

1 Table of Contents

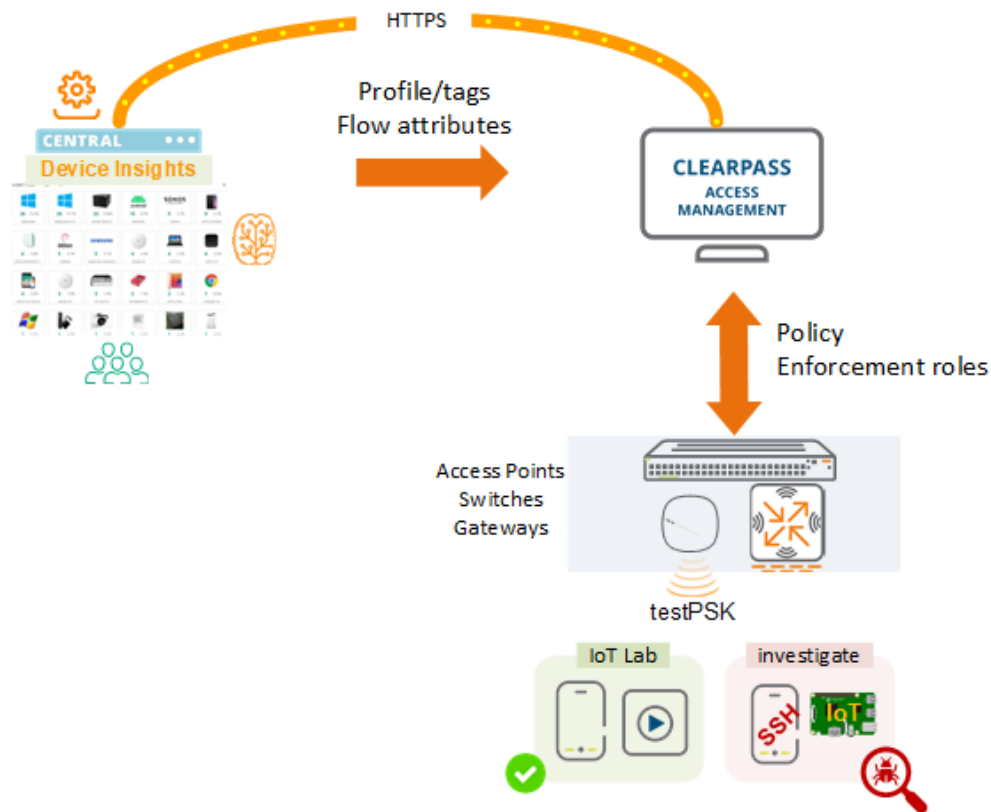
- 1 Table of Contents 1
 - 1.1 Revision History 1
- 2 Aruba Classic Central Device Insights and ClearPass..... 2
 - 2.1 Things you need 2
 - 2.2 Assumptions 2
- 3 Aruba Classic Central Integration with ClearPass..... 3
 - 3.1 Aruba Central Configuration 3
 - 3.2 ClearPass Configuration..... 3
 - 3.3 Integration Status..... 5
- 4 Using Device Insight Tag 8
 - 4.1 AOS10 Configuration 8
 - 4.2 ClearPass Service 9
- 5 Device Attribute Testing..... 11
 - 5.1 Initial Device Attribute Testing..... 11
 - 5.2 Creating Device Tags 14
 - 5.3 Device Insight Tag Testing..... 17

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
11 Jan 2025	0.1	Ariya Parsamanesh	Initial creation
28 Jan 2025	0.2	Ariya Parsamanesh	Client Testing

2 Aruba Classic Central Device Insights and ClearPass

This short technote covers integrating Aruba Classic Central with ClearPass Policy that enables Aruba Central to send the device profiling information and tags 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 and send them to Aruba Central for analysis.



The main benefits are

- Providing much richer device profiling information and visibility
- Creating device tags based on flow attribute to be used in ClearPass enforcement policies

In this scenario IoT devices connect to a tunnelled PSK SSID, get classified and put into IoT Lab user role. However, one of IoT devices starts a SSH session to an internal server. DI identifies this flow and automatically notifies ClearPass that then puts the device in a “investigate” restricted user role.

With this integration, ClearPass uses DI instead of its profiler for all device discovery and classification. Bidirectional metadata is automatically sent 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-605H) running Aruba AOS10 10.7.x.x or later
- ClearPass Policy Manager 6.11.x

2.2 Assumptions

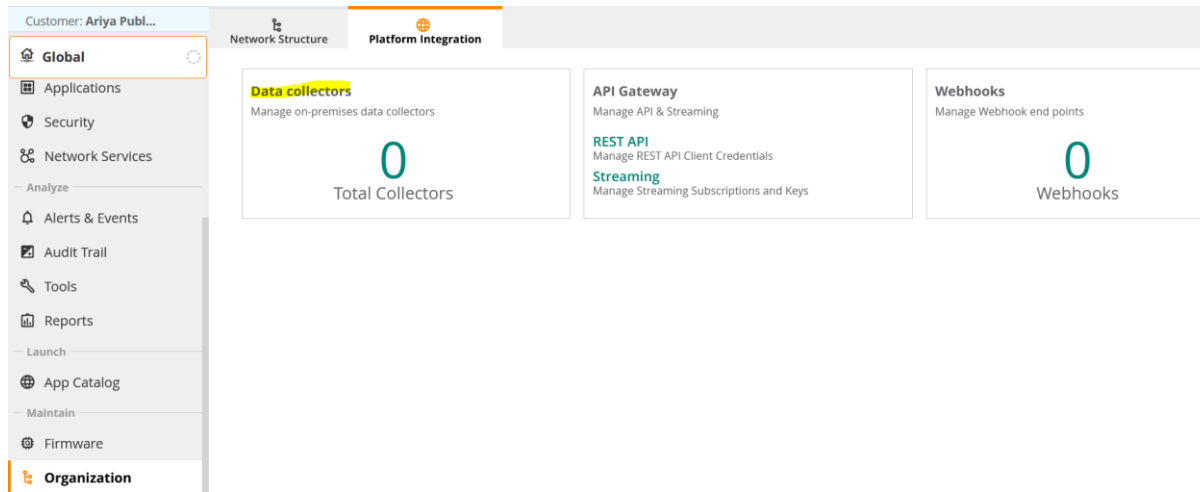
- Aruba AP and the gateway are visible and online in Aruba Central and have a valid subscription.

