1 Table of Contents

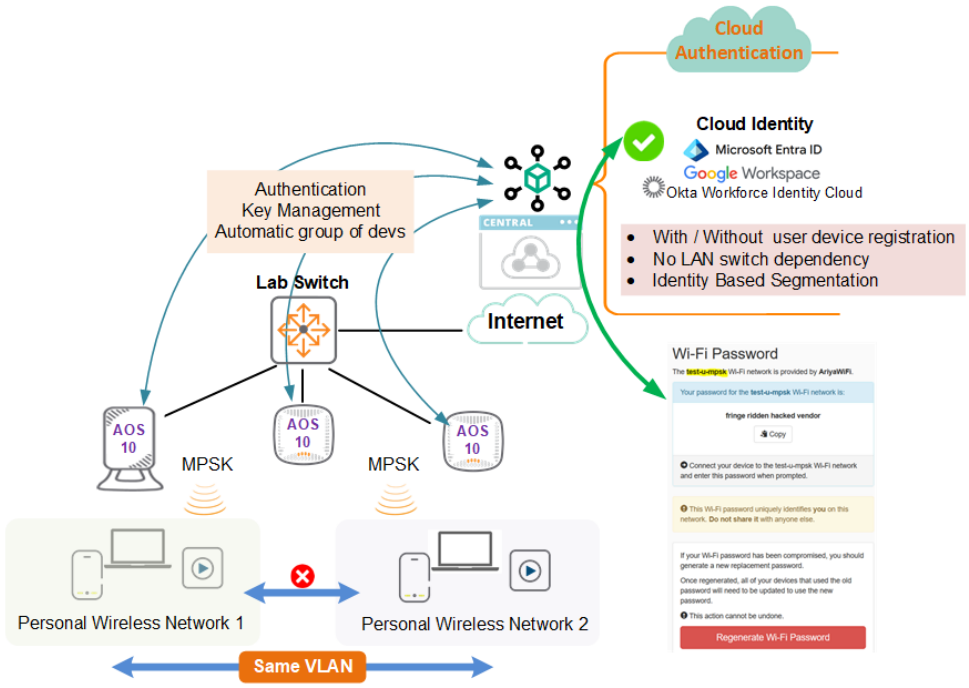
1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
30 Dec 2024	0.1	Ariya Parsamanesh	Initial creation

2 Personal Wireless Network with Aruba Central Cloud Auth

Personal Wireless Networks (PWN) are groups of user-owned Wi-Fi devices that connect and operate together in a VLAN. It’s essential to ensure that only devices within the designated group can interact in one another, along with an added ability for the device owners to permit Multicast DNS (mDNS) and Simple Service Discovery Protocol (SSDP) based services to be shared with their friends.

In this technote I’ll be demonstrating PWN solution, using Multi Pre-Shared Key (MPSK) on AOS10 APs and CloudAuth to provide user role-based policies for segmentation using an identity store. There are two parts to this solution, one is the automating the operation workflow for user device registration and the second is the access policy part to provide segmentation.



Wi-Fi Password

The test-u-mpsk Wi-Fi network is provided by AriyaWiFi.

Your password for the test-u-mpsk Wi-Fi network is:

fringe ridden hacked vendor

Connect your device to the test-u-mpsk Wi-Fi network and enter this password when prompted.

This Wi-Fi password uniquely identifies **you** on this network. **Do not share it** with anyone else.

If your Wi-Fi password has been compromised, you should generate a new replacement password.

Once regenerated, all of your devices that used the old password will need to be updated to use the new password.

This action cannot be undone.

PWN Benefits are

- Self-service portal makes it easy for users like students and faculty to onboard multiple personal devices
- You can use this solution with or without the identity stores
- It eliminates IT help desk tickets through a user-driven, SSID-based approach
- There is no dependency on LAN infrastructure

2.1 Things you need

We need the following.

- 2x APs (I am using AP-515 and AP-605H) running Aruba AOS10 10.7.x.x or later
- Aruba Central account and a few wireless clients

2.2 Assumptions

- Aruba AP is visible and online in Aruba Central and it has a valid subscription.
- Cloud Auth is configured with an identity store and connected.
- Deny Intra VLAN Traffic is not enabled as it is mutually exclusive with PWN

3 CloudAuth and Personal Wireless networks

PWN with Aruba Central is a solution that uses several features to provide the outcome and those features include

- MPSK with AOS10 APs
- Cloud Auth
- AirGroup
- User roles-based policies for North-south traffic
- VXLAN and Group Based Policy (GBP) for East-West Traffic

First you need to configure MPSK to be the authentication mode for a WLAN. Note that MPSK and MAC authentication are mutually exclusive and AOS 10.4 and above is needed to support the MPSK feature.

The unique PSKs are assigned based on two methods

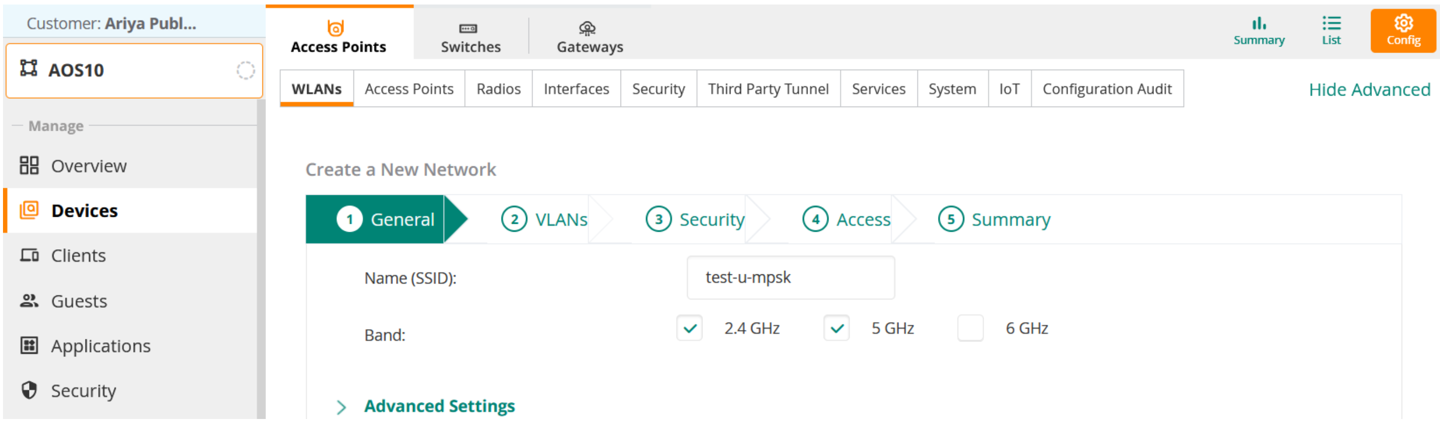
1. **Admin Managed MPSK** - This is also known as Named MPSK, in which PSKs are auto-generated when the administrator creates a named MPSK entry that can be shared with one or more users or use it to configure multiple devices without dependency on identity store. This is for the use cases where devices that may need to connect to MPSK network do not have any user identity associated
2. **User Managed MPSK** - These PSKs are specific to the user in the identity store and are auto-generated when the user signs in to the MPSK portal with their credentials. Then the users can connect multiple devices with this MPSK. So, there is a dependency on identity store.

Note that an identity provider should be configured before using the user-managed MPSK. Only the admin-managed MPSK (named MPSK) will work without configuring the identity provider which we cover it in the last technote.

We'll be covering User Managed MPSK here.

3.1 WLAN MPSK configuration

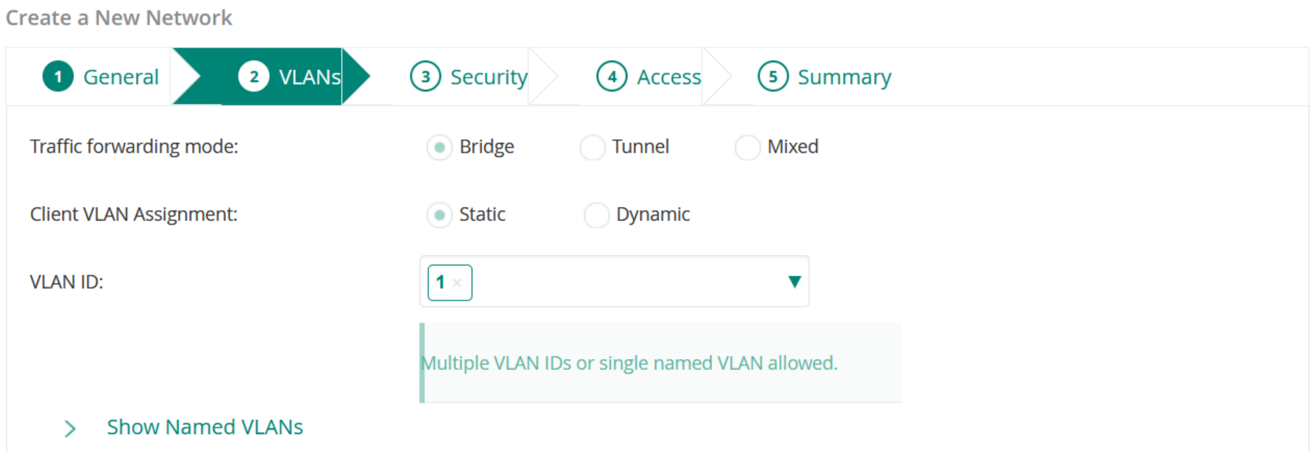
Here we'll configure "test-u-mpsk" WLAN that will be used for our demonstration.



Name (SSID): test-u-mpsk

Band: ☑ 2.4 GHz ☑ 5 GHz □ 6 GHz

Here are the details of WLAN configuration.



Create a New Network

1 General | 2 VLANs | 3 Security | 4 Access | 5 Summary

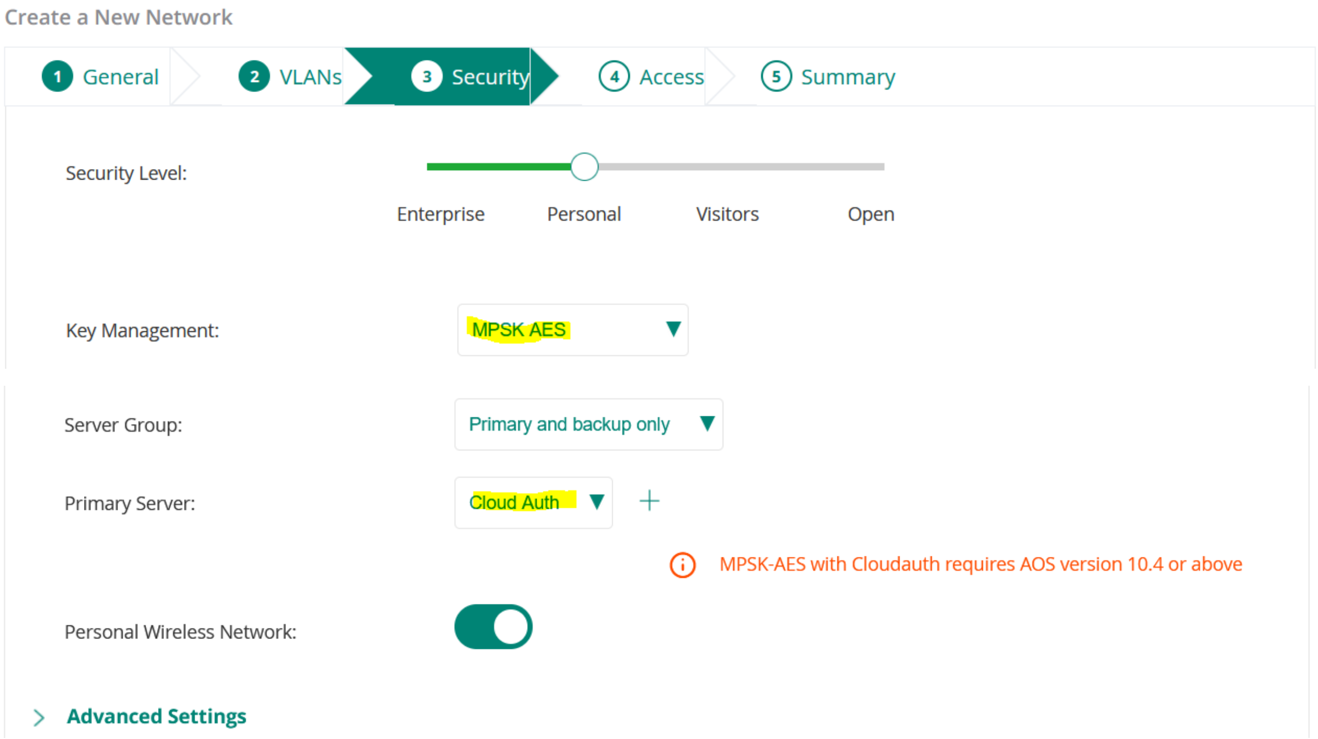
Traffic forwarding mode: ● Bridge ○ Tunnel ○ Mixed

Client VLAN Assignment: ● Static ○ Dynamic

VLAN ID: 1 ×

Multiple VLAN IDs or single named VLAN allowed.

