Contents

1.1 Revision History

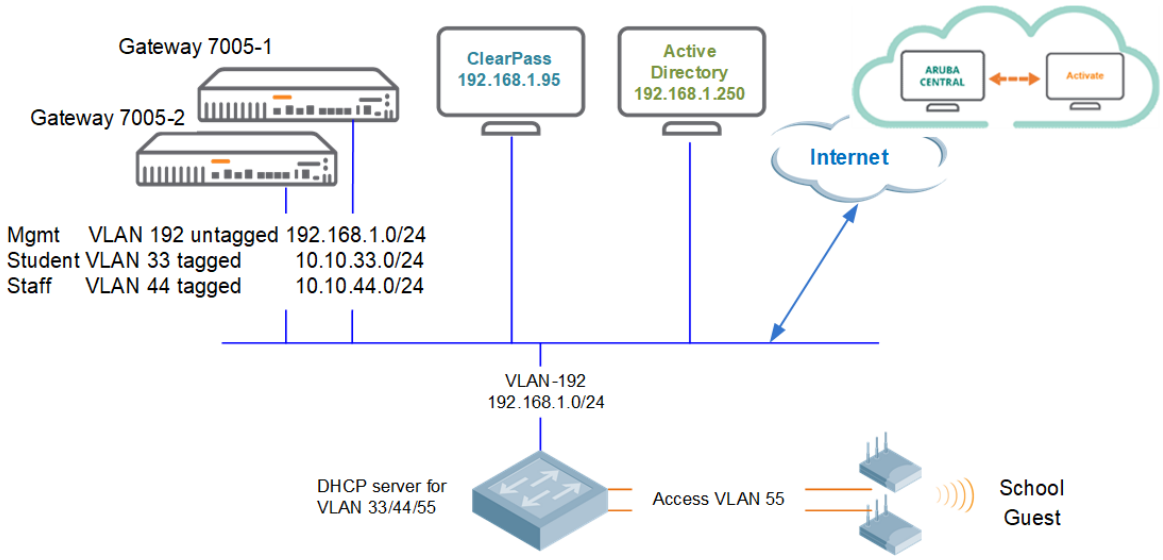
DATE	VERSION	EDITOR	CHANGES
15 Mar 2021	0.1	Ariya Parsamanesh	Initial creation
22 May 2021	0.2	Ariya Parsamanesh	Added the ClearPass guest operator login
04 Jul 2021	0.3	Ariya Parsamanesh	Added the Monitoring section

2 Demo Topology

The aim here is to provide the starting point to put together a solution that include the AOS10 APs, two gateways, ClearPass and obviously Aruba Central.

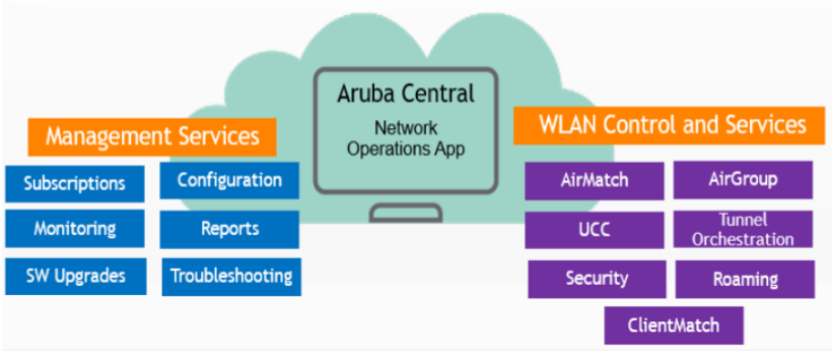
Note that APs in AOS10 support bridged, tunnelled and mix mode wireless LANs (WLAN) however in this technote we'll be deploying tunnelled mode WLANs. We'll also demonstrate the gateway clustering with AOS10.

This is type of deployment is particularly useful when all the buildings in a school/college campus have L3 IP demarcation and are routed to various part of the campus.



With AOS10, the campus architecture consists of two layers:

1. **The infrastructure layer** consists of a WLAN setup which can be either a campus setup or a branch setup. The campus setup can consist only of access points (APs) or APs combined with gateway clusters. In case of a branch setup, the infrastructure layer includes an AP. Here we have combined the Instant APs and Campus APs into just APs, and you bridge, or tunnel user traffic based on the configuration on the APs.
2. **The cloud management layer** consists of Aruba Central which is a cloud management SaaS platform. The Network Operations app is one of the Aruba apps which is a part of Aruba Central and this app helps to create the SSID profiles for the different WLAN campus and branch setups.



As you can see in the above diagram, the classic components that would normally run on mobility master or instant APs are now run as services in Aruba Central. I am talking about Airmatch, Roaming, clientmatch, etc.

Here we'll not go to the details of the architecture for that please refer to this link

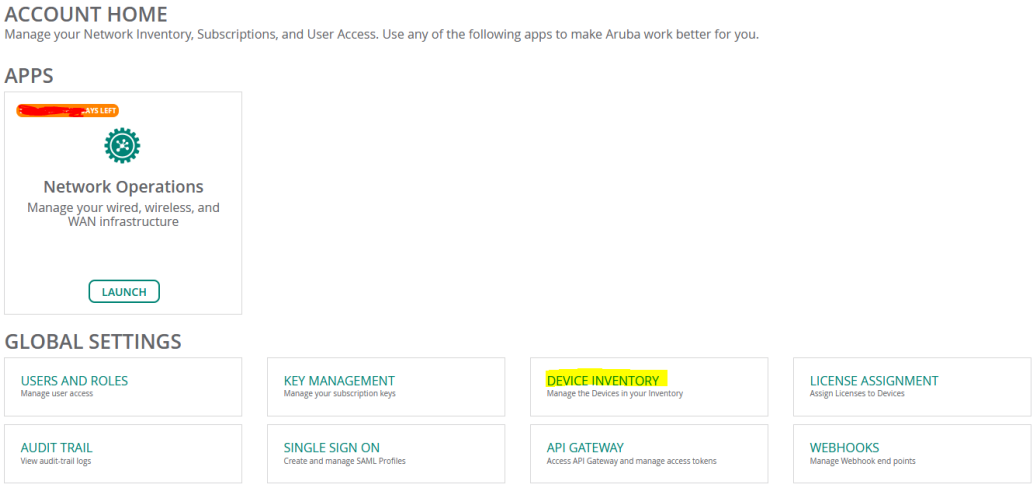
https://www.arubanetworks.com/techdocs/AOS10X_OLH/Content/overview/architecture-overview.htm

3 Aruba Central Account

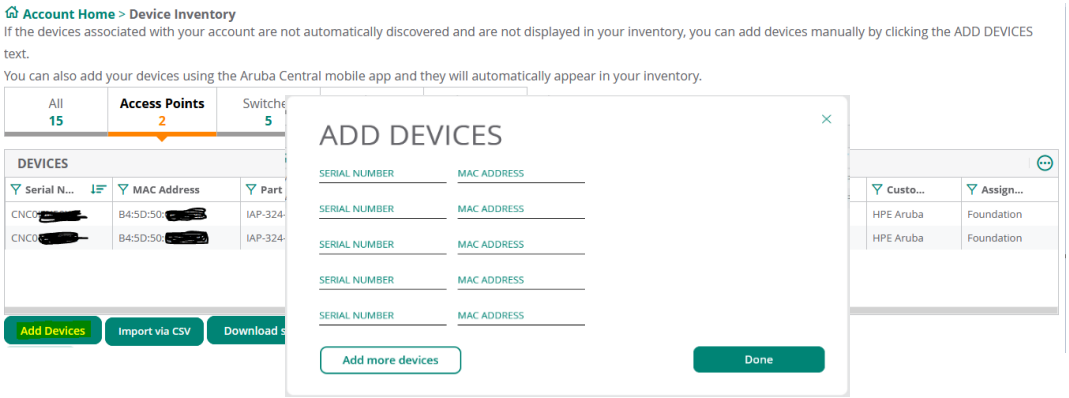
You need an Aruba Central account with appropriate licenses for APs and gateways. You can sign up for a 90 days trial from this link

https://www.arubanetworks.com/products/network-management-operations/central/eval/

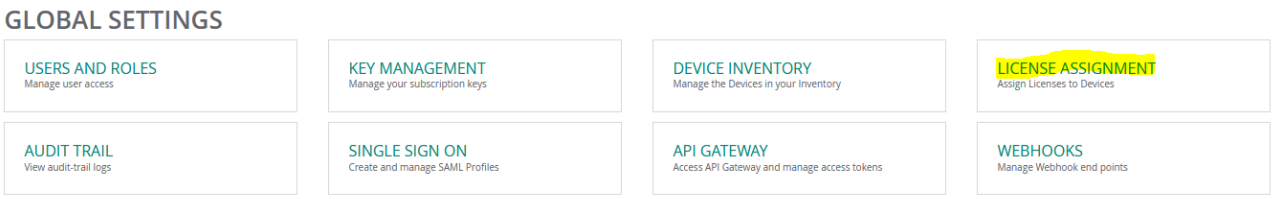
Once you login to your Central account you need to add your devices (APs and Gateways) to the device inventory

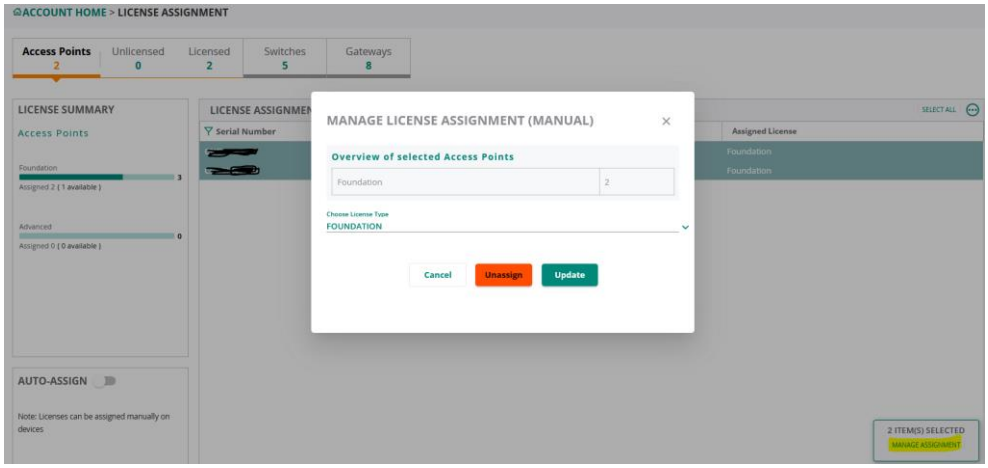


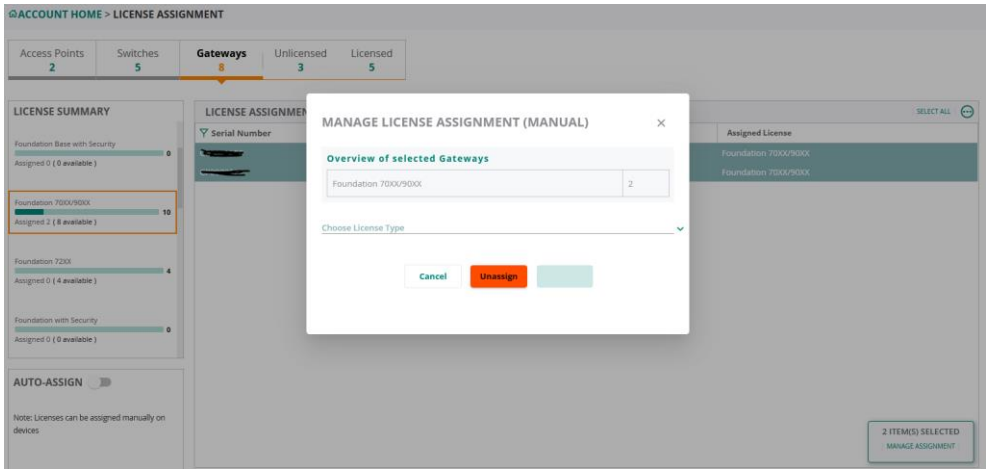
Here I have already added my APs.



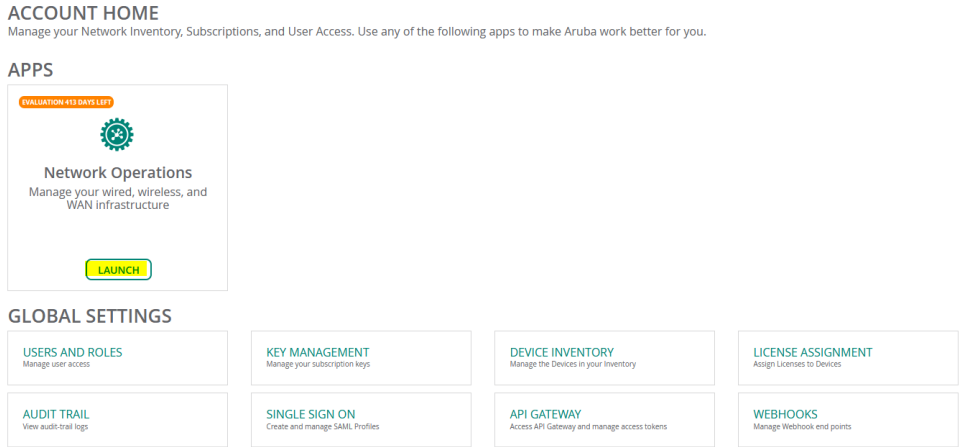
You do the same for the gateways as well. Then you need to assign the licenses to the devices, for this from Account home you need to go to “License Assignment”



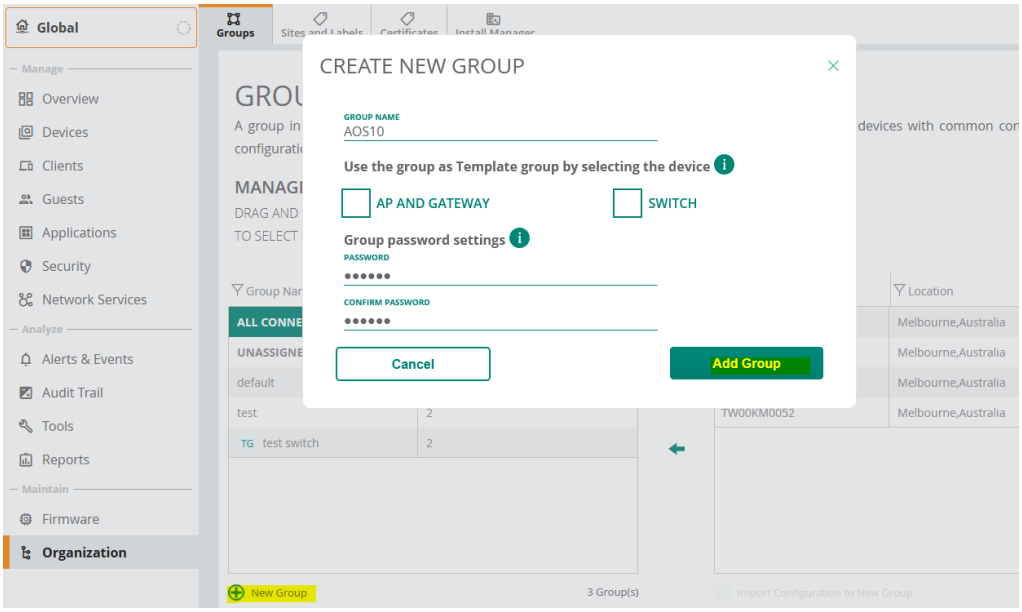




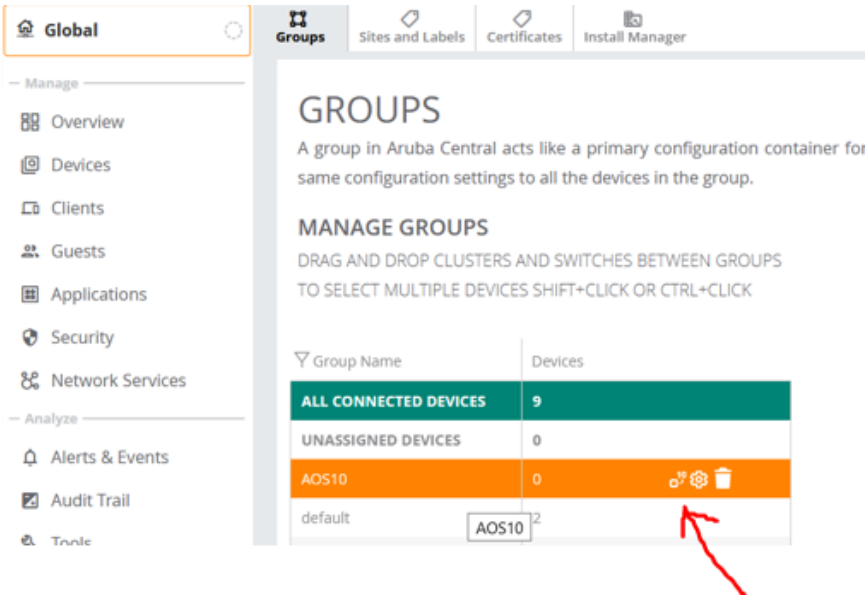
Now, we'll go the network operations App in Aruba Central.

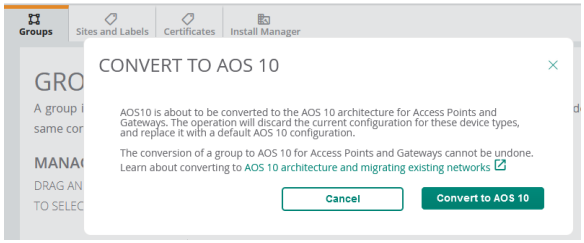


Here we'll create a group and move the devices into it. The groups are used for device configurations.

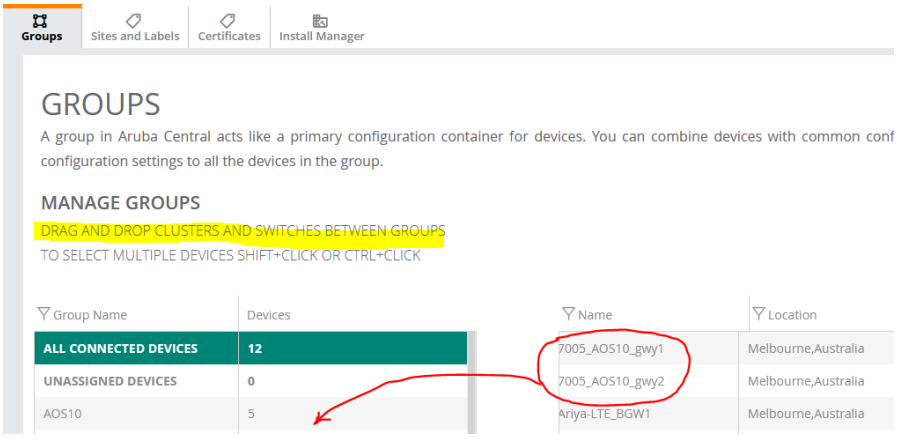


Then you need to convert the group to AOS10.





Once the group is converted, you can then drag and drop the devices from the right hand side table.

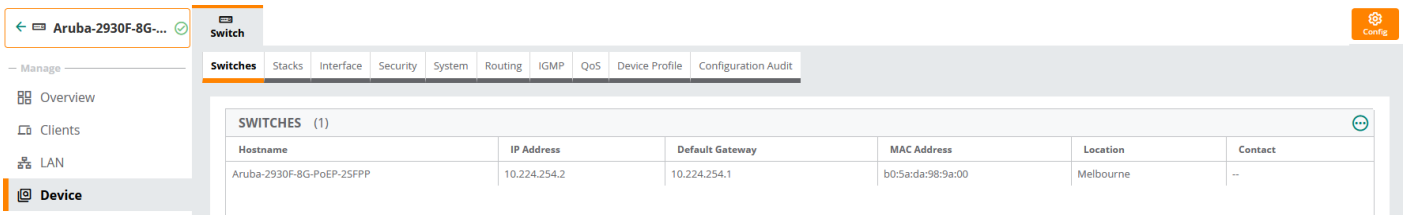


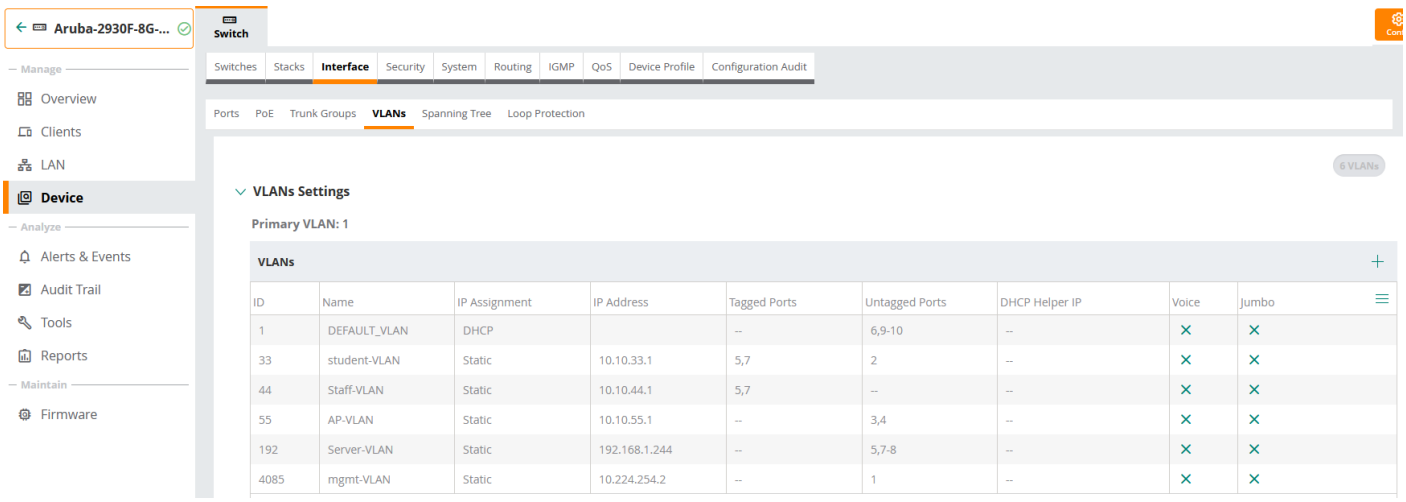
4 Aruba Central Configuration

For this demo, I have also added Aruba 2930F switch to Aruba Central's AOS10 group. We'll start with the configuration of the LAN switch to which we'll connect the APs and the gateways.

4.1 LAN Switch Configuration

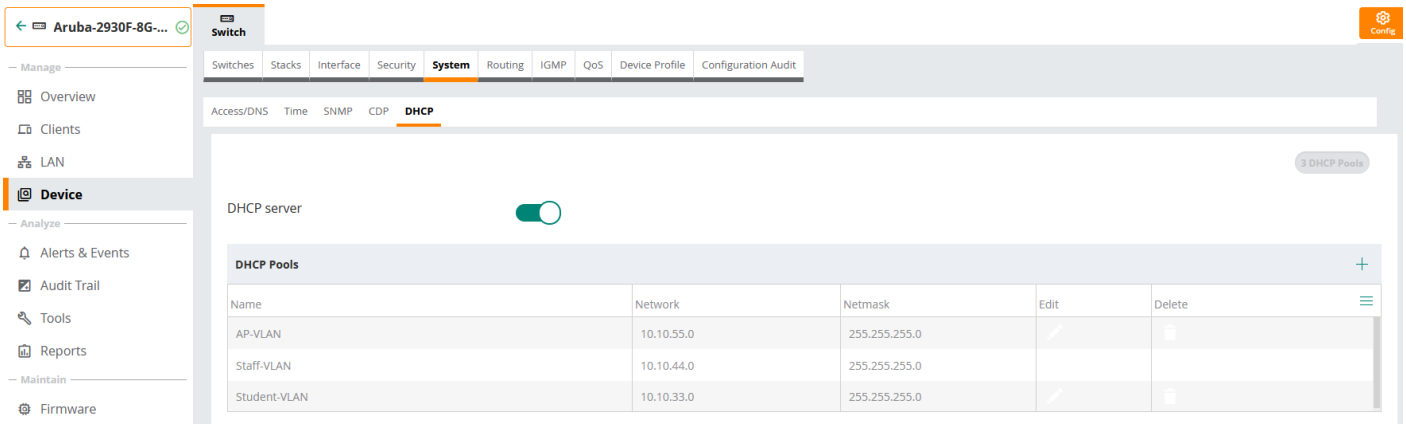
We won't go deep in this section as the focus here is AOS 10 demo. Take a note of the VLANs that are configured.





As the names suggests, APs are connected to AP-VLAN, gateways and ClearPass are connected to Server VLAN.

The gateways are connected to port 5 and 7 that are configured for VLAN trunking. DHCP for AP, staff, and student VLANs are configured on the switch.




```
dhcp-server pool "AP-VLAN"
   default-router "10.10.55.1"
   dns-server "10.224.254.1"
   lease 00:08:00
   network 10.10.55.0 255.255.255.0
   range 10.10.55.10 10.10.55.19
   exit
dhcp-server pool "Staff-VLAN"
```

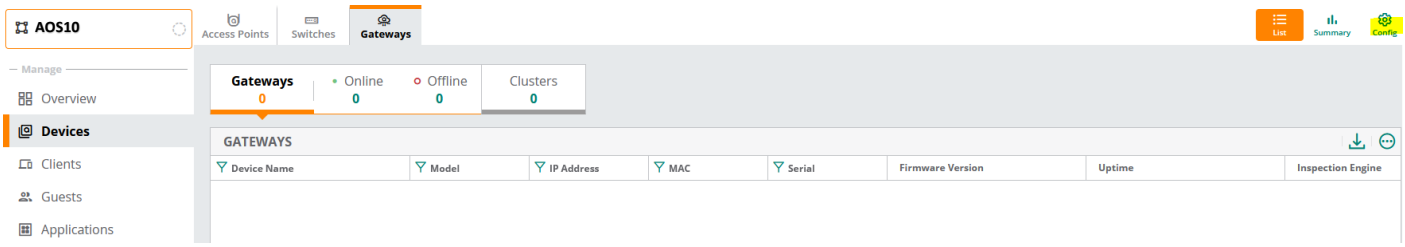
```
   default-router "10.10.44.1"
   dns-server "1.1.1.1"
   lease 00:04:00
   network 10.10.44.0 255.255.255.0
   range 10.10.44.50 10.10.44.59
   exit
dhcp-server pool "Student-VLAN"
   default-router "10.10.33.1"
   dns-server "1.1.1.1"
   lease 00:04:00
   network 10.10.33.0 255.255.255.0
   range 10.10.33.50 10.10.33.59
   exit
dhcp-server enable

Aruba-2930F-8G-PoEP-2SFPP#
```

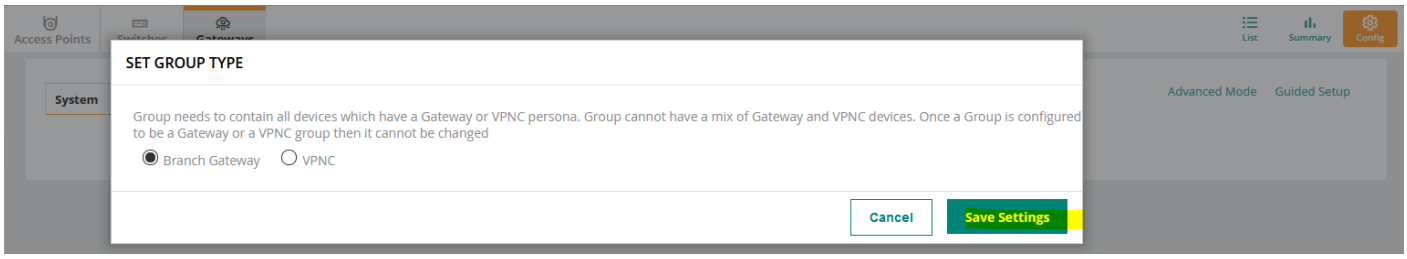
4.2 Gateway Configuration

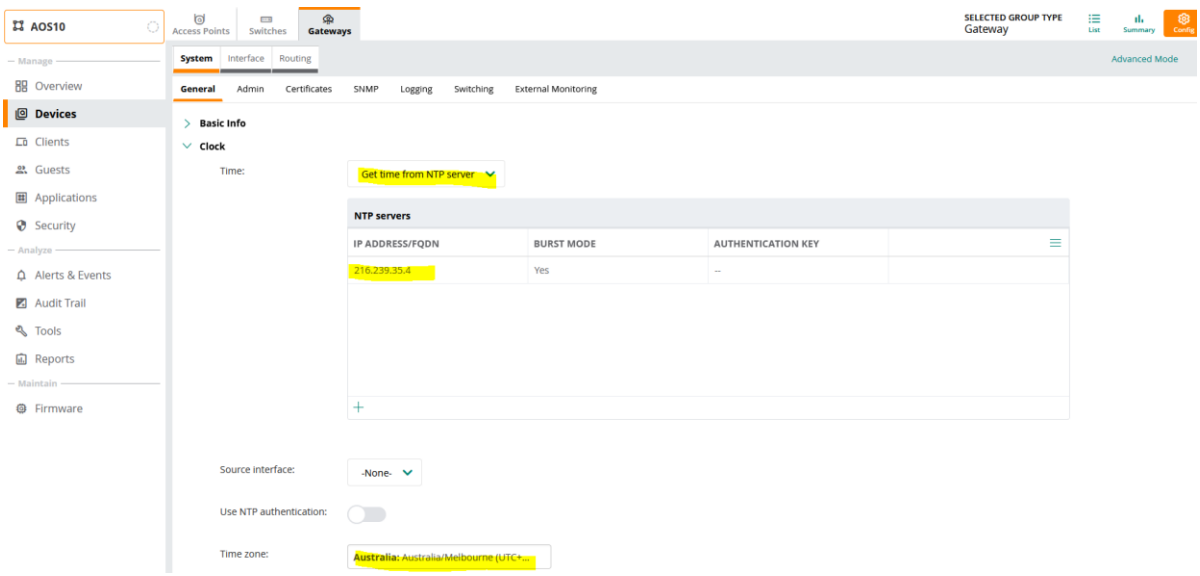
Note that with AOS 10, Gateways are not mandatory. They are required if you want to tunnel user traffic to a central location particularly useful for scenarios that you need L2 roaming between APs in different subnets.

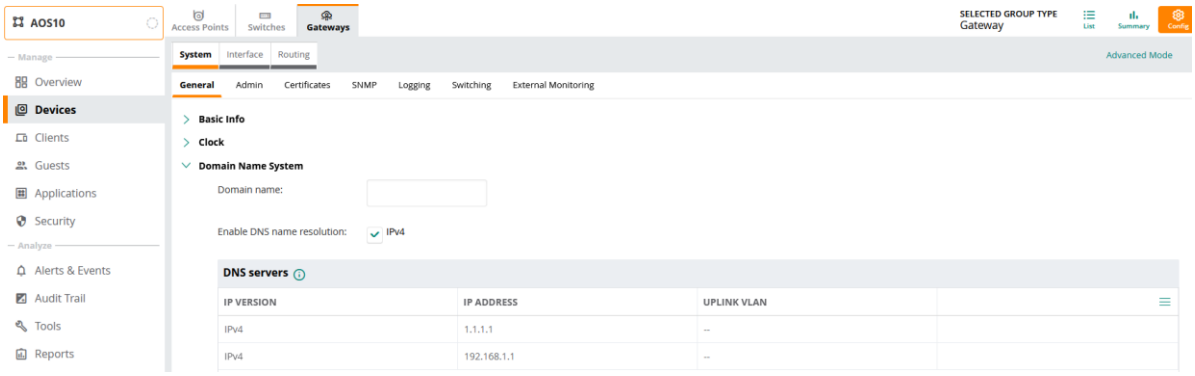
We'll start the configuration at group level before powering up the gateways. This is to minimise the reboots and some potential network issues especially when it comes to changing IP address and loosing connectivity.

We'll be using Aruba 7005 gateways which have 4x ports.

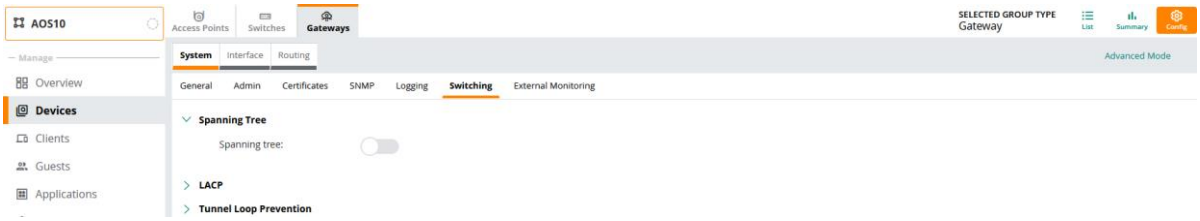




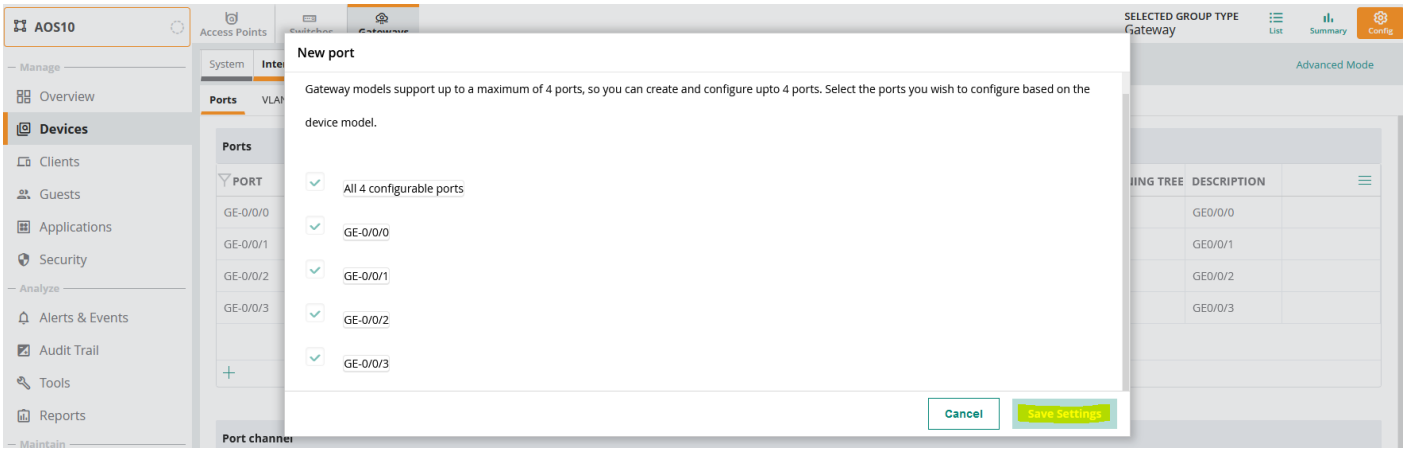




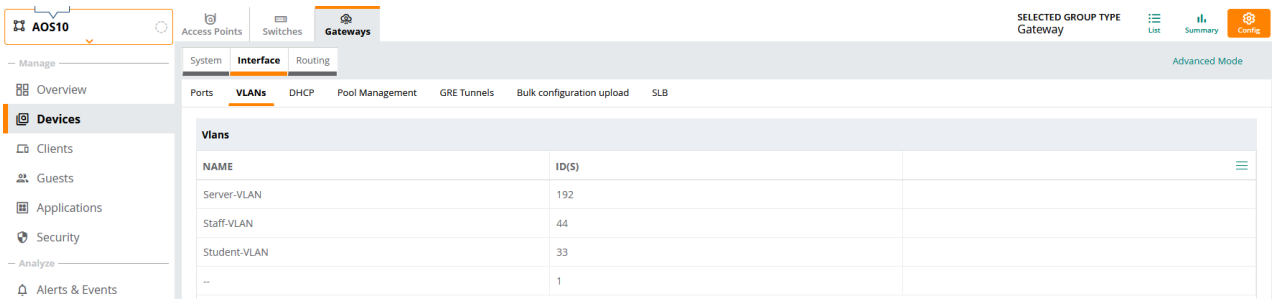
Disabling spanning tree



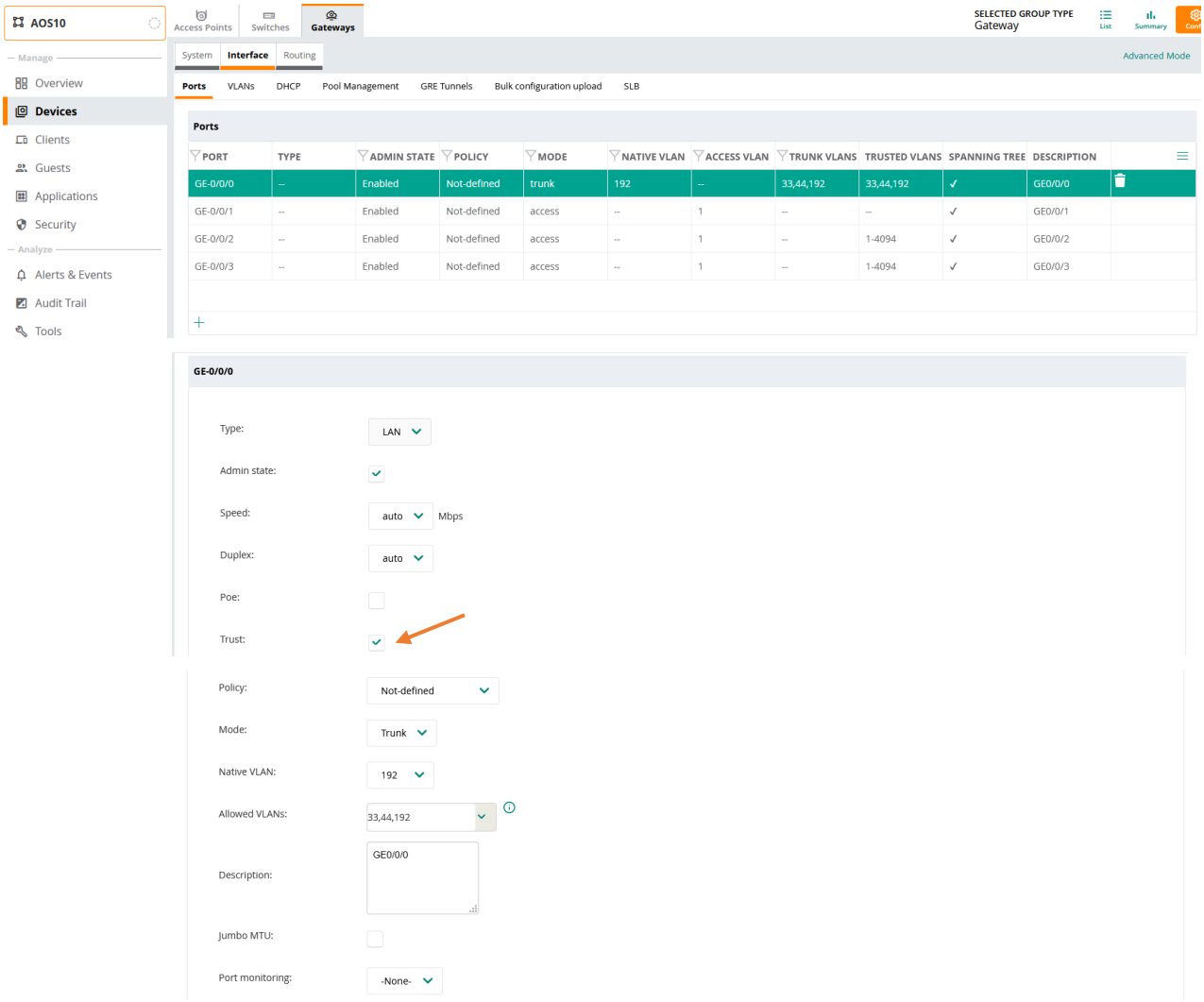
Adding the relevant ports for Aruba 7005 gateway.



