Table of Contents

Revision History

DATE	VERSION	EDITOR	CHANGES
11 Aug 2024	0.1	Ariya Parsamanesh	Initial creation
26 Aug 2024	0.2	Ariya Parsamanesh	Added the testing section

1 MAC Auth for AP-605H downlink Ethernet Ports

Cloud Auth is part of Aruba Central which provides simple but powerful NAC and authentication solution. It provides 802.1x EAP-TLS authentication based on its integration with cloud identity store such as Google Workspace or Entra ID and assign the users the right level of network access. Additionally, Cloud Auth supports MAC authentication for both wired and wireless access.

Here we'll be configuring it for MAC authentication for downlink wired ports of our AP-605H. Once profiled and authenticated, they will be assigned their appropriate access and VLAN policies.

This enables secure connectivity without hassle of static configuration particularly for scenarios that you need to connect speaker and cameras to these ports.

1.1 Things you need

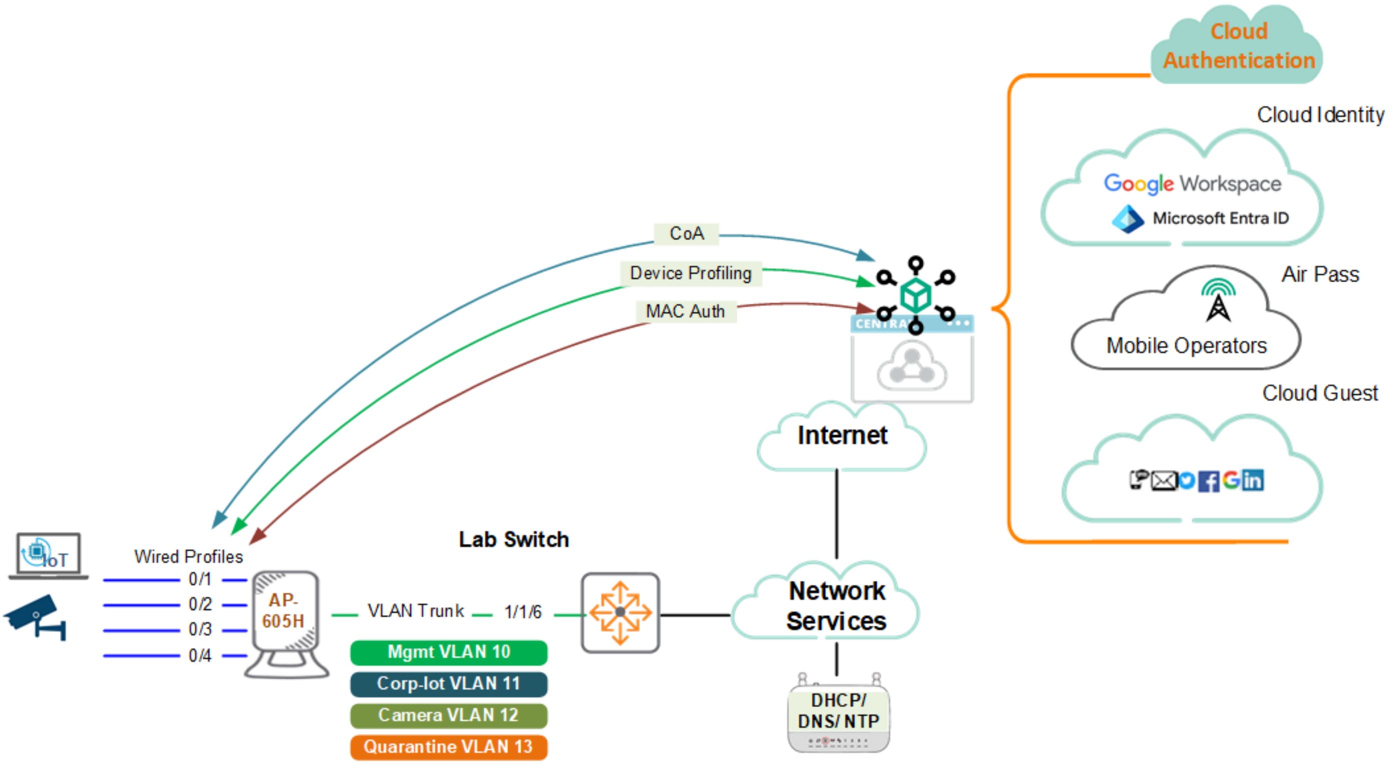
- AP-605H running Aruba Instant firmware 8.12.0.1 or later
- Aruba Central for management
- LAN switch and network services (DHCP, DNS, NTP)

Note that this solution will work with AOS10 APs that are managed by Aruba Central as well.

1.2 Topology

The main use case here is securely connecting IoT, Camera and Speakers to the wired downlink of the APs as you might not have a spare switch port or unavailability of a cable drop. This is where you can use the multiple Ethernet ports that are available on Aruba APs particularly AP-605H that has 4x Ethernet ports where the AP can also provide 802.3af/at PoE output for 2x Ethernet ports.

As shown we'll be using Cloud Auth functionality that comes with Aruba Central.



Here we'll have two devices to test and basically we want to connect a corporate IoT device and a camera and then based on their device types and category, they will be assigned the following policies.

User roles	VLANs	Access policies
Corp-Dev	11	Allow-all
camera	12	Only to Camera subnet
quarantine	13	Only to DHCP and DNS

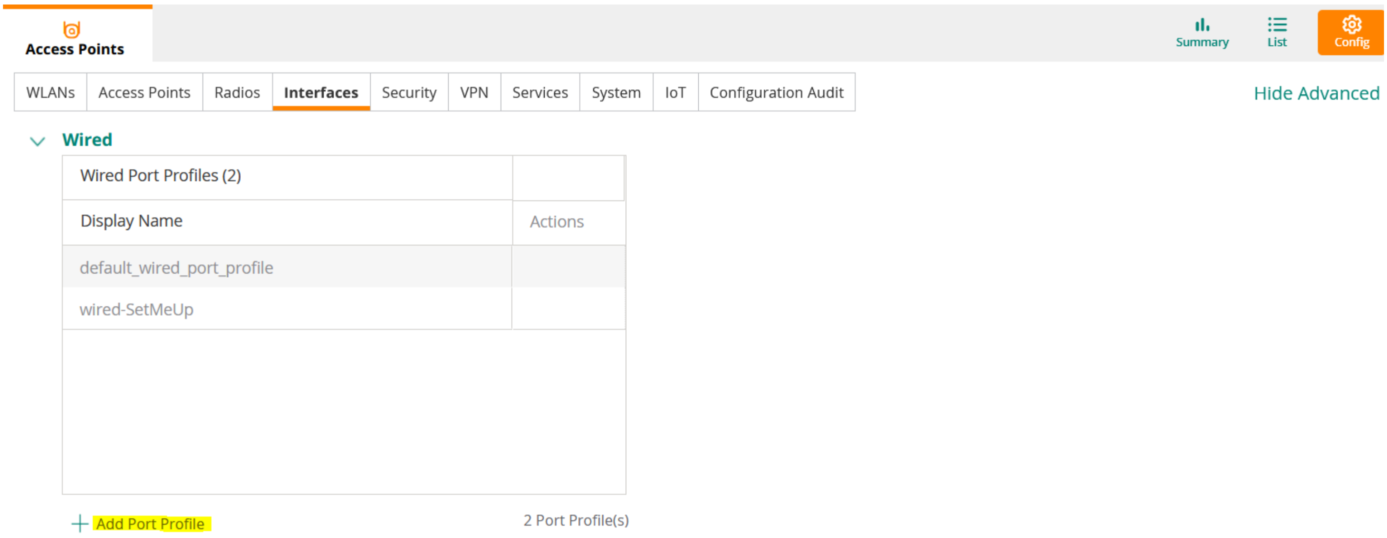
1.3 Aruba Central configuration

We are using AP-605H that has 4x Ethernet ports

- Downlink (E1-E4): Ethernet wired network ports (RJ-45)
- Auto-sensing link speed (10/100/1000BASE-T) and MDI/ MDX
- 802.3az Energy Efficient Ethernet (EEE)
- E1&E2: POE-PSE: 802.3af/at POE output; dual 802.3af (both ports) or single 802.3at (E1 only); 30W max

