Contents

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
15 Dec 2023	0.1	Ariya Parsamanesh	Initial creation
08 Jan 2024	0.2	Ariya Parsamanesh	Updated mixed mode

2 Demo Topology

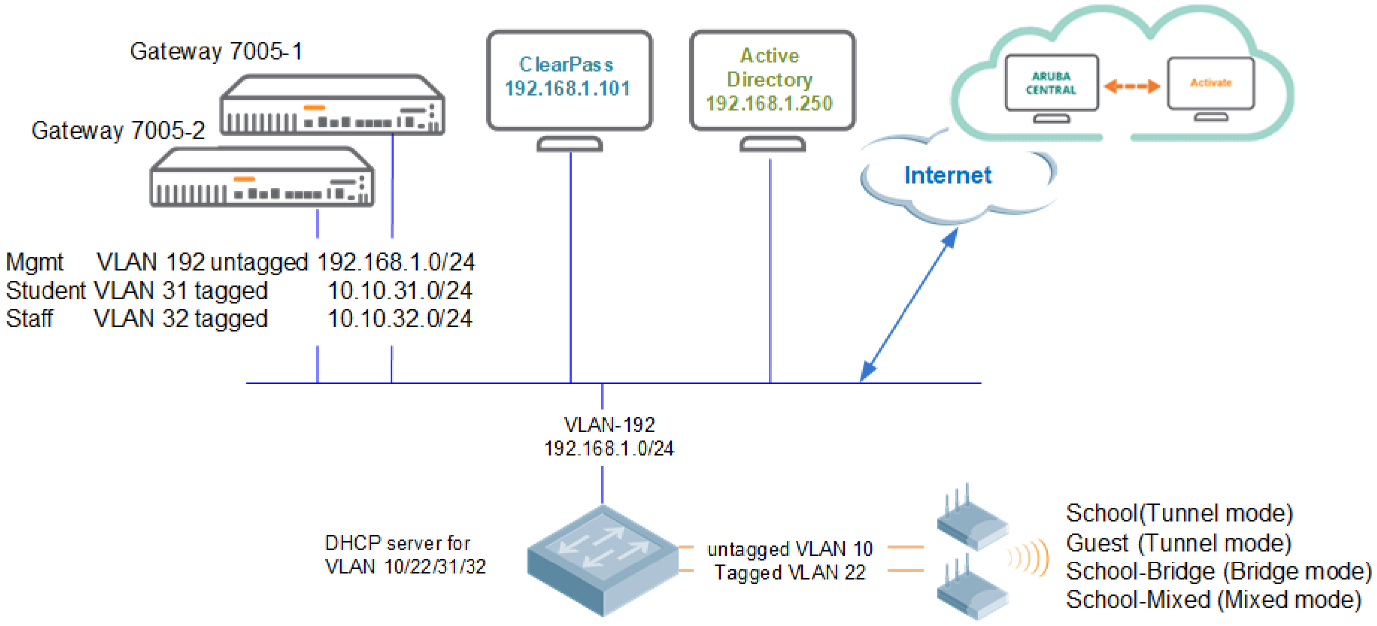
This is the first part of this 4x parts AOS10.4 tutorial series. The aim here is to provide the starting point to put together a solution that include the AOS10 APs, two gateways, ClearPass and obviously Aruba Central.

This part covers the configuration for

- Aruba Central AP group
- Aruba Central gateway group
- ClearPass

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.

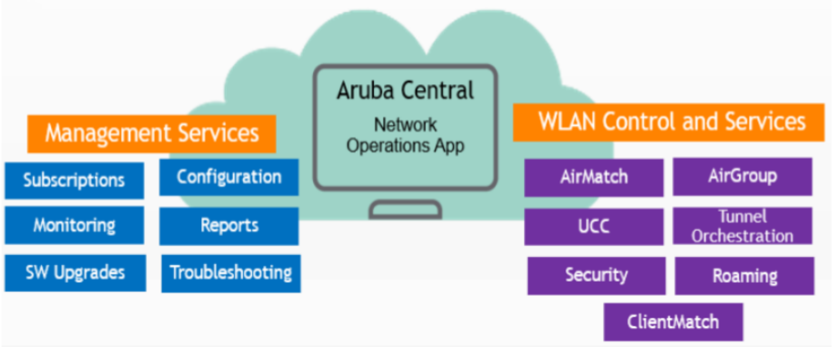
This is type of deployment is particularly useful when all the buildings in a school/college campus have L3 IP demarcation and are routed to various part of the campus.



Gateway 7005-1
Gateway 7005-2
ClearPass 192.168.1.101
Active Directory 192.168.1.250
ARUBA CENTRAL
Activate
Internet
Mgmt VLAN 192 untagged 192.168.1.0/24
Student VLAN 31 tagged 10.10.31.0/24
Staff VLAN 32 tagged 10.10.32.0/24
VLAN-192
192.168.1.0/24
DHCP server for VLAN 10/22/31/32
untagged VLAN 10
Tagged VLAN 22
School(Tunnel mode)
Guest (Tunnel mode)
School-Bridge (Bridge mode)
School-Mixed (Mixed mode)

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/central/latest/content/aos10x/aos10x-overview/architecture-overview-aos10.htm

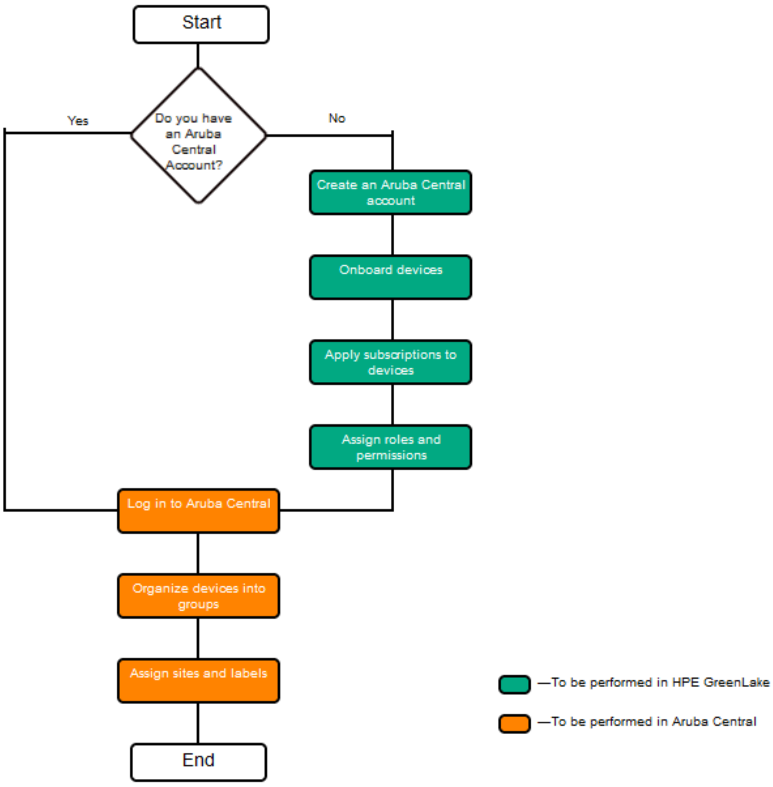
3 Aruba Central Account

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

https://www.arubanetworks.com/techdocs/central/latest/content/nms/get-started/typical_workflow.htm

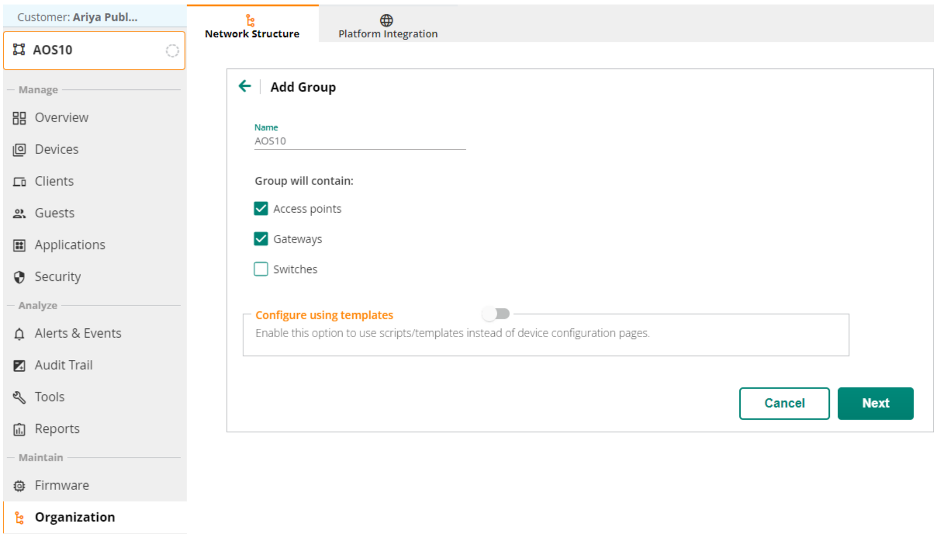
Getting Started with Aruba Central

The following illustration summarizes the steps required for getting started with Aruba Central:


Start
Do you have an Aruba Central Account?
Yes
No
Create an Aruba Central account
Onboard devices
Apply subscriptions to devices
Assign roles and permissions
Log in to Aruba Central
Organize devices into groups
Assign sites and labels
End
🟩 —To be performed in HPE GreenLake
🟧 —To be performed in Aruba Central

Here we have assumed your gateways and APs are added And subscribed to your greenlake account.

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



Add Group

Name
AOS10

Group will contain:

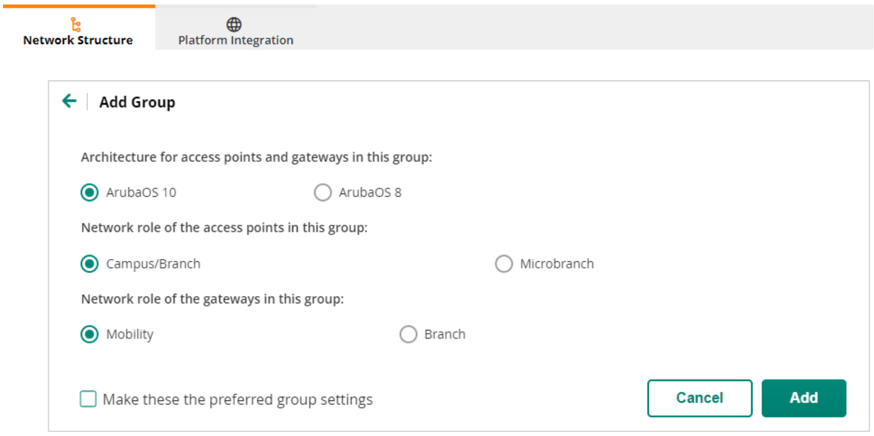
☑ Access points

☑ Gateways

☐ Switches

Configure using templates

Enable this option to use scripts/templates instead of device configuration pages.