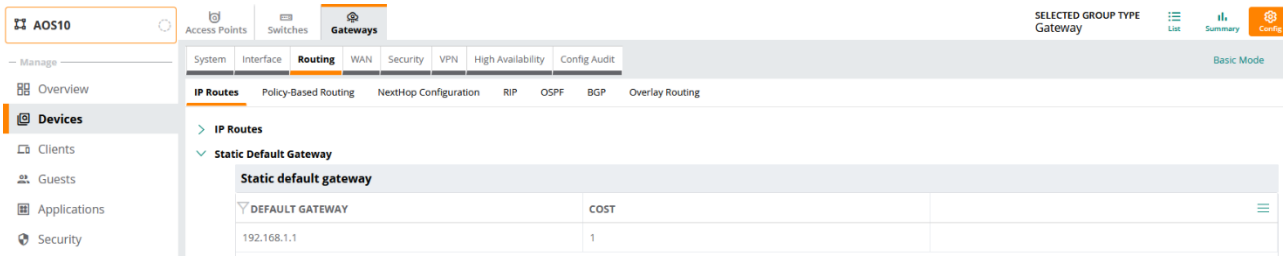
I am planning to sue interface 0/0/0 as my gateway uplink. This port needs to be in trunk mode and here we'll add the relevant VLANs.



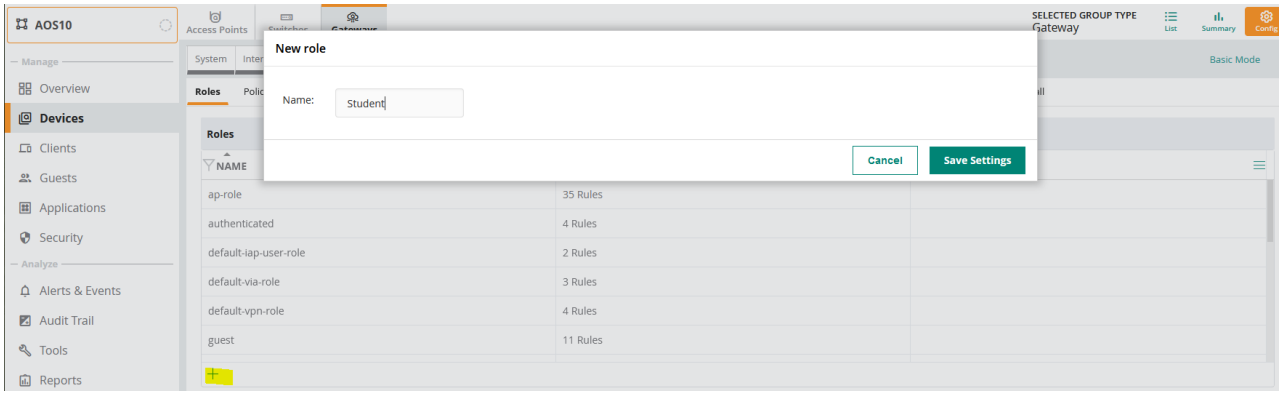
Adding the VLANs to appropriate ports.

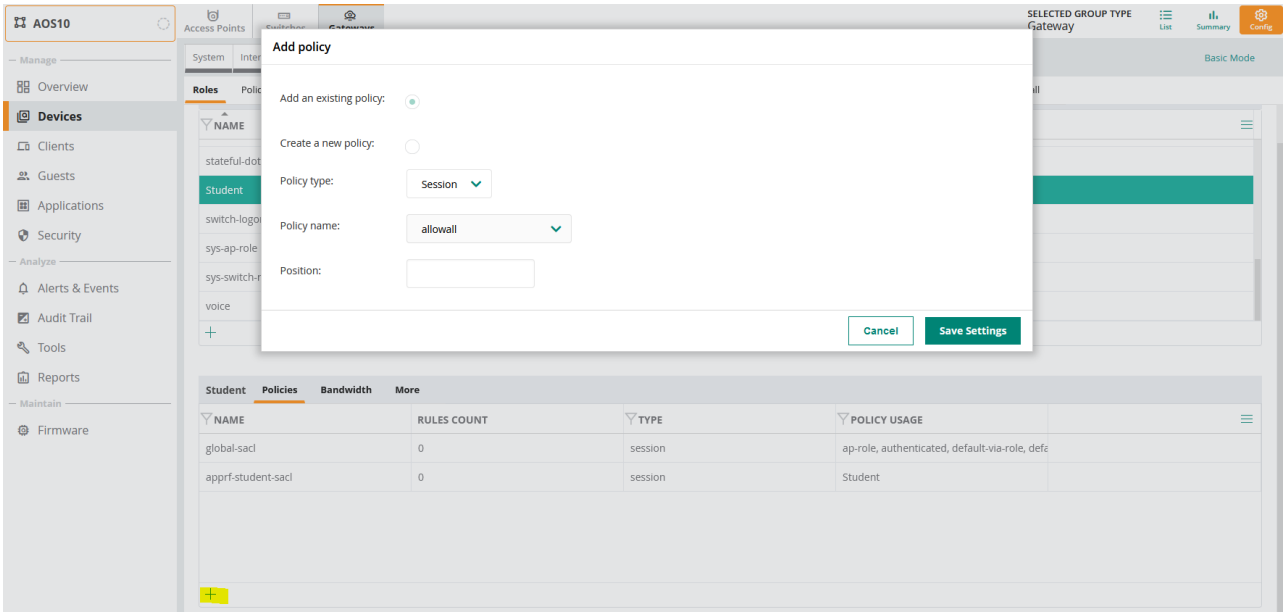


Adding the default route

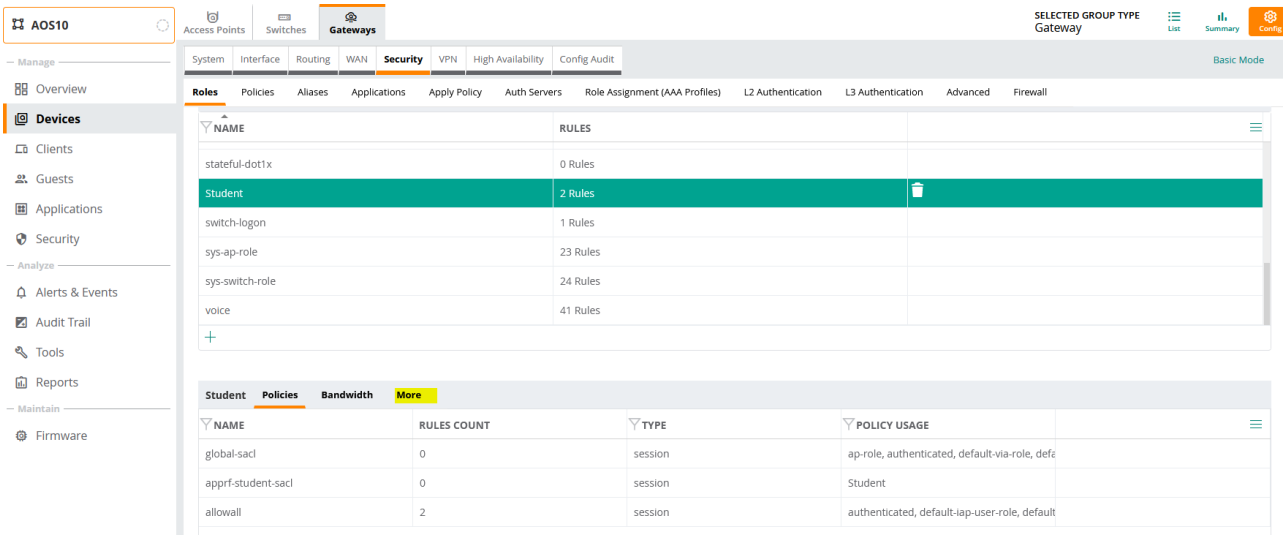


Adding the user roles by going to “security tab”

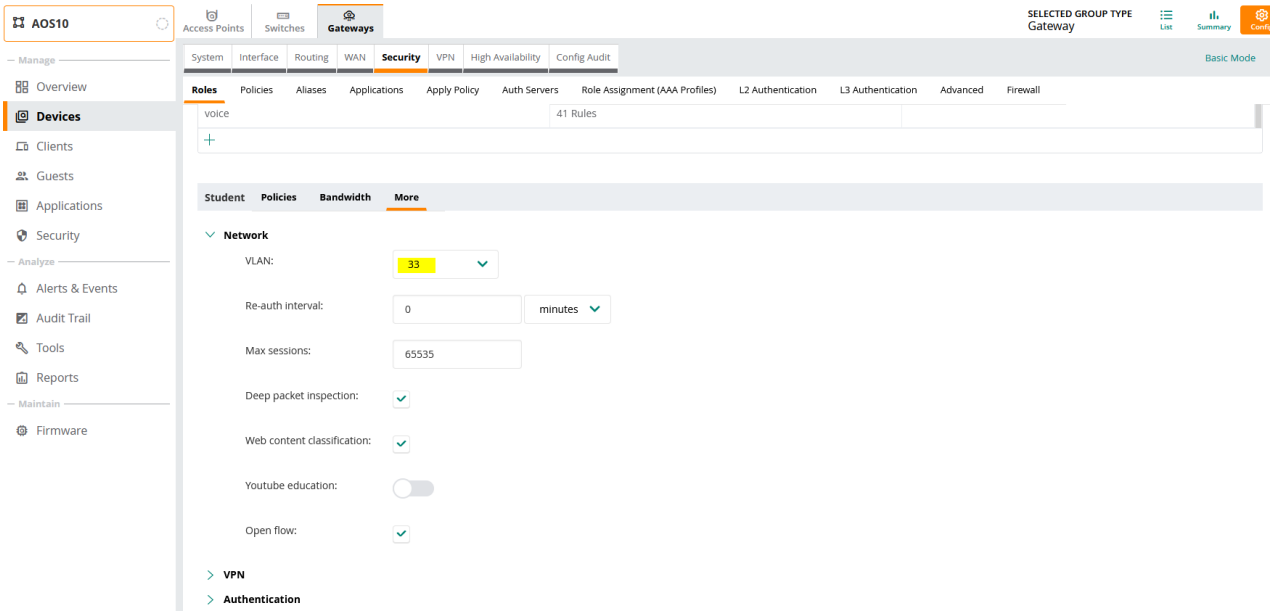




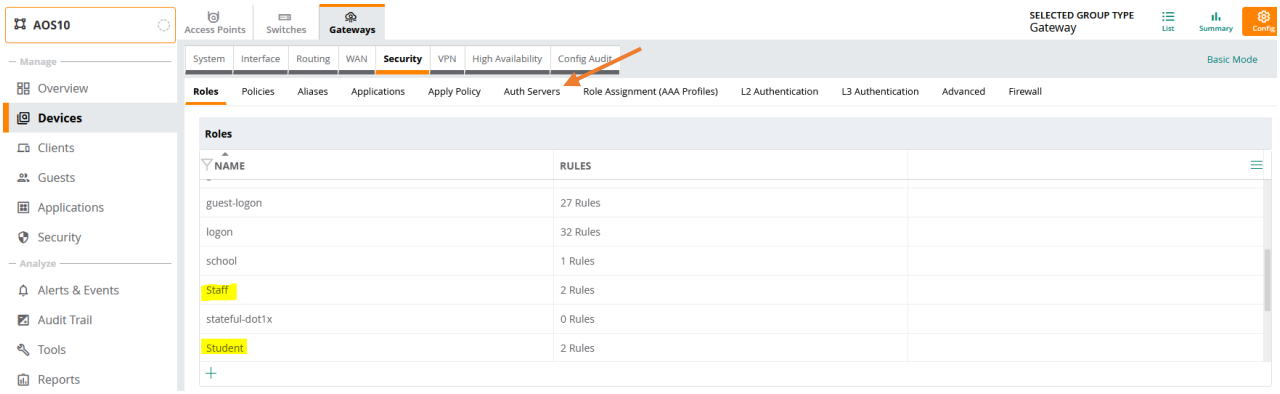
Here we'll add the allow-all policy.



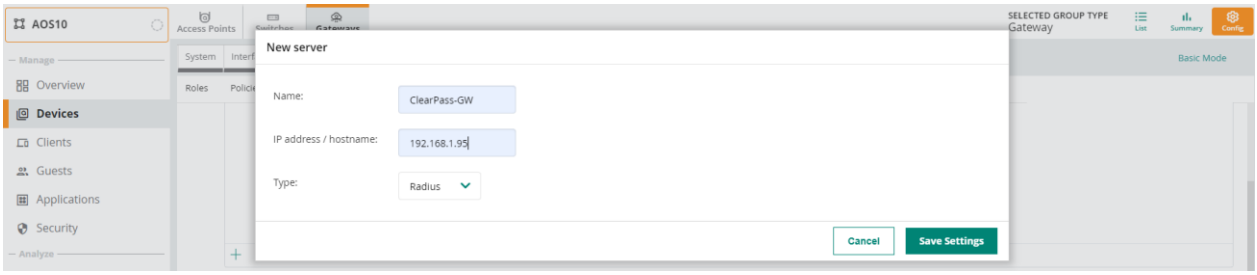
Next, we'll assign a VLAN to this role.



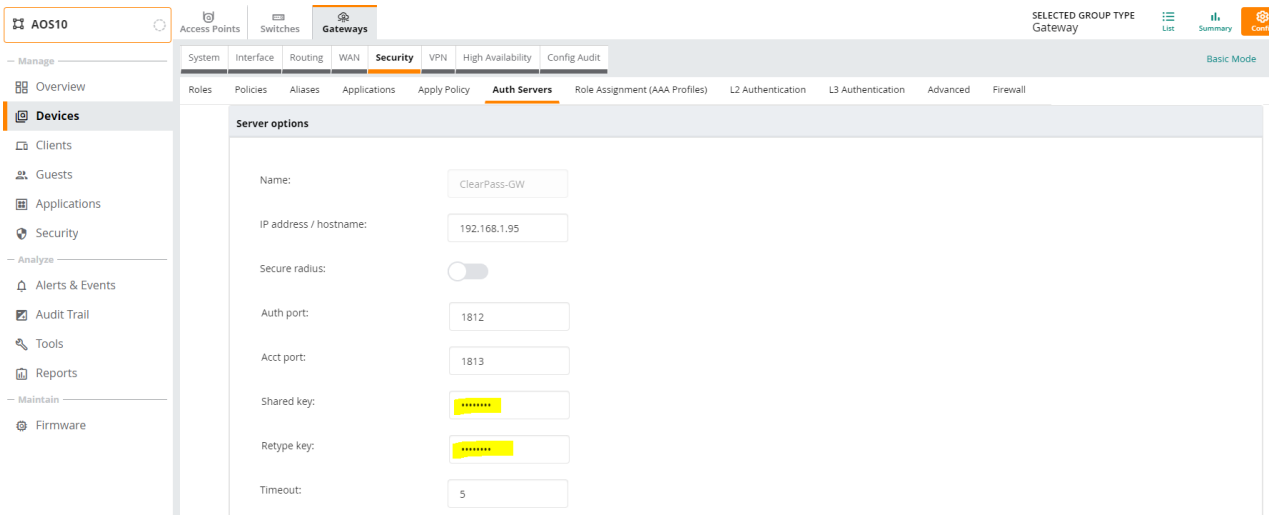
We'll create a new user role staff and as before, we'll add a allow-all policy and assign VLAN 44 to it.



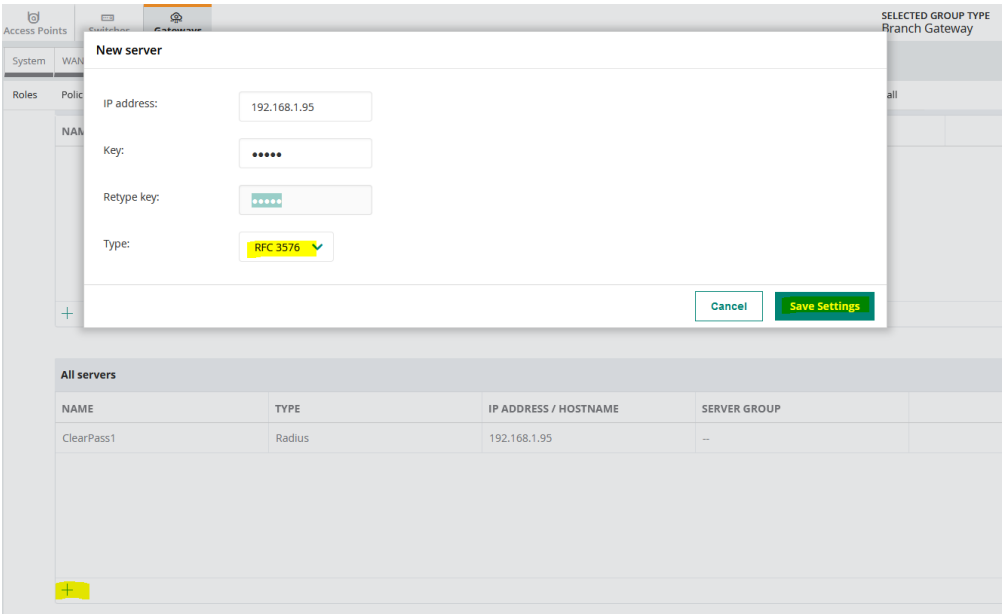
We'll configure the authentication server and RFC3576 for RADIUS CoA



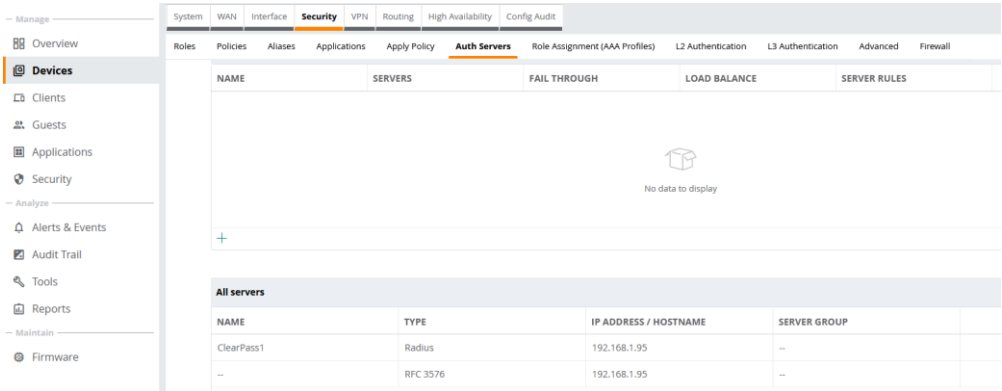
Then once saved, click on it to set the RADIUS secret key



And finally add a rfc3576 server for CoA.

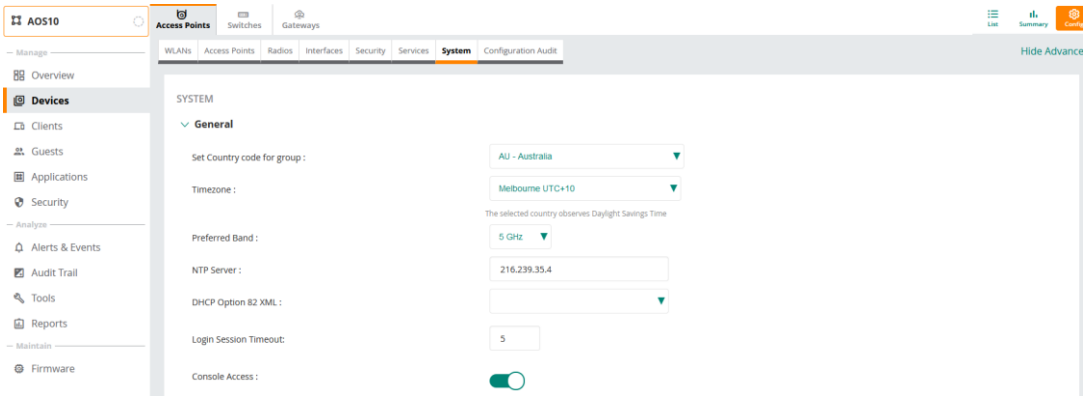


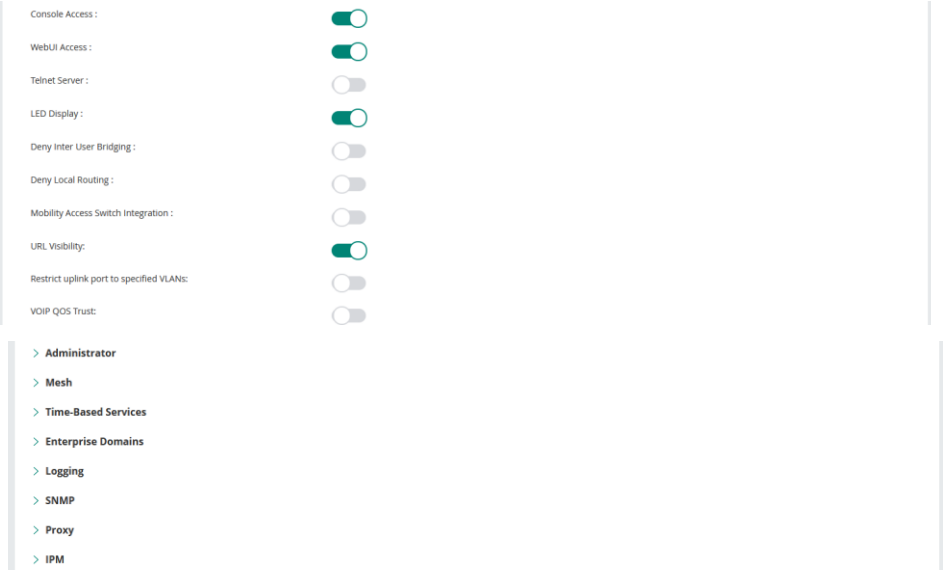
Note that they are not assigned to any authentication server groups.

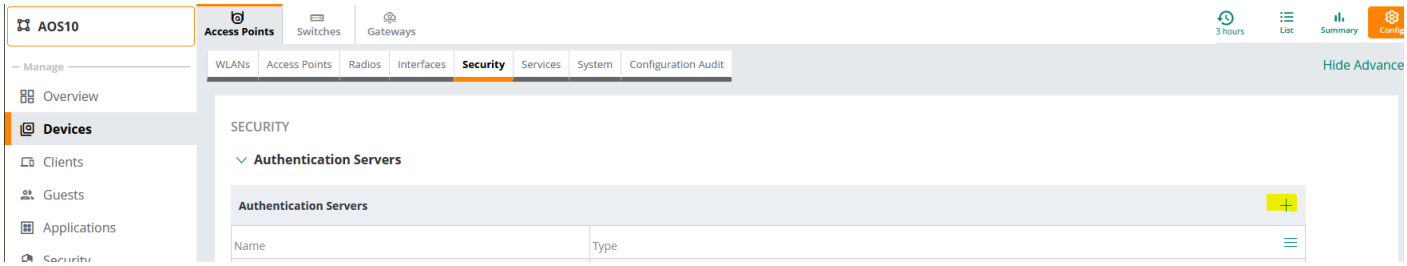


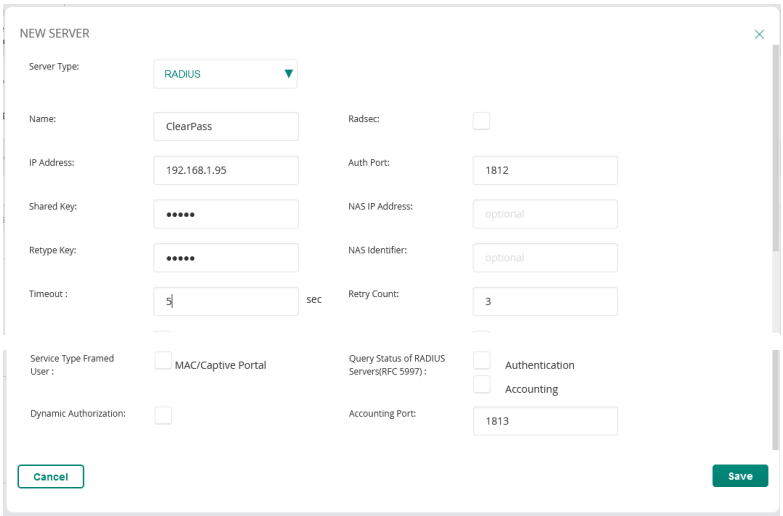
4.3 AP Configuration

Here we'll go through the AP configuration. As always, we'll do the bulk of configuration at the group level.

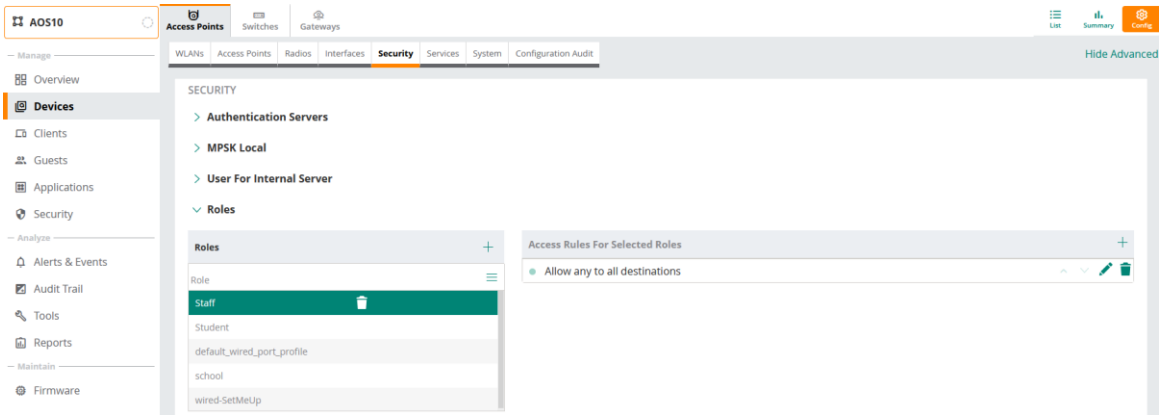








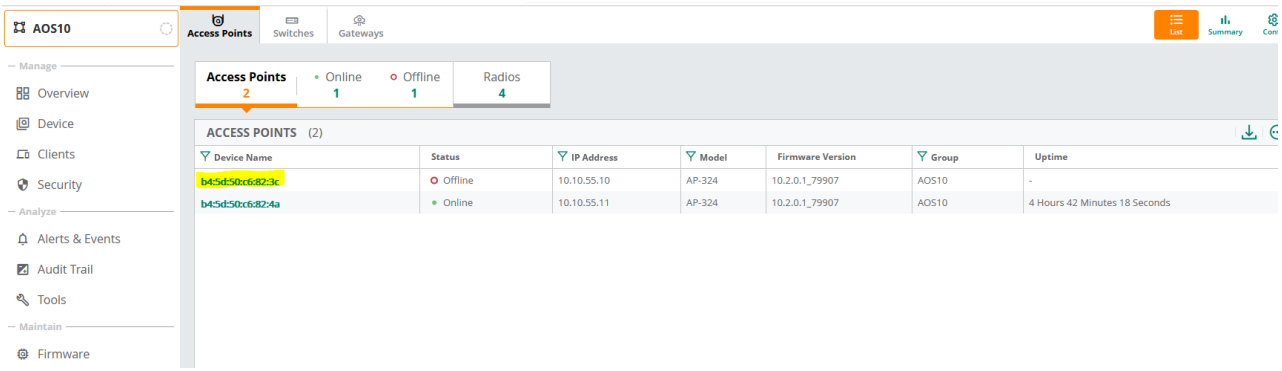
As we did with gateways, we'll create various user roles here as well.

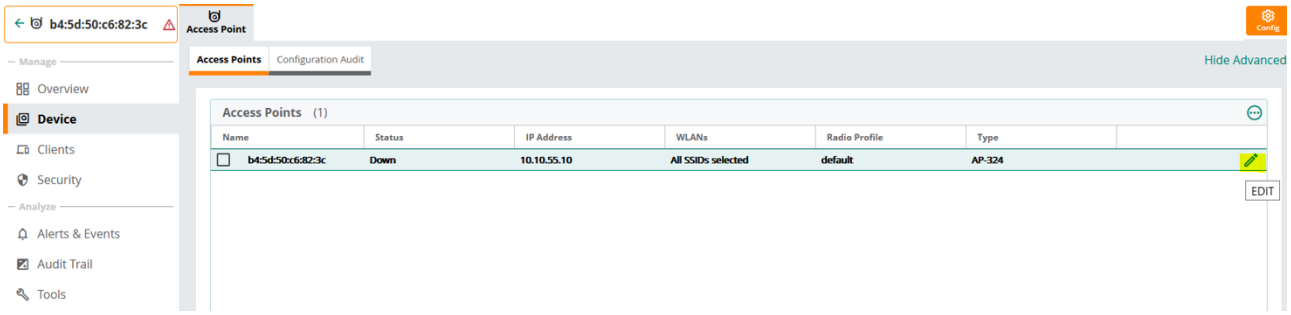


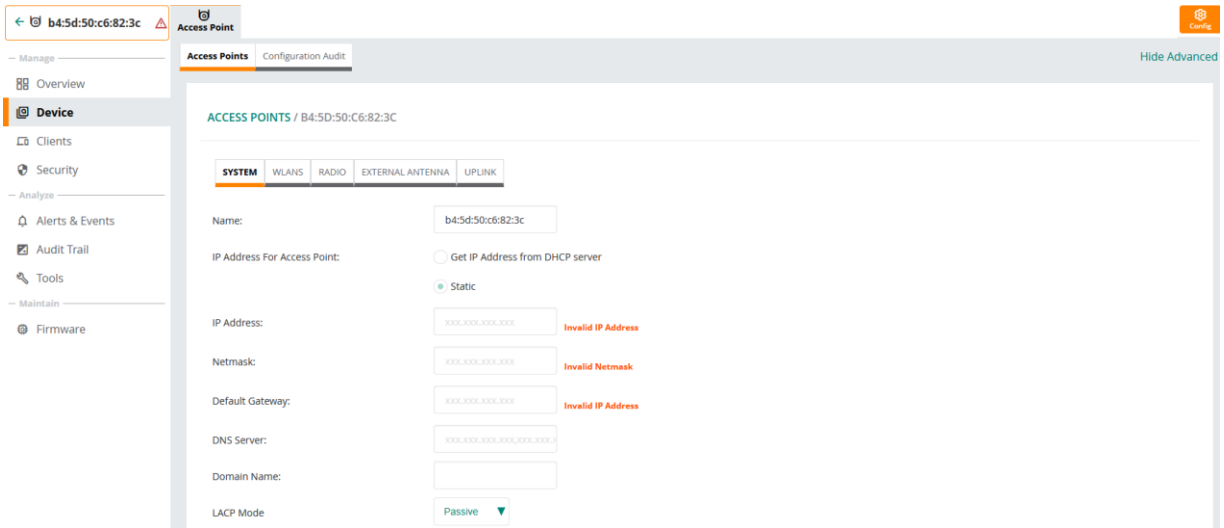
This is in case we want to change from tunnel mode to bridge mode for user traffic, otherwise we don't need these roles here.

4.4 Assigning Static IP addresses for APs

In most of the cases you'll go with DHCP based IP addresses, but in case you need to assign static IP addresses, it is done as shown below.







4.5 Firmware Upgrade

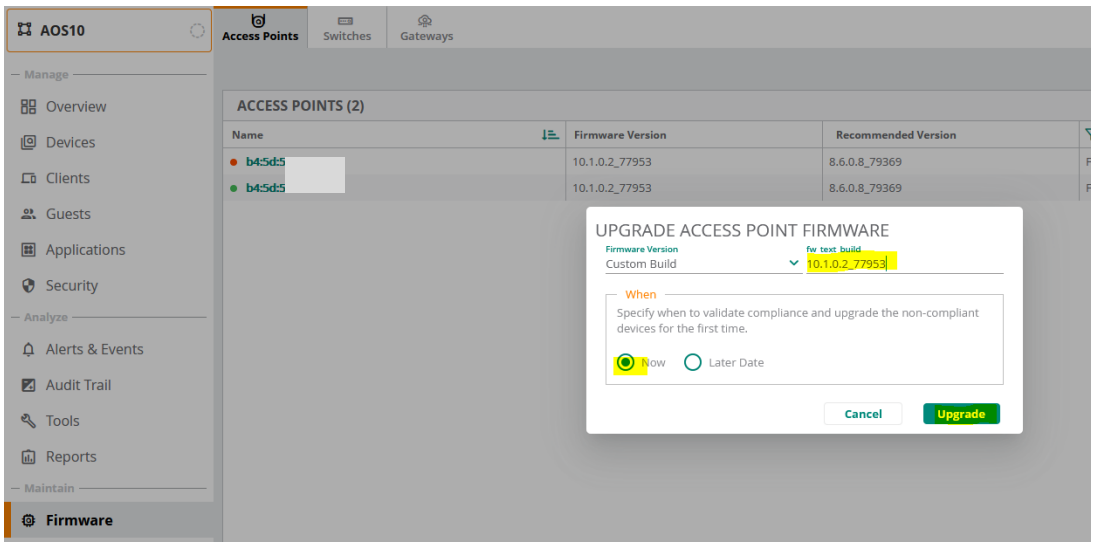
We'll now connect the APs that we previously added to Aruba Central inventory that are running Instant software to the network. The network must have Internet access. Ensure that the APs are in factory default mode to get rid of any previous configuration. When they are powered up, they will get DHCP IP address and with a valid DNS and will then contact Central and will end up in AOS10 group that we created before.