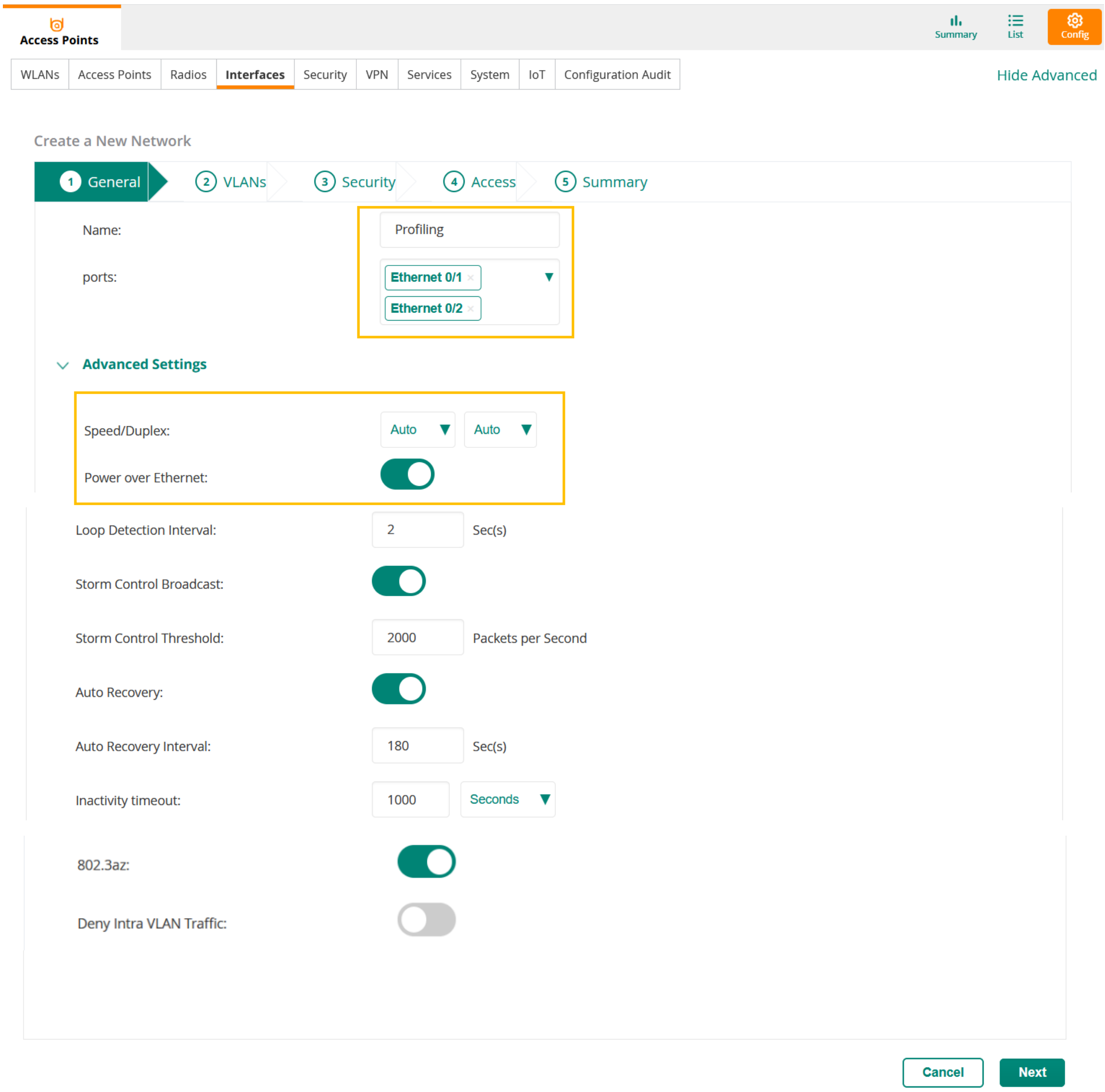
The wired ports of an AP allow third-party devices such as IP phones, Cameras or printers to connect to it as if it were a LAN switch along with the full security you have for your wireless clients such as various modes of authentication, Role based access, etc.

Here we'll start with Ethernet port profiles and we'll do all the configurations at group level of Aruba Central.



Wired Port Profiles (2)	
Display Name	Actions
default_wired_port_profile	
wired-SetMeUp	

We'll add a wired port profile called "profiling" and assign it to E1 and E2 ports.



Create a New Network

Name: Profiling

ports: Ethernet 0/1, Ethernet 0/2

Advanced Settings

Speed/Duplex: Auto Auto

Power over Ethernet: On

Loop Detection Interval: 2 Sec(s)

Storm Control Broadcast: On

Storm Control Threshold: 2000 Packets per Second

Auto Recovery: On

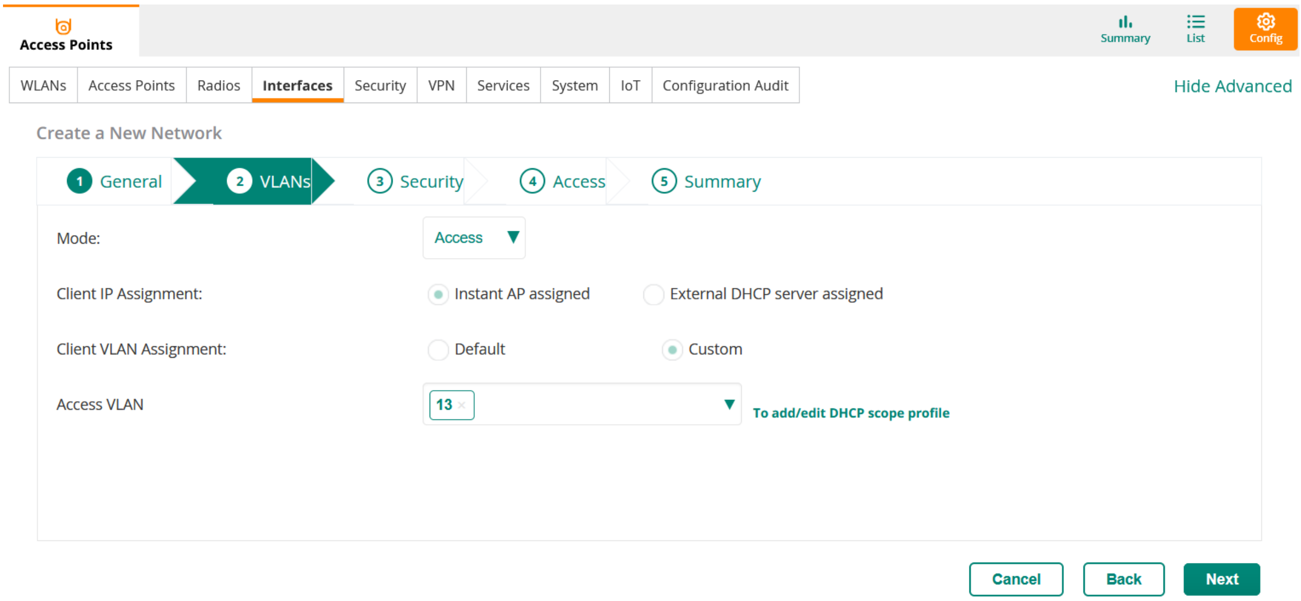
Auto Recovery Interval: 180 Sec(s)

Inactivity timeout: 1000 Seconds

802.3az: On

Deny Intra VLAN Traffic: Off

Note that we have enabled loop detection, 802.3az, storm control along with auto recovery incase a loop was detected. Our catch-all (quarantine) VLAN is VLAN 13 that has limited access.



