

# Contents

- 1.1 Revision History ..... 1
- 2 Demo Topology ..... 2
- 3 Aruba Central Account ..... 3
- 4 Aruba Central Configuration ..... 6
  - 4.1 LAN Switch Configuration ..... 6
  - 4.2 Gateway Configuration ..... 7
  - 4.3 AP Configuration..... 12
  - 4.4 Assigning Static IP addresses for APs..... 14
  - 4.5 Firmware Upgrade ..... 14
  - 4.6 Gateway Cluster ..... 17
  - 4.7 Monitoring Gateway Cluster ..... 17
- 5 ClearPass Initial Configuration ..... 20
  - 5.1 Joining AD Domain..... 21
  - 5.2 ClearPass dot1x Service ..... 22
  - 5.3 NAD Configuration..... 24
- 6 WLAN Configuration..... 25
  - 6.1 Tunnelled Wireless Configuration ..... 25
  - 6.2 Wireless dot1x Testing..... 27
- 7 RF Monitoring ..... 31
- 8 Guest Access Configuration ..... 37
  - 8.1 Guest Wireless Configuration..... 37
  - 8.2 ClearPass Guest policy Configuration ..... 41
  - 8.3 ClearPass Guest Portal Configuration ..... 46
  - 8.4 Guest Testing..... 50

## 1.1 Revision History

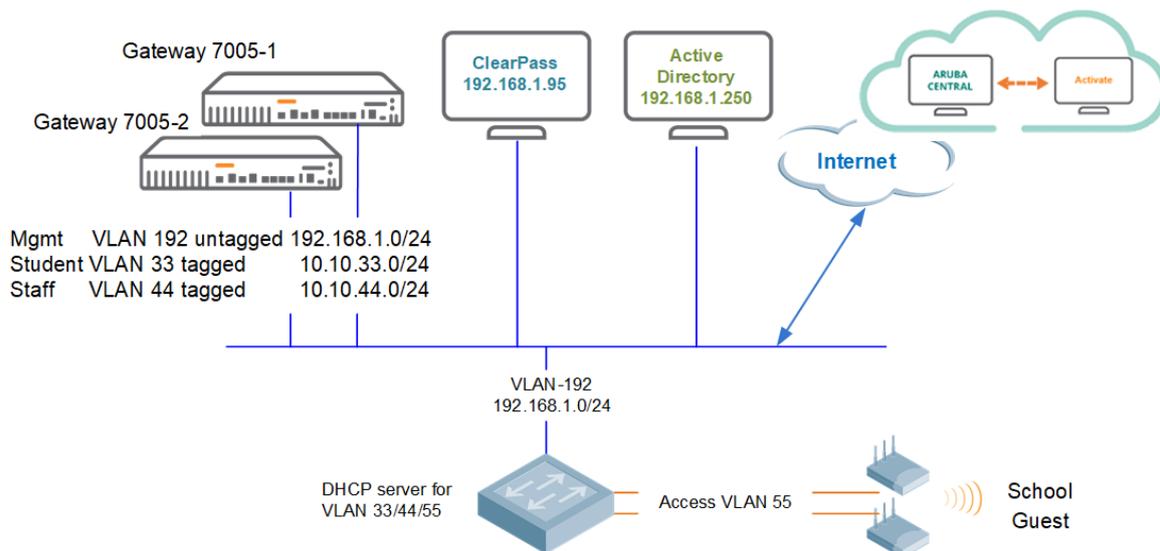
DATE	VERSION	EDITOR	CHANGES
15 Mar 2021	0.1	Ariya Parsamanesh	Initial creation
22 May 2021	0.2	Ariya Parsamanesh	Added the ClearPass guest operator login
04 Jul 2021	0.3	Ariya Parsamanesh	Added the Monitoring section

## 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.

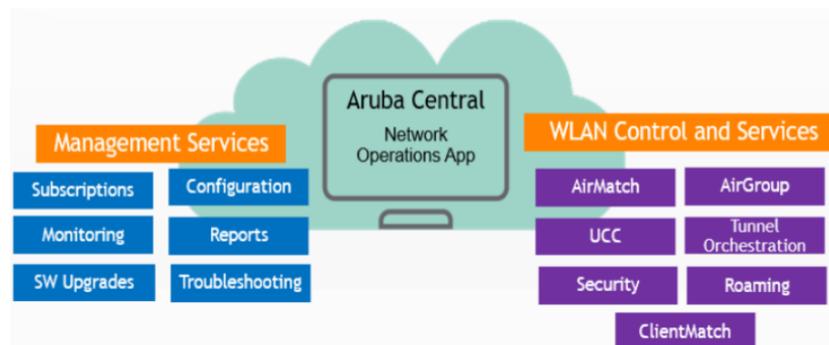
Note that APs in AOS10 support bridged, tunnelled and mix mode wireless LANs (WLAN) however in this technote we'll be deploying tunnelled mode WLANs. We'll also demonstrate the gateway clustering with AOS10.

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](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

## ACCOUNT HOME

Manage your Network Inventory, Subscriptions, and User Access. Use any of the following apps to make Aruba work better for you.

### APPS

90 DAYS LEFT



### Network Operations

Manage your wired, wireless, and WAN infrastructure

LAUNCH

### GLOBAL SETTINGS

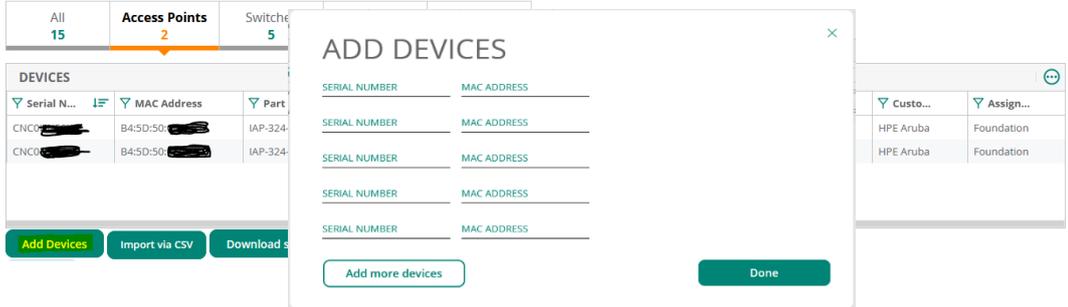
<b>USERS AND ROLES</b> Manage user access	<b>KEY MANAGEMENT</b> Manage your subscription keys	<b>DEVICE INVENTORY</b> Manage the Devices in your Inventory	<b>LICENSE ASSIGNMENT</b> Assign Licenses to Devices
<b>AUDIT TRAIL</b> View audit-trail logs	<b>SINGLE SIGN ON</b> Create and manage SAML Profiles	<b>API GATEWAY</b> Access API Gateway and manage access tokens	<b>WEBHOOKS</b> Manage Webhook end points

Here I have already added my APs.

## Account Home > Device Inventory

If the devices associated with your account are not automatically discovered and are not displayed in your inventory, you can add devices manually by clicking the ADD DEVICES text.

You can also add your devices using the Aruba Central mobile app and they will automatically appear in your inventory.

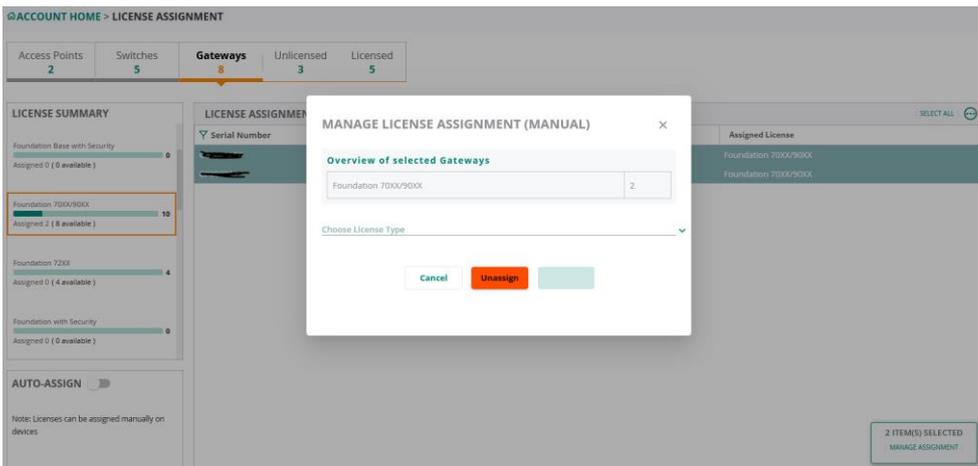
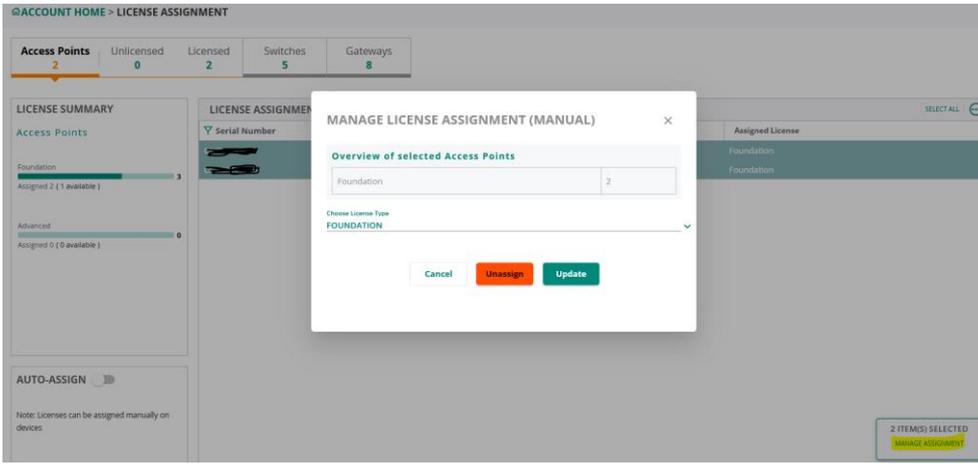


The screenshot shows the 'Device Inventory' page with a modal window titled 'ADD DEVICES'. The modal contains a table with columns for 'SERIAL NUMBER' and 'MAC ADDRESS', and a 'Done' button at the bottom right. The background page shows a table of devices with columns for 'Serial N...', 'MAC Address', and 'Part'.

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"

### GLOBAL SETTINGS

<b>USERS AND ROLES</b> Manage user access	<b>KEY MANAGEMENT</b> Manage your subscription keys	<b>DEVICE INVENTORY</b> Manage the Devices in your Inventory	<b>LICENSE ASSIGNMENT</b> Assign Licenses to Devices
<b>AUDIT TRAIL</b> View audit-trail logs	<b>SINGLE SIGN ON</b> Create and manage SAML Profiles	<b>API GATEWAY</b> Access API Gateway and manage access tokens	<b>WEBHOOKS</b> Manage Webhook end points



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

#### ACCOUNT HOME

Manage your Network Inventory, Subscriptions, and User Access. Use any of the following apps to make Aruba work better for you.

#### APPS

EVALUATION 413 DAYS LEFT



**Network Operations**

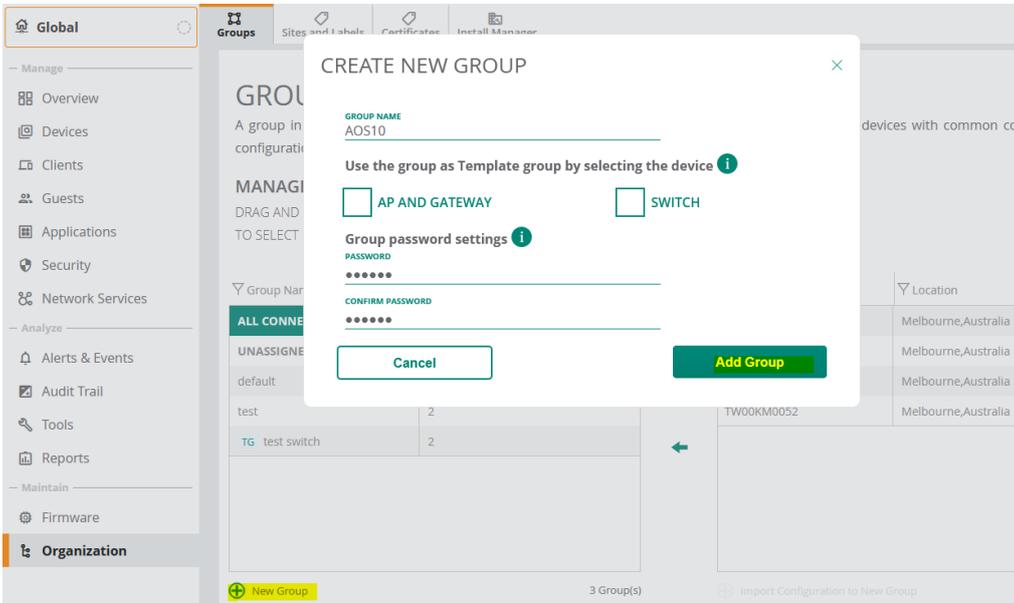
Manage your wired, wireless, and WAN infrastructure

LAUNCH

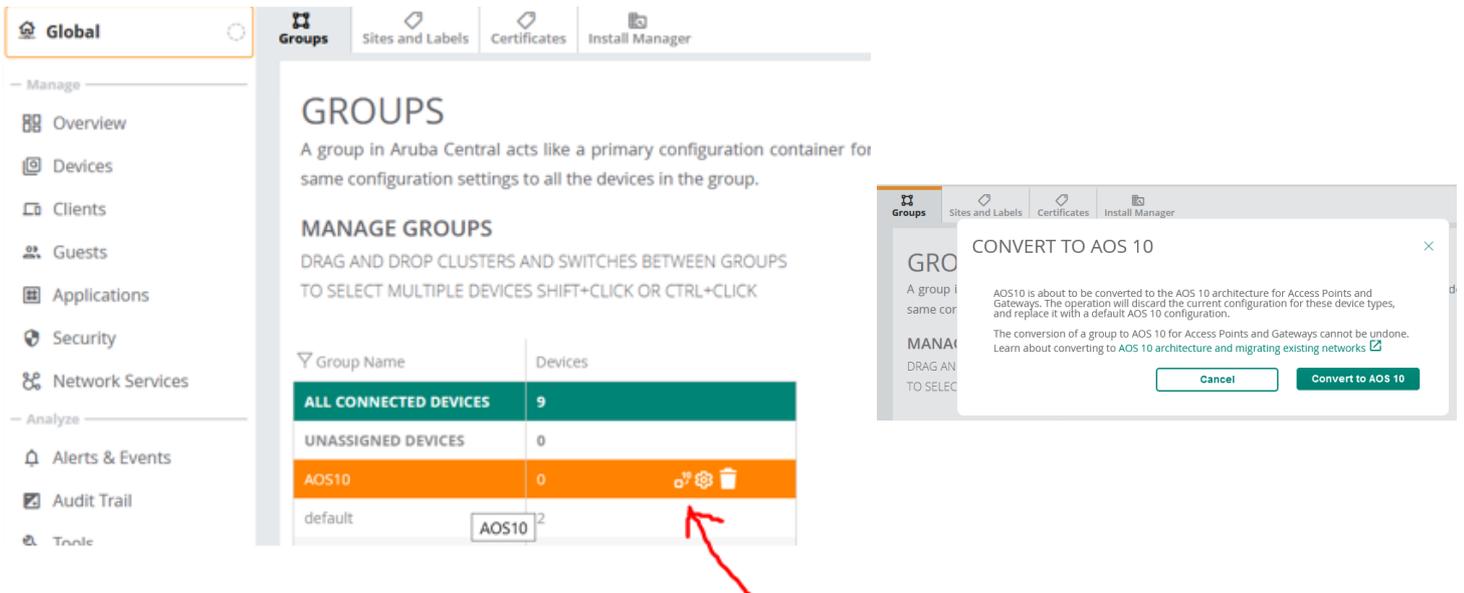
#### GLOBAL SETTINGS

<p style="font-size: 0.8em; margin: 0;"><b>USERS AND ROLES</b></p> <p style="font-size: 0.7em; margin: 0;">Manage user access</p>	<p style="font-size: 0.8em; margin: 0;"><b>KEY MANAGEMENT</b></p> <p style="font-size: 0.7em; margin: 0;">Manage your subscription keys</p>	<p style="font-size: 0.8em; margin: 0;"><b>DEVICE INVENTORY</b></p> <p style="font-size: 0.7em; margin: 0;">Manage the Devices in your inventory</p>	<p style="font-size: 0.8em; margin: 0;"><b>LICENSE ASSIGNMENT</b></p> <p style="font-size: 0.7em; margin: 0;">Assign Licenses to Devices</p>
<p style="font-size: 0.8em; margin: 0;"><b>AUDIT TRAIL</b></p> <p style="font-size: 0.7em; margin: 0;">View audit-trail logs</p>	<p style="font-size: 0.8em; margin: 0;"><b>SINGLE SIGN ON</b></p> <p style="font-size: 0.7em; margin: 0;">Create and manage SAML Profiles</p>	<p style="font-size: 0.8em; margin: 0;"><b>API GATEWAY</b></p> <p style="font-size: 0.7em; margin: 0;">Access API Gateway and manage access tokens</p>	<p style="font-size: 0.8em; margin: 0;"><b>WEBHOOKS</b></p> <p style="font-size: 0.7em; margin: 0;">Manage Webhook end points</p>

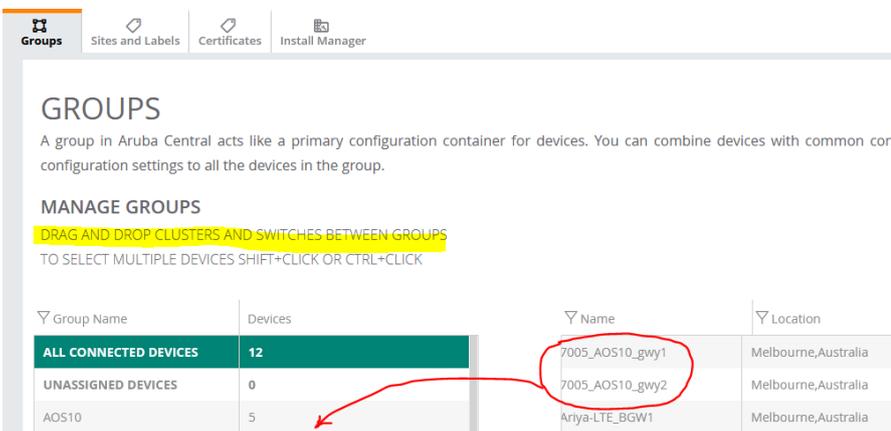
Here we'll create a group and move the devices into it. The groups are used for device configurations.



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.

The screenshot shows the configuration page for an Aruba 2930F switch. The 'SWITCHES' tab is active, displaying a table with the following data:

Hostname	IP Address	Default Gateway	MAC Address	Location	Contact
Aruba-2930F-8G-PoEP-25FPP	10.224.254.2	10.224.254.1	b0:5a:da:98:9a:00	Melbourne	--

The screenshot shows the 'VLANs Settings' configuration page for the switch. The 'VLANs' table is expanded, showing the following data:

ID	Name	IP Assignment	IP Address	Tagged Ports	Untagged Ports	DHCP Helper IP	Voice	Jumbo
1	DEFAULT_VLAN	DHCP		--	6,9-10	--	×	×
33	student-VLAN	Static	10.10.33.1	5,7	2	--	×	×
44	Staff-VLAN	Static	10.10.44.1	5,7	--	--	×	×
55	AP-VLAN	Static	10.10.55.1	--	3,4	--	×	×
192	Server-VLAN	Static	192.168.1.244	--	5,7-8	--	×	×
4085	mgmt-VLAN	Static	10.224.254.2	--	1	--	×	×

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.