3 Aruba Classic Central Integration with ClearPass

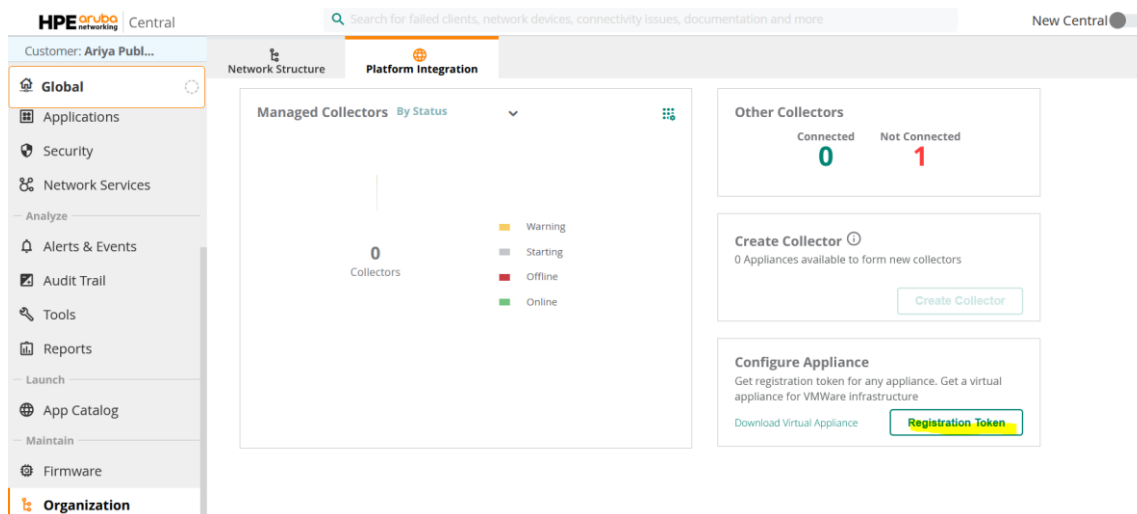
Here we'll cover the configurations steps that are needed for this integration.

3.1 Aruba Central Configuration

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



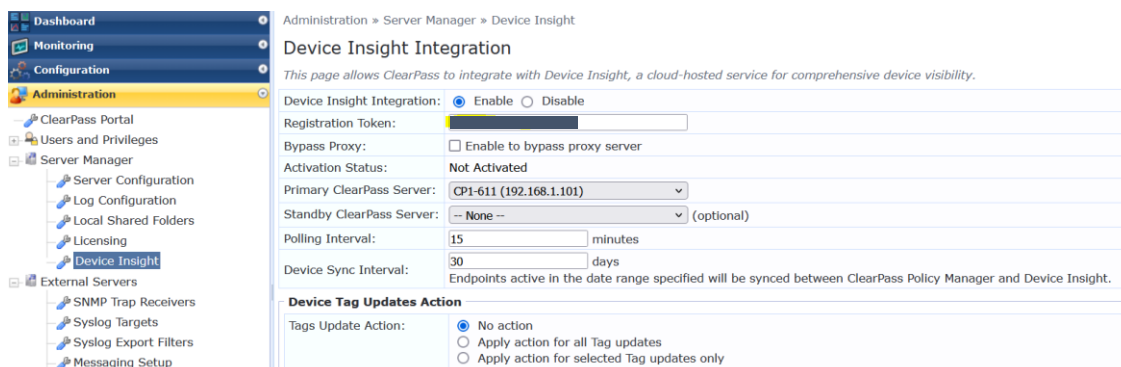
The integration between ClearPass and Aruba Central need registration token. This is where we generate a token to be used when configuring ClearPass.

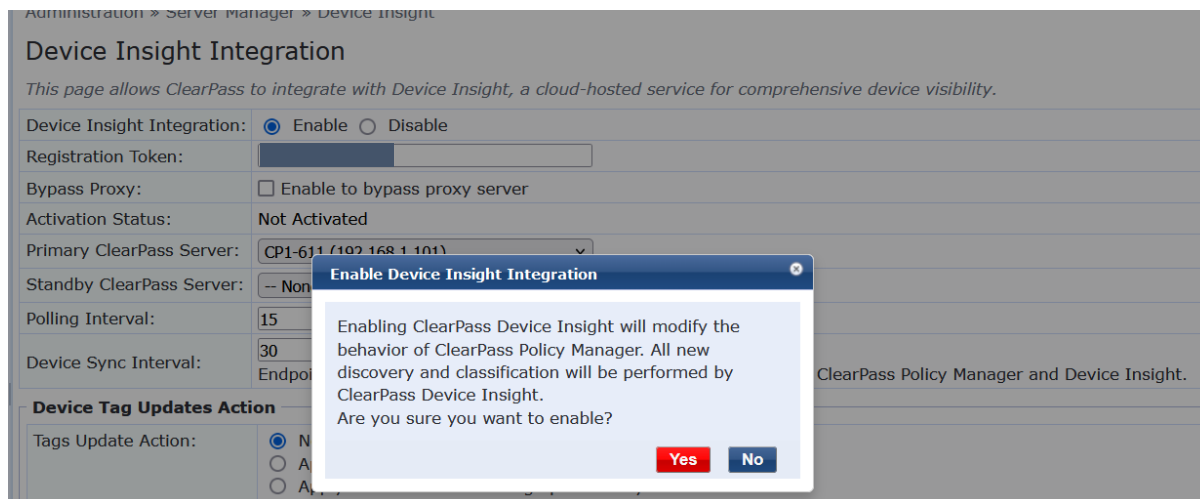


Click on the “Registration Token” and copy it. The registration token will last for 2 days. Then go to ClearPass.