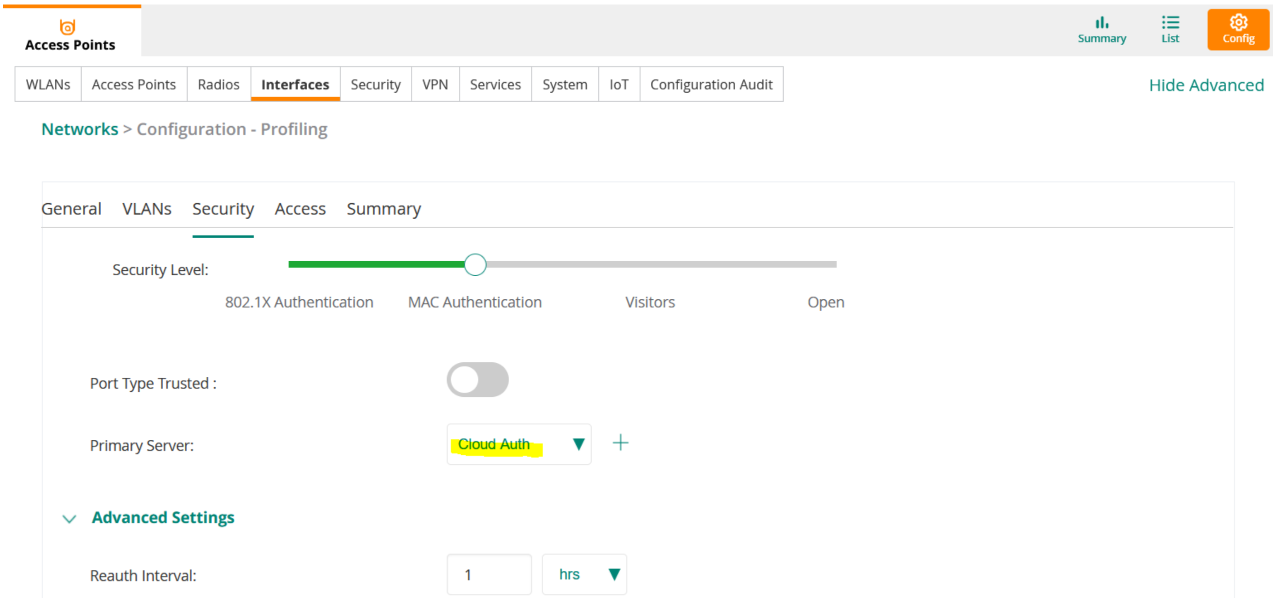
Create a New Network

Mode: Access

Client IP Assignment: ● Instant AP assigned ○ External DHCP server assigned

Client VLAN Assignment: ○ Default ● Custom

Access VLAN: 13



Networks > Configuration - Profiling

Security Level: 802.1X Authentication | MAC Authentication | Visitors | Open

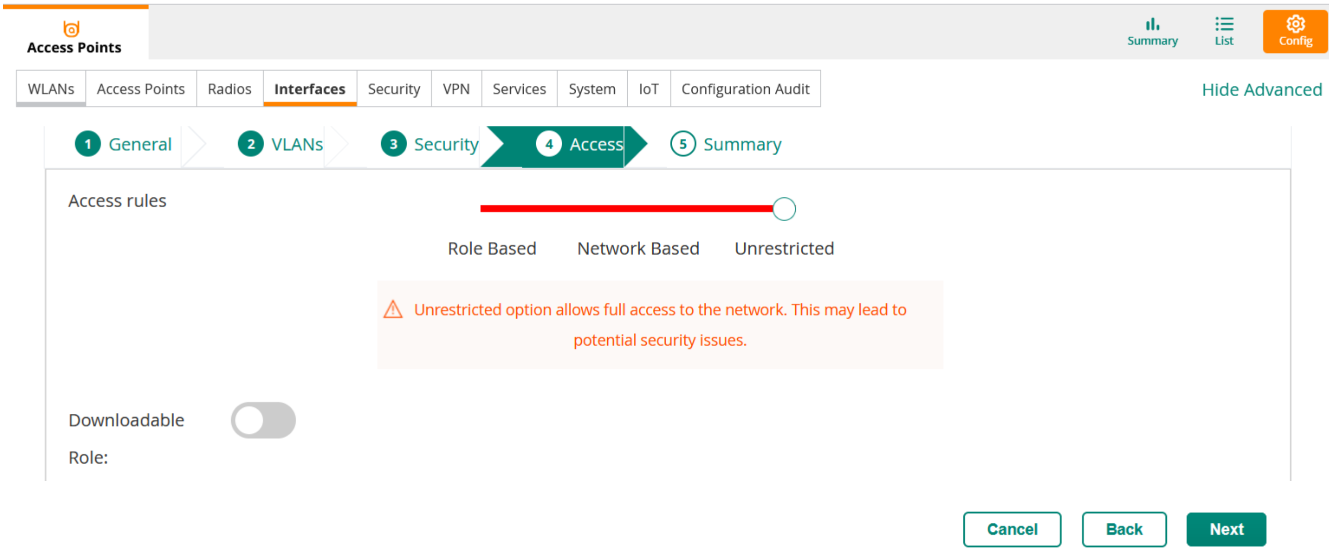
Port Type Trusted :

Primary Server: Cloud Auth

Advanced Settings

Reauth Interval: 1 hrs

We are selecting MAC authentication and choosing Cloud Auth as the authentication server.

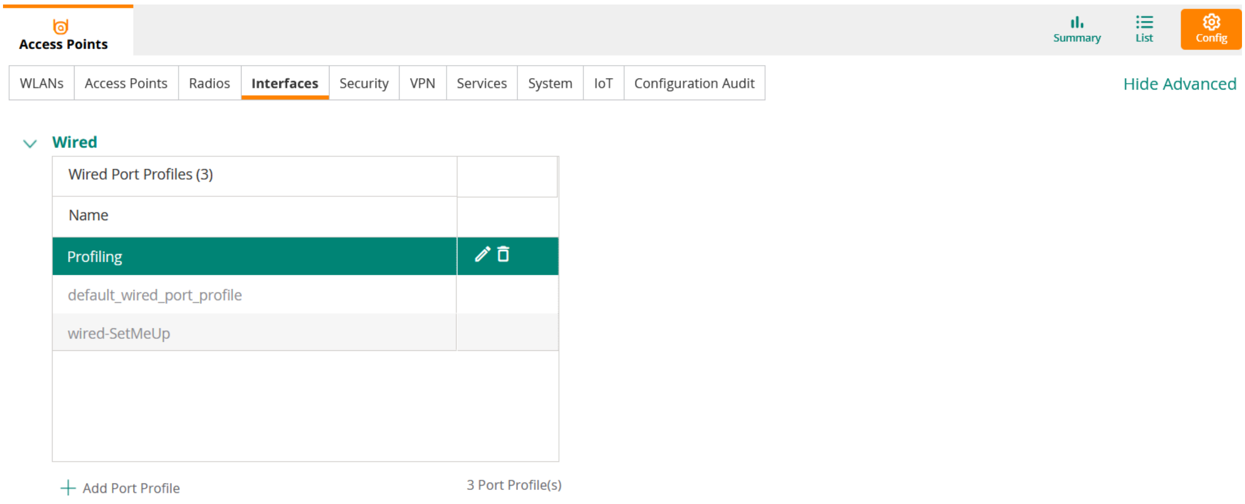


Access rules: Role Based | Network Based | Unrestricted

⚠ Unrestricted option allows full access to the network. This may lead to potential security issues.

Downloadable Role:

Finally we'll select access rules to be "unrestricted". This means that by default the devices will be on a quarantine VLAN with limited access. Once you finish this and save it, you have the new "Profiling" port profile that have been applied to E1 and E2 ports.



Wired

Wired Port Profiles (3)
Name
Profiling
default_wired_port_profile
wired-SetMeUp

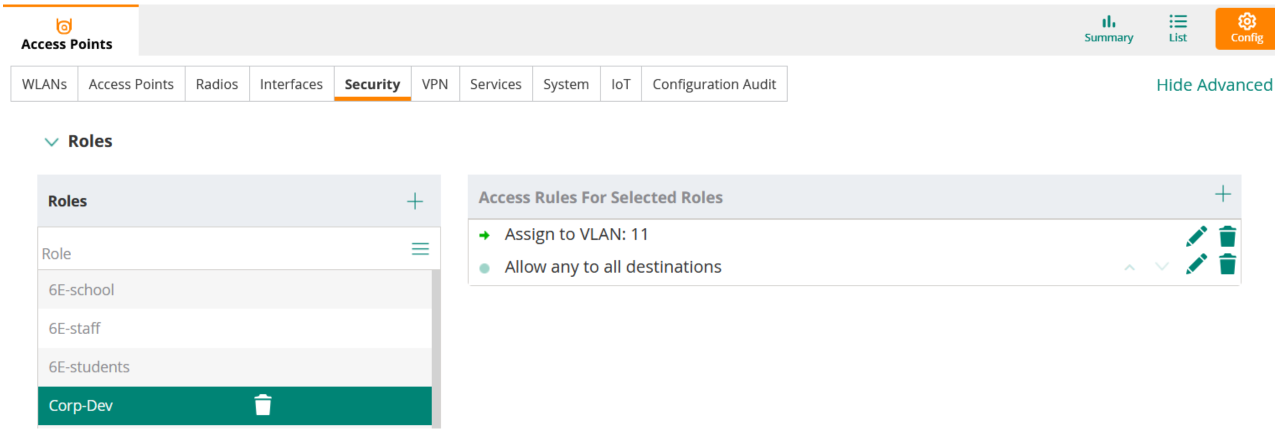
3 Port Profile(s)

1.4 Instant AP User Roles

Next, we'll add the user roles along with their VLAN assignments and access policies.

