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 Mode Wireless Configuration 25

6.2 Tunnelled Mode Wireless dot1x Testing 27

6.3 Bridge Mode Wireless Configuration 31

6.4 ClearPass Service Modifications 34

6.5 Bridge Mode Wireless dot1x Testing 36

6.6 Mixed Mode Wireless Configuration 38

6.7 ClearPass Service Modifications 43

6.8 Mixed Mode Wireless dot1x Testing 44

7 RF Monitoring 47

8 Guest Access Configuration 53

8.1 Guest Wireless Configuration 53

8.2 ClearPass Guest policy Configuration 57

8.3 ClearPass Guest Portal Configuration 62

8.4 Guest Testing 66

1.1 Revision History

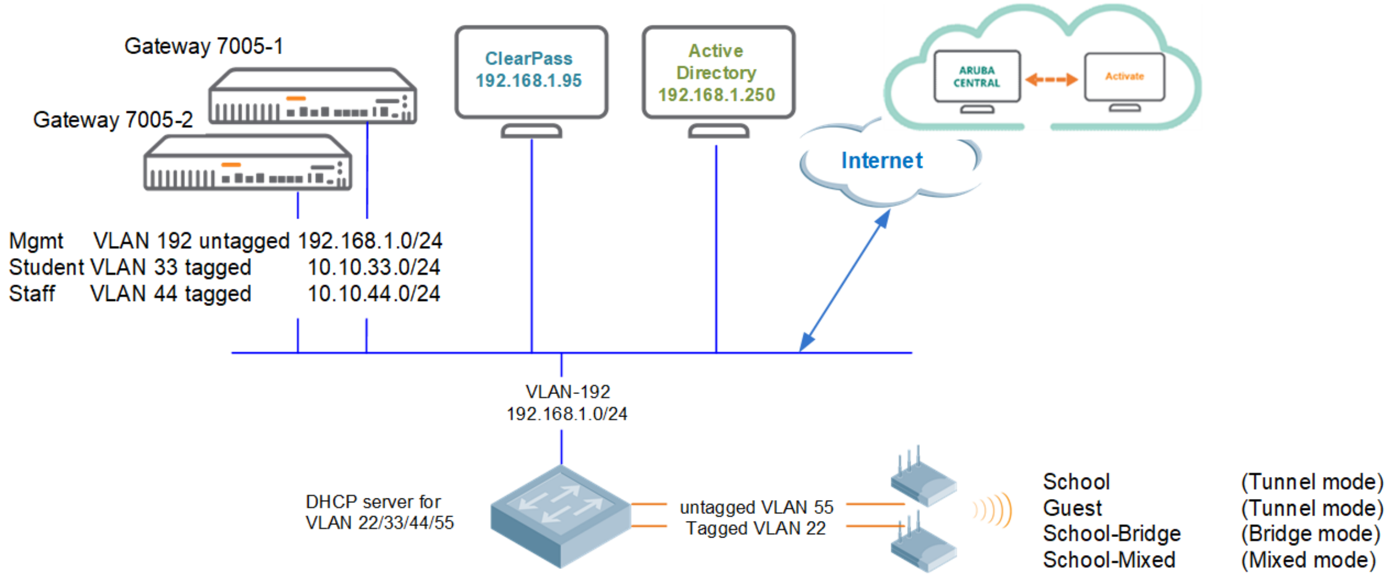
DATE	VERSION	EDITOR	CHANGES
15 Mar 2021	0.1	Ariya Parsamanesh	Initial creation
22 May 2021	0.2	Ariya Parsamanesh	Added the ClearPass guest operator login
04 Jul 2021	0.3	Ariya Parsamanesh	Added the Monitoring section
12 Jul 2021	0.4	Ariya Parsamanesh	Added the bridge and mixed mode WLANs

2 Demo Topology

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

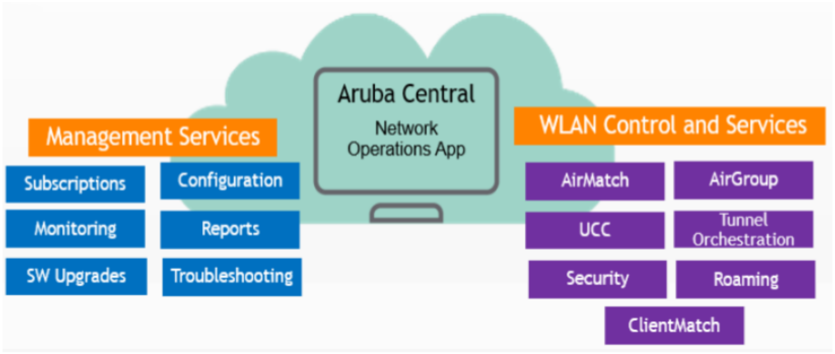
Note that APs in AOS10 support bridged, tunnelled and mix mode wireless LANs (WLAN) however in this technote we'll be deploying tunnelled mode WLANs. We'll also demonstrate the gateway clustering with AOS10.

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



With AOS10, the campus architecture consists of two layers:

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



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

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

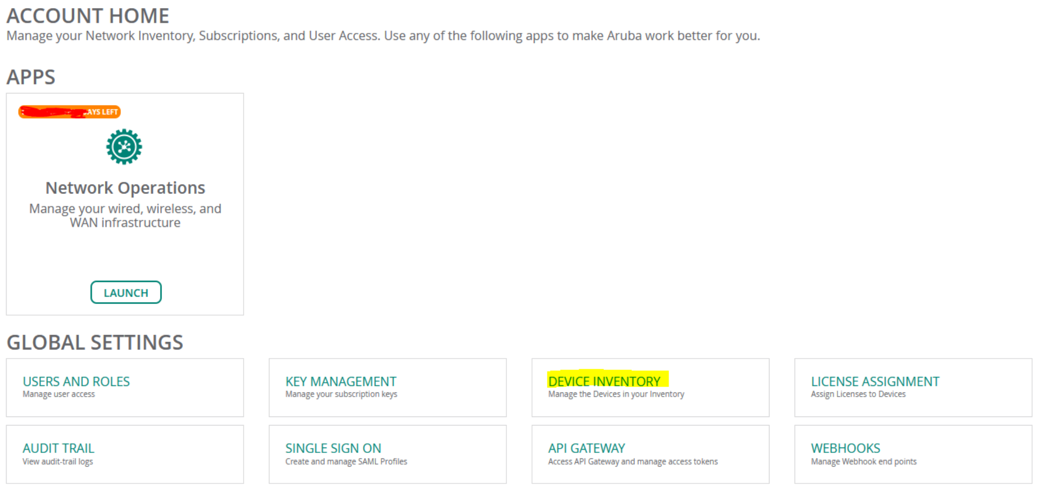
https://www.arubanetworks.com/techdocs/AOS10X_OLH/Content/overview/architecture-overview.htm

3 Aruba Central Account

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

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

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



ACCOUNT HOME

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

APPS

[redacted]AYS LEFT

Network Operations

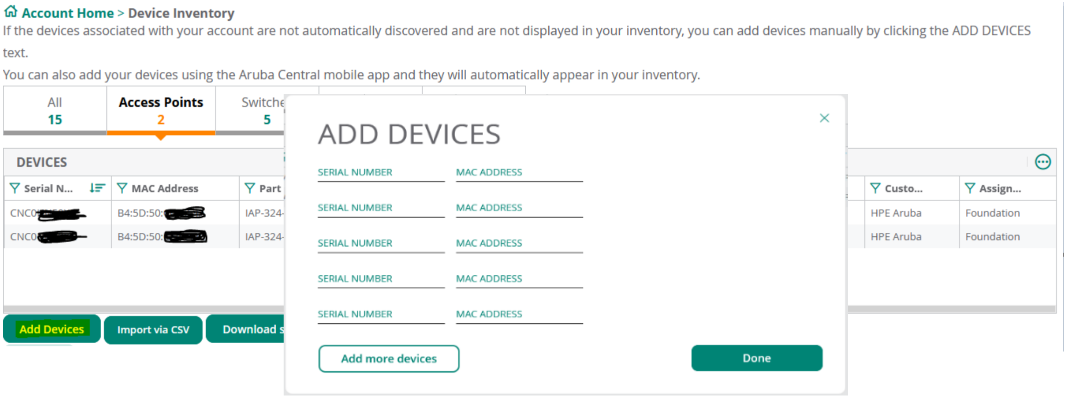
Manage your wired, wireless, and WAN infrastructure

LAUNCH

GLOBAL SETTINGS

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

All 15 | Access Points 2 | Switche 5

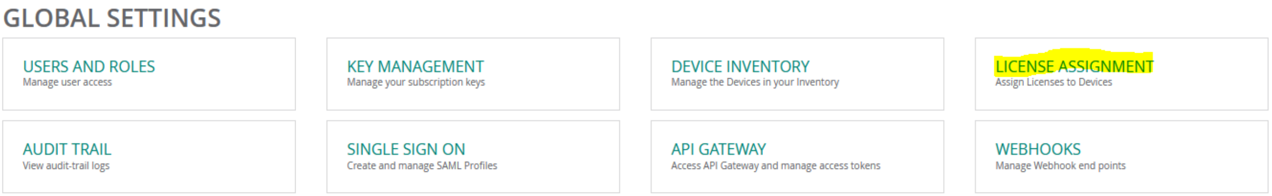
DEVICES

Serial N...	MAC Address	Part	Custo...	Assign...
CNC0[redacted]	B4:5D:50:[redacted]	IAP-324-	HPE Aruba	Foundation
CNC0[redacted]	B4:5D:50:[redacted]	IAP-324-	HPE Aruba	Foundation

ADD DEVICES

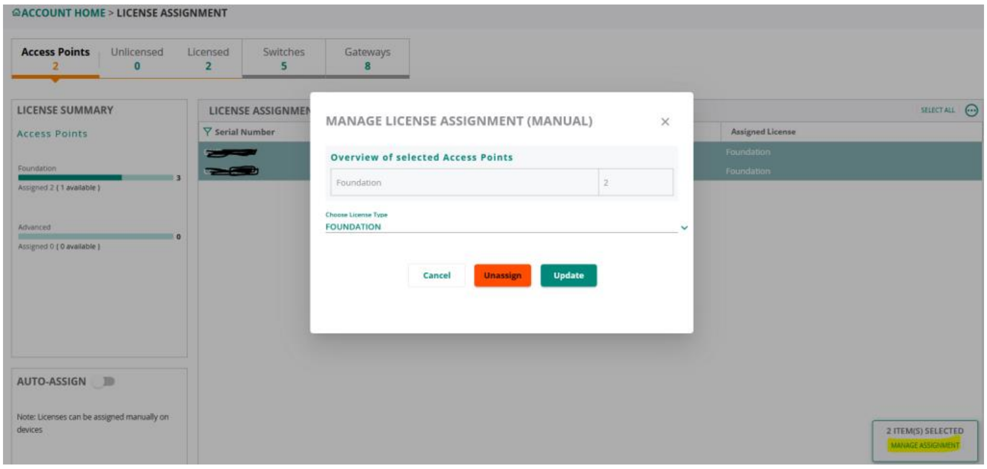
SERIAL NUMBER	MAC ADDRESS
SERIAL NUMBER	MAC ADDRESS
SERIAL NUMBER	MAC ADDRESS
SERIAL NUMBER	MAC ADDRESS
SERIAL NUMBER	MAC ADDRESS

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

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



ACCOUNT HOME > LICENSE ASSIGNMENT

LICENSE SUMMARY

Access Points

Foundation 3
Assigned 2 (1 available)

Advanced 0
Assigned 0 (0 available)

AUTO-ASSIGN

Note: Licenses can be assigned manually on devices

LICENSE ASSIGNMENT

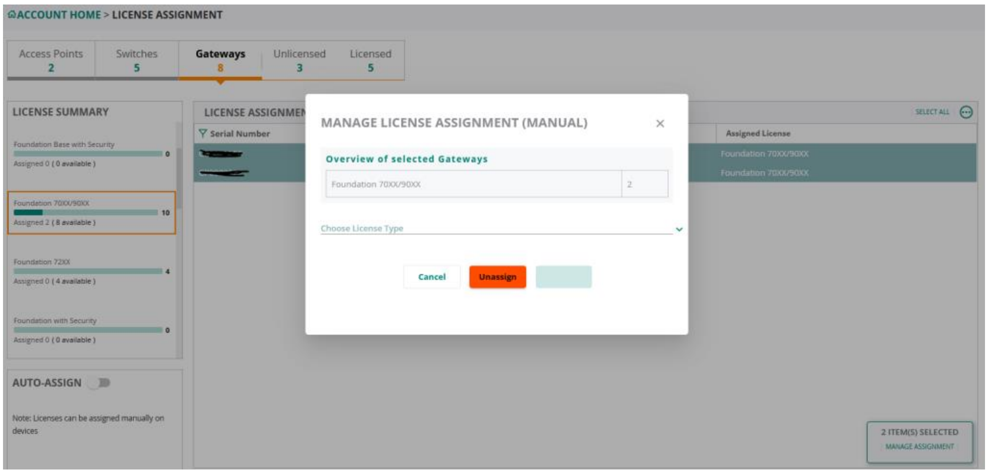
Serial Number	Assigned License
[redacted]	Foundation
[redacted]	Foundation

MANAGE LICENSE ASSIGNMENT (MANUAL)

Overview of selected Access Points

Foundation	2

Choose License Type: FOUNDATION



ACCOUNT HOME > LICENSE ASSIGNMENT

LICENSE SUMMARY

Foundation Base with Security 0
Assigned 0 (0 available)

Foundation 70XX/90XX 10
Assigned 2 (8 available)

Foundation 72XX 4
Assigned 0 (4 available)

Foundation with Security 0
Assigned 0 (0 available)

AUTO-ASSIGN

Note: Licenses can be assigned manually on devices

LICENSE ASSIGNMENT

Serial Number	Assigned License
[redacted]	Foundation 70XX/90XX
[redacted]	Foundation 70XX/90XX

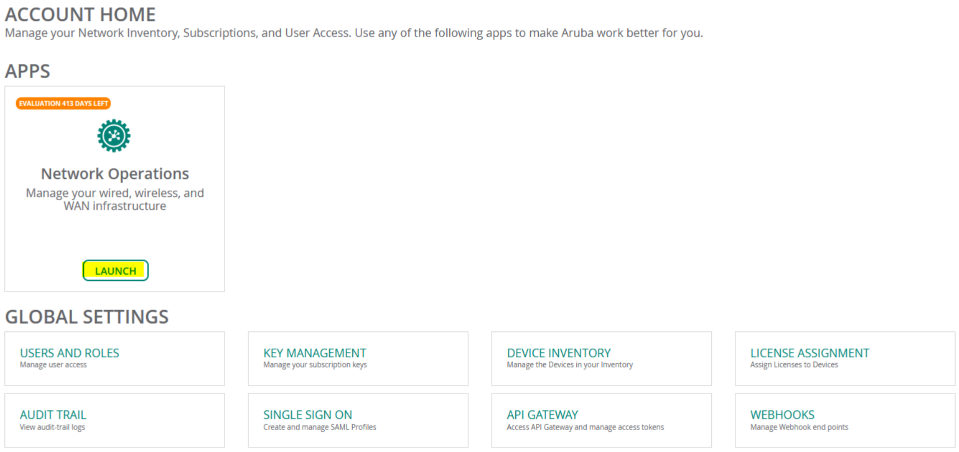
MANAGE LICENSE ASSIGNMENT (MANUAL)

Overview of selected Gateways

Foundation 70XX/90XX	2

Choose License Type

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

GLOBAL SETTINGS

USERS AND ROLES
Manage user access

KEY MANAGEMENT
Manage your subscription keys

DEVICE INVENTORY
Manage the Devices in your Inventory

LICENSE ASSIGNMENT
Assign Licenses to Devices

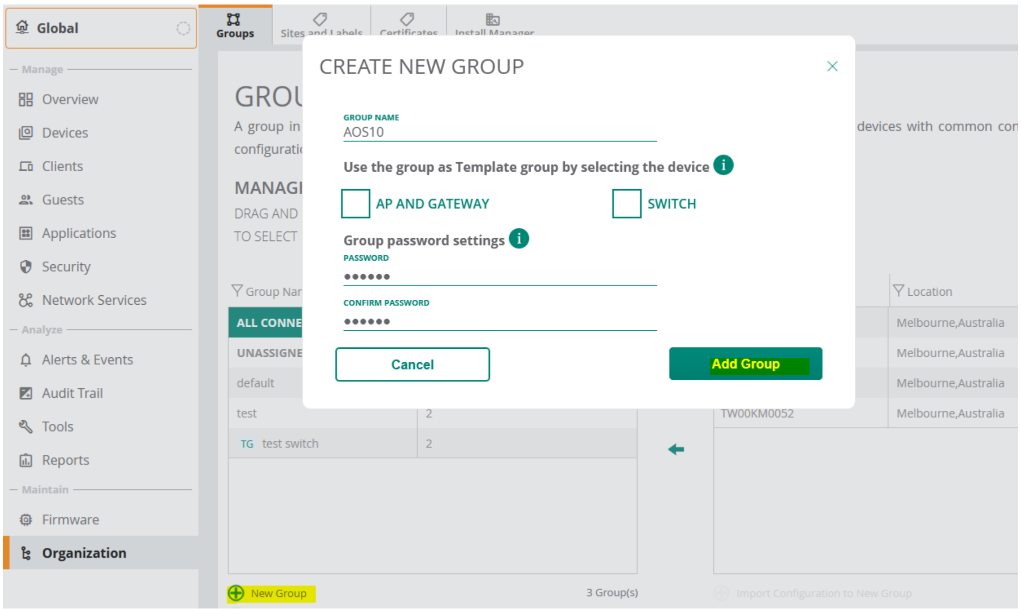
AUDIT TRAIL
View audit-trail logs

SINGLE SIGN ON
Create and manage SAML Profiles

API GATEWAY
Access API Gateway and manage access tokens

WEBHOOKS
Manage Webhook end points

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



CREATE NEW GROUP

GROUP NAME: AOS10

Use the group as Template group by selecting the device

□ AP AND GATEWAY □ SWITCH

Group password settings

PASSWORD: ●●●●●●

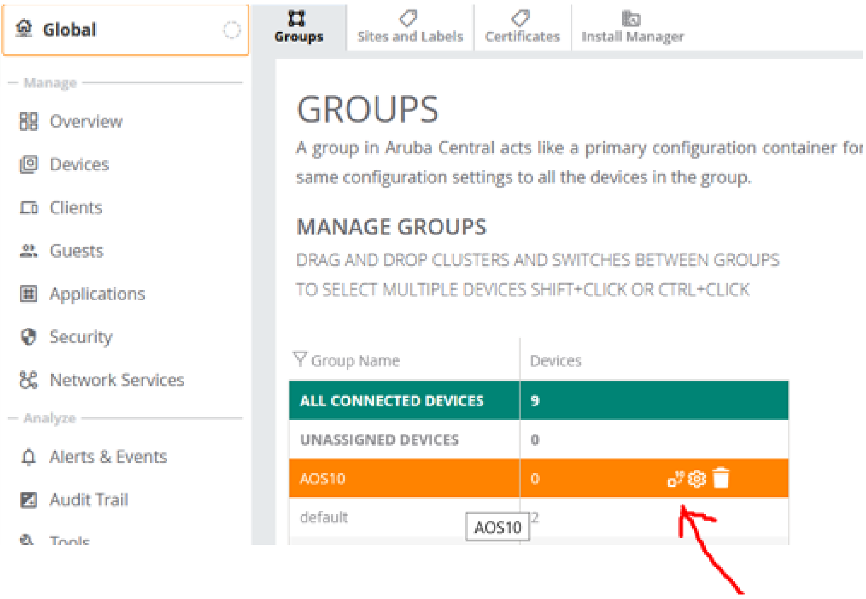
CONFIRM PASSWORD: ●●●●●●

Cancel | Add Group

Group Name	Devices
ALL CONNE	
UNASSIGNE	
default	
test	2
TG test switch	2

	Location
	Melbourne,Australia
	Melbourne,Australia
	Melbourne,Australia
TW00KM0052	Melbourne,Australia

Then you need to convert the group to AOS10.