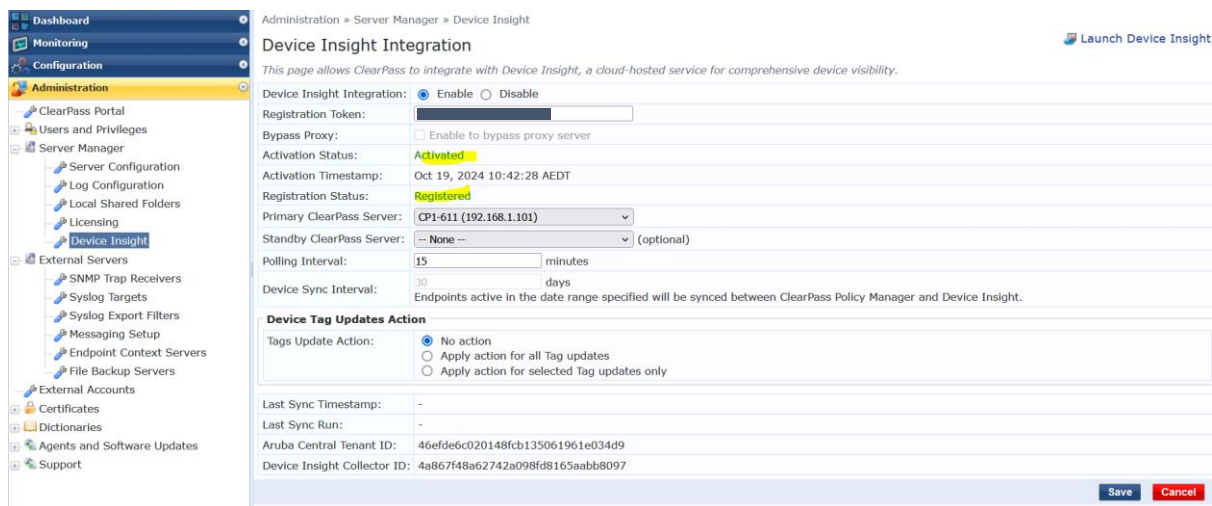
3.2 ClearPass Configuration

On the ClearPass side we need to configure it in two places. First, we need to enable “Device Insight” integration. This is where we use our Aruba Central token that we copied earlier.

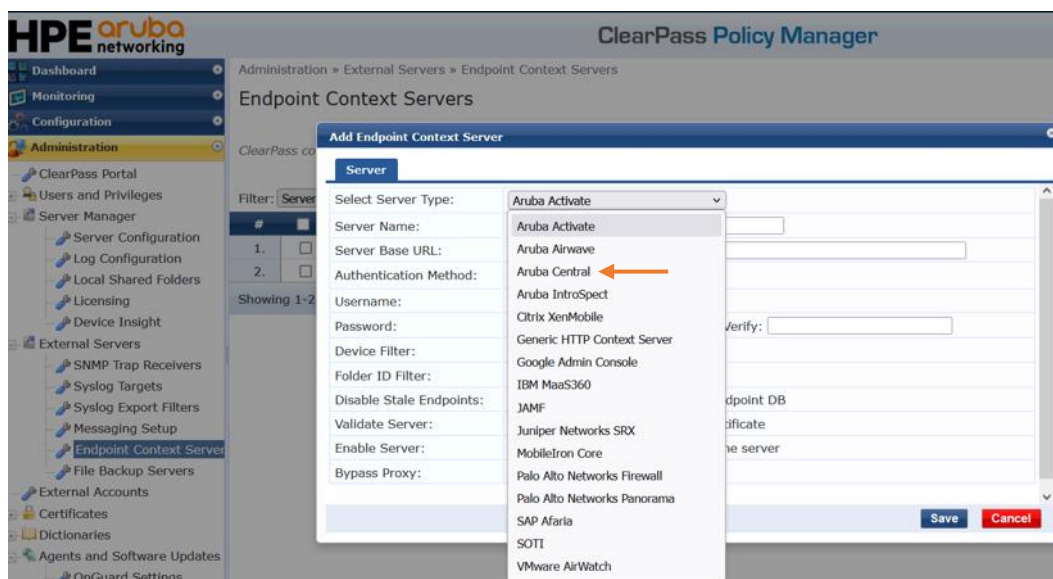




Note that the profiling behaviour will change as stated above.



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.



Here we'll choose Aruba Central from the list.

Administration » External Servers » Endpoint Context Servers

Endpoint Context Servers

Modify Endpoint Context Server

Server

Certificates

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

Update

Cancel

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

Server

Certificates

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

Update

Cancel

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

[Add](#)

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

Filter: contains Show records

#	<input type="checkbox"/>	Subject	Usage	Validity	Enabled
1.	<input type="checkbox"/>	CN=AAA Certificate Services,O=Comodo CA Limited,L=Salford,ST=Greater Manchester,C=GB	Others	Valid	Enabled
2.	<input type="checkbox"/>	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.	<input type="checkbox"/>	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.

Customer: Ariya Publ...

Network Structure Platform Integration

Global

Applications

Security

Network Services

Analyze

Alerts & Events

Audit Trail

Tools

Reports

Launch

App Catalog

Maintain

Firmware

Organization

Data Collectors

Managed Collectors By Status

0 Collectors

Warning

Starting

Offline

Online

Other Collectors

Connected 1

Not Connected 1

Create Collector ⓘ

0 Appliances available to form new collectors

Create Collector

Configure Appliance

Get registration token for any appliance. Get a virtual appliance for VMWare infrastructure

Download Virtual Appliance

Registration Token

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

Customer: Ariya Publ...

Network Structure Platform Integration

Global

Applications

Security

Network Services

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

HPE aruba networking

ClearPass Policy Manager

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

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

Last Sync Timestamp: Jan 09, 2025 15:58:23 AEDT

Last Sync Run: Jan 09, 2025 16:33:36 AEDT

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.

Configuration » Identity » Endpoints

Endpoints

Add

Import

Export

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 Go Clear Filter

Show 50 records

#	MAC Address	Hostname	Device Category	Device OS Family	Status	Profiled
1.	CE-55-81-30-F8-3C		Computer	Windows	Unknown	Yes
2.	06-25-4A-F2-85-2A		SmartDevice	Android	Unknown	Yes

Edit Endpoint

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

Endpoint	Attributes	Device Fingerprints
MAC Address	CE-55-81-30-F8-3C	Profiling Information IPv4 Address: 10.10.22.20 IPv6 Address: - Static IP: FALSE Hostname: - Device Category: Computer Device OS Family: Windows Device Name: Windows 8/10/11 Device Insight Tags: Iot [Computers & Servers] Profiled by: Device Insight First Profiled At: Oct 14, 2024 13:00:48 AEDT Last Profiled At: Oct 14, 2024 16:39:53 AEDT
Description		
Status	<input type="radio"/> Known client <input checked="" type="radio"/> Unknown client <input type="radio"/> Disabled client	
MAC Vendor		
Added by	Device Insight	
Added At	Oct 19, 2024 10:44:07 AEDT	
Updated At	Oct 19, 2024 10:44:08 AEDT	
Online Status	Not Available	
Connection Type	Unknown	
Randomized MAC Address	TRUE	
School_Asset	<input type="radio"/> Yes <input checked="" type="radio"/> No	

Here is access tracker for an authentication session and we simply can 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.

HPE aruba networking **ClearPass Policy Manager**

Request Details

Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R00000000-05-6794469a		
Date and Time:	Jan 25, 2025 13:04:10 AEDT		
End-Host Identifier:	2C-1F-23-D0-2F-48		Open in Central
End-Host Profile:	SmartDevice / Apple / Apple iPod		
End-Host Status:	Unknown		Mark as Known
Username:	2c1f23d02f48		
Access Device IP (Port):	192.168.1.243		
Access Device Name:	AOS10-gateway1 (AOS10-gateway1 / Aruba)		
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], [Endpoints Repository], [Time Source]		
Roles:	IoT, [User Authenticated]		
Enforcement Profiles:	W-IoT		
Service Monitor Mode:	Disabled		
Online Status:	Not Available		

Make sure you first login to Aruba Central and then click on the “open in Central” link and you’ll see the client data path in another browser tab.