The screenshot shows the 'DHCP' configuration page for the switch. The 'DHCP server' toggle is turned on. The 'DHCP Pools' table is expanded, showing the following data:

Name	Network	Netmask	Edit	Delete
AP-VLAN	10.10.55.0	255.255.255.0	/	
Staff-VLAN	10.10.44.0	255.255.255.0	/	
Student-VLAN	10.10.33.0	255.255.255.0	/	

```
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#

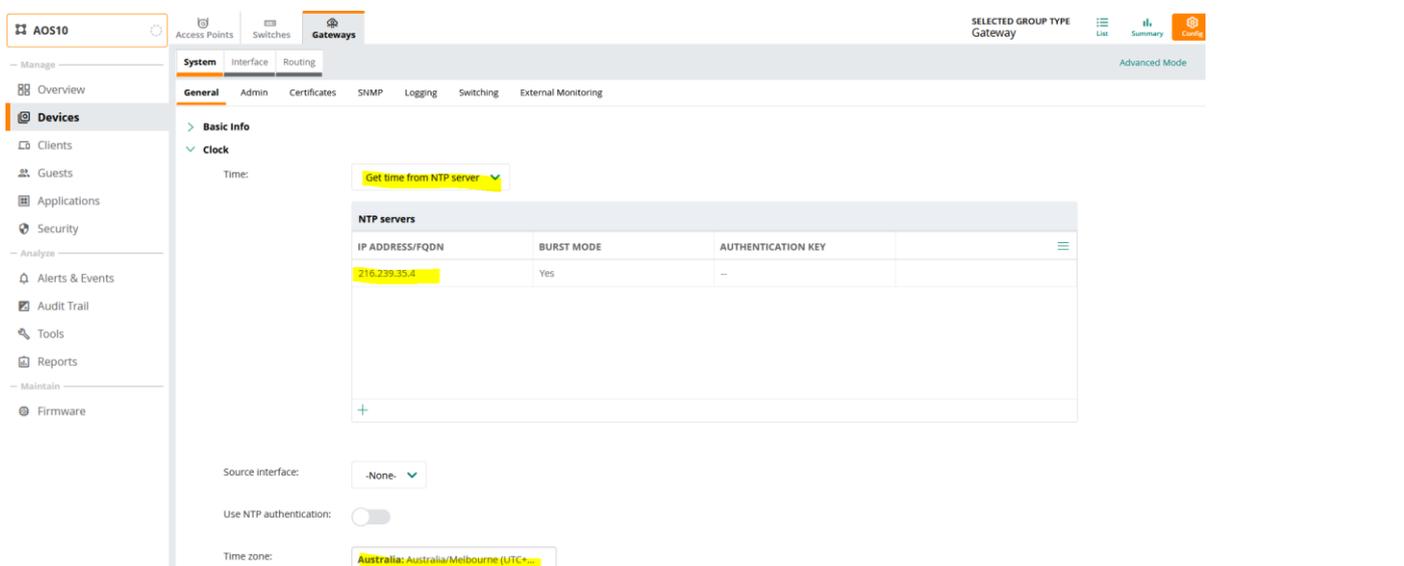
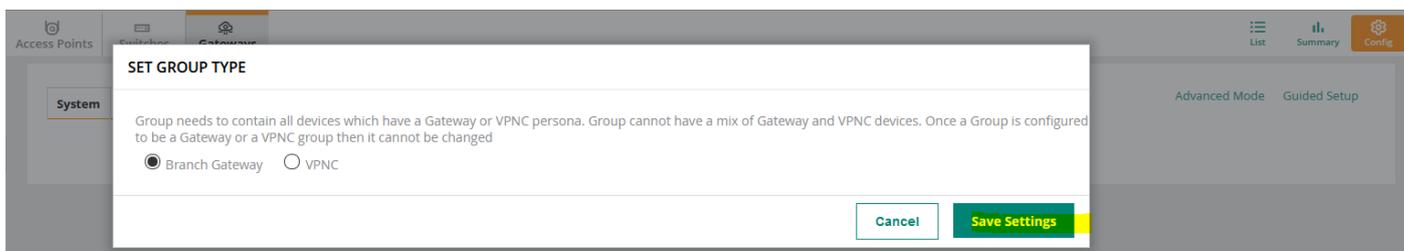
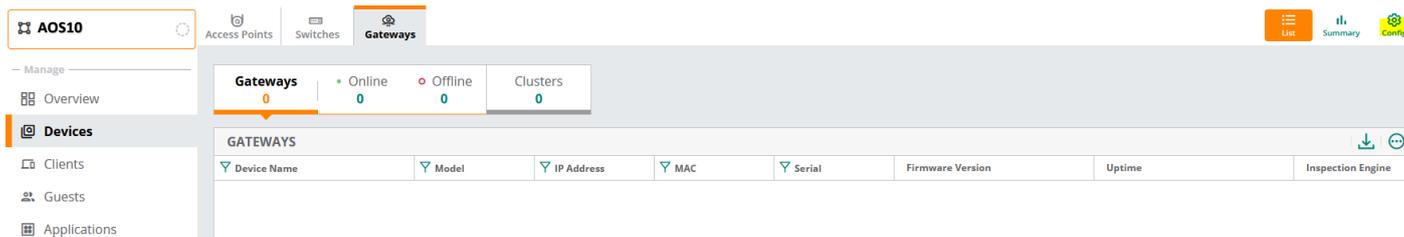
```

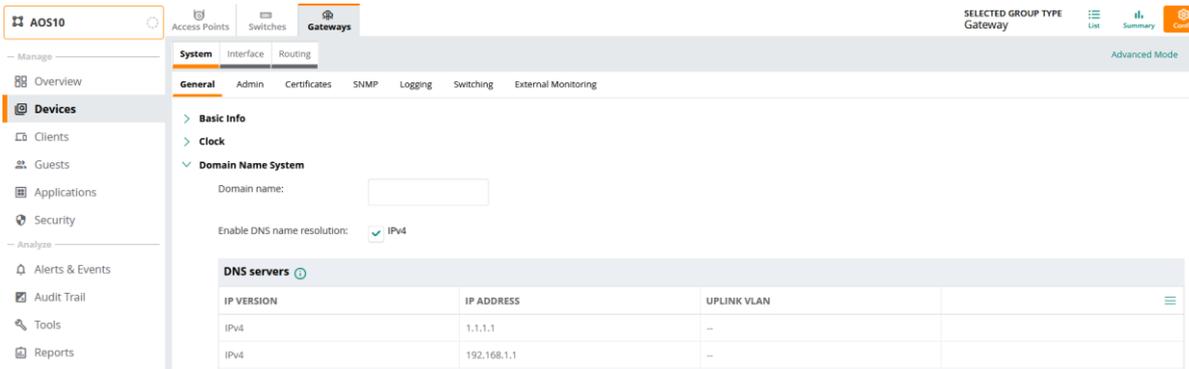
## 4.2 Gateway Configuration

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.

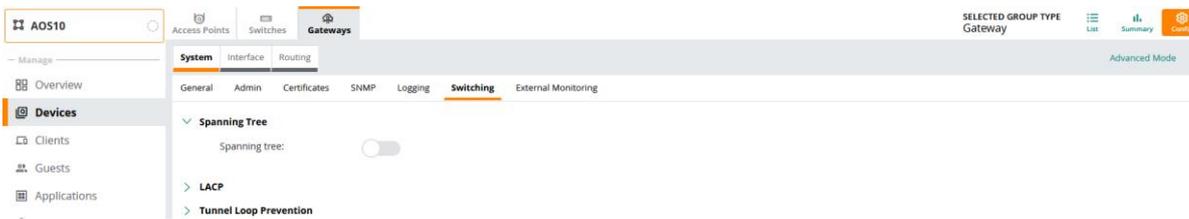
We'll start the configuration at group level before powering up the gateways. This is to minimise the reboots and some potential network issues especially when it comes to changing IP address and losing connectivity.

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

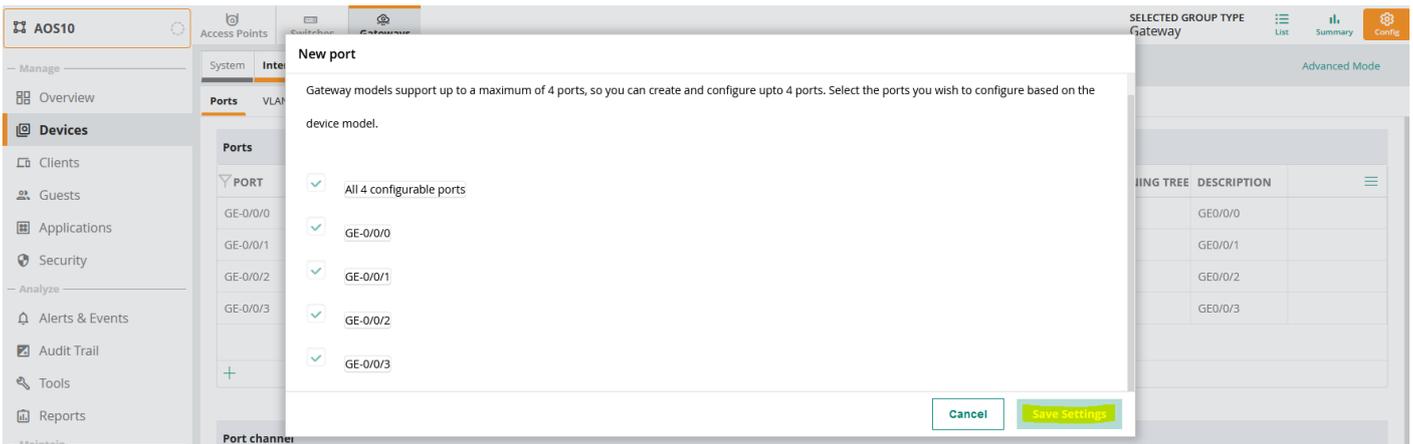




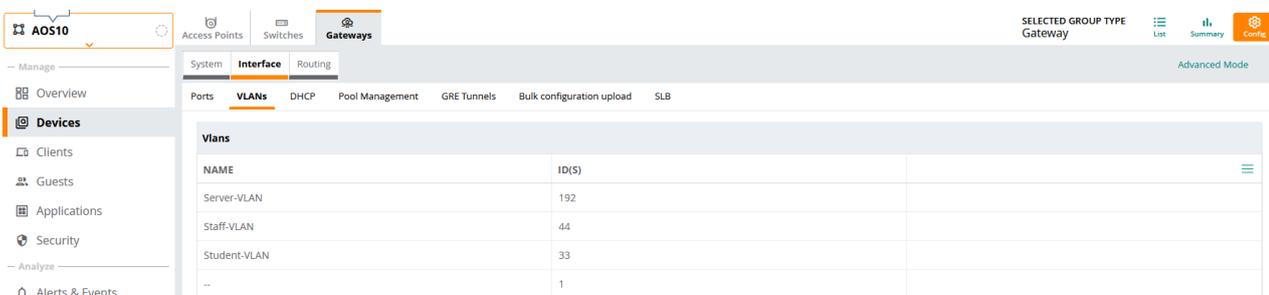
## Disabling spanning tree



## Adding the relevant ports for Aruba 7005 gateway.



I am planning to use 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.

**AOS10** | Access Points | Switches | Gateways | SELECTED GROUP TYPE Gateway | List | Summary | Config | Advanced Mode

System | Interface | Routing

Ports | VLANs | DHCP | Pool Management | GRE Tunnels | Bulk configuration upload | SLB

PORT	TYPE	ADMIN STATE	POLICY	MODE	NATIVE VLAN	ACCESS VLAN	TRUNK VLANS	TRUSTED VLANS	SPANNING TREE	DESCRIPTION
GE-0/0/0	--	Enabled	Not-defined	trunk	192	--	33,44,192	33,44,192	✓	GE0/0/0
GE-0/0/1	--	Enabled	Not-defined	access	--	1	--	--	✓	GE0/0/1
GE-0/0/2	--	Enabled	Not-defined	access	--	1	--	1-4094	✓	GE0/0/2
GE-0/0/3	--	Enabled	Not-defined	access	--	1	--	1-4094	✓	GE0/0/3

**GE-0/0/0**

Type: LAN

Admin state:

Speed: auto Mbps

Duplex: auto

Poe:

Trust:  

Policy: Not-defined

Mode: Trunk

Native VLAN: 192

Allowed VLANs: 33,44,192

Description: GE0/0/0

Jumbo MTU:

Port monitoring: -None-

### Adding the default route

**AOS10** | Access Points | Switches | Gateways | SELECTED GROUP TYPE Gateway | List | Summary | Config | Basic Mode

System | Interface | Routing | WAN | Security | VPN | High Availability | Config Audit

IP Routes | Policy-Based Routing | NextHop Configuration | RIP | OSPF | BGP | Overlay Routing

IP Routes

Static Default Gateway

DEFAULT GATEWAY	COST
192.168.1.1	1

### Adding the user roles by going to "security tab"

**AOS10** | Access Points | Switches | Gateways | SELECTED GROUP TYPE Gateway | List | Summary | Config | Basic Mode

System | Interface | Roles | Policy

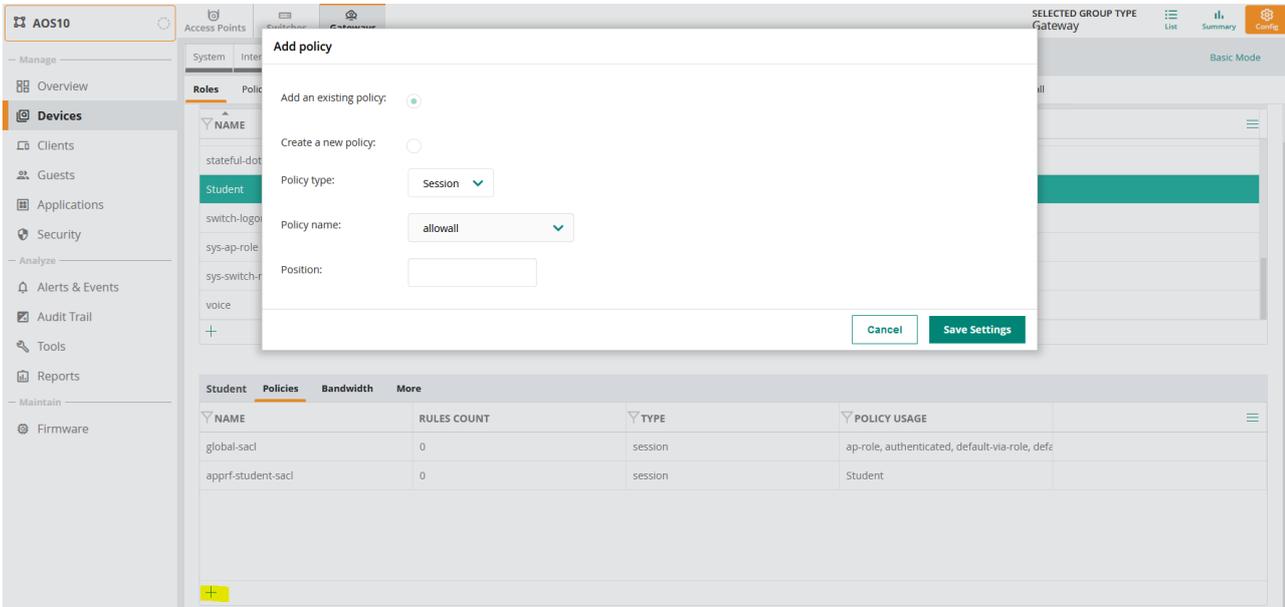
Roles

New role

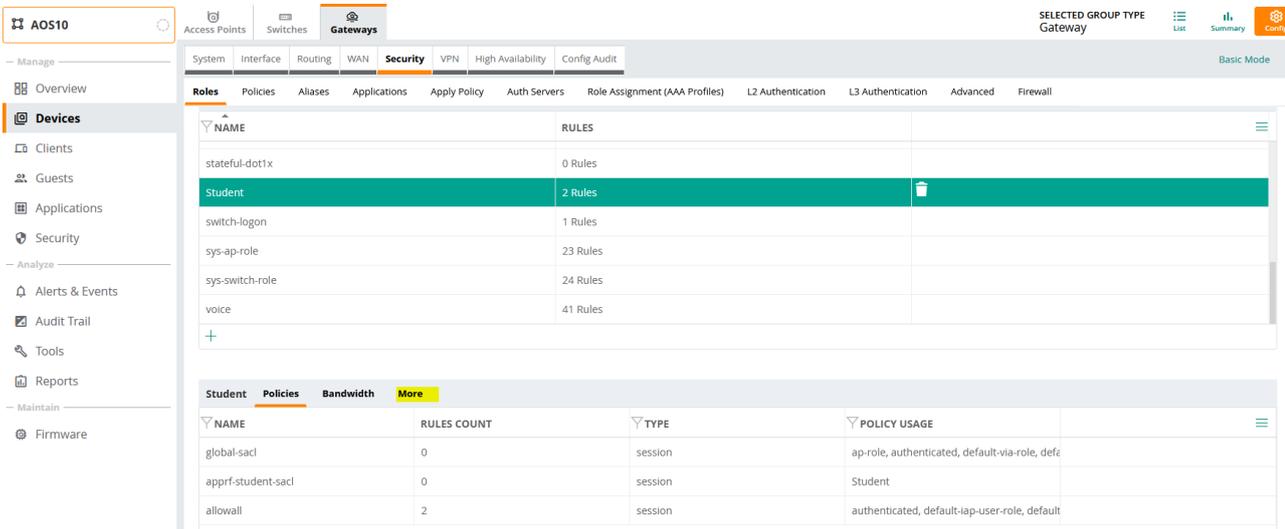
Name: Student

Cancel | Save Settings

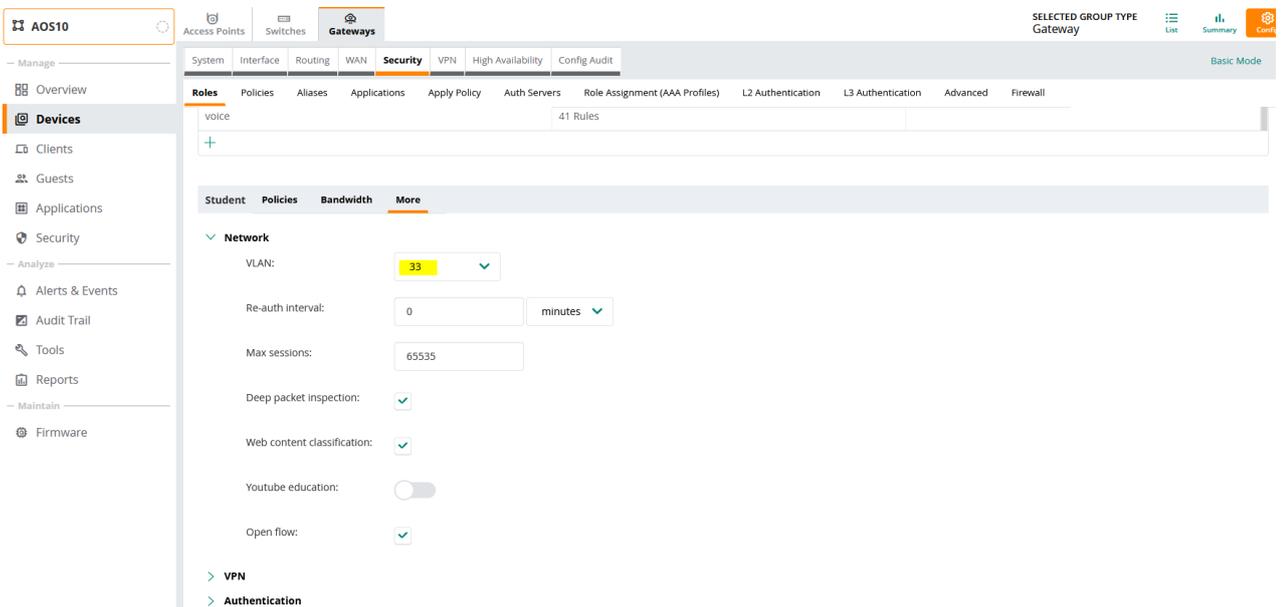
NAME	Rules
ap-role	35 Rules
authenticated	4 Rules
default-iap-user-role	2 Rules
default-via-role	3 Rules
default-vpn-role	4 Rules
guest	11 Rules



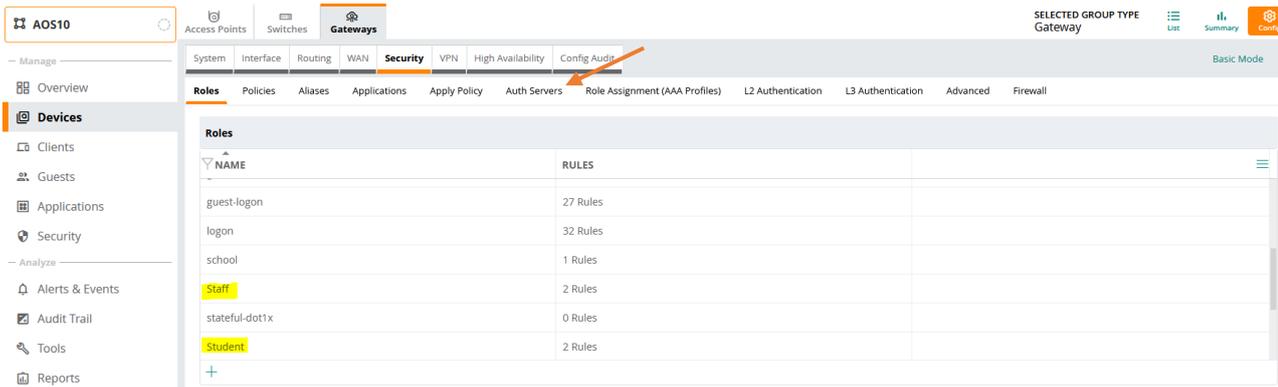
Here we'll add the allow-all policy.



