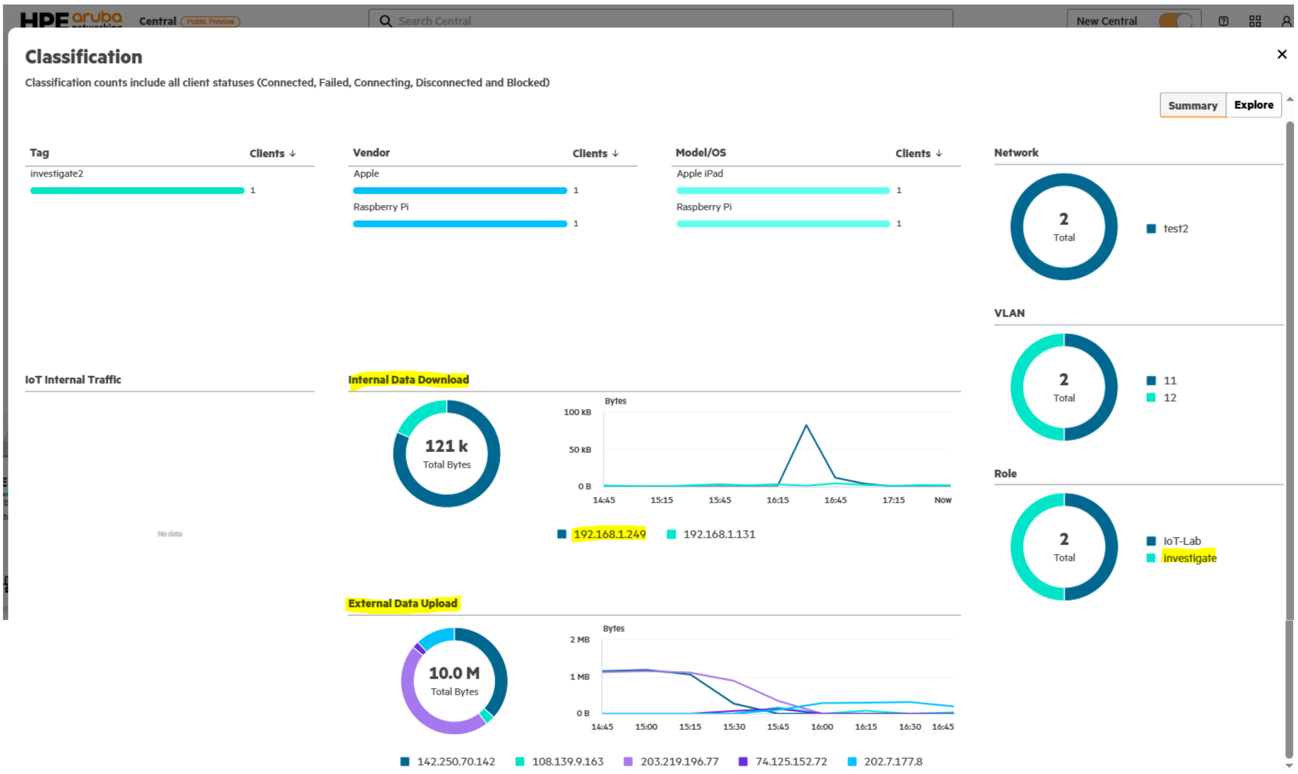
Note that application attributes-based tag are not permanent, and they get re-evaluated the next time client connects.

5.5 New Central Site Level View

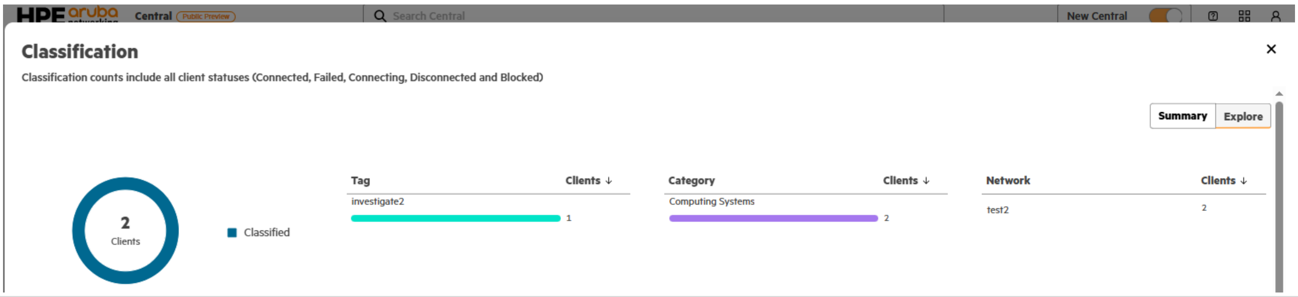
In this section we'll explore the site level view for clients and classifications.