Add Group

Architecture for access points and gateways in this group:

● ArubaOS 10 ○ ArubaOS 8

Network role of the access points in this group:

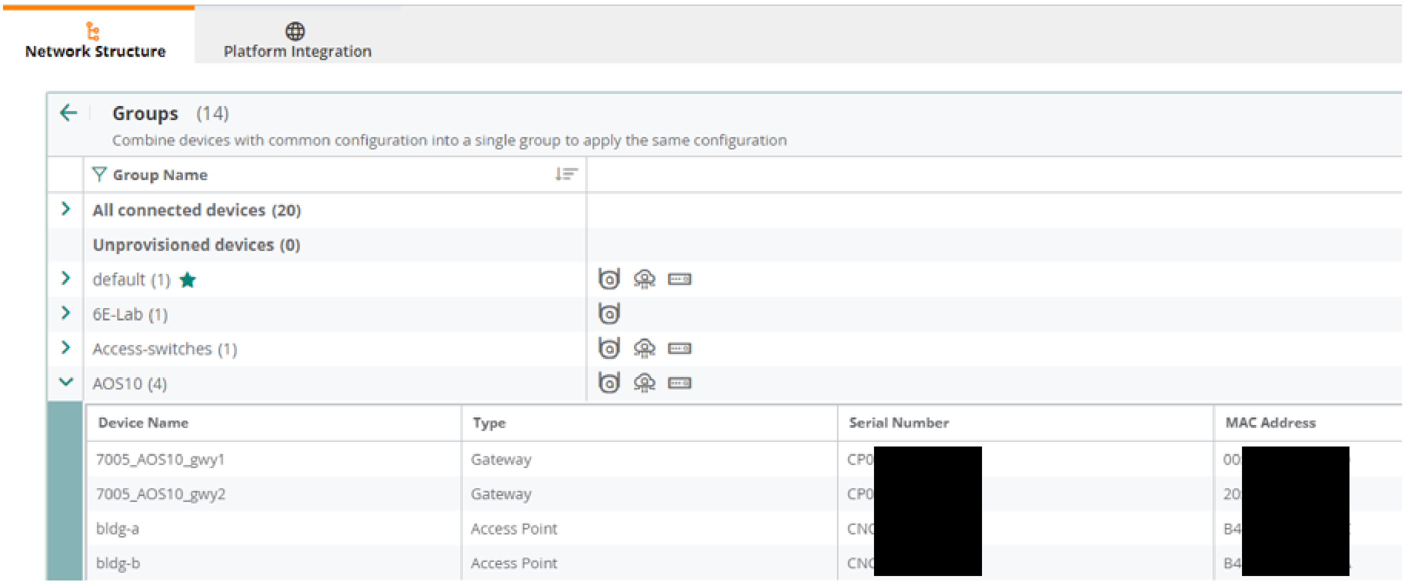
● Campus/Branch ○ Microbranch

Network role of the gateways in this group:

● Mobility ○ Branch

□ Make these the preferred group settings

Once you add the new group, you can then move the APs and gateways to it.



Groups (14)

Combine devices with common configuration into a single group to apply the same configuration

Group Name
All connected devices (20)
Unprovisioned devices (0)
default (1) ★
6E-Lab (1)
Access-switches (1)
AOS10 (4)

Device Name	Type	Serial Number	MAC Address
7005_AOS10_gwy1	Gateway	[redacted]	[redacted]
7005_AOS10_gwy2	Gateway	[redacted]	[redacted]
bldg-a	Access Point	[redacted]	[redacted]
bldg-b	Access Point	[redacted]	[redacted]

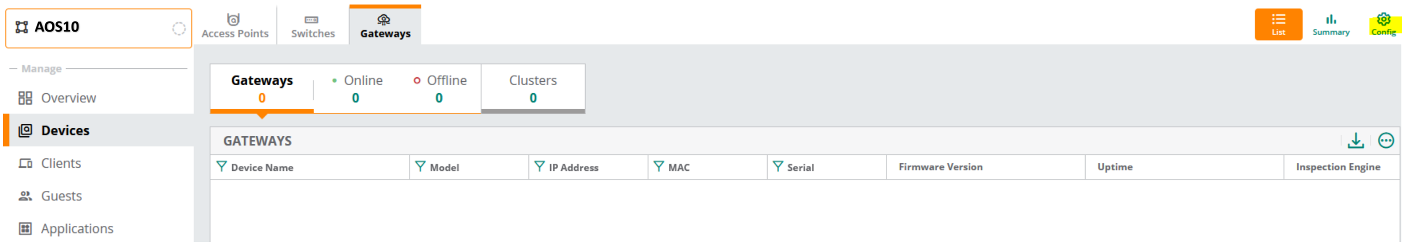
4 Aruba Central Configuration

4.1 Gateway Configuration

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

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

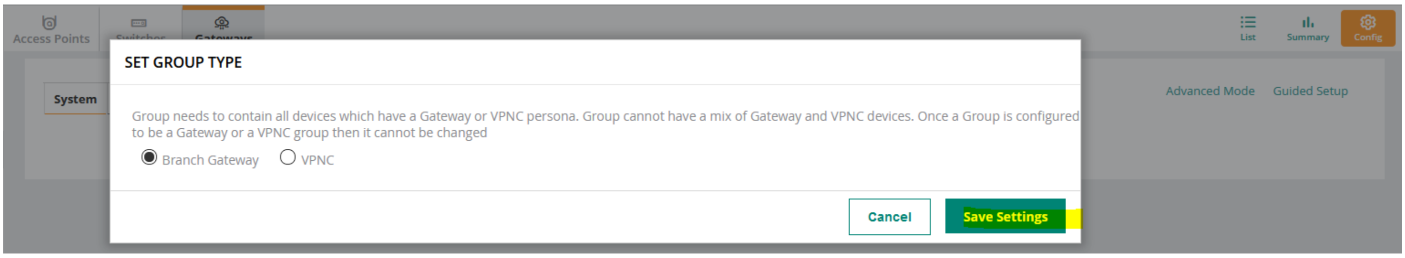
We'll be using Aruba 7005 gateways which have 4x ports.



Gateways	Online	Offline	Clusters
0	0	0	0

GATEWAYS

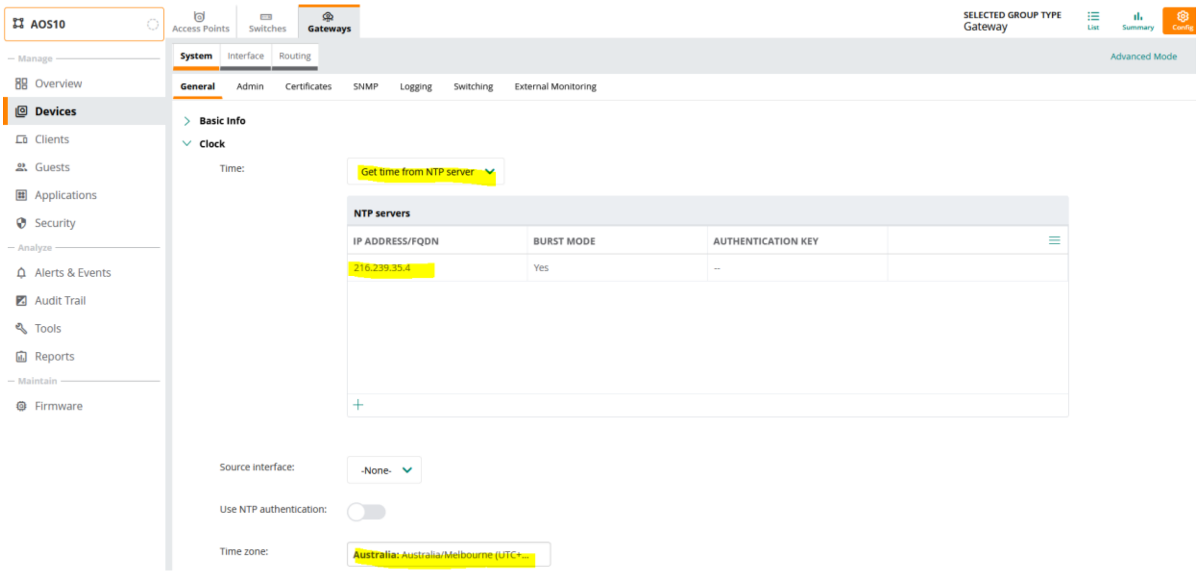
Device Name	Model	IP Address	MAC	Serial	Firmware Version	Uptime	Inspection Engine



SET GROUP TYPE

Group needs to contain all devices which have a Gateway or VPNC persona. Group cannot have a mix of Gateway and VPNC devices. Once a Group is configured to be a Gateway or a VPNC group then it cannot be changed

● Branch Gateway ○ VPNC



SELECTED GROUP TYPE
Gateway

Time: Get time from NTP server

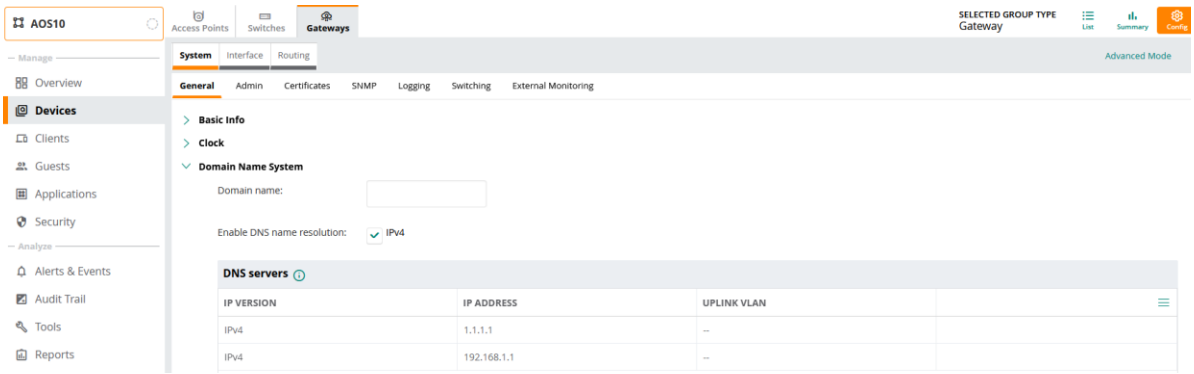
NTP servers

IP ADDRESS/FQDN	BURST MODE	AUTHENTICATION KEY
216.239.35.4	Yes	--

Source interface: -None-

Use NTP authentication:

Time zone: Australia: Australia/Melbourne (UTC+...



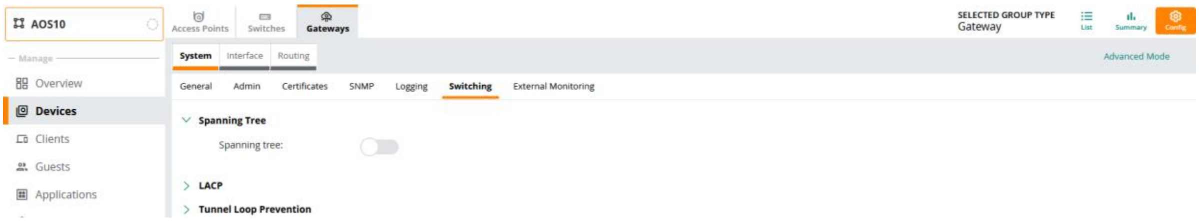
Domain name:

Enable DNS name resolution: ☑ IPv4

DNS servers

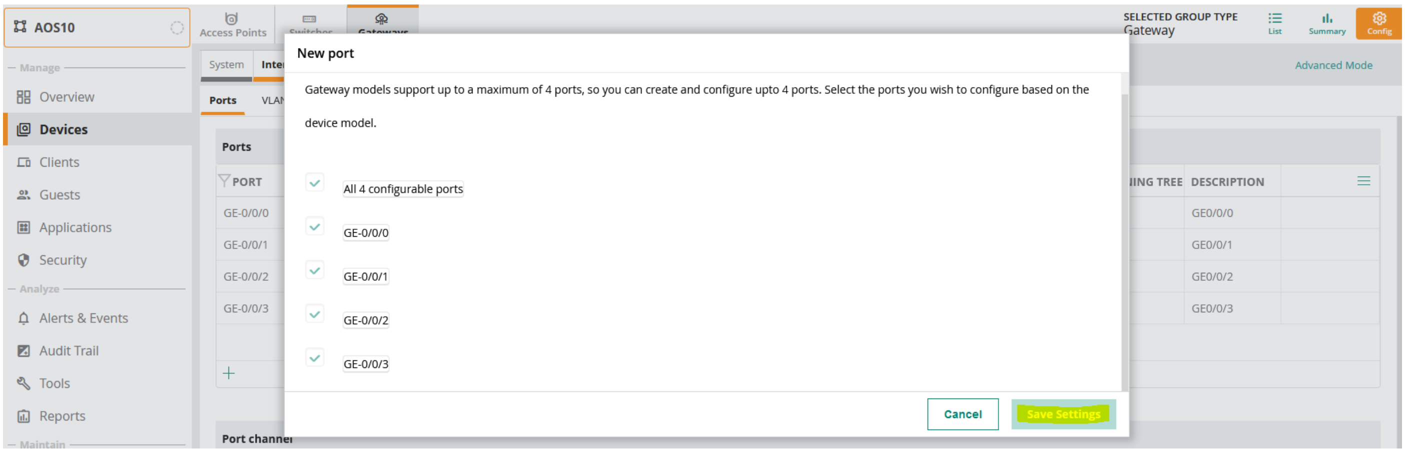
IP VERSION	IP ADDRESS	UPLINK VLAN
IPv4	1.1.1.1	--
IPv4	192.168.1.1	--

Disabling spanning tree



Spanning tree: ○

Adding the relevant ports for Aruba 7005 gateway.