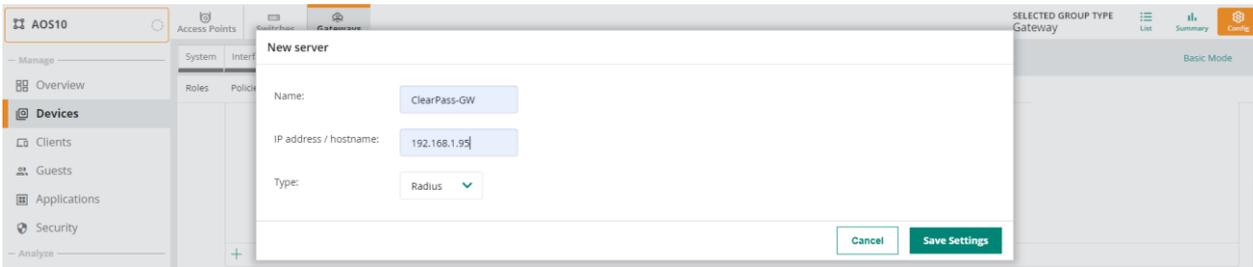
Next, we'll assign a VLAN to this role.



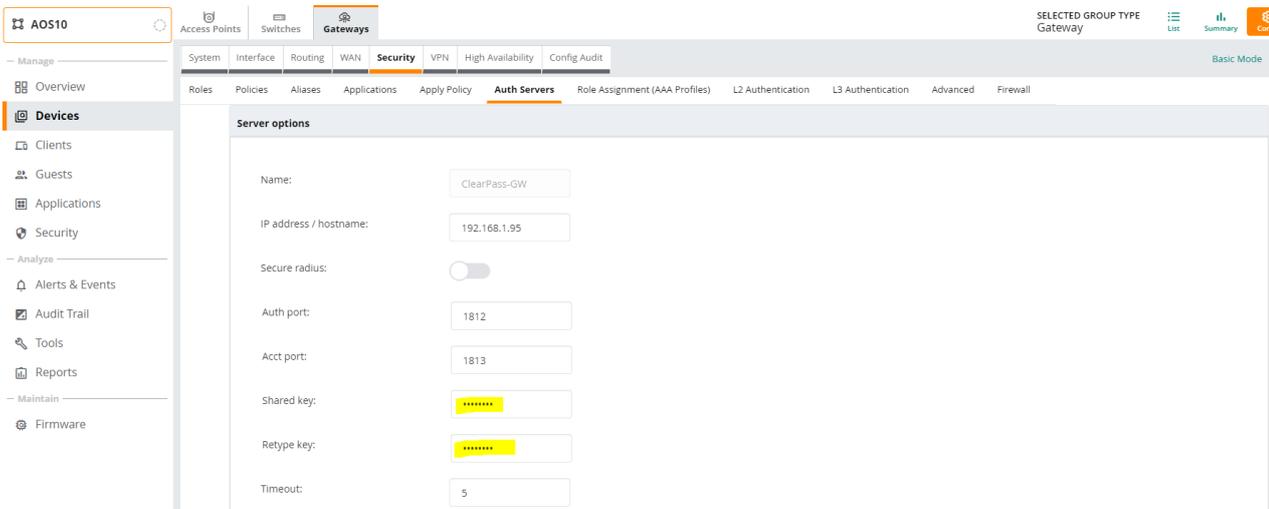
We'll create a new user role staff and as before, we'll add a allow-all policy and assign VLAN 44 to it.



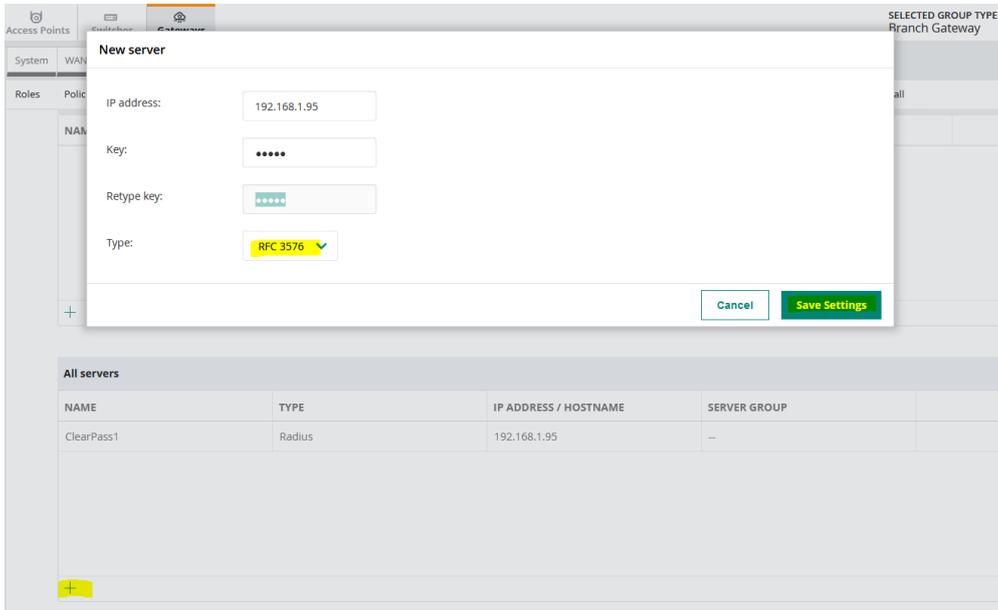
We'll configure the authentication server and RFC3576 for RADIUS CoA



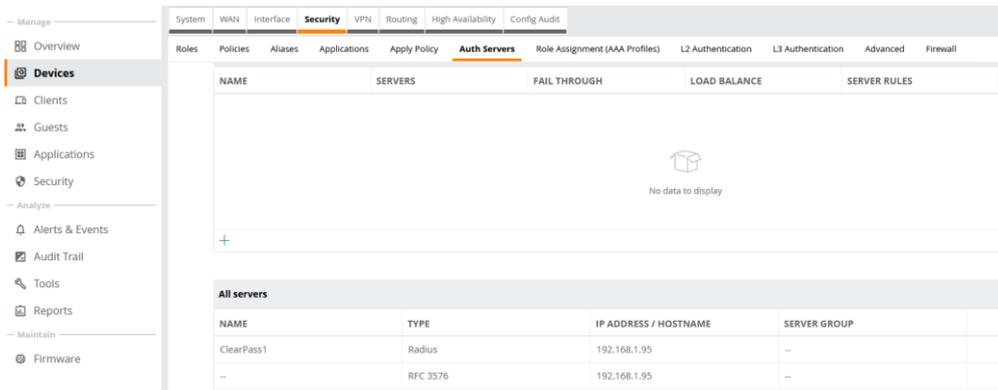
Then once saved, click on it to set the RADIUS secret key



And finally add a rfc3576 server for CoA.

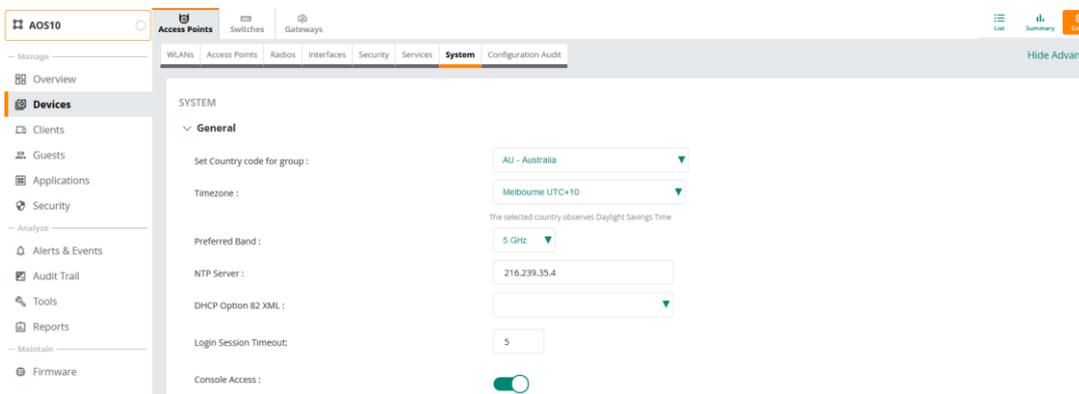


Note that they are not assigned to any authentication server groups.



### 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.



Console Access :

WebUI Access :

Telnet Server :

LED Display :

Deny Inter User Bridging :

Deny Local Routing :

Mobility Access Switch Integration :

URL Visibility :

Restrict uplink port to specified VLANs :

VOIP QoS Trust :

- > Administrator
- > Mesh
- > Time-Based Services
- > Enterprise Domains
- > Logging
- > SNMP
- > Proxy
- > IPM

**AOS10** | Access Points | Switches | Gateways

WLANs | Access Points | Radios | Interfaces | **Security** | Services | System | Configuration Audit

SECURITY

Authentication Servers

Name	Type

NEW SERVER

Server Type: RADIUS

Name: ClearPass Radsec:

IP Address: 192.168.1.95 Auth Port: 1812

Shared Key: \*\*\*\*\* NAS IP Address: optional

Retype Key: \*\*\*\*\* NAS Identifier: optional

Timeout: 5 sec Retry Count: 3

Service Type Framed User:  MAC/Captive Portal  Query Status of RADIUS Servers(RFC 5997):  Authentication  Accounting

Dynamic Authorization:  Accounting Port: 1813

Cancel Save

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

**AOS10** | Access Points | Switches | Gateways

WLANs | Access Points | Radios | Interfaces | **Security** | Services | System | Configuration Audit

SECURITY

Authentication Servers

MPSK Local

User For Internal Server

Roles

Role
Staff
Student
default_wired_port_profile
school
wired-SetMeUp

Access Rules For Selected Roles

- Allow any to all destinations

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.

The screenshot shows the Aruba Central interface for AOS10. The 'Access Points' section is expanded, showing a summary of 2 Online and 1 Offline APs. Below this, a table lists the APs:

Device Name	Status	IP Address	Model	Firmware Version	Group	Uptime
b4:5d:50:c6:82:3c	Offline	10.10.55.10	AP-324	10.2.0.1_79907	AOS10	-
b4:5d:50:c6:82:4a	Online	10.10.55.11	AP-324	10.2.0.1_79907	AOS10	4 Hours 42 Minutes 18 Seconds

The screenshot shows the configuration audit for a specific Access Point. The 'Access Points' tab is active, showing a table with one entry:

Name	Status	IP Address	WLANs	Radio Profile	Type
b4:5d:50:c6:82:3c	Down	10.10.55.10	All SSIDs selected	default	AP-324

The screenshot shows the configuration page for a specific Access Point. The 'SYSTEM' tab is active, showing the following configuration fields:

- Name: b4:5d:50:c6:82:3c
- IP Address For Access Point:  Get IP Address from DHCP server,  Static
- IP Address: xxx.xxx.xxx.xxx (Invalid IP Address)
- Netmask: xxx.xxx.xxx.xxx (Invalid Netmask)
- Default Gateway: xxx.xxx.xxx.xxx (Invalid IP Address)
- DNS Server: xxx.xxx.xxx.xxx,xxx.xxx.xxx
- Domain Name:
- LACP Mode: Passive

## 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
```

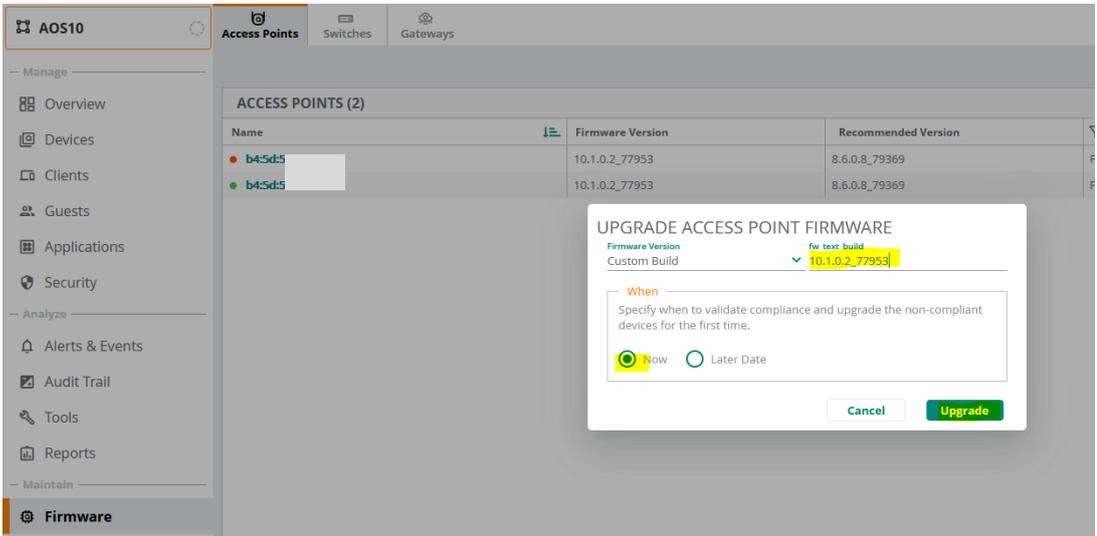
```
Enter System name [Aruba7005]: 7005-1
Enter Switch Role (standalone|md) [md]:
Enter IP type to terminate IPsec tunnel (ipv4|ipv6) [ipv4]:
Enter Master switch IP address/FQDN or ACP IP address/FQDN: device-
apacsouth.central.arubanetworks.com
Enter Master switch type(MM|ACP) ACP
Enter Uplink Vlan 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>

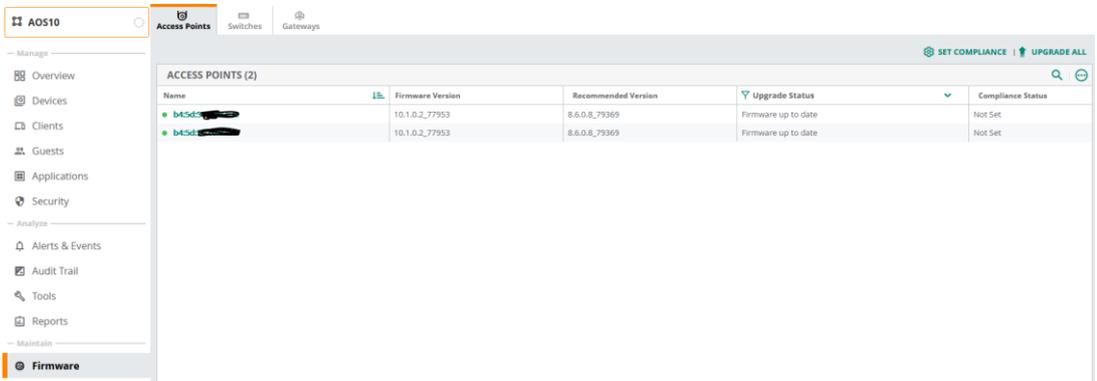
System will now restart!

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

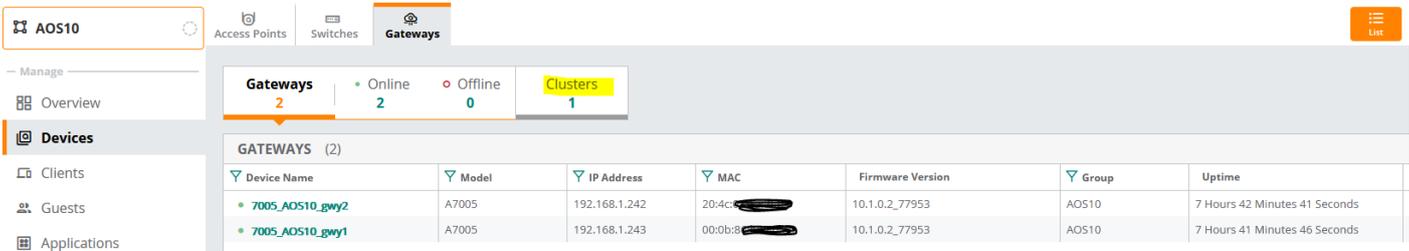
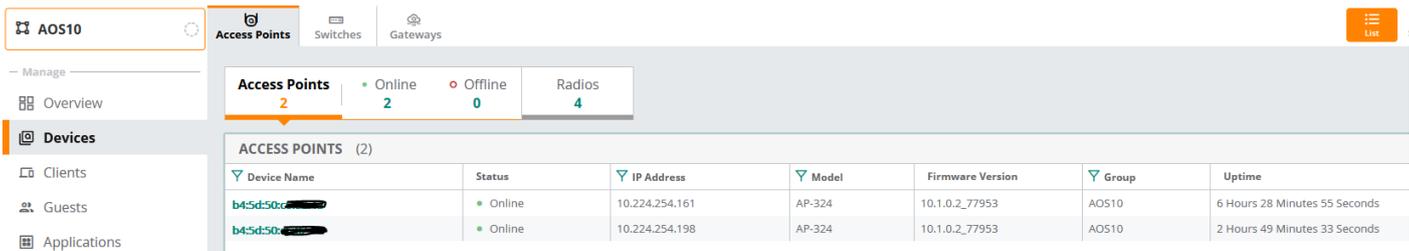
Once the APs and gateways are online in Aruba Central, we'll upgrade them to AOS10 image. In the next release SD-branch and AOS10 firmware will merge. I have already upgraded my APs, but this is how you can do it.