Customer: Ariya Publ...

2c1f23d02f48

Overview

Applications

Security

Analyze

Live Events

Events

Tools

CLIENT DETAILS

DATA PATH

CLIENT: 2c1f23d02f48 CONNECTED

SSID: testPSK UP

AP: AP-605H-5d5b UP

GATEWAY: 7005_AOS10_gw1 UP

CLIENT

USERNAME: 2c1f23d02f48

HOSTNAME: 2c1f23d02f48

IP ADDRESS: 10.10.31.31

CLIENT CATEGORY: SmartDevice

CLIENT OS: Apple iPod

CLIENT TYPE: Wireless

MAC ADDRESS: 2c1f23d02f48

CLIENT FAMILY: Apple

CONNECTED SINCE: Jan 25, 2025, 13:04:16

NETWORK

VLAN: 31

AP ROLE: IoT-Lab

GATEWAY ROLE: IoT-Lab

SEGMENTATION: OVERLAY

AUTH SERVER: -

VLAN DERIVATION: -

AP DERIVATION: -

SWITCH ROLE: -

DHCP SERVER: -

CONNECTION

CHANNEL: 36 (40 MHz)

BAND: 5 GHz

CLIENT CAPABILITIES: 802.11an, 802.11r

CLIENT MAX SPEED: -

LEDs on ACCESS POINT (AP-605H-5d5b): Blink LEDs

4 Using Device Insight Tag

The lab setup uses a client that connects to AP-605H broadcasting “testPSK” that is tunnelled to a AOS10 gateway.

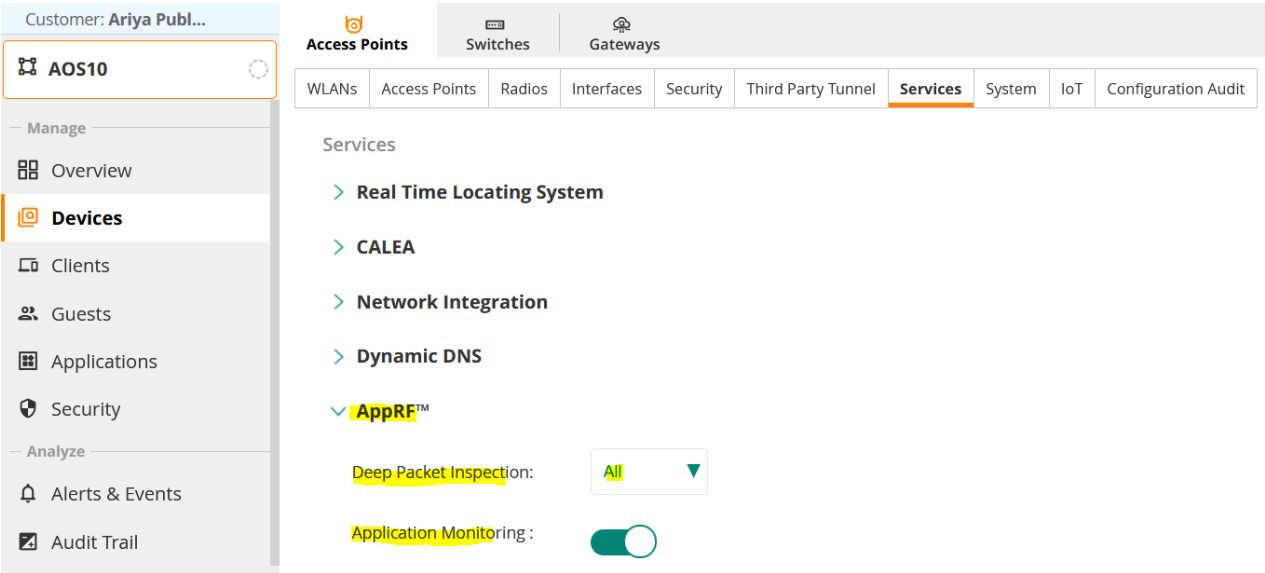
4.1 AOS10 Configuration

This is configuration for a simple PSK WLAN that is tunnelled to a cluster of AOS10 gateways. This WLAN is uses ClearPass for MAC authentication, in which like always ClearPass send a Local user role to the AP/gateway.

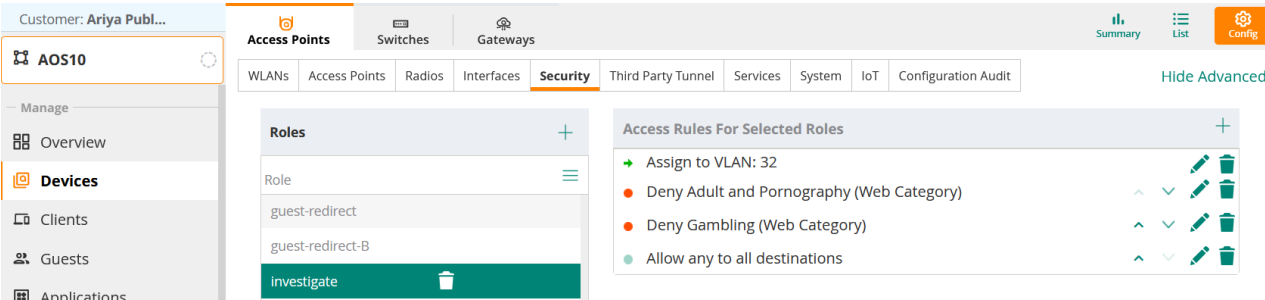
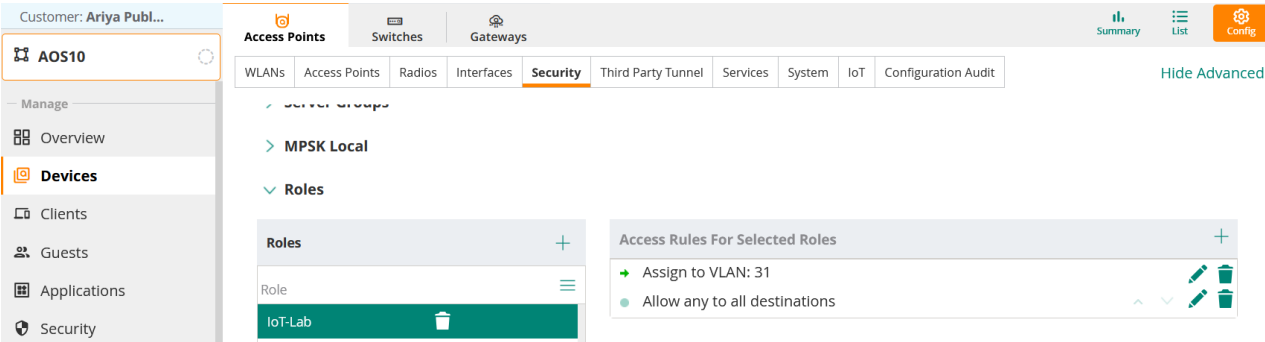
The screenshot displays the AOS10 configuration interface for a WLAN named 'testPSK'. The interface is divided into several sections:

- General Tab:** Shows the ESSID as 'testPSK' and the Band as 2.4 GHz (selected) and 5 GHz (selected). The 6 GHz band is unselected.
- VLANs Tab:** Shows the Traffic forwarding mode as 'Tunnel'. The Primary Gateway Cluster is 'AOS10:auto_gwcluster_178_0'. The Secondary Gateway Cluster is 'None'. The Client VLAN Assignment is 'Static'. The VLAN ID is '1(1)'.
- Security Tab:** Shows the Security Level as 'Enterprise'. The Key Management is 'WPA2-Personal'. The Passphrase Format is '8-63 chars'. The Passphrase is masked with dots. The Advanced Settings section includes: DPP (disabled), MAC Authentication (enabled), Reauth Interval (30 min), Denylisting (enabled), Enforce DHCP (disabled), Use IP for Calling Station ID (disabled), Called Station ID Type (MAC Address), Called Station ID Include SSID (disabled), and Primary Server (ClearPass-GW).
- Access Tab:** Shows the Access rules as 'Unrestricted'. A warning message states: 'Unrestricted option allows full access to the network. This may lead to potential security issues.'

Next, make sure you have enabled AppRF so that the APs can do deep packet inspection.



And finally add two user roles IoT-Lab and “investigate”



4.2 ClearPass Service

Now we need a ClearPass authentication service for this WLAN that we have called “simple MAC Authentication CI tags”.

Summary	Service	Authentication	Authorization	Roles	Enforcement	Profiler
Name:	<div>simple MAC Authentication CI tags</div>					
Description:	<div>MAC Authentication for client-insight tags</div>					
Type:	MAC Authentication					
Status:	Enabled					
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement					
More Options:	<input checked="" type="checkbox"/> Authorization <input type="checkbox"/> Audit End-hosts <input checked="" type="checkbox"/> Profile Endpoints <input type="checkbox"/> Accounting Proxy					
Service Rule						
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:						
Type	Name	Operator	Value			
1.	Connection	Client-Mac-Address	EQUALS	% {Radius:IETF:User-Name}		
2.	Connection	SSID	EQUALS	testPSK		

Summary Service **Authentication** Authorization Roles Enforcement Profiler

Authentication Methods: [Allow All MAC AUTH] [Add New Authentication Method](#)

Move Up ↑
Move Down ↓
Remove
View Details
Modify

--Select to Add--

Authentication Sources: [Endpoints Repository] [Local SQL DB] [Add New Authentication Source](#)

Move Up ↑
Move Down ↓
Remove
View Details
Modify

--Select to Add--

Strip Username Rules: ☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

Summary Service **Authentication** **Authorization** Roles Enforcement Profiler

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]

Remove
View Details
Modify

--Select to Add-- [Add New Authentication Source](#)

In our use case, if we see a device insight tag that contains “investigate”, we’ll assign it the “investigate” role.

Summary Service **Authentication** **Authorization** **Roles** Enforcement Profiler

Role Mapping Policy: CI MAC Authentication Role Mapping [Modify](#) [Add New Role Mapping Policy](#)

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 CONTAINS [Mobile & Gadgets])	IoT
4. (Authorization:[Endpoints Repository]:Category EQUALS Computer) AND (Authorization:[Endpoints Repository]:OS Family EQUALS Linux) AND (Authorization:[Endpoints Repository]:Hostname CONTAINS RPI)	IoT
5. (Authorization:[Endpoints Repository]:Category EQUALS Network Camera)	camera

Summary Service **Authentication** **Authorization** Roles **Enforcement** Profiler

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: CI tags MAC Auth Enforcement Policy [Modify](#) [Add New 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]

Summary Service **Authentication** **Authorization** Roles Enforcement **Profiler**

Endpoint Classification: Select the classification(s) after which an action must be triggered -

Any Category / OS Family / Name

Remove

-- Select --

RADIUS CoA Action: [ArubaOS Wireless - Terminate Session] [View Details](#) [Modify](#) [Add New RADIUS CoA Action](#)

The enforcement profiles for

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

5 Device Attribute Testing

5.1 Initial Device Attribute Testing

Now we get a client connect to the testPSK. It shows up in Aruba Central client list . We see that it has the correct user-role = IoT-Lab

The screenshot shows the Aruba Central interface. On the left, the 'Clients' menu is selected. The main area displays a table of clients. The client with MAC address a4d1d25f3252 is connected to testPSK and has a role of IoT-Lab.

Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role
a4d1d25f3252	Connected	10.10.31.44	31	AP-605H-5d6b	testPSK	IoT-Lab

Next, we need to click on this client to see the details.

The screenshot shows the 'Client Details' page for client a4d1d25f3252. The 'Data Path' section shows a flow from the client to the SSID (testPSK), then to the AP (AP-605H-5d6b), and finally to the Gateway (7005_AOS10_gw1).

Check if the applications are being identified as we have enabled AppRF.

The screenshot shows the 'Applications' page for client a4d1d25f3252. It displays a table of applications being used, including Amazon Web Services/Cloudfront CDN, ESPN, TCP, iTunes, Google Tag Manager, Google Ads, and Apple Location.

APPLICATION	CATEGORY	USAGE
Amazon Web Services/Cloudfront CDN	Amazon SAAS	1.8 MB
ESPN	Web	1.7 MB
TCP	Network Service	352 KB
iTunes	Streaming	252 KB
Google Tag Manager	Google SAAS	172 KB
Google Ads	Google SAAS	63 KB
Apple Location	Web	27 KB

Next, check the profiling information. The first thing to note is that the current system tag is applied.

The screenshot shows the 'Profile' page for client a4d1d25f3252. It displays classification information, including the system rule and conditions for the fingerprint attribute.

Fingerprint Attribute	Operator	Value
Host Name	Contains	ipad
MAC Vendor	Contains	apple

We are interested in seeing the “Flow Attributes” that we can use to build our role assignment.

Customer: Ariya Publ...