New port

Gateway models support up to a maximum of 4 ports, so you can create and configure upto 4 ports. Select the ports you wish to configure based on the device model.

☑ All 4 configurable ports

☑ GE-0/0/0

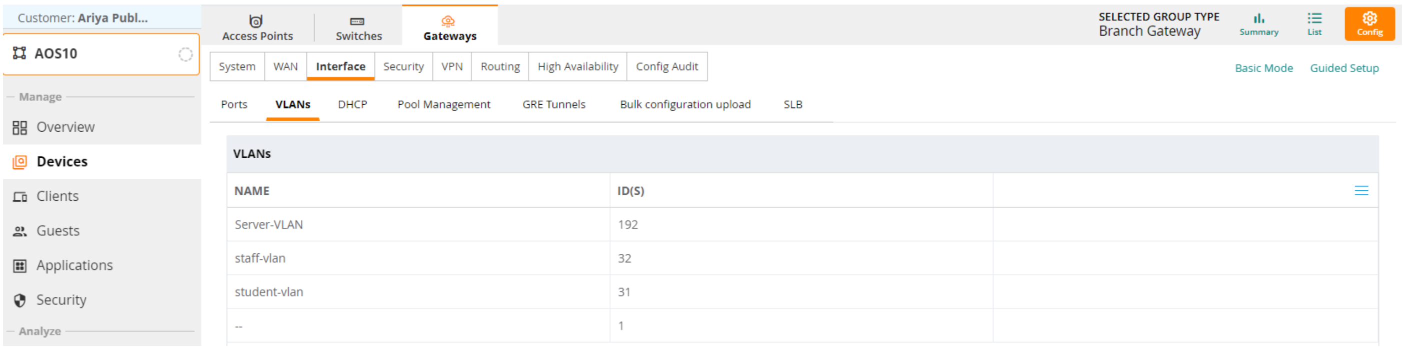
☑ GE-0/0/1

☑ GE-0/0/2

☑ GE-0/0/3

PORT	DESCRIPTION
GE-0/0/0	GE0/0/0
GE-0/0/1	GE0/0/1
GE-0/0/2	GE0/0/2
GE-0/0/3	GE0/0/3

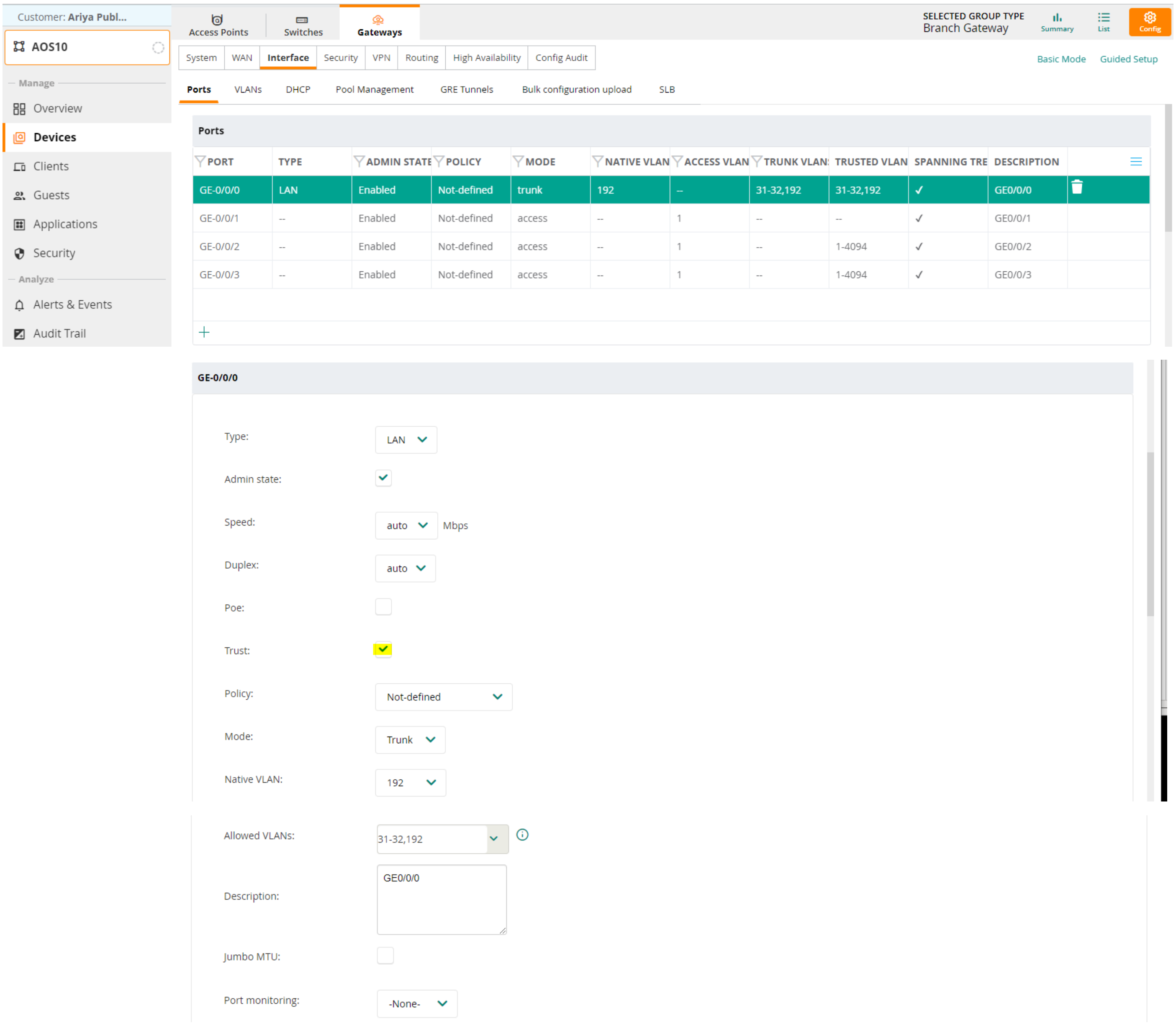
I am planning to sue interface 0/0/0 as my gateway uplink. This port needs to be in trunk mode and here we'll add the relevant VLANs.



VLANs

NAME	ID(S)
Server-VLAN	192
staff-vlan	32
student-vlan	31
--	1

Adding the VLANs to appropriate ports.



Ports

PORT	TYPE	ADMIN STATE	POLICY	MODE	NATIVE VLAN	ACCESS VLAN	TRUNK VLAN:	TRUSTED VLAN	SPANNING TRE	DESCRIPTION
GE-0/0/0	LAN	Enabled	Not-defined	trunk	192	--	31-32,192	31-32,192	✓	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

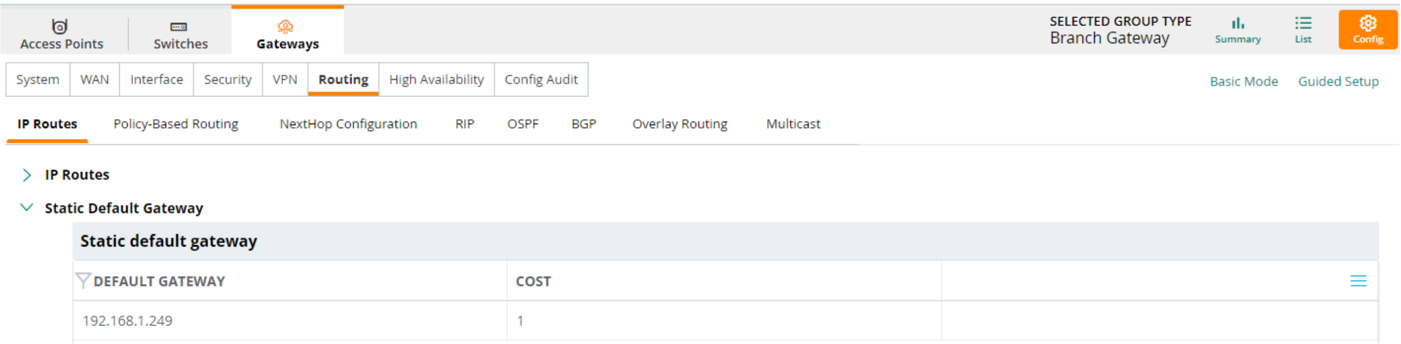
Allowed VLANs: 31-32,192

Description: GE0/0/0

Jumbo MTU: □

Port monitoring: -None-

Adding the default route

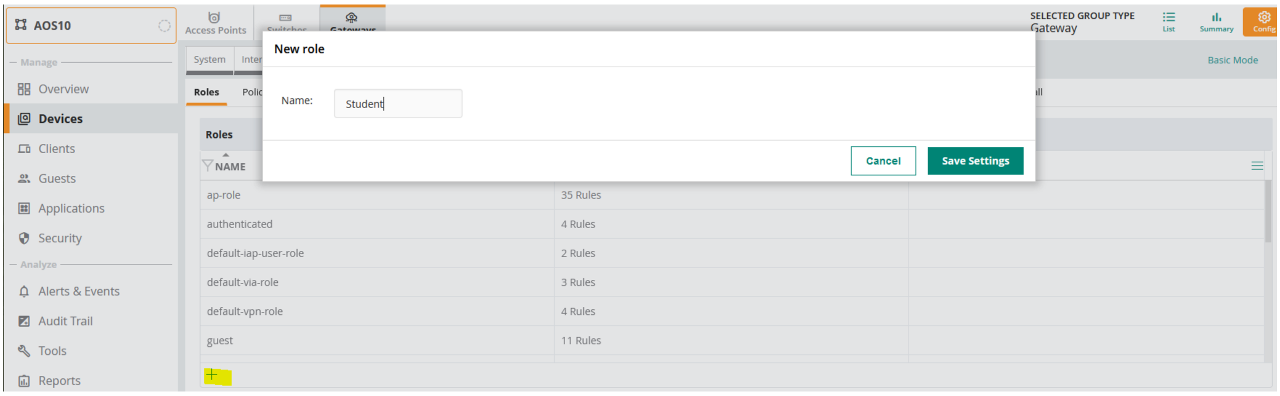


Static default gateway

DEFAULT GATEWAY	COST
192.168.1.249	1

Adding the user roles by going to “security tab”. Here we’ll add staff and student user-roles.