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

Name	Group	AP Tunnel	Clients	Model	Site	Version	Hitless Failover	Max Gateway Failover
auto_gwcluster_178_0 (2)	AOS10	4	2	A7005		10.1.0.2_77953	POSSIBLE	1

Gateway Name	AP Tunnel	Clients	Model	Site	Version	MAC Address	IP Address
7005_AOS10_gwy1	2	1	A7005		10.1.0.2_77953	00:0b:86:b8:80:d0	192.168.1.243
7005_AOS10_gwy2	2	1	A7005		10.1.0.2_77953	20:4c:03:1a:2fb4	192.168.1.242

**CLUSTER INFO**

CLUSTER NAME	CLUSTER CLIENT CAPACITY	VLAN MISMATCH	CURRENT LEADER VERSION
auto_gwcluster_178_0	4096	Yes	10.1.0.2_77953
MAX GATEWAY FAILURE WITHSTAND COUNT	SITE		
1	-		

**CLIENT CAPACITY**

7005\_AOS10\_GWY1  
7005\_AOS10\_GWY2

Legend: > 80% (Dark Blue), > 40% (Medium Blue), < 40% (Light Blue), Invalid (Grey)

**GATEWAYS (2)**

Gateway Name	IP Address	Status	Client Capacity (Active   Standby)	Model	Role	Version
7005_AOS10_gwy1	192.168.1.243	Up	1 (0   1)	A7005	Member	10.1.0.2_77953
7005_AOS10_gwy2	192.168.1.242	Up	1 (1   0)	A7005	Leader	10.1.0.2_77953

**GATEWAY PEER DETAIL (2)**

Type	IP Address	Status	Role	VLAN Mismatch
SELF	192.168.1.243	-	Member	-
PEER	192.168.1.242	Connected	Leader	1

The screenshot shows a network management interface with the following components:

- Navigation:** auto\_gwcluster\_1... (selected), Summary, Gateways, Tunnels.
- Overview:** Alerts & Events, Audit Trail.
- GATEWAY CLUSTER DETAILS:**
  - TUNNEL DOWN - SUMMARY:** A table with columns: AP Name, IP Address, Last Connected, Last Key Recd By AP, Last Key Recd By Gateway, Reason, Gateway Name. It is currently empty.
  - GATEWAYS:** 7005\_AOS10\_GWY1
 

AP Name	IP Address	SSID	Status	Uptime	Last Key Recd By Gateway	Last Key Recd By AP
b4:5d:50:c6:82:3c	10.224.254.198	school	Up	15 Mins 41 Secs	15 Mins: 47 Secs ago	
b4:5d:50:c6:82:4a	10.224.254.161	school	Up	15 Mins 42 Secs	15 Mins: 47 Secs ago	

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.

Administration > Server Manager > Server Configuration

Server Configuration

Change Cluster Password  
Cluster-Wide Parameters  
Clear Machine Authentication Cache  
Make Subscriber  
Manage Policy Manager Zones  
NetEvents Targets  
**Set Date & Time**  
Virtual IP Settings

Publisher Server: victory [192.168.1.95]

#	Server Name	Management Port	Data Port	Zone	Cluster Sync	Last Sync Time
1.	victory	(IPv4) 192.168.1.95	-	default	Enabled	-

Showing 1-1 of 1

Collect Logs Back Up Restore Cleanup Shutdown Reboot

### Change Date and Time

This will change Date & Time for all nodes in the cluster:

**Date & Time** | Time Zone on Publisher

Synchronize time with NTP server

**Primary Server:**

NTP Server: 216.239.35.4

Key ID: [ ]

Key Value: [ ]

Algorithm: [ ]

**Secondary Server (1):**

NTP Server: [ ]

Key ID: [ ]

Key Value: [ ]

Algorithm: [ ]

**WARNING:** After command execution, Policy Manager services will be restarted. This may take a few minutes.

Save Cancel

### Change Date and Time

This will change Date & Time for all nodes in the cluster:

**Date & Time** | Time Zone on Publisher

To change the time zone, select your area from the list below:

- Africa/Abidjan
- Africa/Accra
- Africa/Addis\_Ababa
- Africa/Algiers
- Africa/Asmara
- Africa/Asmera
- Africa/Bamako
- Africa/Bangui
- Africa/Banjul
- Africa/Bissau

Current time zone: Australia/Melbourne(GMT +11:00)

**WARNING:** After command execution, Policy Manager services will be restarted. This may take a few minutes.

Save Cancel

Administration > Server Manager > Server Configuration - victory

Server Configuration - victory (192.168.1.95)

System Services Control Service Parameters System Monitoring Network FIPS

Hostname: victory

FQDN: victory.clearpass.info

Policy Manager Zone: default Manage Policy

Enable Performance Monitoring Display:  Enable this server for performance monitoring display

Insight Setting:  Enable Insight  Enable as Insight Master Current Master:-

Enable Ingress Events Processing:  Enable Ingress Events processing on this server

Master Server in Zone: Primary master

Span Port: -- None --

	IPv4	IPv6	Action
Management Port	IP Address	192.168.1.95	Configure
	Subnet Mask	255.255.255.0	
	Default Gateway	192.168.1.249	
Data/External Port	IP Address		Configure
	Subnet Mask		
	Default Gateway		
DNS Settings	Primary	192.168.1.250	Configure
	Secondary	192.168.1.130	
	Tertiary		
	DNS Caching	Disabled	

AD Domains: [ ] Join AD Domain

## 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.

Policy Manager Zone: default [Manage Policy Manager Zones](#)

Enable Prof: **Join AD Domain**

Enter the FQDN of the controller and the short (NETBIOS) name for the domain:

Domain Controller: wlan-dc.wlan.net

NetBIOS Name: WLAN

In case of a controller name conflict

Use specified Domain Controller

Use Domain Controller returned by DNS query

Fail on conflict

Use default domain admin user [Administrator]

Username: [ ]

Password: [ ]

**Save** **Cancel**

**AD Domains:** Policy Manager is not part of any domain. Join to domain here. **Join AD Domain**

**Join AD Domain**

**Adding host to AD domain**

Adding host to AD domain...

INFO - Fetched REALM 'WLAN.NET' from domain FQDN 'wlan-dc.wlan.net'

INFO - Fetched the NETBIOS name 'WLAN'

INFO - Creating domain directories for 'WLAN'

INFO - Using Administrator as the WLAN-DC's username

Enter Administrator's password:

Using short domain name -- WLAN

Joined 'CP63LAB' to dns domain 'wlan.net'

INFO - Creating service scripts for 'WLAN'

Starting cpass-domain-server\_WLAN: [ OK ]

**Close**

**Join AD Domain**

**Added host to the domain**

INFO - Creating service scripts for 'WLAN'

Starting cpass-domain-server\_WLAN: [ OK ]

INFO - updating domain configuration files

Stopping cpass-domain-server\_WLAN: [ OK ]

[ OK ]

Starting cpass-domain-server\_WLAN: [ OK ]

Stopping cpass-sysmon-server: [ OK ]

Starting cpass-sysmon-server: [ OK ]

Stopping cpass-radius-server: [ OK ]

Starting cpass-radius-server: [ OK ]

INFO - CP63Lab joined the domain WLAN.NET

**Close**

Now we need to add the AD as authentication source

Configuration » Authentication » Sources » Add - Ariya AD

**Authentication Sources - Ariya AD**

**Summary** **General** **Primary** **Attributes**

Name: Ariya AD

Description: [ ]

Type: Active Directory

Use for Authorization:  Enable to use this Authentication Source to also fetch role mapping attributes

Authorization Sources: [ ] **Remove** **View Details**

-- Select --

Server Timeout: 10 seconds

Cache Timeout: 36000 seconds

Backup Servers Priority: [ ] **Move Up ↑** **Move Down ↓** **Add Backup** **Remove**

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: [REDACTED]

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	-
4. Onboard Device Owner	operatingSystemServicePack	OSServicePack	-
	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.

aruba ClearPass Policy Manager

Configuration » Services

### Services

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	✓

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:	<div style="border: 1px solid #ccc; padding: 5px;">           [EAP PEAP]            [EAP TLS]         </div>		<div style="text-align: right;"> <input type="button" value="Move Up ↑"/>  <input type="button" value="Move Down ↓"/>  <input type="button" value="Remove"/>  <input type="button" value="View Details"/>  <input type="button" value="Modify"/> </div>	
	<input type="text" value="--Select to Add--"/>			
Authentication Sources:	<div style="border: 1px solid #ccc; padding: 5px;">           Ariya AD [Active Directory]         </div>		<div style="text-align: right;"> <input type="button" value="Move Up ↑"/>  <input type="button" value="Move Down ↓"/>  <input type="button" value="Remove"/>  <input type="button" value="View Details"/>  <input type="button" value="Modify"/> </div>	
	<input type="text" value="--Select to Add--"/>			
Strip Username Rules:	<input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes			
Service Certificate:	<input type="text" value="--Select to Add--"/>			

Summary	Service	Authentication	Roles	Enforcement
Role Mapping Policy:	<input type="text" value="--Select--"/> <input type="button" value="Modify"/>		<a href="#">Add New Role Mapping Policy</a>	
<b>Role Mapping Policy Details</b>				
Description:	-			
Default Role:	-			
Rules Evaluation Algorithm:	-			

Conditions	Role
------------	------

Summary	Service	Authentication	Roles	Enforcement
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions			
Enforcement Policy:	<input type="text" value="AA Aruba 802.1X Wireless Enforcement Policy"/> <input type="button" value="Modify"/>		<a href="#">Add New Enforcement Policy</a>	
<b>Enforcement Policy Details</b>				
Description:				
Default Profile:	AA Aruba 802.1X Wireless Default Profile			
Rules Evaluation Algorithm:	first-applicable			
<b>Conditions</b>		<b>Enforcement Profiles</b>		
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
<b>Profile:</b>		
Name:	AA Aruba 802.1X Wireless Default Profile	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
<b>Attributes:</b>		
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	
<b>Profile:</b>					
Name:	AA-Aruba 802.1X Wireless Staff Profile				
Description:					
Type:	RADIUS				
Action:	Accept				
Device Group List:	-				
<b>Attributes:</b>					
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	
<b>Profile:</b>					
Name:	AA-Aruba 802.1X Wireless Student Profile				
Description:					
Type:	RADIUS				
Action:	Accept				
Device Group List:	-				
<b>Attributes:</b>					
Type	Name		Value		
1.	Radius:Aruba	Aruba-User-Role	=	Student	

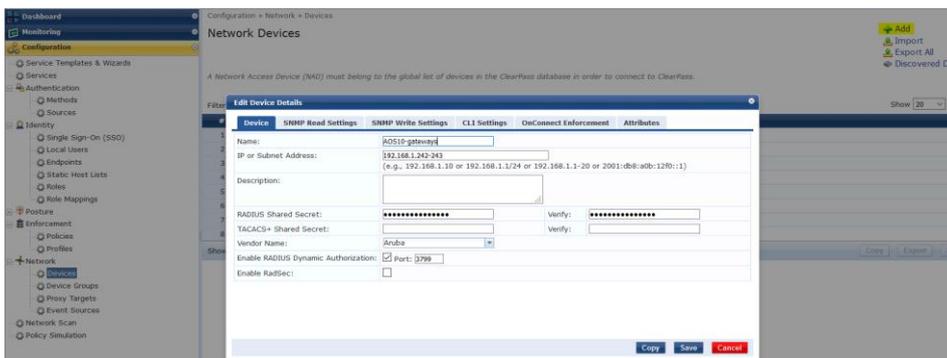
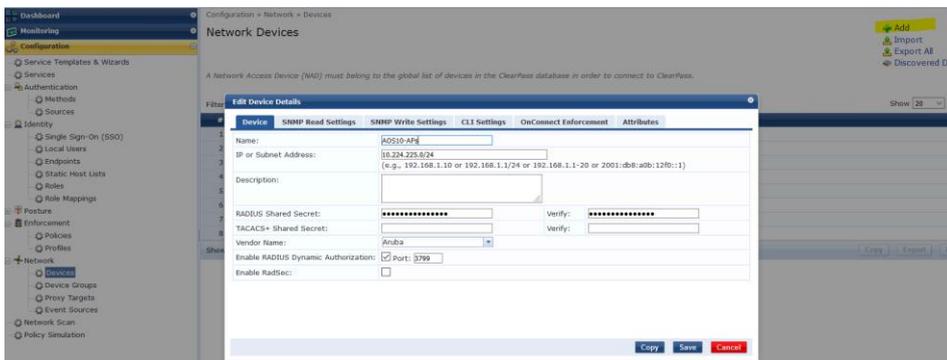
## Enforcement Profiles - AA Aruba 802.1X Wireless Update Endpoint Location

Note: This Enforcement Profile is created by Service Template

Summary		Profile		Attributes	
<b>Profile:</b>					
Name:	AA Aruba 802.1X Wireless Update Endpoint Location				
Description:					
Type:	Post_Authentication				
Action:					
Device Group List:	-				
<b>Attributes:</b>					
Type	Name		Value		
1.	Endpoint	Last Known Location	=	%({Radius:IETF:NAS-IP-Address});-%({Radius:Aruba:Aruba-Location-Id})	

## 5.3 NAD Configuration

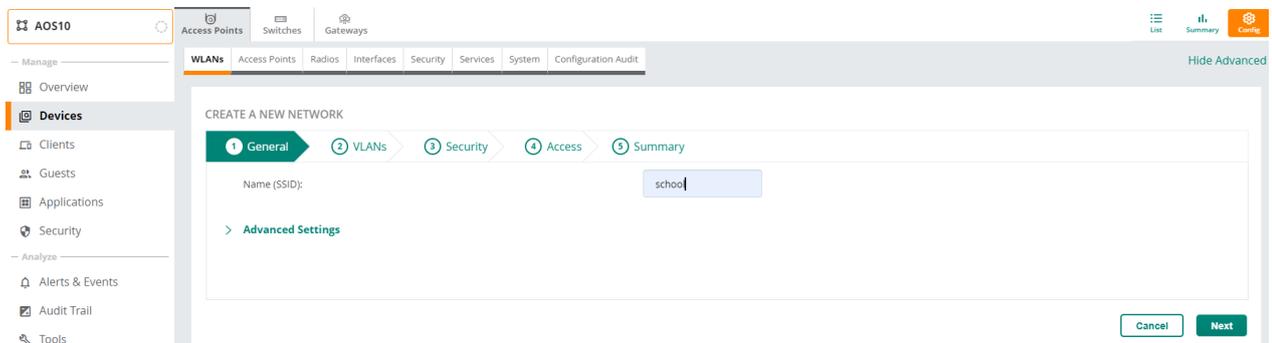
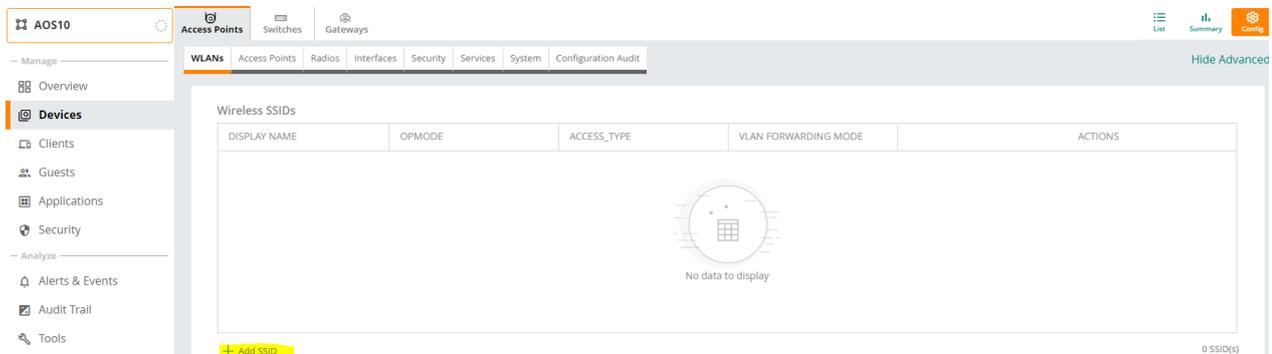
Here we are adding Network Access Devices (NAD). This will be the AOS10 APs and gateways. Note that you need to either add the AP IP addresses individually or just add their subnet as I have done here.



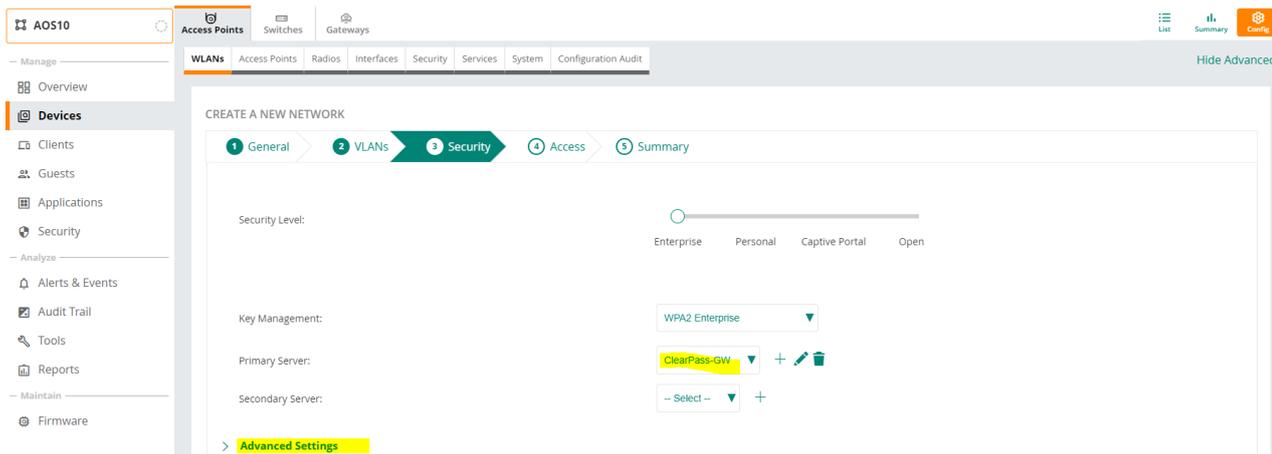
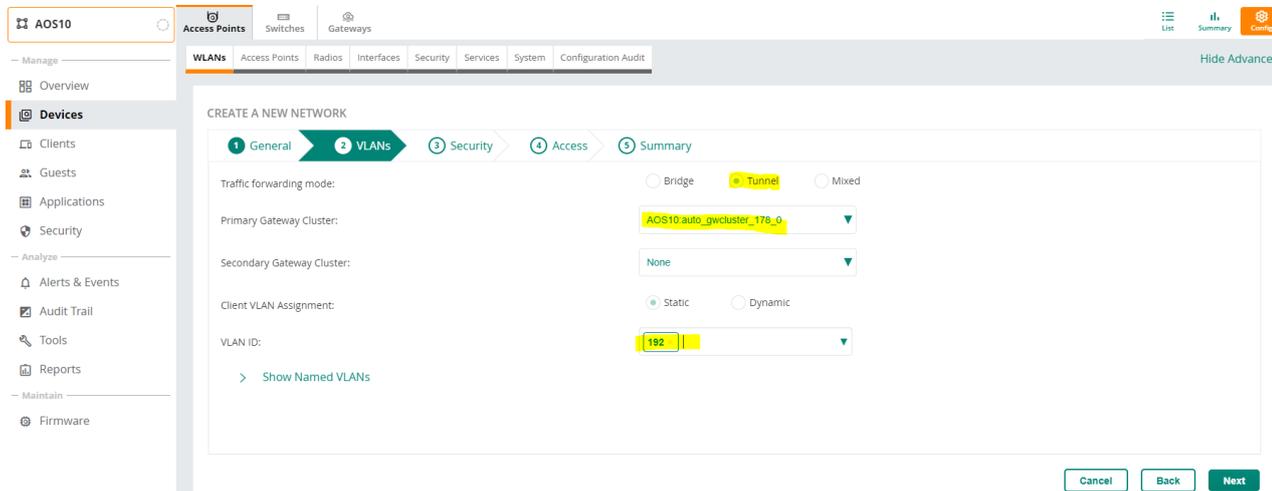
# 6 WLAN Configuration