← a4d1d25f3252

Manage

Overview

Applications

Security

Analyze

Live Events

Events

Tools

Summary

AI Insights

Location

Sessions

Profile

Flow Attributes

Expand All | Collapse All

Application Group

business-systems.cloud-security

business-systems.encrypted-tunnel

business-systems.general-business

Show 6 more

Application ID

abc-au

akamai

amazon

Show 22 more

Destination Connection

103.43.90.19:0:tcp

13.248.150.189:0:tcp

17.253.121.202:0:tcp

Show 22 more

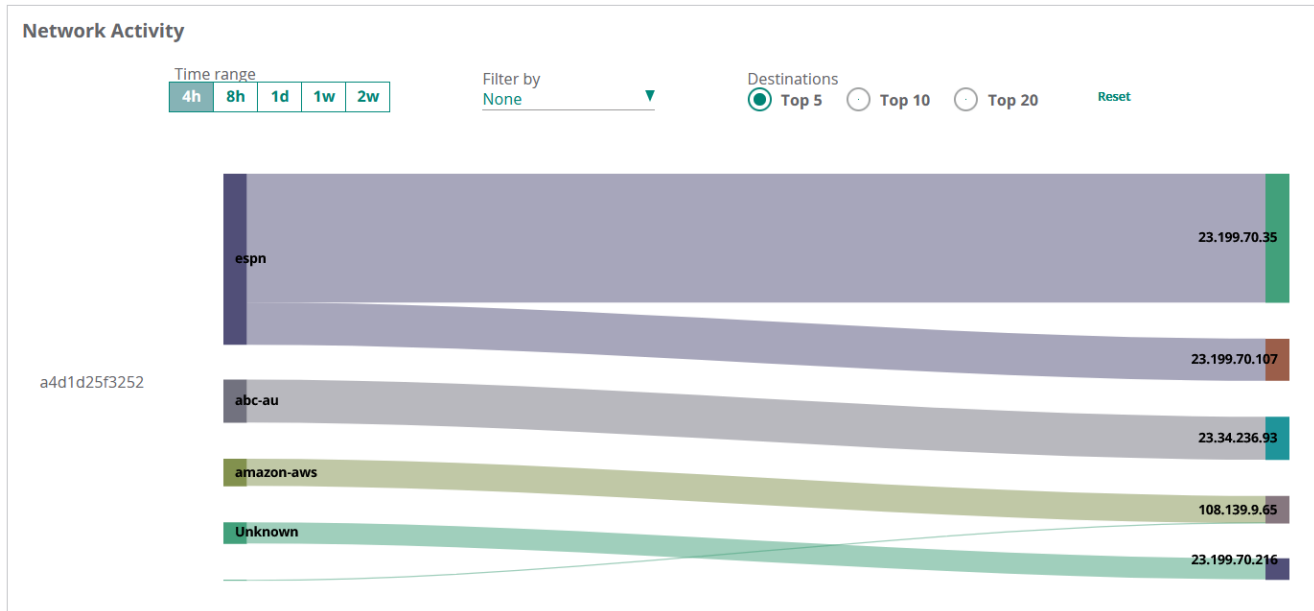
Destination Host

accuradio.com

adnxs.com

apple.com


Show 17 more



As can be seen above Aruba Central collects the following Flow Attributes

- Application Group
- Application ID
- Destination Connection
- Destination Host

Now let's look at the access tracker and see how roles were assigned to this client. Remember that our MAC auth service allows all connection and then the role-mapping policy assigns the roles based on the various attributes.

Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R00000003-05-6795bec9		
Date and Time:	Jan 26, 2025 15:49:13 AEDT		
End-Host Identifier:	A4-D1-D2-5F-32-52		Open in Central
End-Host Profile:	SmartDevice / Apple / Apple iPad		
End-Host Status:	Unknown		Mark as Known
Username:	a4d1d25f3252		
Access Device IP (Port):	192.168.1.243		
Access Device Name:	AOS10-gateway1 (AOS10-gateway1 / Aruba)		
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], [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.

Summary	Input	Output	Accounting
Username:	a4d1d25f3252		
End-Host Identifier:	A4-D1-D2-5F-32-52 (SmartDevice / Apple / Apple iPad)		
Access Device IP (Port):	192.168.1.243		
Access Device Name:	AOS10-gateway1 (AOS10-gateway1 / Aruba)		
RADIUS Request			
Authorization Attributes			
Authorization:[Endpoints Repository]:Application Group			
Authorization:[Endpoints Repository]:Application ID			
Authorization:[Endpoints Repository]:Category	SmartDevice		
Authorization:[Endpoints Repository]:Conflict	false		
Authorization:[Endpoints Repository]:Destination Connections			
Authorization:[Endpoints Repository]:Device Name	Apple iPad		
Authorization:[Endpoints Repository]:Fingerprint	{\"dhcp\":{\"option55\": [\"1,121,3,6,15,119,252\"],\"options\": [\"53,55,57,61,50,54,12\"]},\"host\": {\"mac_oui\": [\"a4d1d2\"]}}		
Authorization:[Endpoints Repository]:Hostname	ariyaps-ipad		
Authorization:[Endpoints Repository]:Open Ports			
Authorization:[Endpoints Repository]:OS Family	Apple		
Authorization:[Endpoints Repository]:Other Category			
Authorization:[Endpoints Repository]:Other Device Name			
Authorization:[Endpoints Repository]:Other OS Family			
Authorization:[Endpoints Repository]:StaticIp	false		
Authorization:[Endpoints Repository]:User Agent			

Next, we'll look at the Endpoint Attributes that includes the flow attributes we spoke about earlier.

Summary	Input	Output	Accounting
Endpoint Attributes			
MAC Vendor	Apple, Inc.		
Added by	Policy Manager		
Status	Unknown		
Device Category	SmartDevice		
Device OS Family	Apple		
Device Name	Apple iPad		
MAC Address	a4d1d25f3252		
IP Address	10.10.31.44		
Static IP	false		
Hostname	ariyaps-ipad		
Profiler Conflict	false		
Added Date	Jan 26, 2025 15:43:53 AEDT		
Updated Date	Jan 26, 2025 17:08:11 AEDT		

Fingerprint Details -

Application Group	["business-systems.cloud-security","business-systems.encrypted-tunnel","business-sy
Application ID	["unknown","abc-au","akamai","amazon","amazon-aws","apns","apple","apple-locatio
Destination Connections	["103.43.90.19:0:tcp","108.139.9.107:0:tcp","13.248.150.189:0:tcp","17.253.121.20
DHCP Option55	["1,121,3,6,15,119,252"]
DHCP Options	["53,55,57,61,51,12"]
fingerprint.host_dst_hosts	["accu.fm","accuradio.com","adnxs.com","app-measurement.com","apple.com","arubanetworks.com","chartbeat.net","cloudfront.net
Host User Agent	["1/9.3.5 (13G36)","AppleCoreMedia/1.0.0.13G36 (iPad; U; CPU OS 9_3_5 like Mac OS
MAC OUI	["a4d1d2"]

5.2 Creating Device Tags

Here we'll create a new tag to catch if the IoT devices are initiating SSH.