> Show Named VLANs



Create a New Network

1 General | 2 VLANs | 3 Security | 4 Access | 5 Summary

Security Level: Enterprise | **Personal** | Visitors | Open

Key Management: MPSK AES

Server Group: Primary and backup only

Primary Server: Cloud Auth +

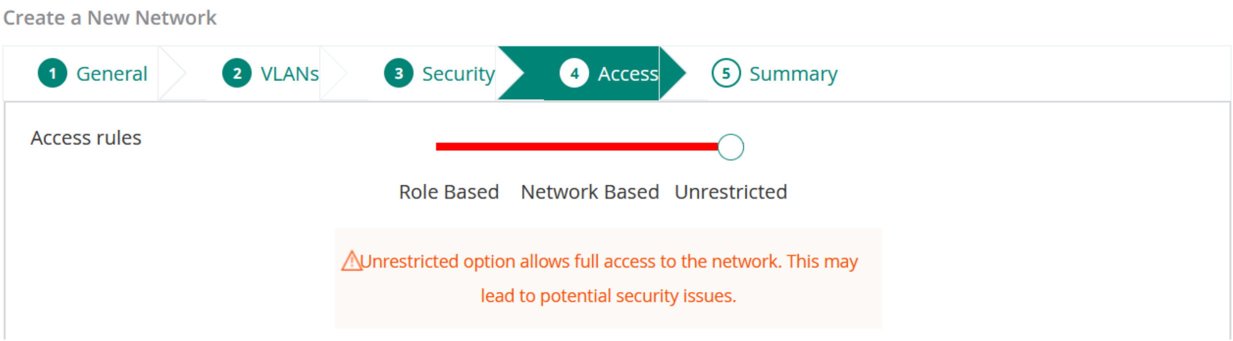
ⓘ MPSK-AES with Cloudauth requires AOS version 10.4 or above

Personal Wireless Network: ON

> **Advanced Settings**

The important thing here is that we have selected MPSK AES and Personal Wireless Network (PWN). By selecting PWN Aruba Central's Cloud auth will auto generate a Personal Area Network id (PAN-id) for each user community and shares it with the APs. Then devices with the same PAN-id can communicate together while devices with different PAN-id cannot have any access to one another. This is how the micro segmentation is achieved.

Using PWN, user's devices can roam from one AP to another while maintaining access to their devices with no risk of access of their devices to other end users. This is done using a PAN ID that is embedded into network traffic and restricts traffic to flow only between devices that belong to the same user.



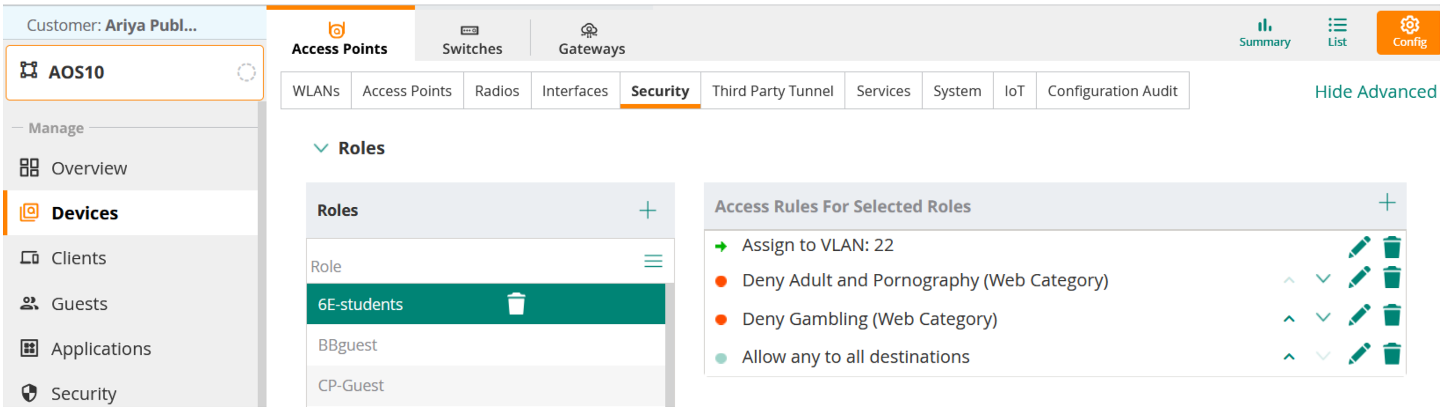
Create a New Network

1 General | 2 VLANs | 3 Security | 4 Access | 5 Summary

Access rules: Role Based | Network Based | **Unrestricted**

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

Next, we'll also configure a new user-role "6E-Student" that we'll be using for our PWN based MPSK wireless network.



Roles

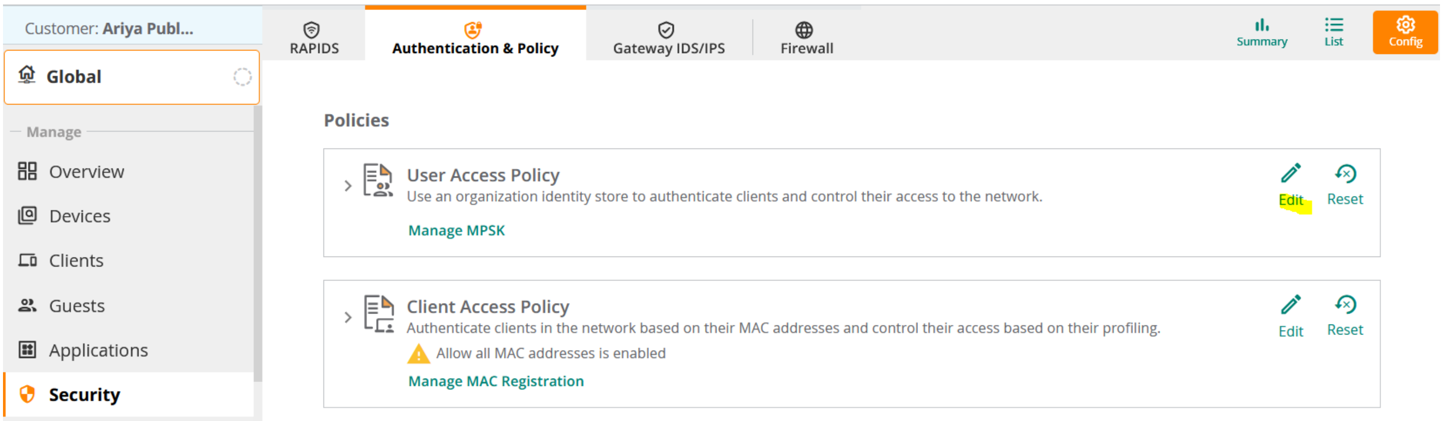
Roles
Role
6E-students
BBguest
CP-Guest

Access Rules For Selected Roles

- Assign to VLAN: 22
- Deny Adult and Pornography (Web Category)
- Deny Gambling (Web Category)
- Allow any to all destinations

3.2 Configuring the Cloud Identity

In this section we'll cover the basics of configuring a cloud identity so Aruba Central's CloudAuth can authenticate against.

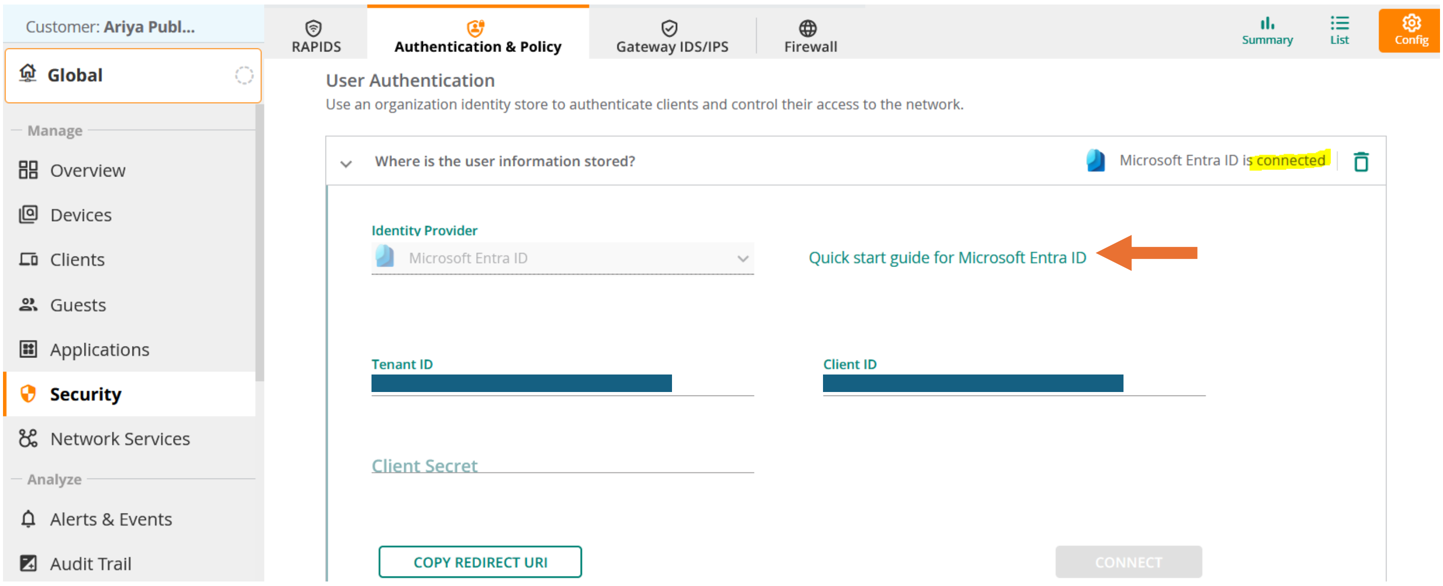


Policies

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

We are using Microsoft Entra ID and for it, you need 3x pieces of information that are shown below. For the details you can refer to the "Quick start guide for Microsoft Entra ID".



User Authentication
Use an organization identity store to authenticate clients and control their access to the network.

Where is the user information stored? Microsoft Entra ID is connected

Identity Provider: Microsoft Entra ID

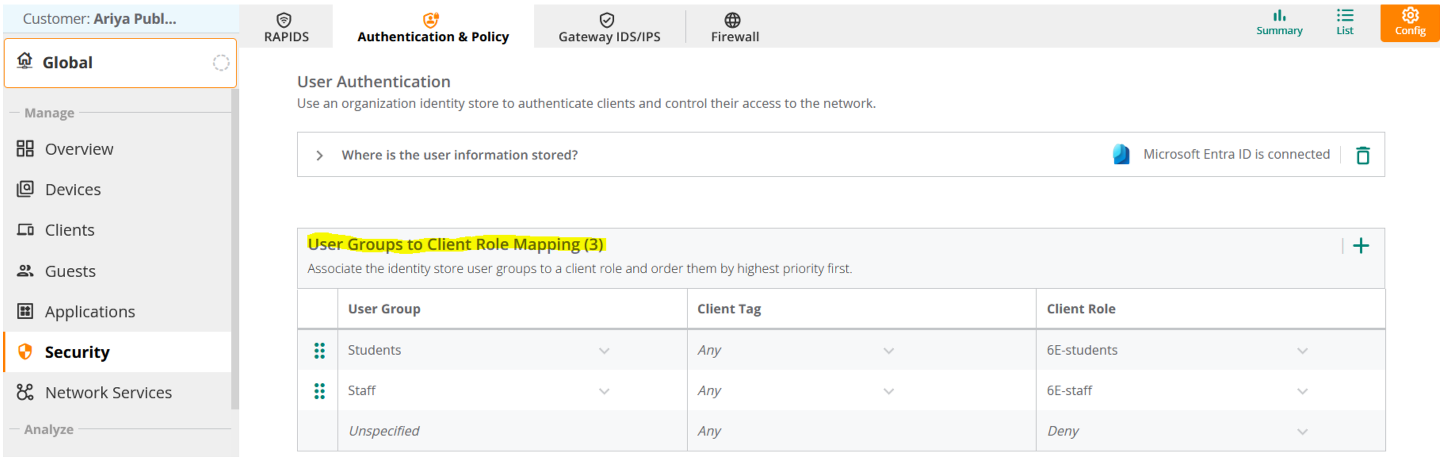
Quick start guide for Microsoft Entra ID

Tenant ID: [redacted]

Client ID: [redacted]

Client Secret

Once you have your Entra ID in “connected” state, you can start with some basic user group to client role mapping. As shown below I have 2x rules configured that maps the Entra ID group membership of the users to user roles.