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

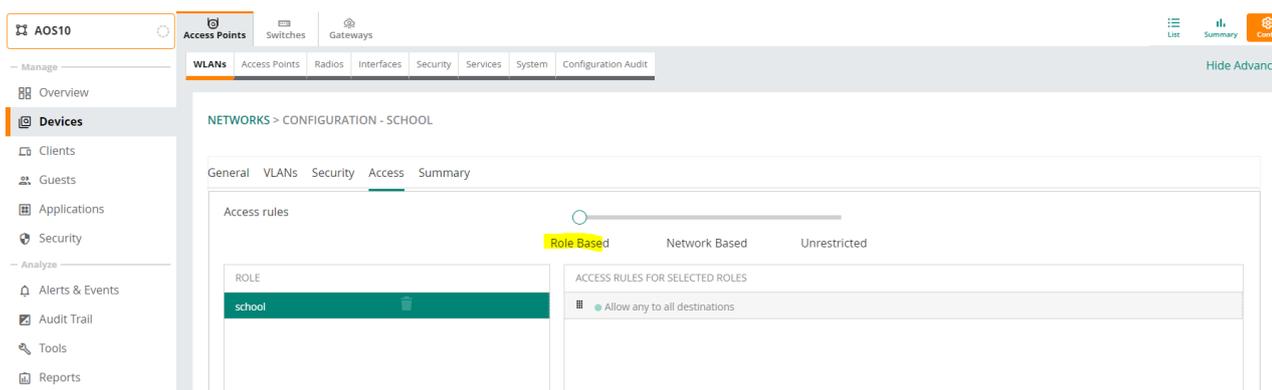
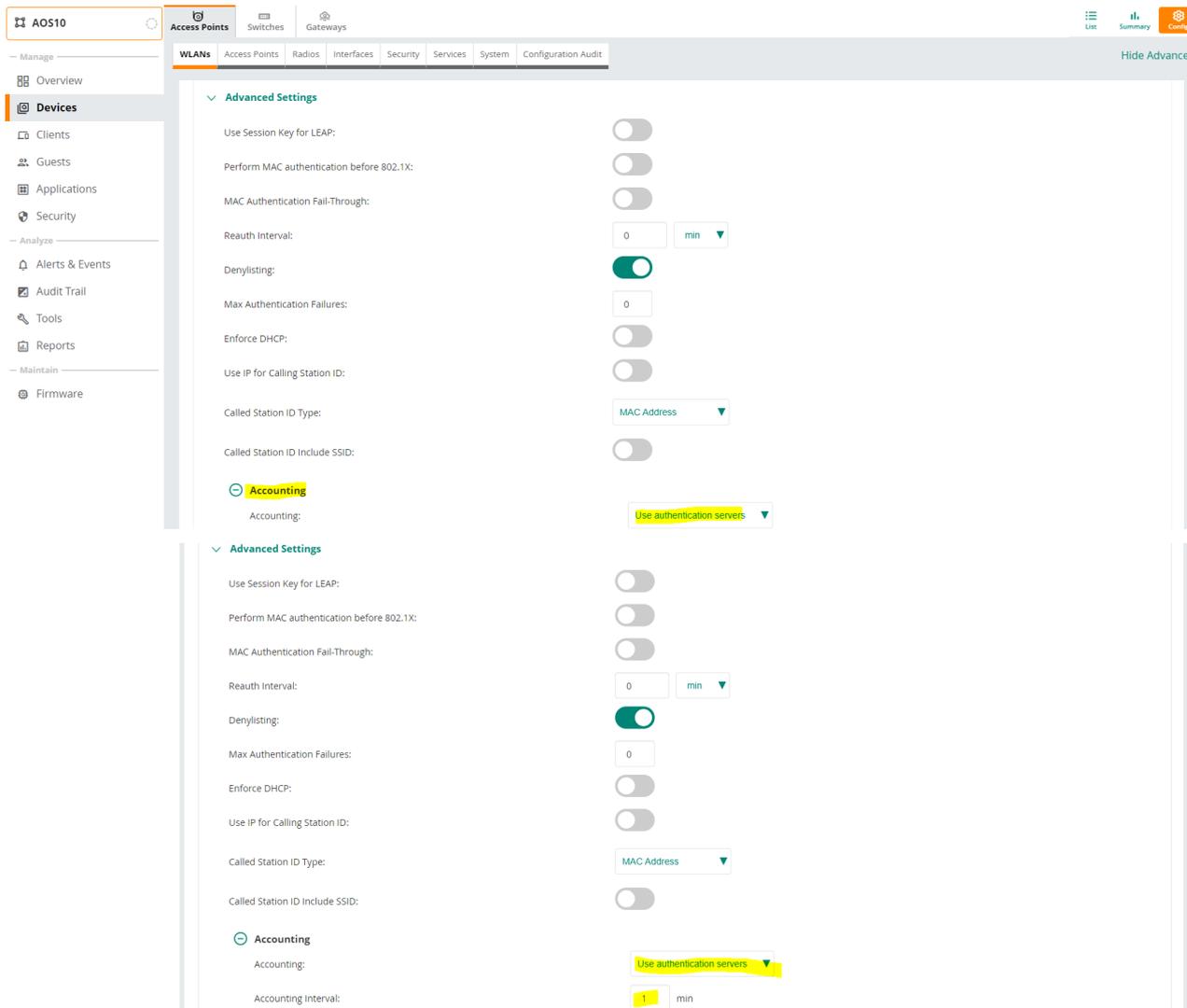
## 6.1 Tunnelled Wireless Configuration



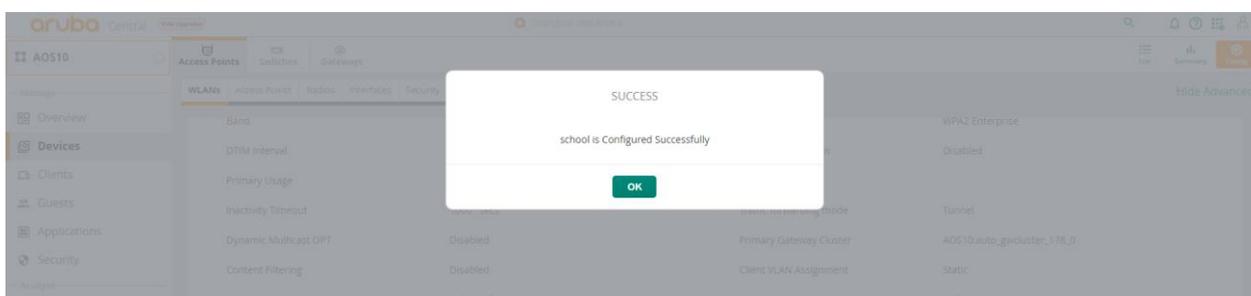
You can choose the cluster from the menu. Also note that the VLAN IDs are being displayed from the gateways.



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 from the AP's tunnel configuration.

The screenshot shows the Aruba NetworkOS Gateway configuration interface. The 'Security' tab is selected, and the 'Auth Servers' sub-tab is active. The 'Authentication Servers' section contains two tables:

Server groups					
NAME	SERVERS	FAIL THROUGH	LOAD BALANCE	SERVER RULES	
school_#1615532079504_41#_acct_svg	1	--	--	0	
school_#1615532079504_41#_auth_svg	1	--	--	0	
school_#1615532079504_41#_cp_svg	1	--	--	0	

All servers				
NAME	TYPE	IP ADDRESS / HOSTNAME	SERVER GROUP	
ClearPass-GW	Radius	192.168.1.95	school_#1615532079504_41#_acct_svg_sc	
--	RFC 3576	192.168.1.95	--	

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

The screenshot shows the ClearPass Policy Manager 'Access Tracker' interface. The 'Access Tracker' page displays a real-time display of per-session access activity. The following table shows the access activity:

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.95	RADIUS	staff1	AA Aruba 802.1X Wireless	ACCEPT	2021/03/12 17:58:39

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.

The screenshot shows the 'Request Details' page for the staff1 login. The 'Summary' tab is selected, displaying the following information:

Login Status:	ACCEPT
Session Identifier:	R00000006-01-604b111f
Date and Time:	Mar 12, 2021 17:58:39 AEDT
End-Host Identifier:	A0-88-B4-50-C0-84 (Computer / Windows / Windows)
Username:	staff1
Access Device IP/Port:	192.168.1.242
Access Device Name:	10.224.254.161
System Posture Status:	UNKNOWN (100)

**Policies Used -**

Service:	AA Aruba 802.1X Wireless
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:192.168.1.250
Authorization Source:	Ariya AD
Roles:	[User Authenticated]
Enforcement Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless

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

**Request Details**

Summary Input Output Accounting

Enforcement Profiles: AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless Staff Profile

System Posture Status: UNKNOWN (100)

Audit Posture Status: UNKNOWN (100)

**RADIUS Response**

Endpoint:Last Known Location 192.168.1.242:b4:5d:50:c6:82:4a

Radius:Aruba:Aruba-User-Role Staff

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

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

**Request Details**

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

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

**Request Details**

**Access Control Capabilities -**

Select Access Control Type :  Agent  SNMP  RADIUS CoA  Server Action

RADIUS CoA Type: [ArubaOS Wireless - Terminat ▼]

Submit Cancel

**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		
<b>Network Details</b>			
<b>Utilization</b>			
<b>Authentication Sessions Details</b>			

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

Now looking at Aruba Central pages.

**AOS10** Clients

244.08 MB ( 8.04 MB | 236.05 MB )

ALL | 1 Connecting | 1 Connected | 0 Failed | 0 Offline | 0 Blocked | 1 Wireless | 0 Wired | 0 Remote

Client Name	Status	IP Address	VLAN	Connected To	Gateway Role	SSID/Port	Health	Usage
staff1	Connected	10.10.44.50	44	b45d50c6824a	Staff	school		244.08 MB

**staff1** Summary | AI Insights | Location | Sessions

CLIENT DETAILS

DATA PATH: CLIENT (staff1 CONNECTED) -> SSID (school UP) -> AP (b45d50c6824a UP) -> SWITCH (Aruba-2930F-8G-PoEP-25PPP UP) -> GATEWAY (7005\_A0510\_gwy2 UP)

CLIENT	NETWORK	CONNECTION
<b>CLIENT</b> USERNAME: staff1 HOSTNAME: AriyaP IP ADDRESS: 10.10.44.50 GLOBAL UNICAST IPV6 ADDRESS: -- CLIENT OS: Win10 MANUFACTURER: Intel Corporate AI INSIGHTS: 0 0 0	<b>NETWORK</b> VLAN: 44 AP ROLE: Staff GATEWAY ROLE: Staff SEGMENTATION: -- AUTH SERVER: 192.168.1.242 TUNNELED: --	<b>CONNECTION</b> CHANNEL: 149 (40 MHz) CLIENT CAPABILITIES: 802.11n CLIENT MAX SPEED: 600 Mbps LEDs on ACCESS POINT (b45d50c6824a): 0 Blink LEDs

**staff1** Visibility | Applications | Websites

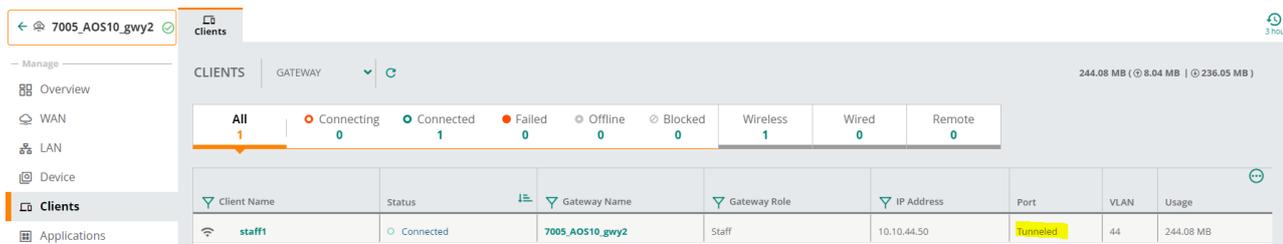
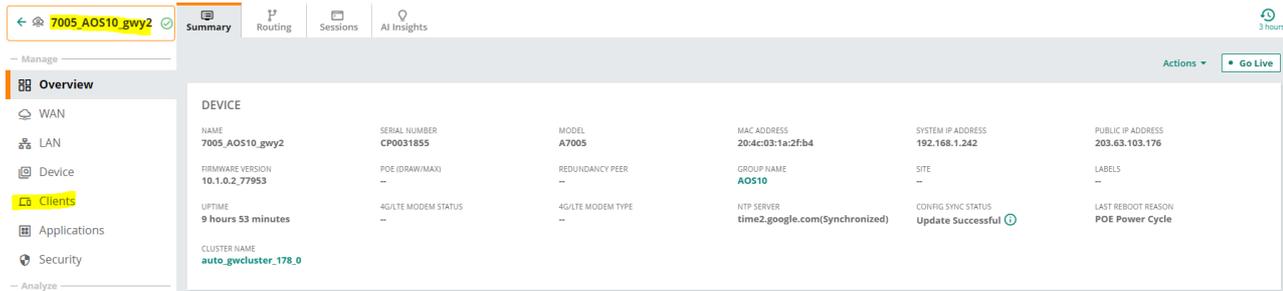
APPLICATIONS

Passive Monitoring

Total Transferred: 1.4 GB

APPLICATION	CATEGORY	USAGE	SENT	RECEIVED
YouTube	Streaming	1.3 GB (93.21%)	28.0 MB	1.3 GB
TCP	Network Service	19.9 MB (1.40%)	386 KB	19.5 MB
Microsoft	Office365 SAAS	2.2 MB (0.16%)	309 KB	1.9 MB
HTTPS	Web	959 KB (0.07%)	101 KB	858 KB
Google Ads	Google SAAS	355 KB (0.02%)	72 KB	284 KB
Mozilla	Web	319 KB (0.02%)	57 KB	262 KB
Google Generic	Google SAAS	212 KB (0.01%)	110 KB	102 KB
Microsoft OneDrive	sharepoint_onedrive_saas	163 KB (0.01%)	12 KB	151 KB
Netbios Name Service	Network Service	76 KB (0.01%)	76 KB	0 B
Bing.com	Web	51 KB (0.00%)	7 KB	44 KB
Microsoft Azure	Office365 SAAS	47 KB (0.00%)	3 KB	43 KB
SOAP	Network Service	42 KB (0.00%)	42 KB	0 B
Microsoft Office 365	Office365 SAAS	35 KB (0.00%)	4 KB	31 KB
Server Message Block	Network Service	13 KB (0.00%)	13 KB	0 B
Unclassified	Unclassified	72.3 MB (5.08%)	798 KB	71.5 MB

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
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#
    
```

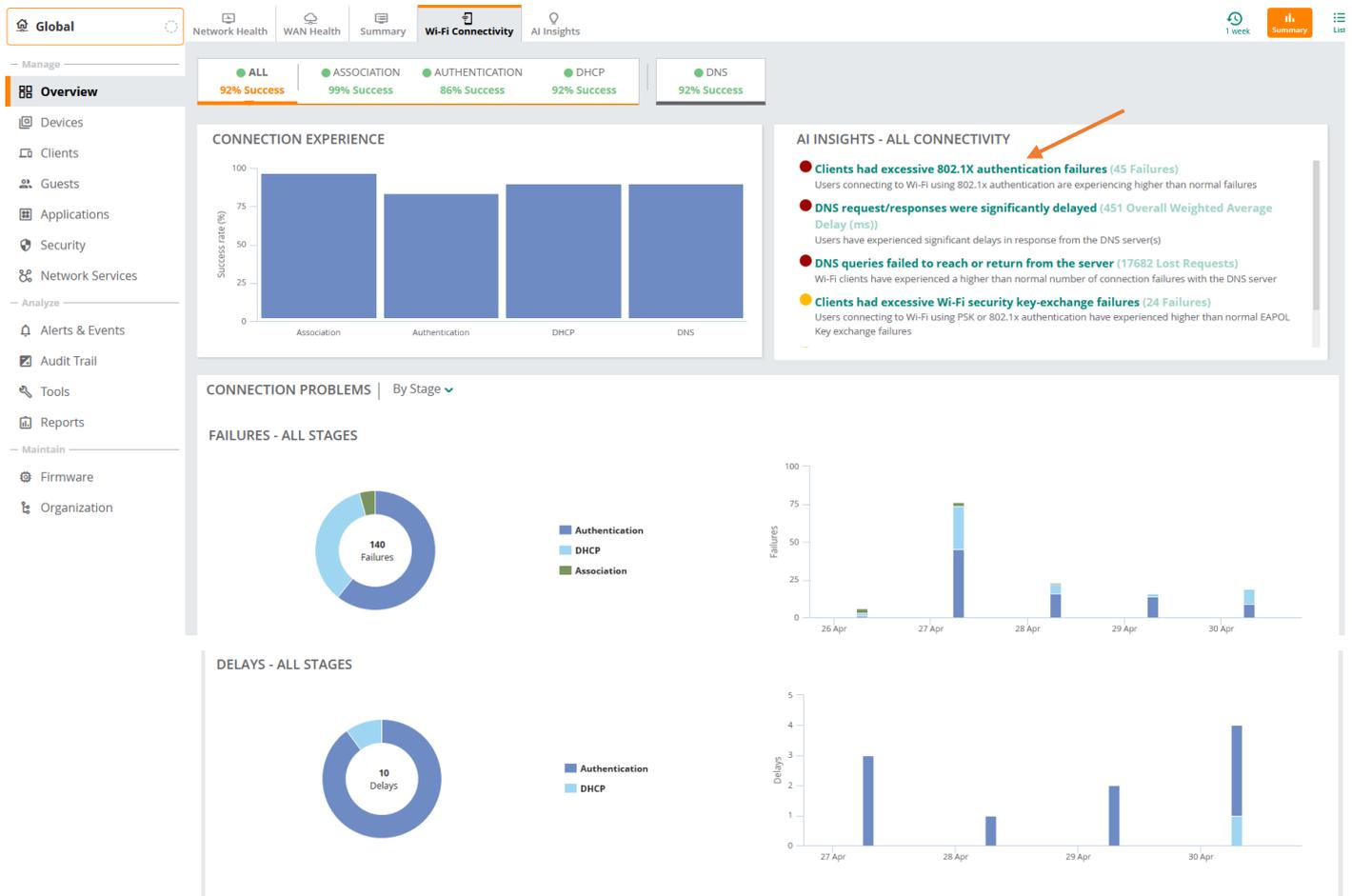
checking the IPSEC tunnels from the AP