GROUPS

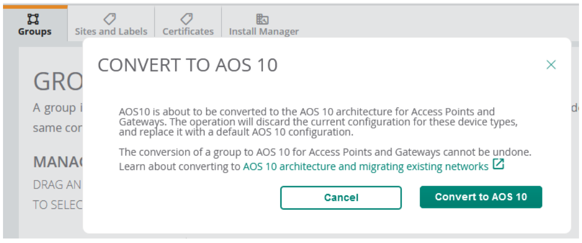
A group in Aruba Central acts like a primary configuration container for same configuration settings to all the devices in the group.

MANAGE GROUPS

DRAG AND DROP CLUSTERS AND SWITCHES BETWEEN GROUPS

TO SELECT MULTIPLE DEVICES SHIFT+CLICK OR CTRL+CLICK

Group Name	Devices
ALL CONNECTED DEVICES	9
UNASSIGNED DEVICES	0
AOS10	0
default	2



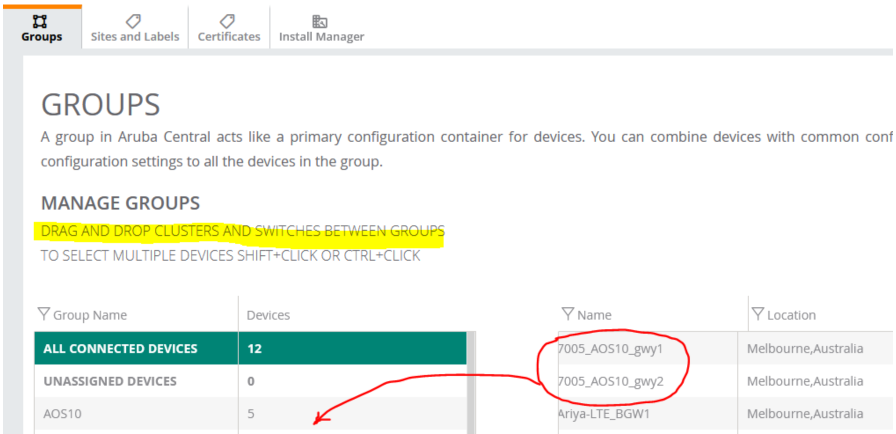
CONVERT TO AOS 10

AOS10 is about to be converted to the AOS 10 architecture for Access Points and Gateways. The operation will discard the current configuration for these device types, and replace it with a default AOS 10 configuration.

The conversion of a group to AOS 10 for Access Points and Gateways cannot be undone. Learn about converting to AOS 10 architecture and migrating existing networks

Cancel | Convert to AOS 10

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



GROUPS

A group in Aruba Central acts like a primary configuration container for devices. You can combine devices with common conf configuration settings to all the devices in the group.

MANAGE GROUPS

DRAG AND DROP CLUSTERS AND SWITCHES BETWEEN GROUPS

TO SELECT MULTIPLE DEVICES SHIFT+CLICK OR CTRL+CLICK

Group Name	Devices
ALL CONNECTED DEVICES	12
UNASSIGNED DEVICES	0
AOS10	5

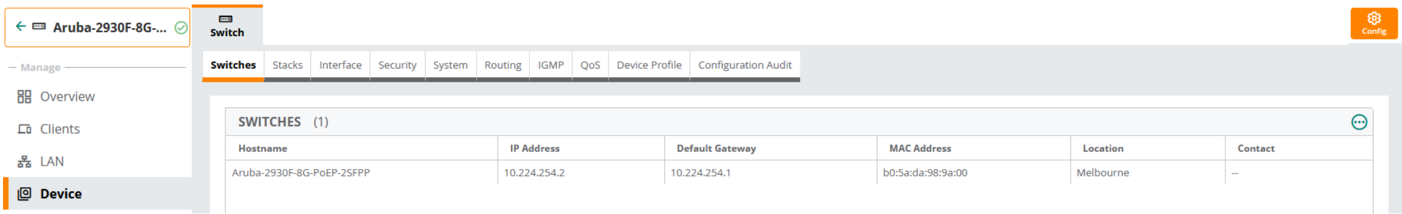
Name	Location
7005_AOS10_gwy1	Melbourne,Australia
7005_AOS10_gwy2	Melbourne,Australia
Ariya-LTE_BGW1	Melbourne,Australia

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.

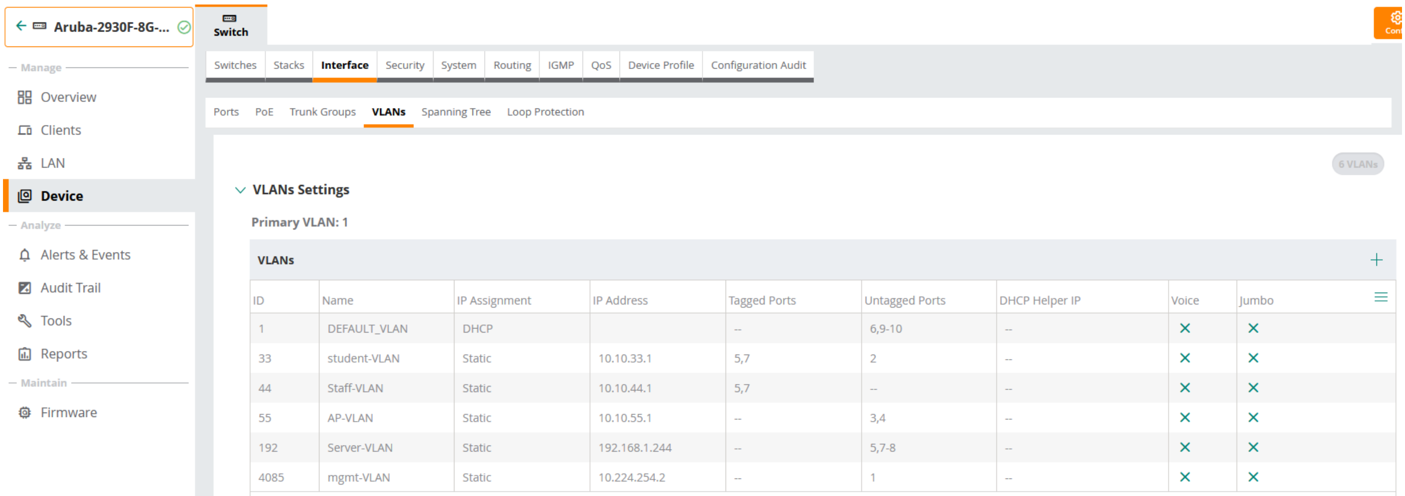
4.1 LAN Switch Configuration

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.



SWITCHES (1)

Hostname	IP Address	Default Gateway	MAC Address	Location	Contact
Aruba-2930F-8G-PoEP-2SFPP	10.224.254.2	10.224.254.1	b0:5a:da:98:9a:00	Melbourne	--



VLANs Settings

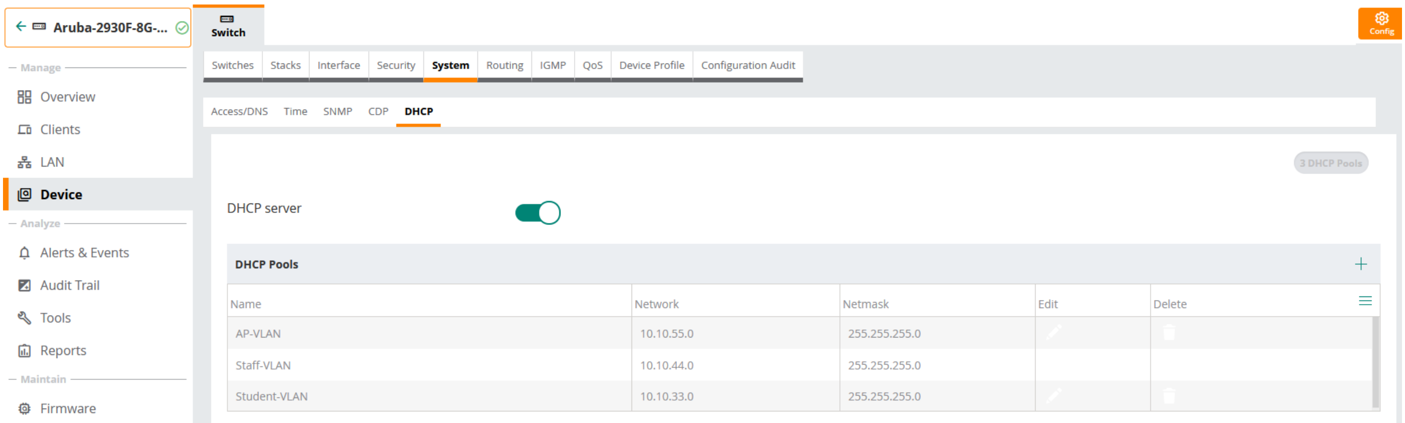
Primary VLAN: 1

VLANs

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.



DHCP server ●

DHCP Pools

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"
```

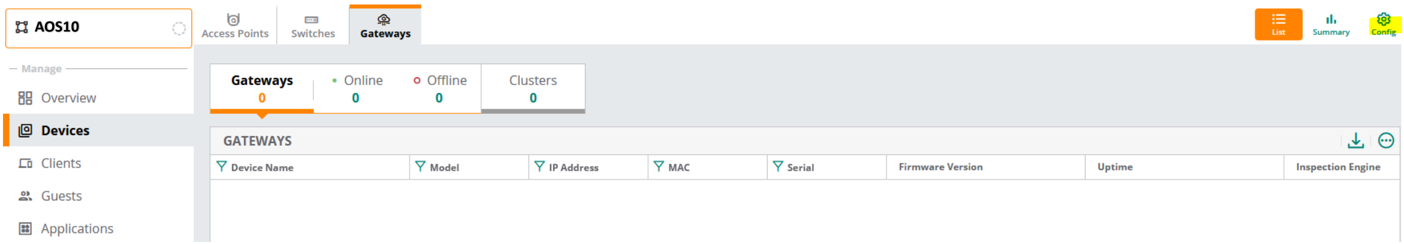
```
   default-router "10.10.44.1"
   dns-server "1.1.1.1"
   lease 00:04:00
   network 10.10.44.0 255.255.255.0
   range 10.10.44.50 10.10.44.59
   exit
dhcp-server pool "Student-VLAN"
   default-router "10.10.33.1"
   dns-server "1.1.1.1"
   lease 00:04:00
   network 10.10.33.0 255.255.255.0
   range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

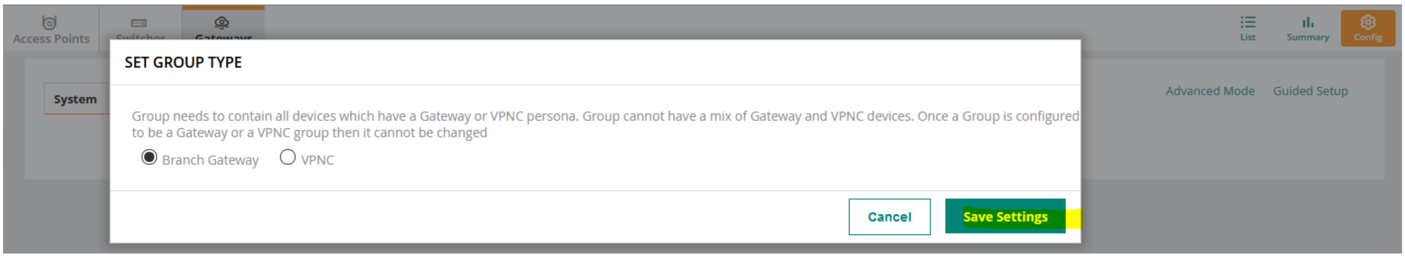
We'll be using Aruba 7005 gateways which have 4x ports.



Gateways	Online	Offline	Clusters
0	0	0	0

GATEWAYS

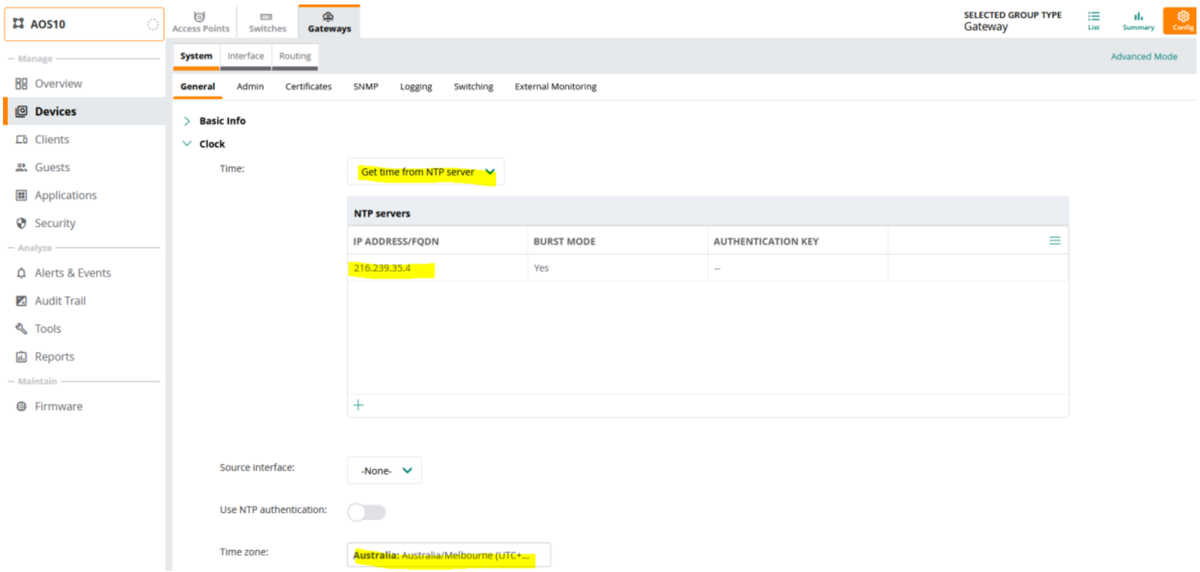
Device Name	Model	IP Address	MAC	Serial	Firmware Version	Uptime	Inspection Engine