User Authentication

Use an organization identity store to authenticate clients and control their access to the network.

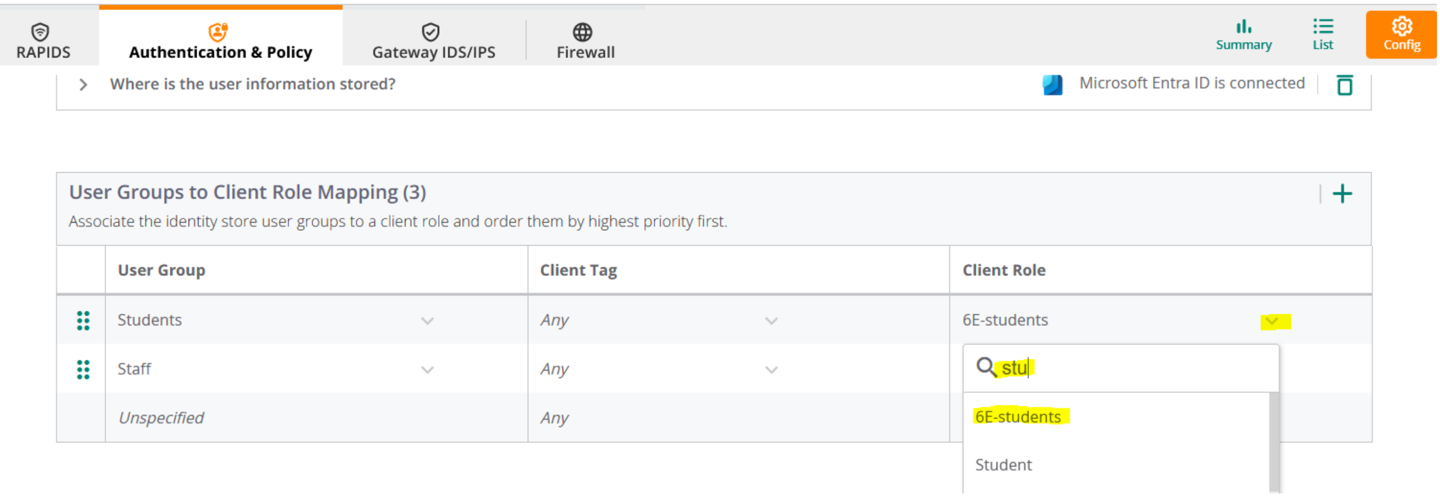
Where is the user information stored? Microsoft Entra ID is connected

User Groups to Client Role Mapping (3)

Associate the identity store user groups to a client role and order them by highest priority first.

User Group	Client Tag	Client Role
Students	Any	6E-students
Staff	Any	6E-staff
Unspecified	Any	Deny

Note that you need to configure your user roles before so you can select them from the drop-down menu.



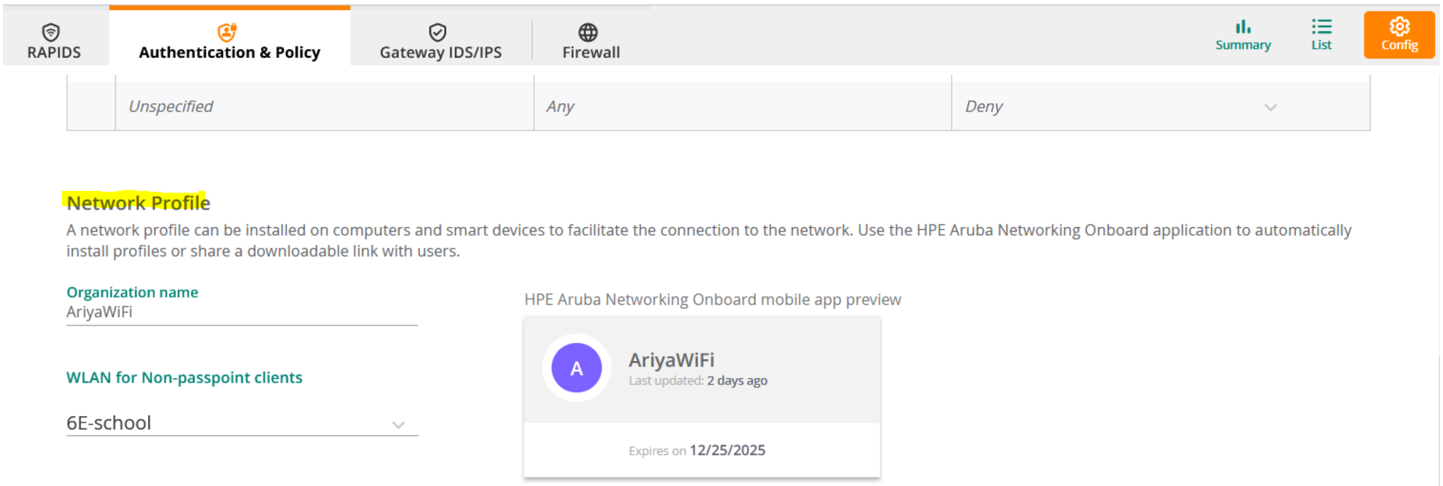
Where is the user information stored? Microsoft Entra ID is connected

User Groups to Client Role Mapping (3)

Associate the identity store user groups to a client role and order them by highest priority first.

User Group	Client Tag	Client Role
Students	Any	6E-students
Staff	Any	
Unspecified	Any	

Finally, you can configure and customise the network profiles.



Unspecified	Any	Deny

Network Profile

A network profile can be installed on computers and smart devices to facilitate the connection to the network. Use the HPE Aruba Networking Onboard application to automatically install profiles or share a downloadable link with users.

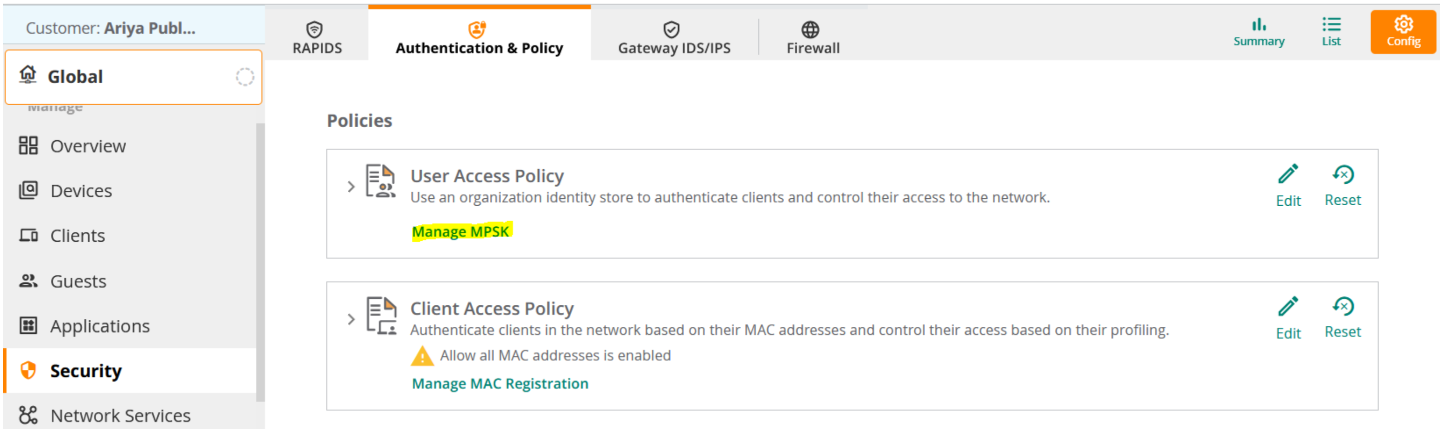
Organization name: AriyaWiFi

WLAN for Non-passpoint clients: 6E-school

HPE Aruba Networking Onboard mobile app preview

3.3 User Managed MPSK

In this section we’ll configure MPSK management for students which are in the same user roles (6E-Student), that will create their own two device communities.



User Access Policy

Use an organization identity store to authenticate clients and control their access to the network.

Manage MPSK

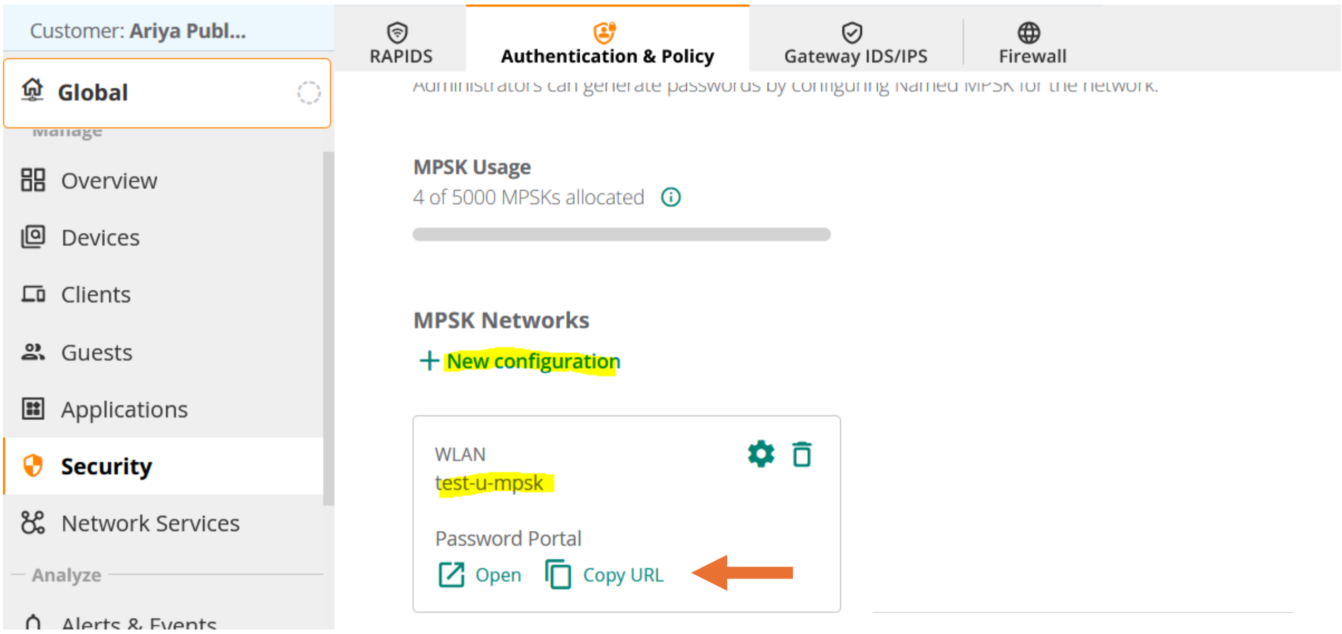
Client Access Policy

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’ll add the new WLAN that we configured.



Administrators can generate passwords by configuring Named MPSK for the network.