```

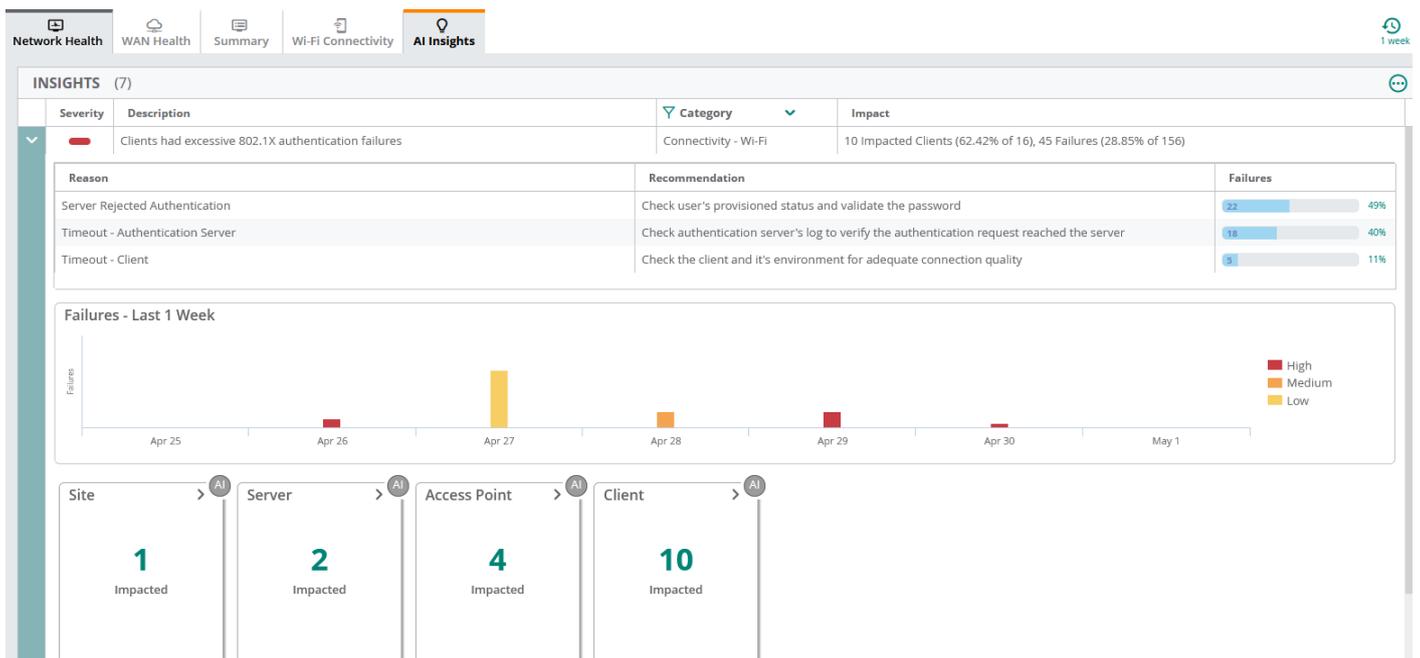
b4:5d:50:c6:82:4a# sh ata endpoint
ATA Endpoint Status
-----
UUID          IP ADDR      STATE          TUN DEV  TUN SPI(OUT/IN)  PORT(SRC/DST)  VALID TIME(s)  TUNNEL TYPE
GRE VLANs     HBT(Jiff/Missed/Sent/Rcv)  INNER IP      UP TIME(s)
-----
522d59ab-05d0-43b6-ab49-177e49fb7bb0  192.168.1.242  SM STATE_CONNECTED  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 802.1x failures"





Access Points 5 | Radios 10 | 2.4 GHz 5 | 5 GHz 5

RADIOS (5)

Access Point	Radio MAC Address	Band	Bandwidth	Channel	Utilization (%)	Channel Changes	Power (dBm)	Power Changes	Noise floor (dBm)
AP515-AtlasDesk	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-NBRReception	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 Points 5 | Radios 10 | 2.4 GHz 5 | 5 GHz 5

RADIOS (5)

Access Point	Radio MAC Address	Band	Bandwidth	Channel	Utilization (%)	Channel Changes	Power (dBm)	Power Changes	Noise floor (dBm)
AP515-AtlasDesk	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-NBRReception	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

Access Points - | Radios 10 | 2.4 GHz 5 | 5 GHz 5

RADIOS | CHANNEL DISTRIBUTION

CHANNEL CHANGES

16 Channel changes in the last 1 Week

POWER CHANGES

3 Power changes in the last 1 Week

### Looking at 5GHz band

Access Points - | Radios 10 | 2.4 GHz 5 | 5 GHz 5

RADIOS | CHANNEL DISTRIBUTION

CHANNEL CHANGES

10 Channel changes in the last 1 Week

POWER CHANGES

1 Power changes in the last 1 Week

CHANNEL CHANGES (10)					
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.

Global | Access Points | Switches | Gateways

Manage

Overview

Devices

- Clients
- Guests
- Applications
- Security
- Network Services

Access Points: 5 Online, 4 Offline, 1 Radios: 10

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

Manage

Overview

- Device
- Clients
- Security

Analyze

- Live Events
- Alerts & Events
- Audit Trail

Maintain

- Firmware

**DEVICE**

AP MODEL: AP-515

COUNTRY CODE: AU

MAC: d0:15:a[REDACTED]

SERIAL NUMBER: [REDACTED]

UPTIME: 5 Days 22 Hours 30 Minutes

LAST REBOOT REASON: AP reload

FIRMWARE VERSION: 10.2.0.1\_79907

CONFIGURATION STATUS: Synchronized  
Last Config Changed on Apr 28, 2021, 03:51

BAND SELECTION: Dual Band

POWER DRAW: 13.16 W

POWER NEGOTIATION: 802.3 at

GROUP: AOS10-Group

LABELS: -

LEDs on ACCESS POINT: [REDACTED] Blink LED

**NETWORK**

ETH0: Up  
SPEED (Mbps) / DUPLEX: 1000 / Full  
VLAN: Trunk (all)

ETH1: Down  
SPEED (Mbps) / DUPLEX: -  
VLAN: -

CURRENT UPLINK: Ethernet (br0)

UPLINK CONNECTED TO: -

IP ADDRESS: 10.2.136.13 (DHCP)

PUBLIC IP ADDRESS: 203.1.203.51

DNS NAME SERVERS: 10.99.64.202

DEFAULT GATEWAY: 10.2.136.1 (DHCP)

NTP SERVER: 10.250.136.1

Actions | Go Live

Manage

Actions **Go Live**

Overview

Device

Clients

Security

Analyze

Live Events

Alerts & Events

Audit Trail

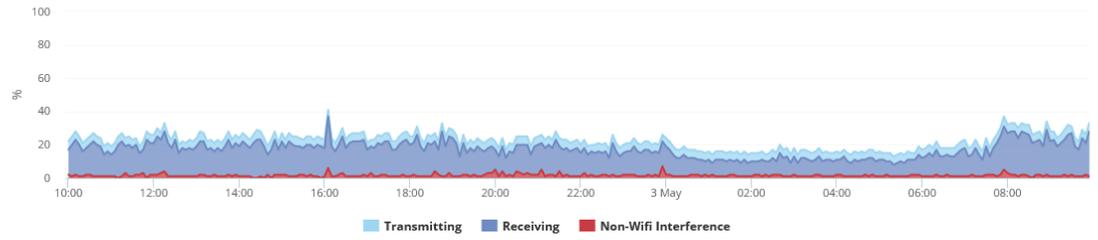
Tools

Maintain

Firmware

RADIO 2.4 GHz RADIO 5 GHz

CHANNEL UTILIZATION



NOISE FLOOR

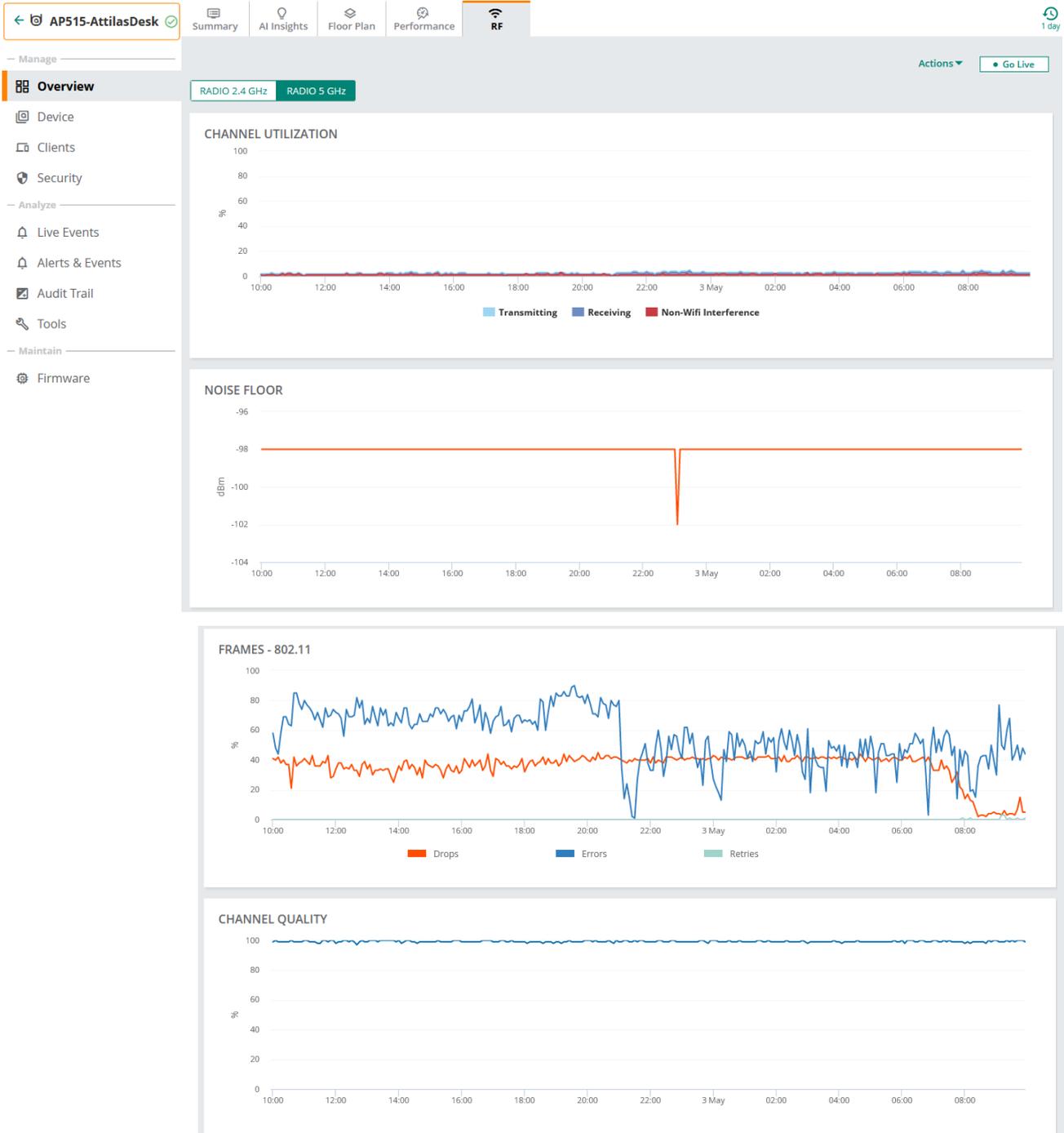


FRAMES - 802.11

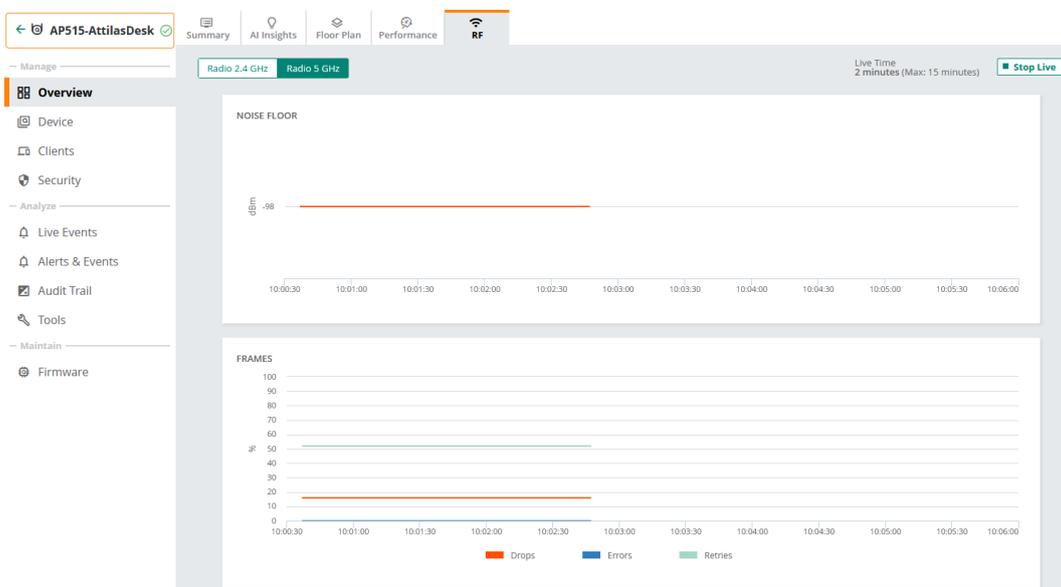


CHANNEL QUALITY





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.

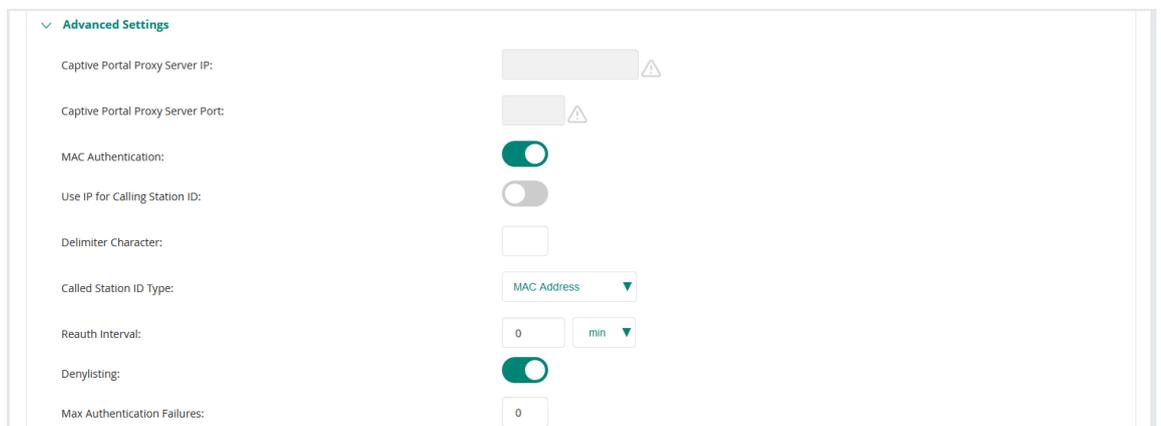
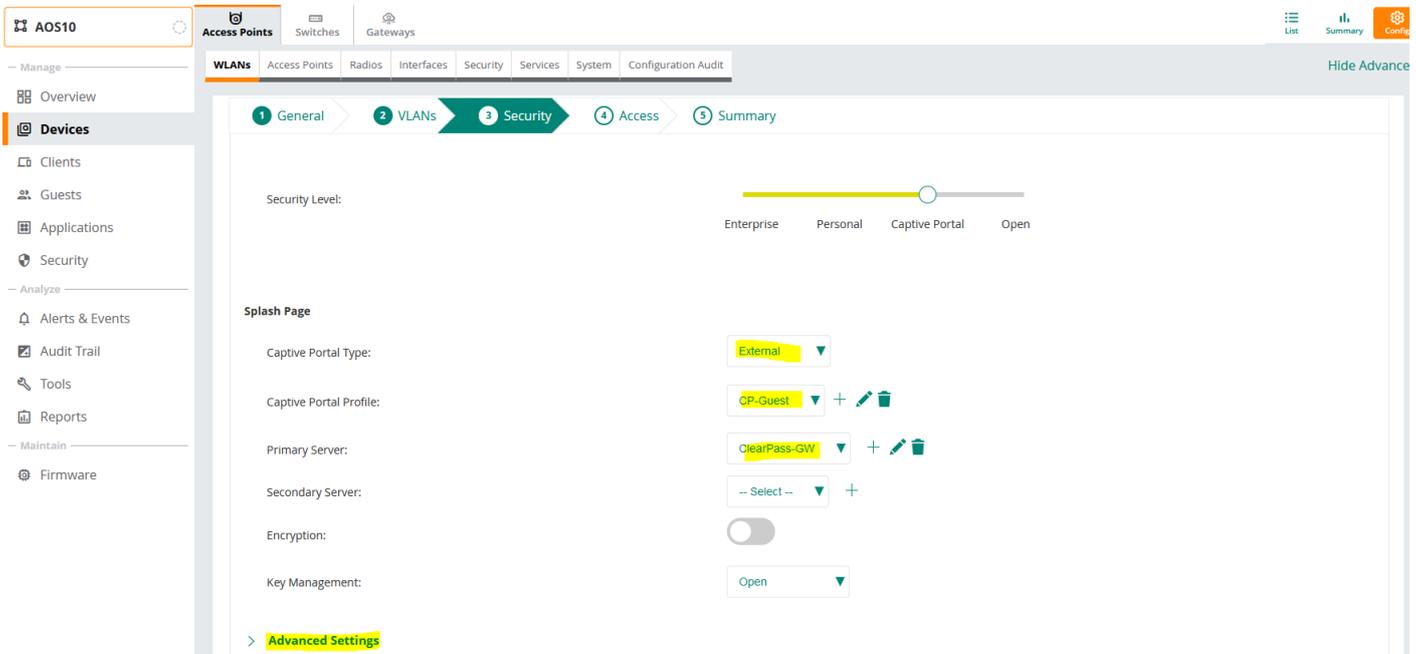
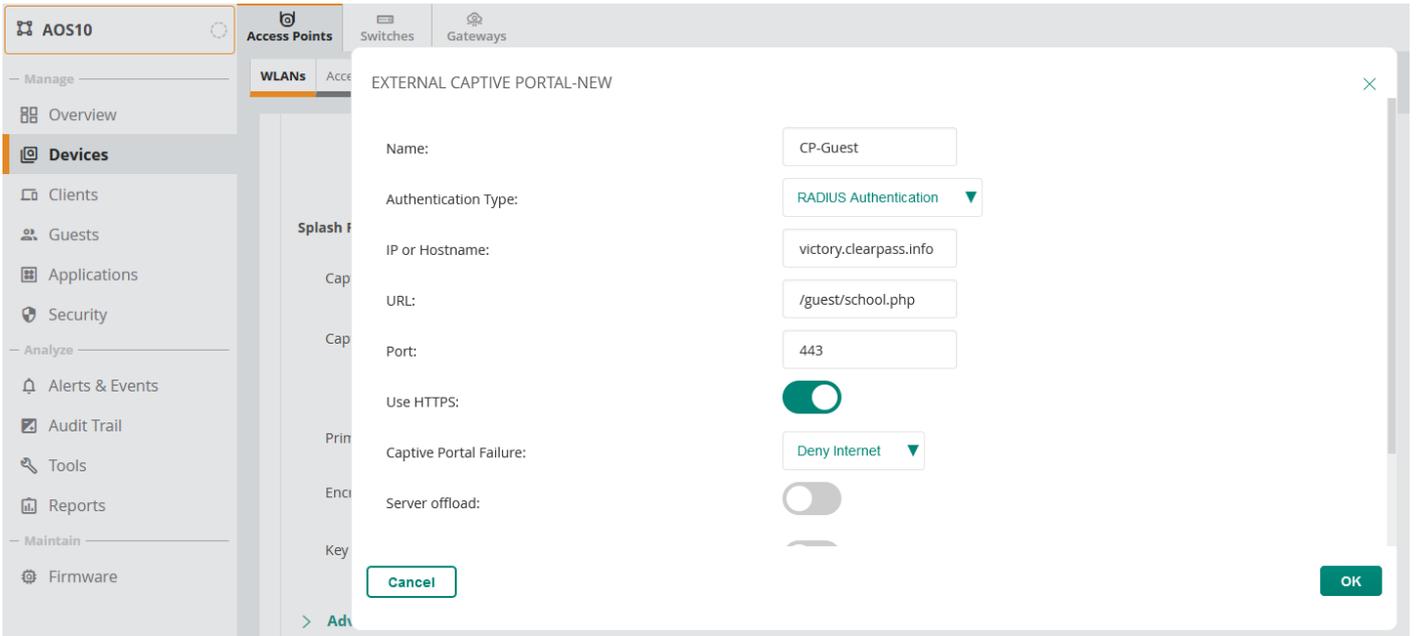
## 8.1 Guest Wireless Configuration

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

This screenshot shows the 'CREATE A NEW NETWORK' configuration page in the 'General' step. The breadcrumb trail is 'WLANs > Access Points > Radios > Interfaces > Security > Services > System > Configuration Audit'. The left sidebar shows the 'Devices' section. The main content area has a progress bar with five steps: 1. General (active), 2. VLANs, 3. Security, 4. Access, and 5. Summary. Below the progress bar, the 'Name (SSID):' field is set to 'Schoo-Guest'. Under the 'Advanced Settings' section, several options are listed with expandable icons: Broadcast/Multicast, Transmit Rates (Legacy Only), Bandwidth Control, WiFi Multimedia, Miscellaneous, and Time Range Profiles. At the bottom right, there are 'Cancel' and 'Next' buttons.