User roles	VLANs	Access policies
Corp-Dev	11	Allow-all
camera	12	Only to Camera and NVR subnets
quarantine	13	Only to DHCP and DNS

Here are the access policies for reach role.

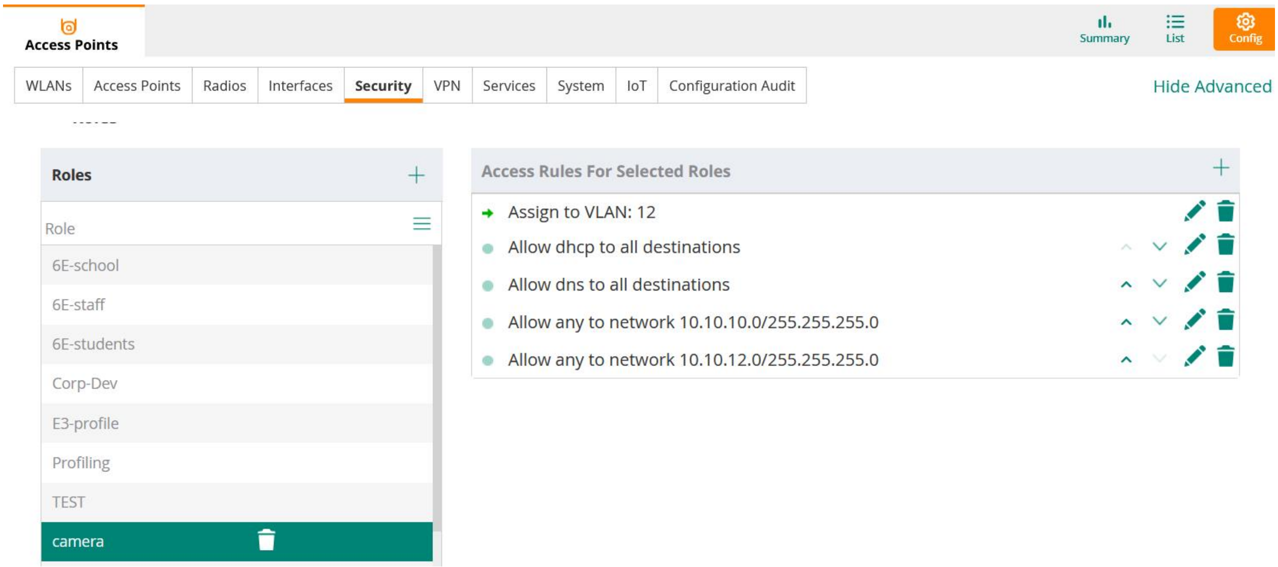


Roles

Roles
Role
6E-school
6E-staff
6E-students
Corp-Dev

Access Rules For Selected Roles

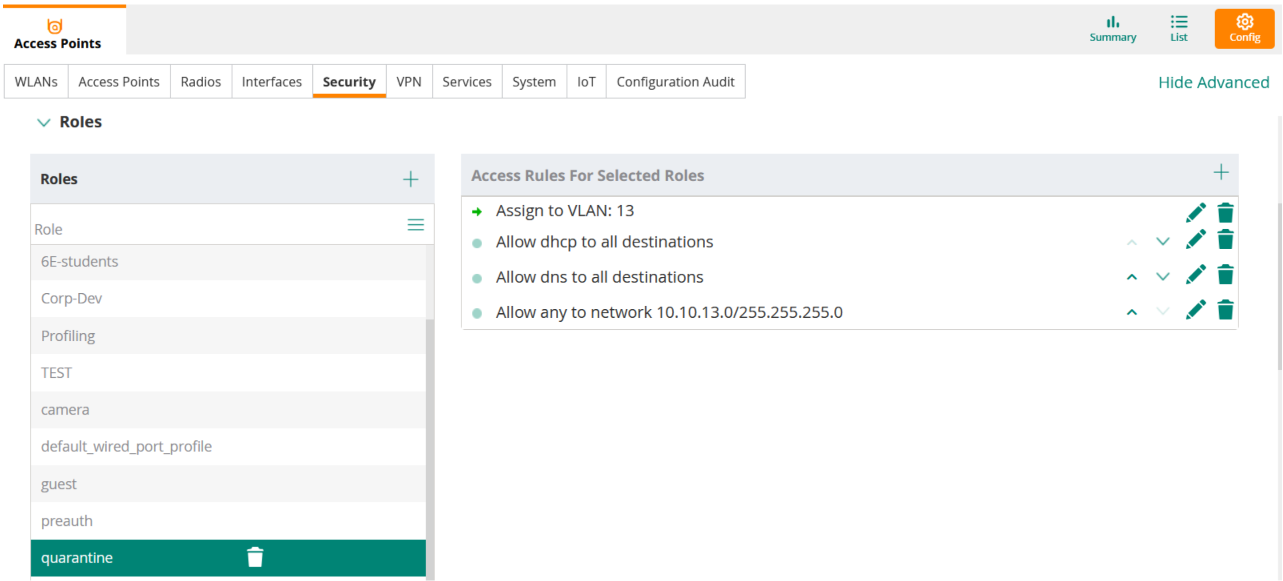
- Assign to VLAN: 11
- Allow any to all destinations



Roles
Role
6E-school
6E-staff
6E-students
Corp-Dev
E3-profile
Profiling
TEST
camera

Access Rules For Selected Roles

- Assign to VLAN: 12
- Allow dhcp to all destinations
- Allow dns to all destinations
- Allow any to network 10.10.10.0/255.255.255.0
- Allow any to network 10.10.12.0/255.255.255.0



Roles

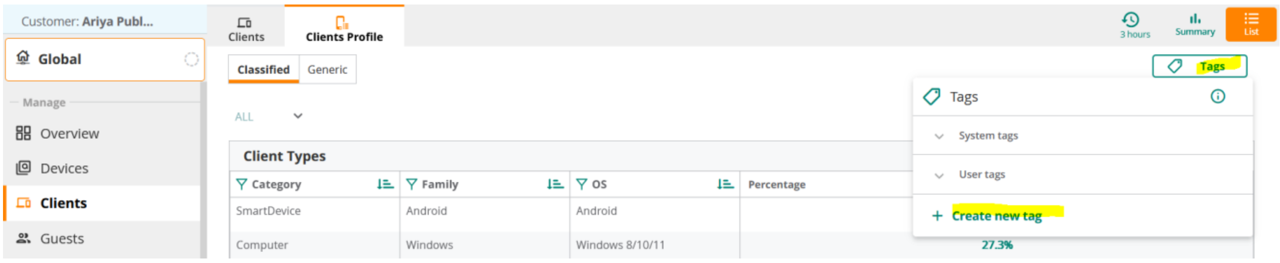
Roles
Role
6E-students
Corp-Dev
Profiling
TEST
camera
default_wired_port_profile
guest
preauth
quarantine

Access Rules For Selected Roles

- Assign to VLAN: 13
- Allow dhcp to all destinations
- Allow dns to all destinations
- Allow any to network 10.10.13.0/255.255.255.0