MPSK Usage

4 of 5000 MPSKs allocated ⓘ

MPSK Networks

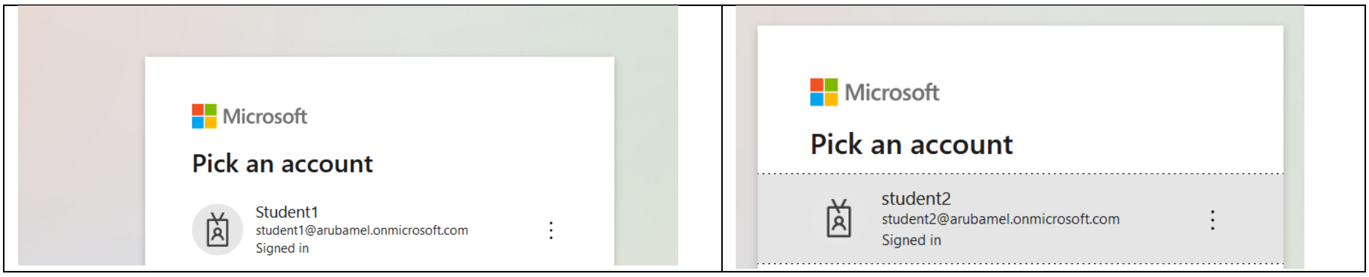
+ New configuration

WLAN: test-u-mpsk

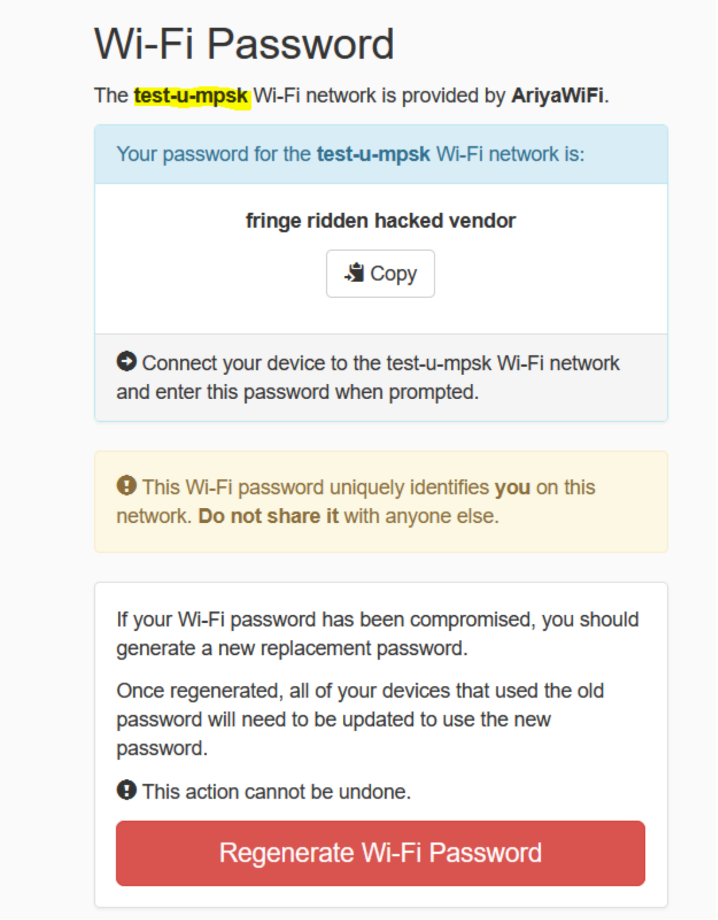
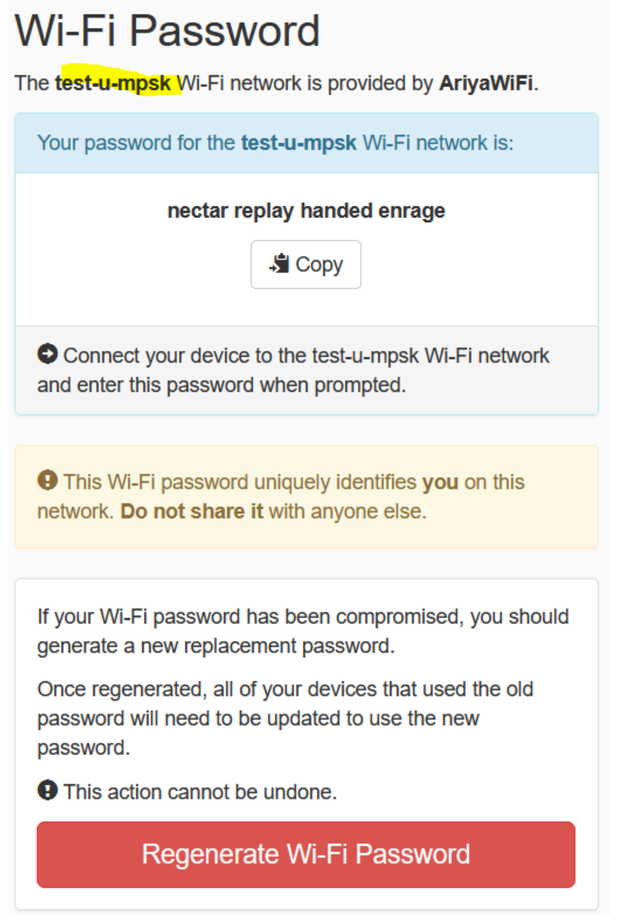
Password Portal

Now you can “copy URL” from above and send it to the user to manage their own MPSKs.

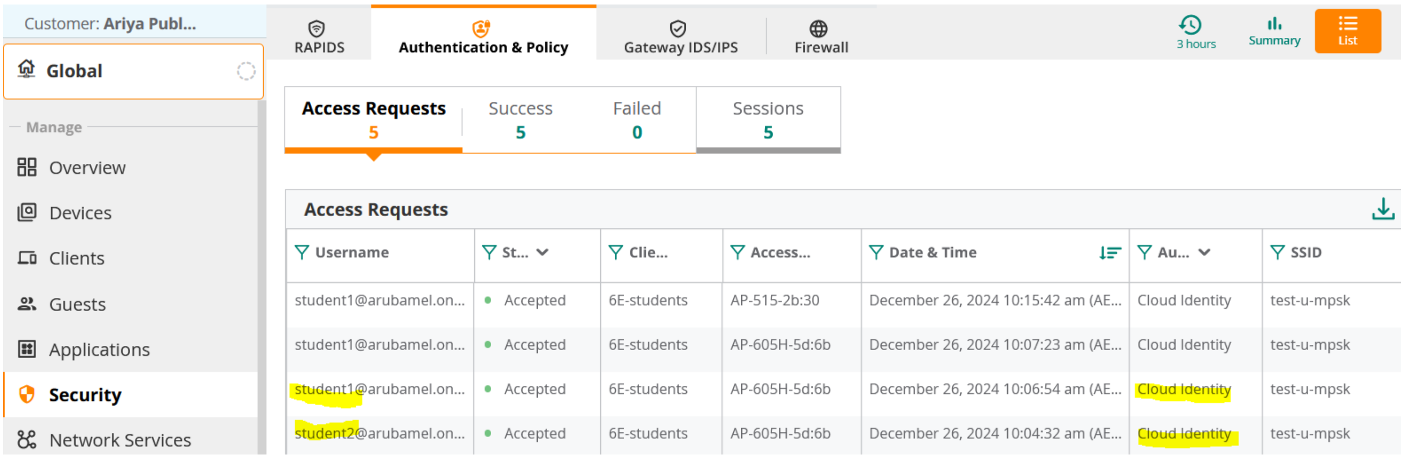
When you or the user open the Password Portal, they will get authenticated and since Entra ID enforces 2FA, they must go through that as well.



And once the students are authenticated each of them will see their own portal with different auto generated PSKs as shown below. They also can generate their own PSKs.

Student 1	Student2
	
Wi-Fi Password The **test-u-mpsk** Wi-Fi network is provided by **AriyaWiFi**. Your password for the **test-u-mpsk** Wi-Fi network is: **fringe ridden hacked vendor** Copy Connect your device to the test-u-mpsk Wi-Fi network and enter this password when prompted. This Wi-Fi password uniquely identifies **you** on this network. **Do not share it** with anyone else. If your Wi-Fi password has been compromised, you should generate a new replacement password. Once regenerated, all of your devices that used the old password will need to be updated to use the new password. This action cannot be undone. Regenerate Wi-Fi Password	Wi-Fi Password The **test-u-mpsk** Wi-Fi network is provided by **AriyaWiFi**. Your password for the **test-u-mpsk** Wi-Fi network is: **nectar replay handed enrage** Copy Connect your device to the test-u-mpsk Wi-Fi network and enter this password when prompted. This Wi-Fi password uniquely identifies **you** on this network. **Do not share it** with anyone else. If your Wi-Fi password has been compromised, you should generate a new replacement password. Once regenerated, all of your devices that used the old password will need to be updated to use the new password. This action cannot be undone. Regenerate Wi-Fi Password

The next part of the workflow is for the student1 and student2 to copy their respective passwords and use it on their device to connect to test-u-mpsk WLAN.

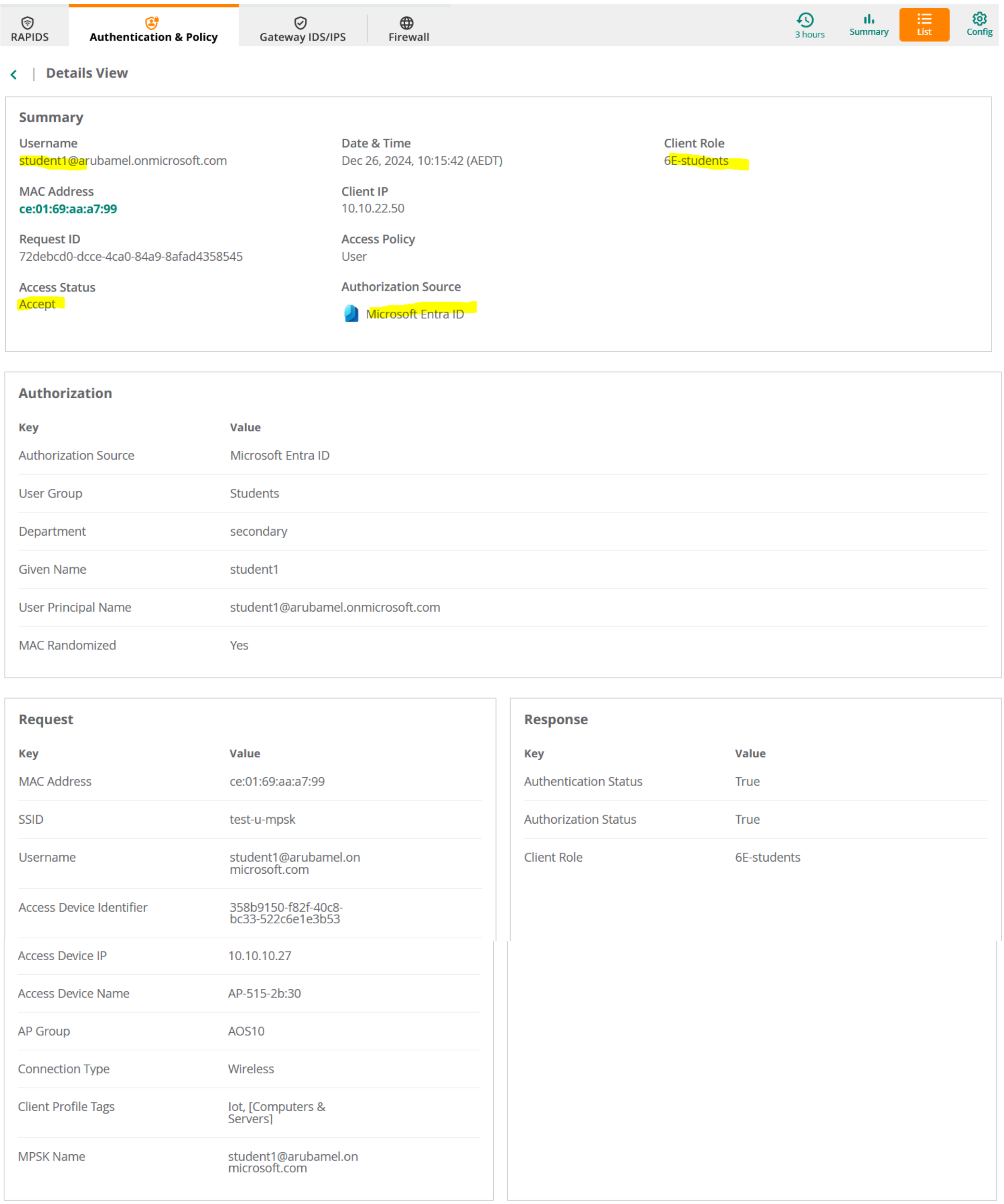


Access Requests	Success	Failed	Sessions
5	5	0	5

Access Requests

Username	St...	Clie...	Access...	Date & Time	Au...	SSID
student1@arubamel.on...	Accepted	6E-students	AP-515-2b:30	December 26, 2024 10:15:42 am (AE...	Cloud Identity	test-u-mpsk
student1@arubamel.on...	Accepted	6E-students	AP-605H-5d:6b	December 26, 2024 10:07:23 am (AE...	Cloud Identity	test-u-mpsk
student1@arubamel.on...	Accepted	6E-students	AP-605H-5d:6b	December 26, 2024 10:06:54 am (AE...	Cloud Identity	test-u-mpsk
student2@arubamel.on...	Accepted	6E-students	AP-605H-5d:6b	December 26, 2024 10:04:32 am (AE...	Cloud Identity	test-u-mpsk

We'll check the first entry for student1, just to show the various fields that are available in authentication and authorisation.