The screenshot displays the HPE Aruba Central interface for creating a new device tag. The top section shows the 'Clients' profile with a 'Tags' dropdown menu. The bottom section shows the 'Edit Tag' dialog box where conditions are being set for a tag named 'Investigate'.

Top Section: Clients Profile

- Customer: Ariya Publ...
- Global (selected)
- Manage
- Overview
- Devices
- Clients (selected)
- Guests

Bottom Section: Edit Tag

Select conditions to be included in the rule

Tag details

Tag name: Investigate

Description (optional): gadget is using SSH

Conditions

- Device Type: Apple iPad
- Application ID: ssh
- Destination Host: 192.168.1.131

Buttons: Cancel, Save

Customer: Ariya Publ...

Global

Manage

Overview

Devices

Clients

Guests

Applications

Clients Profile

Classified

Generic

ALL

Client Types

Category	Family	OS
SmartDevice	Android	Android
SmartDevice	Apple	Apple iPhone
Network Camera	Dahua	Dahua Camera

Tags

System tags

User tags

investigate (0)

+ Create new tag

11.8%

So now we have started a SSH session form the iPad to 192.168.1.131

Customer: Ariya Publ...

a4d1d25f3252

Manage

Overview

Applications

Security

Analyze

Visibility

AirGroup

Applications

Websites

APPLICATIONS (Passive Monitoring)

TOTAL TRANSFERRED: 37.8 MB

APPLICATION	CATEGORY	USAGE
Google Analytics	Google SAAS	91 KB
apple.com	Web	85 KB
Secure Shell	Encrypted	27 KB

Under the profile tab we should see SSH under Application ID

Customer: Ariya Publ...

a4d1d25f3252

Manage

Overview

Applications

Security

Analyze

Live Events

Events

Tools

Summary

AI Insights

Location

Sessions

Profile

Flow Attributes

Expand All

Collapse All

Application Group

business-systems.cloud-security

business-systems.encrypted-tunnel

business-systems.general-business

Show 6 more

Application ID

abc-au

akamai

amazon

amazon-aws

apns

google-tags

http2

icloud

ntp

ssh

We also see a hit under the new tag that we created.

Customer: Ariya Publ...

Global

Manage

Overview

Devices

Clients

Guests

Applications

Clients Profile

Classified

Generic

ALL

Client Types

Category	Family	OS	Percentage
SmartDevice	Android	Android	
SmartDevice	Apple	Apple iPhone	

Tags

System tags

User tags

investigate (1)

+ Create new tag

Customer: Ariya Publ...

Global

Manage

Overview

Devices

Clients

Clients

Clients Profile

Classified

Generic

ALL

Client Types

Category	Family	OS	Percentage
SmartDevice	Apple	Apple iPad	100%

Clicking on it will take us to the client with this tag.

Customer: Ariya Publ...

Global

Manage

Overview

Devices

Clients

Clients Profile

Back

CONNECTED

Apple iPad Clients: (1)

MAC	IP Address	Host Name	MAC Vendor	Category	Family	OS	Client Source
a4d1d25f3252	10.10.31.44	ariyaps-iPad	Apple, Inc.	SmartDevice	Apple	Apple iPad	CP1-611

Customer: Ariya Publ...

Summary

AI Insights

Location

Sessions

Profile

← a4d1d25f3252

Manage

Overview

Category SmartDevice

Family Apple

OS Apple iPad

Tags

[Mobile & Gadgets]

investigate

Actions

Even though we have a device that has matched with our newly created “investigate” device tag, still the device is on the network using IoT-Lab user role.

Customer: Ariya Publ...

AOS10

Manage

Overview

Devices

Clients

Guests

Applications

Clients

ALL

0 bytes (0 by)

All 1

Connecting 0

Connected 1

Failed 0

Offline 0

Blocked 0

Wireless 1

Wired 0

Remote 0

CLIENTS

Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role
a4d1d25f3252	Connected	10.10.31.44	31	AP-605H-5d:6b	testPSK	IoT-Lab

The aim here is to send a Change of Authorisation (CoA) to the NAD to reauthenticate the device and during this re authentication the device is associated with a different user-role.

So, we need to configure ClearPass to send a CoA for devices when the device tags changes. We'll do this by navigating to Administration » Server Manager » Device Insight and change the “Device Tag Updates Action”.

Device Tag Updates Action

Tags Update Action:

☐ No action

☐ Apply action for all Tag updates

☒ Apply action for selected Tag updates only

Selected Tags for Action:

investigate

Remove

Add

RADIUS Action:

[Aerohive - Terminate Session]

NOTE -

Any Disconnect or RADIUS CoA type action can be specified per Service for any device, authenticating to the network, under the Profile tab for each Service. When no Disconnect or RADIUS CoA action is applicable, the RADIUS action configured in this page will be used.

Note that we already had enabled profiler for our ClearPass service.

5.3 Device Insight Tag Testing

So here is our final test in which we first get the device to connect to our WLAN and as before it connects and gets the IoT-Lab user-role.

The screenshot shows the Aruba Central interface. On the left, the 'Clients' tab is selected. The main area displays a table of clients. The client with MAC address a4:d1:d2:5f:32:52 is shown as 'Connected' to AP-605H-5d:6b. The table headers are: Client Name, Status, IP Address, VLAN, Connected To, SSID/Port, and AP Role.

Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role
a4:d1:d2:5f:32:52	Connected	10.10.31.44	31	AP-605H-5d:6b	testPSK	IoT-Lab

Now from it, we start a SSH session to an internal server. Aruba Central DI will assign the “investigate” tag.

The screenshot shows the 'Profile' tab for the client a4d1d25f3252. The 'Tags' section shows a tag named 'investigate' with a yellow highlight.

And it will send this info to ClearPass. We'll go to the access tracker for the details of authentications.

The screenshot shows the ClearPass Access Tracker interface. It displays two authentication requests for the client a4d1d25f3252. The first request is for 'W-IoT' and the second is for 'W-investigate'.