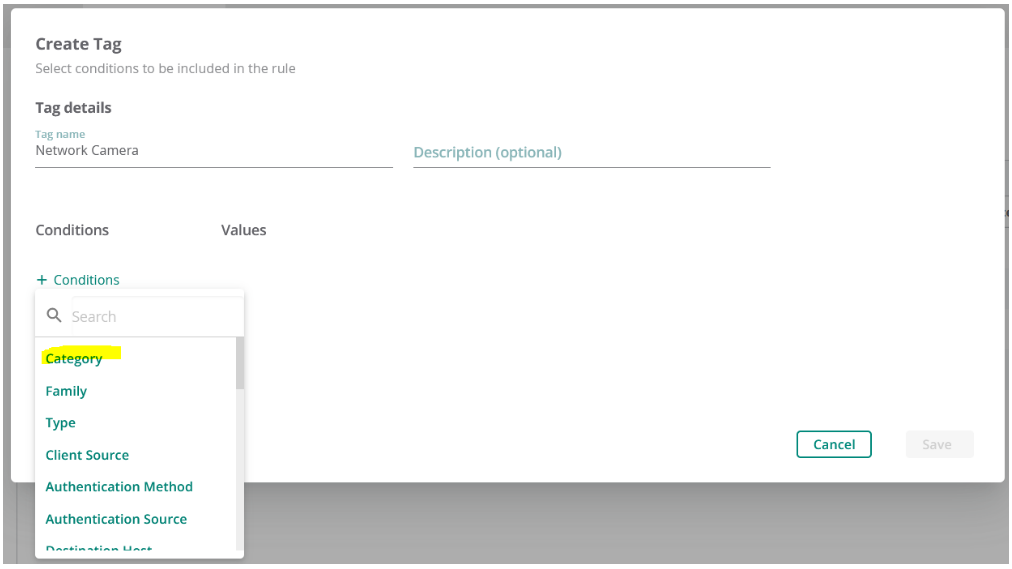
1.5 User Defined Tags

Next we need to create our device tags so that you can make use of them in our cloud auth client access policy.



Client Types

Category	Family	OS	Percentage
SmartDevice	Android	Android	
Computer	Windows	Windows 8/10/11	27.3%



Create Tag

Select conditions to be included in the rule

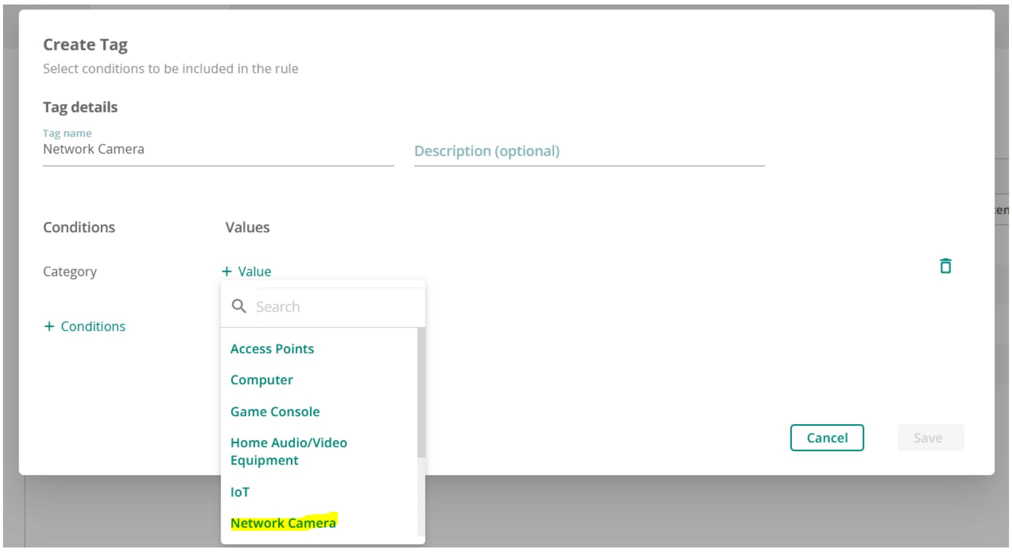
Tag details

Tag name

Network Camera

Description (optional)

Conditions   Values



Create Tag

Select conditions to be included in the rule

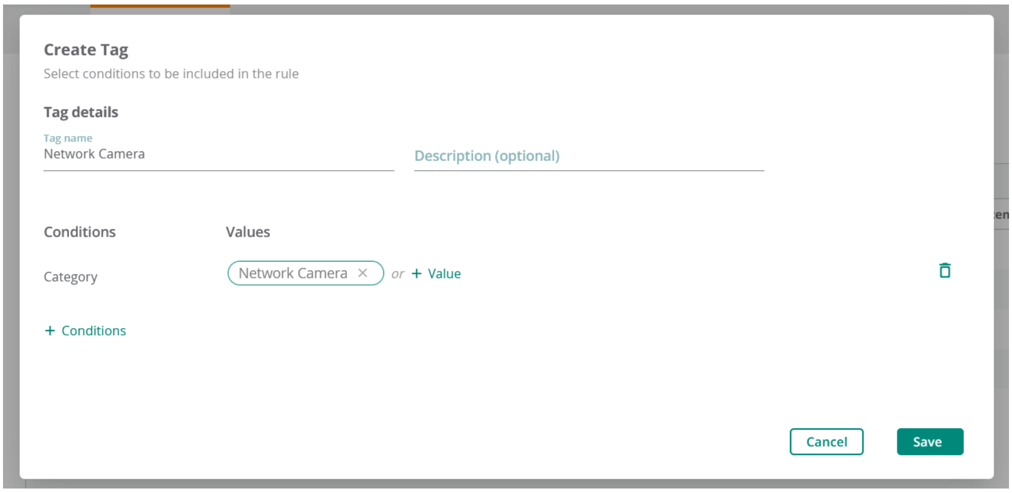
Tag details

Tag name
Network Camera

Description (optional)

Conditions	Values
Category	+ Value

+ Conditions



Create Tag

Select conditions to be included in the rule

Tag details

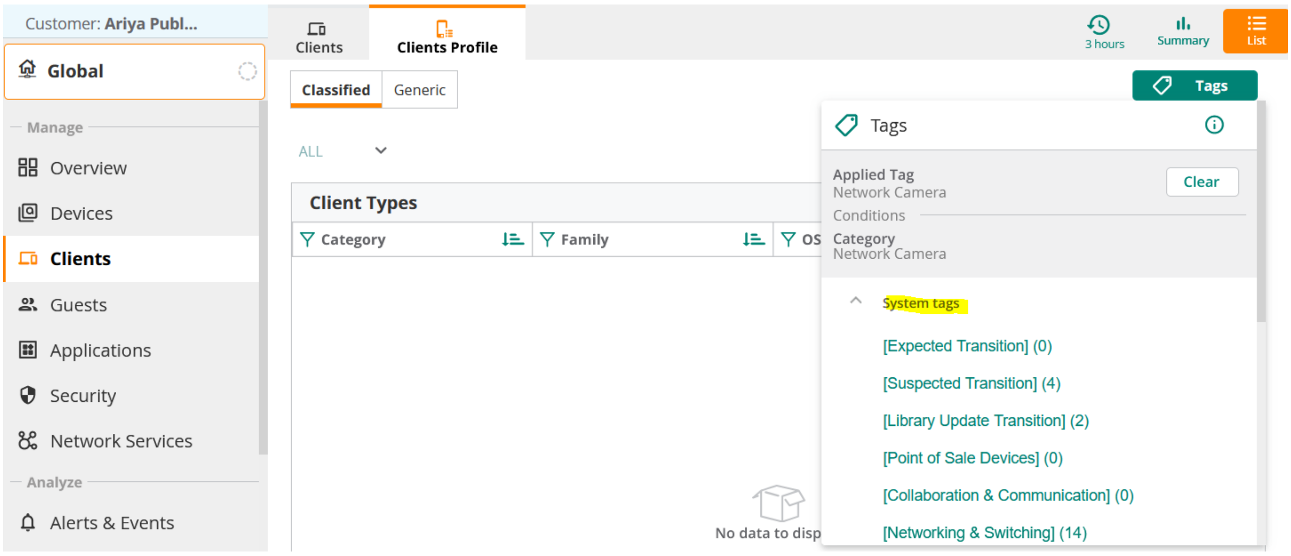
Tag name
Network Camera

Description (optional)

Conditions	Values
Category	Network Camera ✕ *or* + Value

+ Conditions

Note that you can add additional conditions to suit your specific cases. Also as shown below, here is where you can see all the system and user defined tags where you can modify/delete them.