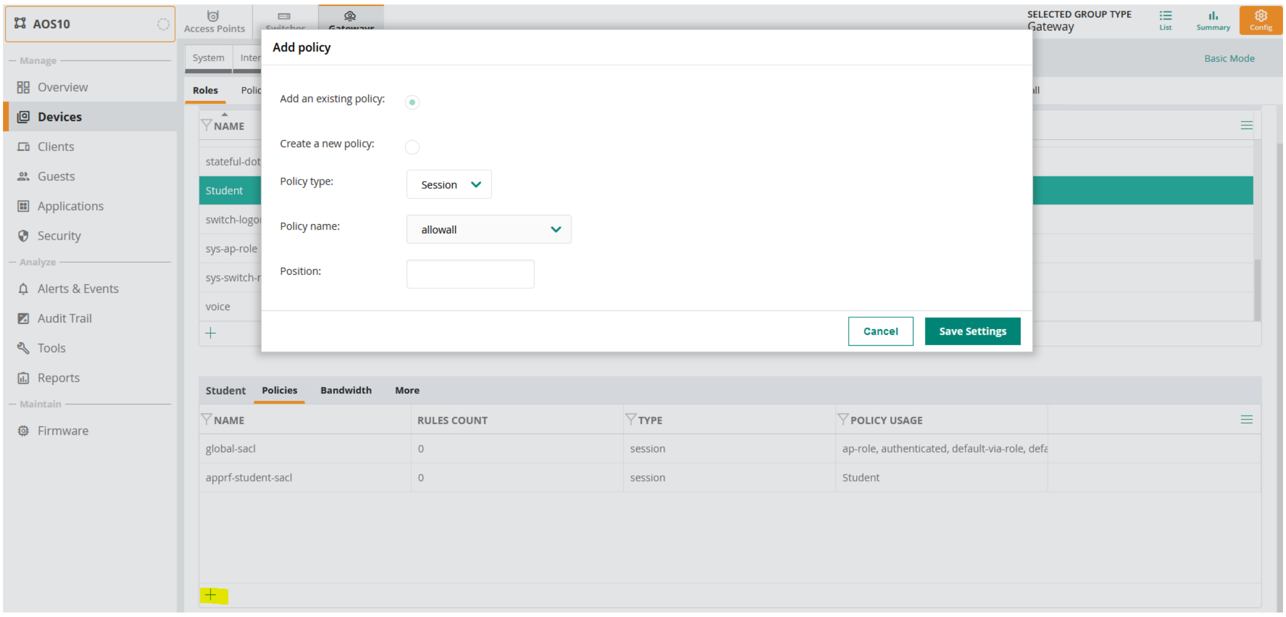
Now a note on the user-roles on the gateways. When you configure a tunnel mode in WLAN on the AOS10 APs, the user roles get send to gateways as well so you don’t need to configure them here. Aruba Central does this orchestration.



New role

Name: Student

NAME	
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



Add policy

Add an existing policy: ●

Create a new policy: ○

Policy type: Session

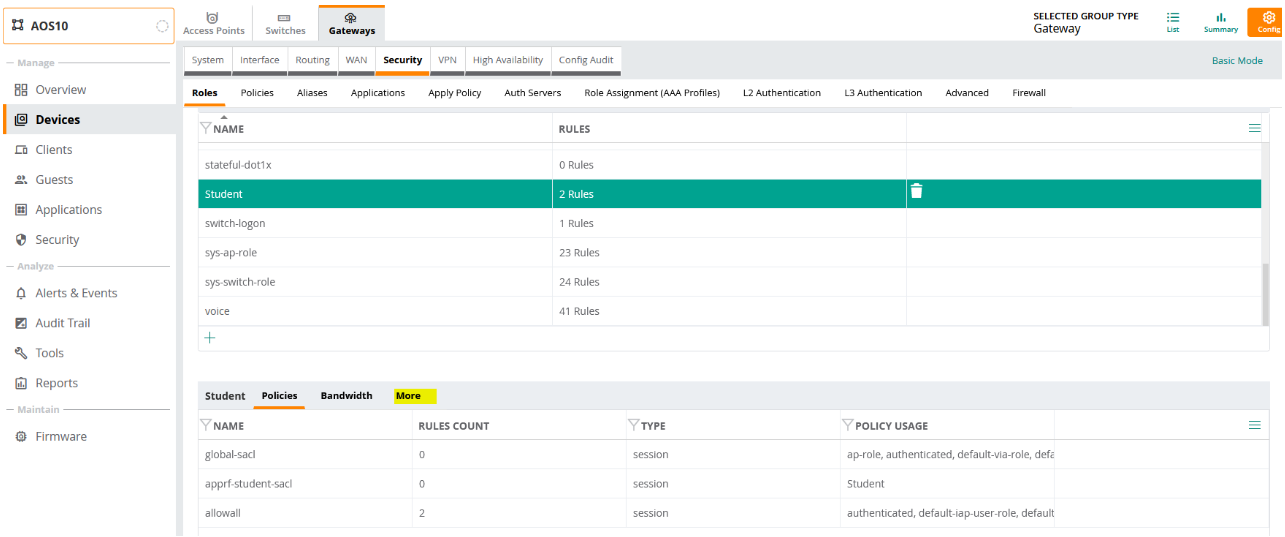
Policy name: allowall

Position:

Student | Policies | Bandwidth | More

NAME	RULES COUNT	TYPE	POLICY USAGE
global-sacl	0	session	ap-role, authenticated, default-via-role, defa
apprf-student-sacl	0	session	Student

Here we'll add the allow-all policy.

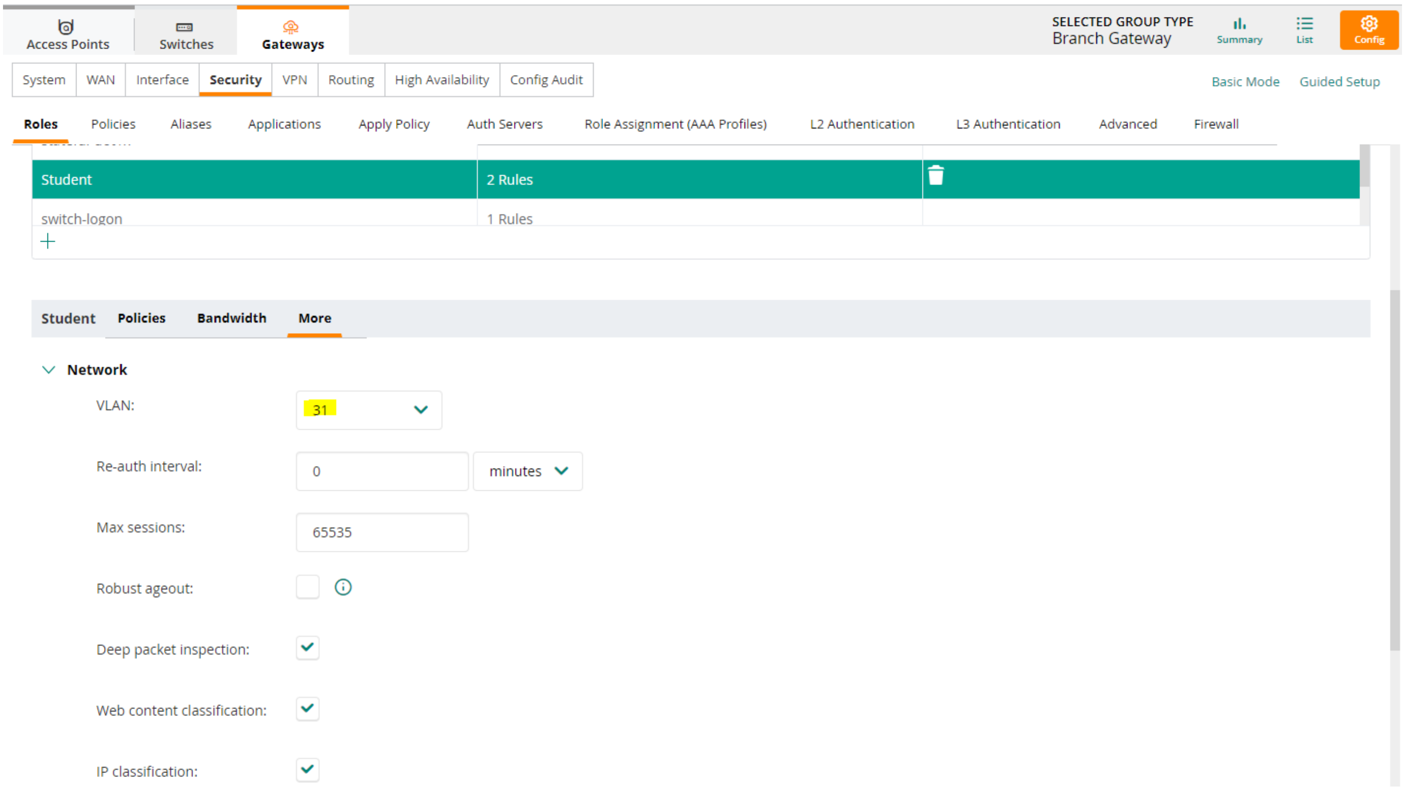


NAME	RULES
stateful-dot1x	0 Rules
Student	2 Rules
switch-logon	1 Rules
sys-ap-role	23 Rules
sys-switch-role	24 Rules
voice	41 Rules

Student | Policies | Bandwidth | More

NAME	RULES COUNT	TYPE	POLICY USAGE
global-sacl	0	session	ap-role, authenticated, default-via-role, defa
apprf-student-sacl	0	session	Student
allowall	2	session	authenticated, default-iap-user-role, default

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



Student	2 Rules
switch-logon	1 Rules

Network

VLAN: 31

Re-auth interval: 0 minutes

Max sessions: 65535

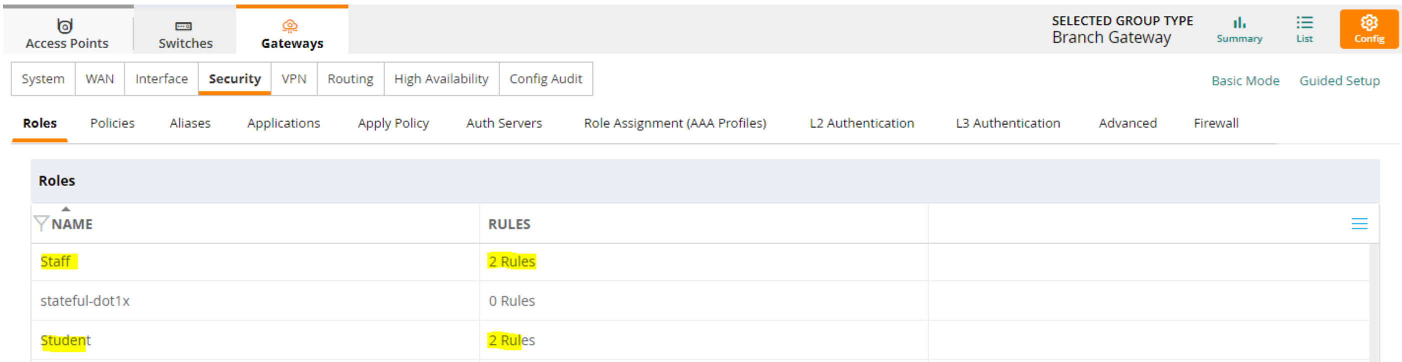
Robust ageout: □

Deep packet inspection: ☑

Web content classification: ☑

IP classification: ☑

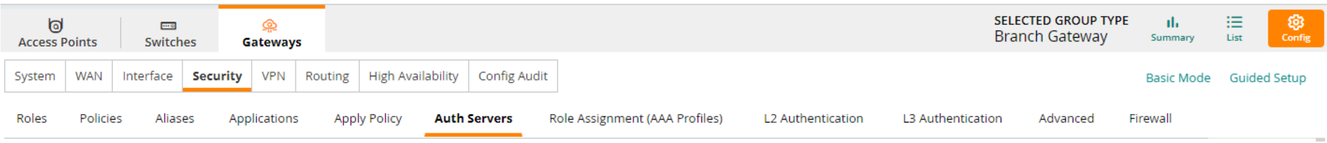
We’ll create a new user role staff and as before, we’ll add a allow-all policy and assign VLAN 32 to it.