Details View

Summary

Username student1@arubamel.onmicrosoft.com	Date & Time Dec 26, 2024, 10:15:42 (AEDT)	Client Role 6E-students
MAC Address ce:01:69:aa:a7:99	Client IP 10.10.22.50	
Request ID 72debcd0-dcce-4ca0-84a9-8afad4358545	Access Policy User	
Access Status Accept	Authorization Source Microsoft Entra ID	

Authorization

Key	Value
Authorization Source	Microsoft Entra ID
User Group	Students
Department	secondary
Given Name	student1
User Principal Name	student1@arubamel.onmicrosoft.com
MAC Randomized	Yes

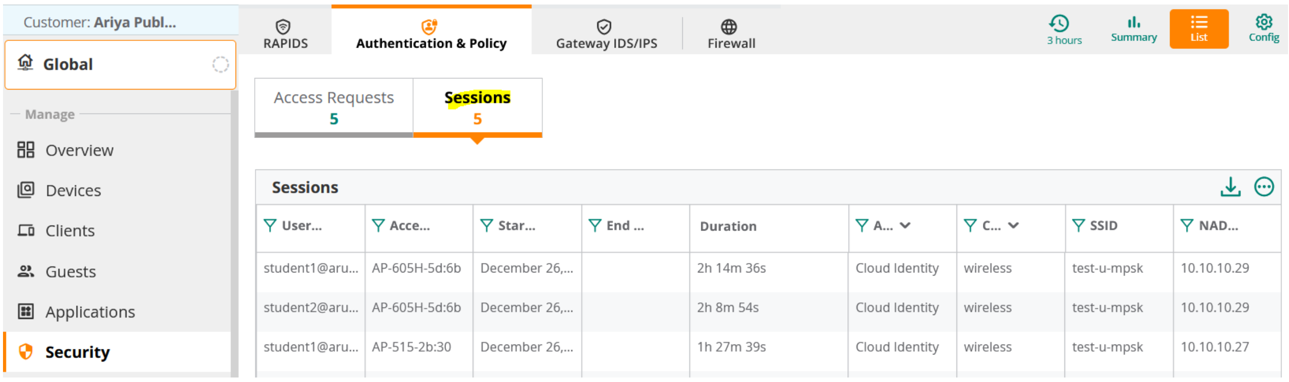
Request

Key	Value
MAC Address	ce:01:69:aa:a7:99
SSID	test-u-mpsk
Username	student1@arubamel.onmicrosoft.com
Access Device Identifier	358b9150-f82f-40c8-bc33-522c6e1e3b53
Access Device IP	10.10.10.27
Access Device Name	AP-515-2b:30
AP Group	AOS10
Connection Type	Wireless
Client Profile Tags	Iot, [Computers & Servers]
MPSK Name	student1@arubamel.onmicrosoft.com

Response

Key	Value
Authentication Status	True
Authorization Status	True
Client Role	6E-students

CloudAuth also provides session details of client devices that are connected to the APs managed by HPE Aruba Networking Central.

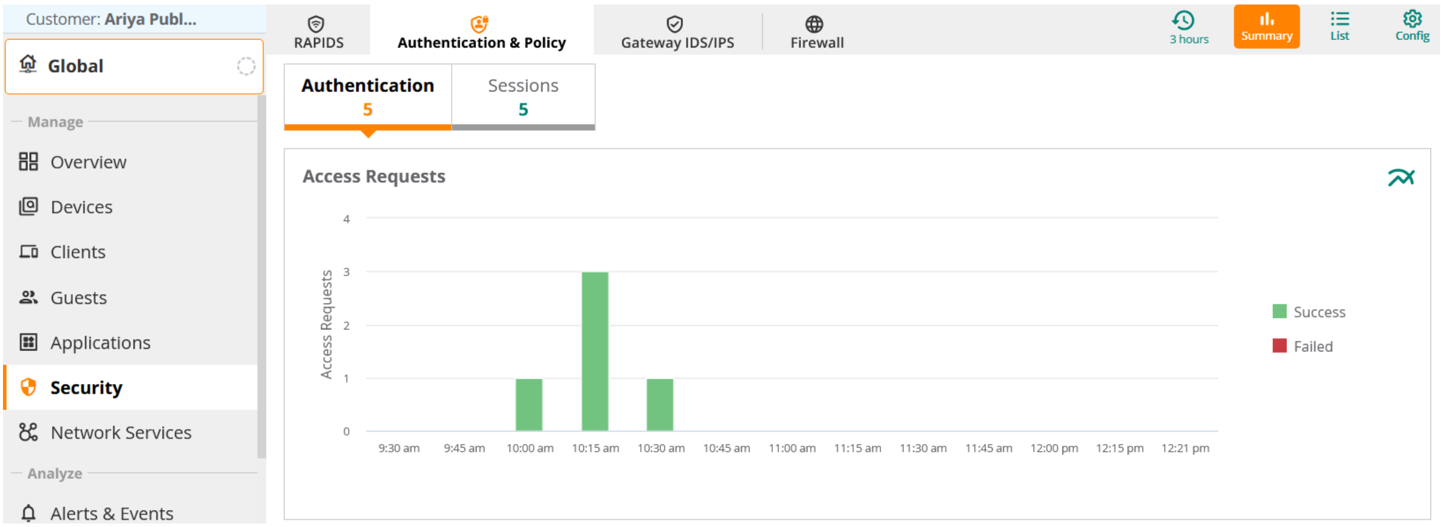


Access Requests 5 | Sessions 5

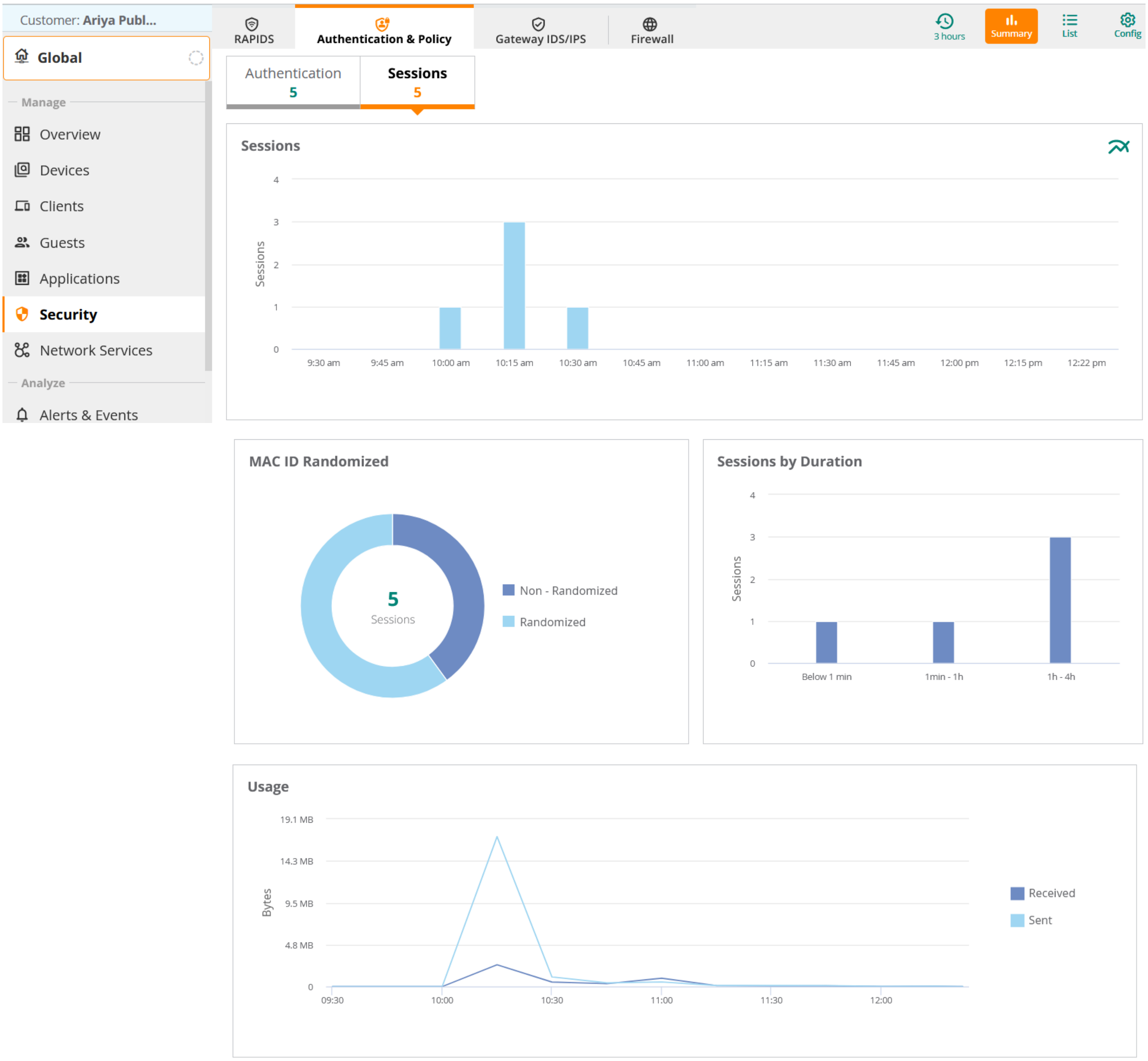
Sessions

User...	Acce...	Star...	End ...	Duration	A...	C...	SSID	NAD...
student1@aru...	AP-605H-5d:6b	December 26,...		2h 14m 36s	Cloud Identity	wireless	test-u-mpsk	10.10.10.29
student2@aru...	AP-605H-5d:6b	December 26,...		2h 8m 54s	Cloud Identity	wireless	test-u-mpsk	10.10.10.29
student1@aru...	AP-515-2b:30	December 26,...		1h 27m 39s	Cloud Identity	wireless	test-u-mpsk	10.10.10.27

You can select the summary view.

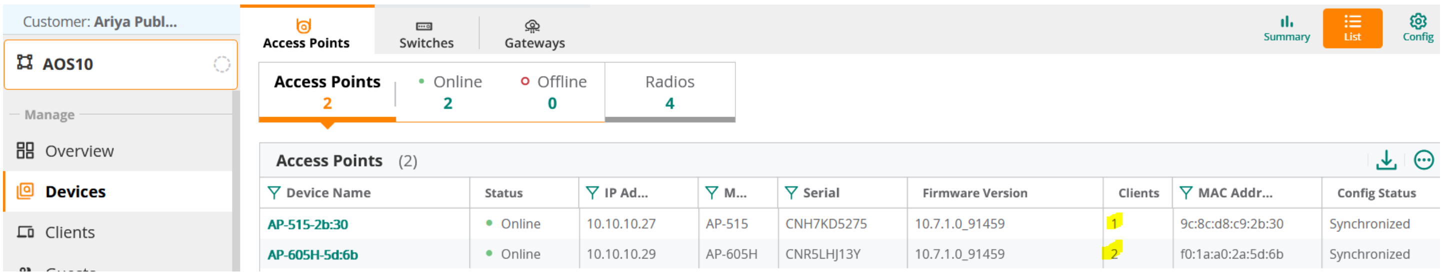


And here is the summary view of the sessions.



4 PWN Testing

We have connected two APs in the AOS10 group that are configured with “test-u-mpsk” WLAN.