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



Time: Get time from NTP server

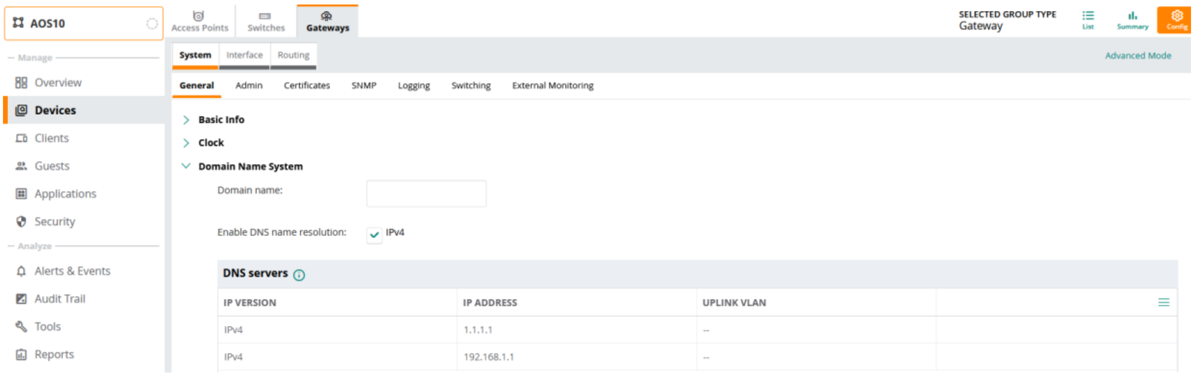
NTP servers

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

Source interface: -None-

Use NTP authentication: ○

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



Basic Info

Clock

Domain Name System

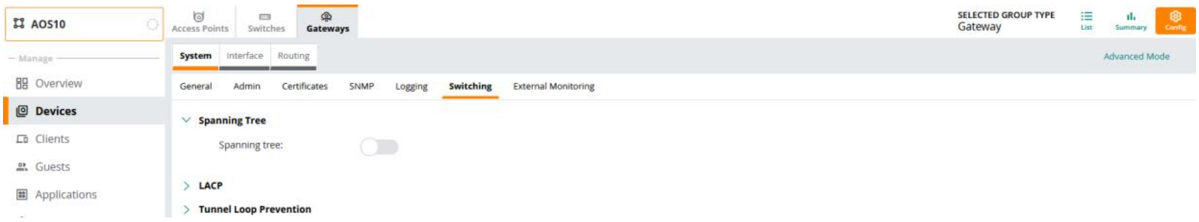
Domain name:

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



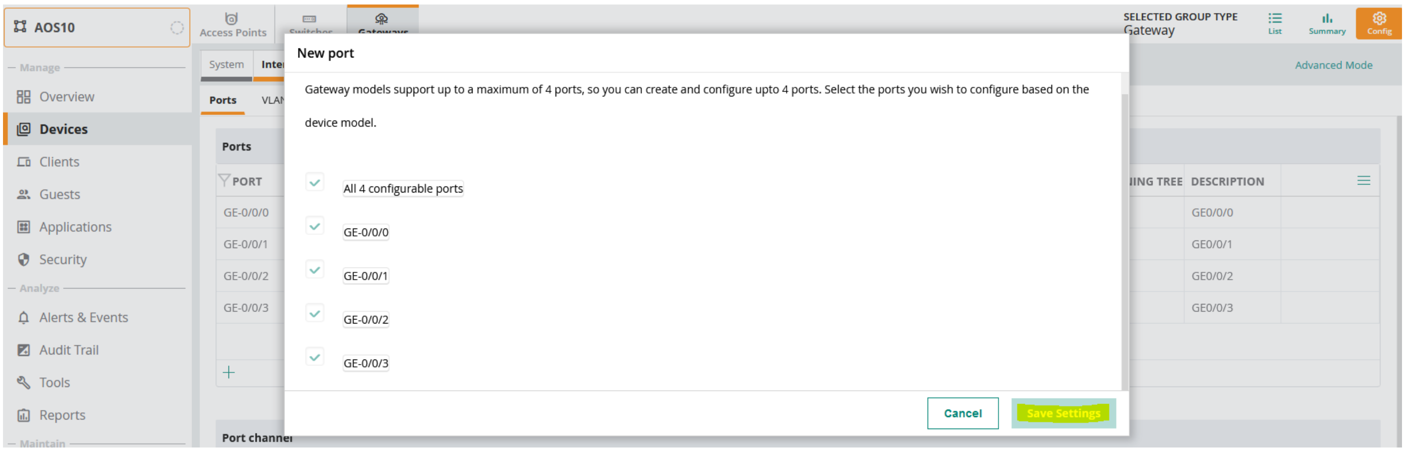
Spanning Tree

Spanning tree: ○

LACP

Tunnel Loop Prevention

Adding the relevant ports for Aruba 7005 gateway.



PORT	...ING TREE	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

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

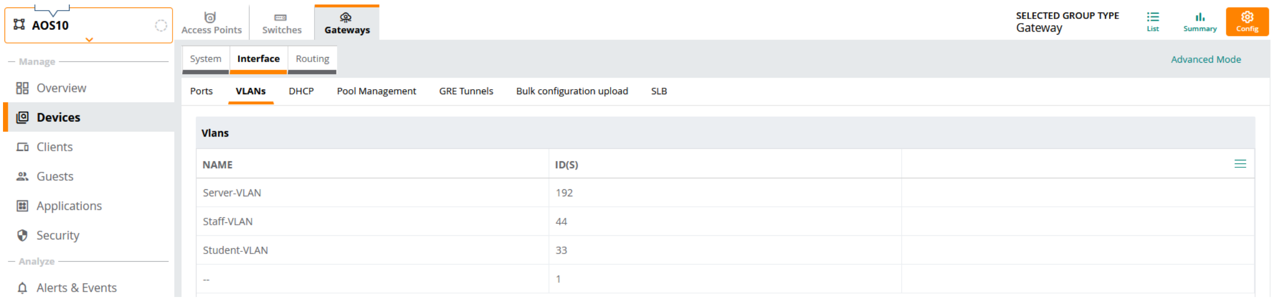
✓ GE-0/0/1

✓ GE-0/0/2

✓ GE-0/0/3

Cancel | Save Settings

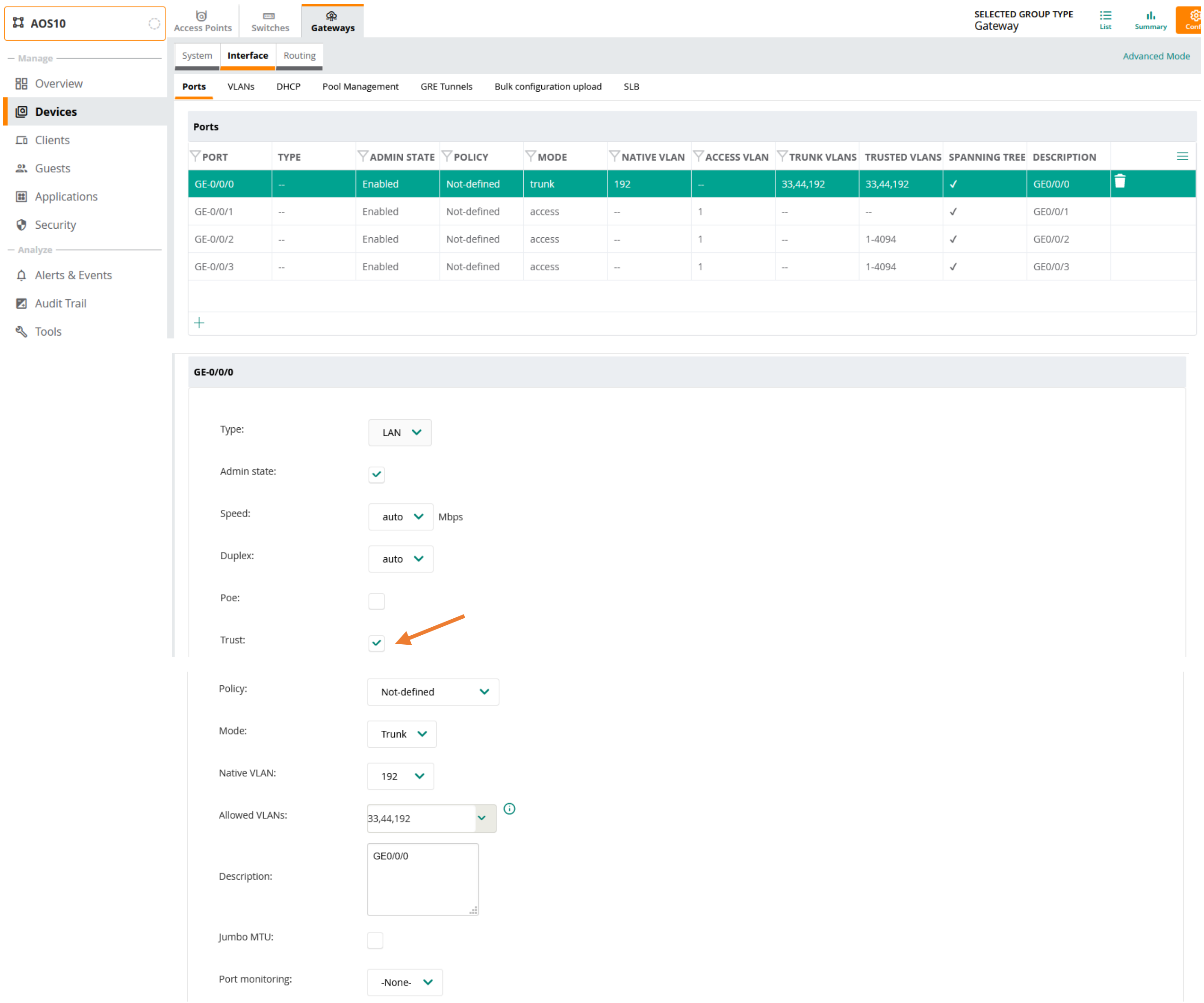
I am planning to sue interface 0/0/0 as my gateway uplink. This port needs to be in trunk mode and here we'll add the relevant VLANs.



Vlans

NAME	ID(S)
Server-VLAN	192
Staff-VLAN	44
Student-VLAN	33
--	1

Adding the VLANs to appropriate ports.



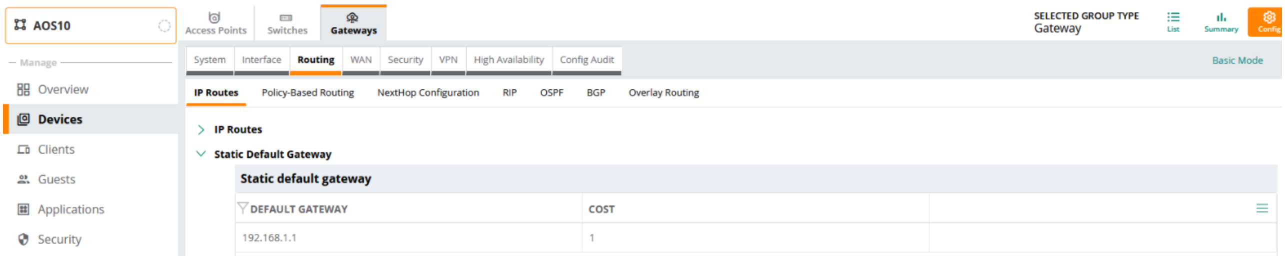
Ports

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-

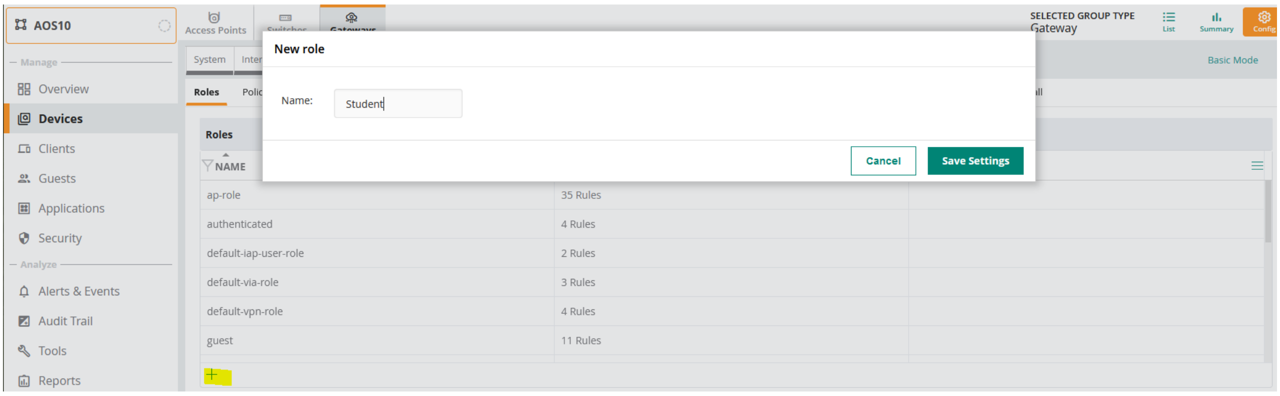
Adding the default route



Static default gateway

DEFAULT GATEWAY	COST
192.168.1.1	1

Adding the user roles by going to "security tab"

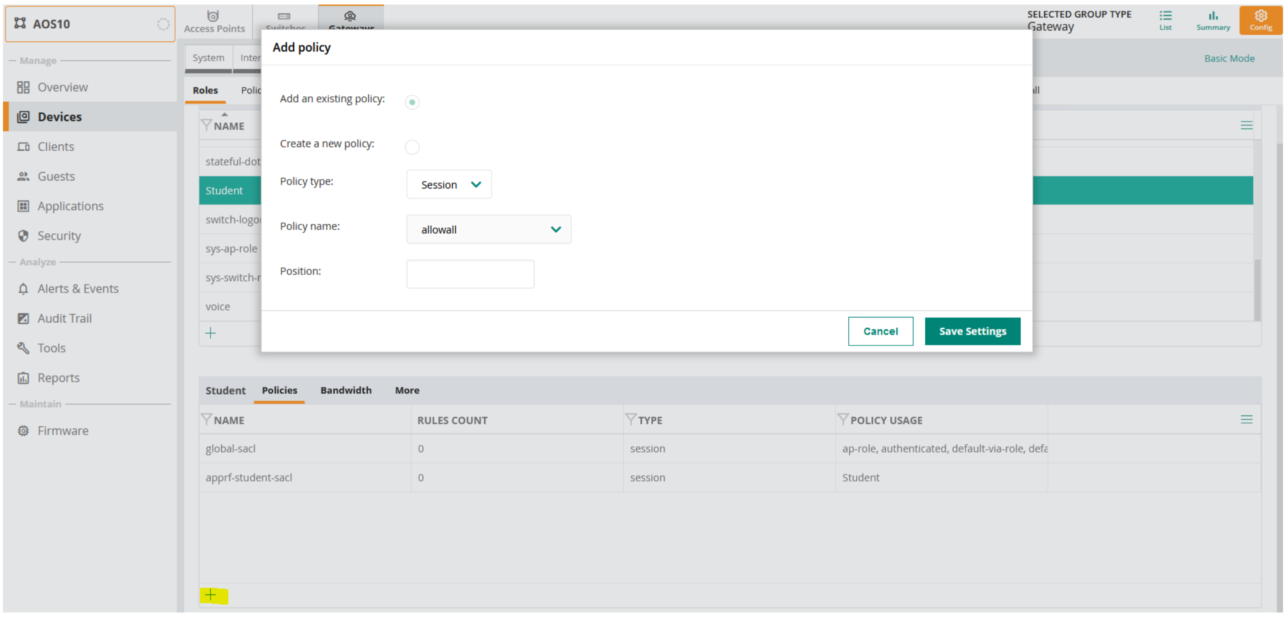


New role

Name: Student

Roles

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

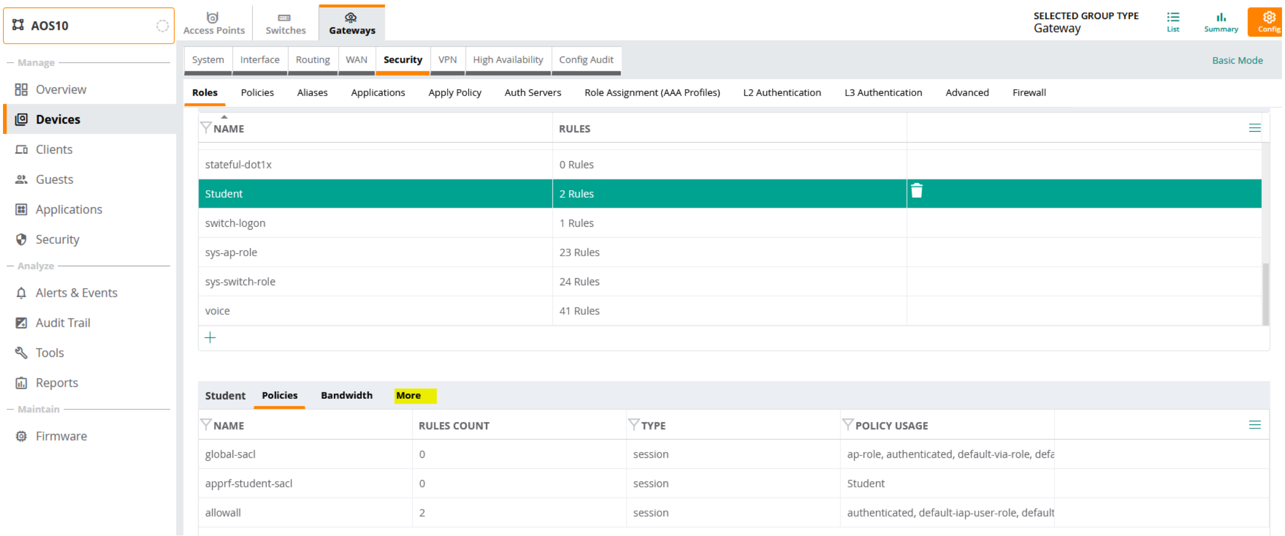
Policy name: allowall

Position:

Cancel | Save Settings

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

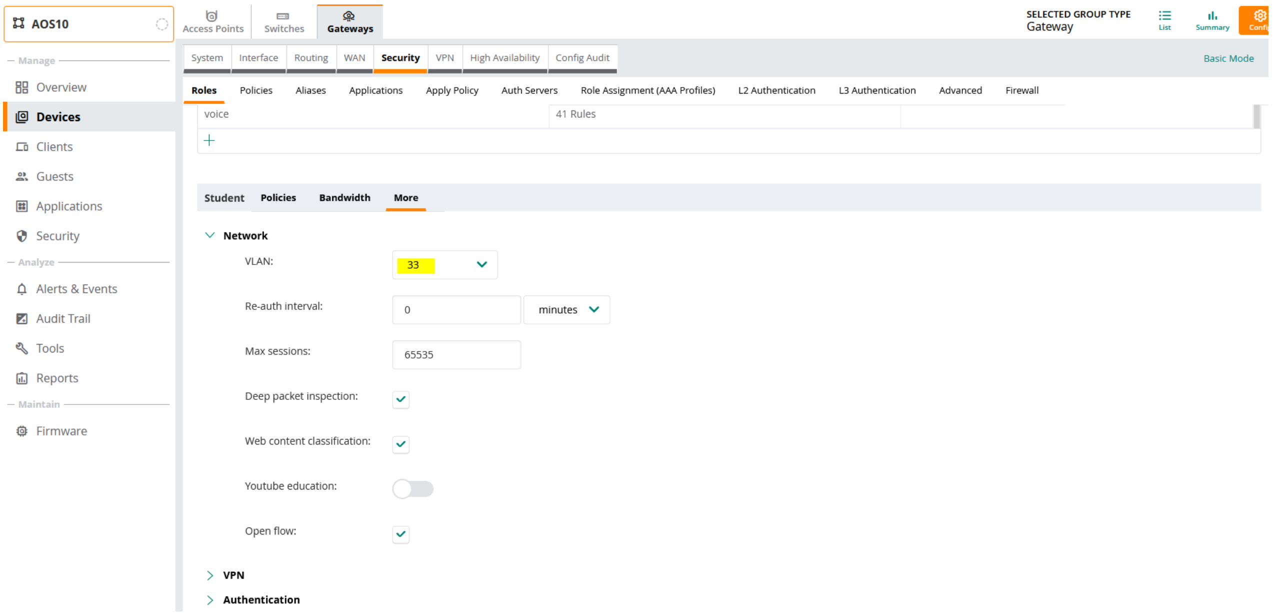
Here we’ll add the allow-all policy.