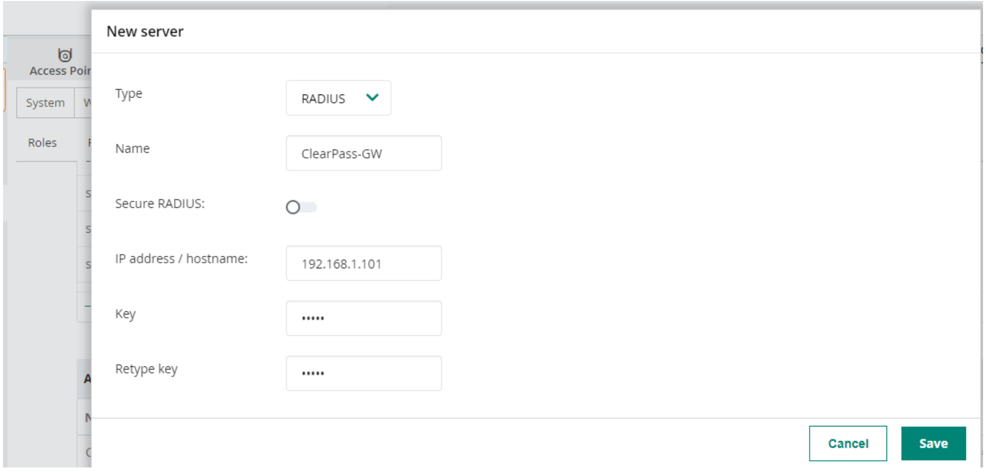


Roles

NAME	RULES
Staff	2 Rules
stateful-dot1x	0 Rules
Student	2 Rules

Next, we’ll configure the authentication server and RFC3576 for RADIUS CoA.





New server

Type: RADIUS

Name: ClearPass-GW

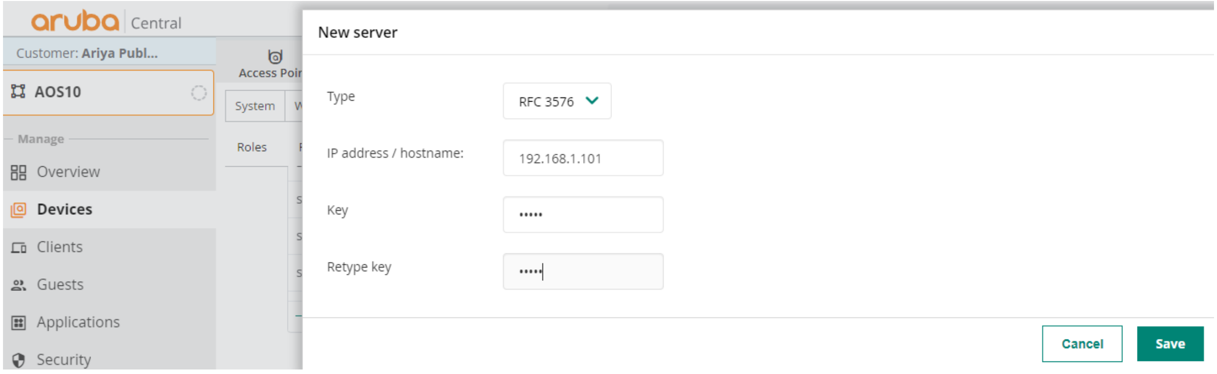
Secure RADIUS: ○

IP address / hostname: 192.168.1.101

Key: •••••

Retype key: •••••

Once saved, click on it to set the RADIUS secret key and finally add a rfc3576 server for CoA.



New server

Type: RFC 3576

IP address / hostname: 192.168.1.101

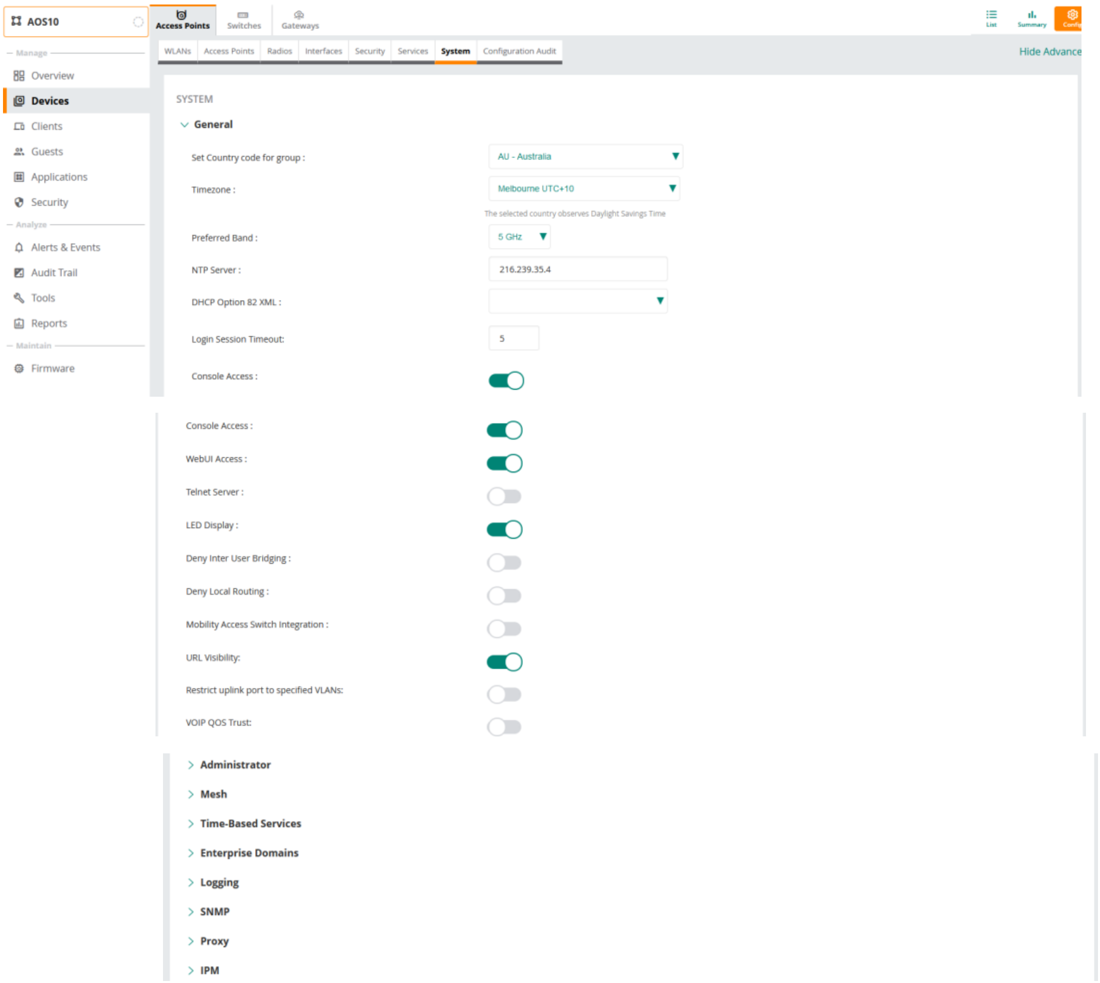
Key: •••••

Retype key: •••••

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

4.2 AP Configuration

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



SYSTEM

General

Set Country code for group : AU - Australia

Timezone : Melbourne UTC+10

The selected country observes Daylight Savings Time

Preferred Band : 5 GHz

NTP Server : 216.239.35.4

DHCP Option 82 XML :

Login Session Timeout: 5

Console Access : ●

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

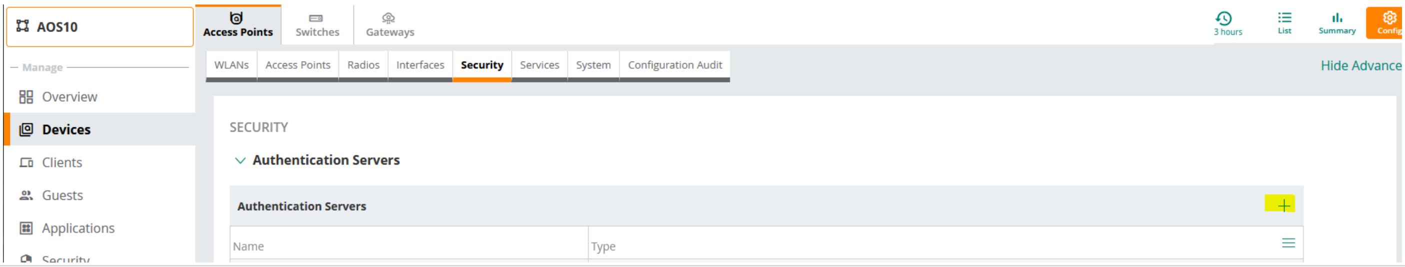
Enterprise Domains

Logging

SNMP

Proxy

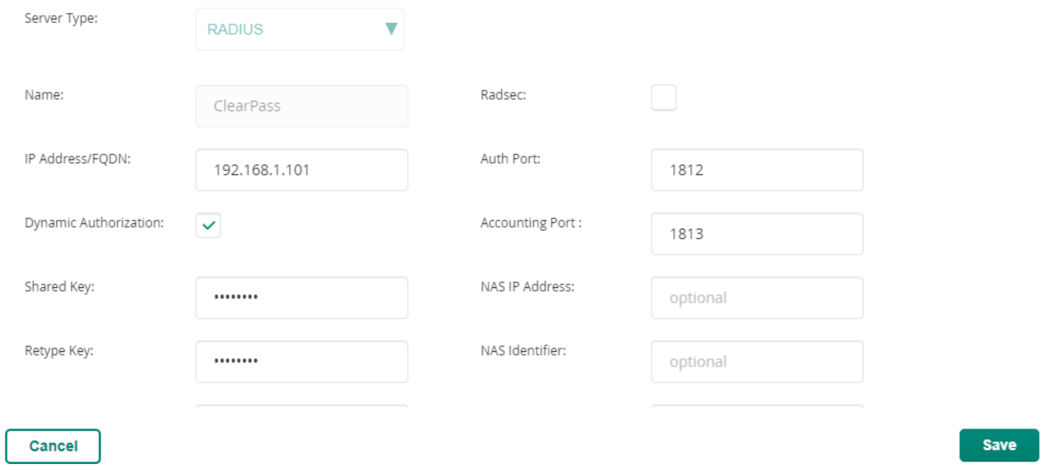
IPM



SECURITY

Authentication Servers

Authentication Servers	
Name	Type



Server Type: RADIUS

Name: ClearPass

Radsec: □

IP Address/FQDN: 192.168.1.101

Auth Port: 1812

Dynamic Authorization: ☑

Accounting Port : 1813

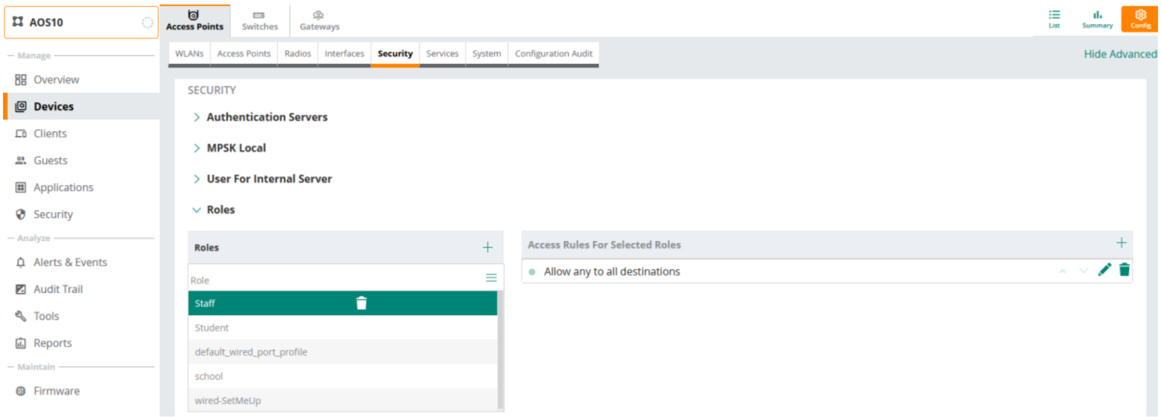
Shared Key: ••••••••

NAS IP Address: optional

Retype Key: ••••••••

NAS Identifier: optional

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



SECURITY

- Authentication Servers
- MPSK Local
- User For Internal Server
- Roles

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.