For the gateways ensure they are factory default and running the SD-branch image 8.6.0.4-2.2.x.x or better. Again, like the APs, once the gateways are powered up they can use DHCP to get their IP addresses and will then contact Aruba Central, but we'll go through the full setup without DHCP.

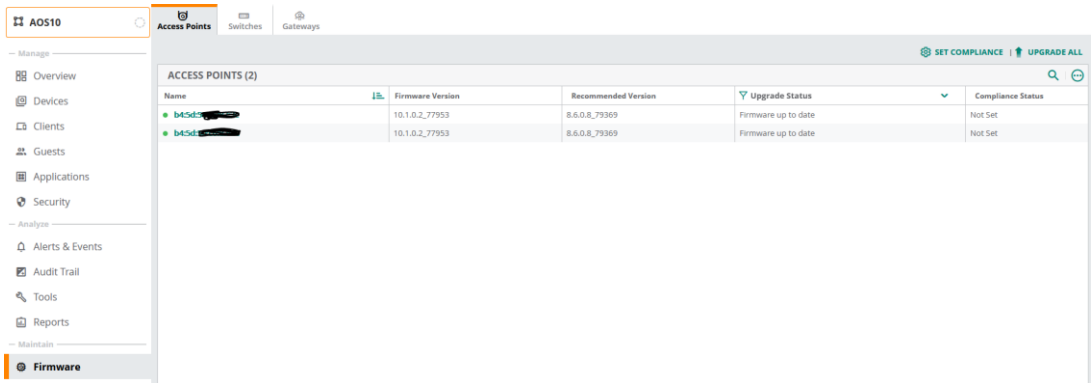
```
Auto-provisioning is in progress. It requires DHCP and Activate servers
Choose one of the following options to override or debug auto-provisioning...
    'enable-debug'       : Enable auto-provisioning debug logs
```

```
    'disable-debug'     : Disable auto-provisioning debug logs
    'mini-setup'        : Start mini setup dialog. Provides minimal customization and
requires DHCP server
    'full-setup'        : Start full setup dialog. Provides full customization
    'static-activate'   : Provides customization for static or PPPOE ip assignment.
Uses activate for master information

Enter Option (partial string is acceptable): full-setup

Are you sure that you want to stop auto-provisioning and start full setup dialog?
(yes/no): yes

***************** Welcome to the Aruba7005 setup dialog *****************
This dialog will help you to set the basic configuration for the switch.
These settings, except for the Country Code, can later be changed from the
Command Line Interface or Graphical User Interface.

Commands: <Enter> Submit input or use [default value], <ctrl-I> Help
<ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end
<ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line
<ctrl-P> Previous question <ctrl-X> Restart beginning <ctrl-R> Reload box

Enter System name [Aruba7005]: 7005-1
Enter Switch Role (standalone|md) [md]:
Enter IP type to terminate IPSec tunnel (ipv4|ipv6) [ipv4]:
Enter Master switch IP address/FQDN or ACP IP address/FQDN: device-
apacsouth.central.arubanetworks.com
Enter Master switch type(MM|ACP) ACP
Enter Uplink Vlan ID [1]:192
Enter Uplink port [GE 0/0/0]:
Enter Uplink port mode (access|trunk) [access]:
Enter Uplink Vlan IP assignment method (dhcp|static|pppoe) [static]:
Enter Uplink Vlan Static IP address [172.16.0.254]: 192.168.1.243
Enter Uplink Vlan Static IP netmask [255.255.255.0]:
Enter IP default gateway [none]: 192.168.1.1
Enter DNS IP address [none]: 192.168.1.1
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
Do you want to configure dynamic port-channel (yes|no) [no]:
Enter Country code (ISO-3166), <ctrl-I> for supported list: AU
You have chosen Country code AU for Australia (yes|no)?: yes
Enter the controller's IANA Time zone [America/Los_Angeles]: Australia/Melbourne
Enter Time in UTC [12:53:36]:
Enter Date (MM/DD/YYYY) [12/3/2021]:
Do you want to create admin account (yes|no) [yes]:
Enter Password for admin login (up to 32 chars): ********
Re-type Password for admin login: ********

<omitted the other lines>

System will now restart!

[12:55:07]:Starting rebootme
[12:55:07]:Shutdown processing started
```

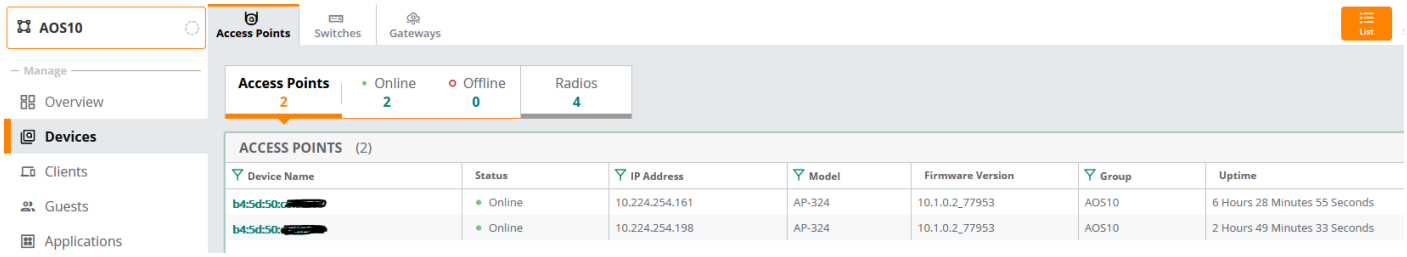
Once the APs and gateways are online in Aruba Central, we'll upgrade them to AOS10 image. In the next release SD-branch and AOS10 firmware will merge. I have already upgraded my APs, but this is how you can do it.

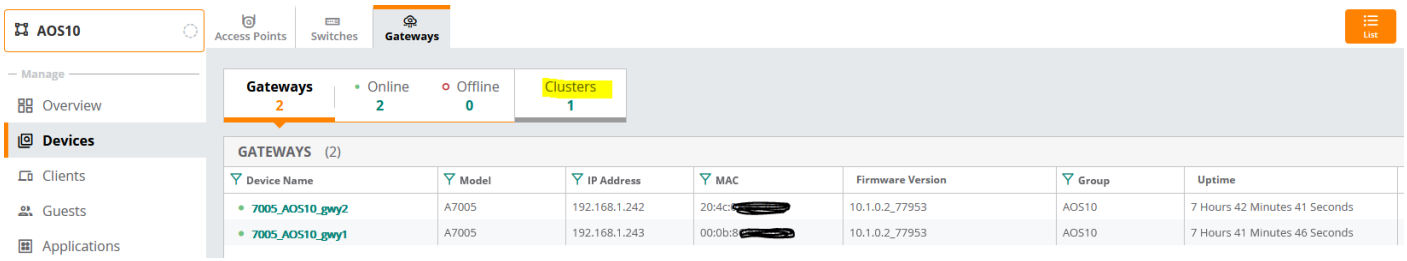


We'll use the same firmware version for the gateways as well.



Here we'll check to see if the APs and gateways are online with the correct firmware





Notice that there is one gateway cluster. The cluster will automatically be formed between gateways on the network using their system IP addresses.

4.6 Gateway Cluster

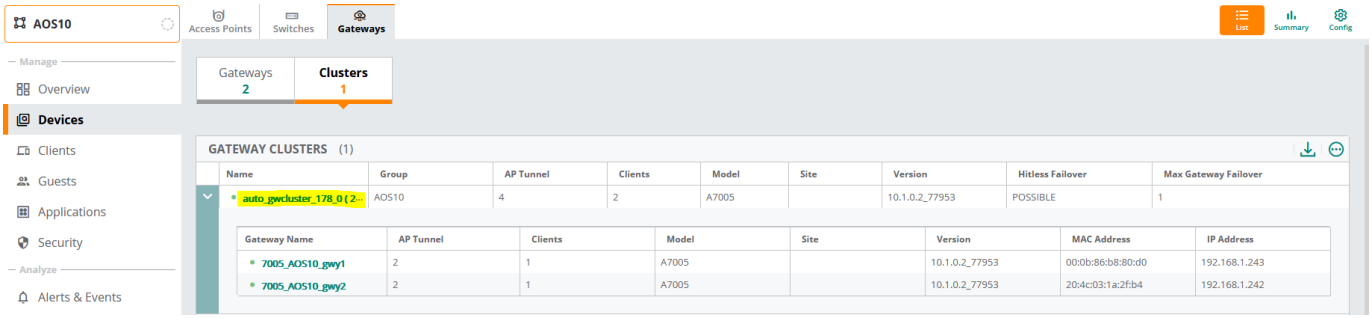
Cluster is a combination of multiple MDs working together to provide high availability to all the clients and ensure service continuity when a failover occurs. The gateways need not be identical and can be either L2- connected or L3-connected with a mixed configuration. In case of failover, the client SSO works for the L2- connected managed devices and the clients are de-authenticated for L3-connected managed devices in a cluster.

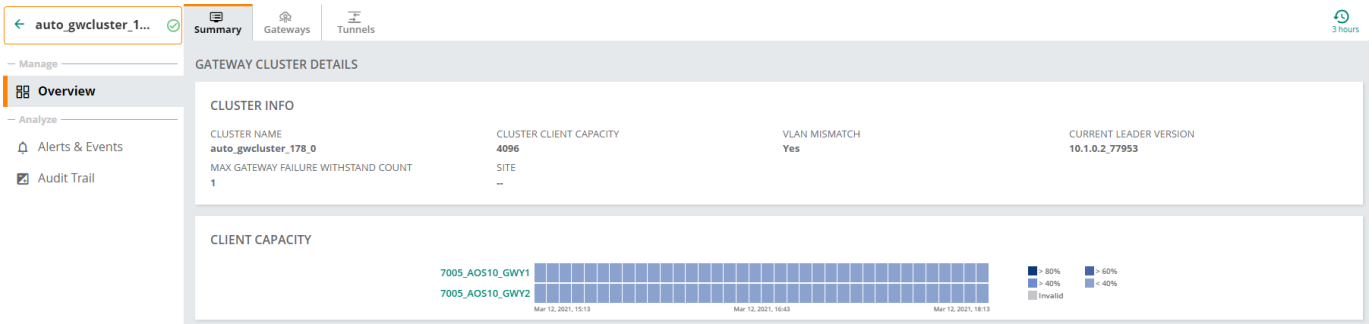
The aims of clustering are

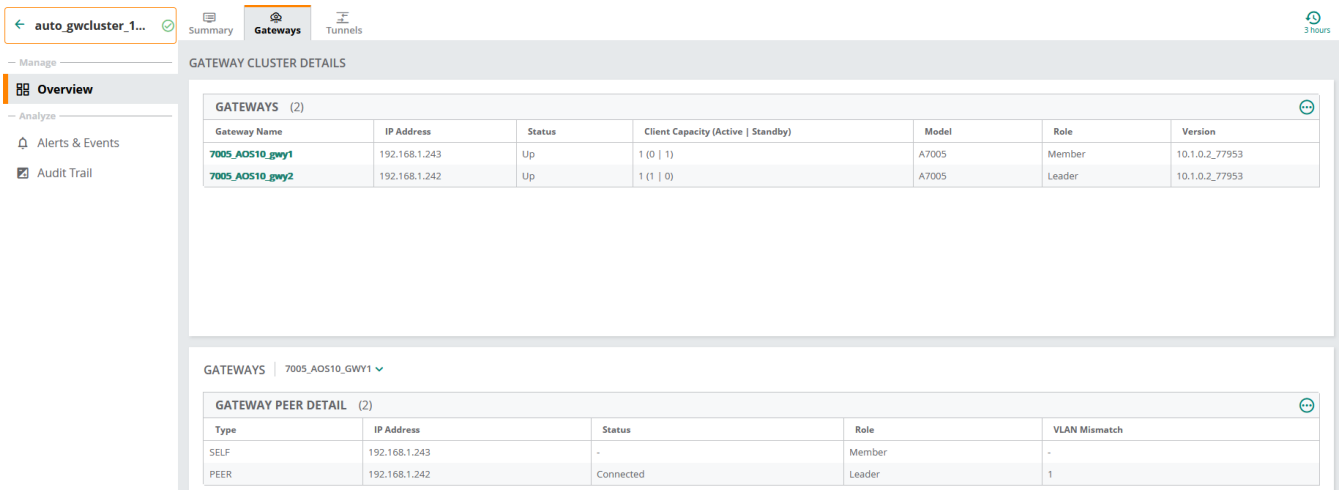
- seamless Campus Roaming: When a client roams between APs of different managed devices within a large L2 domain, the client retains the same subnet and IP address to ensure seamless roaming. The clients remain anchored to a single managed device in a cluster throughout their roaming area which makes their roaming experience seamless because their L2 or L3 information and sessions remain on the same managed device.
- Hitless Client Failover: When a managed device fails, all the users fail over to their standby managed device seamlessly without any disruption to their wireless connectivity or existing high-value sessions.
- Client and AP Load Balancing: When there is excessive workload among the managed devices, the client and AP load is evenly balanced among the cluster members. Both clients and APs are load balanced seamlessly.

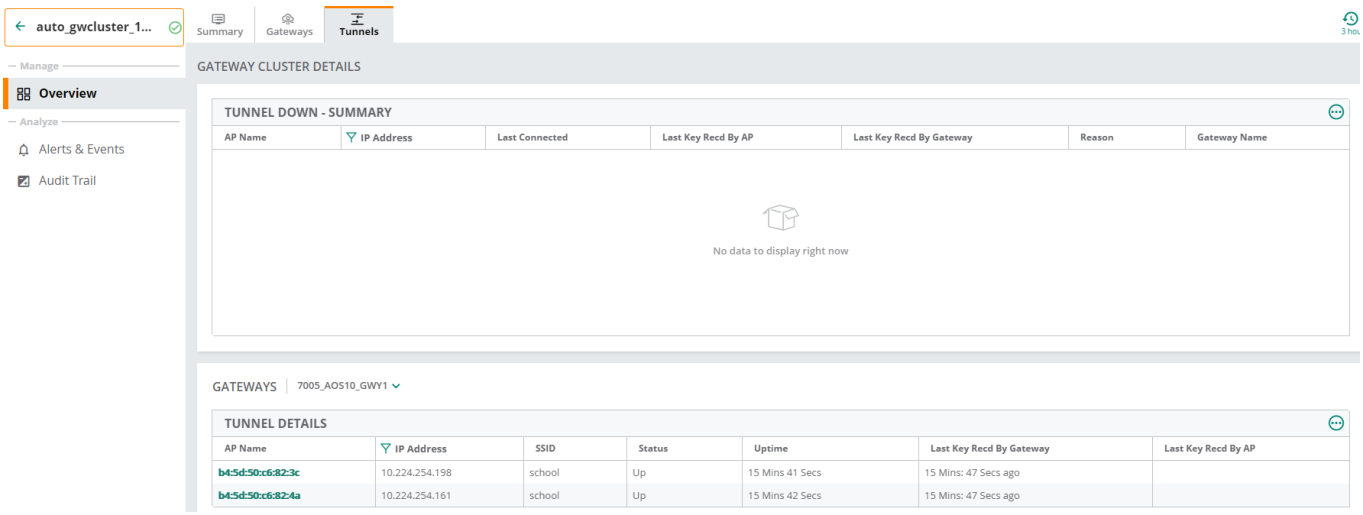
4.7 Monitoring Gateway Cluster

Here is how to check the gateway cluster









Here is the CLI command to check the operation of the cluster.

```
(7005_AOS10_gwy1) #show lc-cluster group-membership

Cluster Enabled, Profile Name = "auto_gwcluster_178_0"
Heartbeat Threshold = 900 msec
Cluster Info Table
------------------
Type IPv4 Address    Priority Connection-Type STATUS
---- --------------- -------- --------------- ------
self   192.168.1.243      128             N/A CONNECTED (Member)
peer   192.168.1.242      128    L2-Connected CONNECTED (Leader)

(7005_AOS10_gwy1) #show lc-cluster load distribution client

Cluster Load Distribution for Clients
-------------------------------------
Type IPv4 Address    Active Clients Standby Clients
---- --------------- -------------- ---------------
self   192.168.1.243              0               1
peer   192.168.1.242              1               0
Total: Active Clients 1 Standby Clients 1

(7005_AOS10_gwy1) #
(7005_AOS10_gwy1) #show lc-cluster load distribution ap

Cluster Load Distribution for APs
---------------------------------
Type IPv4 Address    Active APs     Standby APs
---- --------------- -------------- ---------------
self   192.168.1.243              1               1
peer   192.168.1.242              1               1
Total: Active APs 2 Standby APs 2

(7005_AOS10_gwy1) #
```

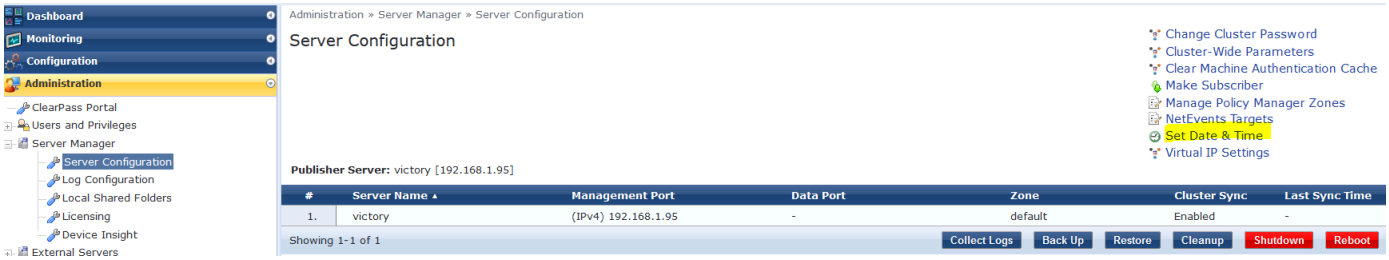
Now checking the second gateway. Note we have 1x client and 2x APs that are connected.

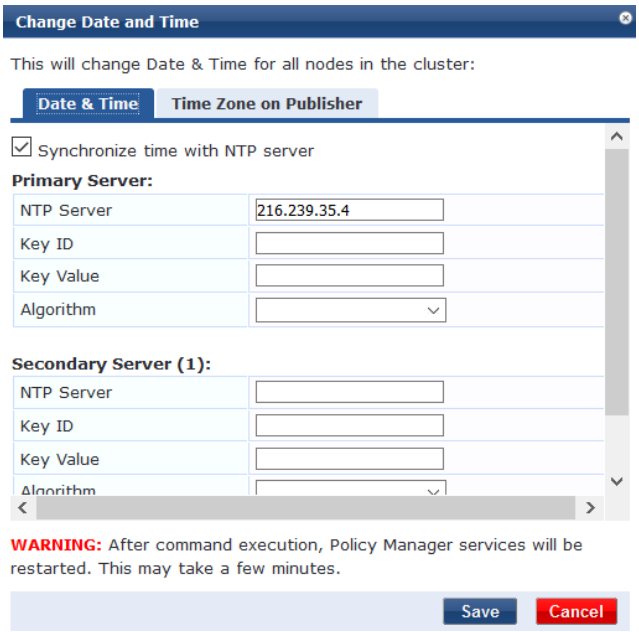
```
(7005_AOS10_gwy2) #show lc-cluster group-membership

Cluster Enabled, Profile Name = "auto_gwcluster_178_0"
Heartbeat Threshold = 900 msec
Cluster Info Table
------------------
Type IPv4 Address    Priority Connection-Type STATUS
---- --------------- -------- --------------- ------
peer   192.168.1.243      128    L2-Connected CONNECTED (Member)
self   192.168.1.242      128             N/A CONNECTED (Leader)

(7005_AOS10_gwy2) #
(7005_AOS10_gwy2) #
(7005_AOS10_gwy2) #show lc-cluster load distribution client
```

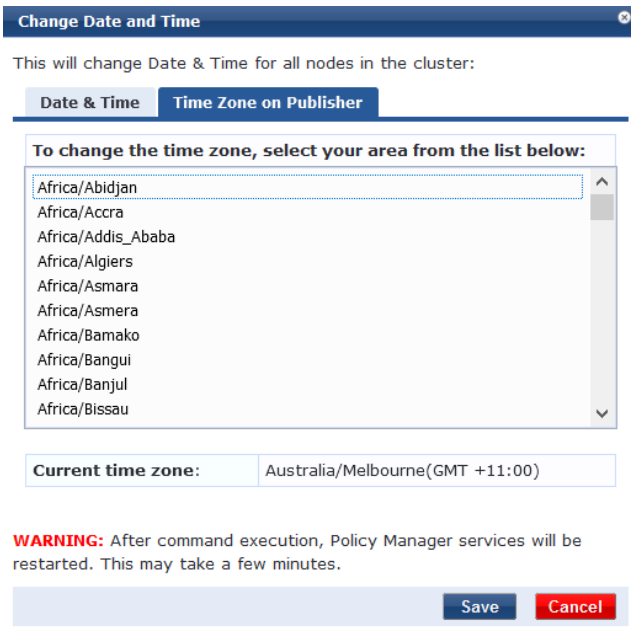
```
Cluster Load Distribution for Clients
-------------------------------------
Type IPv4 Address    Active Clients Standby Clients
---- --------------- -------------- ---------------
peer   192.168.1.243              0               1
self   192.168.1.242              1               0
Total: Active Clients 1 Standby Clients 1

(7005_AOS10_gwy2) #
(7005_AOS10_gwy2) #show lc-cluster load distribution ap

Cluster Load Distribution for APs
---------------------------------
Type IPv4 Address    Active APs     Standby APs
---- --------------- -------------- ---------------
peer   192.168.1.243              1               1
self   192.168.1.242              1               1
Total: Active APs 2 Standby APs 2

(7005_AOS10_gwy2) #
```

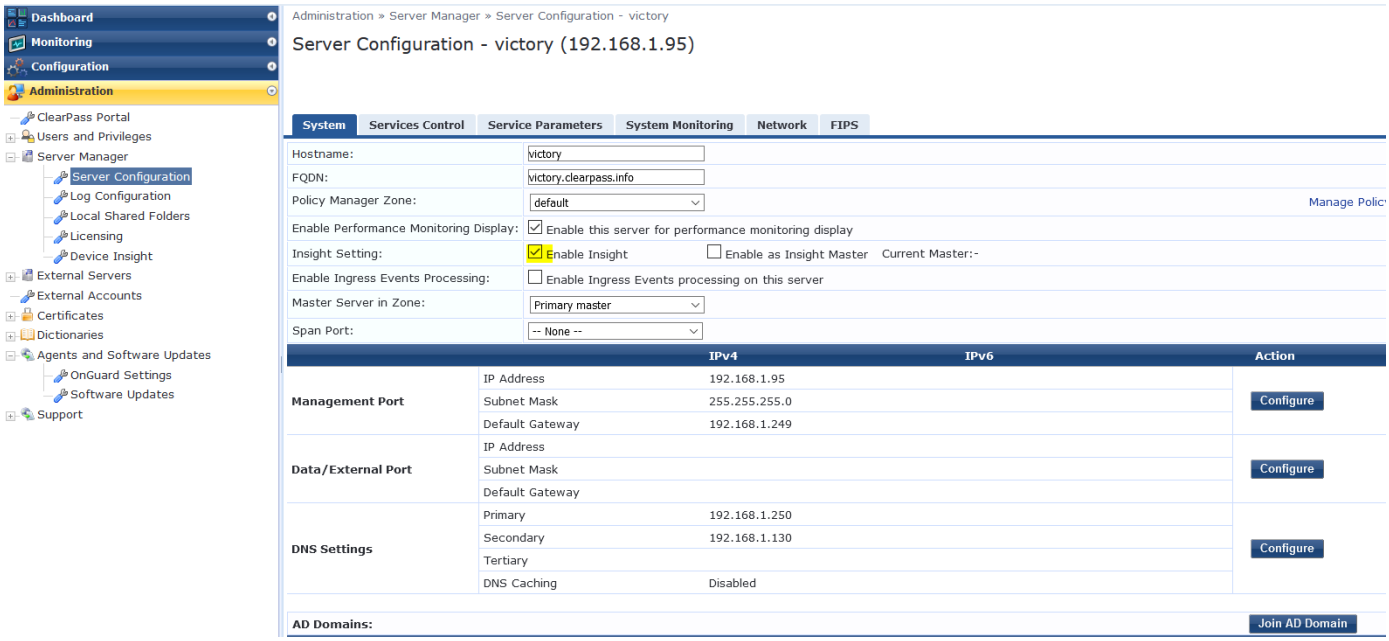
5 ClearPass Initial Configuration

Here we'll do the basic ClearPass configuration and join it to the AD domain along with creation of dot1x service policy. We'll start with NTP and time zone.



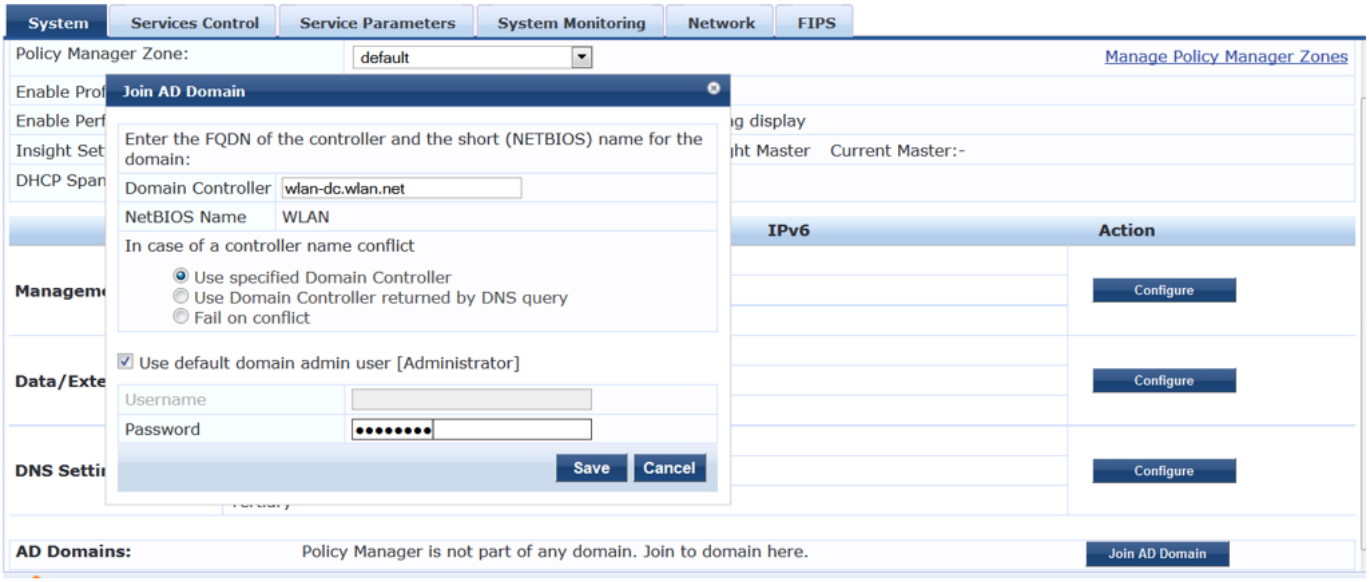


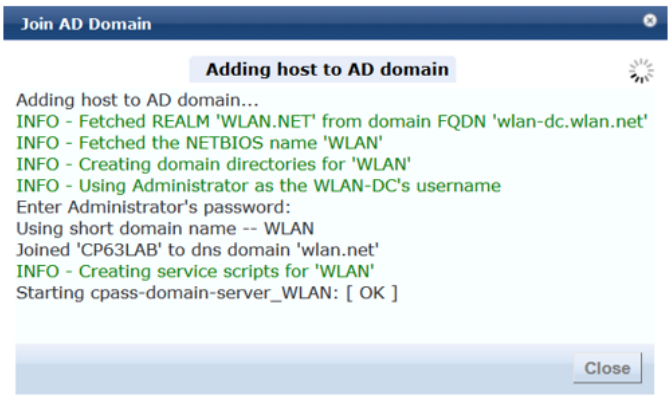


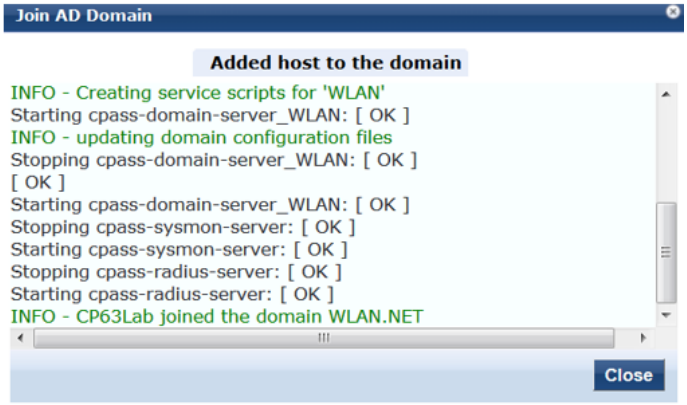


5.1 Joining AD Domain

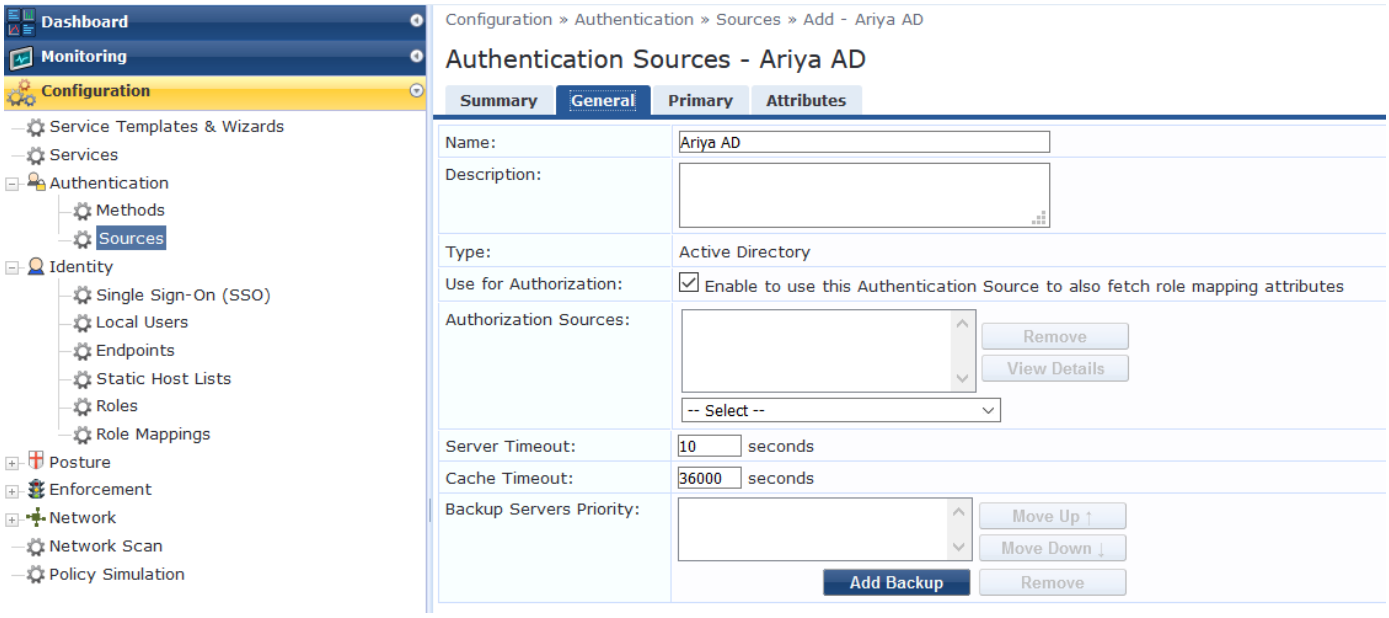
Configure the IP addresses and the rest as per your Lab setup but ensure you have the IP address of your domain controller as the primary DNS. CPPM needs to join the AD domain, in order to authenticate against it. Make sure the clock time for AD and CPPM are almost in sync. It is best to use NTP. If they are not in sync, then CPPM will not be able to join the domain. When you click on the "join domain" button, you need to provide the FQDN of the DC and that's why you need the DNS entry to resolve the name of your domain controller.







Now we need to add the AD as authentication source



Configuration » Authentication » Sources » Add - Ariya AD

Authentication Sources - Ariya AD

Summary | General | Primary | Attributes

Connection Details	
Hostname:	192.168.1.250
Connection Security:	None
Port:	389 (For secure connection, use 636)
Verify Server Certificate:	☑ Enable to verify Server Certificate for secure connection
Bind DN:	administrator@wlan.net (e.g. administrator@example.com OR cn=administrator,cn=users,dc=example,dc=com)
Bind Password:	••••••••••••••••
NetBIOS Domain Name:	WLAN
Base DN:	dc=wlan,dc=net Search Base Dn
Search Scope:	SubTree Search
LDAP Referrals:	☐ Follow referrals
Bind User:	☑ Allow bind using user password
User Certificate:	userCertificate
Always use NetBIOS name:	☐ Enable to always use NetBIOS name instead of the domain part in username for authentication
Special Character Handling for LDAP Query:	◉ Enabled ○ Disabled

Configuration » Authentication » Sources » Add - Ariya AD

Authentication Sources - Ariya AD

Summary | General | Primary | Attributes

Specify filter queries used to fetch authentication and authorization attributes

	Filter Name	Attribute Name	Alias Name	Enabled As
1.	Authentication	dn	UserDN	-
		department	Department	-
		title	Title	-
		company	company	-
		memberOf	memberOf	-
		telephoneNumber	Phone	-
		mail	Email	-
		displayName	Name	-
		accountExpires	Account Expires	-
2.	Group	cn	Groups	-
3.	Machine	dNSHostName	HostName	-
		operatingSystem	OperatingSystem	-
		operatingSystemServicePack	OSServicePack	-
4.	Onboard Device Owner	memberOf	Onboard memberOf	-
5.	Onboard Device Owner Group	cn	Onboard Groups	-

5.2 ClearPass dot1x Service

Here we create a dot1x service for wireless access.

ClearPass Policy Manager

Configuration » Services

Services

This page shows the current list and order of services that ClearPass follows during authentication and authorization.

#	Order	Name	Type	Template	Status
1.	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	
2.	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	
3.	3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	
4.	4	[Guest Operator Logins]	Application	Aruba Application Authentication	
5.	5	[Insight Operator Logins]	Application	Aruba Application Authentication	
6.	6	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	
7.	7	AA Aruba 802.1X Wireless	RADIUS	Aruba 802.1X Wireless	

Summary | Service | Authentication | Roles | Enforcement

Name:	AA Aruba 802.1X Wireless
Description:	To authenticate users to an Aruba wireless network via 802.1X.
Type:	Aruba 802.1X Wireless
Status:	Enabled
Monitor Mode:	☐ Enable to monitor network access without enforcement
More Options:	☐ Authorization ☐ Posture Compliance ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

Service Rule

Matches ○ ANY or ◉ ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Radius:Aruba	Aruba-Essid-Name	EQUALS	school
4.	Click to add...			