Tags

Applied Tag
Network Camera

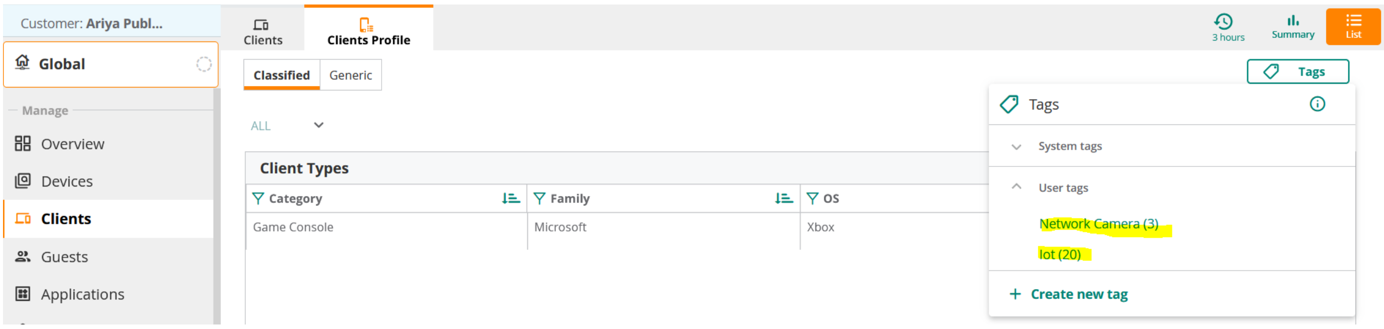
Clear

Conditions

Category
Network Camera

System tags

- [Expected Transition] (0)
- [Suspected Transition] (4)
- [Library Update Transition] (2)
- [Point of Sale Devices] (0)
- [Collaboration & Communication] (0)
- [Networking & Switching] (14)



Client Types

Category	Family	OS
Game Console	Microsoft	Xbox

Tags

System tags

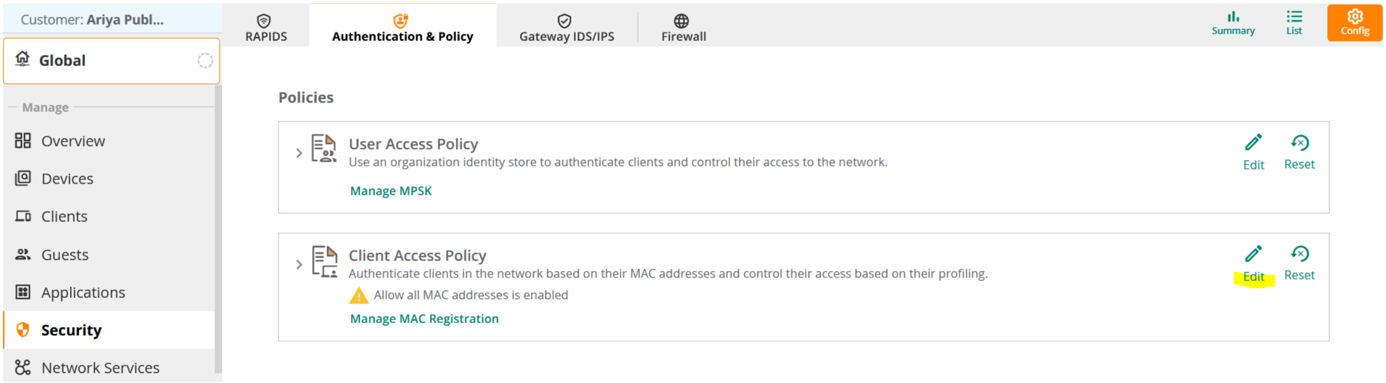
User tags

Network Camera (3)

Iot (20)

1.6 Authentication Policy

Since we are using MAC authentication, we'll create our authentication policy under "client Access policy" as shown below.



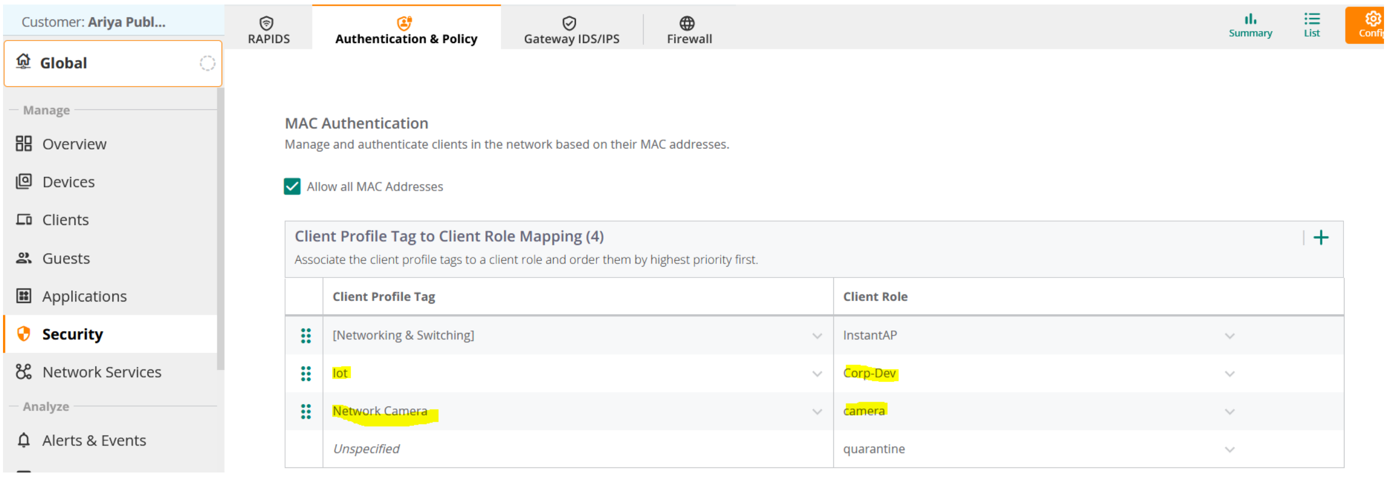
Policies

User Access Policy
Use an organization identity store to authenticate clients and control their access to the network.
Manage MPSK

Client Access Policy
Authenticate clients in the network based on their MAC addresses and control their access based on their profiling.
⚠ Allow all MAC addresses is enabled
Manage MAC Registration

Here we are using one of the system-defined profiles for Instant APs. And the second role mapping is for our camera. Note that the Network Camera is the user tag we just created and "camera" is the user role we configured at group level for our IAPs. The user roles will be automatically available from the drop down menu.

The last role mapping is to catch the rest of unidentified tags that needs to be mapped to quarantine user role.



MAC Authentication
Manage and authenticate clients in the network based on their MAC addresses.

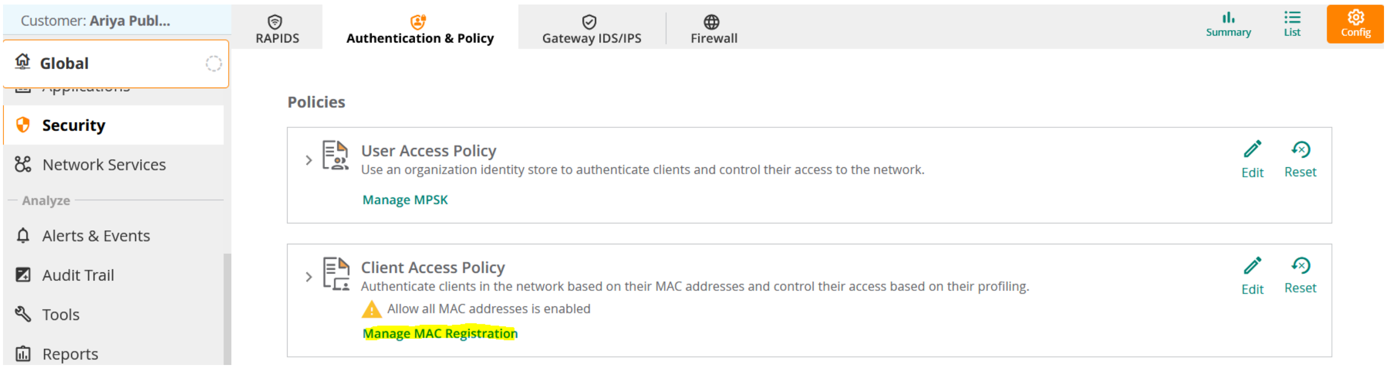
☑ Allow all MAC Addresses

Client Profile Tag to Client Role Mapping (4)
Associate the client profile tags to a client role and order them by highest priority first.