This screenshot shows the 'CREATE A NEW NETWORK' configuration page in the 'VLANs' step. The breadcrumb trail is 'WLANs > Access Points > Radios > Interfaces > Security > Services > System > Configuration Audit'. The left sidebar shows the 'Devices' section. The main content area has a progress bar with five steps: 1. General, 2. VLANs (active), 3. Security, 4. Access, and 5. Summary. The 'Traffic forwarding mode:' section has three radio buttons: Bridge, Tunnel (selected), and Mixed. The 'Primary Gateway Cluster:' dropdown is set to 'AOS10.auto\_gwcluster\_178\_0'. The 'Secondary Gateway Cluster:' dropdown is set to 'None'. The 'Client VLAN Assignment:' section has two radio buttons: Static (selected) and Dynamic. The 'VLAN ID:' dropdown is set to '192'. A link '> Show Named VLANs' is visible below the dropdown. At the bottom right, there are 'Cancel', 'Back', and 'Next' buttons.

This screenshot shows the 'CREATE A NEW NETWORK' configuration page in the 'Security' step. The breadcrumb trail is 'WLANs > Access Points > Radios > Interfaces > Security > Services > System > Configuration Audit'. The left sidebar shows the 'Devices' section. The main content area has a progress bar with five steps: 1. General, 2. VLANs, 3. Security (active), 4. Access, and 5. Summary. The 'Security Level:' section features a slider with four positions: Enterprise, Personal, Captive Portal, and Open. The 'Splash Page' section has two dropdown menus: 'Captive Portal Type:' set to 'External' and 'Captive Portal Profile:' set to '-- Select --'. A red error message 'This field is mandatory.' is displayed below the 'Captive Portal Profile' dropdown. At the bottom right, there are 'Cancel', 'Back', and 'Next' buttons.



Enforce DHCP:

WPA3 Transition:

Called Station ID Include SSID:

Uppercase Support:

**Accounting**

Accounting:  ▼

Accounting Interval:  min

**Disable if uplink type is**

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.

**AOS10** | Access Points | Switches | Gateways

WLANs | Access Points | Radios | Interfaces | Security | Services | System | Configuration Audit

CREATE A NEW NETWORK

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

Access rules

Role Based | Network Based | Unrestricted

ROLE	ACCESS RULES FOR SELECTED ROLES
Schoo-Guest	Allow any to all destinations
school	
CP-Guest	

ROLE ASSIGNMENT RULES

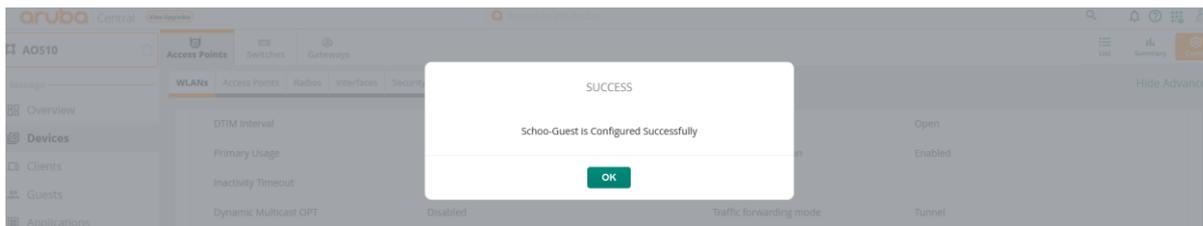
Default role: Schoo-Guest

+ ADD ROLE ASSIGNMENT

ASSIGN PRE-AUTHENTICATION ROLE:  CP-Guest ▼

ENFORCE MAC AUTH ONLY ROLE:

1 Role(s)



Now we have our Guest SSID configured.

**AOS10** | Access Points | Switches | Gateways

WLANs | Access Points | Radios | Interfaces | Security | Services | System | Configuration Audit

Wireless SSIDs

NAME	SECURITY	ACCESS TYPE	TRAFFIC FORWARDING MODE	NETWORK ENABLED
school	wpa2-aes	Unrestricted	Tunnel	Yes
Schoo-Guest	Captive Portal (external)	Role Based	Tunnel	Yes

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

**AOS10** | Access Points | Switches | Gateways

System | Interface | Routing | WAN | Security | VPN | High Availability | Config Audit

Roles | Policies | Aliases | Applications | Apply Policy | Auth Servers | Role Assignment (AAA Profiles) | L2 Authentication | L3 Authentication | Advanced | Firewall

Authentication Servers

Server groups

NAME	SERVERS	FAIL THROUGH	LOAD BALANCE	SERVER RULES
Schoo-Guest_#1615938135060_41#_acct_svg	1	--	--	0
Schoo-Guest_#1615938135060_41#_auth_svg	1	--	--	0
Schoo-Guest_#1615938135060_41#_cp_svg	1	--	--	0
school_#1615532079504_41#_acct_svg	1	--	--	0
school_#1615532079504_41#_auth_svg	1	--	--	0
school_#1615532079504_41#_cp_svg	1	--	--	0

Server Group > Schoo-Guest\_#1615938135060\_41#\_acct\_svg

NAME	TYPE	IP ADDRESS	TRIM FQDN	MATCH RULES
ClearPass-GW	Radius	192.168.1.95	--	0

**AOS10** | Access Points | Switches | Gateways

System | Interface | Routing | WAN | Security | VPN | High Availability | Config Audit

Roles | Policies | Aliases | Applications | Apply Policy | Auth Servers | Role Assignment (AAA Profiles) | L2 Authentication | L3 Authentication | Advanced | Firewall

L3 Authentication

Captive Portal Authentication Profile: New Profile

Captive Portal Authentication Profile: +

- default
- Schoo-Guest\_#1615938...
- school\_#161553207950...
- VIA Authentication
- VIA Connection
- VIA Web Authentication
- VPN Authentication

**AOS10** | Access Points | Switches | Gateways

System | Interface | Routing | WAN | Security | VPN | High Availability | Config Audit

Roles | Policies | Aliases | Applications | Apply Policy | Auth Servers | Role Assignment (AAA Profiles) | L2 Authentication | L3 Authentication | Advanced | Firewall

Roles

NAME	RULES
ap-role	35 Rules
authenticated	4 Rules
CP-Guest	5 Rules
default-lap-user-role	2 Rules
default-via-role	3 Rules
default-vpn-role	4 Rules

CP-Guest Policies Bandwidth More

NAME	RULES COUNT	TYPE	POLICY USAGE
global-sacl	0	session	ap-role, authenticated, CP-Guest, default-via
apprf-cp-guest-sacl	0	session	CP-Guest
cp-guest	5	session	CP-Guest

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.

The screenshot shows the Aruba ClearPass Policy Manager web interface. On the left is a navigation menu with categories: Dashboard, Monitoring, Configuration, and Administration. Under Configuration, 'Service Templates & Wizards' is selected. The main area displays a list of service templates:

- Device MAC Authentication**: To authenticate guest devices based on their MAC address.
- EDUROAM service**: Service template for roaming users to connect to campus networks that are part of the eduroam federation.
- Encrypted Wireless Access via 802.1X Public PEAP method**: Service Template for providing encrypted wireless access to (guest) users via fixed 802.1X PEAP credentials.
- Guest Access**: To authenticate guest users logging in via captive portal. Guests must re-authenticate after their session ends.
- Guest Access - Web Login**: To authenticate guest users logging in via guest portal.
- Guest Authentication with MAC Caching**: To authenticate users once using captive portal and later to allow logins using cached MAC Address of the device.
- OAuth2 API User Access**: Service template for API clients authenticating with username and password (OAuth2 grant type "password").
- Onboard**: Service template for authorizing device credential provisioning and onboarding.
- Onboard Services Only**: Service template for authorizing device credential and onboarding.

Configuration » Service Templates & Wizards

### Service Templates - Guest Authentication with MAC Caching

This screenshot shows the configuration page for the 'Guest Authentication with MAC Caching' service template. The 'General' tab is active. The 'Name Prefix\*' field contains 'GG'. Below this is a 'Description' box with the following text:

Users first login via captive portal and their MAC addresses are cached. Subsequent logins will use MAC authentication and bypass the captive portal. Network access can be restricted based on day of the week, bandwidth limit or number of unique devices used by the User. The cache lifetime of the MAC address can vary according to the user's role (Guest, Employee or Contractor) and after that the user will have to re-authenticate via captive portal. Posture checks can be enabled, optionally, to validate the client device for antivirus, anti-spyware, firewall status. These results will determine the enforcement for the device.

At the bottom of this section are buttons: Back to Service Templates & Wizards, Delete, Next →, Add Service, and Cancel.

This screenshot shows the 'Wireless Network Settings' tab. The 'Select NAD Client' dropdown is set to 'MD-1' and the 'Wireless SSID\*' field contains 'Guest'. At the bottom are buttons: Back to Service Templates & Wizards, Delete, Next →, Add Service, and Cancel.

This screenshot shows the 'MAC Caching Settings' tab. It contains the instruction: 'Enter MAC Caching duration for the users. After this time expires, users will have to re-authenticate via captive portal'. Below this are three rows for setting cache durations:

- Cache duration for Employee: One Month
- Cache duration for Guest: One Day
- Cache duration for Contractor: One Week

At the bottom are buttons: Back to Service Templates & Wizards, Delete, Next →, Add Service, and Cancel.

**Enable Posture Checks to perform health checks after authentication.**

Enable Posture Checks:  Configure Guest Web Login page

- 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\*: GuestCaptivePortal

Days allowed for access\*:  Monday  Tuesday  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

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] Add New Authentication Method

Move Up ↑  
Move Down ↓  
Remove  
View Details  
Modify

--Select to Add--

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

Move Up ↑  
Move Down ↓  
Remove  
View Details  
Modify

--Select to Add--

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] [Remove]  
[Guest User Repository] [Local SQL DB] [View Details]  
[Modify]

--Select to Add-- Add New Authentication Source

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

Role Mapping Policy: GG MAC Authentication Role Mapping Add New Role Mapping Policy

Modify

**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 Add New Enforcement Policy

Modify

**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

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}

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}

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}

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-logout

## 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:	<input type="checkbox"/> Enable to monitor network access without enforcement				
More Options:	<input checked="" type="checkbox"/> Authorization <input type="checkbox"/> Posture Compliance <input type="checkbox"/> Audit End-hosts <input type="checkbox"/> Profile Endpoints <input type="checkbox"/> Accounting Proxy				
Service Rule					
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:					
Type	Name	Operator	Value		
1.	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] Add New Authentication Method

Move Up ↑  
Move Down ↓  
Remove  
View Details  
Modify

--Select to Add--

Authentication Sources: [Guest User Repository] [Local SQL DB] Add New Authentication Source

Move Up ↑  
Move Down ↓  
Remove  
View Details  
Modify

--Select to Add--

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] Add New Authentication Source

Remove  
View Details  
Modify

--Select to Add--

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

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

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

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.

The screenshot displays the ClearPass Policy Manager interface. On the left is a navigation sidebar with categories like Alerts, Applications, Authentication Status, Cluster Status, Device Category, Device Family, Endpoint Profiler Summary, Failed Authentications, Health Status, Latest Authentications, License Usage, MDM Discovery Summary, OnGuard Clients Summary, and Monitoring. The main area contains several widgets: Cluster Status (showing a 'victory' status), System CPU Utilization (a line graph showing low usage), Request Processing Time (a line graph showing a peak at 14:50), and All Requests (a bar chart showing request counts over time). A Quick Links section is also visible, with 'ClearPass Guest' highlighted.

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

aruba ClearPass Guest

Home » Guest

**Guest Manager**

**Guest Account Management**

Use the commands below to manage your network's guest user accounts.

- Create New Guest Account**  
Set up a new account for guest access to your network.
- Create Multiple Guest Accounts**  
Create multiple guest accounts, each with a randomly-assigned username and password.
- Manage Guest Accounts**  
View a list of all current guest accounts. You can modify and remove individual user accounts here.
- Edit Multiple Guest Accounts**  
View a list of all current guest accounts. You can modify and remove one or more user accounts here.
- Active Sessions**  
View active accounting sessions and disconnect or change authorization for sessions.
- Import Guest Accounts**  
Import a list of guests from a text file and create a guest account for each entry in the list.
- Export Guest Accounts**  
Export a list of all current guest accounts to a file. You can select the format you want to export to here.

aruba ClearPass Guest

Home » Guest » Create Account

**Create Guest Account**

New guest account being created by admin.

**Create New Guest Account**

\* Guest's Name:   
Name of the guest.

\* Company Name:   
Company name of the guest.

\* Email Address:   
The guest's email address. This will become their username to log into the network.

Account Activation:   
Select an option for changing the activation time of this account.

Account Expiration:   
Select an option for changing the expiration time of this account.

\* Account Role:   
Role to assign to this account.

Password:

Notes:

\* Terms of Use:  I am the sponsor of this account and accept the terms of use

\* required field

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

aruba ClearPass Guest

Home » Guest » Manage Accounts

**Manage Guest Accounts**

The following table shows the guest accounts that have been created. Click an account to modify it.

Filter:

Username	Role	State	Activation	Expiration
cpguser	[Guest]	Active	23 hours ago	No expiry

1 Showing 1 - 1 of 1  
20 rows per page

Guest

- Active Sessions
- Create Account
- Create Multiple
- Export Accounts
- Import Accounts
- Manage Accounts
- Manage Multiple Accounts

Devices

Onboard

Configuration

Administration

Quick Help Create More Options

Filter:

Username	Role	State	Activation	Expiration
cpguser	[Guest]	Active	23 hours ago	No expiry

Reset password Change expiration Remove Edit Sessions Print Show Details

To update the properties of this guest account, use the form below:

**Edit Account**

\* Guest's Name: cpguser  
Name of the guest.

\* Username: cpguser  
Name of the account.

Account Activation: (No changes: Account is active)   
Select an option for changing the activation time of this account.

Account Expiration: (No changes: Account will not expire)   
Select an option for changing the expiration time of this account.

Account Lifetime: N/A   
The amount of time after the first login before the account will expire and be deleted.

Total Allowed Usage: (No changes)   
Select an option for changing the allowed usage time of this account.

Account Role: (No changes: [Guest])   
Role to assign to this account.

\* Password: Type in a new password   
Select an option for editing the guest account's password.

New password: ●●●●●●  
Type in a new password to assign to the guest account.

Confirm Password: ●●●●●●  
Repeat the new password for the guest account.

Session Limit: 0  
The number of simultaneous sessions allowed for this account. Type 0 for unlimited use.

Notes:

Update Account

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.

Guest

Devices

Onboard

Configuration

- Authentication
- Content Manager
  - Private Files
  - Public Files
- Guest Manager
- Hotspot Manager
- Pages
  - Fields
  - Forms
  - List Views
  - Self-Registrations
  - Web Logins
  - Web Pages
- Receipts
- SMS Services
- Translations

Home » Configuration » Pages » Web Logins

Web Login (school)

Use this form to make changes to the Web Login *school*.

**Web Login Editor**

\* Name: school  
Enter a name for this web login page.

Page Name: school  
Enter a page name for this web login.  
The web login will be accessible from "/guest/page\_name.php".

Description: for AOS-10  
Comments or descriptive text about the web login.

\* Vendor Settings: Aruba  
Select a predefined group of settings suitable for standard network configurations.

Login Method: Controller-initiated — Guest browser performs HTTP form submit  
Select how the user's network login will be handled.  
Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.

\* Address: securelogin.hpe.com  
Enter the IP address or hostname of the vendor's product here.

Secure Login: Use vendor default  
Select a security option to apply to the web login process.

Dynamic Address:  The controller will send the IP to submit credentials  
In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection.  
The address above will be used whenever the parameter is not available or fails the requirements below.

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

Security Hash:    
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:    
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:    
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:    
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:    
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 $errmsg}{nwaicontext type=error}{$errmsg|escape}{/nwaicontext}{/if}

{nwa_text id=7980}<p>
    Please login to the network using your
    username and password.
</p>/nwa_text
```

  
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
```

  
HTML template code displayed after the login form.

Login Message: 

```
{nwa_text id=7978}<p>
Logging in, please wait...
</p>/nwa_text
```

  
HTML template code displayed while the login attempt is in progress.

\* Login Delay:    
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:

**Network Login Access**  
Controls access to the login page.

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

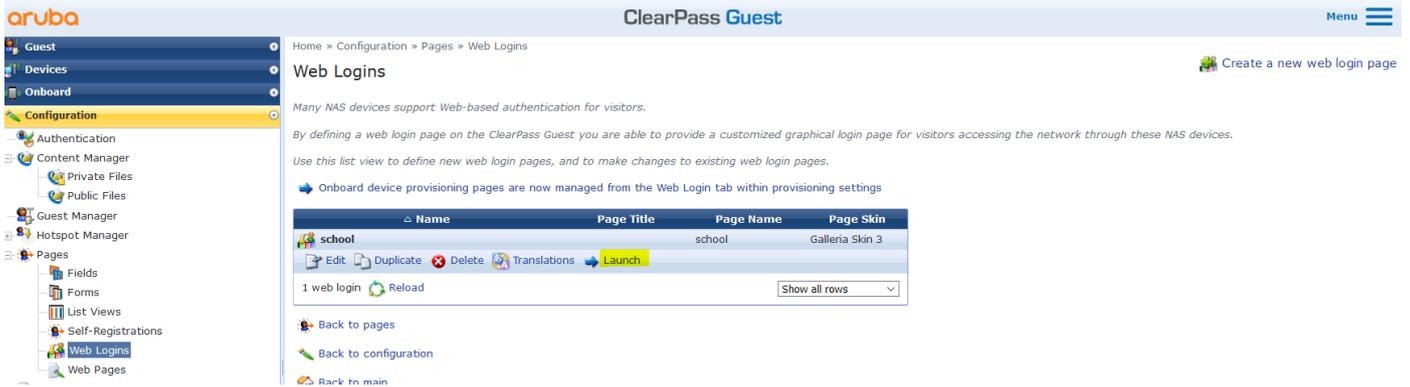
Denied Access:    
Enter the IP addresses and networks that are denied login access.

\* Deny Behavior:    
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.