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

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.



Network

VLAN: 33

Re-auth interval: 0 minutes

Max sessions: 65535

Deep packet inspection: ✓

Web content classification: ✓

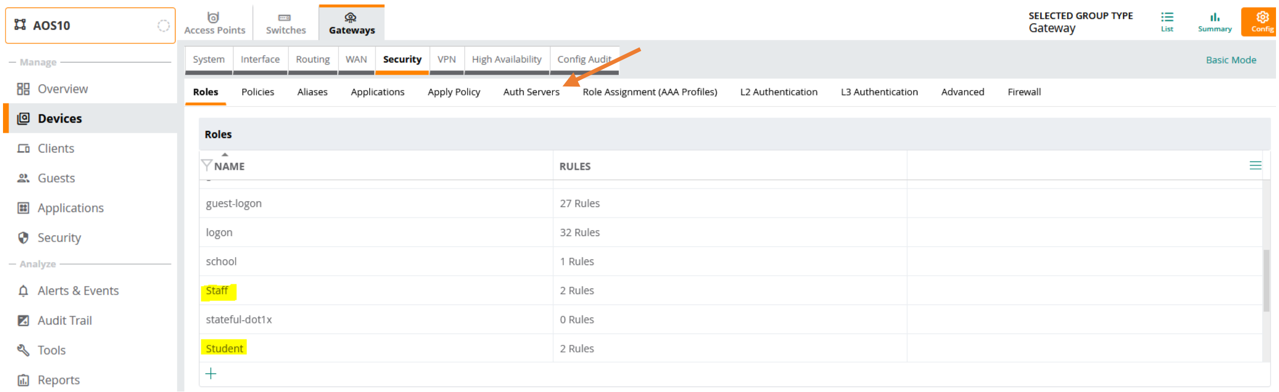
Youtube education: ○

Open flow: ✓

VPN

Authentication

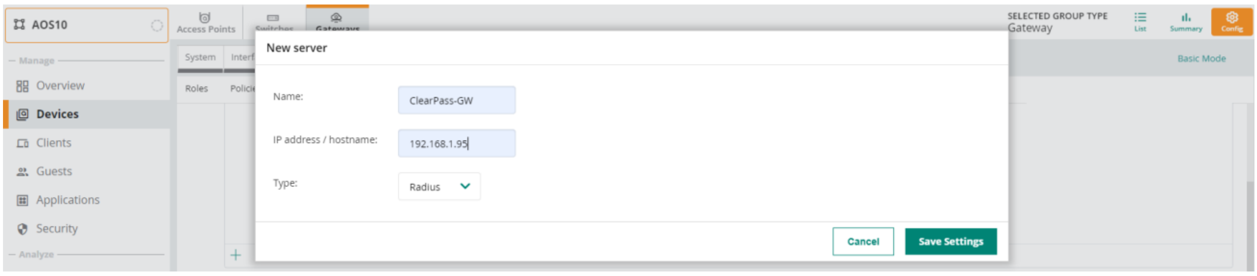
We'll create a new user role staff and as before, we'll add a allow-all policy and assign VLAN 44 to it.



Roles

NAME	RULES
guest-logon	27 Rules
logon	32 Rules
school	1 Rules
Staff	2 Rules
stateful-dot1x	0 Rules
Student	2 Rules

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



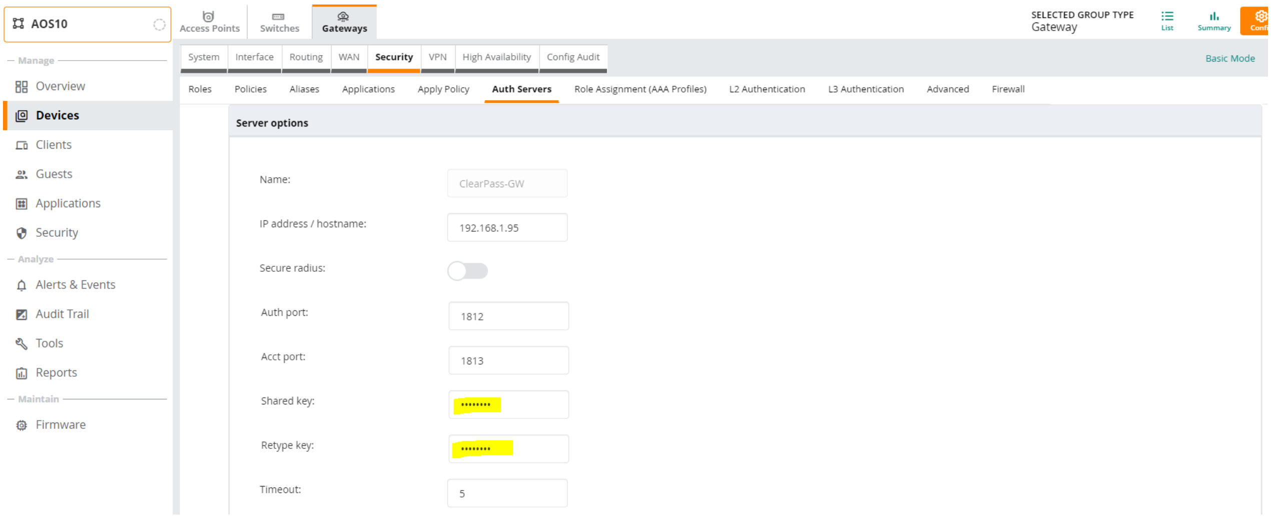
New server

Name: ClearPass-GW

IP address / hostname: 192.168.1.95

Type: Radius

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



Server options

Name: ClearPass-GW

IP address / hostname: 192.168.1.95

Secure radius:

Auth port: 1812

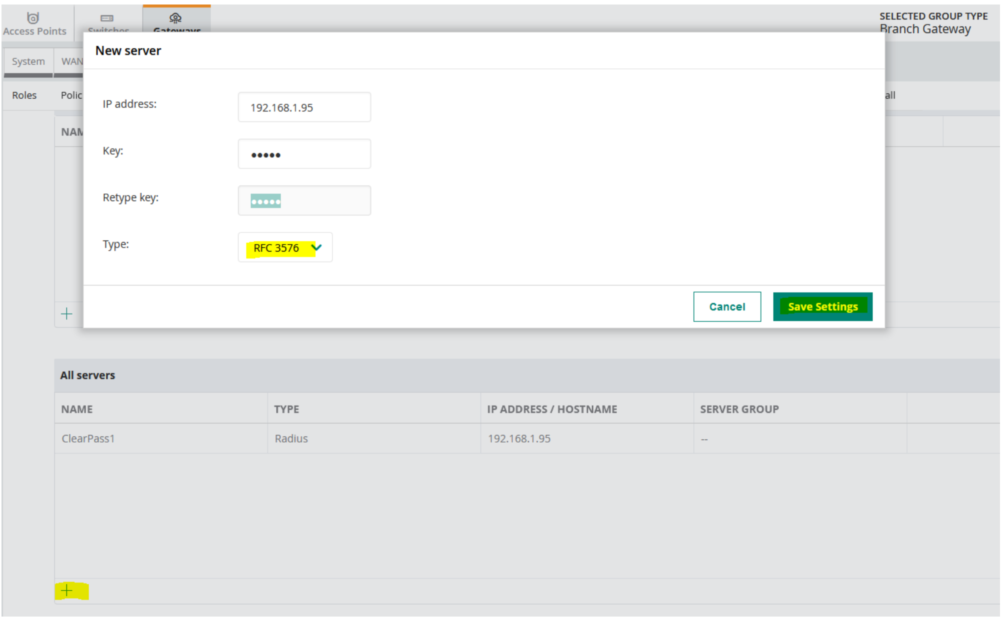
Acct port: 1813

Shared key: ••••••••

Retype key: ••••••••

Timeout: 5

And finally add a rfc3576 server for CoA.



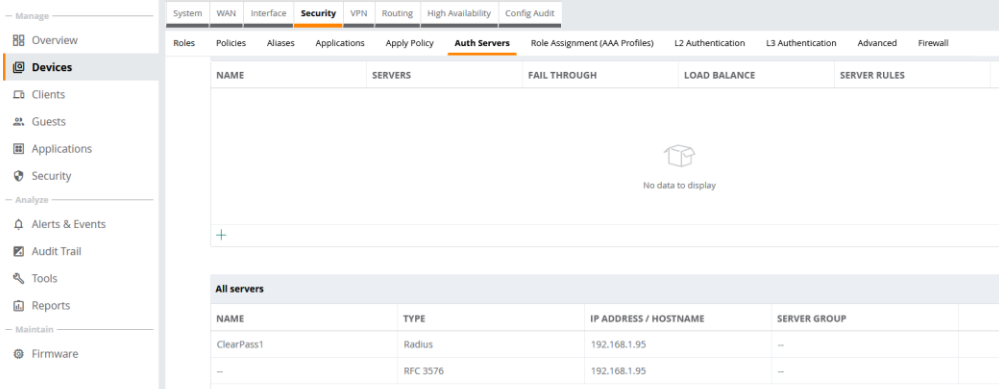
New server

IP address:	192.168.1.95
Key:	•••••
Retype key:	•••••
Type:	RFC 3576

All servers

NAME	TYPE	IP ADDRESS / HOSTNAME	SERVER GROUP
ClearPass1	Radius	192.168.1.95	--

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



NAME	SERVERS	FAIL THROUGH	LOAD BALANCE	SERVER RULES

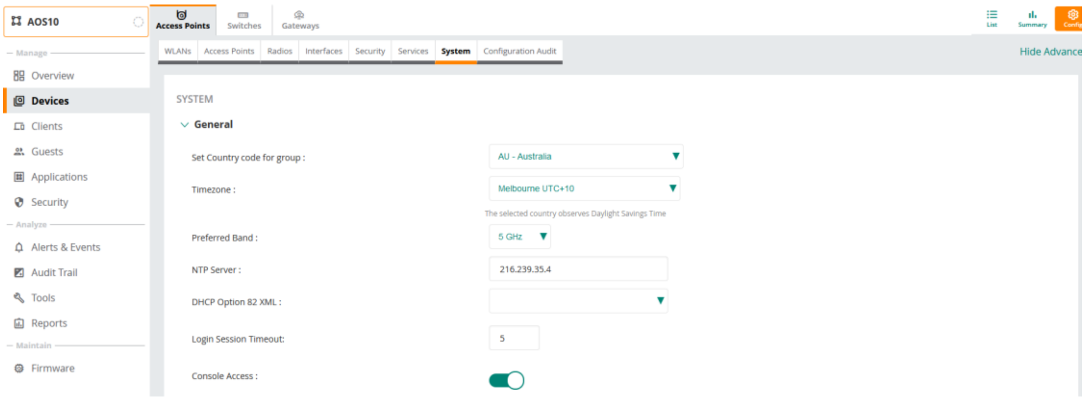
No data to display

All servers

NAME	TYPE	IP ADDRESS / HOSTNAME	SERVER GROUP
ClearPass1	Radius	192.168.1.95	--
--	RFC 3576	192.168.1.95	--

4.3 AP Configuration

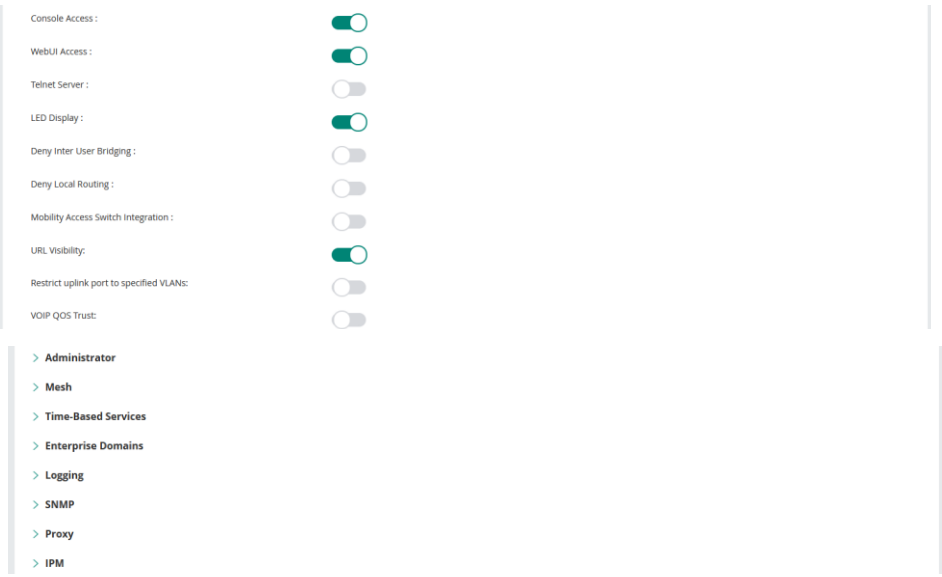
Here we'll go through the AP configuration. As always, we'll do the bulk of configuration at the group level.