4.3 Gateway Cluster

Cluster is a combination of multiple gateways 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.

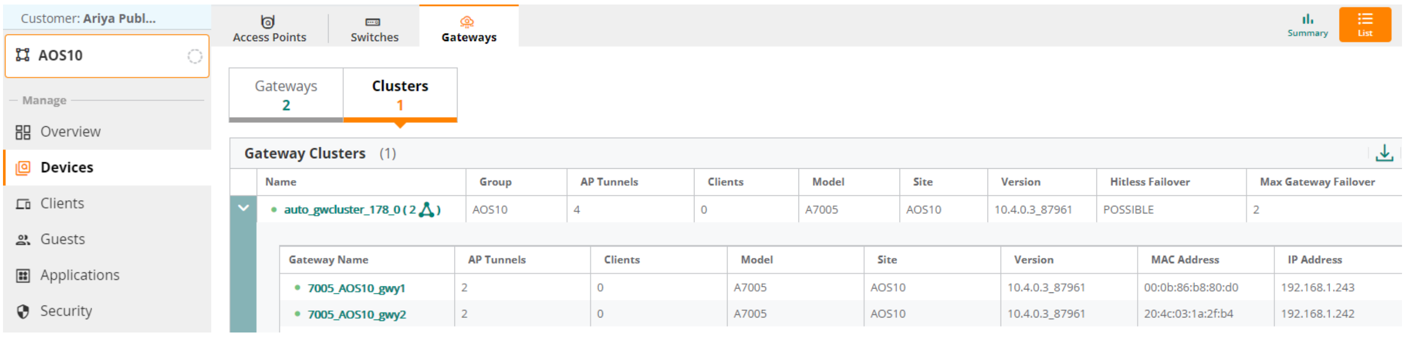
When the gateways in a group are assigned to the same site, the gateways automatically form a cluster among themselves.

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.

4.4 Monitoring Gateway Cluster

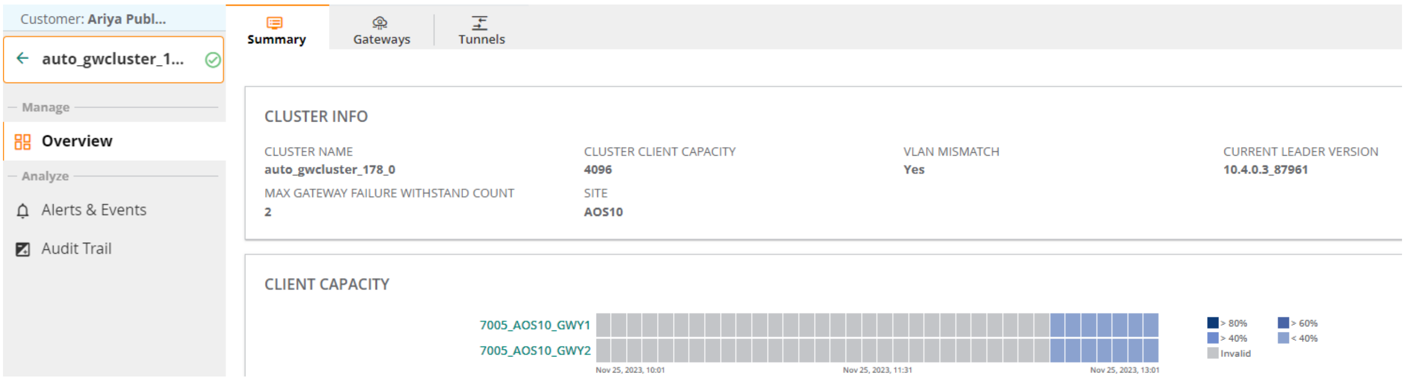
Since we have moved the two gateways to the AOS10 group, they automatically will form a cluster. Here is how to check the status of gateway cluster.



Gateway Clusters (1)

Name	Group	AP Tunnels	Clients	Model	Site	Version	Hitless Failover	Max Gateway Failover
auto_gwcluster_178_0 (2)	AOS10	4	0	A7005	AOS10	10.4.0.3_87961	POSSIBLE	2

Gateway Name	AP Tunnels	Clients	Model	Site	Version	MAC Address	IP Address
7005_AOS10_gwy1	2	0	A7005	AOS10	10.4.0.3_87961	00:0b:86:b8:80:d0	192.168.1.243
7005_AOS10_gwy2	2	0	A7005	AOS10	10.4.0.3_87961	20:4c:03:1a:2f:b4	192.168.1.242



CLUSTER INFO

CLUSTER NAME
auto_gwcluster_178_0

CLUSTER CLIENT CAPACITY
4096

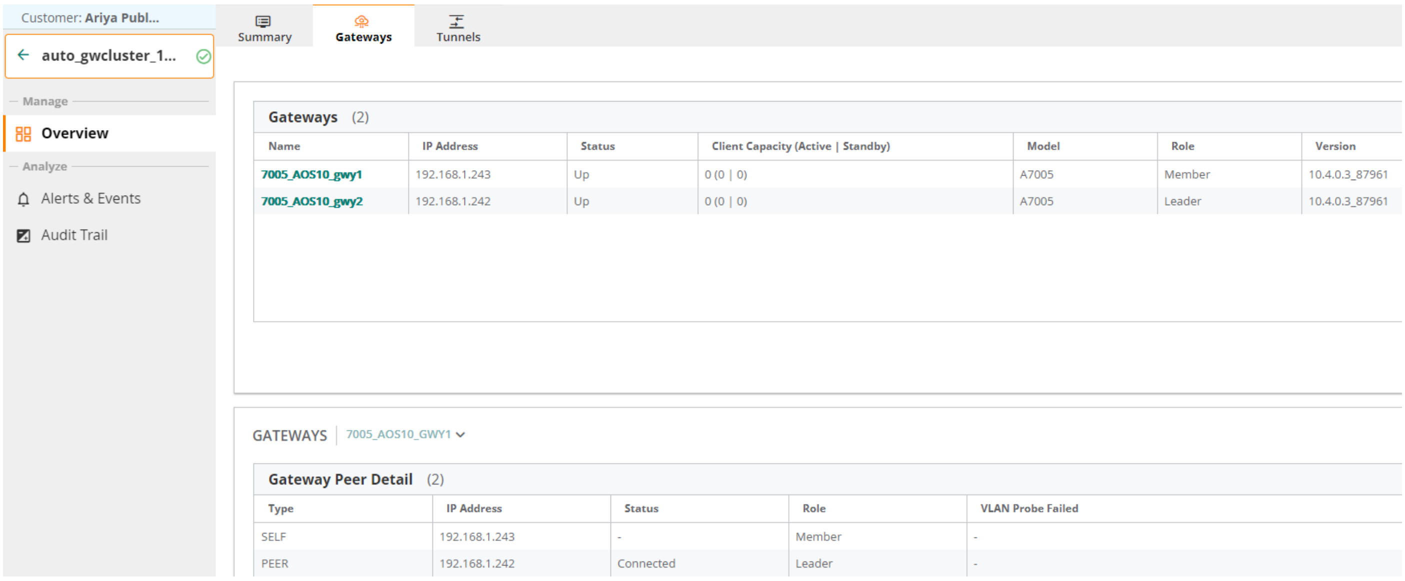
VLAN MISMATCH
Yes

CURRENT LEADER VERSION
10.4.0.3_87961

MAX GATEWAY FAILURE WITHSTAND COUNT
2

SITE
AOS10

CLIENT CAPACITY



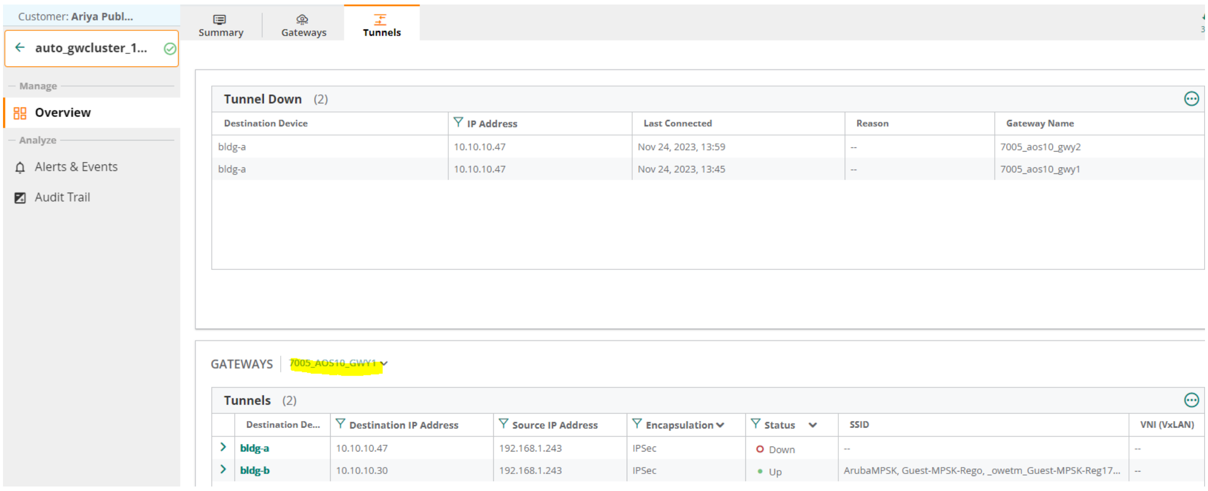
Gateways (2)

Name	IP Address	Status	Client Capacity (Active | Standby)	Model	Role	Version
7005_AOS10_gwy1	192.168.1.243	Up	0 (0 | 0)	A7005	Member	10.4.0.3_87961
7005_AOS10_gwy2	192.168.1.242	Up	0 (0 | 0)	A7005	Leader	10.4.0.3_87961

GATEWAYS 7005_AOS10_GWY1

Gateway Peer Detail (2)

Type	IP Address	Status	Role	VLAN Probe Failed
SELF	192.168.1.243	-	Member	-
PEER	192.168.1.242	Connected	Leader	-