#	NAS IP Address	Server Name	Source	Username	Service	Login Status	Enforcement Profiles	Request Timestamp
1.	192.168.1.243	CP1-611	RADIUS	a4d1d25f3252	simple MAC Authentication CI tags	ACCEPT	W-IoT	2025/01/26 18:31:40
2.	192.168.1.243	CP1-611	RADIUS	a4d1d25f3252	simple MAC Authentication CI tags	ACCEPT	W-investigate	2025/01/26 18:31:02

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 session was run on that client, the second authentication request comes in and this time the enforcement profile that was used is W-investigate.

We'll first open session #2 and here we see that indeed a CoA was sent.

The screenshot shows the 'RADIUS Dynamic Authorization' tab for the client a4d1d25f3252. It displays details about the session, including the login status, session identifier, date and time, end-host identifier, end-host profile, end-host status, username, access device IP (port), access device name, system posture status, and policies used.

Field	Value
Login Status:	ACCEPT
Session Identifier:	R00000014-05-6795e4b6
Date and Time:	Jan 26, 2025 18:31:02 AEDT
End-Host Identifier:	A4-D1-D2-5F-32-52
End-Host Profile:	SmartDevice / Apple / Apple iPad
End-Host Status:	Unknown
Username:	a4d1d25f3252
Access Device IP (Port):	192.168.1.243
Access Device Name:	AOS10-gateway1 (AOS10-gateway1 / Aruba)
System Posture Status:	UNKNOWN (100)
Service:	simple MAC Authentication CI tags
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]
Roles:	IoT, [User Authenticated]
Enforcement Profiles:	W-IoT
Service Monitor Mode:	Disabled
Online Status:	Offline

Summary	Input	Output	Accounting	RADIUS Dynamic Authorization
Dynamic Authorization Action# 1				
Date and Time	Jan 26, 2025 18:31:37 AEDT			
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 a4d1d25f3252.			
RADIUS Dynamic Authorization Attributes	Calling-Station-Id = a4d1d25f3252			

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”

Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R00000015-05-6795e4dc		
Date and Time:	Jan 26, 2025 18:31:40 AEDT		
End-Host Identifier:	A4-D1-D2-5F-32-52		Open in Central
End-Host Profile:	SmartDevice / Apple / Apple iPad		
End-Host Status:	Unknown		Mark as Known
Username:	a4d1d25f3252		
Access Device IP (Port):	192.168.1.243		
Access Device Name:	AOS10-gateway1 (AOS10-gateway1 / Aruba)		
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], [Endpoints Repository], [Time Source]		
Roles:	IoT, [User Authenticated], investigate		
Enforcement Profiles:	W-investigate		

Summary	Input	Output	Accounting
Username:	a4d1d25f3252		
End-Host Identifier:	A4-D1-D2-5F-32-52 (SmartDevice / Apple / Apple iPad)		
Access Device IP (Port):	192.168.1.243		
Access Device Name:	AOS10-gateway1 (AOS10-gateway1 / Aruba)		
RADIUS Request			
Authorization Attributes			
Computed Attributes			
Connection:Src-IP-Address		192.168.1.243	
Connection:Src-Port		51066	
Connection:SSID		testPSK	
Date:Date-Time		2025-01-26 18:31:40	
Endpoint:Device Insight Tags		[Mobile & Gadgets], investigate	
Endpoint:School_Asset		false	
Endpoint Attributes			

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

Endpoint	Attributes	Device Fingerprints
MAC Address	A4-D1-D2-5F-32-52	
Description		
Status	<div><div><input type="radio"/> Known client</div><div><input checked="" type="radio"/> Unknown client</div><div><input type="radio"/> Disabled client</div></div>	
MAC Vendor	Apple, Inc.	
Added by	Policy Manager	
Added At	Jan 26, 2025 17:06:39 AEDT	
Updated At	Jan 26, 2025 18:31:35 AEDT	
Online Status	<div><div><div></div></div>Online</div>	
Connection Type	Wireless	
Access Point	AP-605H-5d:6b	
Network SSID	testPSK	
Randomized MAC Address	FALSE	
School Asset	<div><div><input type="radio"/> Yes</div><div><input checked="" type="radio"/> No</div></div>	

Profiling Information	
IPv4 Address	10.10.31.44
IPv6 Address	-
Static IP	FALSE
Hostname	ariyaps-iPad
Device Category	SmartDevice
Device OS Family	Apple
Device Name	Apple iPad
Device Insight Tags	[Mobile & Gadgets] investigate
Profiled by	Device Insight
First Profiled At	Jan 26, 2025 15:43:53 AEDT
Last Profiled At	Jan 26, 2025 18:31:32 AEDT

Endpoint	Attributes	Device Fingerprints
Endpoint Fingerprint Details		
Application Group:	business-systems.cloud-security, business-systems.encrypted-tunnel, business-systems.general-business, business-systems.network, collaboration.social-media, general-internet.search, general-internet.sports, general-internet.utility, media.audio-streaming, misc.misc	
Application ID:	unknown, abc-au, akamai, amazon, amazon-aws, apns, apple, apple-location, apple-update, appstore, cloudflare, dns, facebook, fcm, flurry, google-ads, google-analytics, google-gen, google-play, google-tags, http2, icloud, ntp, ssh, unknown	
Destination Connections:	10.10.31.1:0:tcp, 103.43.90.19:0:tcp, 108.139.9.107:0:tcp, 13.248.150.189:0:tcp, 17.253.121.202:0:tcp, 17.253.34.131:0:udp, 17.57.145.38:0:tcp, 17.57.145.39:0:tcp, 17.57.145.41:0:tcp, 192.168.1.131:0:tcp, 192.168.1.131:0:udp, 203.219.43.209:0:tcp, accu.fm:0:tcp, accuradio.com:0:tcp, adswizz.com:0:tcp, app-measurement.com:0:tcp, apple.com/bag:0:tcp, apple.com:0:tcp, cloudfront.net:0:tcp, doubleclick.net:0:tcp, facebook.com:0:tcp, gigya.com:0:tcp, googleadservices.com:0:tcp, googleapis.com:0:tcp, tritondigital.com:0:tcp	
DHCP Option12:	ariyaps-iPad	
DHCP Option55:	1,121,3,6,15,119,252	
DHCP Options:	53,55,57,61,50,51,12	
fingerprint.dhcp.transaction_id:	230257218	

Going back to the client view in Aruba Central we'll see the correct user role and VLAN assignment.

Customer: Ariya Publ...

AOS10

Manage

Overview

Devices

Clients

Guests

Applications

Clients

CLIENTS

ALL

127.54 MB (@ 64.78 MB)

All

Connecting

Connected

Failed

Offline

Blocked

1

0

0

0

1

0

Wireless

Wired

Remote

1

0

0

Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role
ariyaps-iPad	Connected	10.10.32.44	32	AP-605H-5d:6b	testPSK	Investigate