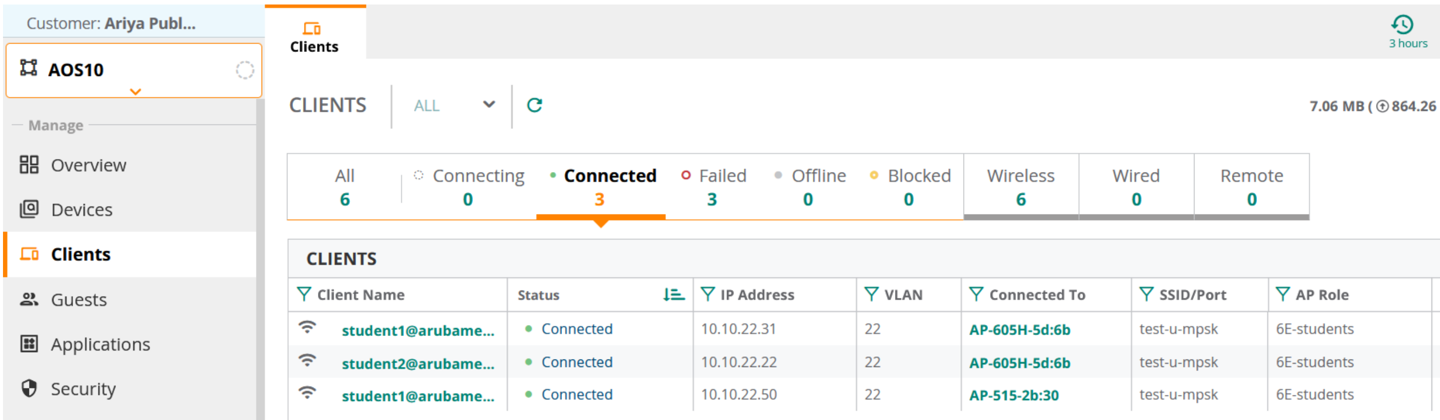


Access Points	Online	Offline	Radios
2	2	0	4

Access Points (2)

Device Name	Status	IP Ad...	M...	Serial	Firmware Version	Clients	MAC Addr...	Config Status
AP-515-2b:30	Online	10.10.10.27	AP-515	CNH7KD5275	10.7.1.0_91459	1	9c:8c:d8:c9:2b:30	Synchronized
AP-605H-5d:6b	Online	10.10.10.29	AP-605H	CNR5LHJ13Y	10.7.1.0_91459	2	f0:1a:a0:2a:5d:6b	Synchronized

We also have 3x connected clients that are connected to “test-u-mpsk” WLAN. There are 2x devices are from student1 and 1x device from student2. Note that the clients are distributed on both APs and all of them are on the same VLAN.



All	Connecting	Connected	Failed	Offline	Blocked	Wireless	Wired	Remote
6	0	3	3	0	0	6	0	0

CLIENTS

Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role
student1@arubame...	Connected	10.10.22.31	22	AP-605H-5d:6b	test-u-mpsk	6E-students
student2@arubame...	Connected	10.10.22.22	22	AP-605H-5d:6b	test-u-mpsk	6E-students
student1@arubame...	Connected	10.10.22.50	22	AP-515-2b:30	test-u-mpsk	6E-students

Here is the CLI view of the AP-605H.

```
AP-605H-5d:6b# sh clients

Client List
-----------
Name                                   IP Address    MAC Address        OS        ESSID
Access Point    Channel  Type  Role          IPv6 Address  Signal(dB)  Speed (Mbps)
----                                   ----------    -----------        --        -----
------------    -------  ----  ----          ------------  ----------  ------------
student2@arubamel.onmicrosoft.com  10.10.22.22  30:07:4d:4a:e5:66  Android  test-u-mpsk
AP-605H-5d:6b   100E     AC    6E-students  --             54(good)    780(good)
student1@arubamel.onmicrosoft.com  10.10.22.31  2c:1f:23:d0:2f:48  Apple    test-u-mpsk
AP-605H-5d:6b   100+     AN    6E-students  --             51(good)    150(good)
Number of Clients    :2
Info timestamp       :2398

AP-605H-5d:6b#
```

You can get the PAN-id from these two commands.

```
AP-605H-5d:6b# sh ap association

The phy column shows client's operational capabilities for current association

Flags: H: Hotspot(802.11u) client, K: 802.11K client, M: Mu beam formee, R: 802.11R client, W: WMM client, w:
802.11w client, V: 802.11v BSS trans capable, P: Punctured preamble, U: HE UL Mu-mimo, O: OWE client, S: SAE
client, E: Enterprise client, m: Agile Multiband client, C: Cellular Data Capable - network available, c:
Cellular Data Capable - network unavailable, T: Individual TWT client, t: Broadcast TWT client

PHY Details: HT   : High throughput;     20: 20MHz;  40: 40MHz; t: turbo-rates (256-QAM)
```

```
             VHT  : Very High throughput; 80: 80MHz; 160: 160MHz; 80p80: 80MHz + 80MHz
             HE   : High Efficiency;       80: 80MHz; 160: 160MHz; 80p80: 80MHz + 80MHz
             EHT  : Extremely High throughput;  80: 80MHz; 160: 160MHz; 80p80: 80MHz + 80MHz; 320: 320MHz
             <n>ss: <n> spatial streams

MLO Bands: Indicates the band of each link. * indicates the band where the association occurred.

Association Table
-----------------
Name           bssid              mac                auth  assoc  aid  l-int  essid        vlan-id  phy_cap
phy                 assoc. time  num assoc  Flags  DataReady  UAC      user-panid  mlo-bands
----           -----              ---                ----  -----  ---  -----  -----        -------  -------
---                 -----------  ---------  -----  ---------  ---      ----------  ---------
AP-605H-5d:6b  50:e4:e0:14:0e:51  30:07:4d:4a:e5:66  y     y      2    10     test-u-mpsk  22       5GHz-VHT-
80sgi-2ss-RVM  5GHz-VHT-80sgi-2ss  26m:31s      1          WVRM   Yes        0.0.0.0  11080503    -
AP-605H-5d:6b  50:e4:e0:14:0e:51  2c:1f:23:d0:2f:48  y     y      1    20     test-u-mpsk  22       5GHz-HT-
40sgi-1ss-R     5GHz-HT-40sgi-1ss   32m:15s      1          WR     Yes        0.0.0.0  15986759    -
Num Clients:2

AP-605H-5d:6b#
```

Here you'll see the mpskcache that Aruba Central sent to the APs.

```
AP-605H-5d:6b# sh ap mpskcache

PPSK Cache Table
----------------
Client MAC          Key                          Del  Expiry  Role          VLAN  ESSID
Seqno  IP
----------          ---                          ---  ------  ----          ----  -----
-----  --
30:07:4d:4a:e5:66  (6): 5b 77 be 16 fe 7b ...  No   -       6E-students   22    test-u-
mpsk  1186   10.10.22.22
2c:1f:23:d0:2f:48  (6): 4d 4f da df 8f cf ...  No   -       6E-students   22    test-u-
mpsk  1182   10.10.22.31
PPSK Cache Count:3

AP-605H-5d:6b#
```

This is the mpskcasche for student1's device

```
AP-605H-5d:6b# sh ap mpskcache 2c:1f:23:d0:2f:48

Station MAC address          :2c:1f:23:d0:2f:48
Seq no                       :1182
Key                          :(6): 4d 4f da df 8f cf
ESSID                        :test-u-mpsk
Name                         :student1@arubamel.onmicrosoft.com
Role                         :6E-students
Server                       :Not set
VLAN                         :22
To Del                       :No
Expire                       :-
Vlanhow                      :254
Rolehow                      :0
ACL Rule Index               :RADIUS-7ffe
User panid                   :15986759
Session timeout              :28800
---:

AP-605H-5d:6b#
```

And this is for student2's device.

```
AP-605H-5d:6b# sh ap mpskcache 30:07:4d:4a:e5:66

Station MAC address          :30:07:4d:4a:e5:66
Seq no                       :1186
```

```
Key                           :(6): 5b 77 be 16 fe 7b
ESSID                         :test-u-mpsk
Name                          :student2@arubamel.onmicrosoft.com
Role                          :6E-students
Server                        :Not set
VLAN                          :22
To Del                        :No
Expire                        :-
Vlanhow                       :254
Rolehow                       :0
ACL Rule Index                :RADIUS-7ffe
User panid                    :11080503
Session timeout               :28800
---:

AP-605H-5d:6b#
```

Now I'll check the other AP (AP-515), and we see that the PAN id is the same since they are the devices of the same user studnet1.

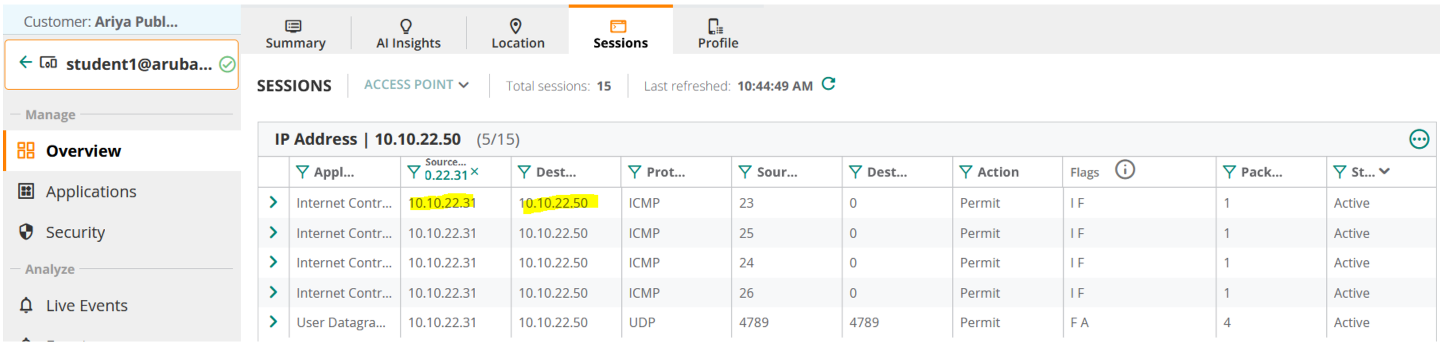
```
AP-515-2b:30# sh clients

Client List
-----------
Name                                 IP Address   MAC Address        OS      ESSID
Access Point  Channel  Type  Role           IPv6 Address  Signal(dB)  Speed (Mbps)
----                                 ----------   -----------        --      -----          -
-----------  -------  ----  ----          ------------  ----------  ------------
student1@arubamel.onmicrosoft.com  10.10.22.50  ce:01:69:aa:a7:99  Win 10  test-u-mpsk
AP-515-2b:30  36E      AC    6E-students  --            45(good)    585(good)
Number of Clients    :1
Info timestamp       :1664

AP-515-2b:30#  sh ap mpskcache  ce:01:69:aa:a7:99

Station MAC address           :ce:01:69:aa:a7:99
Seq no                        :1067
Key                           :(6): 4d 4f da df 8f cf
ESSID                         :test-u-mpsk
Name                          :student1@arubamel.onmicrosoft.com
Role                          :6E-students
Server                        :Not set
VLAN                          :22
To Del                        :No
Expire                        :-
Vlanhow                       :254
Rolehow                       :0
ACL Rule Index                :RADIUS-7ffe
User panid                    :15986759
Session timeout               :28800
---:

AP-515-2b:30#
```

The breakdown of the clients are as follows and all are on the same VLAN/IP subnet.

Username	Clients	MAC address	IP address	User Pan id	AP-name
student-1	iPod	2c:1f:23:d0:2f:48	10.10.22.31	15986759	AP-605H-5d:6b
	Win10	5c:51:4f:e6:a9:83	10.10.22.50	15986759	AP-515-2b:30
student-2	Android	30:07:4d:4a:e5:66	10.10.22.22	11080503	AP-605H-5d:6b

4.1 Microsegmentation Testing

Now we'll ping between the student-1's devices, note that they are associated to different APs. The ping test is successful. You can see here that the ICMP traffic is permitted.