"school" is the name of the SSID

Summary | Service | Authentication | Roles | Enforcement

Authentication Methods:	[EAP PEAP] [EAP TLS] Move Up ↑ / Move Down ↓ / Remove / View Details / Modify --Select to Add--
Authentication Sources:	Ariya AD [Active Directory] 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
Service Certificate:	--Select to Add--

Summary | Service | Authentication | Roles | Enforcement

Role Mapping Policy: --Select-- Modify Add New Role Mapping Policy

Role Mapping Policy Details	
Description:	-
Default Role:	-
Rules Evaluation Algorithm:	-

Conditions	Role

Summary | Service | Authentication | Roles | Enforcement

Use Cached Results:	☐ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	AA Aruba 802.1X Wireless Enforcement Policy Modify Add New Enforcement Policy

Enforcement Policy Details	
Description:	
Default Profile:	AA Aruba 802.1X Wireless Default Profile
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:Ariya AD:memberOf *CONTAINS* Staff)	AA-Aruba 802.1X Wireless Staff Profile, AA Aruba 802.1X Wireless Update Endpoint Location
2.	(Authorization:Ariya AD:memberOf *CONTAINS* Student)	AA-Aruba 802.1X Wireless Student Profile, AA Aruba 802.1X Wireless Update Endpoint Location
3.	(Tips:Role *EQUALS* [Machine Authenticated]) *AND* (Authorization:Ariya AD:memberOf *CONTAINS* Staff)	AA-Aruba 802.1X Wireless Staff Profile, [Update Endpoint Known]
4.	(Tips:Role *EQUALS* [Machine Authenticated]) *AND* (Authorization:Ariya AD:memberOf *CONTAINS* Studen)	AA-Aruba 802.1X Wireless Student Profile, [Update Endpoint Known]

And here are the enforcement profiles that are being used in the enforcement policy

- AA Aruba 802.1X Wireless Default Profile RADIUS
- AA-Aruba 802.1X Wireless Staff Profile RADIUS
- AA-Aruba 802.1X Wireless Student Profile RADIUS
- AA Aruba 802.1X Wireless Update Endpoint Location Post_Authentication

Enforcement Profiles - AA Aruba 802.1X Wireless Default Profile

Note: This Enforcement Profile is created by Service Template

Summary | Profile | Attributes

Profile:

Name:	AA Aruba 802.1X Wireless Default Profile
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Employee

Enforcement Profiles - AA-Aruba 802.1X Wireless Staff Profile

Note: This Enforcement Profile is created by Service Template

Summary | **Profile** | **Attributes**

Profile:

Name:	AA-Aruba 802.1X Wireless Staff Profile
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Staff

Enforcement Profiles - AA-Aruba 802.1X Wireless Student Profile

Note: This Enforcement Profile is created by Service Template

Summary | **Profile** | **Attributes**

Profile:

Name:	AA-Aruba 802.1X Wireless Student Profile
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Student

Enforcement Profiles - AA Aruba 802.1X Wireless Update Endpoint Location

Note: This Enforcement Profile is created by Service Template

Summary | **Profile** | **Attributes**

Profile:

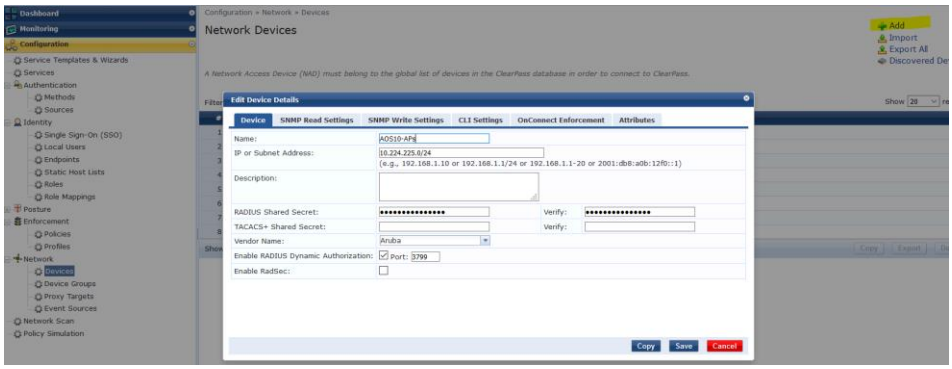
Name:	AA Aruba 802.1X Wireless Update Endpoint Location
Description:	
Type:	Post_Authentication
Action:	
Device Group List:	-

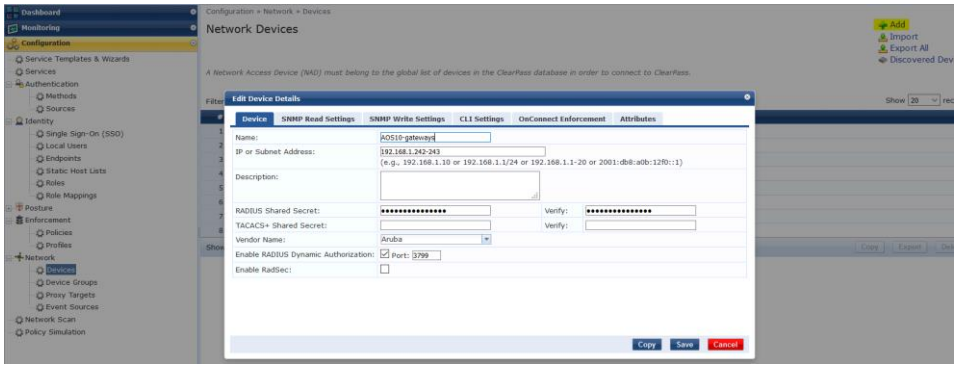
Attributes:

	Type	Name		Value
1.	Endpoint	Last Known Location	=	%{Radius:IETF:NAS-IP-Address}:%{Radius:Aruba:Aruba-Location-Id}

5.3 NAD Configuration

Here we are adding Network Access Devices (NAD). This will be the AOS10 APs and gateways. Note that you need to either add the AP IP addresses individually or just add their subnet as I have done here.

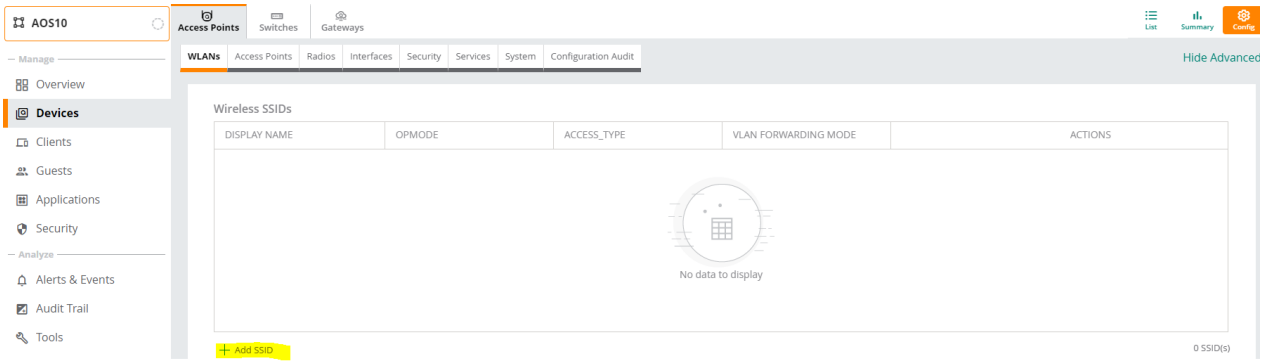


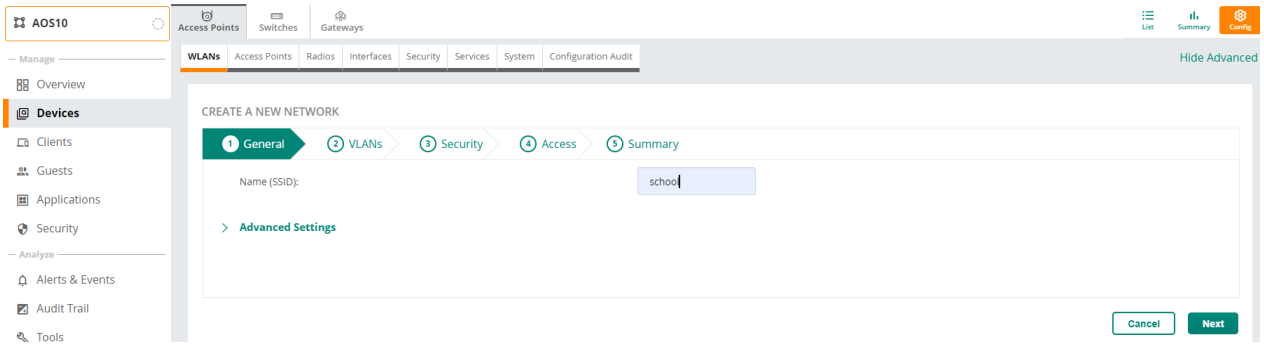


6 WLAN Configuration

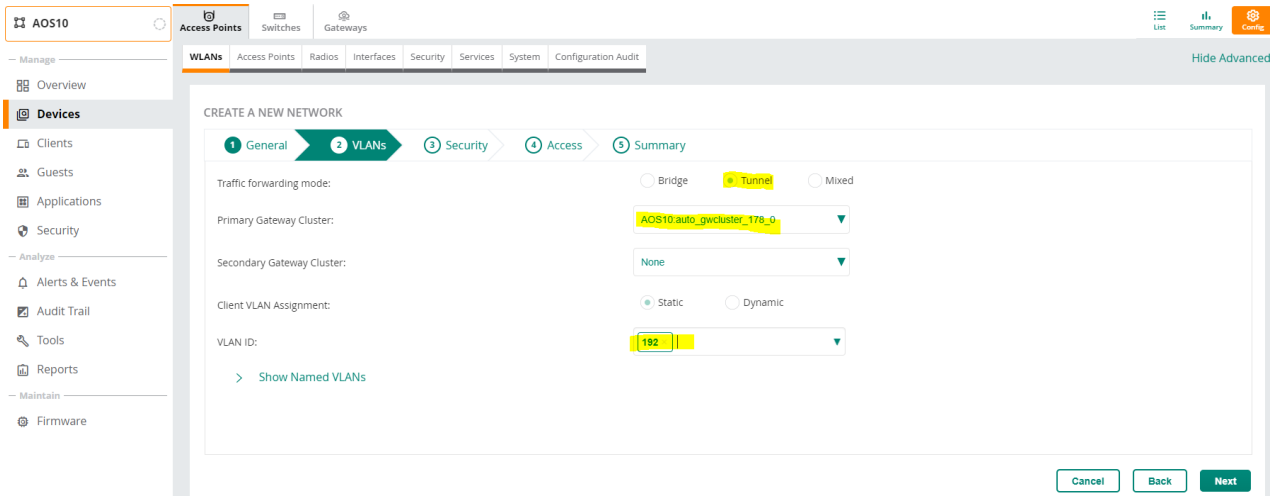
Here we'll configure the AOS10 APs to broadcast a tunnelled SSID. This is done at the group level.

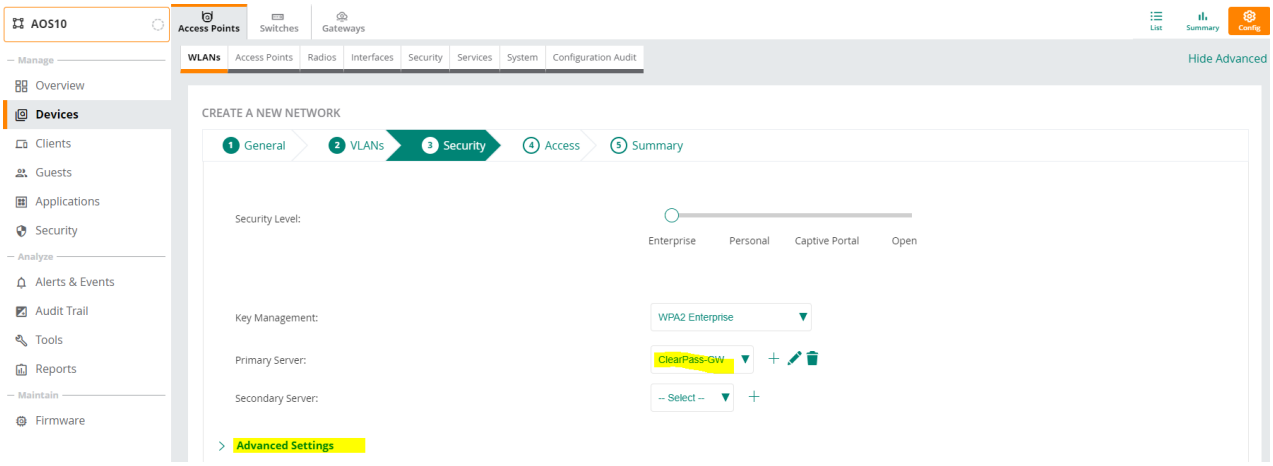
6.1 Tunnelled Wireless Configuration



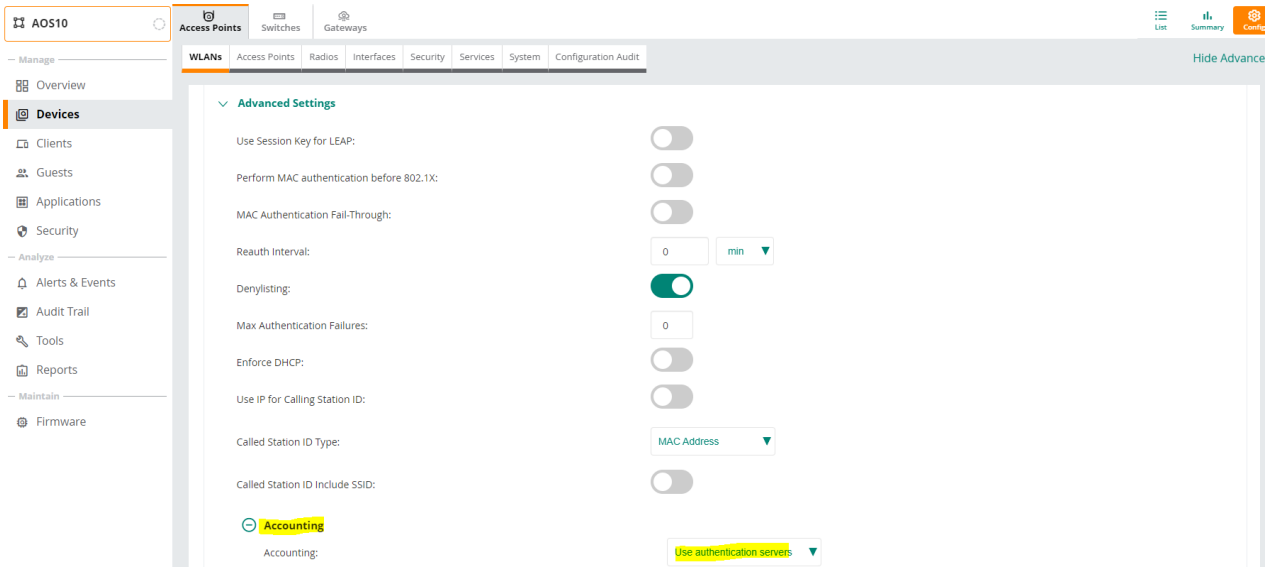


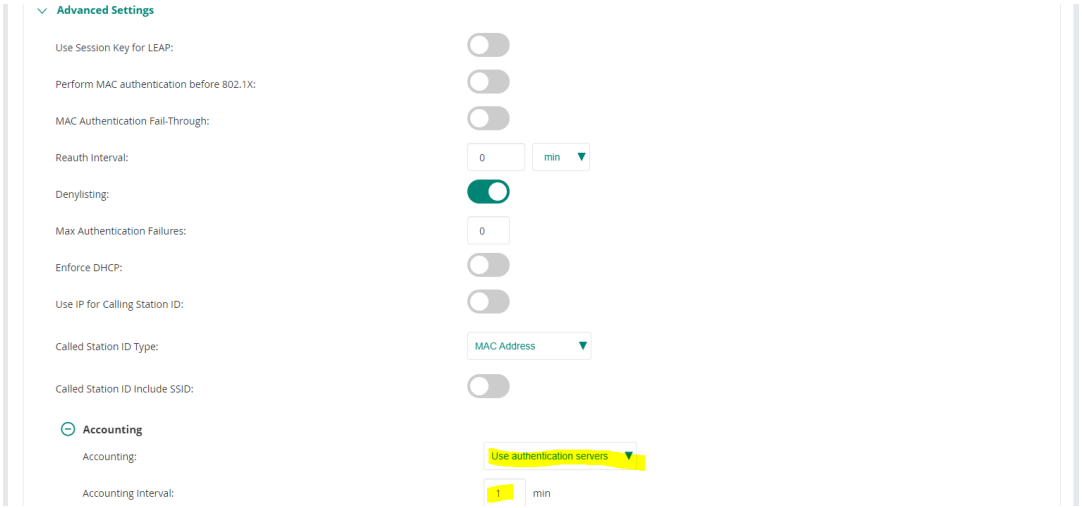
You can choose the cluster from the menu. Also note that the VLAN IDs are being displayed from the gateways.

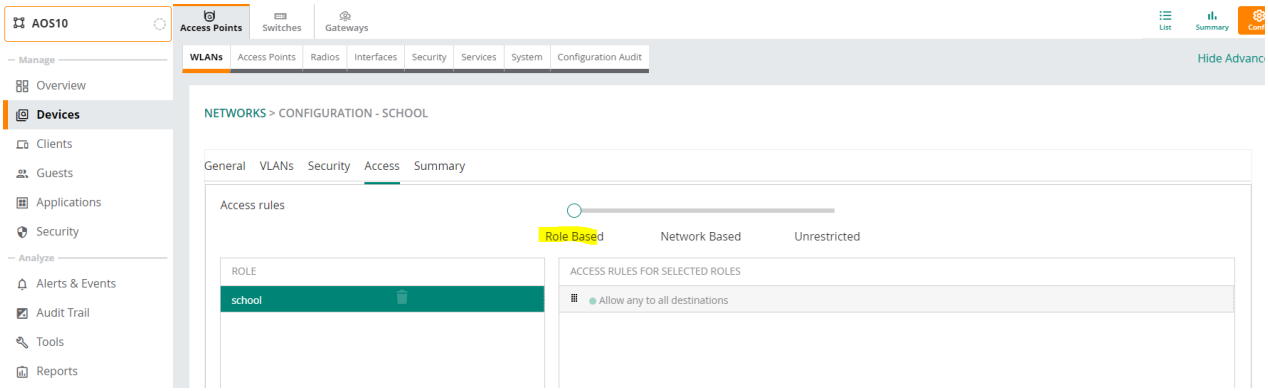




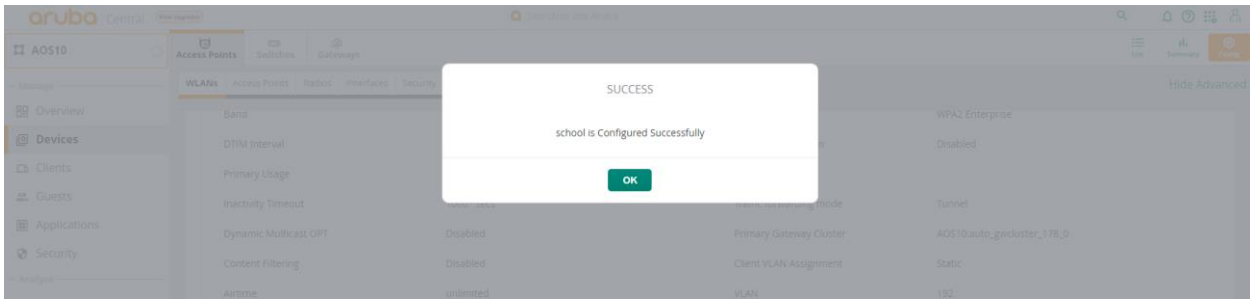
Select the authentication server that we had configured on the gateways. It gets automatically populated using the drop down menu. Note that this is not the RADIUS server that we configured in the AP group but rather from the gateway group. Next select Accounting from the advance Setting section





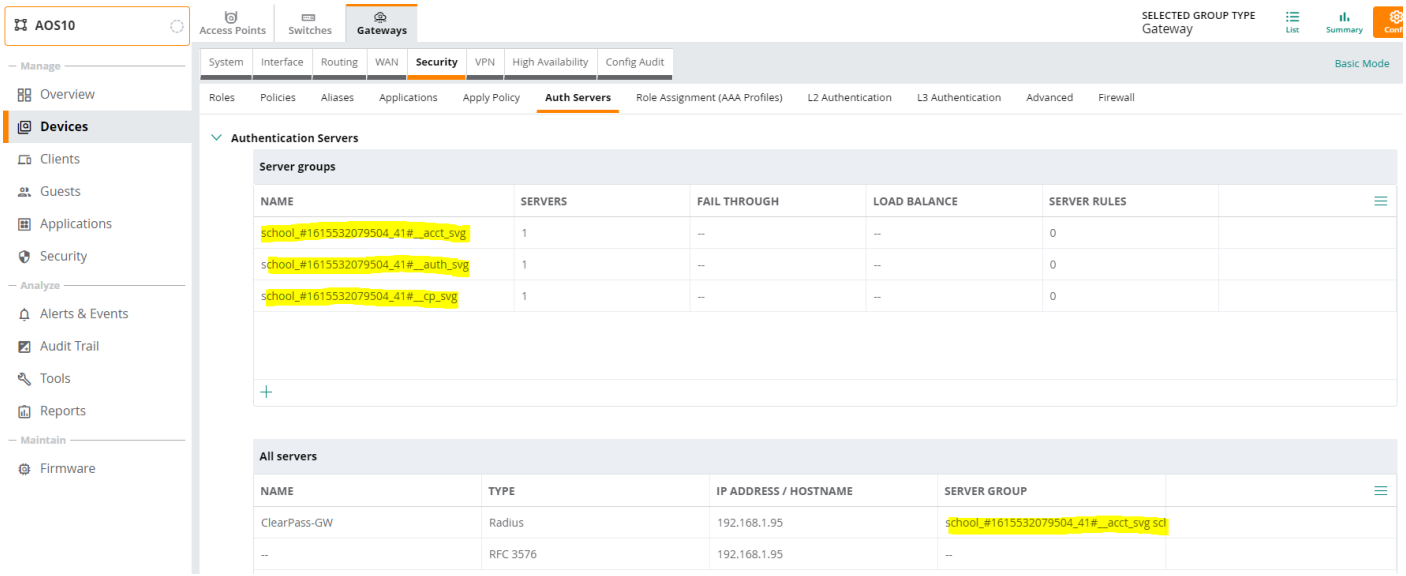


And save the configuration.

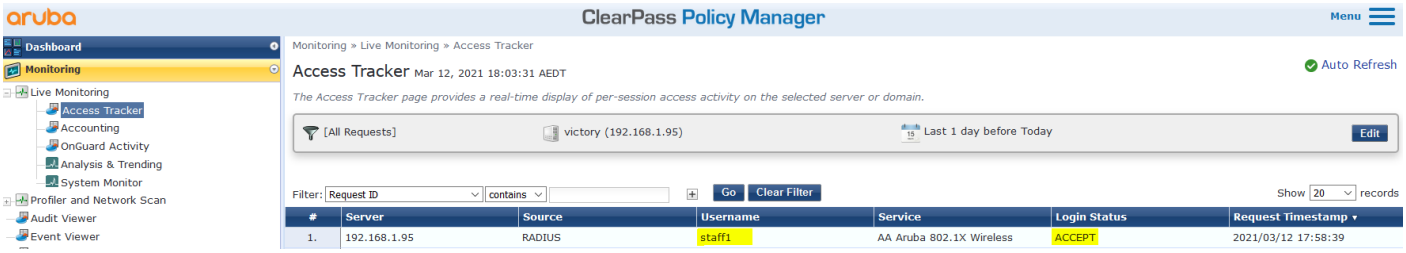


6.2 Wireless dot1x Testing

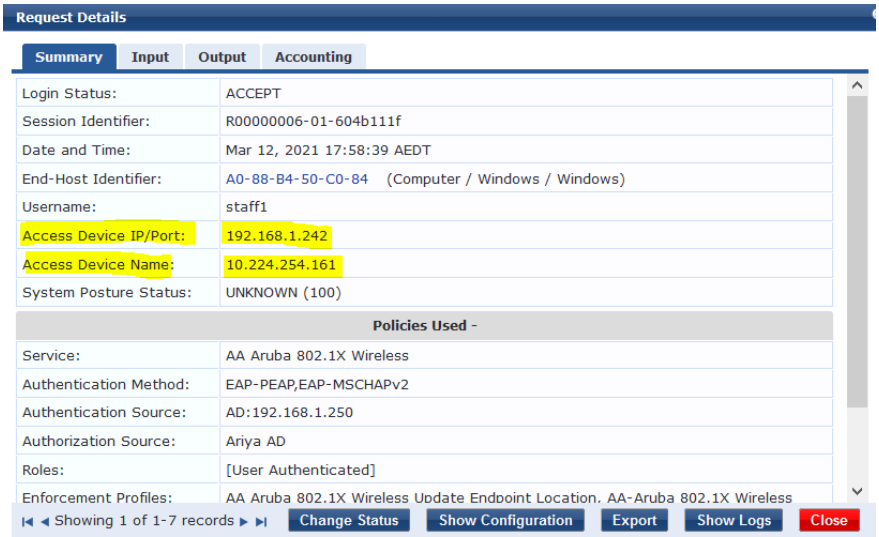
First, we'll check the gateway authentication server configuration, the highlighted lines were pushed form the AP's tunnel configuration.

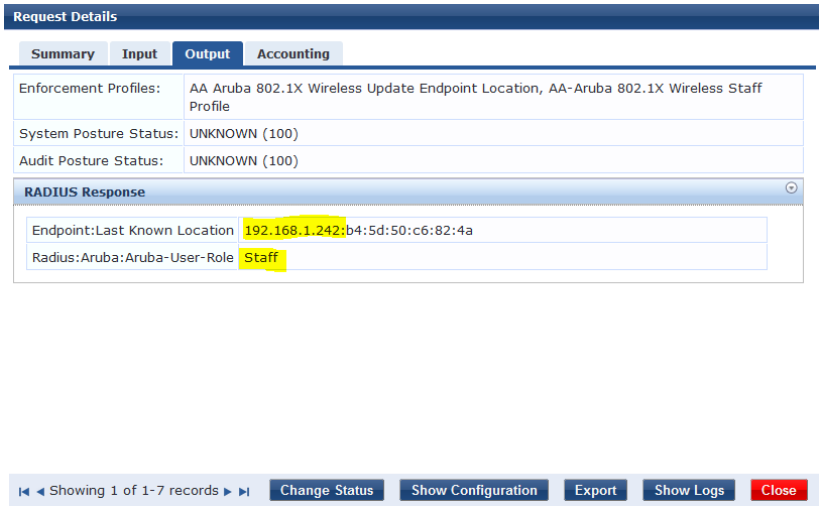


Now we'll get a laptop to connect to "school" SSID with staff1 user credentials and check ClearPass access tracker

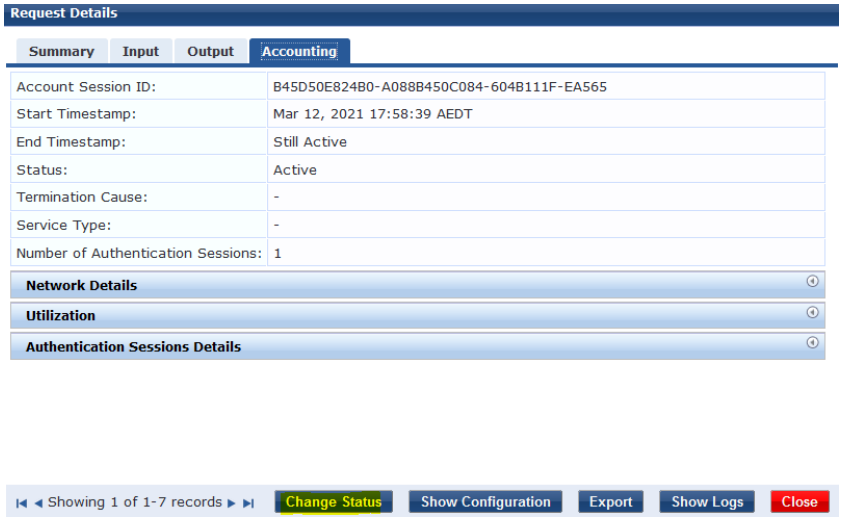


Note that 192.168.1.242 is the IP address of the gateway-1 and 10.224.254.161 is the IP address of the AP.

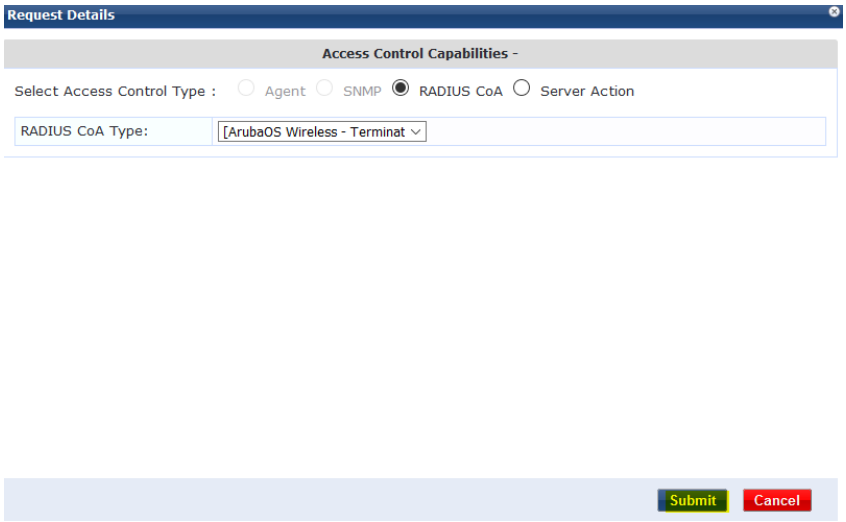




And we also have the accounting tab, which indicates RADIUS accounting is working



Lastly, we need to test if CoA is working, click on the “change status” to terminate the session



Request Details

Radius [ArubaOS Wireless - Terminate Session] successful for client a088b450c084.

Summary | Input | Output | Accounting

Account Session ID:	B45D50E824B0-A088B450C084-604B111F-EA565
Start Timestamp:	Mar 12, 2021 17:58:39 AEDT
End Timestamp:	Still Active
Status:	Active
Termination Cause:	-
Service Type:	-
Number of Authentication Sessions:	1

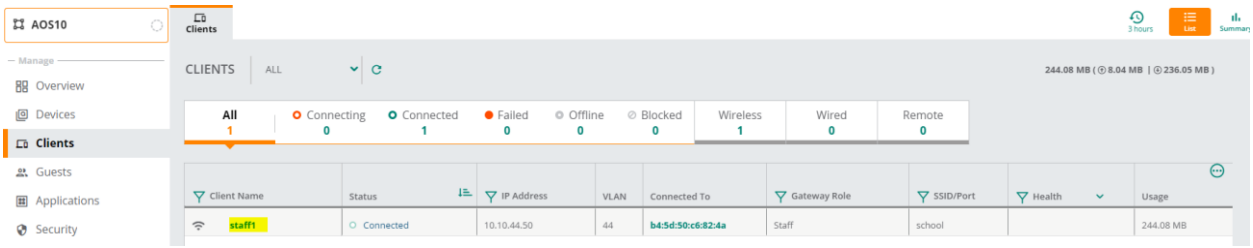
Network Details

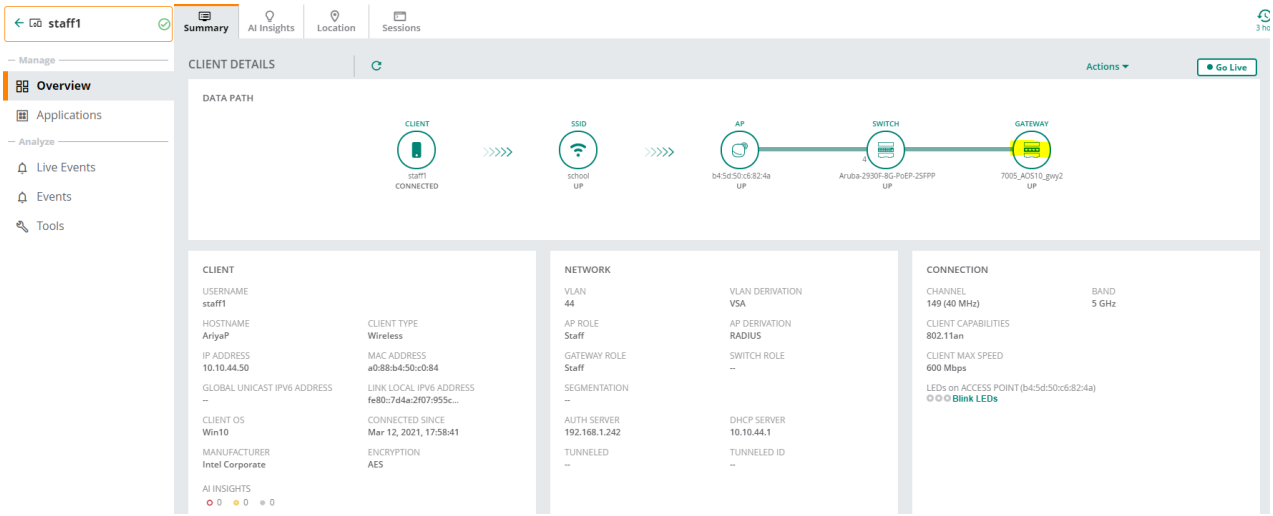
Utilization

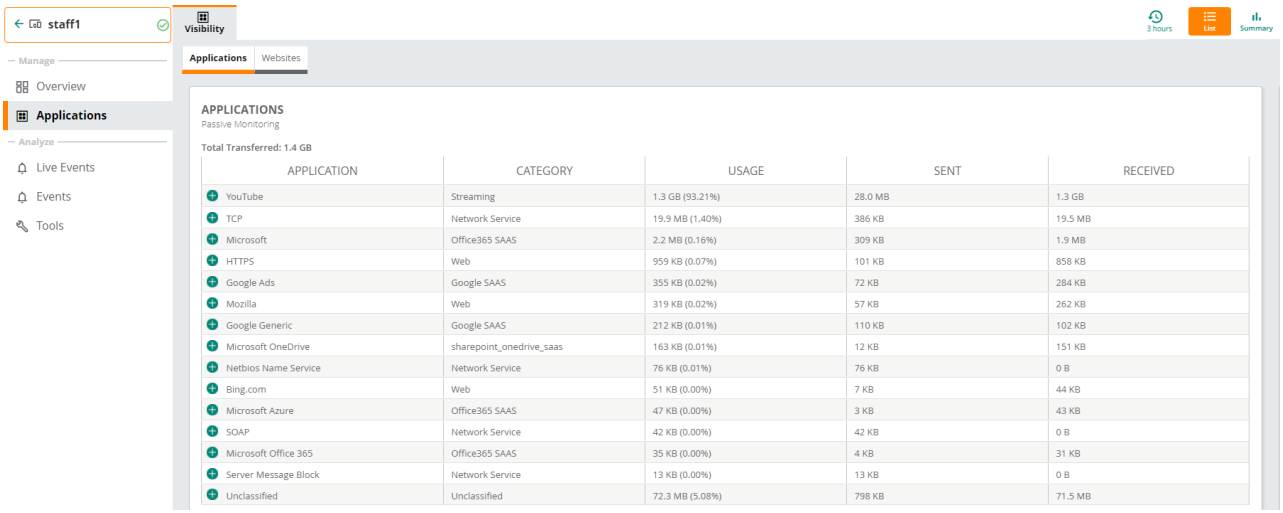
Authentication Sessions Details

Showing 1 of 1-7 records | Change Status | Show Configuration | Export | Show Logs | Close

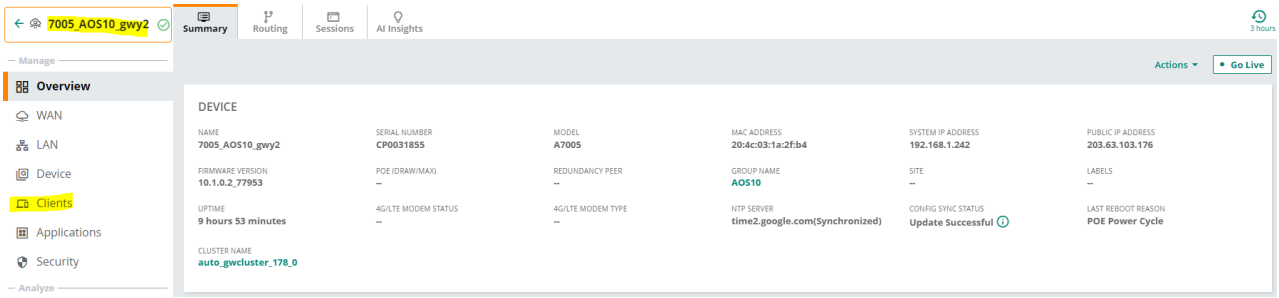
Now looking at Aruba Central pages.

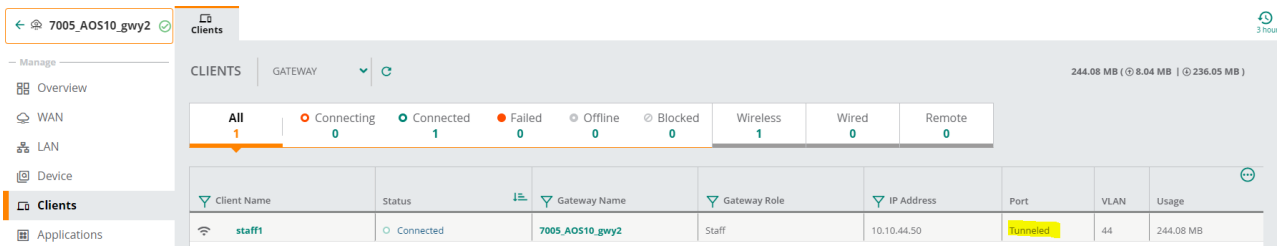






Clicking on the gateway symbol takes us to the gateway that is terminating the user traffic





Now we'll run a few CLI commands.