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 : ☐

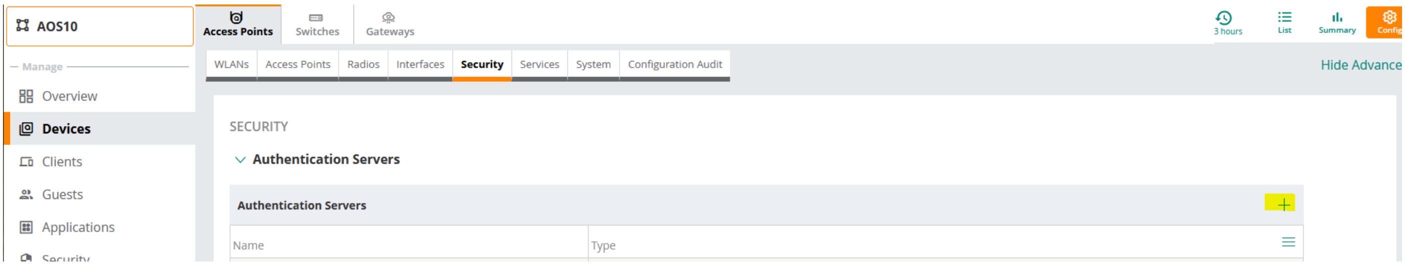
Deny Local Routing : ☐

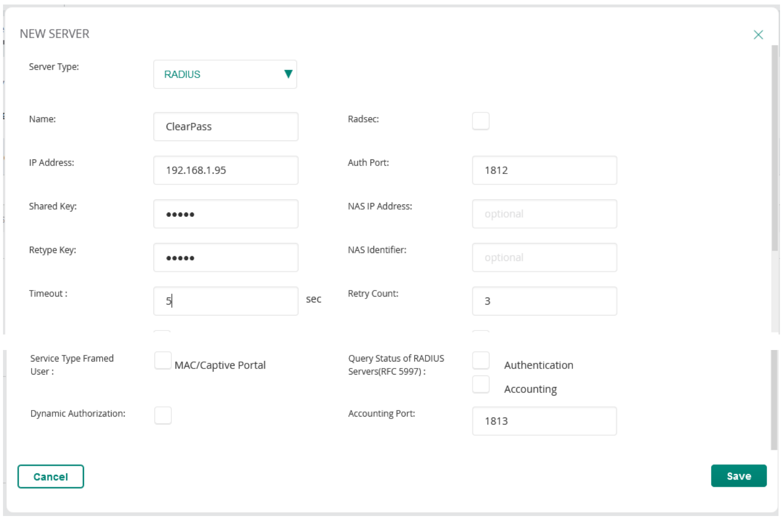
Mobility Access Switch Integration : ☐

URL Visibility: ☑

Restrict uplink port to specified VLANs: ☐

VOIP QOS Trust: ☐

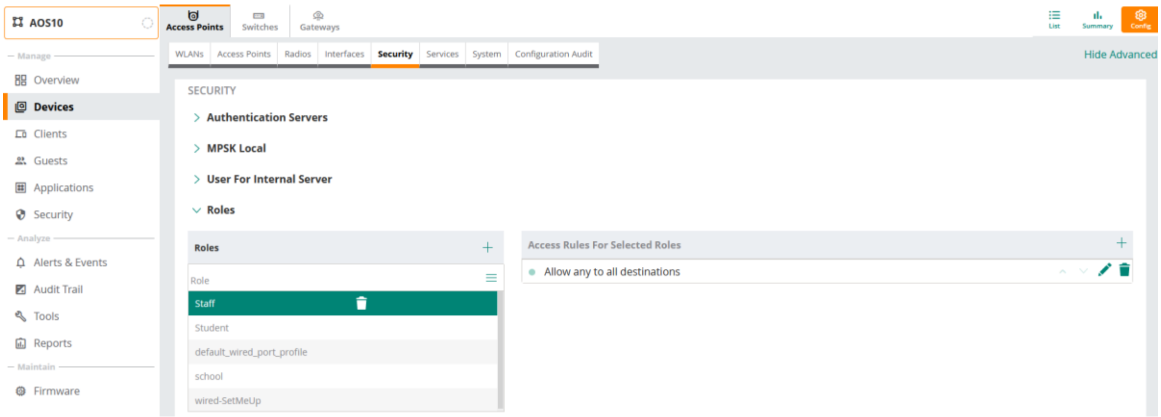




NEW SERVER

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

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



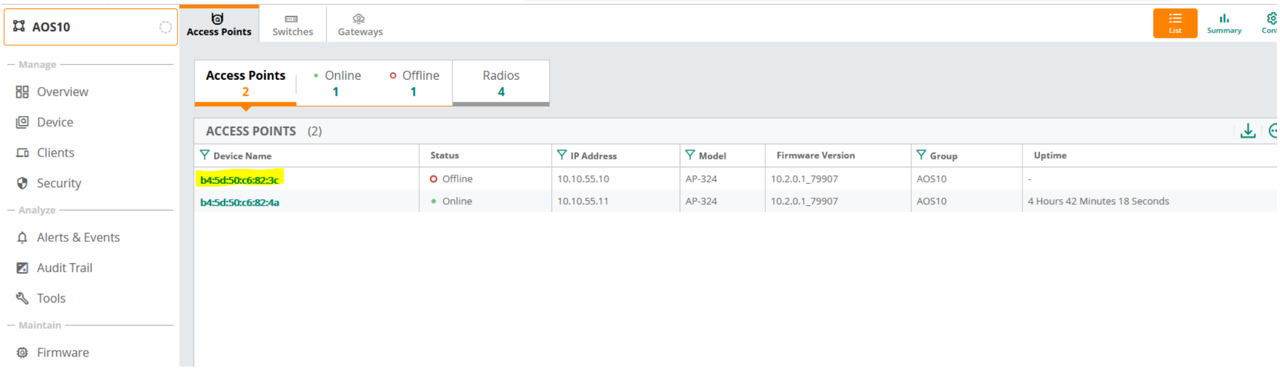
Role
Staff
Student
default_wired_port_profile
school
wired-SetMeUp

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

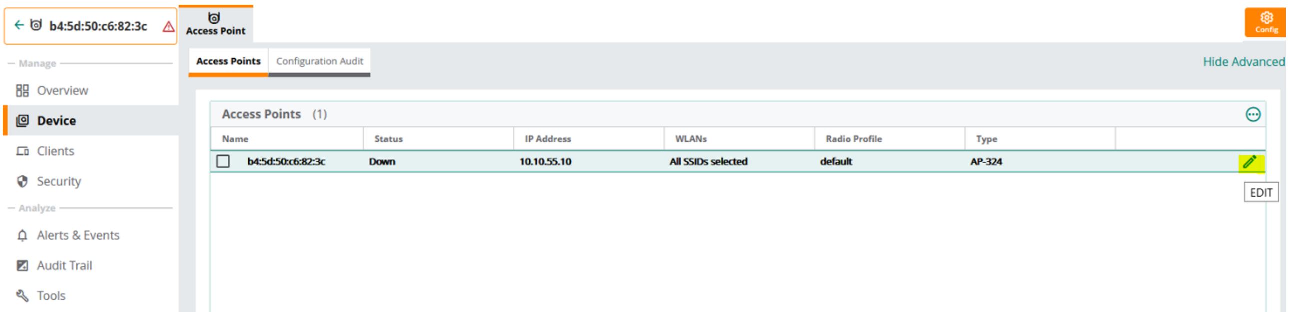
In most of the cases you'll go with DHCP based IP addresses, but in case you need to assign static IP addresses, it is done as shown below.



Access Points	Online	Offline	Radios
2	1	1	4

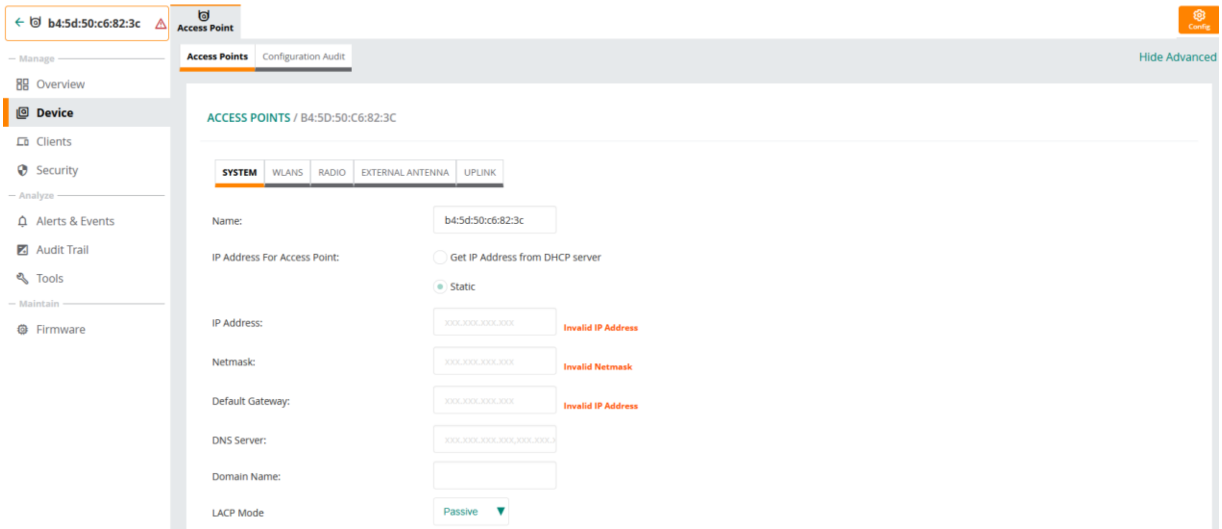
ACCESS POINTS (2)

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



Access Points (1)

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



ACCESS POINTS / B4:5D:50:C6:82:3C

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.x

Domain Name:

LACP Mode: Passive

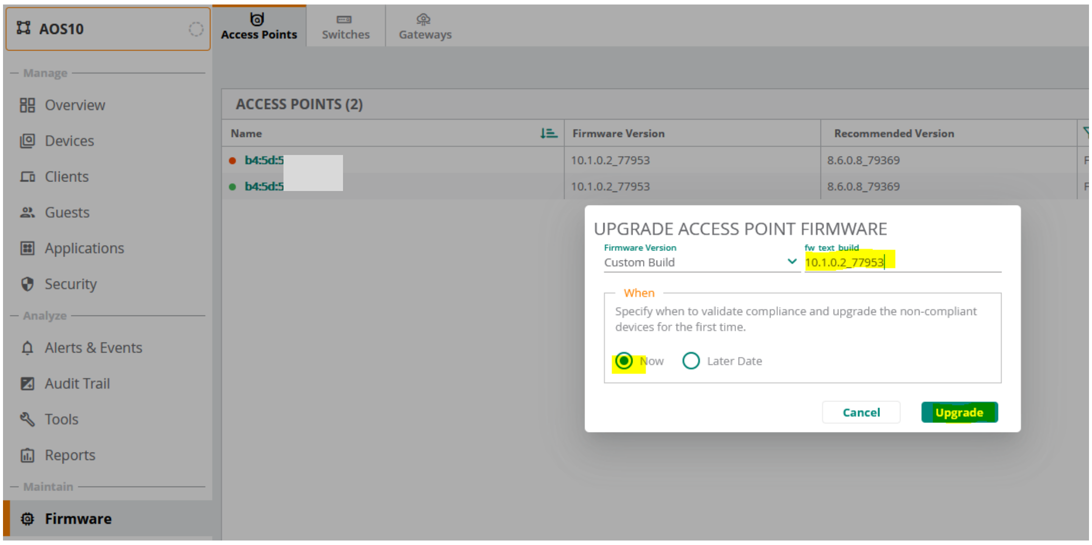
4.5 Firmware Upgrade

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.



ACCESS POINTS (2)

Name	Firmware Version	Recommended Version
● b4:5d:5[redacted]	10.1.0.2_77953	8.6.0.8_79369
● b4:5d:5[redacted]	10.1.0.2_77953	8.6.0.8_79369

UPGRADE ACCESS POINT FIRMWARE

Firmware Version: Custom Build

fw text build: 10.1.0.2_77953

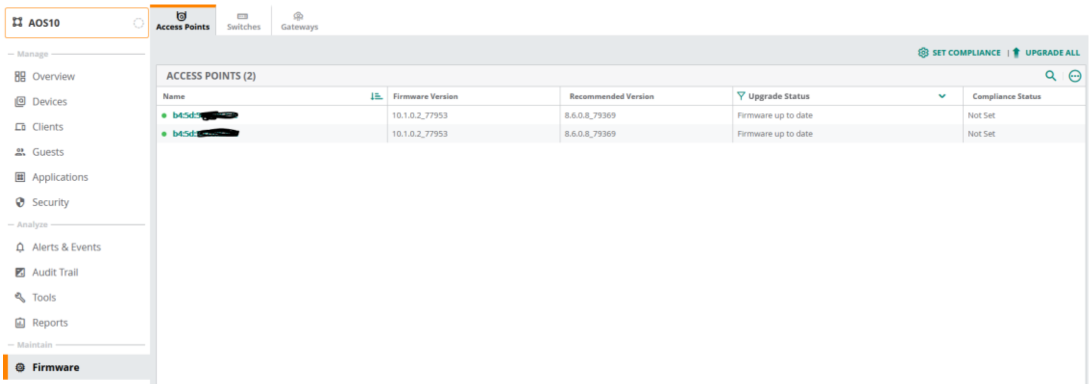
When

Specify when to validate compliance and upgrade the non-compliant devices for the first time.

● Now ○ Later Date

Cancel Upgrade

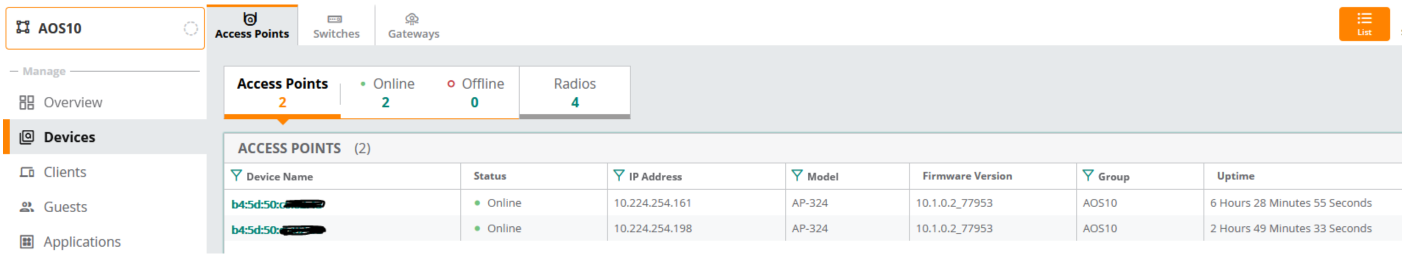
We’ll use the same firmware version for the gateways as well.



ACCESS POINTS (2)

Name	Firmware Version	Recommended Version	Upgrade Status	Compliance Status
● b4:5d:[redacted]	10.1.0.2_77953	8.6.0.8_79369	Firmware up to date	Not Set
● b4:5d:[redacted]	10.1.0.2_77953	8.6.0.8_79369	Firmware up to date	Not Set

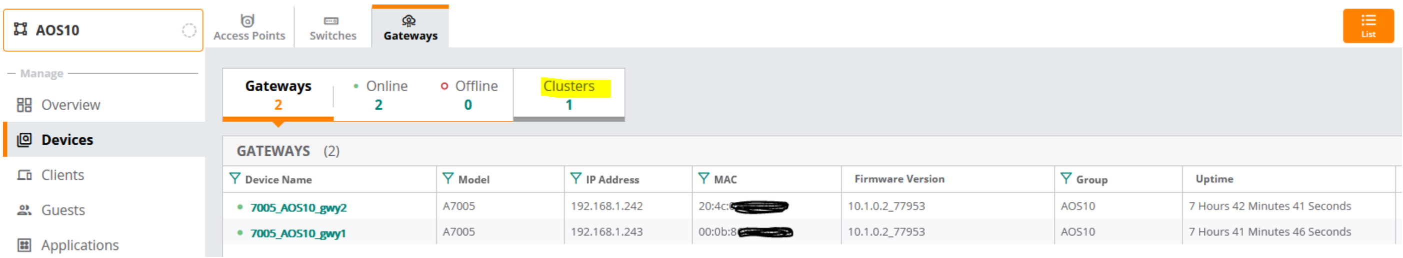
Here we’ll check to see if the APs and gateways are online with the correct firmware



Access Points	Online	Offline	Radios
2	2	0	4

ACCESS POINTS (2)

Device Name	Status	IP Address	Model	Firmware Version	Group	Uptime
b4:5d:50:[redacted]	● Online	10.224.254.161	AP-324	10.1.0.2_77953	AOS10	6 Hours 28 Minutes 55 Seconds
b4:5d:50:[redacted]	● Online	10.224.254.198	AP-324	10.1.0.2_77953	AOS10	2 Hours 49 Minutes 33 Seconds



Gateways	Online	Offline	Clusters
2	2	0	1

GATEWAYS (2)

Device Name	Model	IP Address	MAC	Firmware Version	Group	Uptime
● 7005_AOS10_gwy2	A7005	192.168.1.242	20:4c:[redacted]	10.1.0.2_77953	AOS10	7 Hours 42 Minutes 41 Seconds
● 7005_AOS10_gwy1	A7005	192.168.1.243	00:0b:8[redacted]	10.1.0.2_77953	AOS10	7 Hours 41 Minutes 46 Seconds

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

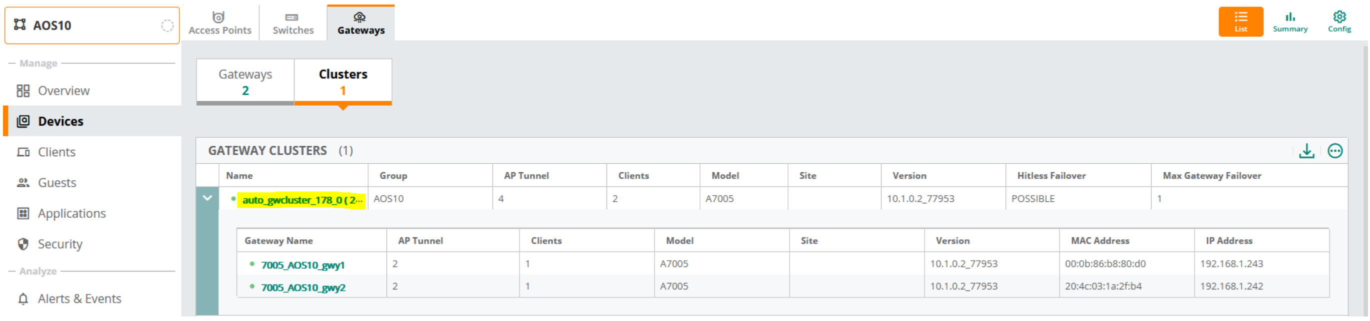
Cluster is a combination of multiple MDs working together to provide high availability to all the clients and ensure service continuity when a failover occurs. The gateways need not be identical and can be either L2- connected or L3- connected with a mixed configuration. In case of failover, the client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

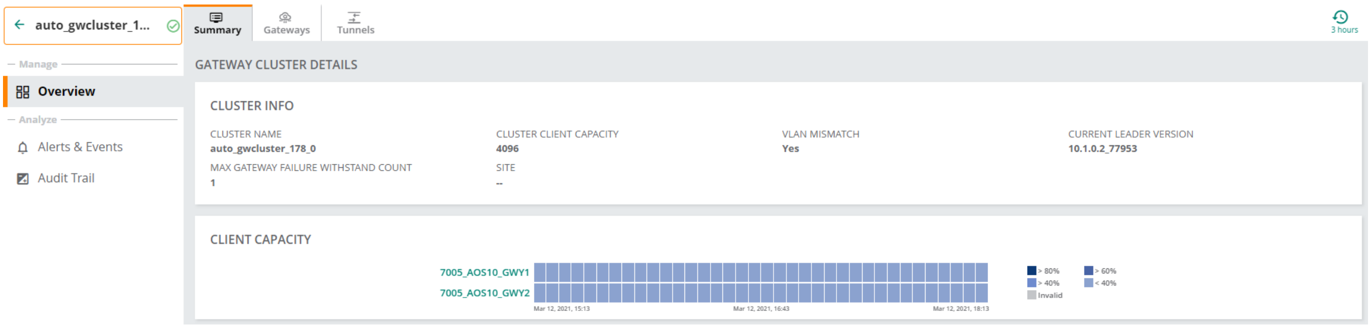
Here is how to check the gateway cluster