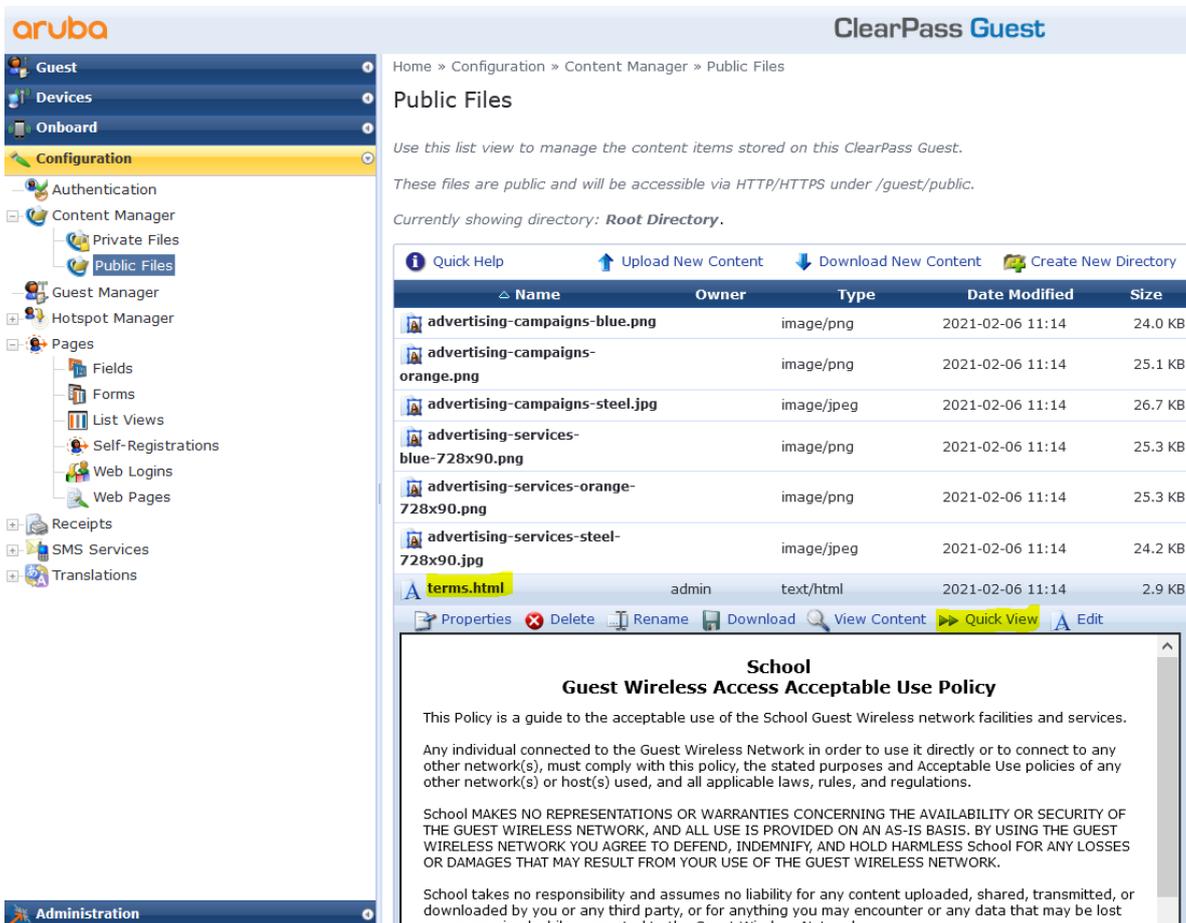
Update Endpoint:  Mark the user's MAC address as a known endpoint   
If selected, the endpoint's attributes will also be updated with other details from the user account.



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>

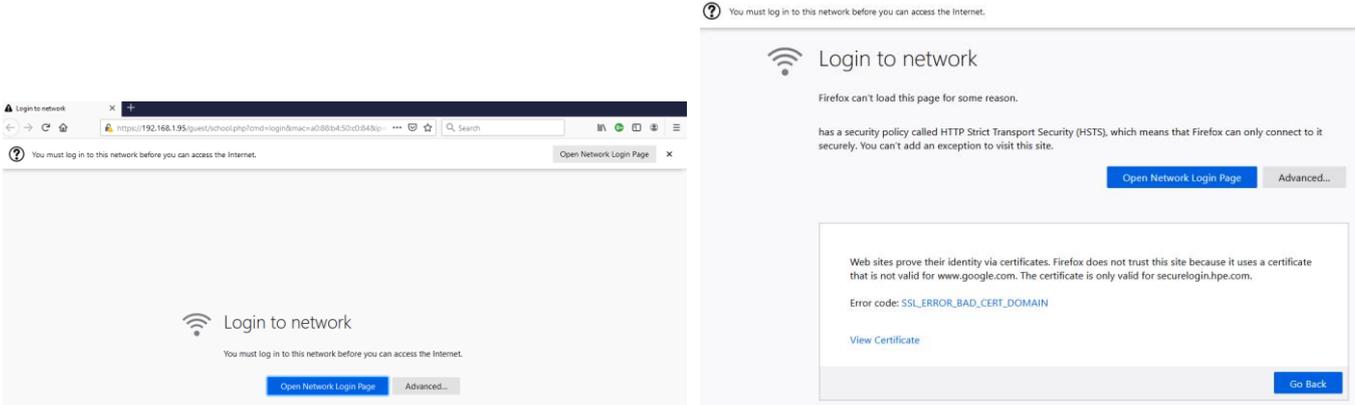
The "guest/school.php" is used in the URL redirection which we configured in MM

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

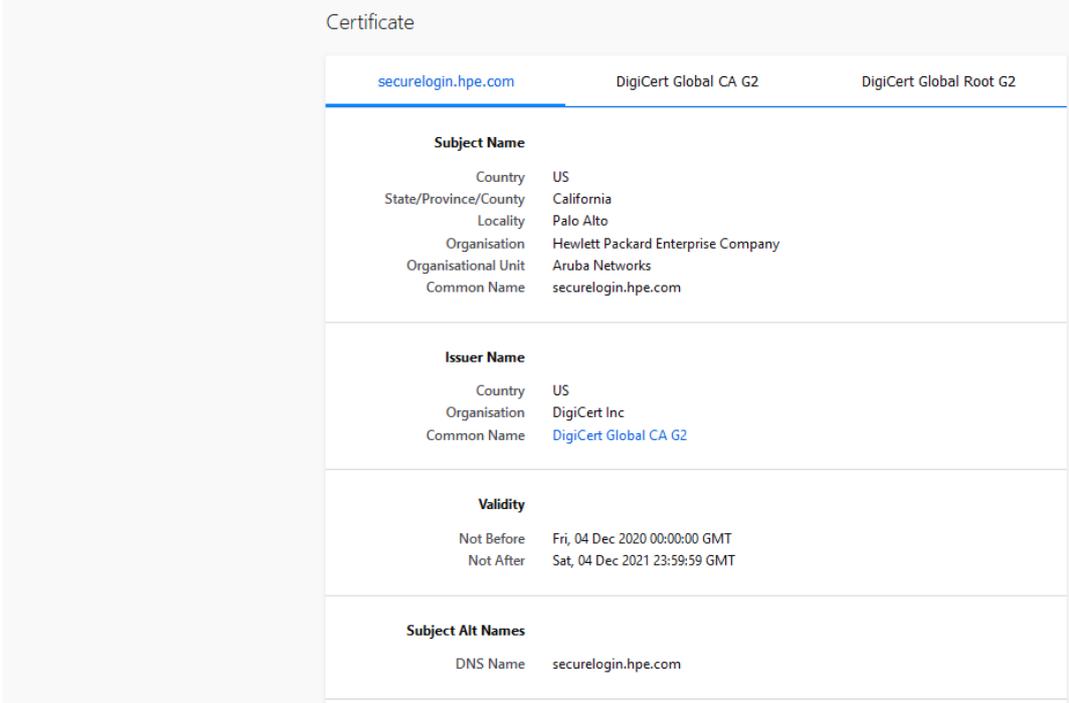


## 8.4 Guest Testing

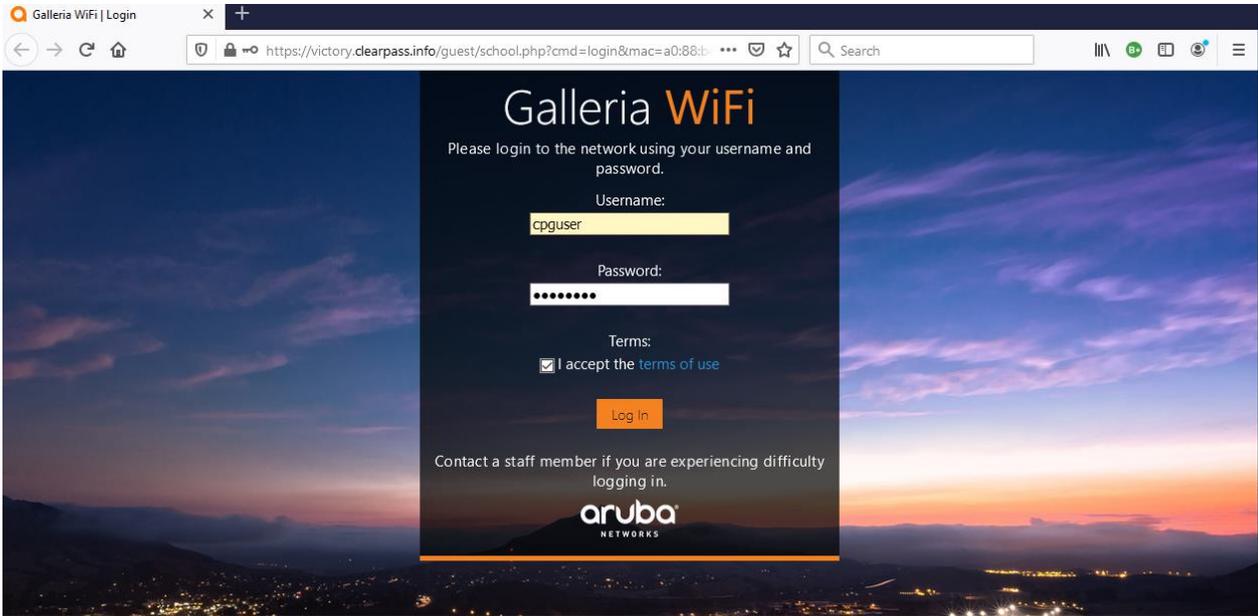
Now we'll get a test device to connect to Guest SSID, it gets automatically redirected to guest page in ClearPass but the browser will issue a warning



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.

The screenshot shows the Aruba MM dashboard. The top navigation bar includes 'AOS10' and 'Clients'. The main content area displays a table of clients with columns for Client Name, Status, IP Address, VLAN, Connected To, Gateway Role, SSID/Port, Health, and Usage. A client with IP 192.168.1.132 and MAC a088b450c084 is highlighted. Below the table, the 'CLIENT DETAILS' section shows a network diagram and detailed information for the selected client.

Client Name	Status	IP Address	VLAN	Connected To	Gateway Role	SSID/Port	Health	Usage
AriyaP	Connected	192.168.1.132	192	b4:5d:50:c6:82:4a	CP-Guest	Schoo-Guest	OK	7.84 MB

CLIENT		NETWORK		CONNECTION	
USERNAME	a088b450c084	VLAN	192	CHANNEL	6 (20 MHz)
HOSTNAME	AriyaP	VLAN DERIVATION	VSA	BAND	2.4 GHz
IP ADDRESS	192.168.1.132	AP ROLE	CP-Guest	CLIENT CAPABILITIES	802.11gn
GLOBAL UNICAST IPV6 ADDRESS	--	GATEWAY ROLE	CP-Guest	CLIENT MAX SPEED	288 Mbps
CLIENT OS	Win10	SEGMENTATION	--	LEDs on ACCESS POINT (b4:5d:50:c6:82:4a)	OK Blink LEDs
MANUFACTURER	Intel Corporate	AUTH SERVER	192.168.1.242		
AI INSIGHTS	0 0 0	TUNNELED	--		

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

The screenshot shows the Aruba ClearPass Policy Manager 'Access Tracker' interface. It displays a table of access requests. The second request shows a failed MAC authentication for the MAC address a088b450c084.

#	Server	SOURCE	Username	Service	Login Status	Request Timestamp
1.	192.168.1.95	RADIUS	cpuser	GG User Authentication with MAC Caching	ACCEPT	2021/03/17 11:26:22
2.	192.168.1.95	RADIUS	a088b450c084	GG MAC Authentication	REJECT	2021/03/17 11:25:58

The first screenshot shows the 'Request Details' for the failed request (ID 2). The 'Login Status' is 'REJECT'. The 'Access Device IP/Port' is 192.168.1.242. The 'Policies Used' section shows 'GG MAC Authentication'.

The second screenshot shows the 'Request Details' for the successful request (ID 1). The 'Login Status' is 'ACCEPT'. The 'Enforcement Profiles' include '[Deny Access Profile]'. The 'System Posture Status' is 'UNKNOWN (100)'.

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
```

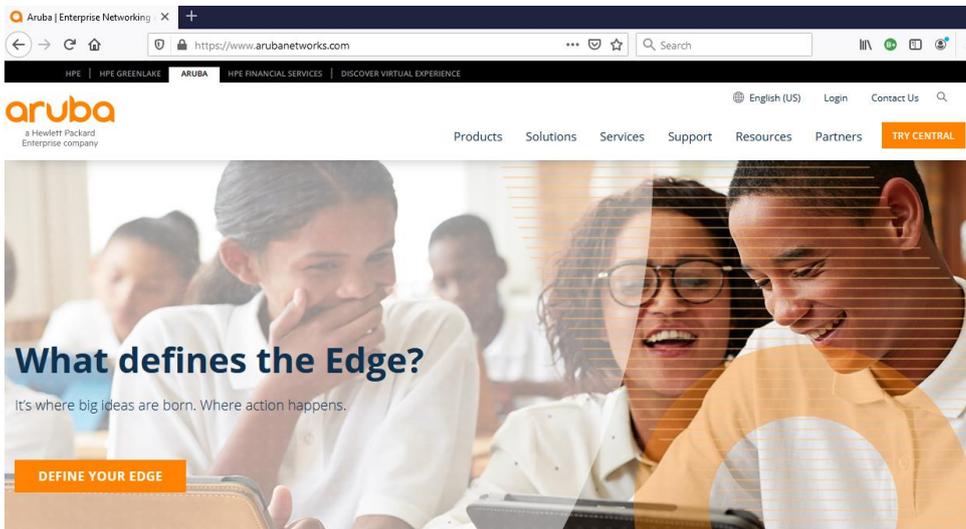
External Captive Portal

```
-----  
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".

All	Connecting	Connected	Failed	Offline	Blocked	Wireless	Wired	Remote
3	0	1	0	2	0	1	2	0

Client Name	Status	IP Address	VLAN	Connected To	Gateway Role	SSID/Port	Health	Usage
cpuser	Connected	192.168.1.132	192	b4:5d:50:c6:82:4a	guest	School-Guest	Good	8.31 MB

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

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.95	RADIUS	cpuser	GG User Authentication with MAC Caching	ACCEPT	2021/03/17 11:26:22
2.	192.168.1.95	RADIUS	a088b450c084	GG MAC Authentication	REJECT	2021/03/17 11:25:58

**Request Details**

Summary | Input | Output | Accounting

Login Status: ACCEPT

Session Identifier: R0000000a-01-60514cae

Date and Time: Mar 17, 2021 11:26:22 AEDT

End-Host Identifier: A0-88-B4-50-C0-84

Username: cpuser

Access Device IP/Port: 192.168.1.242

Access Device Name: AOS10-gateways

System Posture Status: UNKNOWN (100)

**Policies Used -**

Service: GG User Authentication with MAC Caching

Authentication Method: PAP

Authentication Source: Local:localhost

Authorization Source: [Guest User Repository], [Endpoints Repository], [Time Source]

Roles: [Guest], [User Authenticated]

Enforcement Profiles: GG MAC Caching Bandwidth Limit. GG MAC Caching Session Limit. GG Guest MAC

Showing 1 of 1-11 records | Change Status | Show Configuration | Export | Show Logs | Close

**Request Details**

Summary Input **Output** Accounting

Audit Posture Status: UNKNOWN (100)

**RADIUS Response**

Bandwidth-Check:Allowed-Limit	0
Bandwidth-Check:Check-Type	Today
Bandwidth-Check:Limit-Units	MB
Endpoint:Guest Role ID	2
Endpoint:MAC-Auth Expiry	2021-03-18 11:00:00
Endpoint:Username	cpguser
Expire-Time-Update:GuestUser	0
Expiry-Check:Expiry-Action	0
Post-Auth-Check:Action	Disconnect
Post-Auth-Check:Action	Disconnect and Block Access
Radius:Aruba:Aruba-User-Role	Guest
Radius:IETF:Session-Timeout	0

Showing 1 of 1-11 records | Change Status Show Configuration Export Show Logs Close

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

Configuration > Identity > Endpoints

**Endpoints**

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

Filter: MAC Address contains Go Clear Filter Show 20 records

#	MAC Address	Hostname	Device Category	Device OS Family	Status	Profiled
1.	00-0C-29-F3-EF-AF	victory	Server	ClearPass	Unknown	Yes
2.	A0-88-B4-50-C0-84		Computer	Windows	known	Yes

Showing 1-2 of 2 | Authentication Records Bulk Update Bulk Delete Trigger Server Action Update Fingerprint Export Delete

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.

**Request Details**

Summary Input Output Accounting

Login Status: ACCEPT

Session Identifier: R0000000a-01-60514cae

Date and Time: Mar 17, 2021 11:26:22 AEDT

End-Host Identifier: A0-88-B4-50-C0-84

Username: cpguser

Access Device IP/Port: 192.168.1.242

Access Device Name: AOS10-gateways

System Posture Status: UNKNOWN (100)

**Policies Used -**

Service: GG User Authentication with MAC Caching

Authentication Method: PAP

Authentication Source: Local:localhost

Authorization Source: [Guest User Repository], [Endpoints Repository], [Time Source]

Roles: [Guest], [User Authenticated]

Enforcement Profiles: GG MAC Caching Bandwidth Limit. GG MAC Caching Session Limit. GG Guest MAC

Showing 1 of 1-11 records | Change Status Show Configuration Export Show Logs Close

**Request Details**

**Access Control Capabilities -**

Select Access Control Type :  Agent  SNMP  RADIUS CoA  Server Action

RADIUS CoA Type: [ArubaOS Wireless - Terminat]

Submit Cancel

**Request Details**

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

Summary Input Output Accounting

Login Status: ACCEPT

Session Identifier: R0000000a-01-60514cae

Date and Time: Mar 17, 2021 11:26:22 AEDT

End-Host Identifier: A0-88-B4-50-C0-84

Username: cpguser

Access Device IP/Port: 192.168.1.242

Access Device Name: AOS10-gateways

System Posture Status: UNKNOWN (100)

**Policies Used -**

Service: GG User Authentication with MAC Caching

Authentication Method: PAP

Authentication Source: Local:localhost

Authorization Source: [Guest User Repository], [Endpoints Repository], [Time Source]

Roles: [Guest], [User Authenticated]

Enforcement Profiles: GG MAC Caching Bandwidth Limit. GG MAC Caching Session Limit. GG Guest MAC

Showing 1 of 1-11 records | Change Status Show Configuration Export Show Logs Close

aruba ClearPass Policy Manager

Monitoring » Live Monitoring » Access Tracker

Access Tracker Mar 17, 2021 11:33:25 AEDT Auto Refresh

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

[All Requests] victory (192.168.1.95) Last 1 day before Today Edit

Filter: Request ID contains [ ] Go Clear Filter Show 20 records

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.95	RADIUS	cpuser	GG MAC Authentication	ACCEPT	2021/03/17 11:33:04
2.	192.168.1.95	RADIUS	cpuser	GG User Authentication with MAC Caching	ACCEPT	2021/03/17 11:26:22
3.	192.168.1.95	RADIUS	a088b450c084	GG MAC Authentication	REJECT	2021/03/17 11:25:58

### Looking at the details of that session

Request Details

Summary Input Output Accounting

Login Status: ACCEPT  
 Session Identifier: R0000000b-01-60514e40  
 Date and Time: Mar 17, 2021 11:33:04 AEDT  
 End-Host Identifier: A0-88-B4-50-C0-84  
 Username: cpuser  
 Access Device IP/Port: 192.168.1.242  
 Access Device Name: AOS10-gateways  
 System Posture Status: UNKNOWN (100)

**Policies Used -**

Service: GG MAC Authentication  
 Authentication Method: MAC-AUTH  
 Authentication Source: Local:localhost  
 Authorization Source: [Guest User Repository], [Endpoints Repository], [Time Source]  
 Roles: [Guest], [MAC Caching], [User Authenticated]  
 Enforcement Profiles: [Allow Access Profile], GG Guest Device Profile

Request Details

Summary Input Output Accounting

Enforcement Profiles: [Allow Access Profile], GG Guest Device Profile  
 System Posture Status: UNKNOWN (100)  
 Audit Posture Status: UNKNOWN (100)

**RADIUS Response**

Radius:Aruba:Aruba-User-Role Guest  
 Radius:IETF:User-Name cpuser

Showing 1 of 1-12 records Change Status Show Configuration Export Show Logs Close

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
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

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