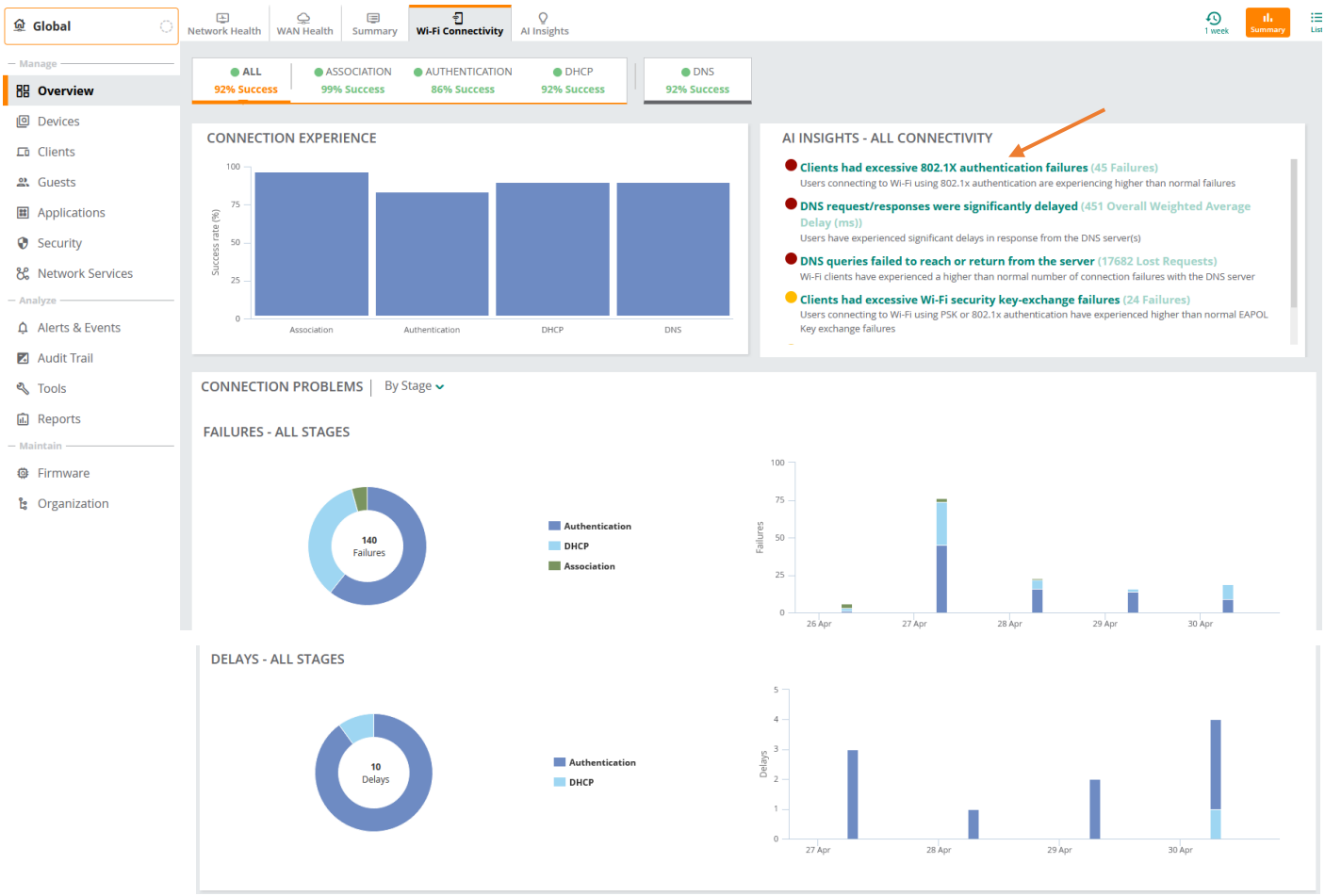
```
b4:5d:50:c6:82:4a# sh ap bss-table

Aruba AP BSS Table
------------------
bss                ess                    port  ip              phy    type  ch/EIRP/max-EIRP  cur-cl  ap name            in-t(s)  tot-t
flags
---                ---                    ----  --              ---    ----  ----------------  ------  -------           -------  -----      --
---
b4:5d:50:e8:24:b0  school                 ?/?   10.224.254.161  a-VHT  ap    36E/15.0/21.5     1       b4:5d:50:c6:82:4a  0        1h:2m:16s
b4:5d:50:e8:24:b1  Guest                  ?/?   10.224.254.161  a-VHT  ap    36E/15.0/21.5     1       b4:5d:50:c6:82:4a  0        4m:29s     o
b4:5d:50:e8:24:b2  _owetm_Guest2874425900 ?/?   10.224.254.161  a-VHT  ap    36E/15.0/21.5     0       b4:5d:50:c6:82:4a  0        4m:28s     WO
b4:5d:50:e8:24:a0  school                 ?/?   10.224.254.161  g-HT   ap    3/7.5/21.5        0       b4:5d:50:c6:82:4a  0        1h:2m:15s
b4:5d:50:e8:24:a1  Guest                  ?/?   10.224.254.161  g-HT   ap    3/7.5/21.5        0       b4:5d:50:c6:82:4a  0        4m:29s     o
b4:5d:50:e8:24:a2  _owetm_Guest2874425900 ?/?   10.224.254.161  g-HT   ap    3/7.5/21.5        0       b4:5d:50:c6:82:4a  0        4m:28s     WO

Channel followed by "*" indicates channel selected due to unsupported configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:6
Num Associations:2

Flags:       K = 802.11K Enabled; W = 802.11W Enabled; 3 = WPA3 BSS; O = Enhanced-open BSS with transition mode; o = Enhanced-open transition
mode open BSS; M = WPA3-SAE mixed mode BSS; E = Enhanced-open BSS without transition mode; m = Agile Multiband (MBO) BSS; c = MBO Cellular Data
Capable BSS; I = Imminent VAP Down; T = Individual TWT Enabled; t = Broadcast TWT Enabled
b4:5d:50:c6:82:4a#
```

checking the IPSEC tunnels from the AP

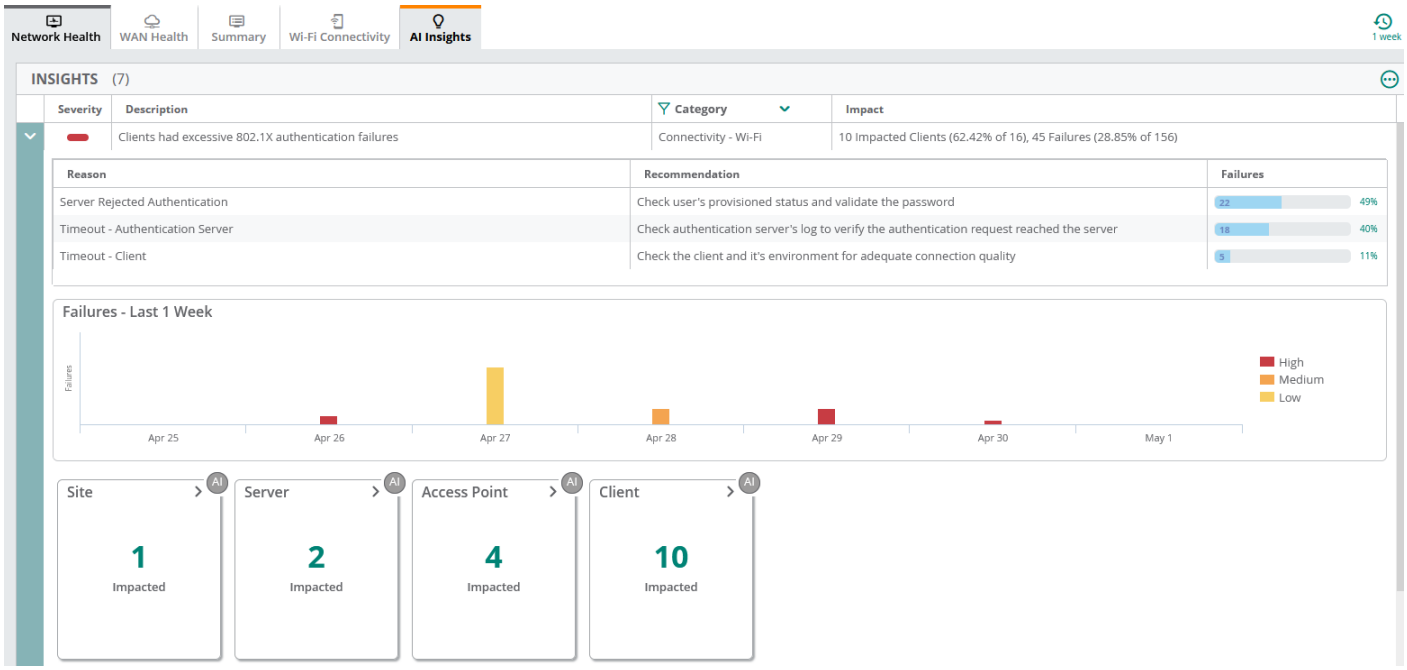
```
b4:5d:50:c6:82:4a# sh ata endpoint

ATA Endpoint Status
-------------------
UUID                                   IP ADDR        STATE               TUN DEV  TUN SPI(OUT/IN)    PORT(SRC/DST)  VALID TIME(s)  TUNNEL TYPE
GRE VLANs          HBT(Jiff/Missed/Sent/Rcv)  INNER IP        UP TIME(s)
----                                   -------        -----               -------  ---------------    -------------  -------------  -----------  -
--------           ------------------------  --------        ----------
522d59ab-05d0-43b6-ab49-177e49fb7bb0   192.168.1.242  SM_STATE_CONNECTED  tun0     1ad1b900/c6d09100  4500/4500      125781         GRE
1,33,44,192,4094   3999/0/3808/3808          10.224.254.161  2021-03-13 08:28:59
5bb2c1da-f402-4afa-af39-c09d4aafa946   192.168.1.243  SM_STATE_CONNECTED  tun1     92607100/969f6100  4500/4500      125783         GRE
1,33,44,192,4094   3999/0/3807/3807          10.224.254.161  2021-03-13 08:29:01
Total Endpoints Count: 2
b4:5d:50:c6:82:4a#
```

7 RF Monitoring

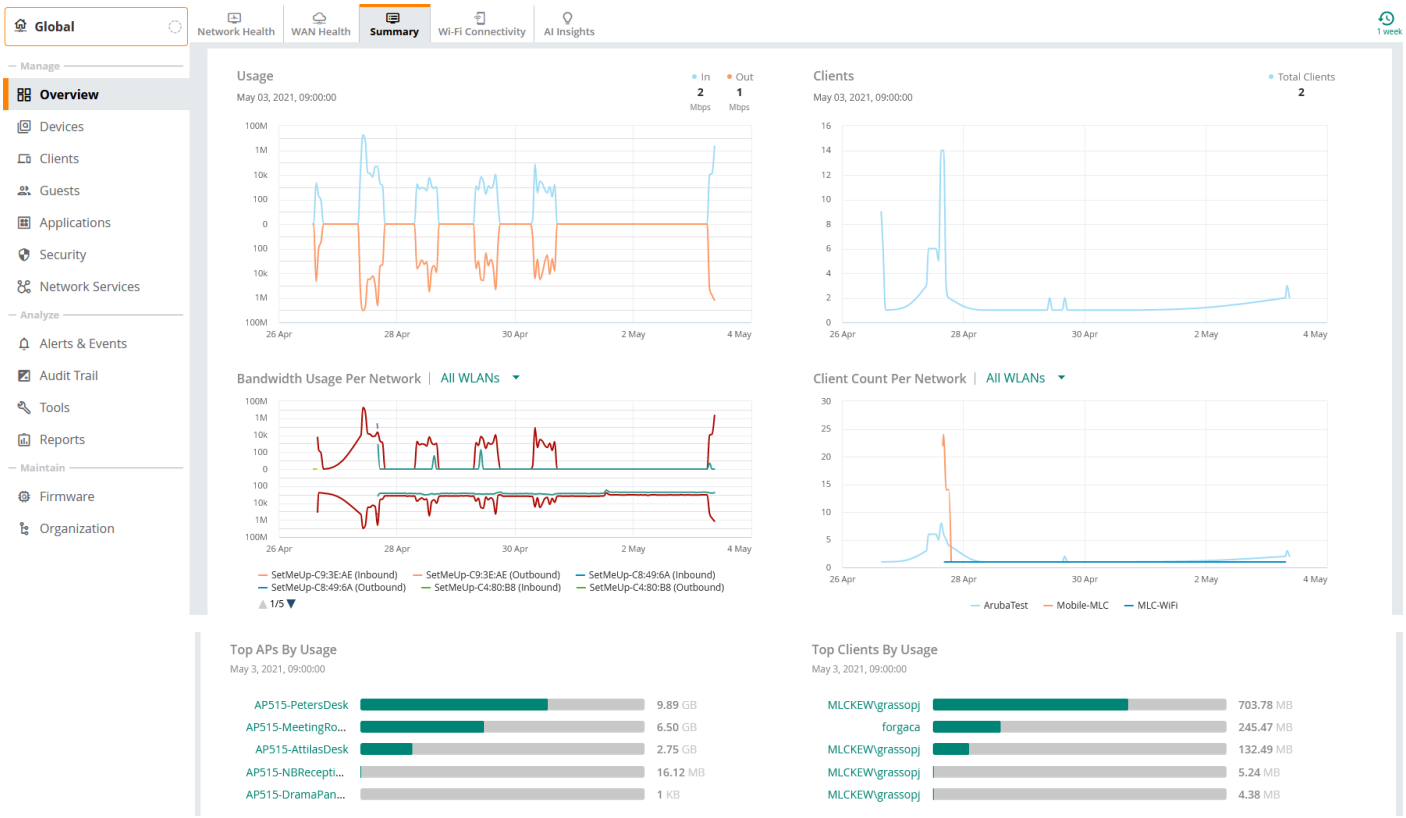
Here we'll just touch on some of the RF mgmt. info that are available in Central. To start with at the global level, you can check the WiFi connectivity and then drill down on any specifics, like AI insights, associations, authentication , etc.



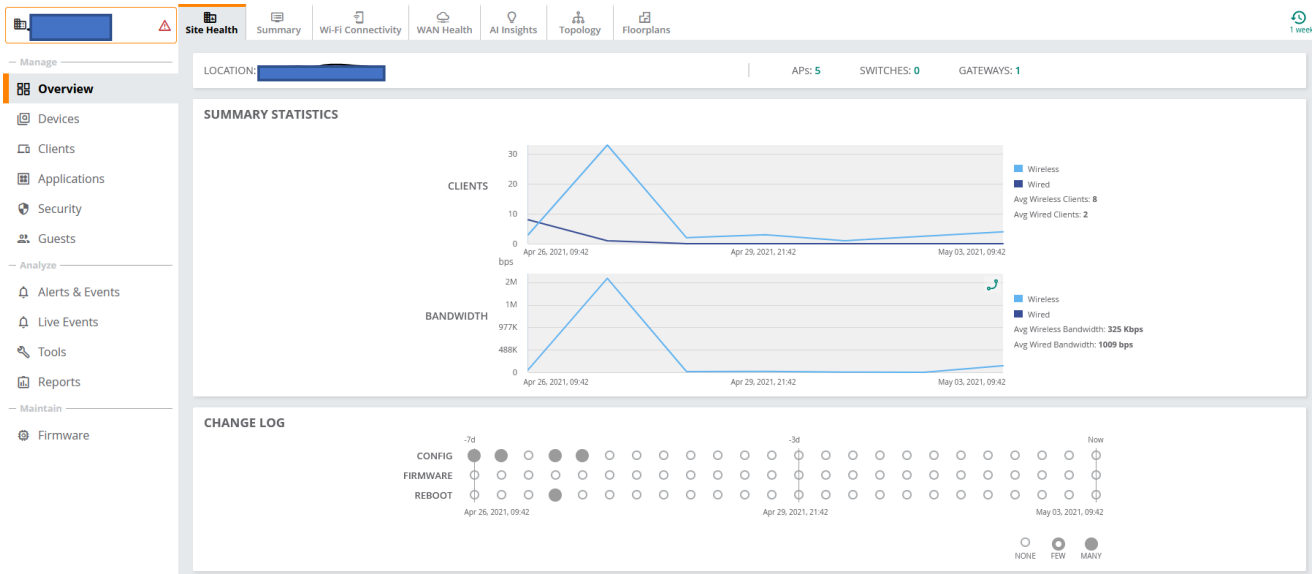
Clicking on "clients had excessive 802.1.x failures"

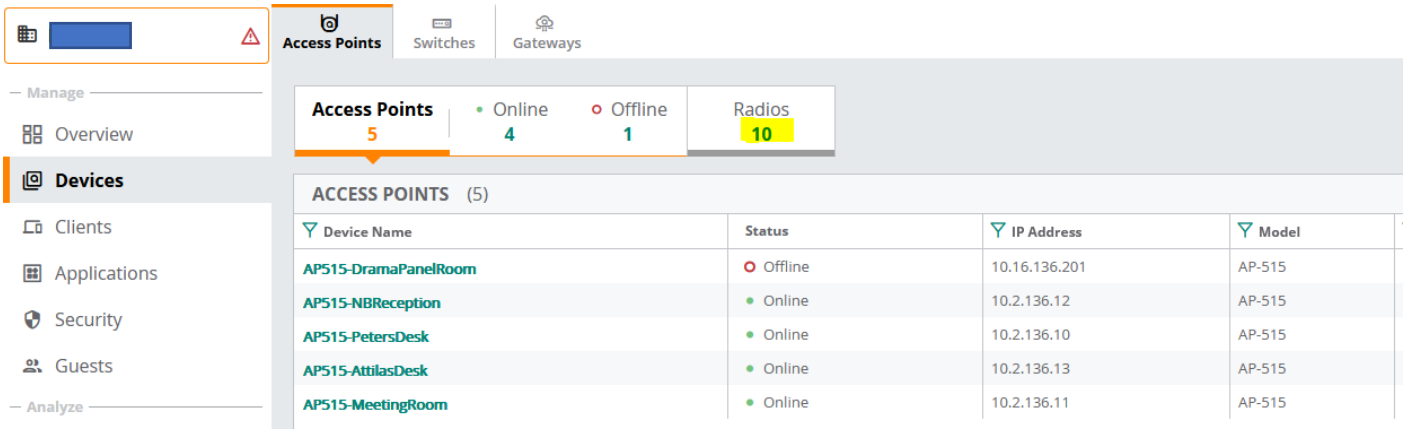


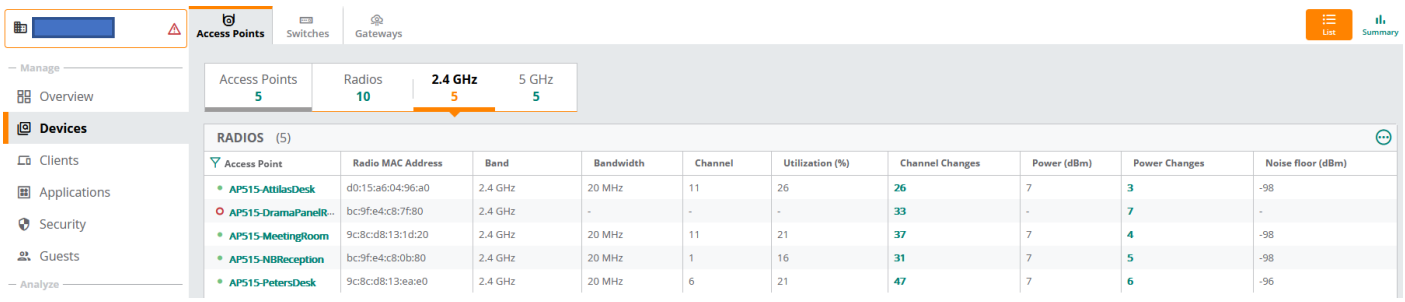
Next, we can check the usage summary



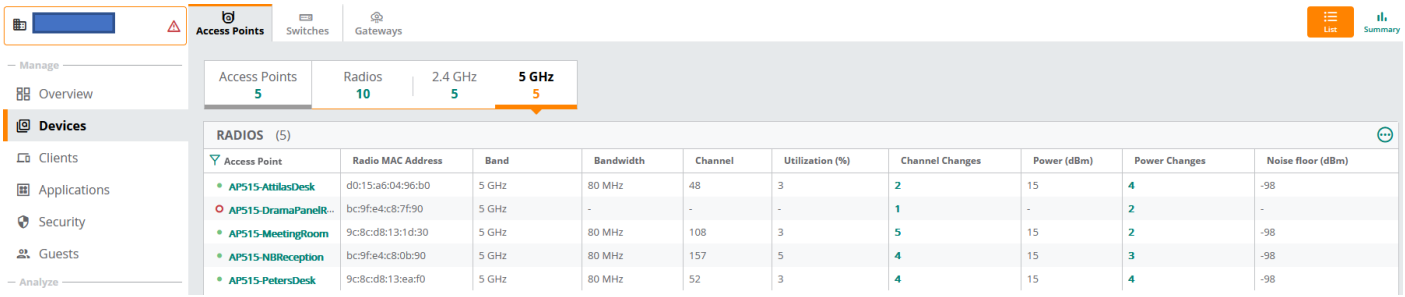
We can then go to the Site level and see some of the stats



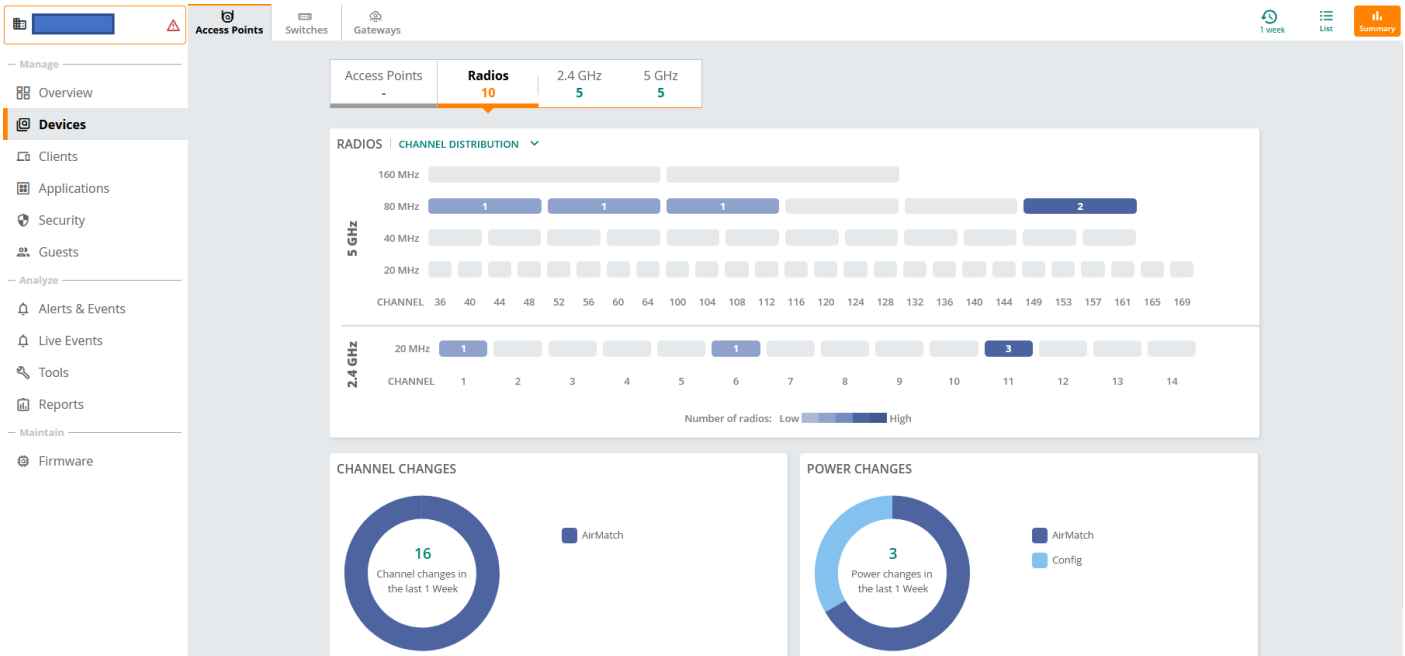




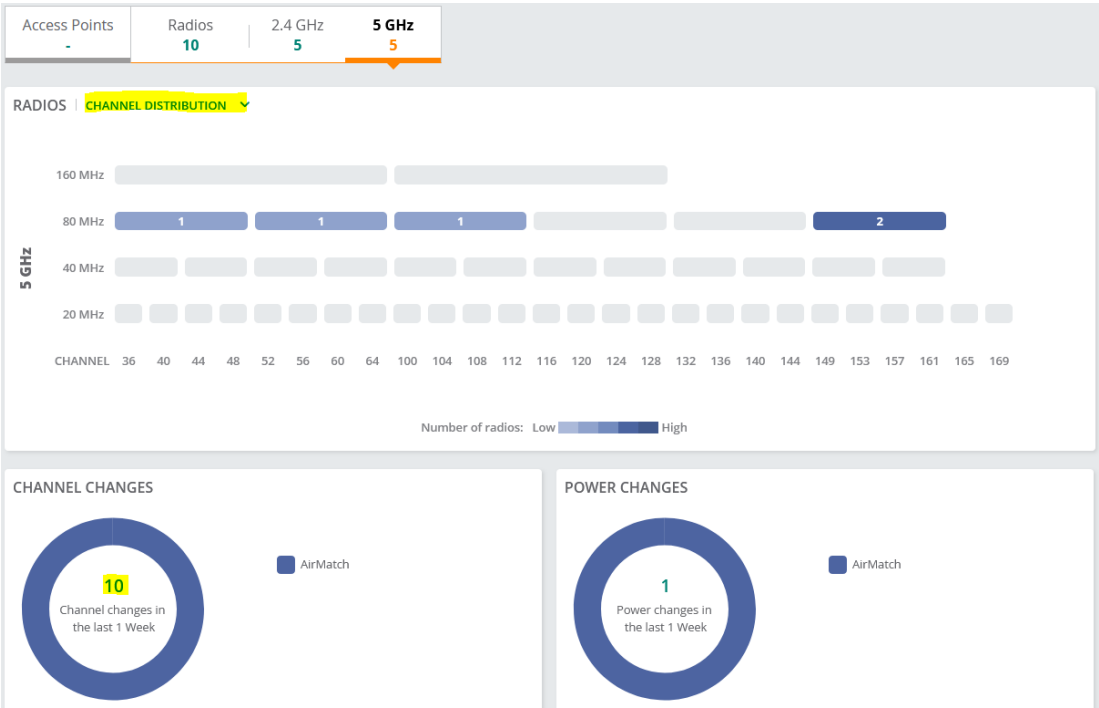
Access Point	Radio MAC Address	Band	Bandwidth	Channel	Utilization (%)	Channel Changes	Power (dBm)	Power Changes	Noise floor (dBm)
AP515-AttilasDesk	d0:15:a6:04:96:a0	2.4 GHz	20 MHz	11	26	26	7	3	-98
AP515-DramaPanelR...	bc:9f:e4:c8:7f:80	2.4 GHz	-	-	-	33	-	7	-
AP515-MeetingRoom	9c:8c:d8:13:1d:20	2.4 GHz	20 MHz	11	21	37	7	4	-98
AP515-NBReception	bc:9f:e4:c8:0b:80	2.4 GHz	20 MHz	1	16	31	7	5	-98
AP515-PetersDesk	9c:8c:d8:13:ea:e0	2.4 GHz	20 MHz	6	21	47	7	6	-96

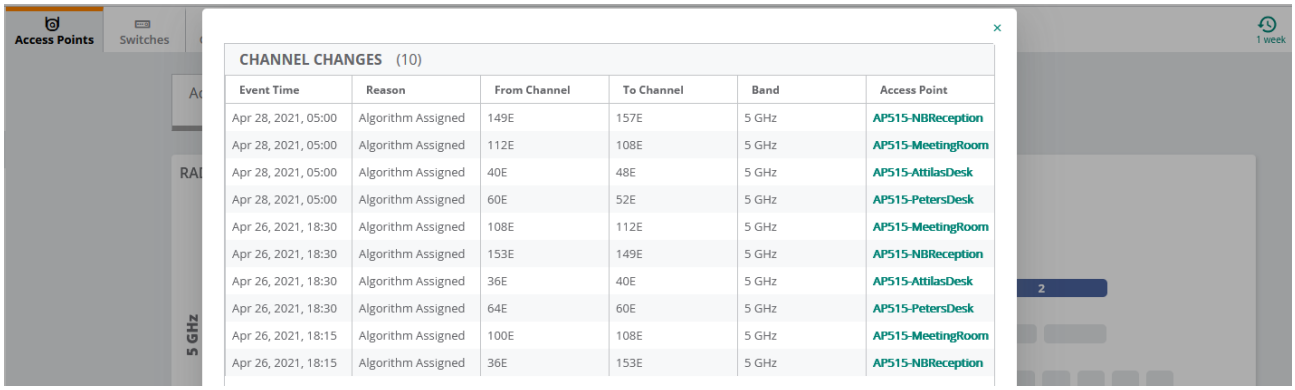


Access Point	Radio MAC Address	Band	Bandwidth	Channel	Utilization (%)	Channel Changes	Power (dBm)	Power Changes	Noise floor (dBm)
AP515-AttilasDesk	d0:15:a6:04:96:b0	5 GHz	80 MHz	48	3	2	15	4	-98
AP515-DramaPanelR...	bc:9f:e4:c8:7f:90	5 GHz	-	-	-	1	-	2	-
AP515-MeetingRoom	9c:8c:d8:13:1d:30	5 GHz	80 MHz	108	3	5	15	2	-98
AP515-NBReception	bc:9f:e4:c8:0b:90	5 GHz	80 MHz	157	5	4	15	3	-98
AP515-PetersDesk	9c:8c:d8:13:ea:f0	5 GHz	80 MHz	52	3	4	15	4	-98



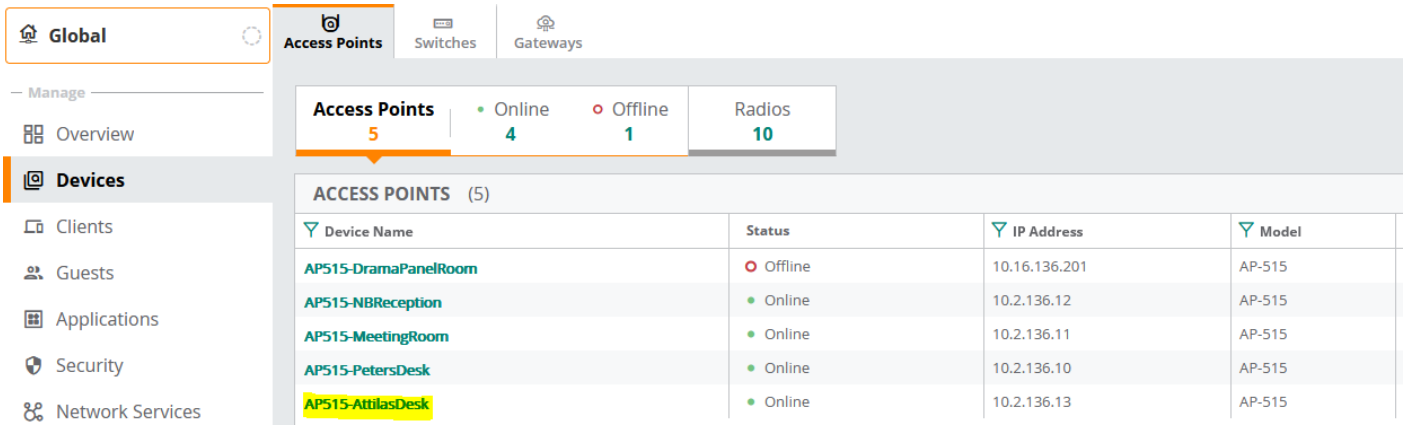
Looking at 5GHz band



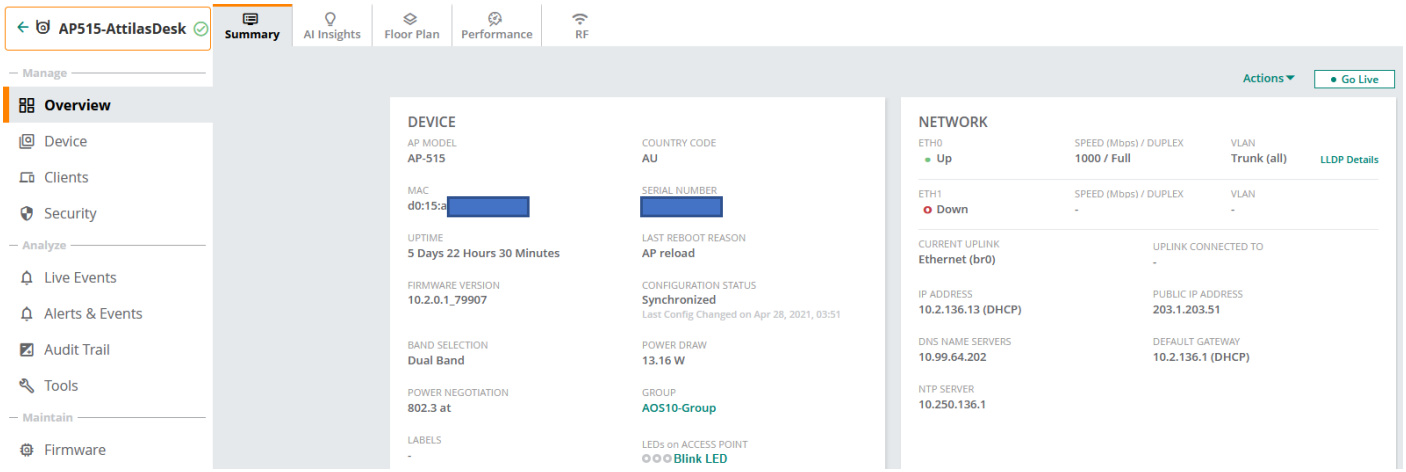


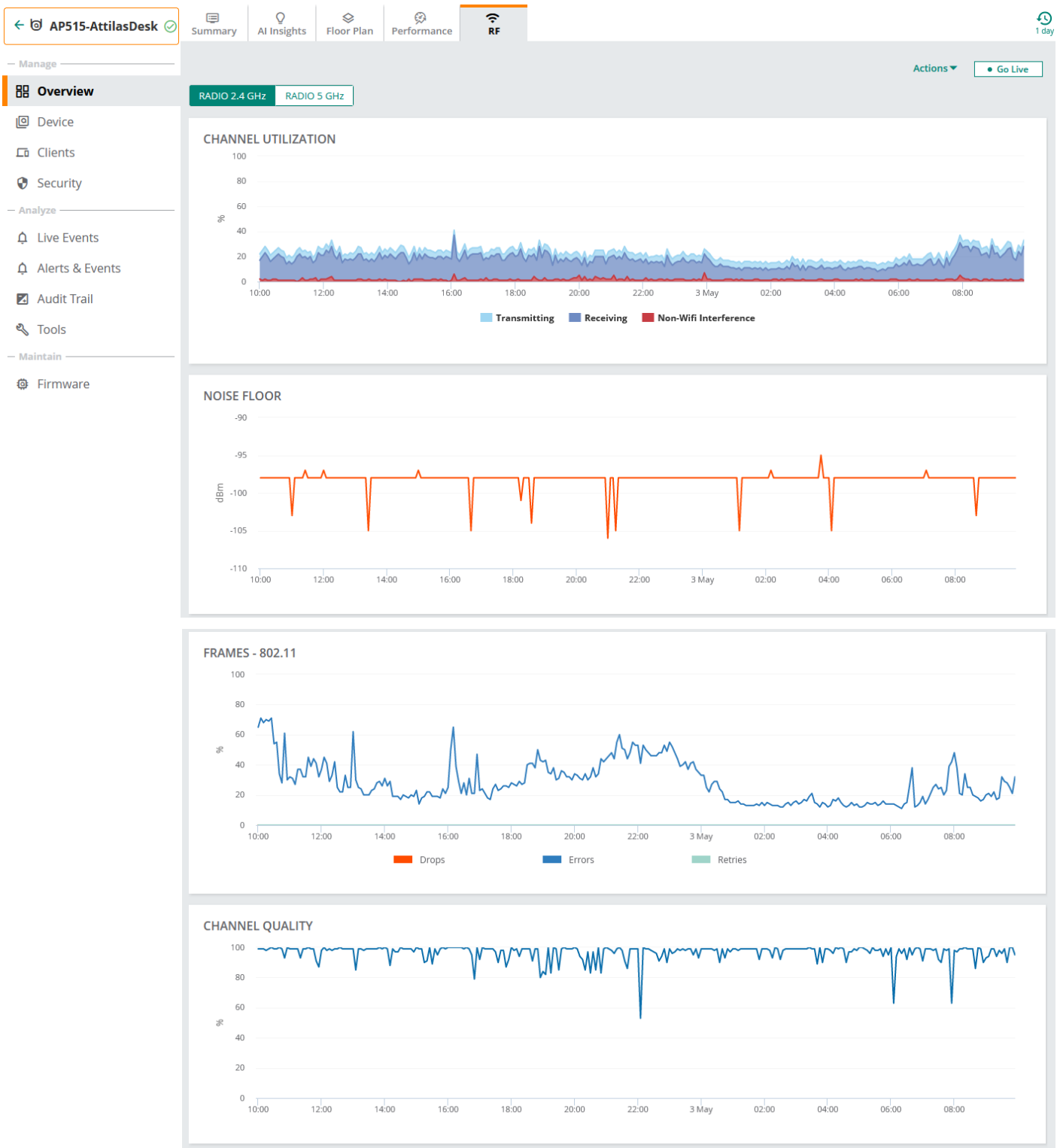
Event Time	Reason	From Channel	To Channel	Band	Access Point
Apr 28, 2021, 05:00	Algorithm Assigned	149E	157E	5 GHz	AP515-NBReception
Apr 28, 2021, 05:00	Algorithm Assigned	112E	108E	5 GHz	AP515-MeetingRoom
Apr 28, 2021, 05:00	Algorithm Assigned	40E	48E	5 GHz	AP515-AttilasDesk
Apr 28, 2021, 05:00	Algorithm Assigned	60E	52E	5 GHz	AP515-PetersDesk
Apr 26, 2021, 18:30	Algorithm Assigned	108E	112E	5 GHz	AP515-MeetingRoom
Apr 26, 2021, 18:30	Algorithm Assigned	153E	149E	5 GHz	AP515-NBReception
Apr 26, 2021, 18:30	Algorithm Assigned	36E	40E	5 GHz	AP515-AttilasDesk
Apr 26, 2021, 18:30	Algorithm Assigned	64E	60E	5 GHz	AP515-PetersDesk
Apr 26, 2021, 18:15	Algorithm Assigned	100E	108E	5 GHz	AP515-MeetingRoom
Apr 26, 2021, 18:15	Algorithm Assigned	36E	153E	5 GHz	AP515-NBReception