SESSIONS ACCESS POINT Total sessions: 15 Last refreshed: 10:44:49 AM

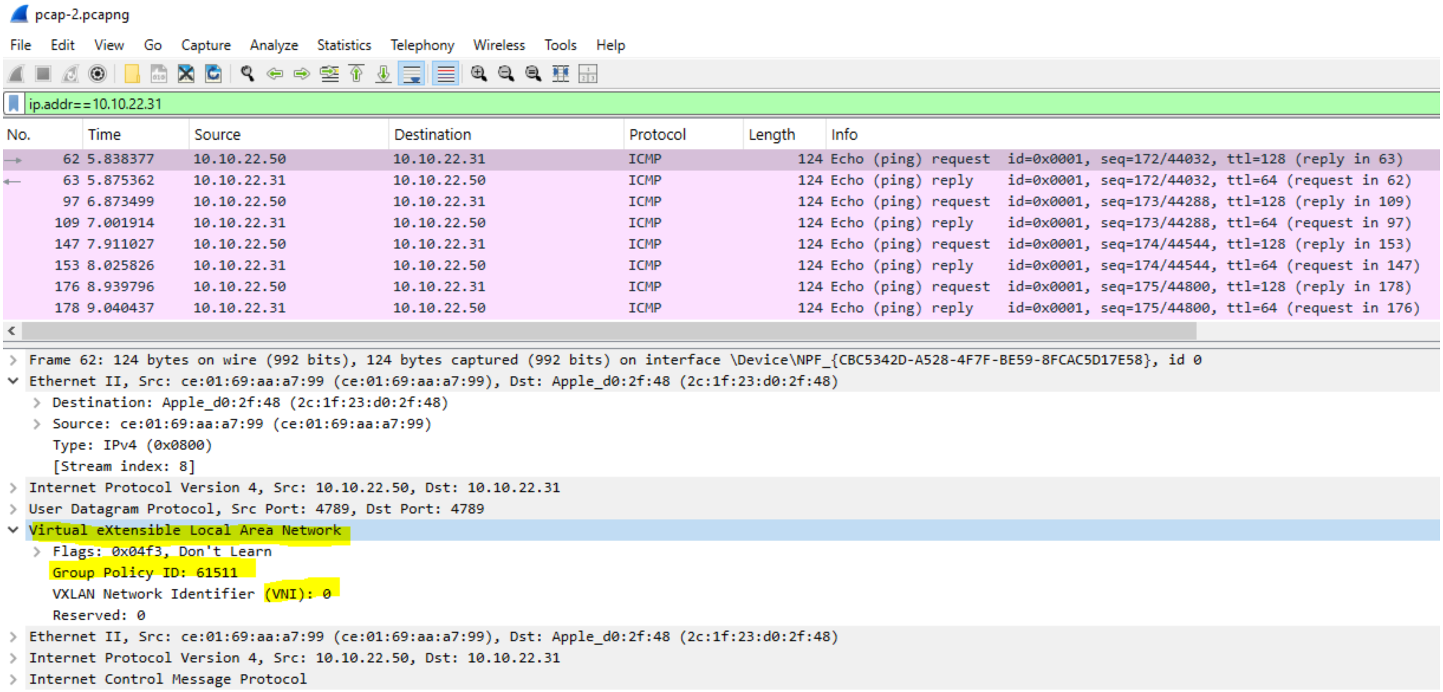
IP Address | 10.10.22.50 (5/15)

Appl...	Source... 0.22.31	Dest...	Prot...	Sour...	Dest...	Action	Flags	Pack...	St...
Internet Contr...	10.10.22.31	10.10.22.50	ICMP	23	0	Permit	I F	1	Active
Internet Contr...	10.10.22.31	10.10.22.50	ICMP	25	0	Permit	I F	1	Active
Internet Contr...	10.10.22.31	10.10.22.50	ICMP	24	0	Permit	I F	1	Active
Internet Contr...	10.10.22.31	10.10.22.50	ICMP	26	0	Permit	I F	1	Active
User Datagra...	10.10.22.31	10.10.22.50	UDP	4789	4789	Permit	F A	4	Active

Because the student-1's devices are on different APs, under the hood, the APs will make a tunnel encapsulation for this traffic. Here is the datapath session table when we were pinging between 10.10.22.50 and .31

```
AP-605H-5d:6b# sh datapath session | incl 10.10.22.31

Datapath Session Table Entries

------------------------------
Flags: A - Application Firewall Inspect
       C - client, D - deny, E - Media Deep Inspect
       F - fast age, G - media signal, H - high prio
       I - Deep inspect, L - ALG session, M - mirror, N - dest NAT
       O - Session is programmed through SDN/Openflow controller
       P - set prio, R - redirect, S - src NAT,
       T - set ToS, U - Locally destined, V - VOIP
       X - Http/https redirect for dpi denied session
       Y - no syn
       a - rtp analysis, h - Https redirect error page
       i - in offload flow, m - media mon
       p - Session is marked as permanent
       s - media signal
       d - DPI cache hit
       f - FIB init pending in session
       c - MSCS or SCS session
RAP Flags: 0 - Q0, 1 - Q1, 2 - Q2, r - redirect to conductor
           t - time based, i - in flow, l - local redirect
Flow Offload Denylist Flags: O - Openflow, E - Default, U - User os unknown, T - Tunnel
                              R - L3 route

10.10.22.50       10.10.22.31     1    27    2048  0    0    0   0   tunnel 1    1a   1   3c    FCI
10.10.22.50       10.10.22.31     1    29    2048  0    0    0   0   tunnel 1    5    1   3c    FCI
10.10.22.50       10.10.22.31     1    28    2048  0    0    0   0   tunnel 1    f    1   3c    FCI
17.57.145.37      10.10.22.31     6    443   51980 0    0    0   3   dev32       7138 16  13c9  i
10.10.22.31       10.10.22.50     1    29    0     0    0    0   0   tunnel 1    5    1   3c    FRI
10.10.22.31       10.10.22.50     1    28    0     0    0    0   0   tunnel 1    f    1   3c    FRI
10.10.22.31       10.10.22.50     1    27    0     0    0    0   1   tunnel 1    1a   1   3c    FRI
10.10.22.31       10.10.22.50     17   4789  4789  0    0    0   0   dev6        1a   3   14a   FA
10.10.22.50       10.10.22.31     17   4789  4789  0    0    0   0   dev6        1a   3   14a   FCA
10.10.22.31       17.57.145.37    6    51980 443   0    0    0   2   dev32       7138 1a  10b6  Ci

AP-605H-5d:6b#
```

I did a packet capture on the switch to see the ICMP ping traffic between the two devices for student-1 that are on different APs. You'll see that there is, indeed an UDP encapsulation between the two APs the port that is used is VXLAN, it also carries the VNI=0 and group Policy ID that is automatically generated and assigned.

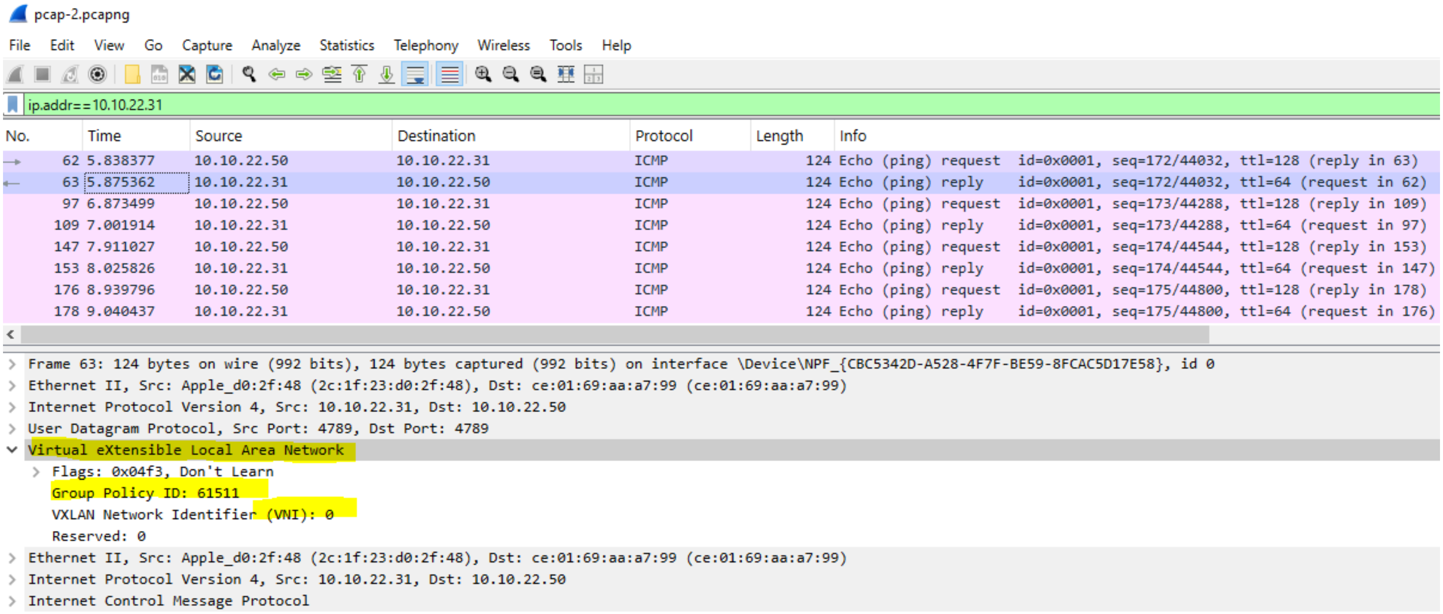

pcap-2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr==10.10.22.31
```

```
No.   Time      Source        Destination   Protocol Length Info
   62 5.838377  10.10.22.50   10.10.22.31   ICMP        124 Echo (ping) request  id=0x0001, seq=172/44032, ttl=128 (reply in 63)
   63 5.875362  10.10.22.31   10.10.22.50   ICMP        124 Echo (ping) reply    id=0x0001, seq=172/44032, ttl=64 (request in 62)
   97 6.873499  10.10.22.50   10.10.22.31   ICMP        124 Echo (ping) request  id=0x0001, seq=173/44288, ttl=128 (reply in 109)
  109 7.001914  10.10.22.31   10.10.22.50   ICMP        124 Echo (ping) reply    id=0x0001, seq=173/44288, ttl=64 (request in 97)
  147 7.911027  10.10.22.50   10.10.22.31   ICMP        124 Echo (ping) request  id=0x0001, seq=174/44544, ttl=128 (reply in 153)
  153 8.025826  10.10.22.31   10.10.22.50   ICMP        124 Echo (ping) reply    id=0x0001, seq=174/44544, ttl=64 (request in 147)
  176 8.939796  10.10.22.50   10.10.22.31   ICMP        124 Echo (ping) request  id=0x0001, seq=175/44800, ttl=128 (reply in 178)
  178 9.040437  10.10.22.31   10.10.22.50   ICMP        124 Echo (ping) reply    id=0x0001, seq=175/44800, ttl=64 (request in 176)
```

```
> Frame 62: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface \Device\NPF_{CBC5342D-A528-4F7F-BE59-8FCAC5D17E58}, id 0
v Ethernet II, Src: ce:01:69:aa:a7:99 (ce:01:69:aa:a7:99), Dst: Apple_d0:2f:48 (2c:1f:23:d0:2f:48)
    > Destination: Apple_d0:2f:48 (2c:1f:23:d0:2f:48)
    > Source: ce:01:69:aa:a7:99 (ce:01:69:aa:a7:99)
      Type: IPv4 (0x0800)
      [Stream index: 8]
> Internet Protocol Version 4, Src: 10.10.22.50, Dst: 10.10.22.31
> User Datagram Protocol, Src Port: 4789, Dst Port: 4789
v Virtual eXtensible Local Area Network
    > Flags: 0x04f3, Don't Learn
      Group Policy ID: 61511
      VXLAN Network Identifier (VNI): 0
      Reserved: 0
> Ethernet II, Src: ce:01:69:aa:a7:99 (ce:01:69:aa:a7:99), Dst: Apple_d0:2f:48 (2c:1f:23:d0:2f:48)
> Internet Protocol Version 4, Src: 10.10.22.50, Dst: 10.10.22.31
> Internet Control Message Protocol
```

And this is the return traffic and note that the group policy Id are the same and hence the traffic is allowed.


pcap-2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

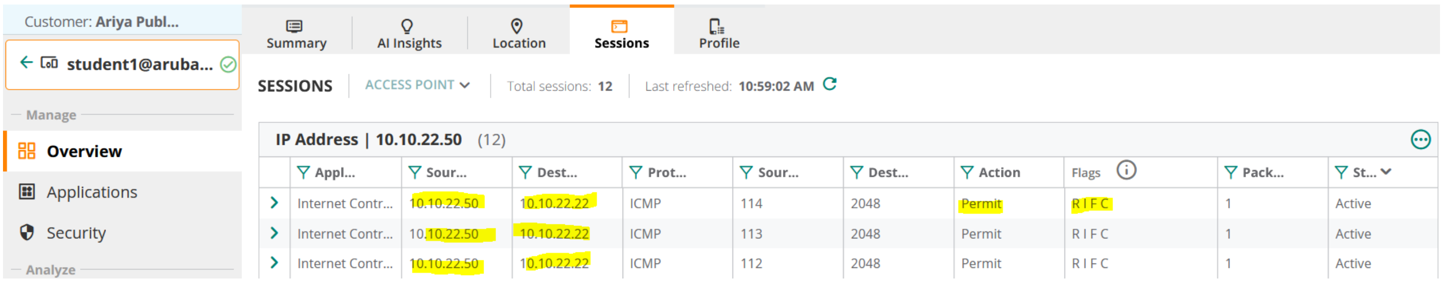
```
ip.addr==10.10.22.31
```