GATEWAY CLUSTERS (1)

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:2f:b4	192.168.1.242



GATEWAY CLUSTER DETAILS

CLUSTER INFO

CLUSTER NAME
auto_gwcluster_178_0

CLUSTER CLIENT CAPACITY
4096

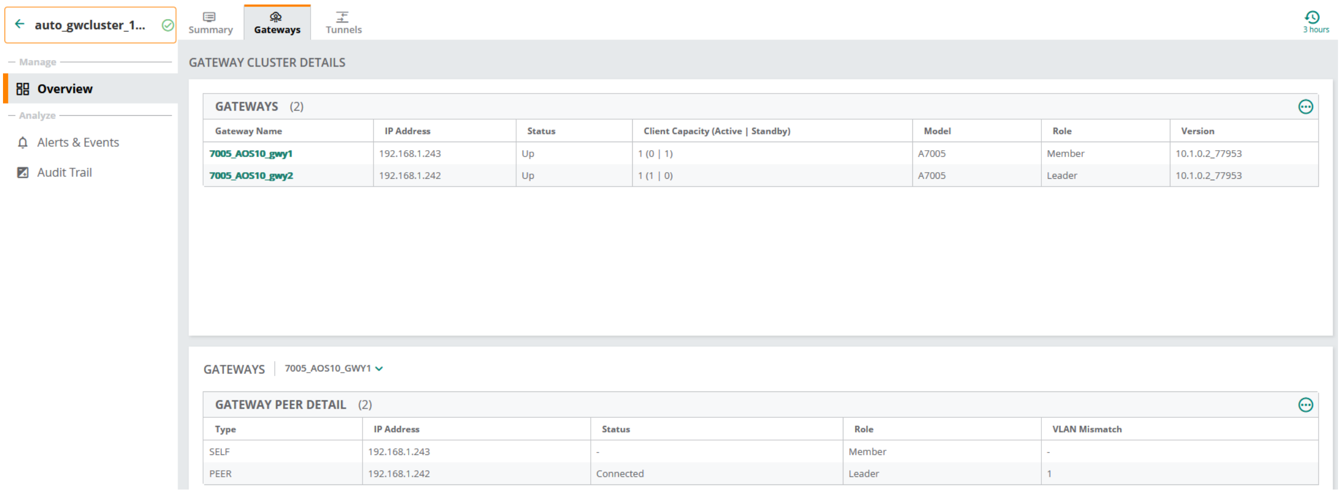
VLAN MISMATCH
Yes

CURRENT LEADER VERSION
10.1.0.2_77953

MAX GATEWAY FAILURE WITHSTAND COUNT
1

SITE
--

CLIENT CAPACITY



GATEWAY CLUSTER DETAILS

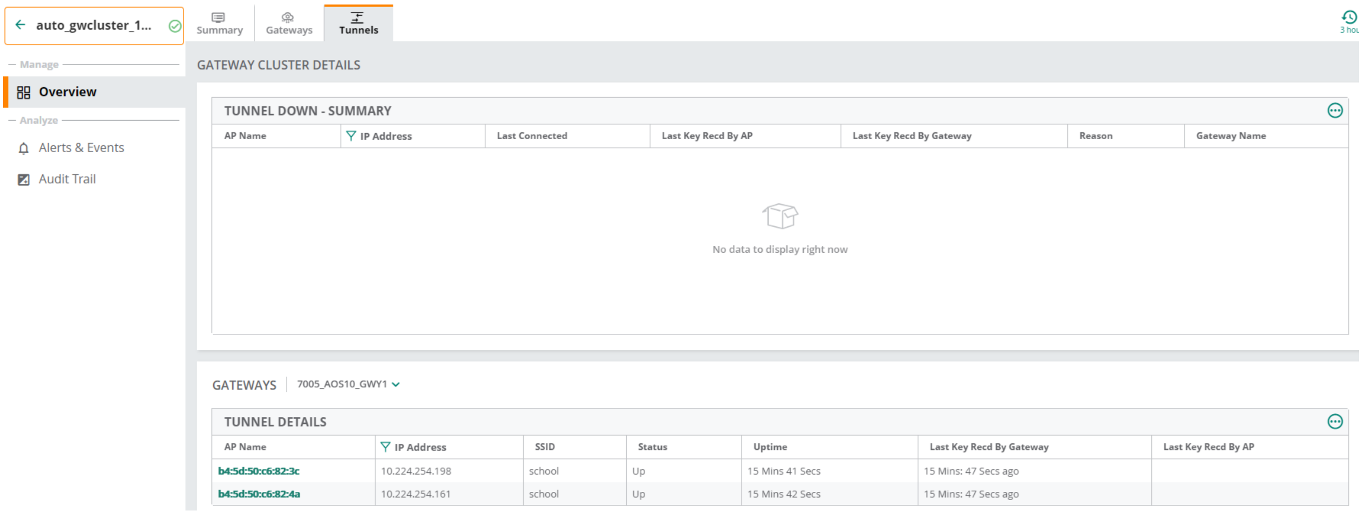
GATEWAYS (2)

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

GATEWAYS | 7005_AOS10_GWY1

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



GATEWAY CLUSTER DETAILS

TUNNEL DOWN - SUMMARY

AP Name	IP Address	Last Connected	Last Key Recd By AP	Last Key Recd By Gateway	Reason	Gateway Name

No data to display right now

GATEWAYS | 7005_AOS10_GWY1

TUNNEL DETAILS

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) #
```

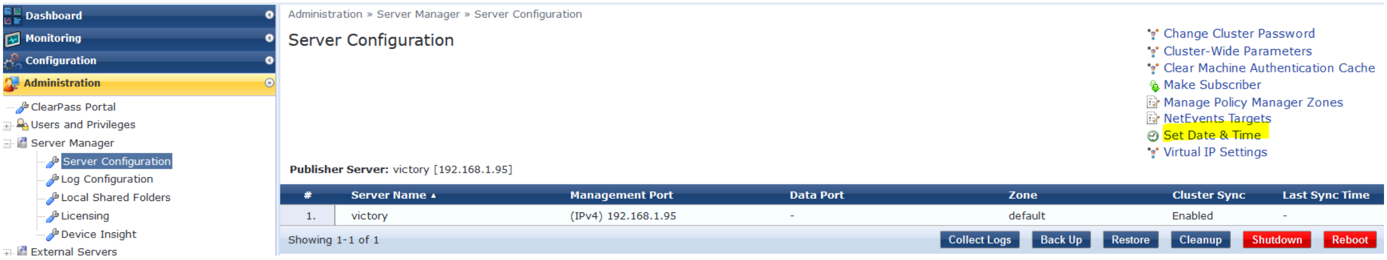
Now checking the second gateway. Note we have 1x client and 2x APs that are connected.

```
(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.



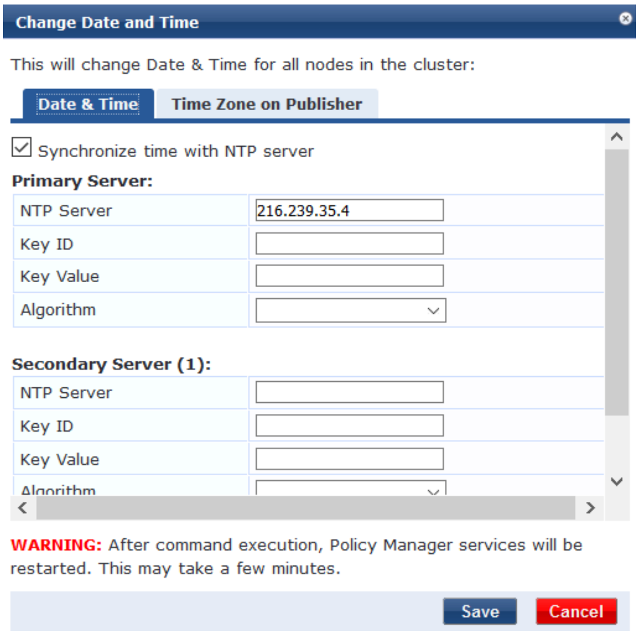
Administration » Server Manager » Server Configuration

Server Configuration

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



Change Date and Time

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

☑ Synchronize time with NTP server

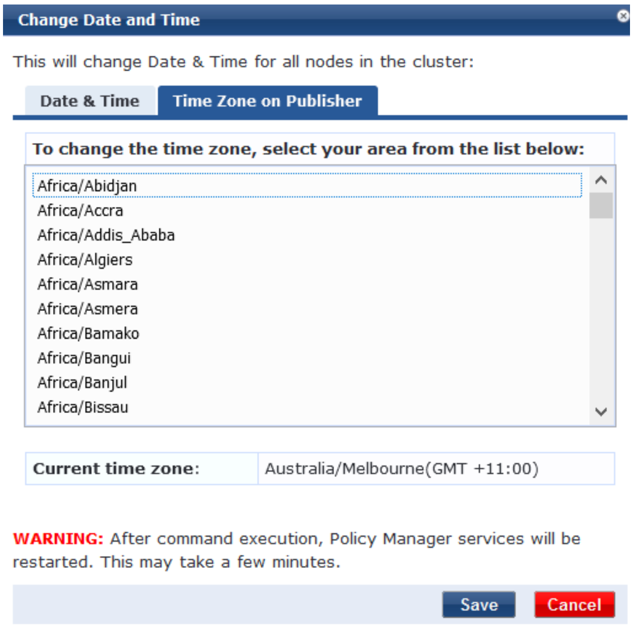
Primary Server:

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.



Change Date and Time

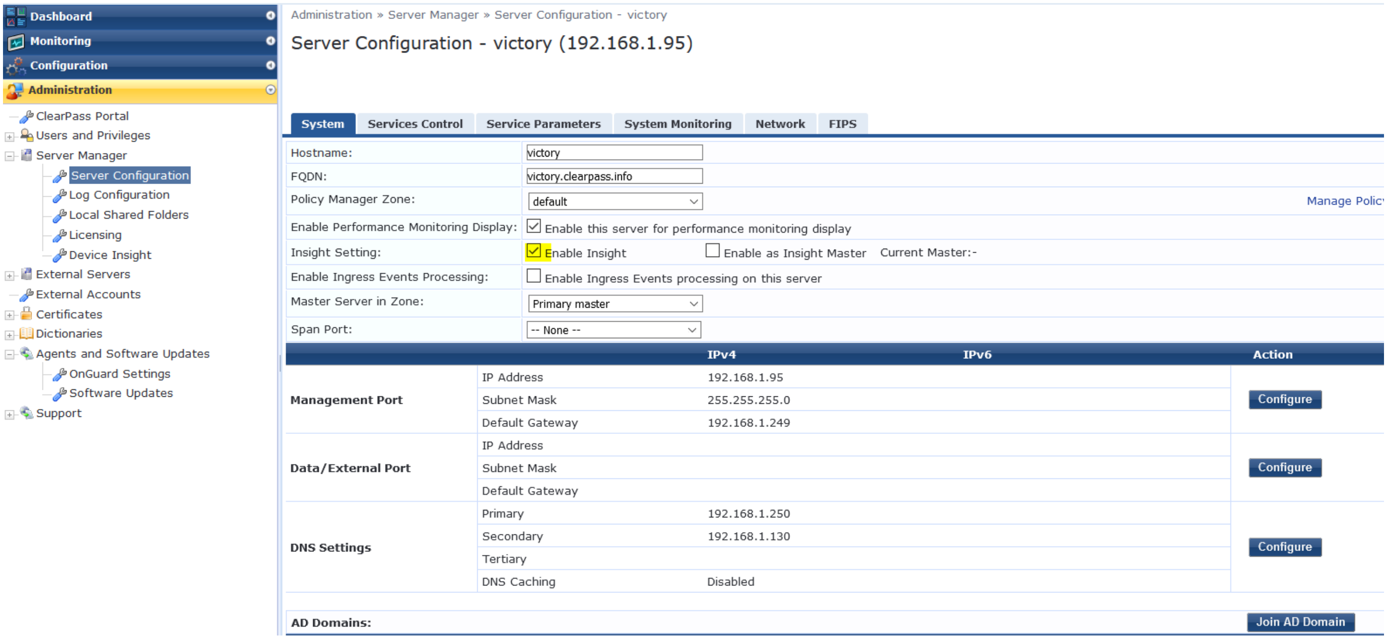
This will change Date & Time for all nodes in the cluster:

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.



Administration » Server Manager » Server Configuration - victory

Server Configuration - victory (192.168.1.95)

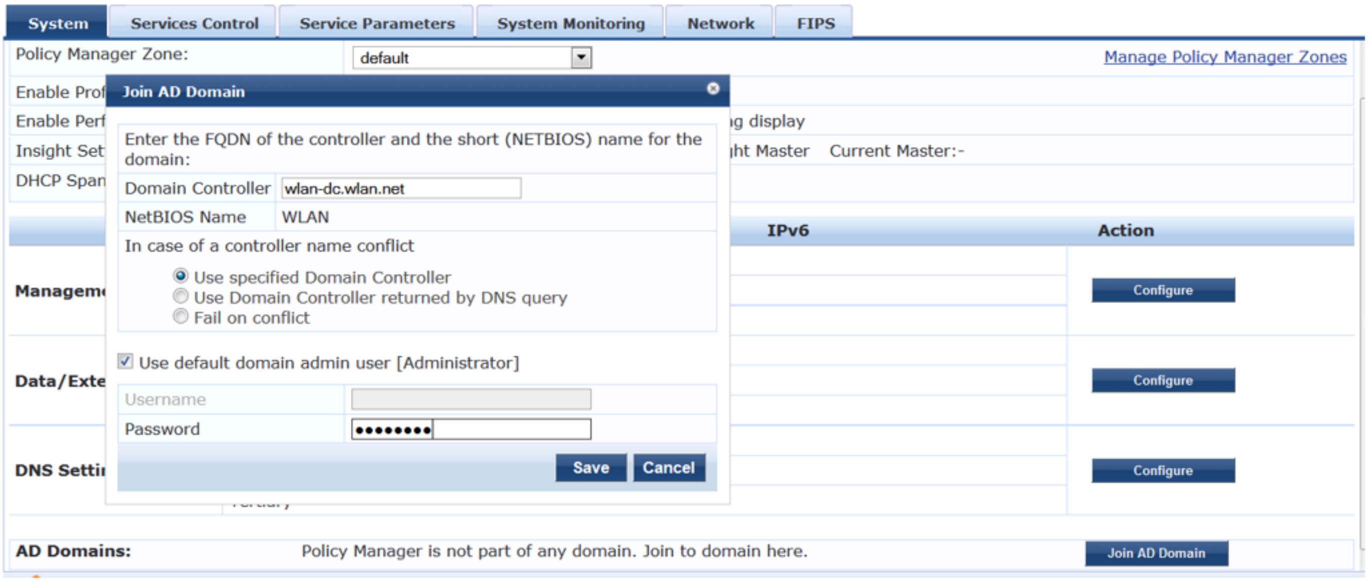
Hostname:	victory
FQDN:	victory.clearpass.info
Policy Manager Zone:	default
Enable Performance Monitoring Display:	☑ Enable this server for performance monitoring display
Insight Setting:	☑ Enable Insight ☐ Enable as Insight Master Current Master:-
Enable Ingress Events Processing:	☐ Enable Ingress events 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:

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

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

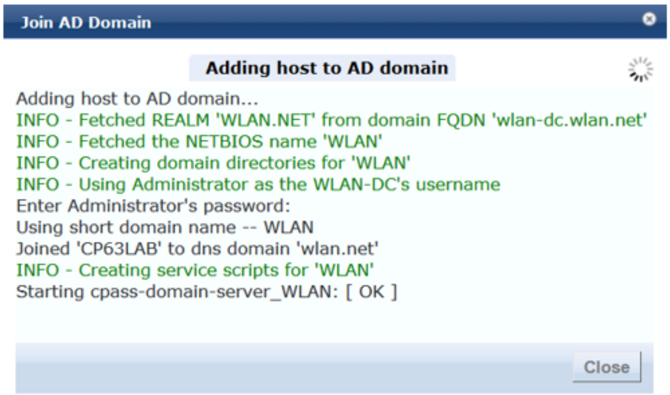
In case of a controller name conflict

● Use specified Domain Controller
○ Use Domain Controller returned by DNS query
○ Fail on conflict

☑ Use default domain admin user [Administrator]