Client Profile Tag	Client Role
[Networking & Switching]	InstantAP
Iot	Corp-Dev
Network Camera	camera
Unspecified	quarantine

Note that we have enabled "Allow all MAC addresses", so that the MAC addresses get registered automatically to have access to the network. Then based on the user-defined tags, we can assign specific user-roles.

If that option was not selected, then we had to register the MAC addresses as shown below. You also have the option of uploading the list of Mac addresses with a CSV file.



Policies

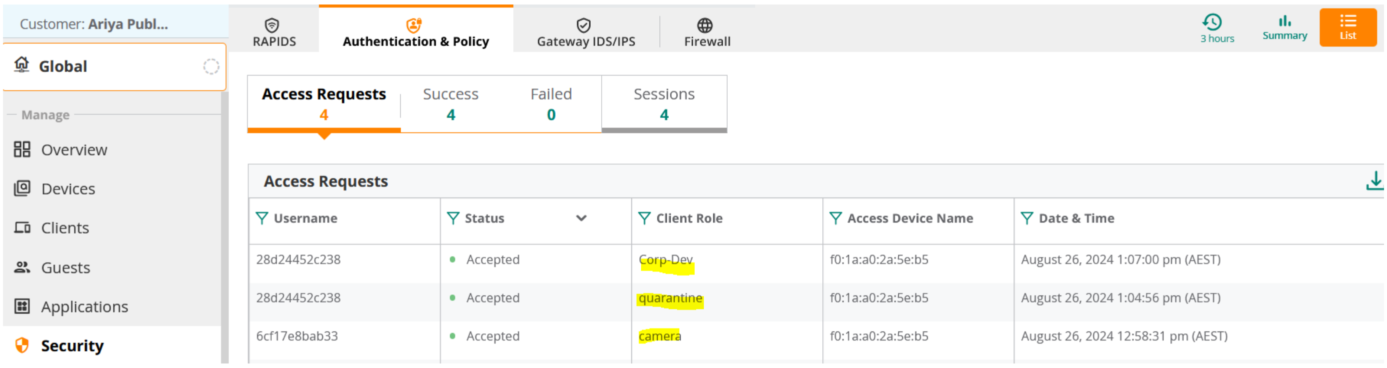
User Access Policy
Use an organization identity store to authenticate clients and control their access to the network.
Manage MPSK

Client Access Policy
Authenticate clients in the network based on their MAC addresses and control their access based on their profiling.
⚠ Allow all MAC addresses is enabled
Manage MAC Registration

Finally once you have all your devices that needs MAC authentication registered, you can turn off “Allow all MAC addresses”.

1.7 Cloud Auth Testing

At this point, we have connected our camera to the E1 port of the AP-605H. As the authentication request come in, it gets displayed under “Access Requests” as shown below.

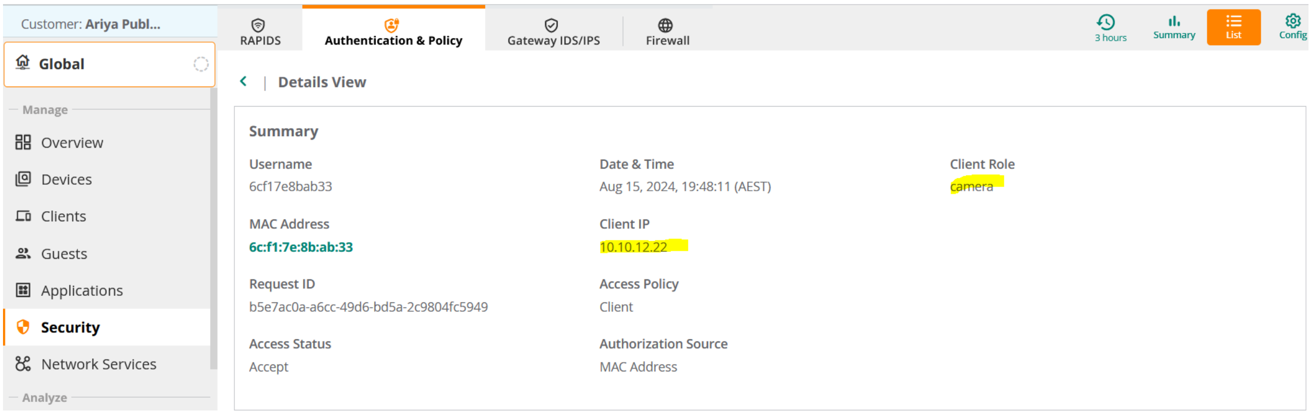


Access Requests	Success	Failed	Sessions
4	4	0	4

Access Requests

Username	Status	Client Role	Access Device Name	Date & Time
28d24452c238	Accepted	Corp-Dev	f0:1a:a0:2a:5e:b5	August 26, 2024 1:07:00 pm (AEST)
28d24452c238	Accepted	quarantine	f0:1a:a0:2a:5e:b5	August 26, 2024 1:04:56 pm (AEST)
6cf17e8bab33	Accepted	camera	f0:1a:a0:2a:5e:b5	August 26, 2024 12:58:31 pm (AEST)

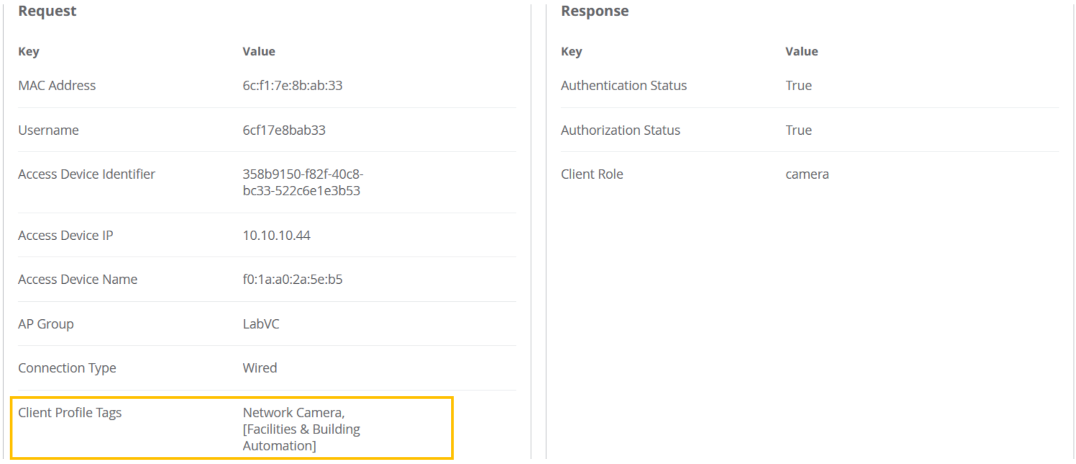
Clicking on the camera username (that is the MAC address displayed above takes us to authentication request details.