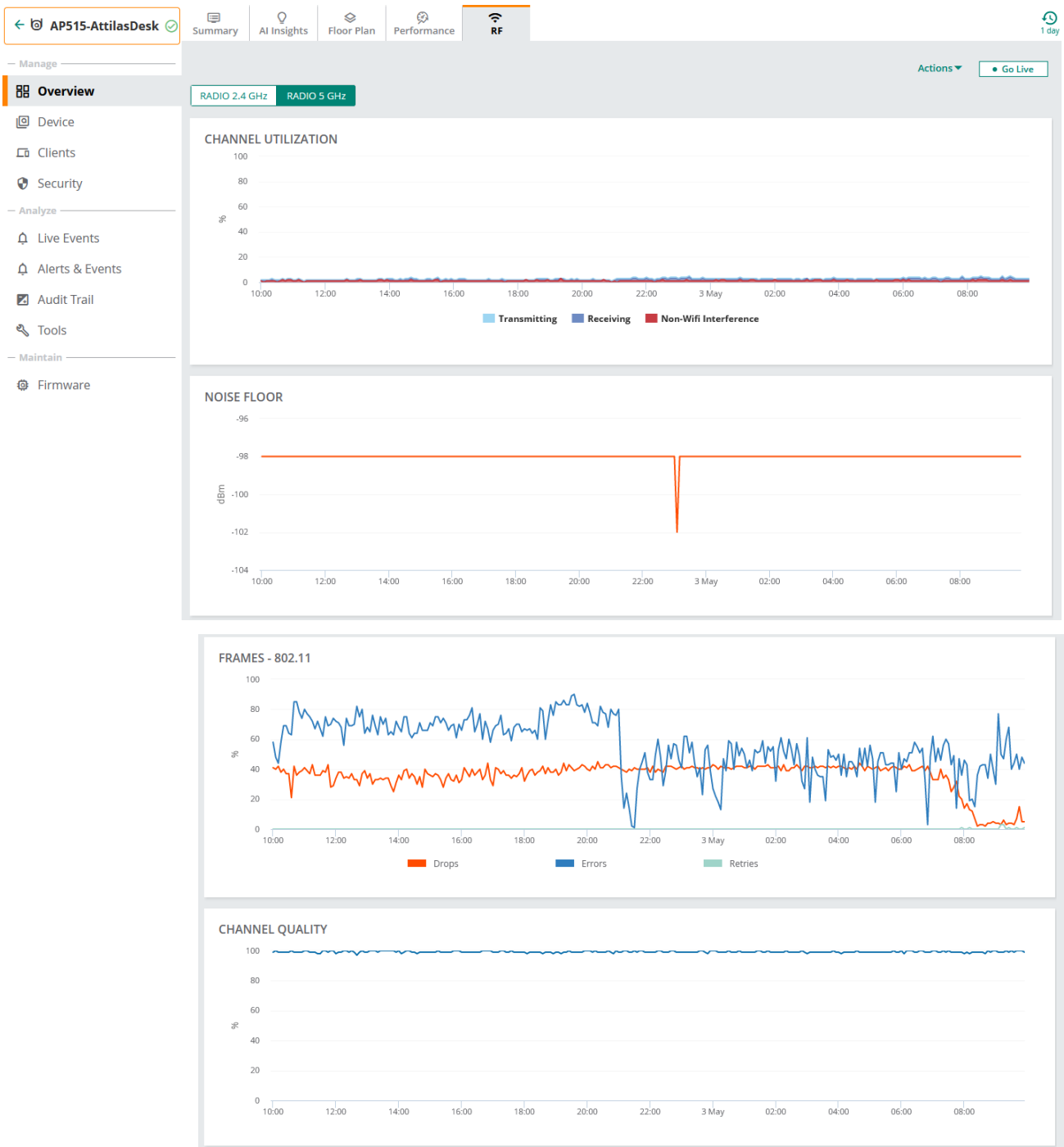
Next, we can have a look at the Live view, for that we'll choose a specific AP.



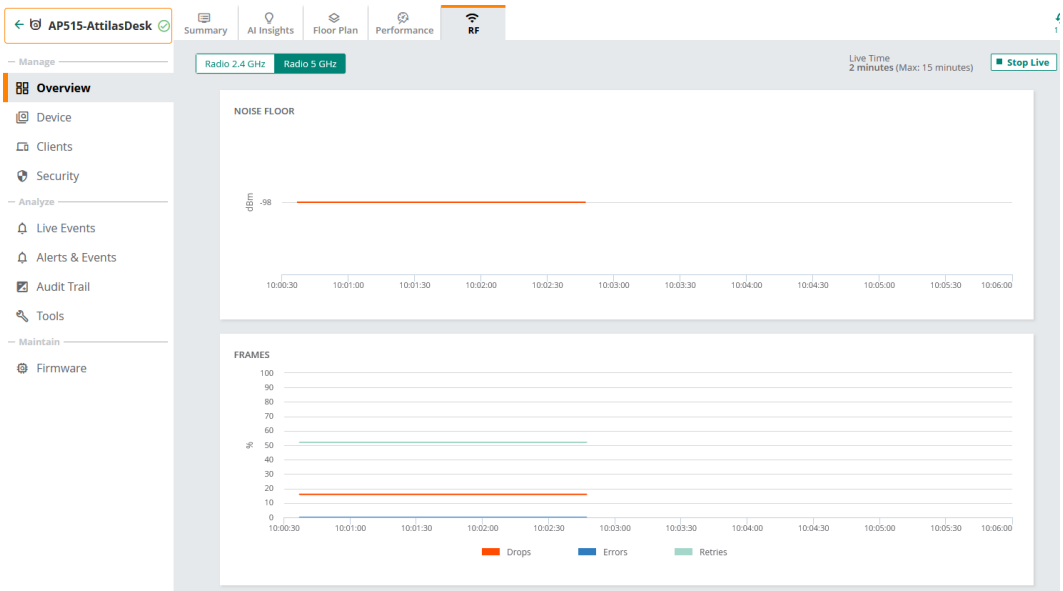
Device Name	Status	IP Address	Model
AP515-DramaPanelRoom	Offline	10.16.136.201	AP-515
AP515-NBReception	Online	10.2.136.12	AP-515
AP515-MeetingRoom	Online	10.2.136.11	AP-515
AP515-PetersDesk	Online	10.2.136.10	AP-515
AP515-AttilasDesk	Online	10.2.136.13	AP-515




AP515-AttilasDesk
Summary
AI Insights
Floor Plan
Performance
RF
1 day
Manage
Overview
Device
Clients
Security
Analyze
Live Events
Alerts & Events
Audit Trail
Tools
Maintain
Firmware
Actions
Go Live
RADIO 2.4 GHz
RADIO 5 GHz
CHANNEL UTILIZATION
%
Transmitting
Receiving
Non-Wifi Interference
NOISE FLOOR
dBm
FRAMES - 802.11
Drops
Errors
Retries
CHANNEL QUALITY



Now you can click on go live to get real-time view of the RF counter for 15min.

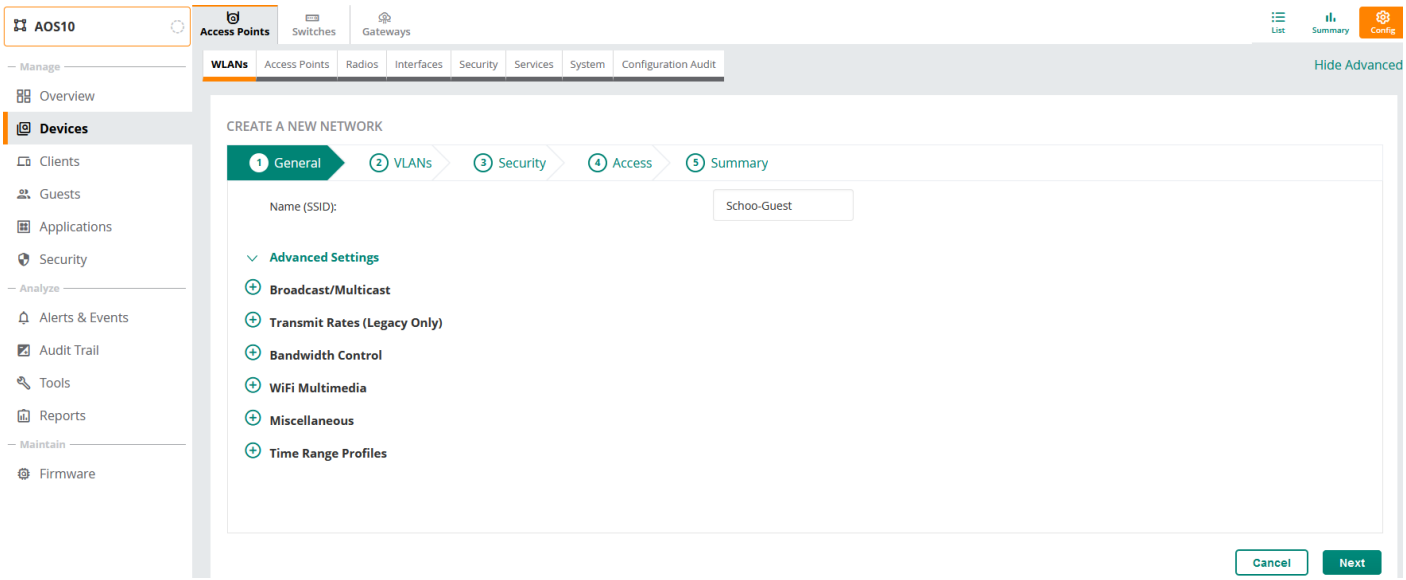


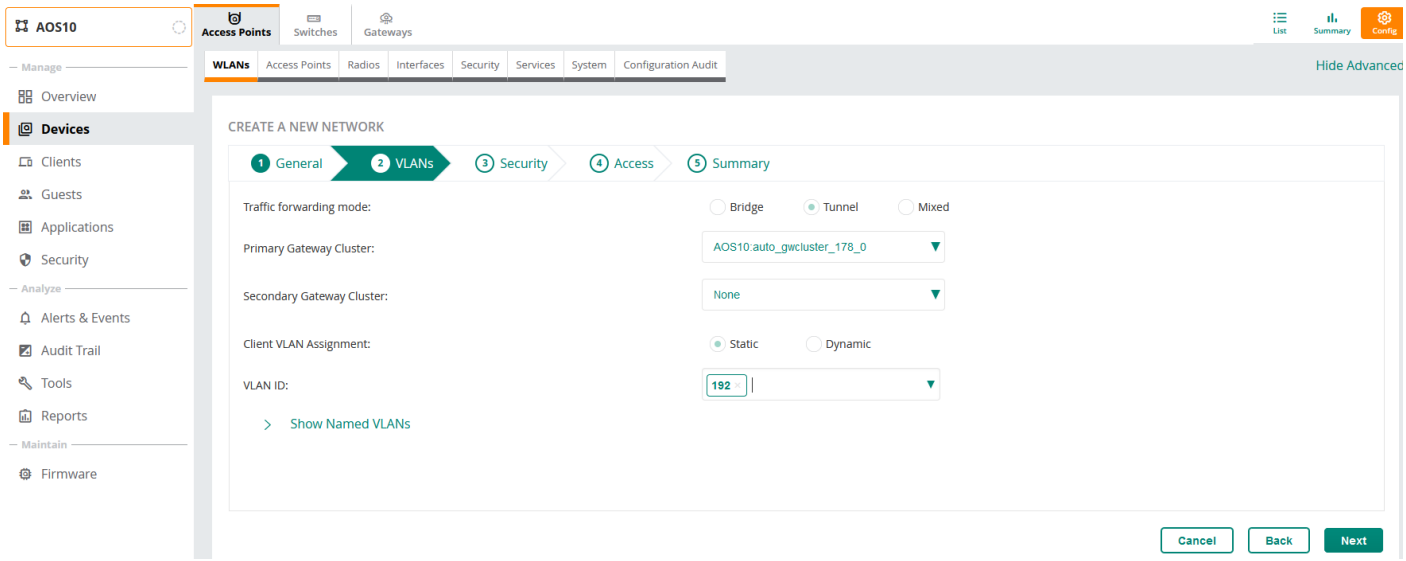
8 Guest Access Configuration

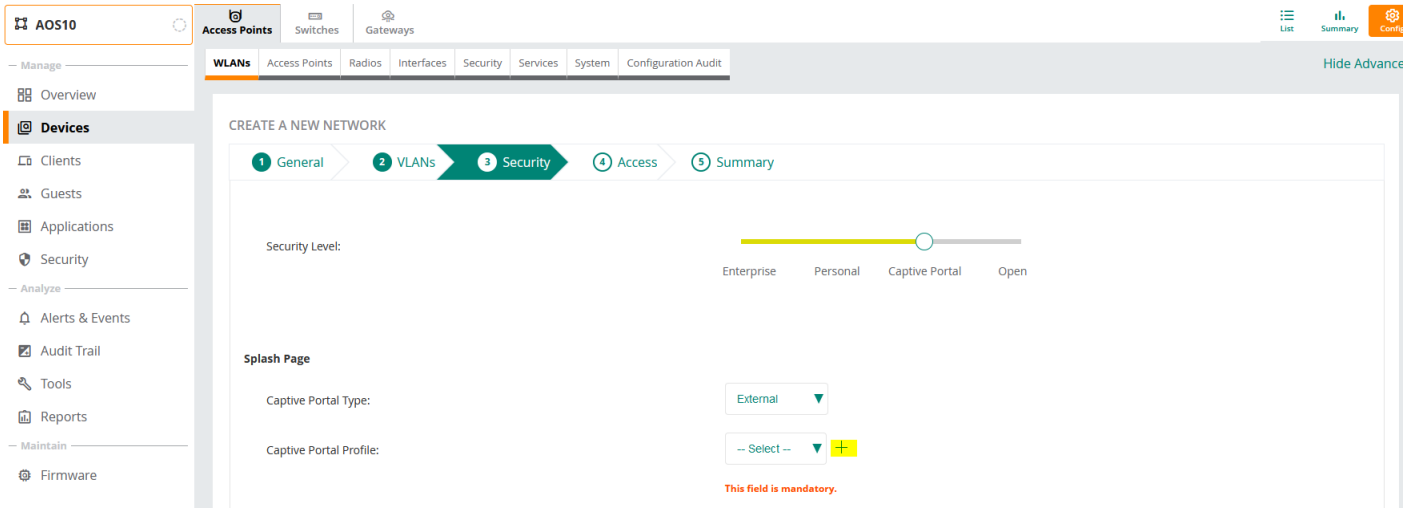
Here we'll start with AP configuration followed by ClearPass.

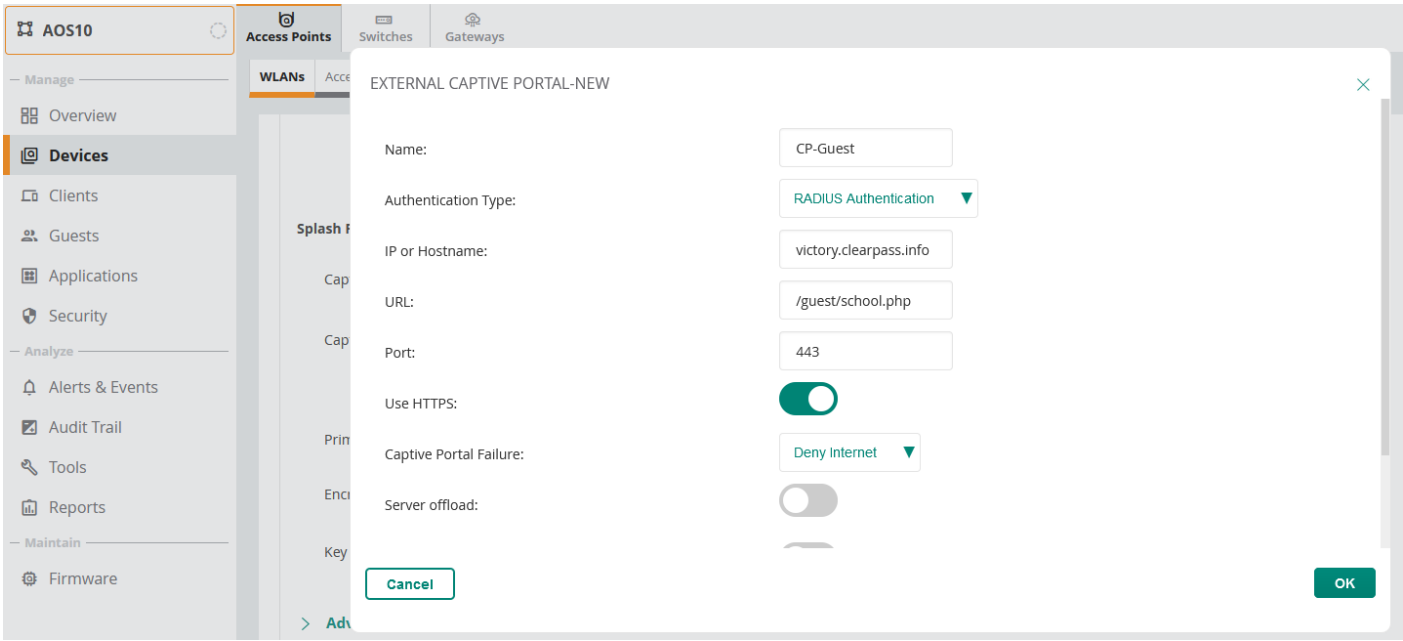
8.1 Guest Wireless Configuration

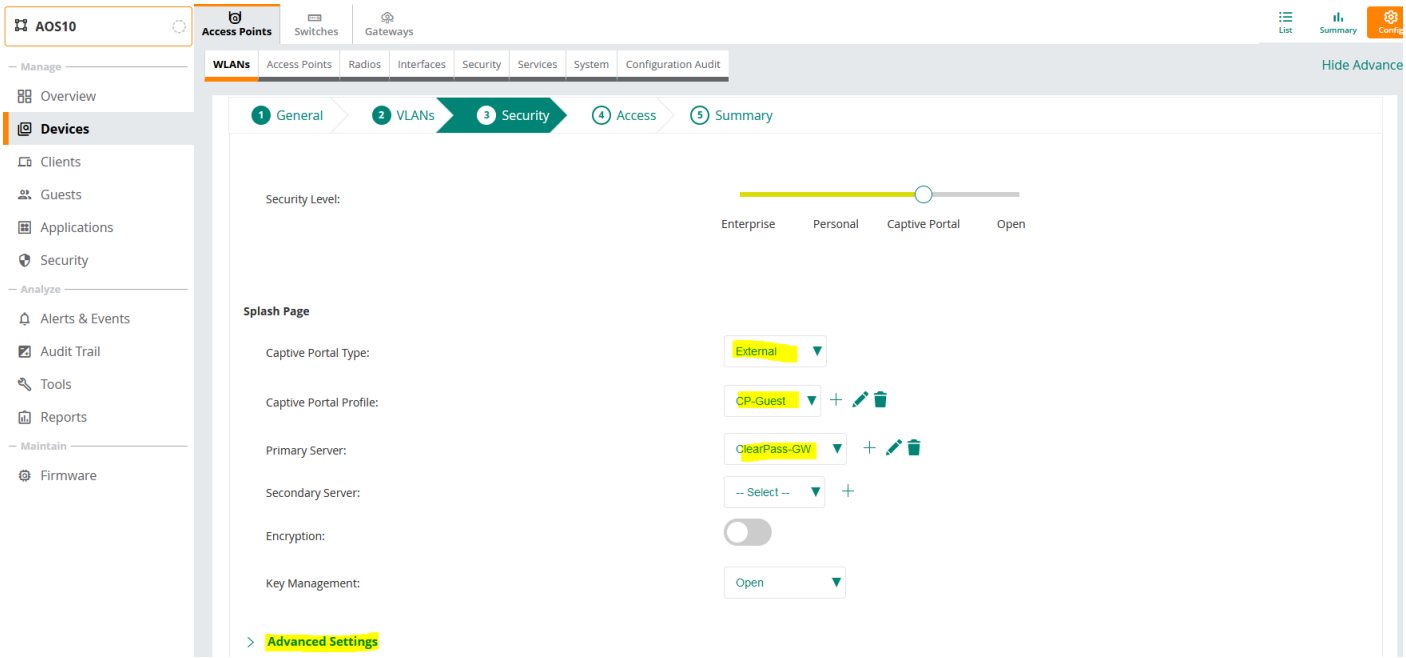
The Guest WLAN will be tunnelled to the gateways, for this scenario all the configuration will take place on the AP group.

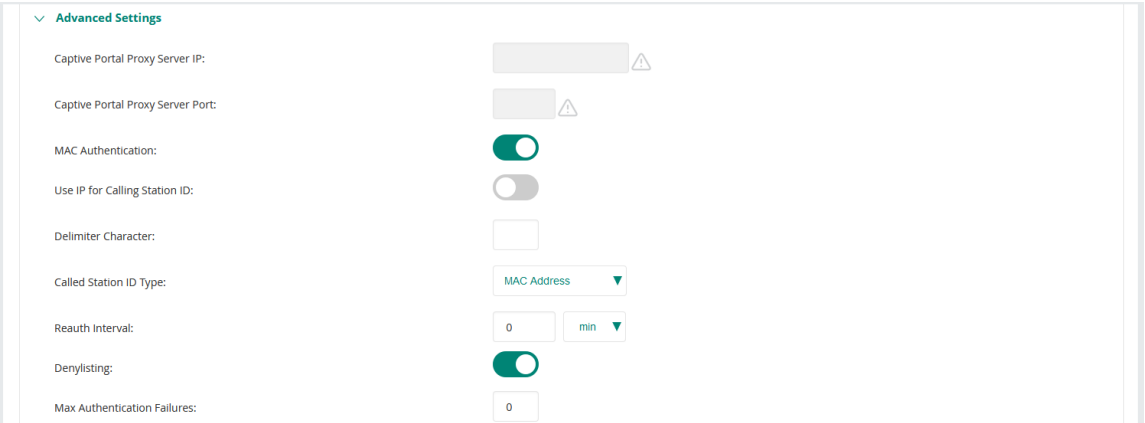


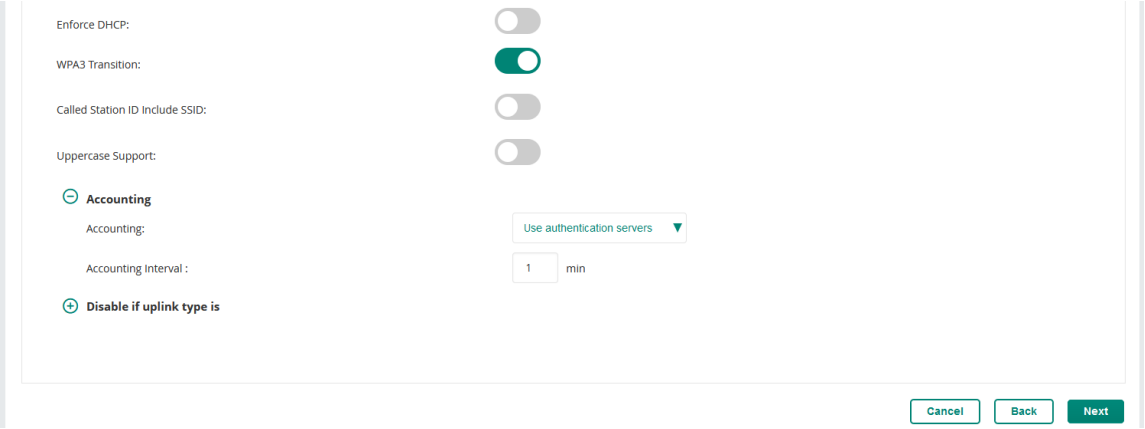




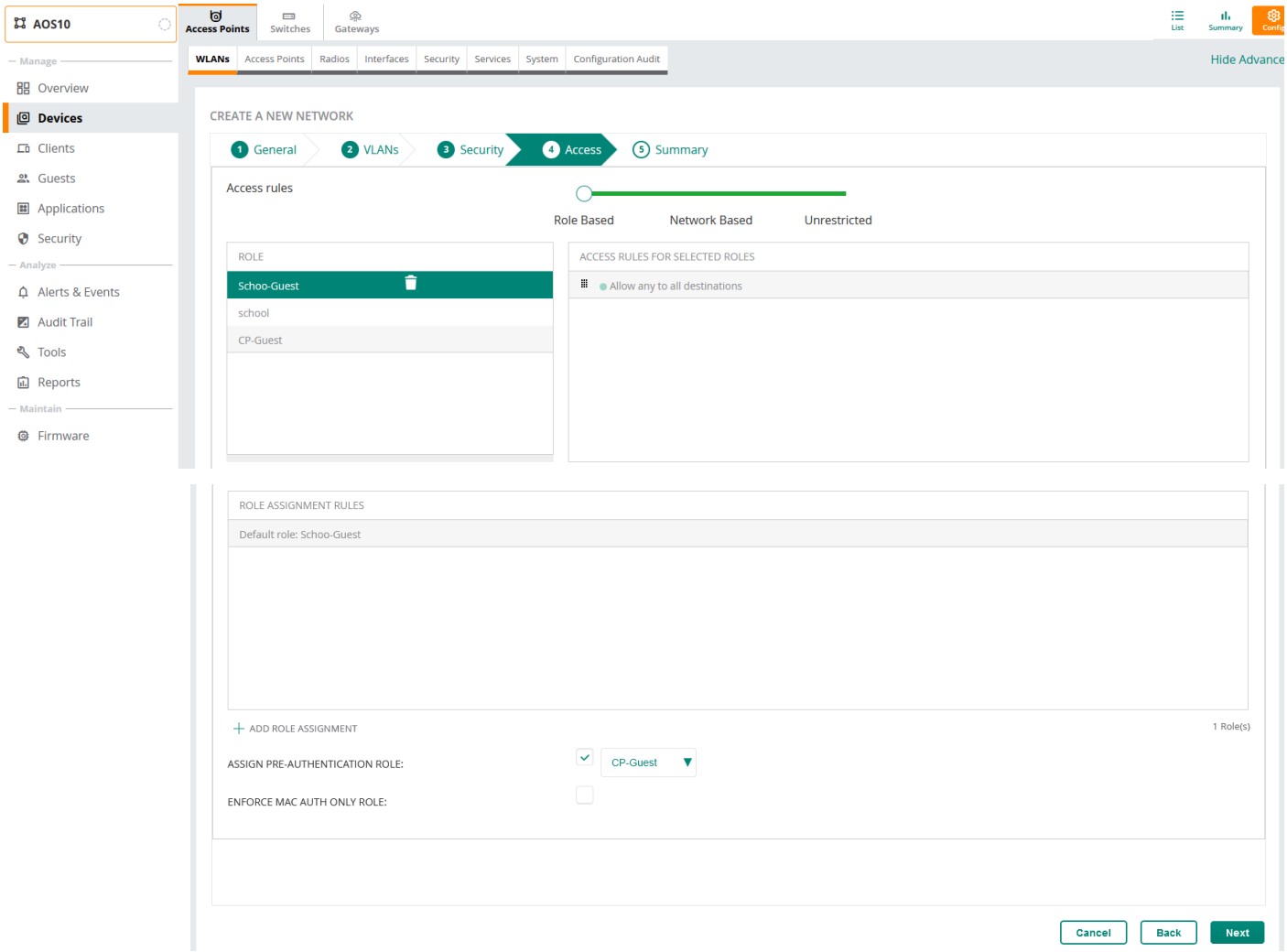

AOS10
Access Points
Switches
Gateways
Manage
Overview
Devices
Clients
Guests
Applications
Security
Analyze
Alerts & Events
Audit Trail
Tools
Reports
Maintain
Firmware
WLANs
EXTERNAL CAPTIVE PORTAL-NEW
Name:
CP-Guest
Authentication Type:
RADIUS Authentication
IP or Hostname:
victory.clearpass.info
URL:
/guest/school.php
Port:
443
Use HTTPS:
Captive Portal Failure:
Deny Internet
Server offload:
Cancel
OK

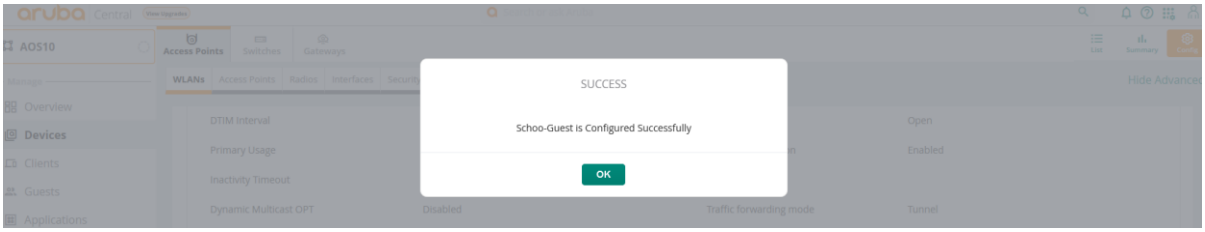

AOS10
Access Points
Switches
Gateways
List
Summary
Config
Manage
Overview
Devices
Clients
Guests
Applications
Security
Analyze
Alerts & Events
Audit Trail
Tools
Reports
Maintain
Firmware
WLANs
Access Points
Radios
Interfaces
Security
Services
System
Configuration Audit
Hide Advance
1 General
2 VLANs
3 Security
4 Access
5 Summary
Security Level:
Enterprise
Personal
Captive Portal
Open
Splash Page
Captive Portal Type:
External
Captive Portal Profile:
CP-Guest
Primary Server:
ClearPass-GW
Secondary Server:
-- Select --
Encryption:
Key Management:
Open
Advanced Settings


Advanced Settings
Captive Portal Proxy Server IP:
Captive Portal Proxy Server Port:
MAC Authentication:
Use IP for Calling Station ID:
Delimiter Character:
Called Station ID Type:
MAC Address
Reauth Interval:
0
min
Denylisting:
Max Authentication Failures:
0

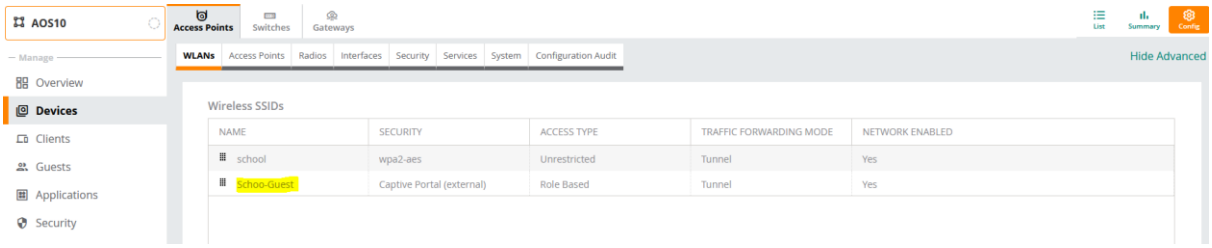


In the above we have also enabled MAC auth and RADIUS accounting. MAC auth is enabled because we want to also enable MAC caching for the guest users.



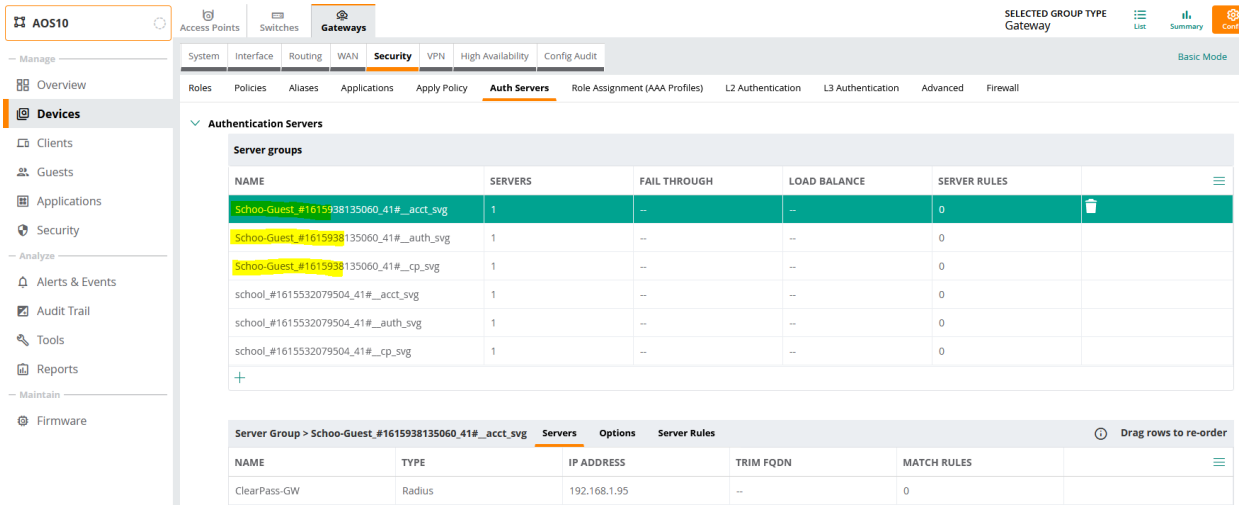


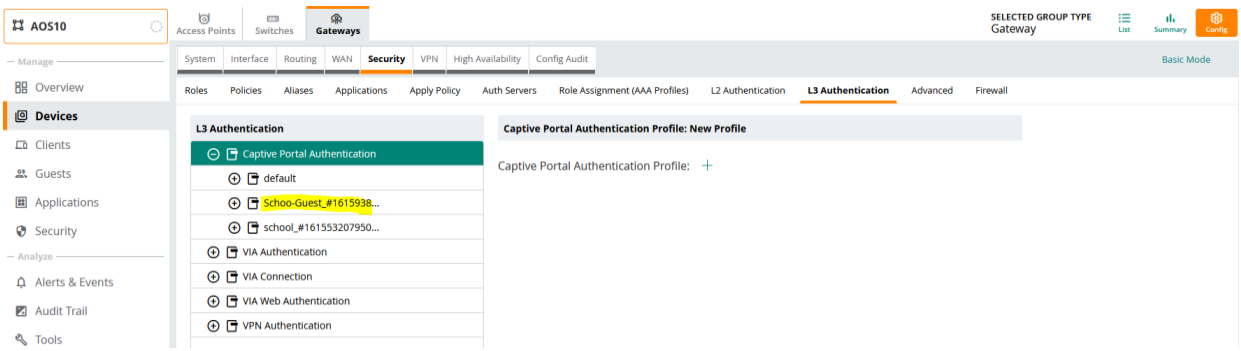
Now we have our Guest SSID configured.