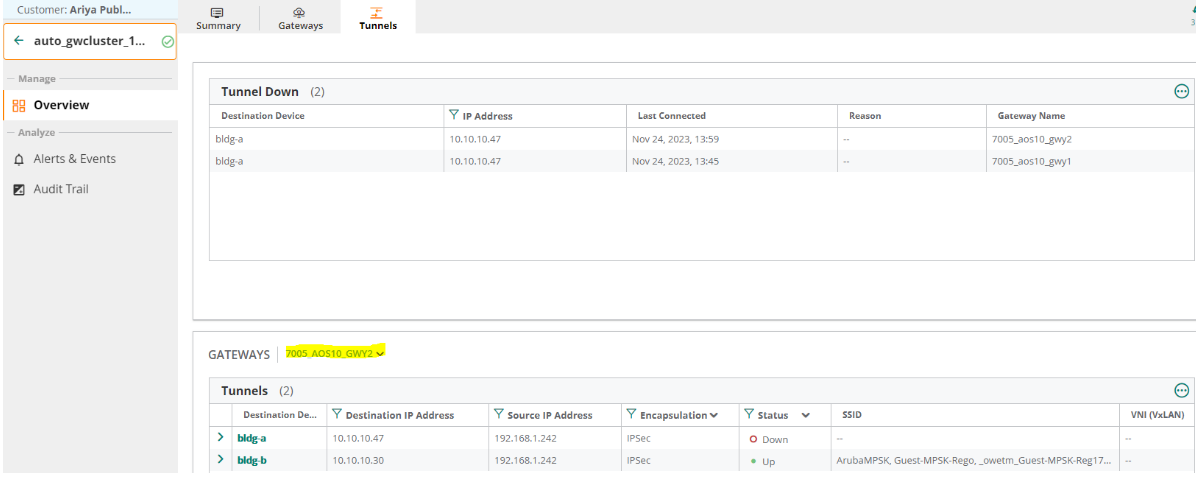
Tunnel Down (2)

Destination Device	IP Address	Last Connected	Reason	Gateway Name
bldg-a	10.10.10.47	Nov 24, 2023, 13:59	--	7005_aos10_gwy2
bldg-a	10.10.10.47	Nov 24, 2023, 13:45	--	7005_aos10_gwy1

GATEWAYS 7005_AOS10_GWY1

Tunnels (2)

Destination De...	Destination IP Address	Source IP Address	Encapsulation	Status	SSID	VNI (VxLAN)
bldg-a	10.10.10.47	192.168.1.243	IPSec	○ Down	--	--
bldg-b	10.10.10.30	192.168.1.243	IPSec	● Up	ArubaMPSK, Guest-MPSK-Rego, _owetm_Guest-MPSK-Reg17...	--



Tunnel Down (2)

Destination Device	IP Address	Last Connected	Reason	Gateway Name
bldg-a	10.10.10.47	Nov 24, 2023, 13:59	--	7005_aos10_gwy2
bldg-a	10.10.10.47	Nov 24, 2023, 13:45	--	7005_aos10_gwy1

GATEWAYS 7005_AOS10_GWY2

Tunnels (2)

Destination De...	Destination IP Address	Source IP Address	Encapsulation	Status	SSID	VNI (VxLAN)
bldg-a	10.10.10.47	192.168.1.242	IPSec	○ Down	--	--
bldg-b	10.10.10.30	192.168.1.242	IPSec	● Up	ArubaMPSK, Guest-MPSK-Rego, _owetm_Guest-MPSK-Reg17...	--