```
No.   Time      Source        Destination   Protocol Length Info
   62 5.838377  10.10.22.50   10.10.22.31   ICMP        124 Echo (ping) request  id=0x0001, seq=172/44032, ttl=128 (reply in 63)
   63 5.875362  10.10.22.31   10.10.22.50   ICMP        124 Echo (ping) reply    id=0x0001, seq=172/44032, ttl=64 (request in 62)
   97 6.873499  10.10.22.50   10.10.22.31   ICMP        124 Echo (ping) request  id=0x0001, seq=173/44288, ttl=128 (reply in 109)
  109 7.001914  10.10.22.31   10.10.22.50   ICMP        124 Echo (ping) reply    id=0x0001, seq=173/44288, ttl=64 (request in 97)
  147 7.911027  10.10.22.50   10.10.22.31   ICMP        124 Echo (ping) request  id=0x0001, seq=174/44544, ttl=128 (reply in 153)
  153 8.025826  10.10.22.31   10.10.22.50   ICMP        124 Echo (ping) reply    id=0x0001, seq=174/44544, ttl=64 (request in 147)
  176 8.939796  10.10.22.50   10.10.22.31   ICMP        124 Echo (ping) request  id=0x0001, seq=175/44800, ttl=128 (reply in 178)
  178 9.040437  10.10.22.31   10.10.22.50   ICMP        124 Echo (ping) reply    id=0x0001, seq=175/44800, ttl=64 (request in 176)
```

```
> Frame 63: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface \Device\NPF_{CBC5342D-A528-4F7F-BE59-8FCAC5D17E58}, id 0
> Ethernet II, Src: Apple_d0:2f:48 (2c:1f:23:d0:2f:48), Dst: ce:01:69:aa:a7:99 (ce:01:69:aa:a7:99)
> Internet Protocol Version 4, Src: 10.10.22.31, Dst: 10.10.22.50
> User Datagram Protocol, Src Port: 4789, Dst Port: 4789
v Virtual eXtensible Local Area Network
    > Flags: 0x04f3, Don't Learn
      Group Policy ID: 61511
      VXLAN Network Identifier (VNI): 0
      Reserved: 0
> Ethernet II, Src: Apple_d0:2f:48 (2c:1f:23:d0:2f:48), Dst: ce:01:69:aa:a7:99 (ce:01:69:aa:a7:99)
> Internet Protocol Version 4, Src: 10.10.22.31, Dst: 10.10.22.50
> Internet Control Message Protocol
```

Next test is to ping from student-1's win10 device to student-2's devices that are on different APs. The ping is unsuccessful, and it gets denied on the destination AP since the PAN-ids don't match.

Below is the screenshot for studnet1's win10 device.

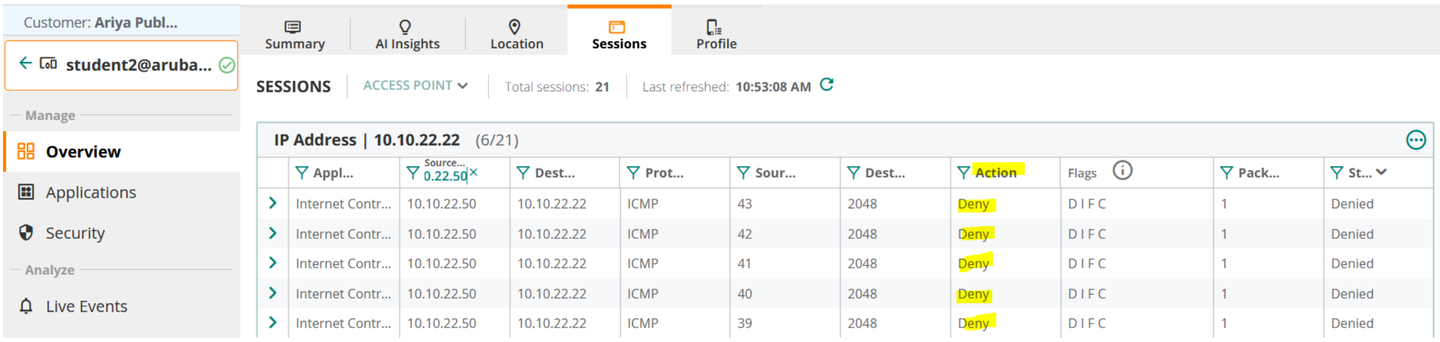


Total sessions: 12 Last refreshed: 10:59:02 AM

IP Address | 10.10.22.50 (12)

	Appl...	Sour...	Dest...	Prot...	Sour...	Dest...	Action	Flags	Pack...	St...
>	Internet Contr...	10.10.22.50	10.10.22.22	ICMP	114	2048	Permit	R I F C	1	Active
>	Internet Contr...	10.10.22.50	10.10.22.22	ICMP	113	2048	Permit	R I F C	1	Active
>	Internet Contr...	10.10.22.50	10.10.22.22	ICMP	112	2048	Permit	R I F C	1	Active

Note that the below screenshot is from the destination client (Student2) which is on a different AP.

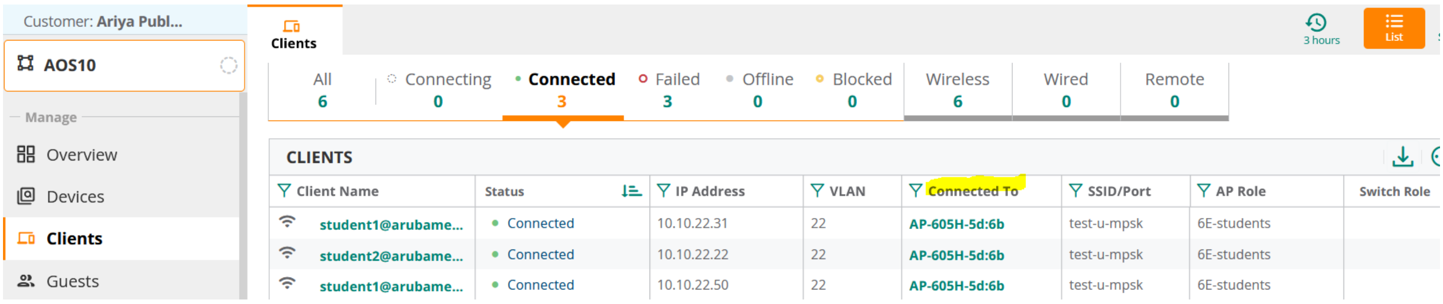


Total sessions: 21 Last refreshed: 10:53:08 AM

IP Address | 10.10.22.22 (6/21)

	Appl...	Source... 0.22.50	Dest...	Prot...	Sour...	Dest...	Action	Flags	Pack...	St...
>	Internet Contr...	10.10.22.50	10.10.22.22	ICMP	43	2048	Deny	D I F C	1	Denied
>	Internet Contr...	10.10.22.50	10.10.22.22	ICMP	42	2048	Deny	D I F C	1	Denied
>	Internet Contr...	10.10.22.50	10.10.22.22	ICMP	41	2048	Deny	D I F C	1	Denied
>	Internet Contr...	10.10.22.50	10.10.22.22	ICMP	40	2048	Deny	D I F C	1	Denied
>	Internet Contr...	10.10.22.50	10.10.22.22	ICMP	39	2048	Deny	D I F C	1	Denied

Our final test is to ping between student-1 and student-2's devices that are on the same AP. Here AP-515 is disconnected, and we see here tat all the clients are on the same AP.



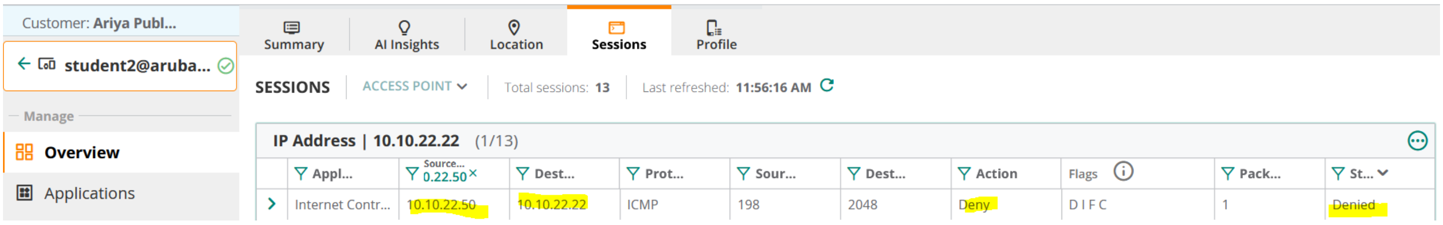
All	Connecting	Connected	Failed	Offline	Blocked	Wireless	Wired	Remote
6	0	3	3	0	0	6	0	0

CLIENTS

Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role	Switch Role
student1@arubame...	Connected	10.10.22.31	22	AP-605H-5d:6b	test-u-mpsk	6E-students	
student2@arubame...	Connected	10.10.22.22	22	AP-605H-5d:6b	test-u-mpsk	6E-students	
student1@arubame...	Connected	10.10.22.50	22	AP-605H-5d:6b	test-u-mpsk	6E-students	

```
AP-605H-5d:6b# sh ap association

The phy column shows client's operational capabilities for current association

Flags: H: Hotspot(802.11u) client, K: 802.11K client, M: Mu beam formee, R: 802.11R client, W: WMM client, w:
802.11w client, V: 802.11v BSS trans capable, P: Punctured preamble, U: HE UL Mu-mimo, O: OWE client, S: SAE
client, E: Enterprise client, m: Agile Multiband client, C: Cellular Data Capable - network available, c:
Cellular Data Capable - network unavailable, T: Individual TWT client, t: Broadcast TWT client

PHY Details: HT   : High throughput;       20: 20MHz;  40: 40MHz; t: turbo-rates (256-QAM)
             VHT  : Very High throughput; 80: 80MHz; 160: 160MHz; 80p80: 80MHz + 80MHz
             HE   : High Efficiency;       80: 80MHz; 160: 160MHz; 80p80: 80MHz + 80MHz
             EHT  : Extremely High throughput;  80: 80MHz; 160: 160MHz; 80p80: 80MHz + 80MHz; 320: 320MHz
             <n>ss: <n> spatial streams

MLO Bands: Indicates the band of each link. * indicates the band where the association occurred.

Association Table
-----------------
Name           bssid              mac                auth  assoc  aid  l-int  essid        vlan-id  phy_cap
phy                 assoc. time  num assoc  Flags  DataReady  UAC  user-panid  mlo-bands
----           -----              ---                ----  -----  ---  -----  -----        -------  -------
---                 -----------  ---------  -----  ---------  ---  ----------  ---------
AP-605H-5d:6b  50:e4:e0:14:0e:51  30:07:4d:4a:e5:66  y     y      2    10     test-u-mpsk  22       5GHz-VHT-
80sgi-2ss-RVM  5GHz-VHT-80sgi-2ss  1h:58m:9s    1          WVRM   Yes        0.0.0.0  11080503    -
AP-605H-5d:6b  50:e4:e0:14:0e:51  2c:1f:23:d0:2f:48  y     y      1    20     test-u-mpsk  22       5GHz-HT-
40sgi-1ss-R     5GHz-HT-40sgi-1ss    2h:3m:53s    1          WR     Yes        0.0.0.0  15986759    -
AP-605H-5d:6b  50:e4:e0:14:0e:51  ce:01:69:aa:a7:99  y     y      3    250    test-u-mpsk  22       5GHz-VHT-
80sgi-2ss-KV   5GHz-VHT-80sgi-2ss  10m:2s       1          WV     Yes        0.0.0.0  15986759    -

Num Clients:3

AP-605H-5d:6b#
```

And as expected the ping test fails as the devices have different PAN-id and drop is shown on the destination client.



SESSIONS | ACCESS POINT | Total sessions: 13 | Last refreshed: 11:56:16 AM

IP Address | 10.10.22.22 (1/13)

	Appl...	Source... 0.22.50	Dest...	Prot...	Sour...	Dest...	Action	Flags	Pack...	St...
>	Internet Contr...	10.10.22.50	10.10.22.22	ICMP	198	2048	Deny	D I F C	1	Denied

When using the CLI, we should be looking for D flag (indicating drops) between 10.10.22.22 and 10.10.22.50. Note that PAN-id will not change for the users even though one might change the MPSK.

```
AP-605H-5d:6b# sh datapath session | incl 10.10.22.50

10.10.22.50      10.10.22.22     1   224   2048 0    0    0    0   dev32      12   1   3c    FDCI
10.10.22.22      10.10.22.50     1   224   0    0    0    0    0   dev32      12   0   0     FDYI
10.10.22.50      20.198.119.84   6   56012 443  0    0    0    14  dev32      8e0  b   9bb   Ci
10.10.22.50      20.198.118.190  6   56008 443  0    0    0    6   dev32      d93  e   c4b   Ci

AP-605H-5d:6b#
```

This is simple yet powerful way to enforce Microsegmentation for this specific use case.