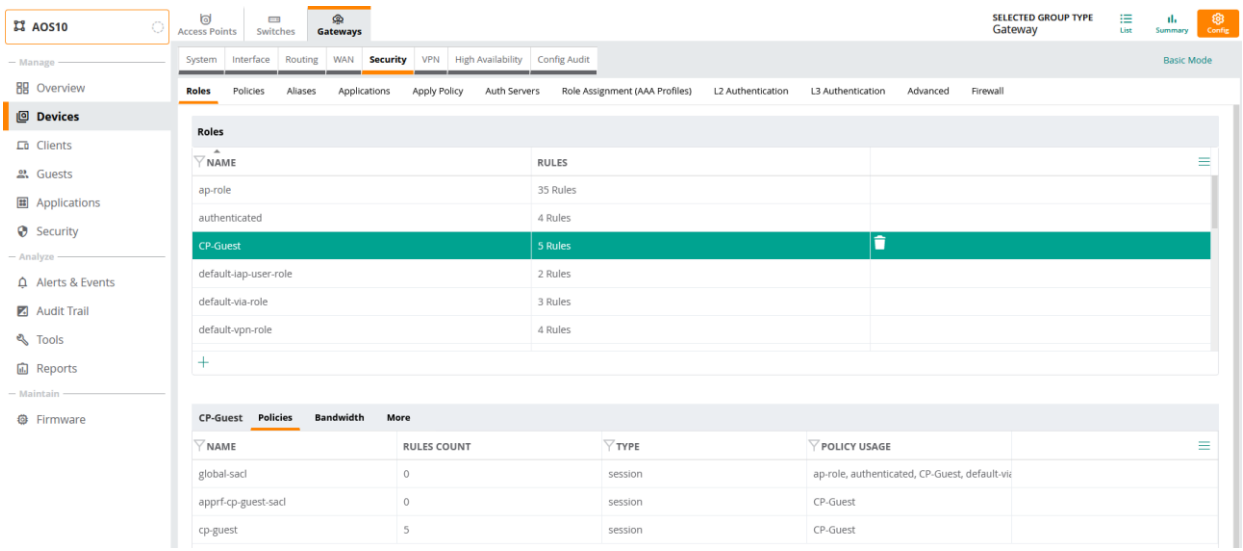


We don't need to do any configuration on the gateways as all the relevant configuration will be pushed to them, which are:

- Authentication Servers and groups.
- L3 Captive Portal Authentication
- Pre-authentication user role



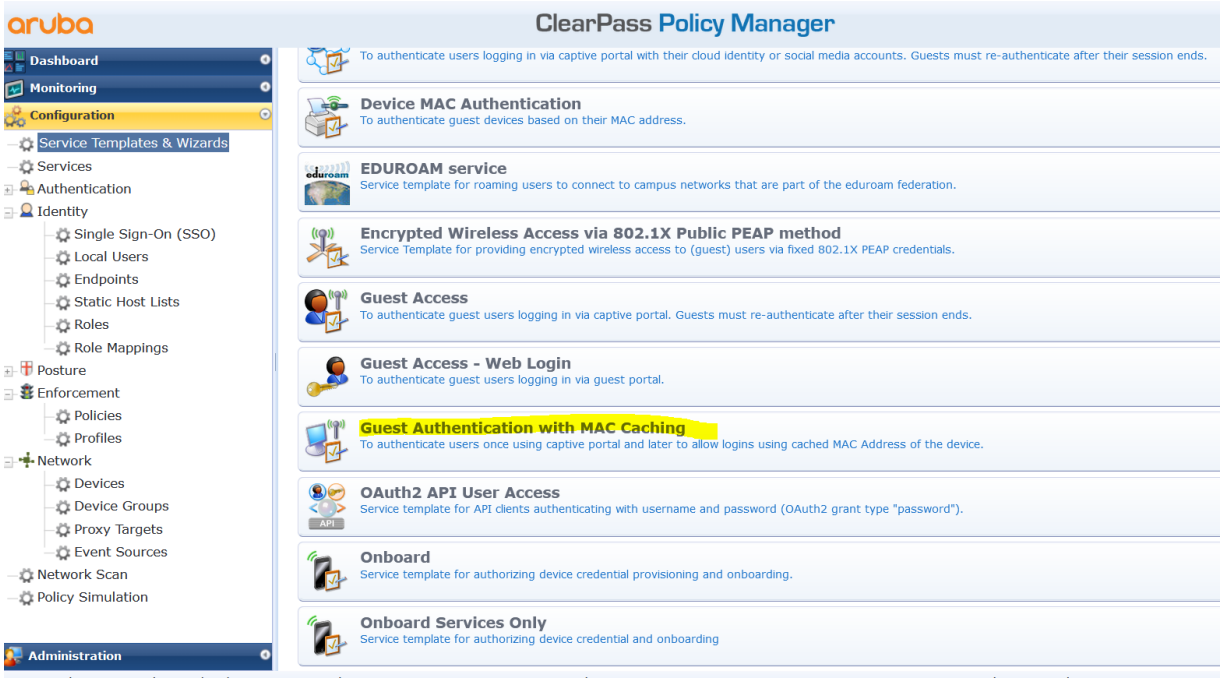


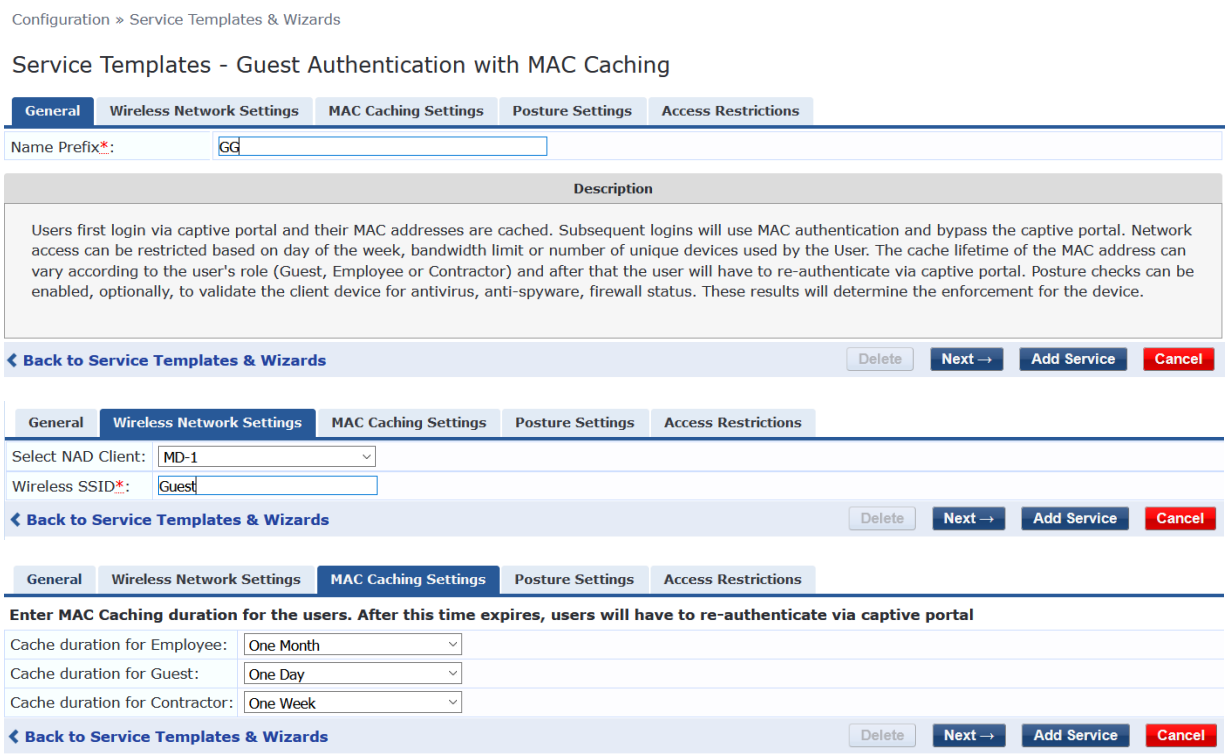


Lastly note that we have not use a publicly signed HTTPS server certificate for the controllers and hence the redirection of a web page will issue a warning on the client's web browser. In all deployment you need to have a public cert for the controllers as well as ClearPass nodes.

8.2 ClearPass Guest policy Configuration

We'll go through the guest confirmation needed on ClearPass. There are two part to it, one is the web pages that the client redirects to and the other is the policy service we need to create. We'll start with the policy service. Here we are using the following template. This creates 2x services one is MAC authentication and the second one is Guest redirection to captive portal page.





General | Wireless Network Settings | MAC Caching Settings | Posture Settings | Access Restrictions

Enable Posture Checks to perform health checks after authentication.

Enable Posture Checks: ☐ Configure Guest Web Login page

Back to Service Templates & Wizards | Delete | Next → | Add Service | Cancel

General | Wireless Network Settings | MAC Caching Settings | Posture Settings | Access Restrictions

- **Enforcement Type applies to the Captive Portal Access, Employee Access, Guest Access, and Contractor Access fields.**
- **Captive Portal Access is used for unauthenticated users and after the MAC caching duration has expired.**
- **At least one of Employee, Guest, and Contractor Access must be provided.**

Enforcement Type*:	Aruba Role Enforcement
Captive Portal Access*:	GuestCptivePortal Guest-guest-logon
Days allowed for access*:	☑ Mon ... Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday
Maximum number of devices allowed per user*:	5
Maximum bandwidth allowed per user*:	0 MB (For unlimited bandwidth, set value to 0)
Employee Access:	Employee-Guest
Guest Access:	Guest
Contractor Access:	Contractor

Back to Service Templates & Wizards | Delete | Next → | Add Service | Cancel

Services

Add
Import
Export All

- **Added 15 Enforcement Profile(s)**
- **Added 2 Enforcement Policies**
- **Added 2 Role Mapping Policies**
- **Added 2 service(s)**

This page shows the current list and order of services that ClearPass follows during authentication and authorization.

Filter: Name contains | Go | Clear Filter | Show 20 records

#	☐	Order	Name	Type	Template	Status
1.	☐	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	●
2.	☐	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	✓
3.	☐	3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	✓
4.	☐	4	[Guest Operator Logins]	Application	Aruba Application Authentication	✓
5.	☐	5	[Insight Operator Logins]	Application	Aruba Application Authentication	✓
6.	☐	6	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	✓
7.	☐	7	AA Aruba 802.1X Wireless	RADIUS	Aruba 802.1X Wireless	✓
8.	☐	8	GG MAC Authentication	RADIUS	MAC Authentication	✓
9.	☐	9	GG User Authentication with MAC Caching	RADIUS	RADIUS Enforcement (Generic)	✓

We'll look at the **MAC authentication service**

Services - GG MAC Authentication

Note: This Service is created by Service Template

Summary | Service | Authentication | Authorization | Roles | Enforcement

Name:	GG MAC Authentication
Description:	MAC Authentication bypass for captive portal users
Type:	MAC Authentication
Status:	Enabled
Monitor Mode:	☐ Enable to monitor network access without enforcement
More Options:	☑ Authorization ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
2.	Radius:Aruba	Aruba-Essid-Name	BEGINS_WITH	Guest
3.	*Click to add...*			

Summary | Service | **Authentication** | Authorization | Roles | Enforcement

Authentication Methods:	[Allow All MAC AUTH] --Select to Add--	Move Up ↑ / Move Down ↓ / Remove / View Details / Modify Add New Authentication Method
Authentication Sources:	[Endpoints Repository] [Local SQL DB] --Select to Add--	Move Up ↑ / Move Down ↓ / Remove / View Details / Modify Add New Authentication Source

Summary | Service | Authentication | **Authorization** | Roles | Enforcement

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

Summary | Service | Authentication | Authorization | **Roles** | Enforcement

Role Mapping Policy: GG 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.	(Authorization:[Endpoints Repository]:Unique-Device-Count *EXISTS*) *AND* (Authorization:[Time Source]:Now DT *LESS_THAN* %{Endpoint:MAC-Auth Expiry}) *AND* (Authorization:[Guest User Repository]:AccountExpired *EQUALS* false) *AND* (Authorization:[Guest User Repository]:AccountEnabled *EQUALS* true)	[MAC Caching]
2.	(Endpoint:Guest Role ID *EQUALS* 1)	[Contractor]
3.	(Endpoint:Guest Role ID *EQUALS* 2)	[Guest]
4.	(Endpoint:Guest Role ID *EQUALS* 3)	[Employee]

Summary | Service | Authentication | Authorization | Roles | **Enforcement**

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

Enforcement Policy: GG MAC Authentication 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 *MATCHES_ALL* [MAC Caching] [Guest] [User Authenticated])	[Allow Access Profile], GG Guest Device Profile
2.	(Tips:Role *MATCHES_ALL* [MAC Caching] [Employee] [User Authenticated])	[Allow Access Profile], GG Employee Device Profile
3.	(Tips:Role *MATCHES_ALL* [MAC Caching] [Contractor] [User Authenticated])	[Allow Access Profile], GG Contractor Device Profile
4.	(Tips:Role *MATCHES_ANY* [Guest] [Contractor] [Employee])	[Allow Access Profile], GG Captive Portal Profile

Back to Services | **Disable** | **Copy** | **Save** | **Cancel**

And here are the enforcement profiles that are used here

Summary | Profile | Attributes

Profile:

Name:	GG Guest Device Profile
Description:	Role/VLAN enforcement for Guest
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Guest
2.	Radius:IETF	User-Name	=	%{Endpoint:Username}

Summary | Profile | Attributes

Profile:

Name:	GG Employee Device Profile
Description:	Role/VLAN enforcement for Employee
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Employee-Guest
2.	Radius:IETF	User-Name	=	%{Endpoint:Username}

Summary | Profile | Attributes

Profile:

Name:	GG Contractor Device Profile
Description:	Role/VLAN enforcement for Contractor
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Contractor
2.	Radius:IETF	User-Name	=	%{Endpoint:Username}

Summary | Profile | Attributes

Profile:

Name:	GG Captive Portal Profile
Description:	Captive Portal Role/VLAN enforcement
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Guest-guest-logon

We'll look at the **User Authentication with MAC caching service**

Services - GG User Authentication with MAC Caching

Summary | Service | Authentication | Authorization | Roles | Enforcement

Name:	GG User Authentication with MAC Caching
Description:	Captive Portal authentication with MAC Caching
Type:	RADIUS Enforcement (Generic)
Status:	Enabled
Monitor Mode:	☐ Enable to monitor network access without enforcement
More Options:	☑ Authorization ☐ Posture Compliance ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

Service Rule

Matches ○ ANY or ◉ ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	Calling-Station-Id	EXISTS	
2.	Connection	Client-Mac-Address	NOT_EQUALS	%{Radius:IETF:User-Name}
3.	Radius:Aruba	Aruba-Essid-Name	BEGINS_WITH	Guest
4.	*Click to add...*			

Summary | Service | **Authentication** | Authorization | Roles | Enforcement

Authentication Methods:	[PAP] [MSCHAP] [CHAP] --Select to Add--	Move Up ↑ / Move Down ↓ / Remove / View Details / Modify Add New Authentication Method
Authentication Sources:	[Guest User Repository] [Local SQL DB] --Select to Add--	Move Up ↑ / Move Down ↓ / Remove / View Details / Modify Add New Authentication Source

Summary | Service | Authentication | **Authorization** | Roles | Enforcement

Authorization Details:

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

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

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

[Endpoints Repository] [Local SQL DB]
[Time Source] [Local SQL DB]

Remove / View Details / Modify

--Select to Add--

Add New Authentication Source

Summary | Service | Authentication | Authorization | **Roles** | Enforcement

Role Mapping Policy: GG User Authentication with MAC Caching Role Mapping **Modify**

Add New Role Mapping Policy

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

	Conditions	Role
1.	(GuestUser:Role ID *EQUALS* 1)	[Contractor]
2.	(GuestUser:Role ID *EQUALS* 2)	[Guest]
3.	(GuestUser:Role ID *EQUALS* 3)	[Employee]

Summary | Service | Authentication | Authorization | Roles | **Enforcement**

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

Enforcement Policy: GG User Authentication with MAC Caching Enforcement Policy **Modify**

Add New Enforcement Policy

Enforcement Policy Details	
Description:	
Default Profile:	[Allow Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:[Endpoints Repository]:Unique-Device-Count *GREATER_THAN* 5)	[Deny Access Profile]
2.	(Tips:Role *EQUALS* [Employee]) *AND* (Date:Day-of-Week *BELONGS_TO* Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)	GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit, GG MAC Caching Session Limit, GG Employee MAC Caching, [Update Endpoint Known], GG MAC Caching Do Expire, GG MAC Caching Expire Post Login, GG Employee Profile
3.	(Tips:Role *EQUALS* [Contractor]) *AND* (Date:Day-of-Week *BELONGS_TO* Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)	GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit, GG MAC Caching Session Limit, GG Contractor MAC Caching, [Update Endpoint Known], GG MAC Caching Do Expire, GG MAC Caching Expire Post Login, GG Contractor Profile
4.	(Tips:Role *EQUALS* [Guest]) *AND* (Date:Day-of-Week *BELONGS_TO* Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)	GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit, GG MAC Caching Session Limit, GG Guest MAC Caching, [Update Endpoint Known], GG MAC Caching Do Expire, GG MAC Caching Expire Post Login, GG Guest Profile

The enforcement profiles

Summary | Profile | Attributes

Profile:

Name:	GG Employee Profile
Description:	Role/VLAN enforcement for Employee
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Employee-Guest

Summary | Profile | Attributes

Profile:

Name:	GG Guest Profile
Description:	Role/VLAN enforcement for Guest
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Guest

Summary | Profile | Attributes

Profile:

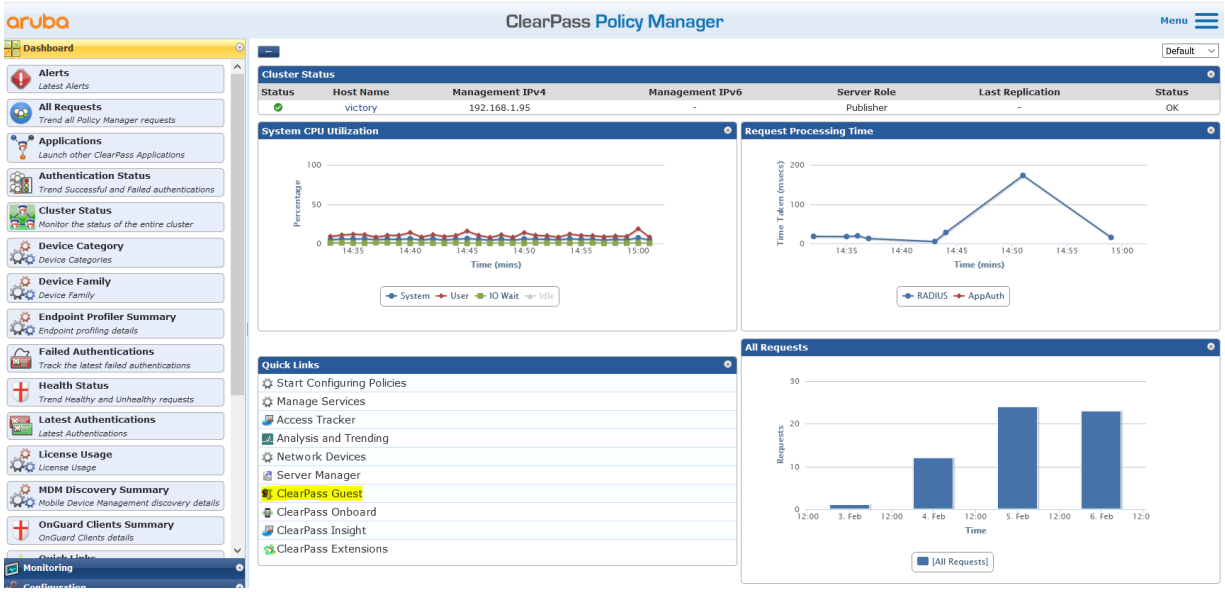
Name:	GG Contractor Profile
Description:	Role/VLAN enforcement for Contractor
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

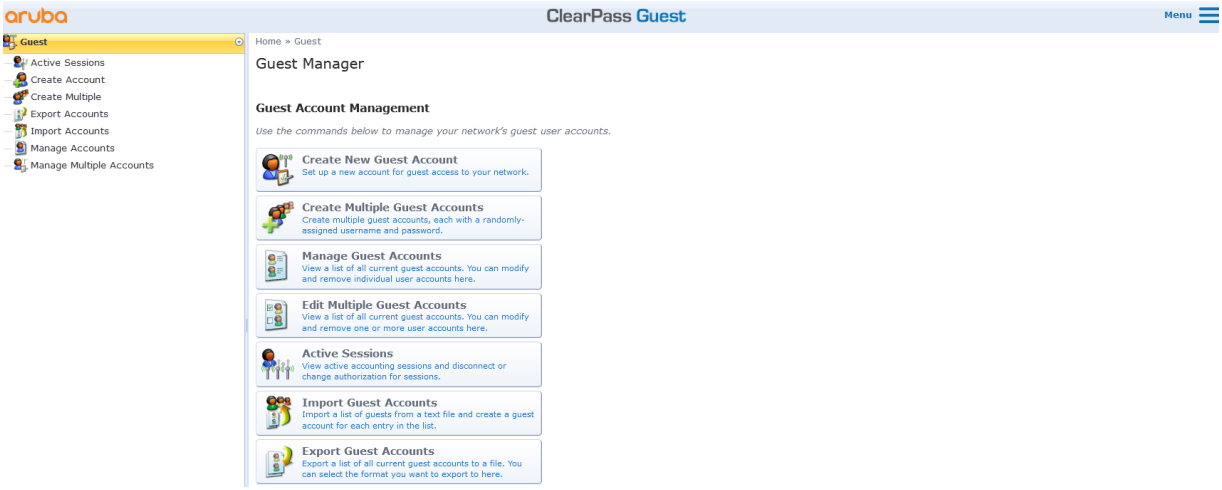
	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Contractor

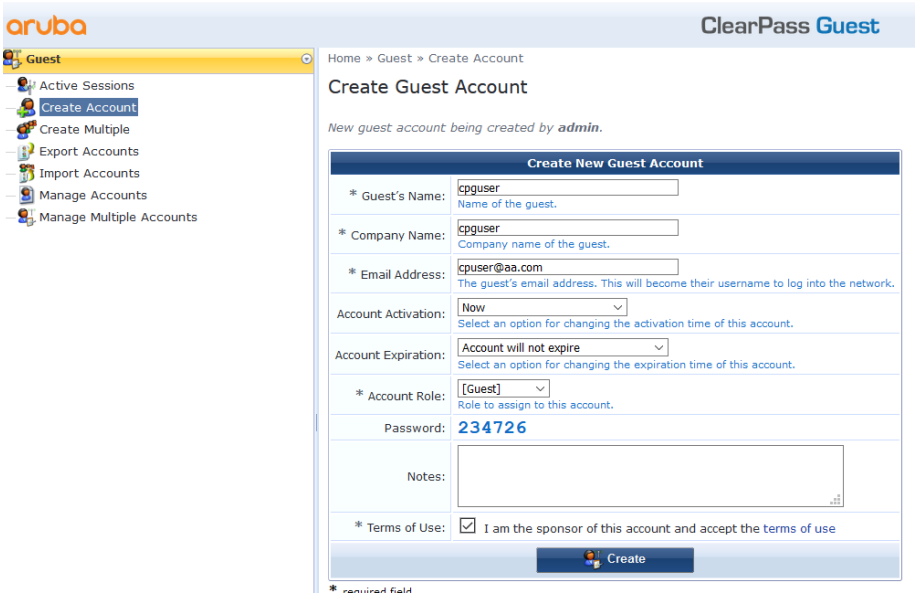
8.3 ClearPass Guest Portal Configuration

Here we'll configure the portal pages.

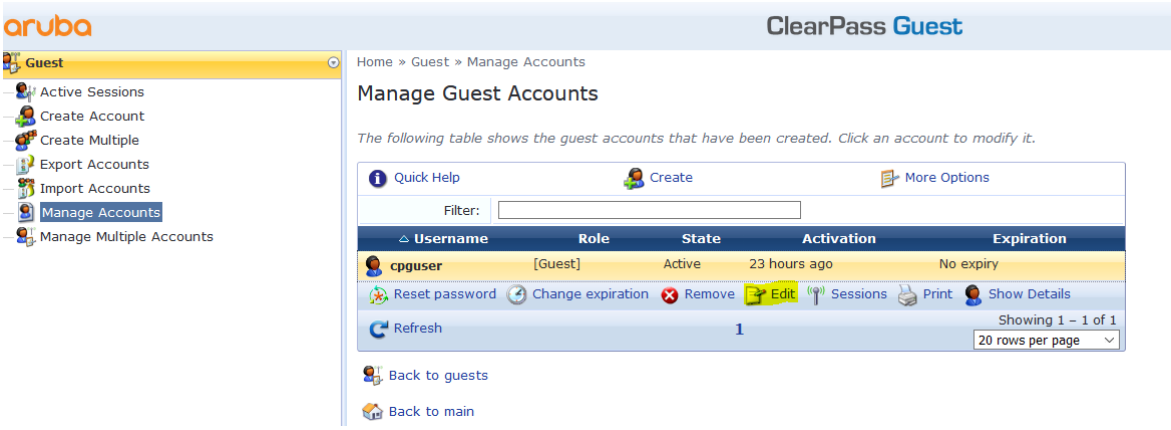


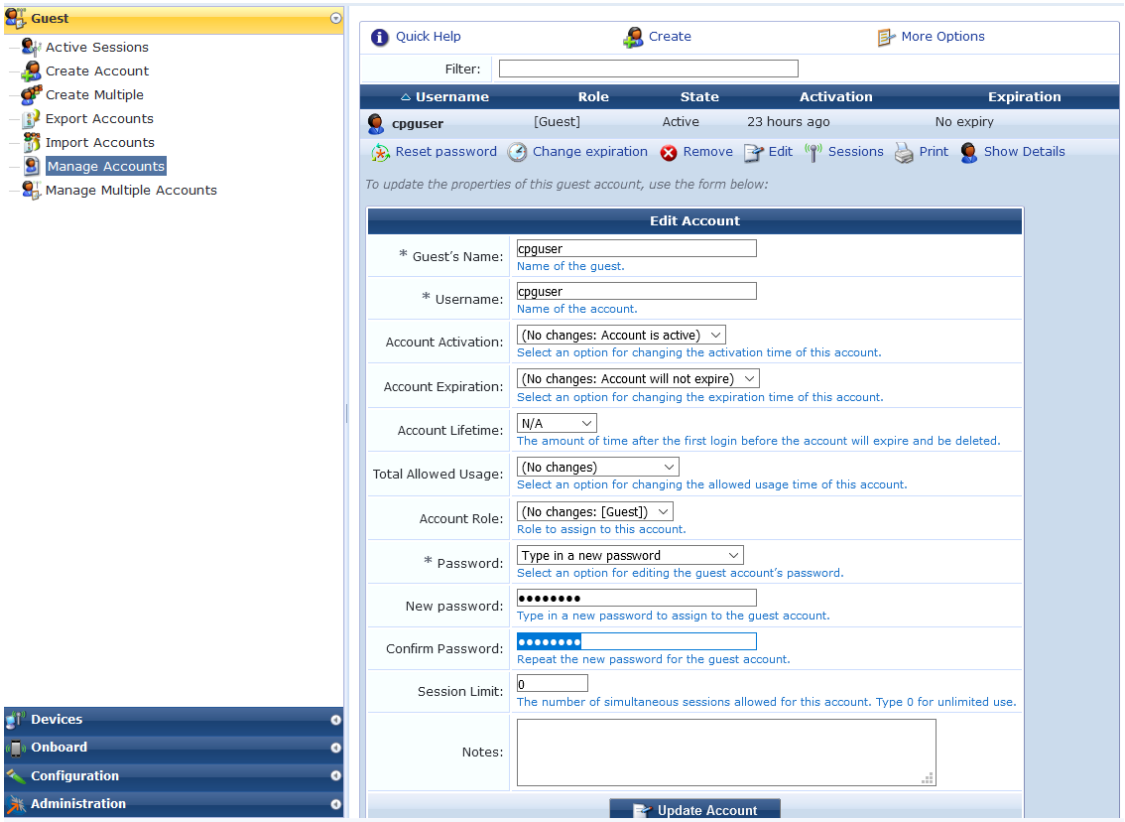
Now we'll create a guest user called cpguser with no expiration on the account.



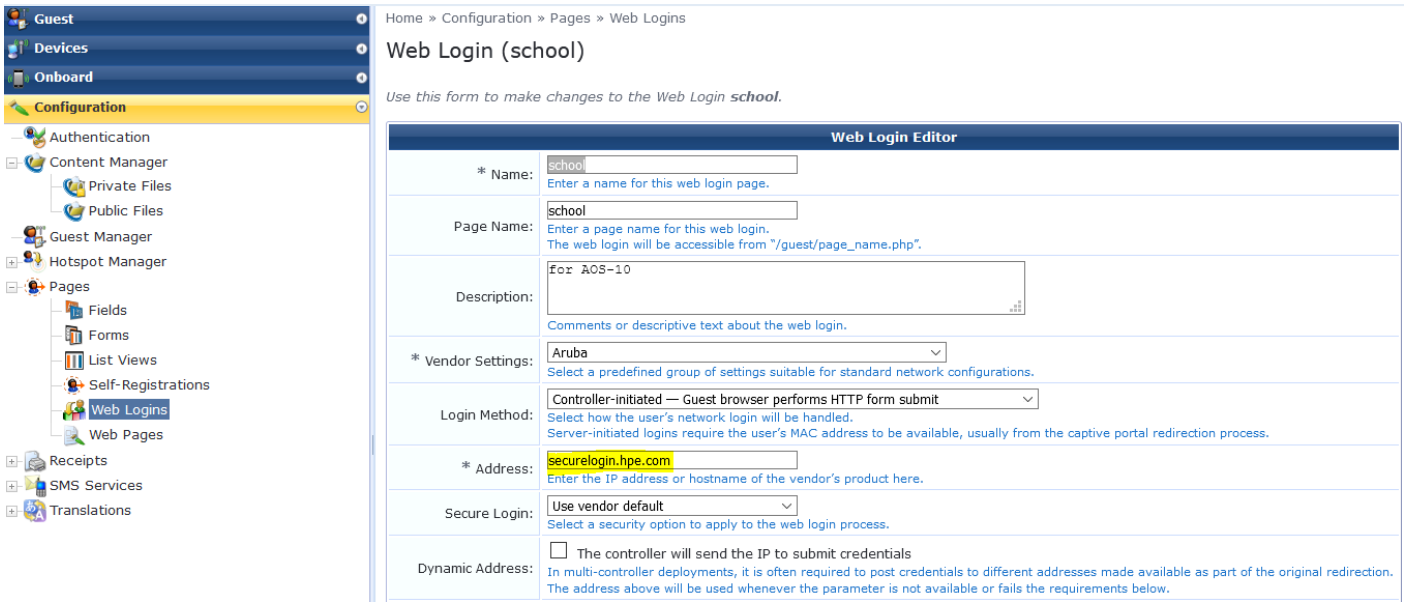


Once created we'll modify it to change the username and password





Next we'll create a weblogin page, note that the page name will be in the redirection URL, also securelogin.hpe.com will need to change to CN in the server certificate on Aruba controller.



Page Redirect
Options for specifying parameters passed in the initial redirect.

Security Hash: Do not check – login will always be permitted
Select the level of checking to apply to URL parameters passed to the web login page.
Use this option to detect when URL parameters have been modified by the user, for example their MAC address.

Login Form
Options for specifying the behaviour and content of the login form.

Authentication: Credentials – Require a username and password
Select the authentication requirement.
Access Code requires a single code (username) to be entered.
Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required.
Auto is similar to anonymous but the page is automatically submitted.
Access Code and Anonymous require the account to have the Username Authentication field set.

Prevent CNA: ☑ Enable bypassing the Apple Captive Network Assistant
The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal.
Note that this option may not work with all vendors, depending on how the captive portal is implemented.

Custom Form: ☐ Provide a custom login form
If selected, you must supply your own HTML login form in the Header or Footer HTML areas.

Custom Labels: ☐ Override the default labels and error messages
If selected, you will be able to alter labels and error messages for the current login form.

* Pre-Auth Check: None — no extra checks will be made
Select how the username and password should be checked before proceeding to the NAS authentication.

Terms: ☑ Require a Terms and Conditions confirmation
If checked, the user will be forced to accept a Terms and Conditions checkbox.

CAPTCHA: None
Select a CAPTCHA mode.

Default Destination
Options for controlling the destination clients will redirect to after login.

* Default URL:
Enter the default URL to redirect clients.
Please ensure you prepend "http://" for any external domain.

Override Destination: ☐ Force default destination for all clients
If selected, the client's default destination will be overridden regardless of its value.

Login Page
Options for controlling the look and feel of the login page.

* Skin: Galleria Skin 3
Choose the skin to use when this web login page is displayed.

Title:
The title to display on the web login page.
Leave blank to use the default (Login).

Header HTML:
```
{nwa_cookiecheck}
{if $errmsg}{nwa_icontext type=error}{$errmsg|escape}{/nwa_icontext}{/if}

{nwa_text id=7980}<p>
    Please login to the network using your
    username and password.
</p>{/nwa_text}
```
Insert...
HTML template code displayed before the login form.

Footer HTML:
```
{nwa_text id=7979}<p>
Contact a staff member if you are experiencing
difficulty logging in.
</p>{/nwa_text}
```
Insert...
HTML template code displayed after the login form.

Login Message:
```
{nwa_text id=7978}<p>
Logging in, please wait...
</p>{/nwa_text}
```
Insert...
HTML template code displayed while the login attempt is in progress.

* Login Delay: 0
The time in seconds to delay while displaying the login message.

Advertising Services
Enable advertising content on the login page.

Advertising: ☐ Enable Advertising Services content

Cloud Identity
Optionally present guests with various cloud identity / social login options.

Enabled: ☐ Enable logins with cloud identity / social network credentials

Multi-Factor Authentication
Require a secondary factor when authenticating.

Provider: No multi-factor authentication

Network Login Access
Controls access to the login page.

Allowed Access:
Enter the IP addresses and networks from which logins are permitted.

Denied Access:
Enter the IP addresses and networks that are denied login access.

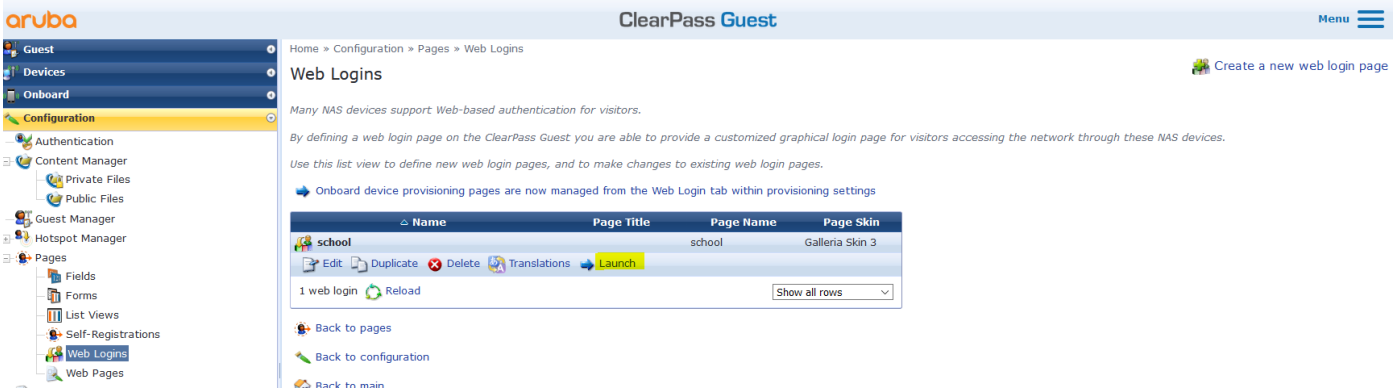
* Deny Behavior: Send HTTP 404 Not Found status
Select the response of the system to a request that is not permitted.

Post-Authentication
Actions to perform after a successful pre-authentication.

Health Check: ☐ Require a successful OnGuard health check
If selected, the guest will be required to pass a health check prior to accessing the network.

Update Endpoint: ☐ Mark the user's MAC address as a known endpoint
If selected, the endpoint's attributes will also be updated with other details from the user account.