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) #
```

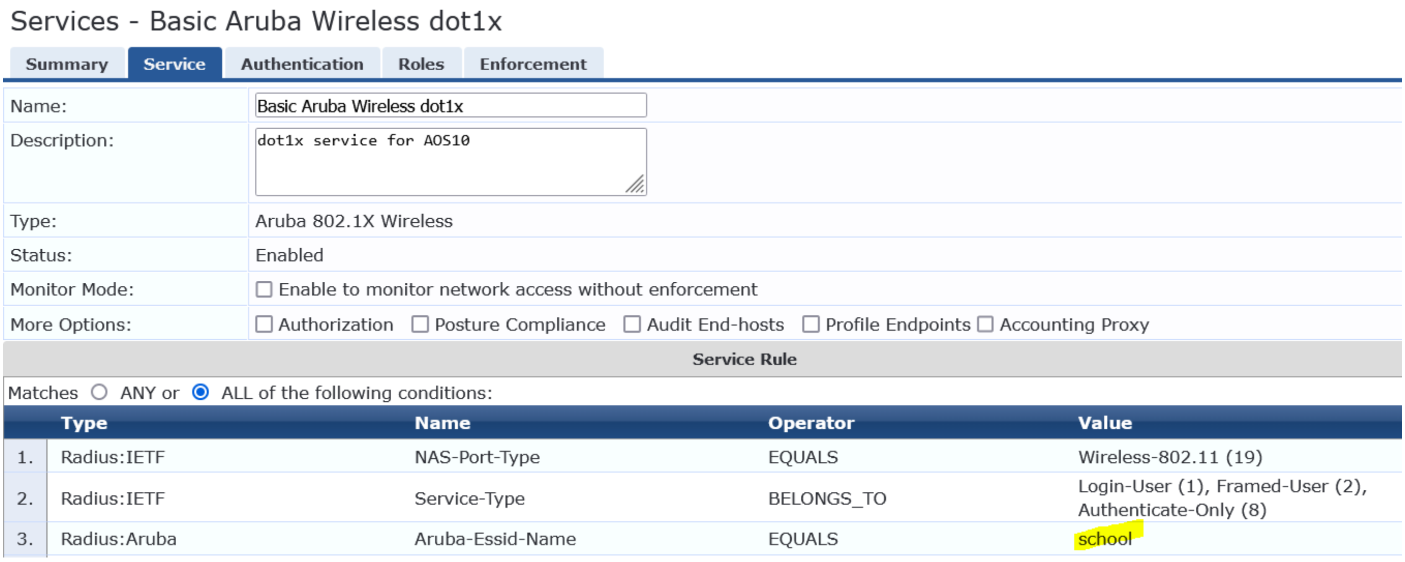
5 ClearPass Initial Configuration

Here we assume that the basic ClearPass configuration is done.

- NTP and time zone.
- Insight is enabled
- Joined the AD domain

5.1 ClearPass dot1x Service

Here we create a dot1x service for wireless access.



Services - Basic Aruba Wireless dot1x

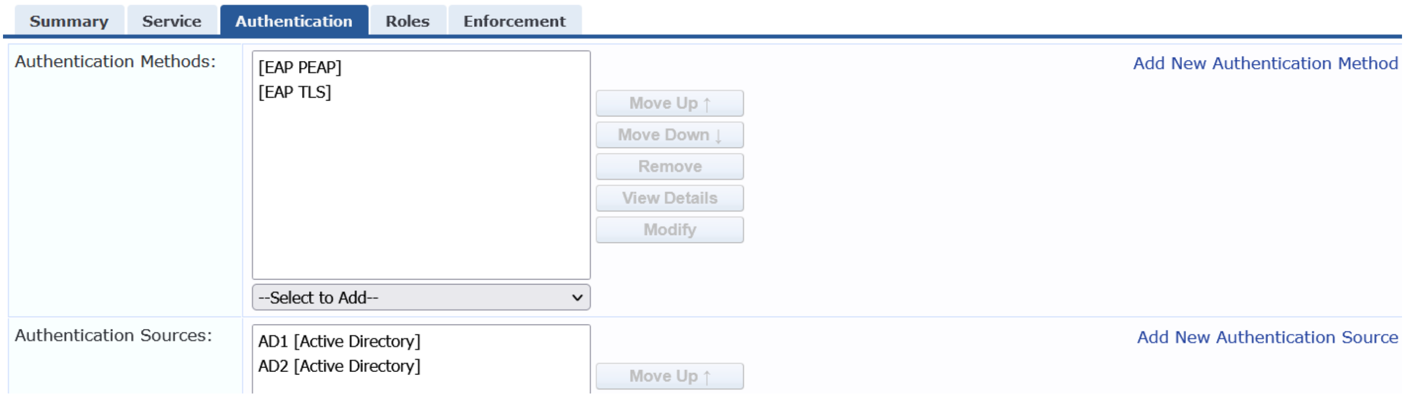
Name:	Basic Aruba Wireless dot1x
Description:	dot1x service for AOS10
Type:	Aruba 802.1X Wireless
Status:	Enabled
Monitor Mode:	□ Enable to monitor network access without enforcement
More Options:	□ Authorization □ Posture Compliance □ Audit End-hosts □ Profile Endpoints □ Accounting Proxy

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

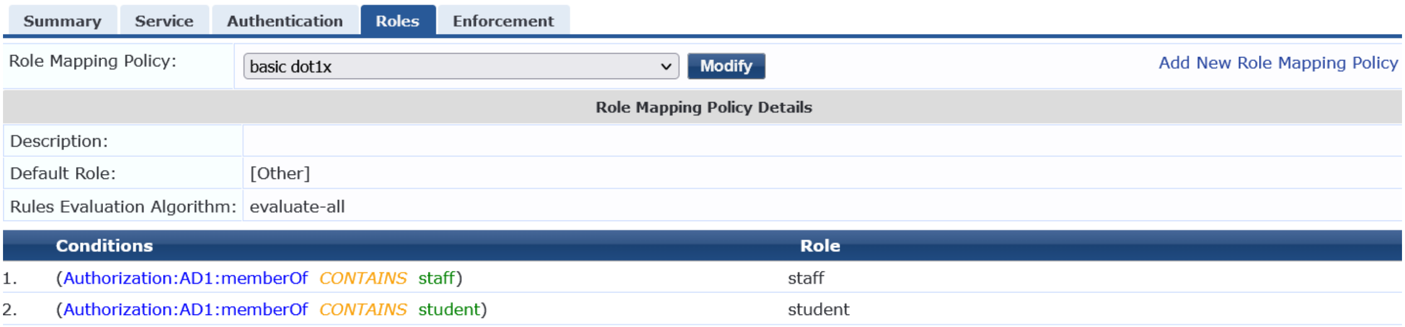
“school” is the name of the SSID



Authentication Methods: [EAP PEAP] [EAP TLS]

--Select to Add--

Authentication Sources: AD1 [Active Directory] AD2 [Active Directory]

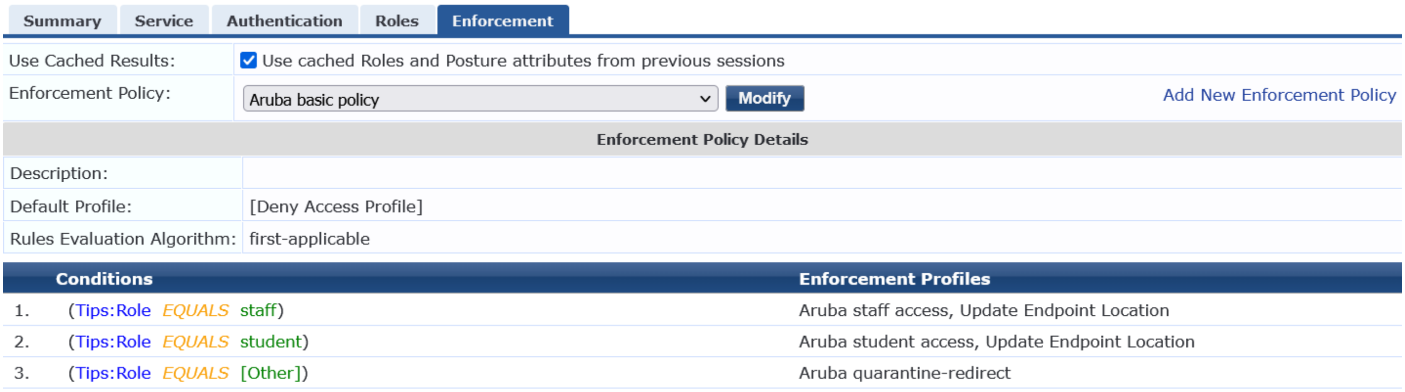


Role Mapping Policy: basic dot1x

Role Mapping Policy Details

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

	Conditions	Role
1.	(Authorization:AD1:memberOf CONTAINS staff)	staff
2.	(Authorization:AD1:memberOf CONTAINS student)	student



Use Cached Results:	☑ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	Aruba basic policy

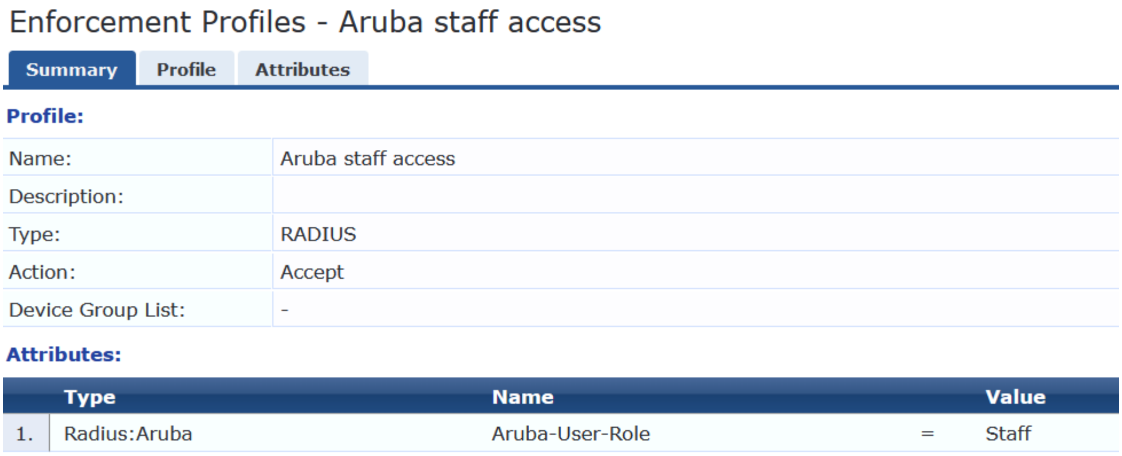
Enforcement Policy Details

Description:	
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Role *EQUALS* staff)	Aruba staff access, Update Endpoint Location
2.	(Tips:Role *EQUALS* student)	Aruba student access, Update Endpoint Location
3.	(Tips:Role *EQUALS* [Other])	Aruba quarantine-redirect

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

Aruba staff access,	RADIUS
Aruba student access,	RADIUS
Aruba quarantine-redirect	RADIUS
Update Endpoint Location	Post_Authentication



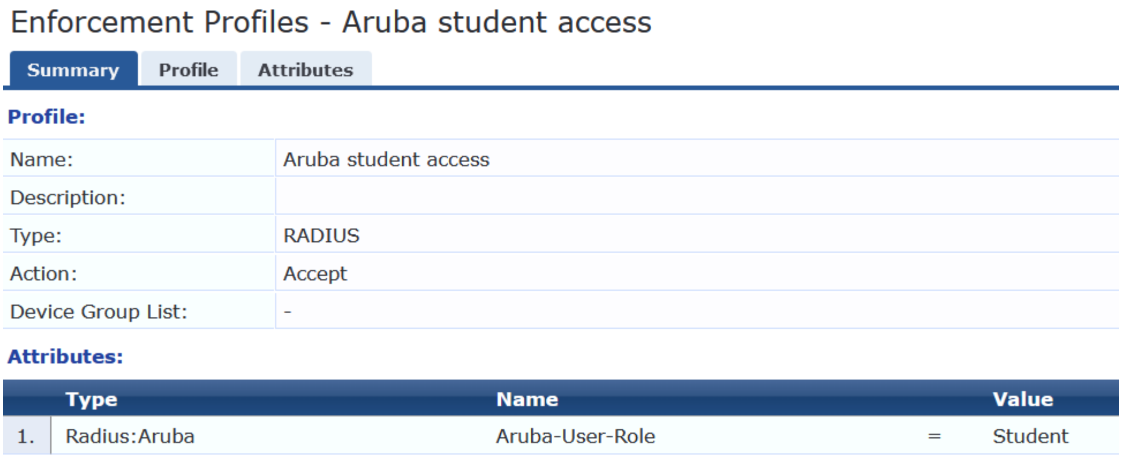
Enforcement Profiles - Aruba staff access

Profile:

Name:	Aruba staff access
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

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



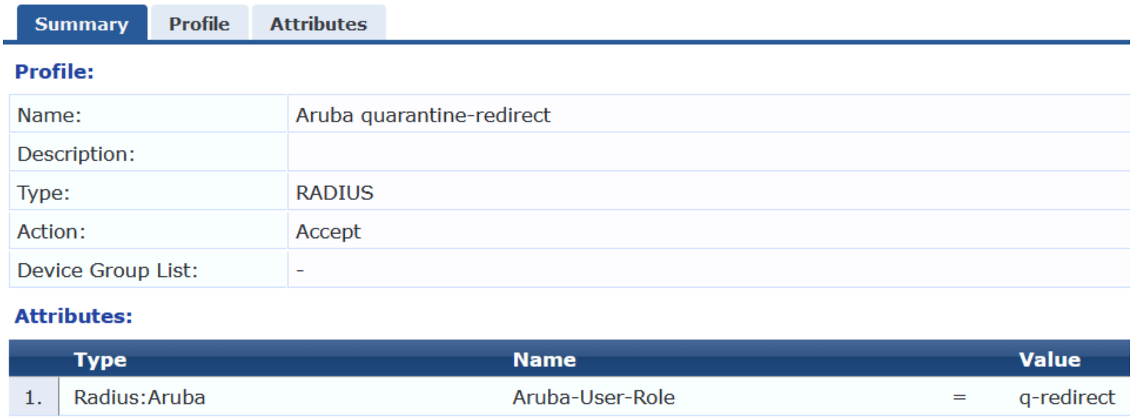
Enforcement Profiles - Aruba student access

Profile:

Name:	Aruba student access
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

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



Profile:

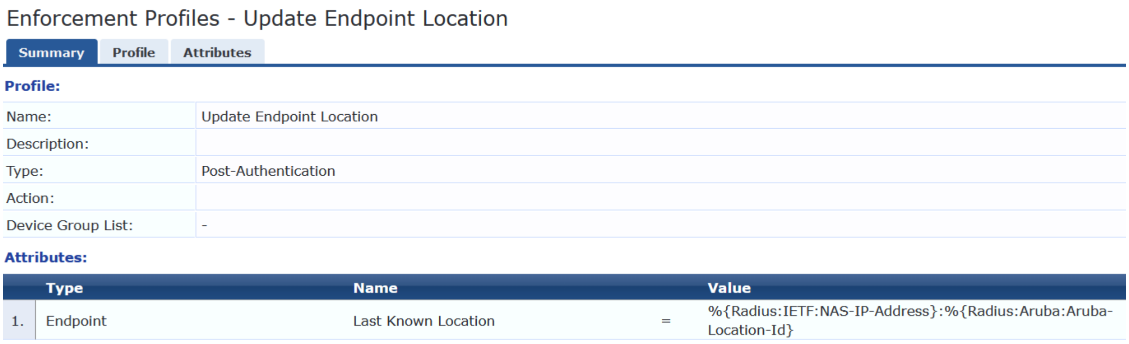
Name:	Aruba quarantine-redirect
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

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

We are using the following enforcement profile to write the location/name of the AP that the clients connect to the client's endpoint information.

This is one way to track a laptop through campus so that one could correlate security footage to establish the where abouts of the clients. So we could add the Radius:Aruba:Aruba-Location-Id to the endpoint repository and then use Insight within ClearPass to create a which gives the timestamps of user authentication and AP IP address and AP names.


Enforcement Profiles - Update Endpoint Location

Profile:

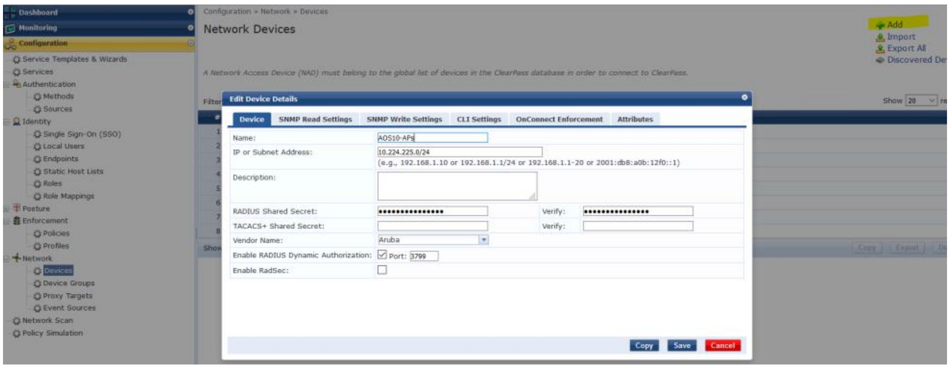
Name:	Update Endpoint Location
Description:	
Type:	Post-Authentication
Action:	
Device Group List:	-

Attributes:

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

5.2 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.



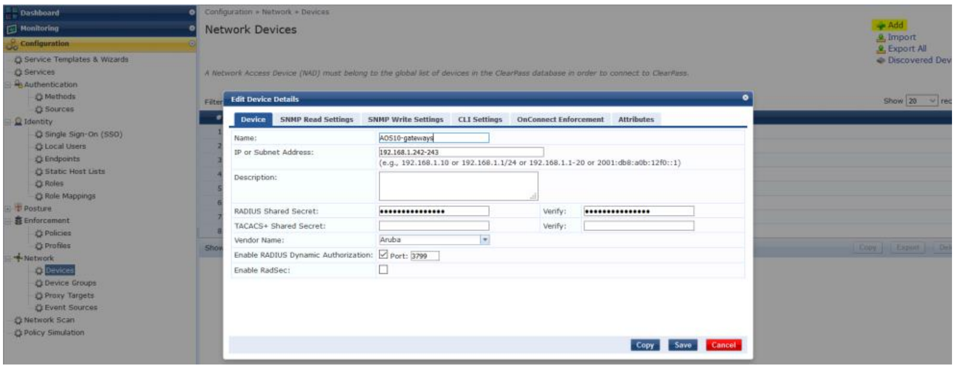
Configuration » Network » Devices

Network Devices

A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.

Edit Device Details

Name:	AOS10-APs		
IP or Subnet Address:	10.224.225.0/24 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20 or 2001:db8:a0b:12f0::1)		
Description:			
RADIUS Shared Secret:	••••••••••••••••	Verify:	••••••••••••••••
TACACS+ Shared Secret:		Verify:	
Vendor Name:	Aruba		
Enable RADIUS Dynamic Authorization:	☑ Port: 3799		
Enable RadSec:	□		



Configuration » Network » Devices

Network Devices

A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.

Edit Device Details

Name:	AOS10-gateways		
IP or Subnet Address:	192.168.1.242-243 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20 or 2001:db8:a0b:12f0::1)		
Description:			
RADIUS Shared Secret:	••••••••••••••••	Verify:	••••••••••••••••
TACACS+ Shared Secret:		Verify:	
Vendor Name:	Aruba		
Enable RADIUS Dynamic Authorization:	☑ Port: 3799		
Enable RadSec:	□		