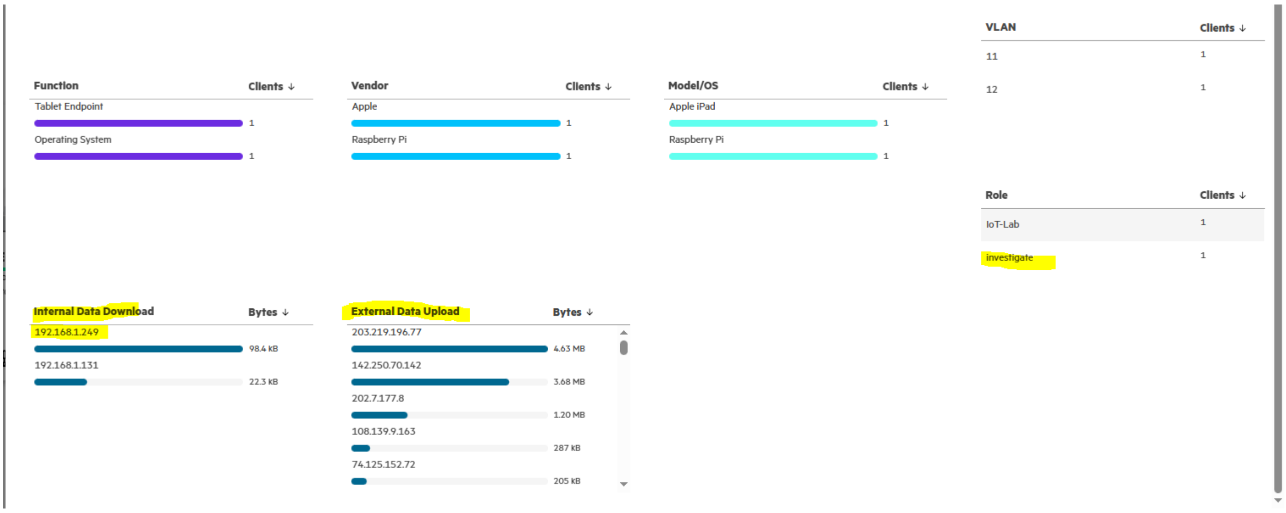


Expanding the classification card at the site levels provides us with Internal/External Data download/upload. Note that SSH session was to an internal IP address 192.168.1.249 which is shown below.



We can now click on the “Explore” tab to get the top talkers and other interesting analytics for this site.