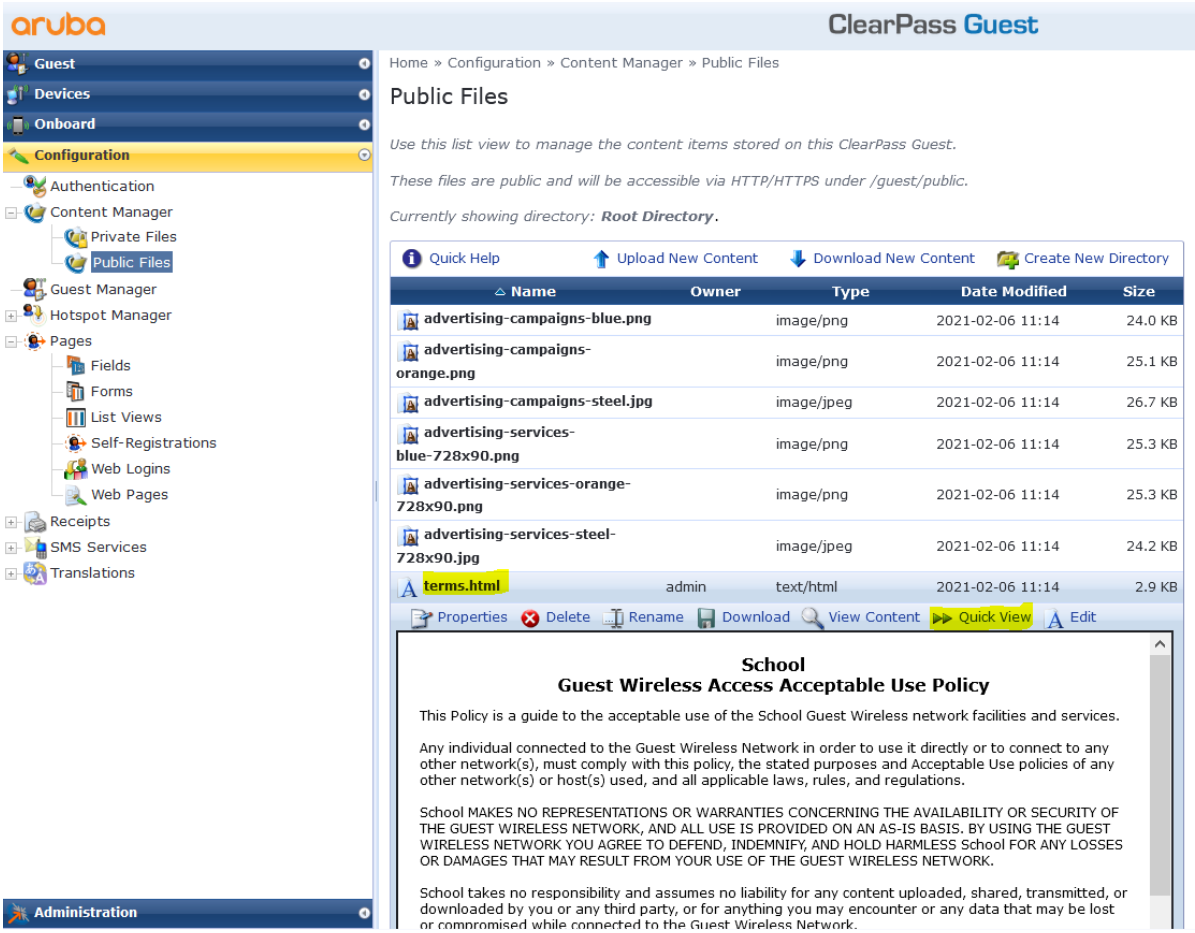
Save Changes | Save and Reload



You can test the page as well, when you'll click on the launch a tab will open and you'll see the captive portal note the URL which in this case is https://victory.clearpass.info/guest/school.php?_browser=1

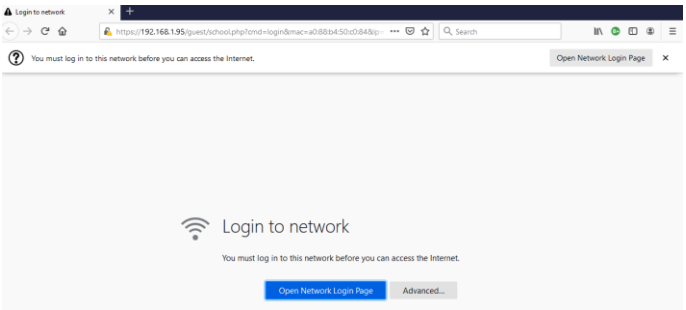
The "guest/school.php" is used in the URL redirection which we configured in MM

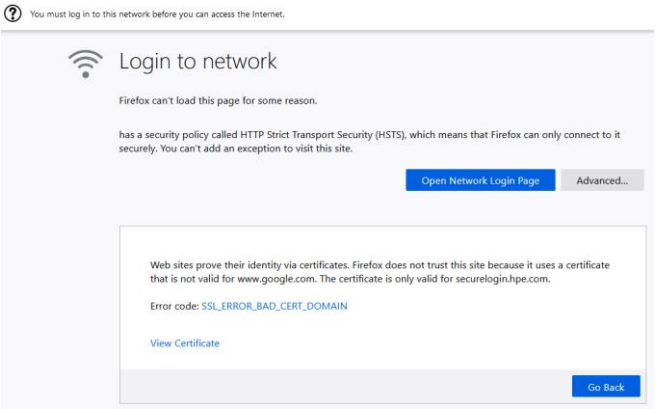
Now go to content manager and upload your terms and condition page.



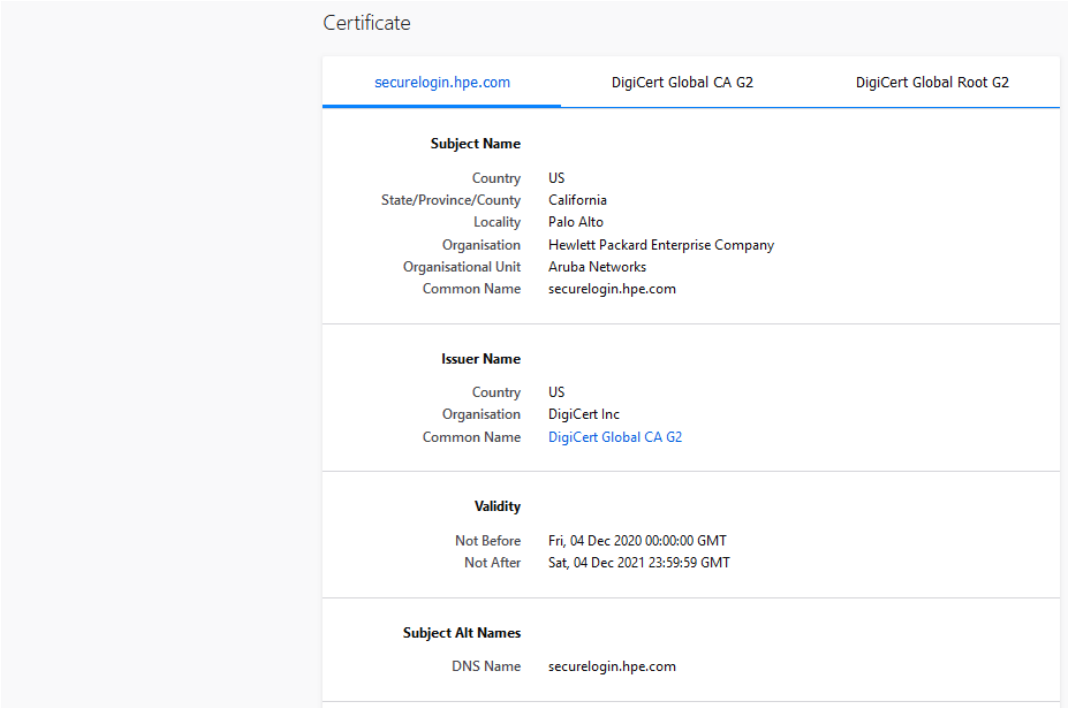
8.4 Guest Testing

Now we'll get a test device to connect to Guest SSID, it gets automatically redirected to guest page in ClearPass but the browser will issue a warning

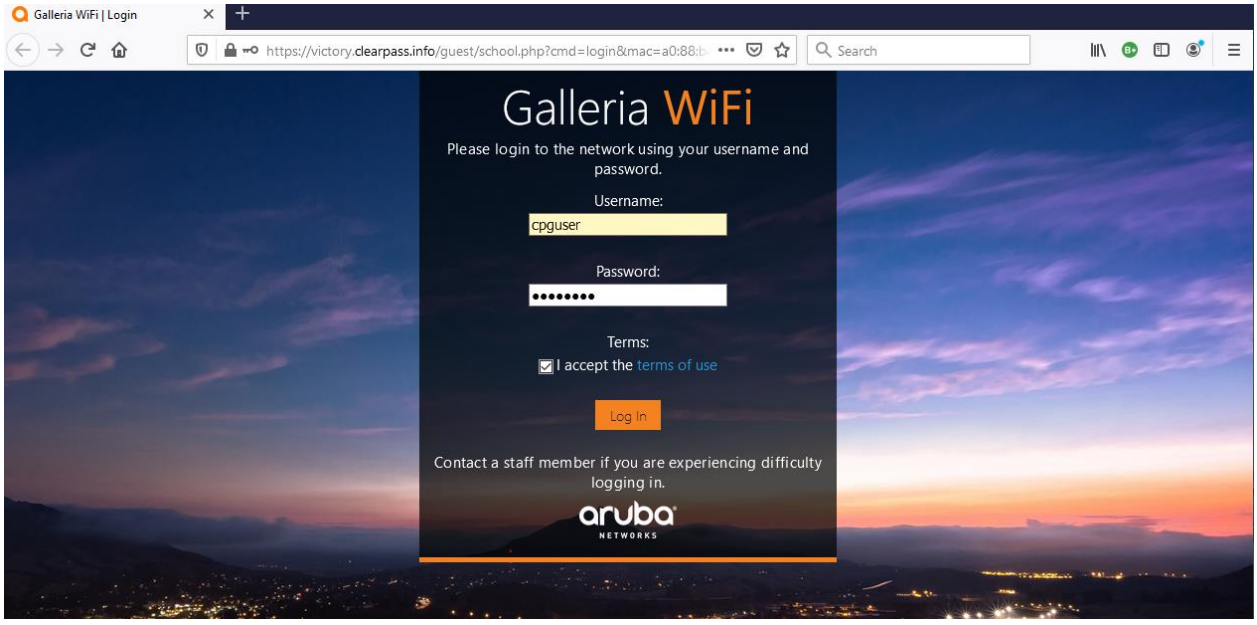




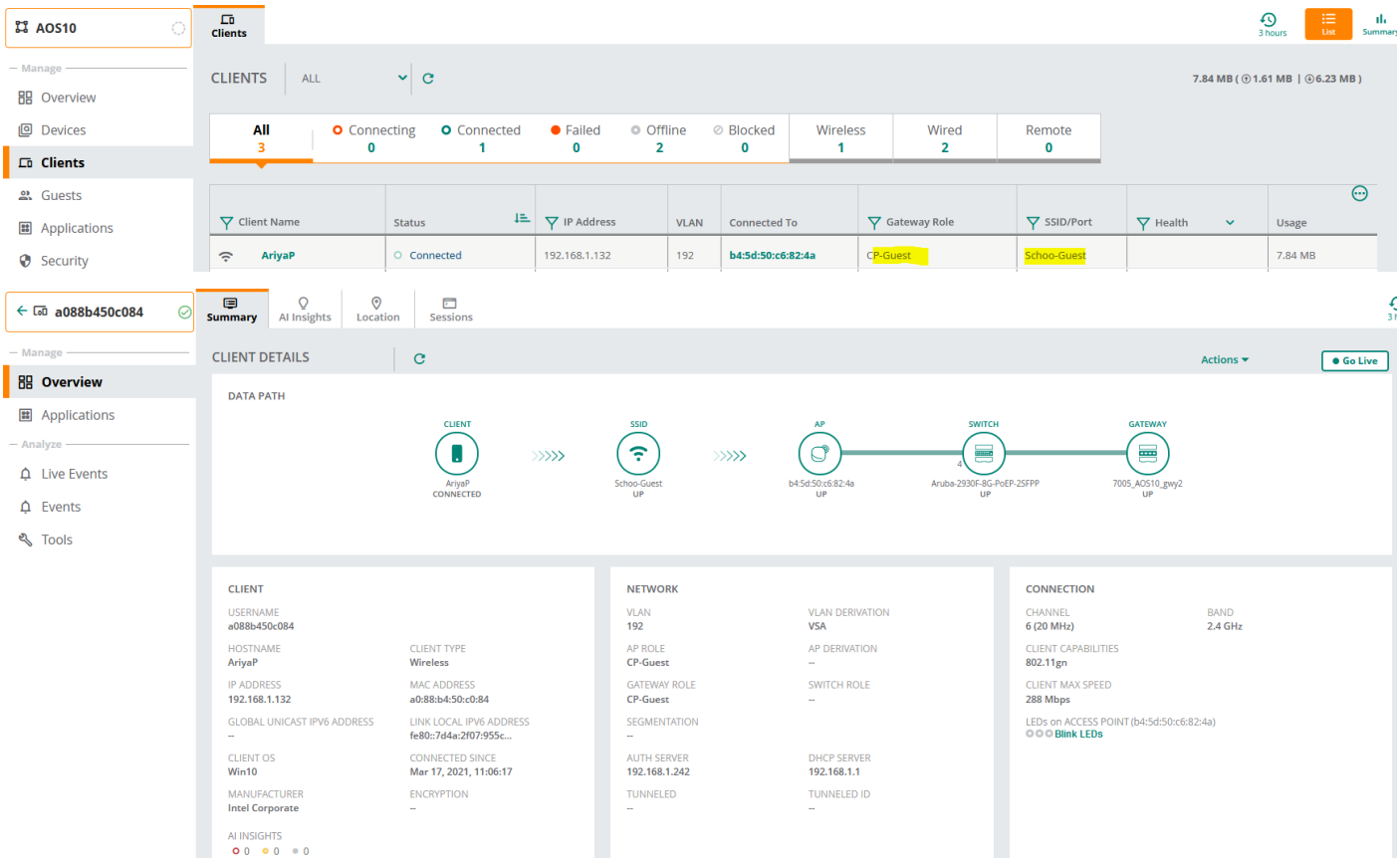
We'll have a look at the certificate, and we'll see it is the default captive portal certificate which is on the controller.



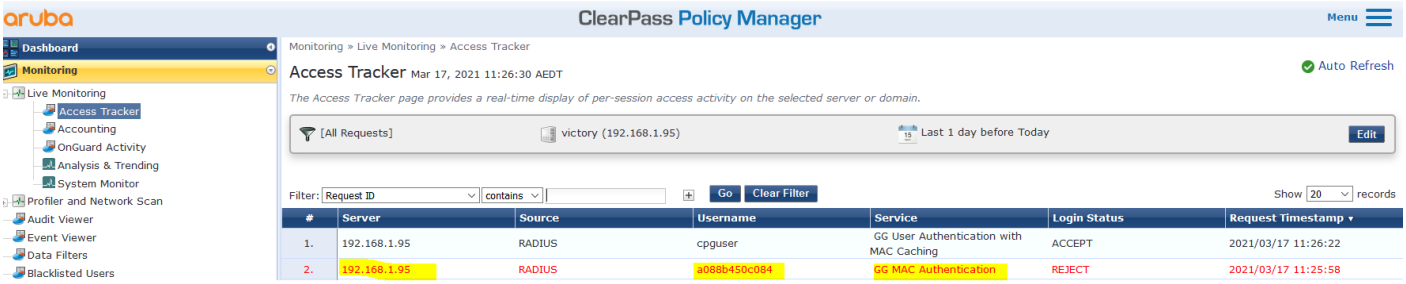
We'll accept this and carry on, but for all deployments you need to have a public server certificate for your controllers. Once we accept the certificate, we'll get redirected to the captive portal page on ClearPass

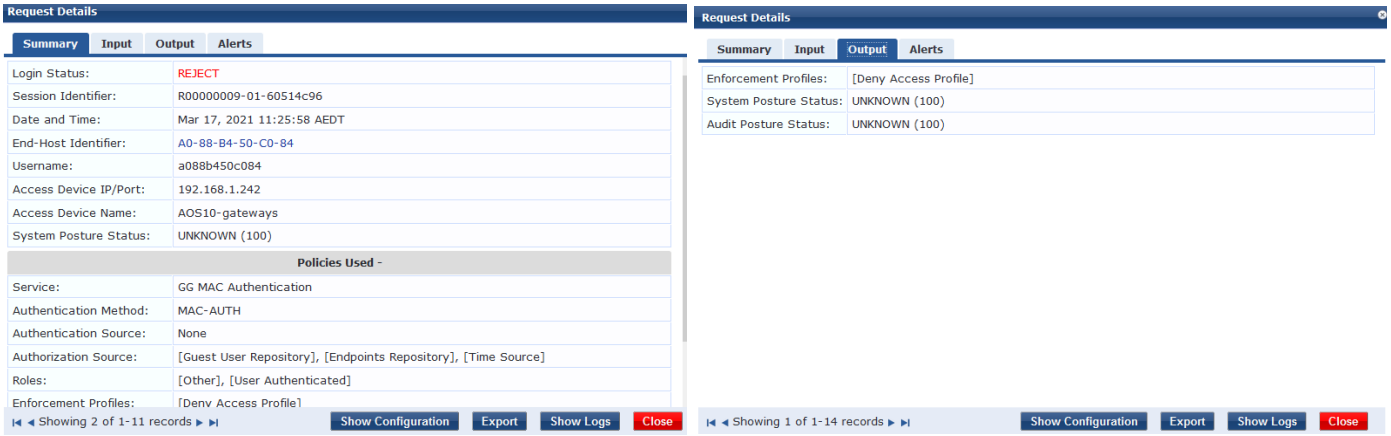


Before we login with our guest credentials, we'll look at the MM dashboard and see the user is in guest-login role with minimum access.



Then we'll check the access tracker and see that we have a failed MAC authentication.





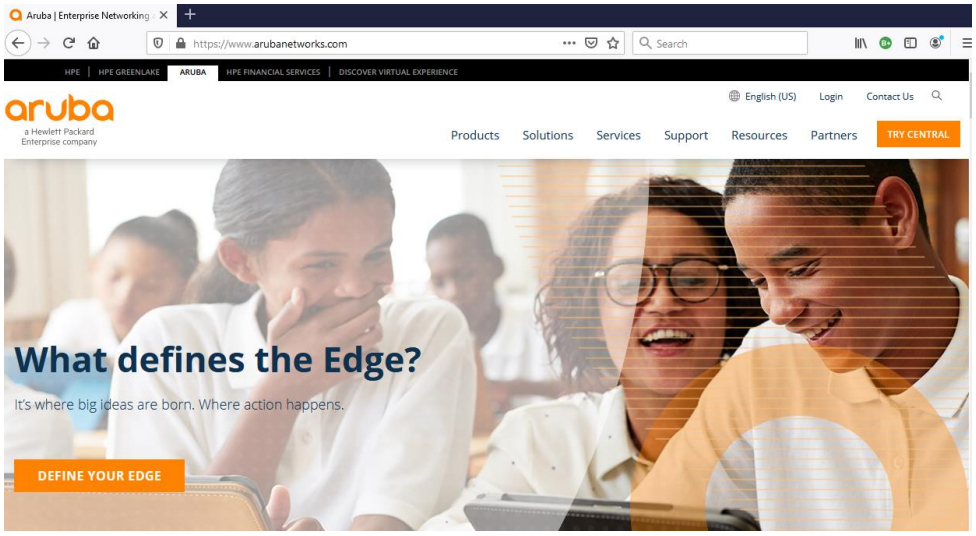
This is normal as this MAC address has not been seen before.

It should be noted that the redirection happens from the AP not the gateways

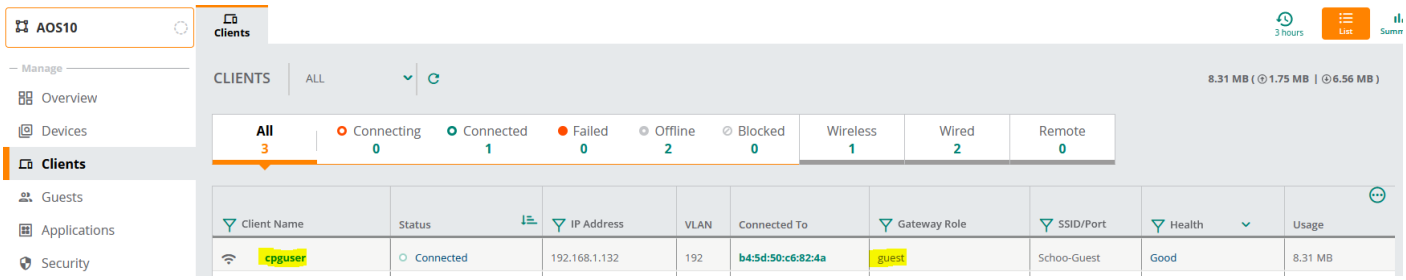
```
b4:5d:50:c6:82:4a# sh client
```

```
Client List
-----------
Name  IP Address  MAC Address  OS  ESSID  Access Point  Channel  Type  Role  IPv6
Address  Signal  Speed (mbps)
----  ----------  -----------  --  -----  ------------  -------  ----  ----  ----------
--  ------  ------------
Number of Clients   :0
Info timestamp      :8460
b4:5d:50:c6:82:4a#
b4:5d:50:c6:82:4a#
b4:5d:50:c6:82:4a# sh client

Client List
-----------
Name          IP Address     MAC Address        OS      ESSID        Access Point
Channel  Type  Role      IPv6 Address              Signal    Speed (mbps)
----          ----------     -----------        --      -----        ------------
-------  ----  ----      ------------              ------    ------------
a088b450c084  192.168.1.132  a0:88:b4:50:c0:84  Win 10  Schoo-Guest  b4:5d:50:c6:82:4a
6        GN    CP-Guest  fe80::7d4a:2f07:955c:cd4f  54(good)  72(ok)

Number of Clients   :1
Info timestamp      :9155

b4:5d:50:c6:82:4a#
b4:5d:50:c6:82:4a# sh external-captive-portal

External Captive Portal
-----------------------
Name      Server                  Port  Url                Auth Text      Redirect Url
Server Fail Through  Disable Auto Whitelist  Use HTTPs  Server Offload  Prevent Frame
Overlay  In Use  Redirect Mode  Switch IP
----      ------                  ----  ---                ---------      ------------
-------------------  ----------------------  ---------  --------------  ---------------
default   localhost               80    /                  Authenticated
Disable              Enable                  Yes        No              Disable
No      Yes            No
CP-Guest  victory.clearpass.info  443   /guest/school.php
http://www.arubanetworks.com  Disable              Enable                  Yes
No              Disable                Yes     Yes            No

b4:5d:50:c6:82:4a# sh external-captive-portal CP-Guest

Name                    :CP-Guest
Server                  :victory.clearpass.info
Port                    :443
Url                     :/guest/school.php
Auth Text               :
Redirect Url            :http://www.arubanetworks.com
Server Fail Throuth     :Disable
Disable Auto Whitelist  :Enable
Use HTTPs               :Yes
Server Offload          :No
Prevent Frame Overlay   :Disable
In Used                 :Yes
Redirect Mode           :Yes
Switch IP               :No
b4:5d:50:c6:82:4a#
```

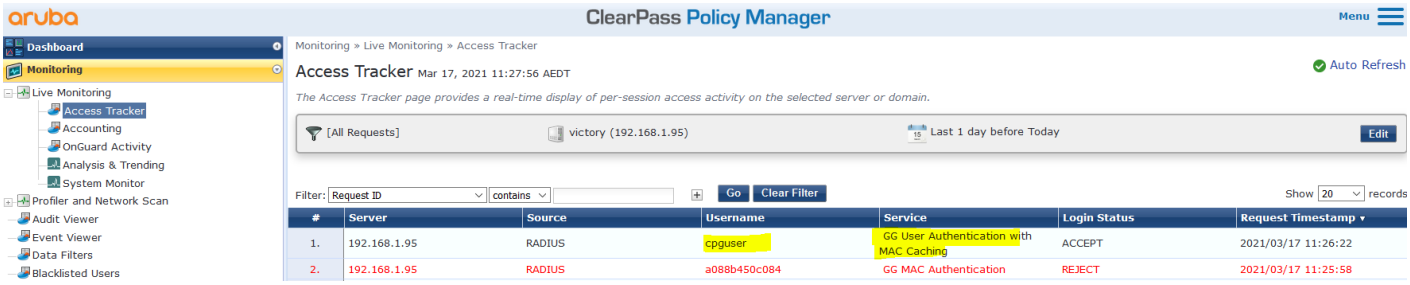
Now when the user performs a successful the login (we are using username cpguser) process, they will be redirected to the “redirect URL” that we specified.

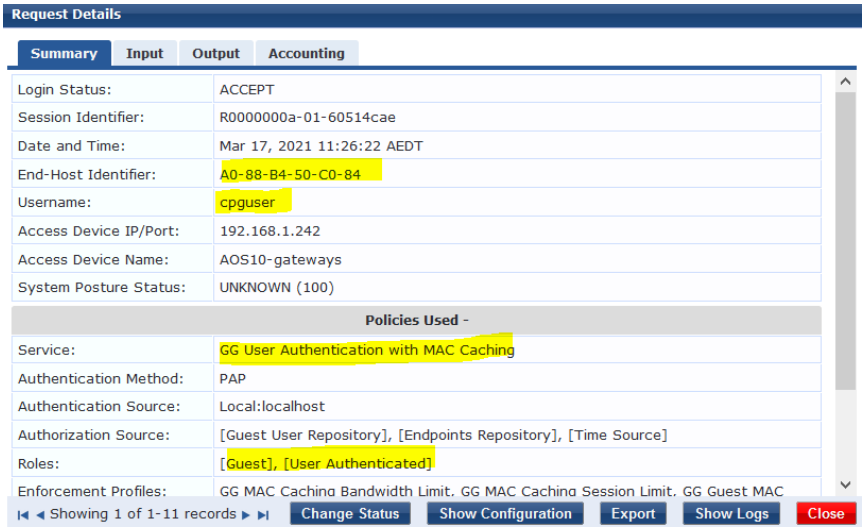


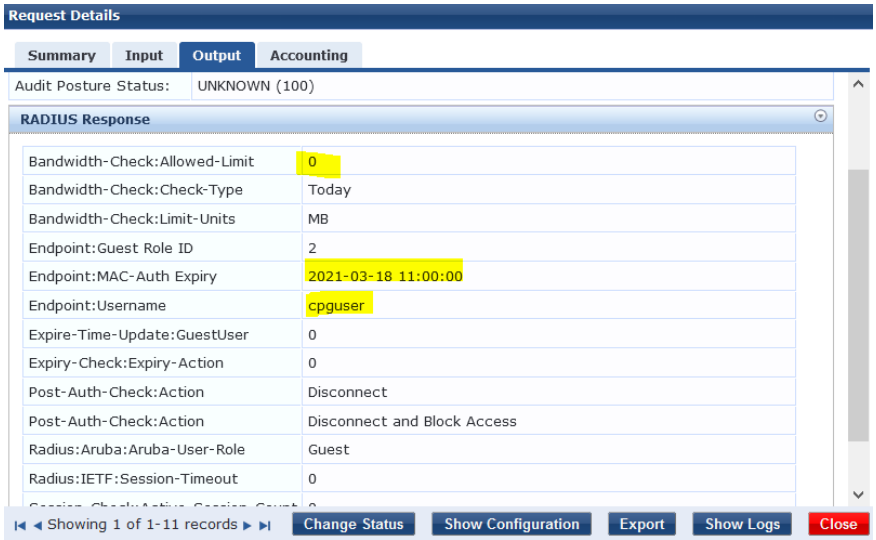
Now let's look at the Client dashboard and access tracker, note that the user role is now "guest".



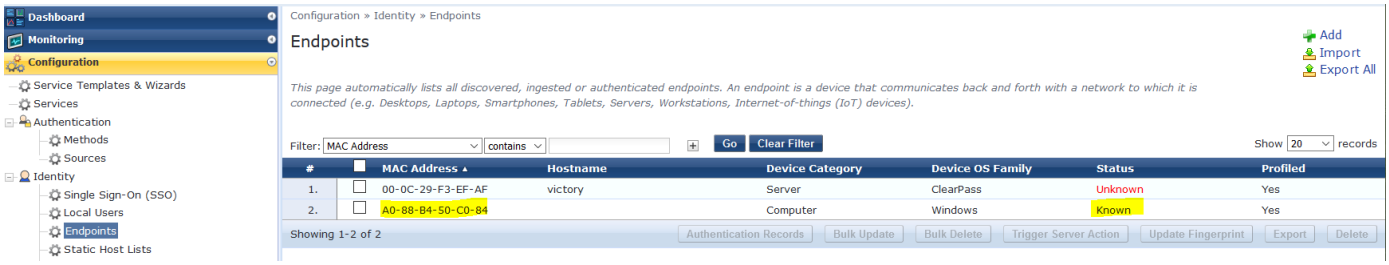
And the access tracker shows a successful authentication that matches with "GG User Authentication with MAC Caching" policy.



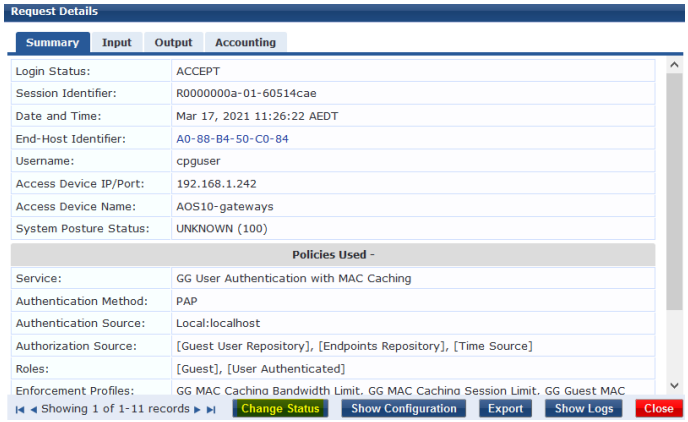


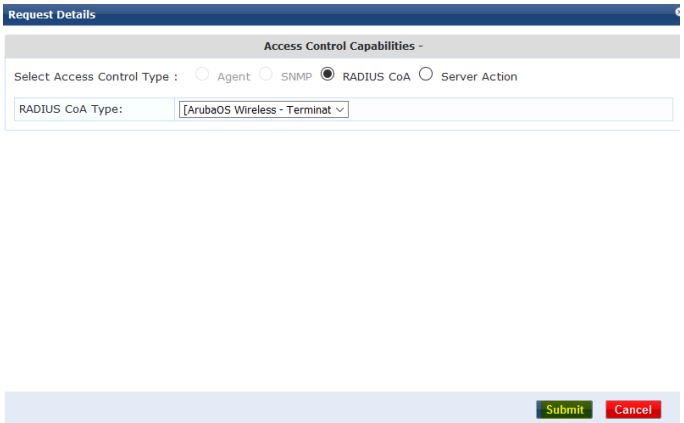


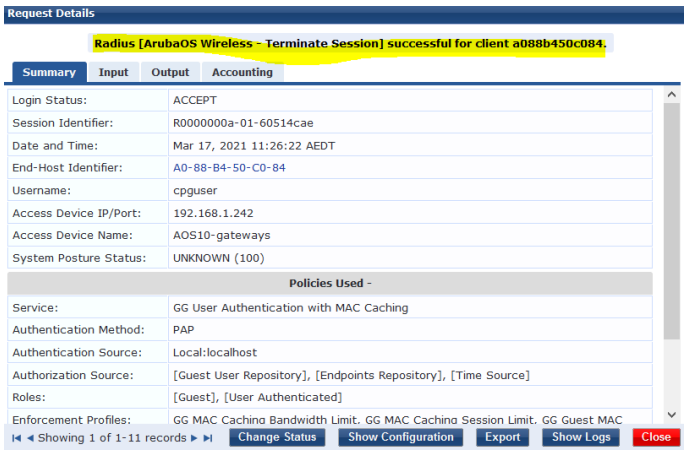
Also note that one of the post authentication actions were to update the endpoint repository status for that MAC address to be known.

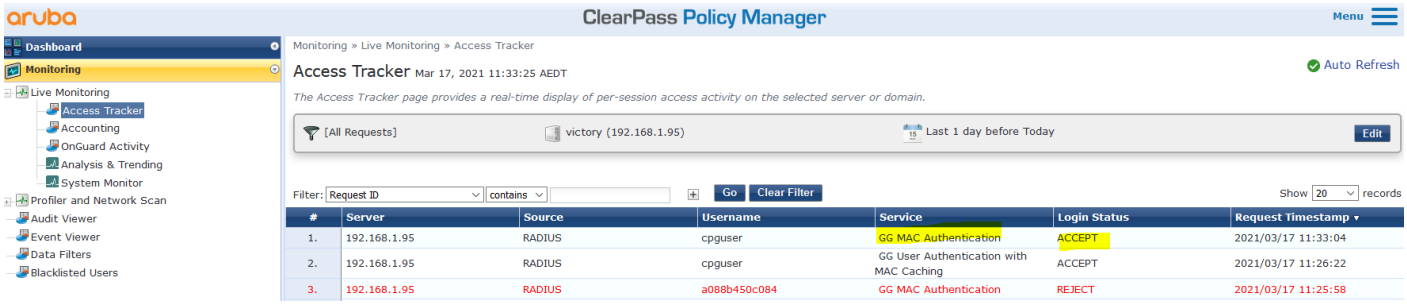


Now because the status of this endpoint is known the next time, this client connects it will not be redirected to the captive portal until its allotted time has expired. So now if we disconnect the client, we should see it will successfully MAC auths. This uses RADIUS CoA. We can do that directly from the access tracker.

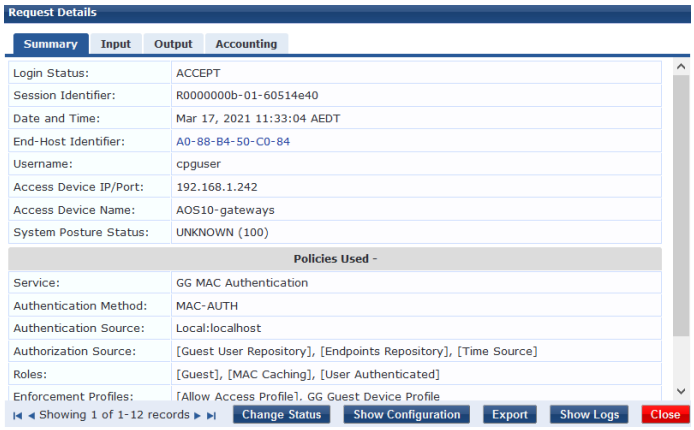


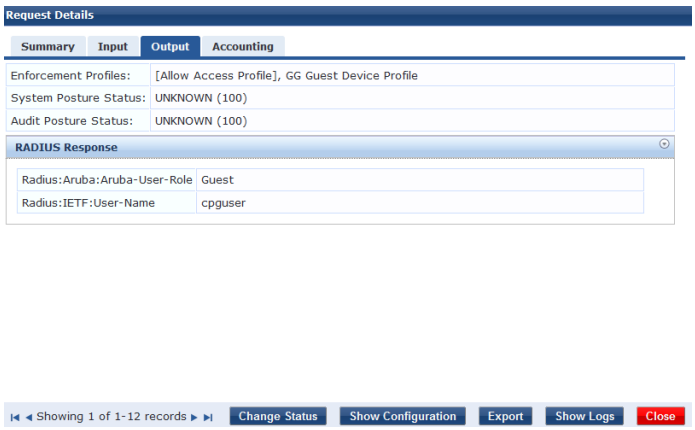






Looking at the details of that session





Here we can see the user in the gateway's user table using tunnel forwarding mode and in guest user role.

```
(7005_AOS10_gwy2) #show user
This operation can take a while depending on number of users. Please be patient ....

Users
-----
    IP              MAC            Name         Role      Age(d:h:m)  Auth  VPN link
Connected To     Roaming   Essid/Bssid/Phy  Profile                          Forward
mode  Type    Host Name  User Type
----------     ------------       ------        ----      ----------  ----  --------  -
----------------  -------   ---------------  -------                        --------
----  ----    ---------  ---------
192.168.1.132  a0:88:b4:50:c0:84  a088b450c084  guest     00:00:03    MAC
b4:5d:50:c6:82:4a   Wireless  Schoo-Guest      Schoo-Guest_#1615938135060_41#_  dtunnel
Win 10             WIRELESS

User Entries: 1/1
 Curr/Cum Alloc:1/6 Free:0/5 Dyn:1 AllocErr:0 FreeErr:0
(7005_AOS10_gwy2) #
```