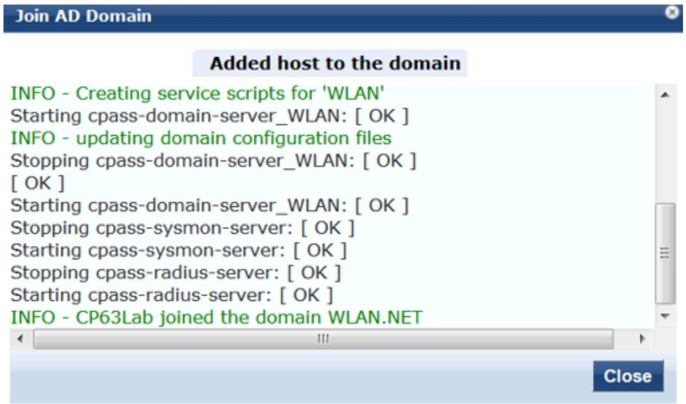
Username	
Password	••••••••

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



Adding host to AD domain

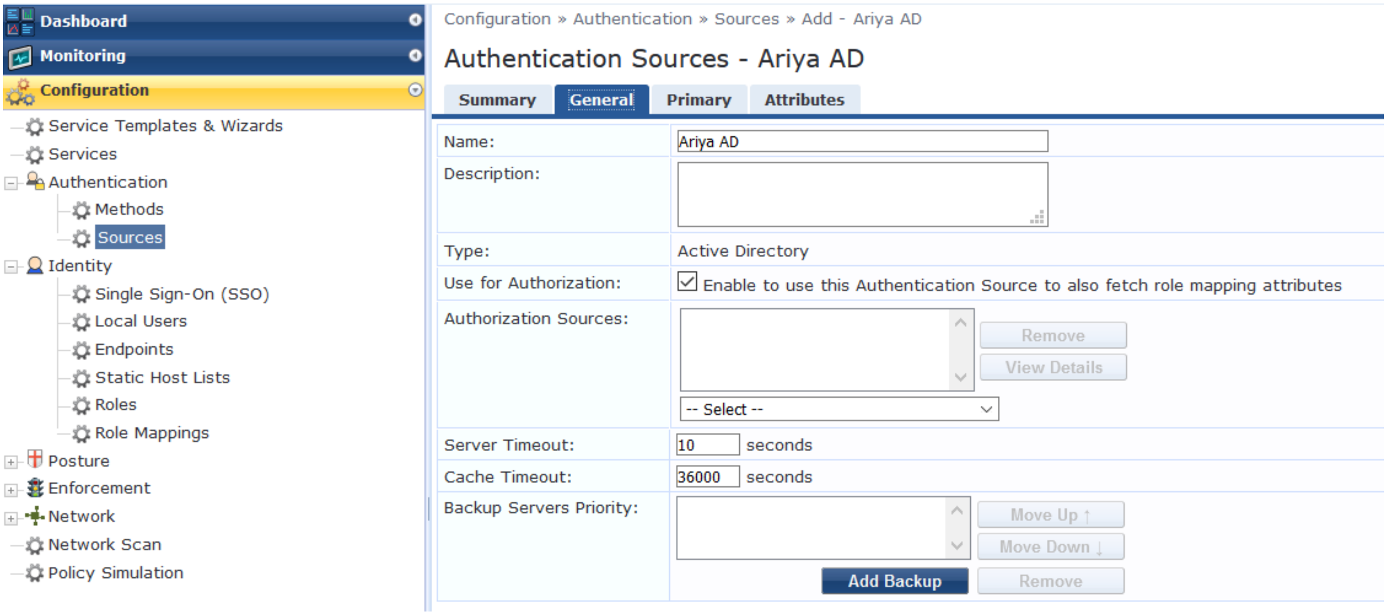
```
Adding host to AD domain...
INFO - Fetched REALM 'WLAN.NET' from domain FQDN 'wlan-dc.wlan.net'
INFO - Fetched the NETBIOS name 'WLAN'
INFO - Creating domain directories for 'WLAN'
INFO - Using Administrator as the WLAN-DC's username
Enter Administrator's password:
Using short domain name -- WLAN
Joined 'CP63LAB' to dns domain 'wlan.net'
INFO - Creating service scripts for 'WLAN'
Starting cpass-domain-server_WLAN: [ OK ]
```