Function	Clients ↓
Tablet Endpoint	1
Operating System	1

Vendor	Clients ↓
Apple	1
Raspberry Pi	1

Model/OS	Clients ↓
Apple iPad	1
Raspberry Pi	1

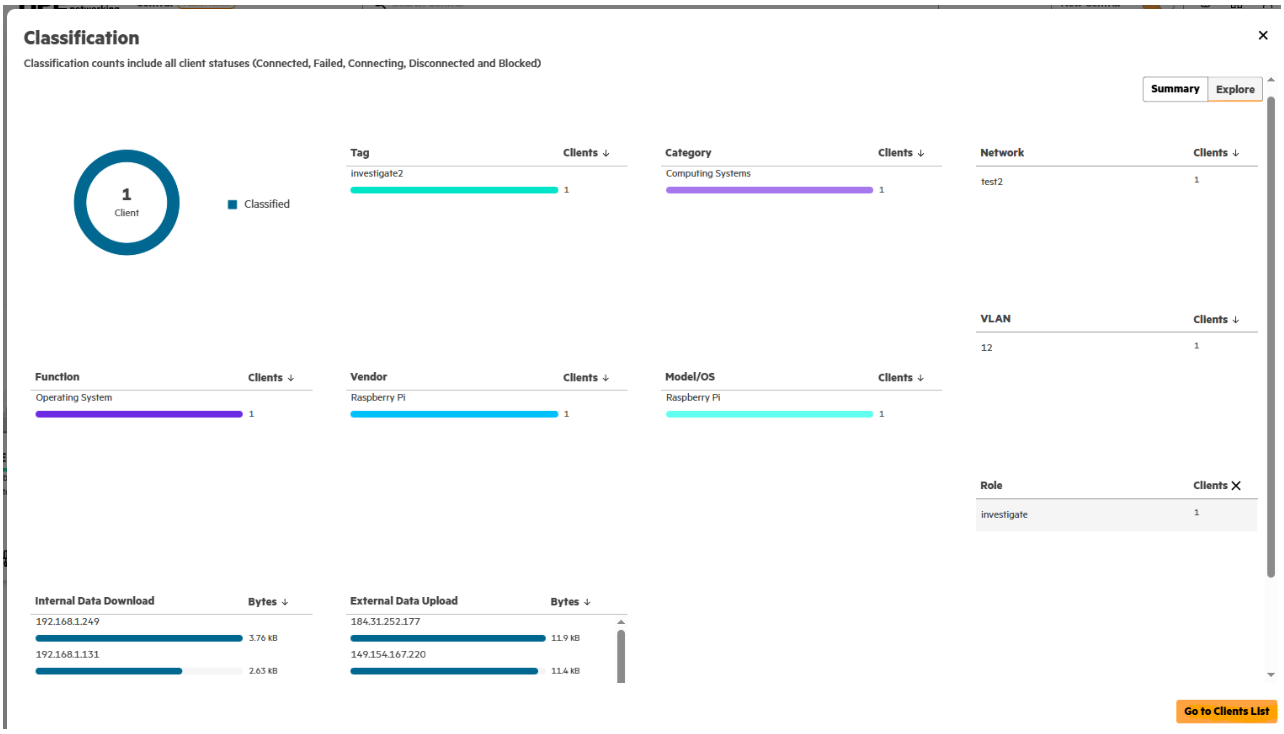
VLAN	Clients ↓
11	1
12	1

Role	Clients ↓
IoT-Lab	1
investigate	1

Internal Data Download	Bytes ↓
192.168.1.249	98.4 kB
192.168.1.131	22.3 kB

External Data Upload	Bytes ↓
203.219.196.77	4.63 MB
142.250.70.142	3.68 MB
202.7.177.8	1.20 MB
108.139.9.163	287 kB
74.125.152.72	205 kB

You can click on "investigate" role to get just the perspective from that user role.



Classification

Classification counts include all client statuses (Connected, Failed, Connecting, Disconnected and Blocked)

Tag	Clients ↓
investigate2	1

Category	Clients ↓
Computing Systems	1

Network	Clients ↓
test2	1

VLAN	Clients ↓
12	1

Function	Clients ↓
Operating System	1

Vendor	Clients ↓
Raspberry Pi	1

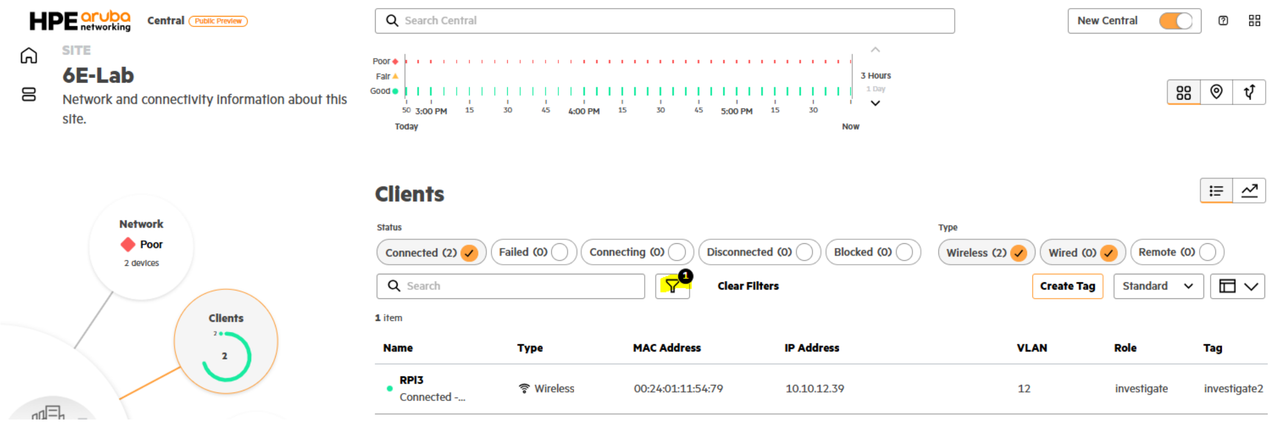
Model/OS	Clients ↓
Raspberry Pi	1

Role	Clients ✕
investigate	1

Internal Data Download	Bytes ↓
192.168.1.249	3.76 kB
192.168.1.131	2.63 kB

External Data Upload	Bytes ↓
184.31.252.177	11.9 kB
149.154.167.220	11.4 kB

And then click on the "Go to Clients List" to see which clients are assigned the "investigate" user role. Note this useful feature automatically adds a filter for it in unified client list to show only those clients with that user role.



Clients

Status: Connected (2) ✓ | Failed (0) ○ | Connecting (0) ○ | Disconnected (0) ○ | Blocked (0) ○

Type: Wireless (2) ✓ | Wired (0) ✓ | Remote (0) ○

1 item

Name	Type	MAC Address	IP Address	VLAN	Role	Tag
RPI3 Connected -...	Wireless	00:24:01:11:54:79	10.10.12.39	12	investigate	investigate2