Details View

Summary

Username: 6cf17e8bab33
Date & Time: Aug 15, 2024, 19:48:11 (AEST)
Client Role: camera
MAC Address: 6c:f1:7e:8b:ab:33
Client IP: 10.10.12.22
Request ID: b5e7ac0a-a6cc-49d6-bd5a-2c9804fc5949
Access Policy: Client
Access Status: Accept
Authorization Source: MAC Address



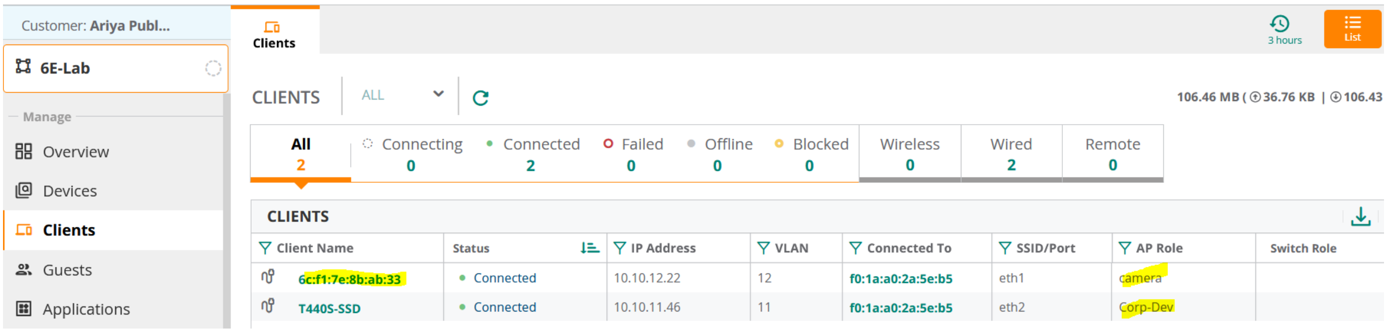
Request

Key	Value
MAC Address	6c:f1:7e:8b:ab:33
Username	6cf17e8bab33
Access Device Identifier	358b9150-f82f-40c8-bc33-522c6e1e3b53
Access Device IP	10.10.10.44
Access Device Name	f0:1a:a0:2a:5e:b5
AP Group	LabVC
Connection Type	Wired
Client Profile Tags	Network Camera, [Facilities & Building Automation]

Response

Key	Value
Authentication Status	True
Authorization Status	True
Client Role	camera

As we are following this user/device, we see that it is indeed connected to E1 of the AP-605H



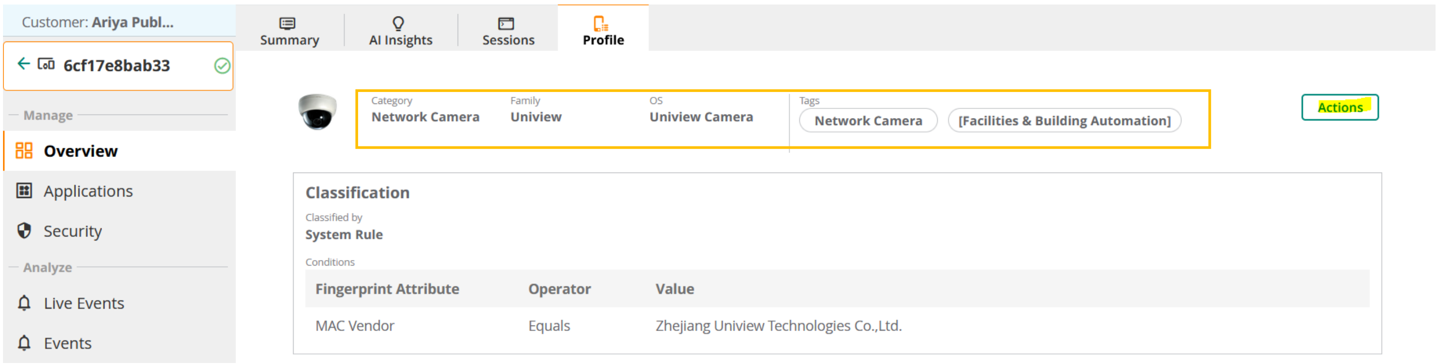
CLIENTS ALL

106.46 MB (36.76 KB | 106.43

All	Connecting	Connected	Failed	Offline	Blocked	Wireless	Wired	Remote
2	0	2	0	0	0	0	2	0

CLIENTS

Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role	Switch Role
6c:f1:7e:8b:ab:33	Connected	10.10.12.22	12	f0:1a:a0:2a:5e:b5	eth1	camera	
T440S-SSD	Connected	10.10.11.46	11	f0:1a:a0:2a:5e:b5	eth2	Corp-Dev	



Category: Network Camera
Family: Uniview
OS: Uniview Camera
Tags: Network Camera [Facilities & Building Automation]

Classification

Classified by
System Rule

Conditions

Fingerprint Attribute	Operator	Value
MAC Vendor	Equals	Zhejiang Uniview Technologies Co.,Ltd.

1.8 Aruba Instant Testing

Here are the CLI commands to check for wired clients, for Aruba Instant AP's.

First let's check the port status of the AP-605H

```
f0:1a:a0:2a:5e:b5# sh port status

Port Status
-----------
Port  Type   Admin-State  Oper-State  STP-State  Dot3az  Loop-Protect  Storm-Control  Loop-
Detection-TX  Loop-Detection-RX
----  ----   -----------  ----------  ---------  ------  ------------  -------------  ----------
-------  -----------------
eth0  2.5GE  up           up          Off        Disable OFF           OFF            0        0
eth1  GE     up           down        Off        Disable ON            ON              0       0
eth2  GE     up           down        Off        Disable ON            ON              0       0
eth3  GE     up           down        Off        Disable OFF           OFF             0       0
eth4  GE     up           down        Off        Disable OFF           OFF             0       0
eth5  USB    up           down        Off        Disable OFF           OFF             0       0

f0:1a:a0:2a:5e:b5#
```

Now checking the wired clients.

```
f0:1a:a0:2a:5e:b5# sh clients wired

Wired Client List
-----------------
Name  IP Address  MAC Address  OS  Network  Access Point  Role  IPv6 Address  Speed
(mbps)
----  ----------  -----------  --  -------  ------------  ----  ------------  ---------
---
Info timestamp      :6510

f0:1a:a0:2a:5e:b5#
```

First the unknown device is put into quarantine user-role, where it will be identified.

```
f0:1a:a0:2a:5e:b5# sh clients wired

Wired Client List
-----------------
Name          IP Address   MAC Address        OS    Network  Access Point       Role
IPv6 Address               Speed (mbps)
----          ----------   -----------        --    -------  ------------       ----
------------               ------------
6cf17e8bab33  10.10.13.22  6c:f1:7e:8b:ab:33  NOFP  eth1     f0:1a:a0:2a:5e:b5
quarantine  fe80::6ef1:7eff:fe8b:ab33  -
Info timestamp      :16042

f0:1a:a0:2a:5e:b5#
```

At this stage a CoA is already sent to the AP and once the camera is reconnected it is identified as camera and placed in its VLAN.

Note that CloudAuth does not send any switch port bounce as a part of CoA, so you need to disconnect and reconnect the device to ensure you trigger a DHCP request on the client.

```
f0:1a:a0:2a:5e:b5# sh clients wired

Wired Client List
-----------------
Name  IP Address  MAC Address  OS  Network  Access Point  Role  IPv6 Address  Speed
(mbps)
----  ----------  -----------  --  -------  ------------  ----  ------------  ---------
---
Info timestamp      :17140

f0:1a:a0:2a:5e:b5# sh clients wired

Wired Client List
-----------------
Name          IP Address   MAC Address        OS    Network  Access Point       Role
IPv6 Address               Speed (mbps)
----          ----------   -----------        --    -------  ------------       ----
------------               ------------
6cf17e8bab33  10.10.12.22  6c:f1:7e:8b:ab:33  NOFP  eth1     f0:1a:a0:2a:5e:b5  camera
fe80::6ef1:7eff:fe8b:ab33  -
Info timestamp      :17599

f0:1a:a0:2a:5e:b5#
```

and when I connect the corporate IoT device to E2 port, it gets profiles and authenticated and will be placed in VLAN11.

```
f0:1a:a0:2a:5e:b5# sh clients wired

Wired Client List
-----------------
Name          IP Address   MAC Address        OS      Network  Access Point       Role
IPv6 Address               Speed (mbps)
----          ----------   -----------        --      -------  ------------       ----
------------               ------------
28d24452c238  10.10.11.46  28:d2:44:52:c2:38  Win 10  eth2     f0:1a:a0:2a:5e:b5  Corp-
Dev  --                         -
6cf17e8bab33  10.10.12.22  6c:f1:7e:8b:ab:33  NOFP    eth1     f0:1a:a0:2a:5e:b5
camera    fe80::6ef1:7eff:fe8b:ab33  -
Info timestamp      :1391

f0:1a:a0:2a:5e:b5#
```