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
```

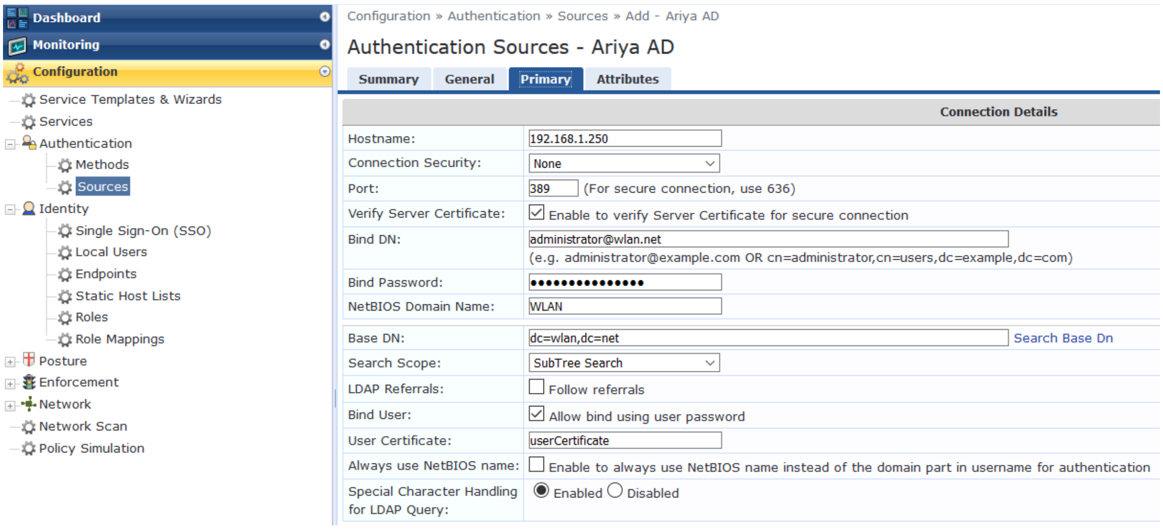
Now we need to add the AD as authentication source



Configuration » Authentication » Sources » Add - Ariya AD

Authentication Sources - Ariya AD

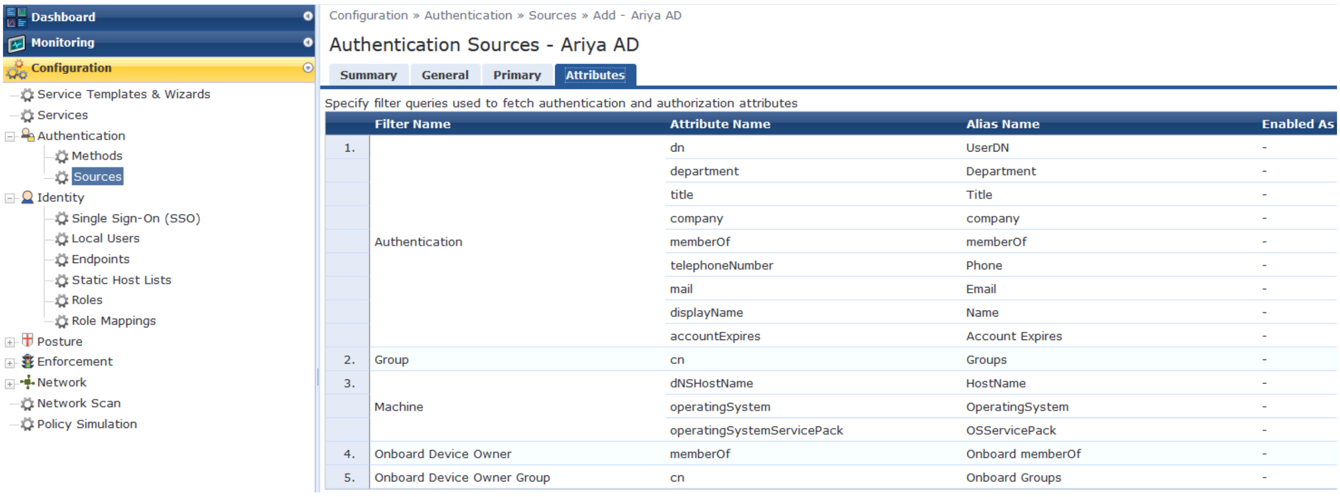
Name:	Ariya AD
Description:	
Type:	Active Directory
Use for Authorization:	☑ Enable to use this Authentication Source to also fetch role mapping attributes
Authorization Sources:	-- Select --
Server Timeout:	10 seconds
Cache Timeout:	36000 seconds
Backup Servers Priority:	



Configuration » Authentication » Sources » Add - Ariya AD

Authentication Sources - Ariya AD

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



Configuration » Authentication » Sources » Add - Ariya AD

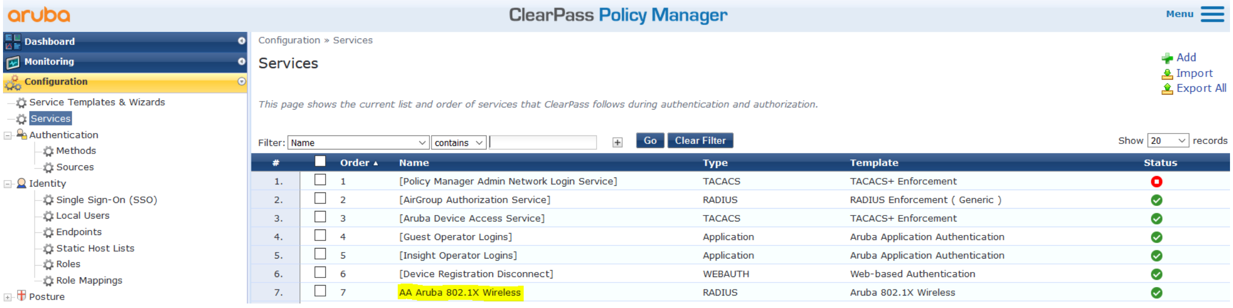
Authentication Sources - Ariya AD

Specify filter queries used to fetch authentication and authorization attributes

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

5.2 ClearPass dot1x Service

Here we create a dot1x service for wireless access.



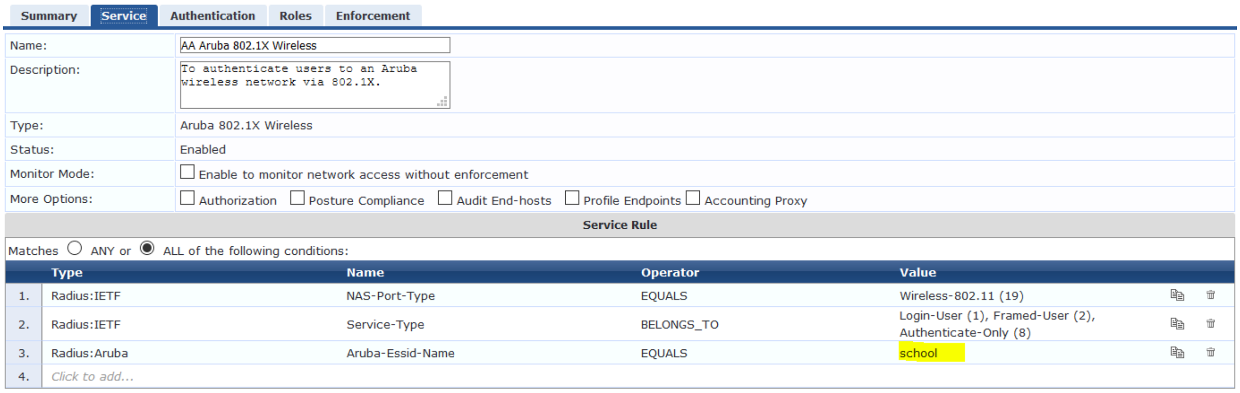
Configuration » Services

Services

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

Filter: Name contains | 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	✓



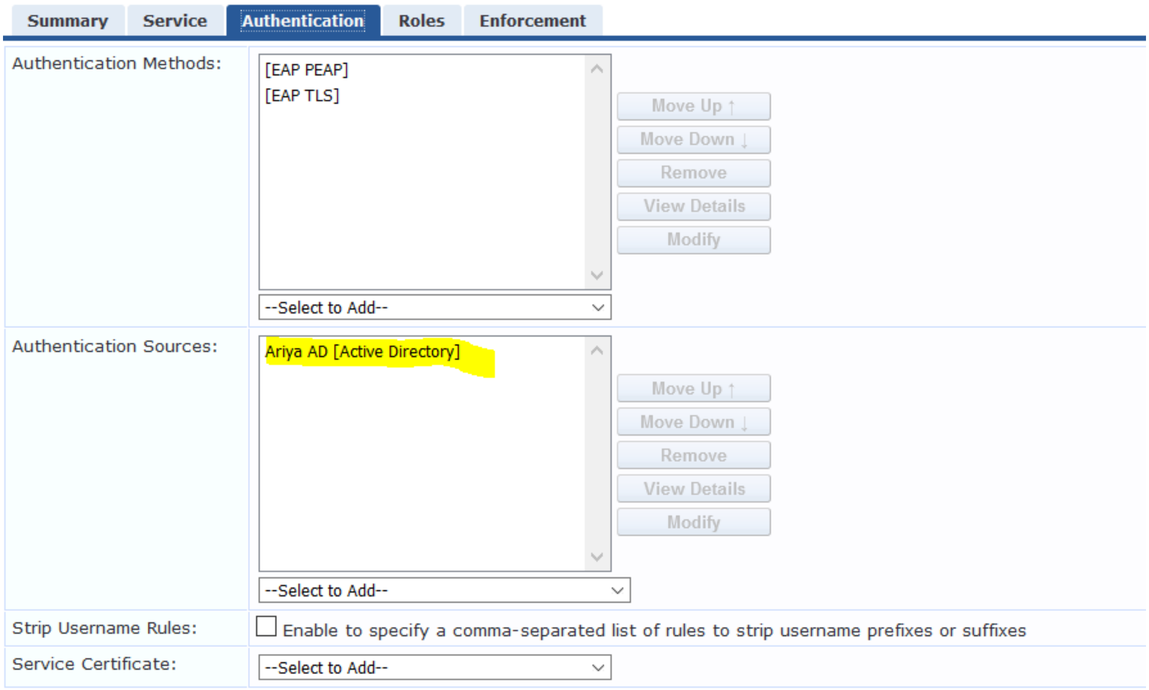
Name:	AA Aruba 802.1X Wireless
Description:	To authenticate users to an Aruba wireless network via 802.1X.
Type:	Aruba 802.1X Wireless
Status:	Enabled
Monitor Mode:	☐ Enable to monitor network access without enforcement
More Options:	☐ Authorization ☐ Posture Compliance ☐ Audit End-hosts ☐ Profile Endpoints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

Service Rule

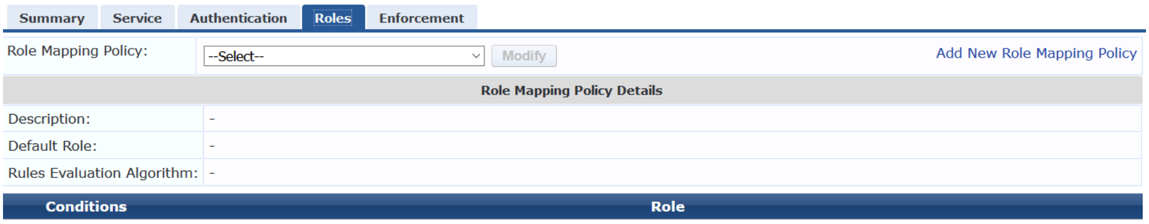
Matches ○ ANY or ● ALL of the following conditions:

	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



Authentication Methods:	[EAP PEAP] [EAP TLS] --Select to Add--
Authentication Sources:	Ariya AD [Active Directory] --Select to Add--
Strip Username Rules:	□ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes
Service Certificate:	--Select to Add--

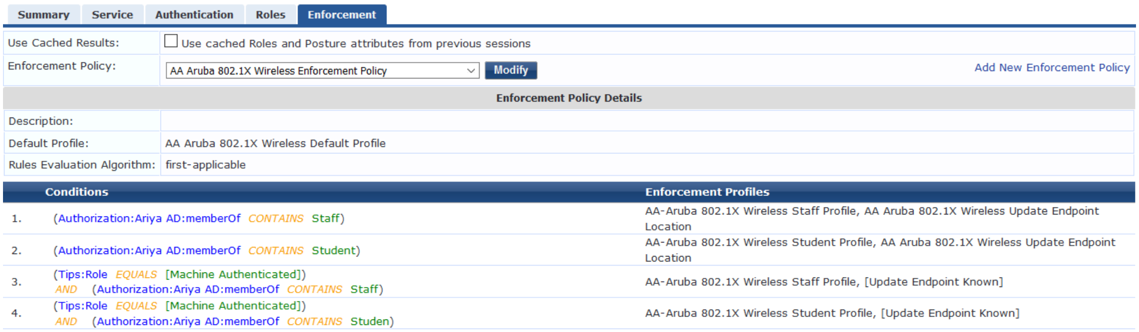


Role Mapping Policy:	--Select--

Role Mapping Policy Details

Description:	-
Default Role:	-
Rules Evaluation Algorithm:	-

Conditions	Role



Use Cached Results:	□ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	AA Aruba 802.1X Wireless Enforcement Policy

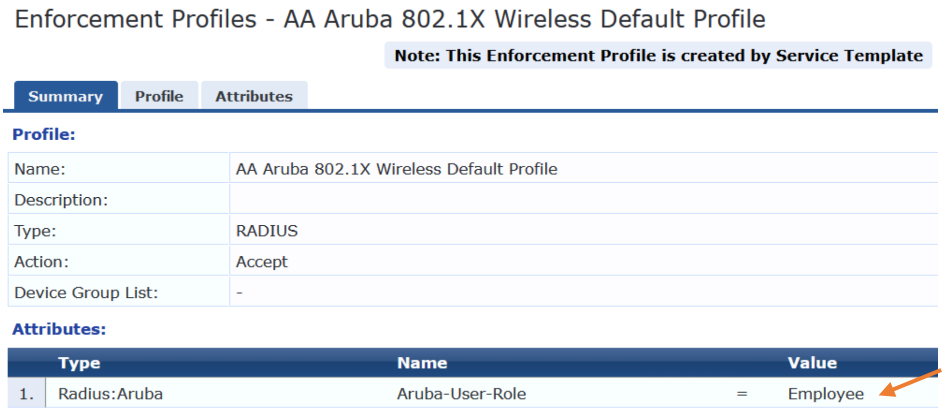
Enforcement Policy Details

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

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

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

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



Enforcement Profiles - AA Aruba 802.1X Wireless Default Profile

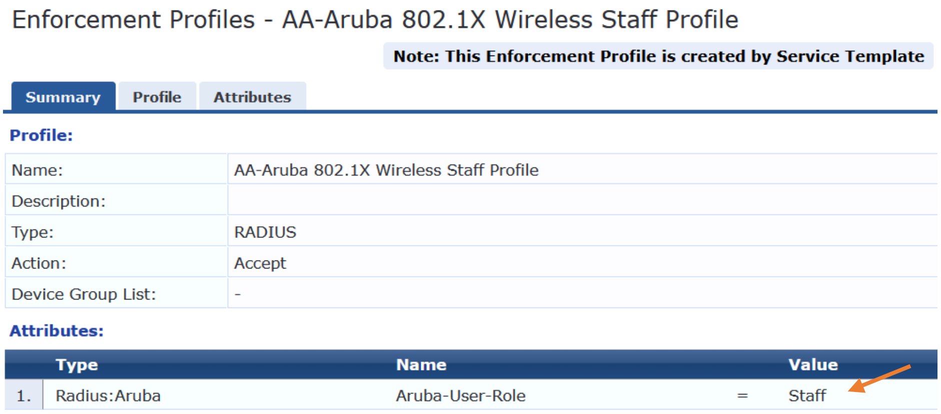
Note: This Enforcement Profile is created by Service Template

Profile:

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

Attributes:

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



Enforcement Profiles - AA-Aruba 802.1X Wireless Staff Profile

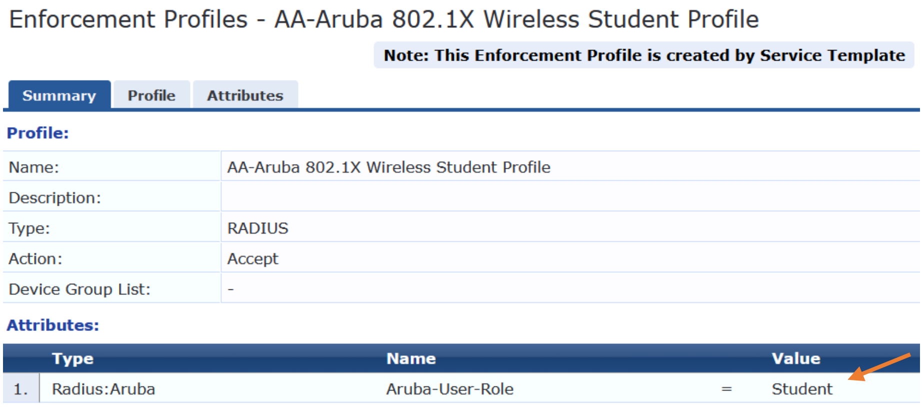
Note: This Enforcement Profile is created by Service Template

Profile:

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

Attributes:

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



Enforcement Profiles - AA-Aruba 802.1X Wireless Student Profile

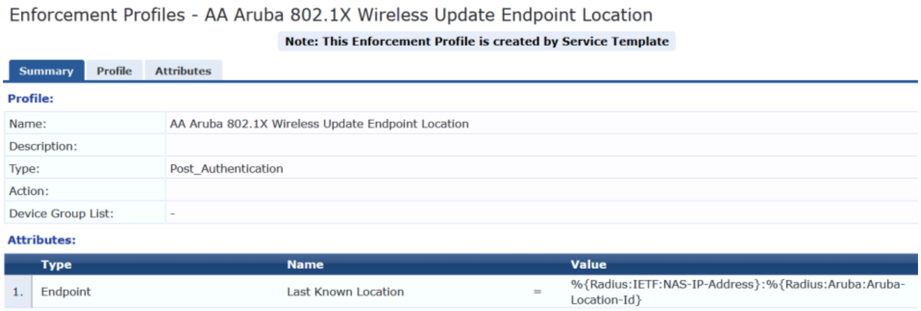
Note: This Enforcement Profile is created by Service Template

Profile:

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

Attributes:

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



Enforcement Profiles - AA Aruba 802.1X Wireless Update Endpoint Location

Note: This Enforcement Profile is created by Service Template

Profile:

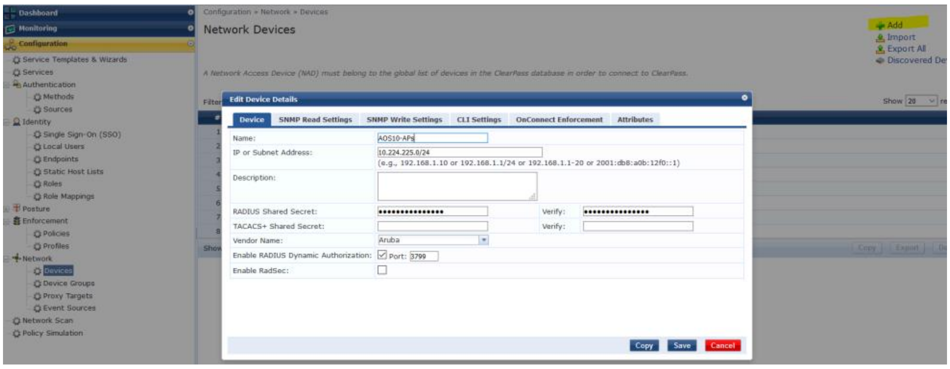
Name:	AA Aruba 802.1X Wireless Update Endpoint Location
Description:	
Type:	Post_Authentication
Action:	
Device Group List:	-

Attributes:

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

5.3 NAD Configuration

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



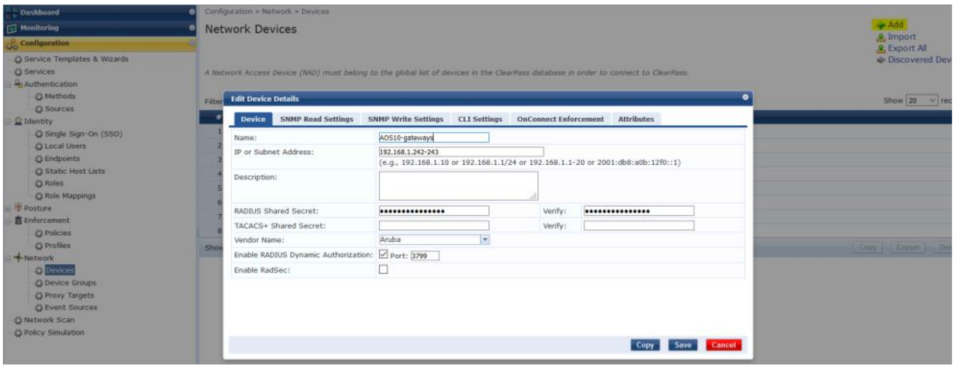
Configuration » Network » Devices

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.

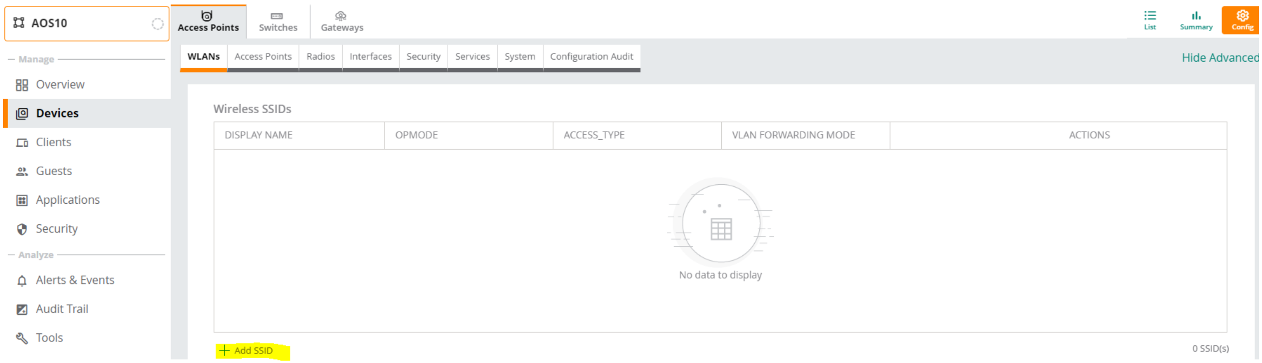
Edit Device Details

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:	□		

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 Mode Wireless Configuration



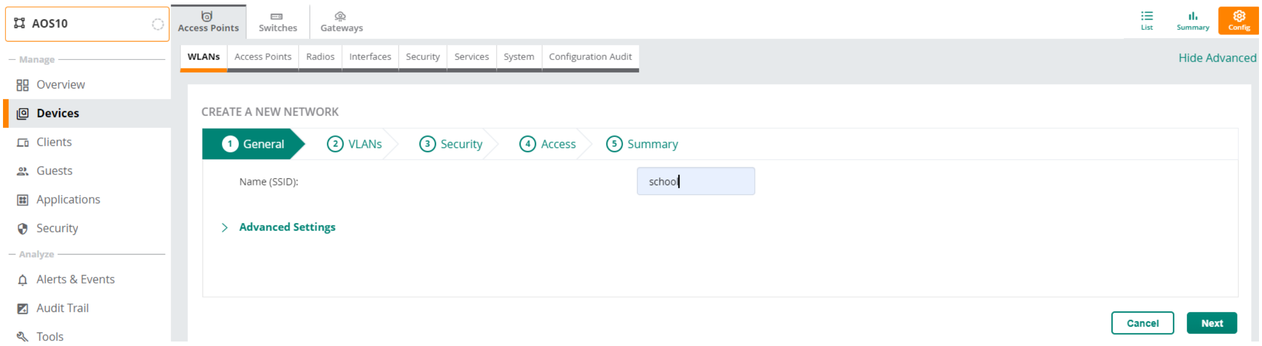
Wireless SSIDs

DISPLAY NAME	OPMODE	ACCESS_TYPE	VLAN FORWARDING MODE	ACTIONS

No data to display

+ Add SSID

0 SSID(s)



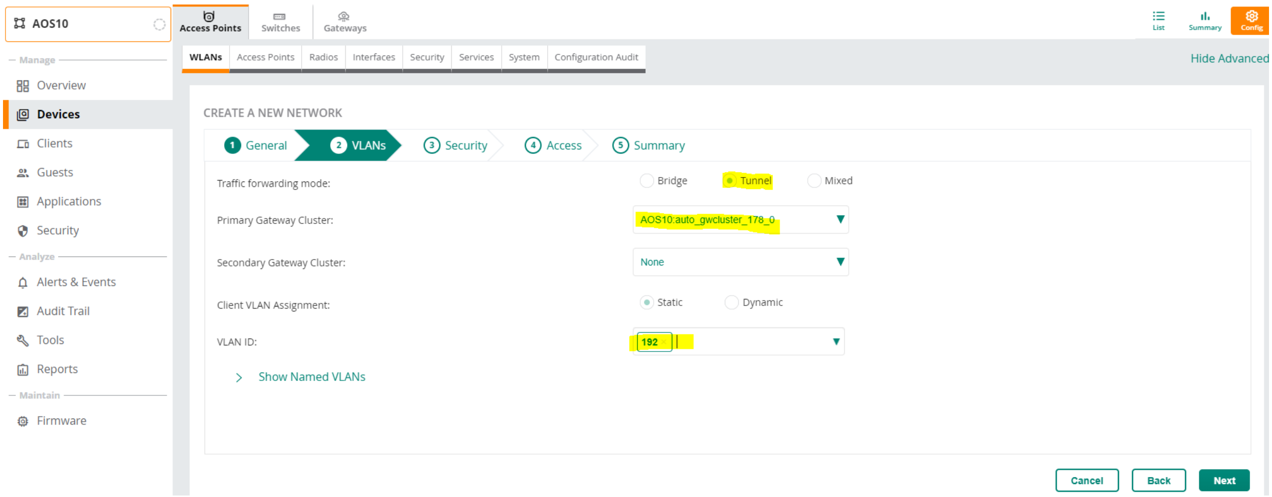
CREATE A NEW NETWORK

1 General 2 VLANs 3 Security 4 Access 5 Summary

Name (SSID): school

Advanced Settings

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



CREATE A NEW NETWORK

1 General 2 VLANs 3 Security 4 Access 5 Summary

Traffic forwarding mode: ○ Bridge ● Tunnel ○ Mixed

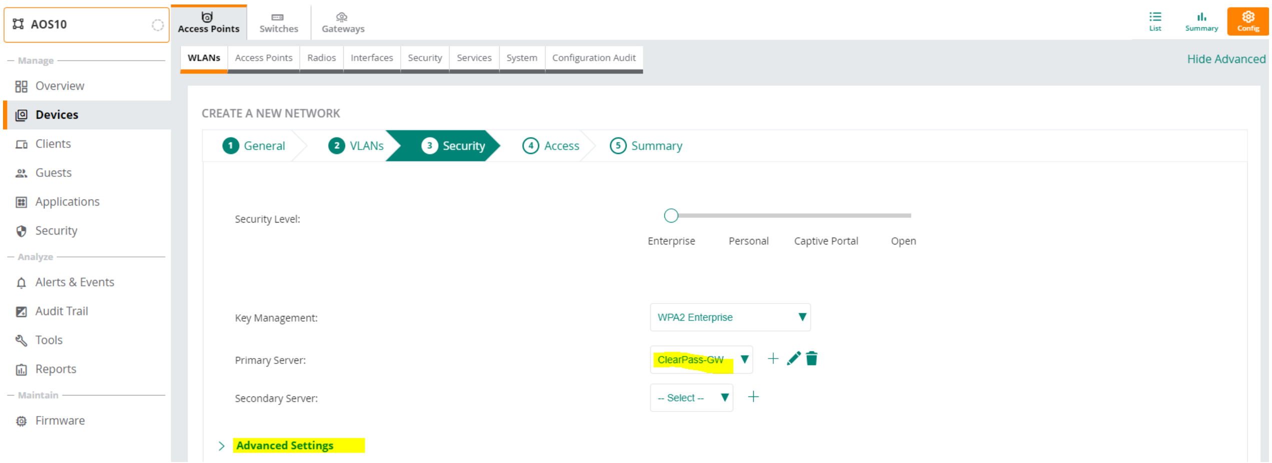
Primary Gateway Cluster: AOS10:auto_gwcluster_178_0

Secondary Gateway Cluster: None

Client VLAN Assignment: ● Static ○ Dynamic

VLAN ID: 192

Show Named VLANs



CREATE A NEW NETWORK

1 General 2 VLANs 3 Security 4 Access 5 Summary

Security Level: Enterprise Personal Captive Portal Open

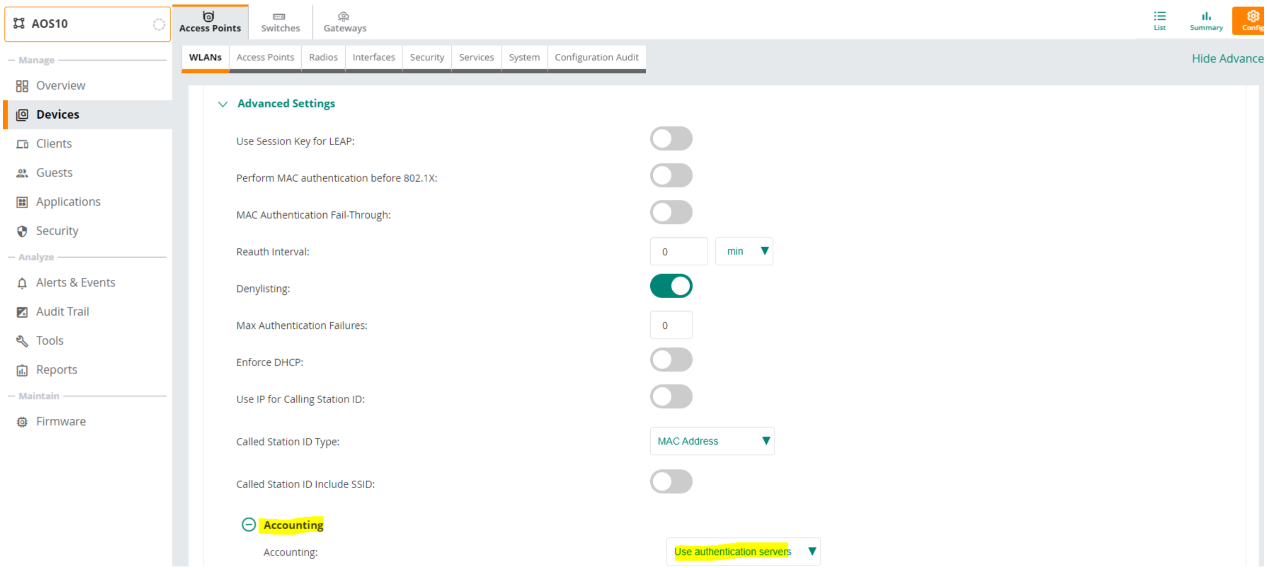
Key Management: WPA2 Enterprise

Primary Server: ClearPass-GW

Secondary Server: -- Select --

Advanced Settings

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



Advanced Settings

Use Session Key for LEAP: ○

Perform MAC authentication before 802.1X: ○

MAC Authentication Fail-Through: ○

Reauth Interval: 0 min

Denylisting: ●

Max Authentication Failures: 0

Enforce DHCP: ○

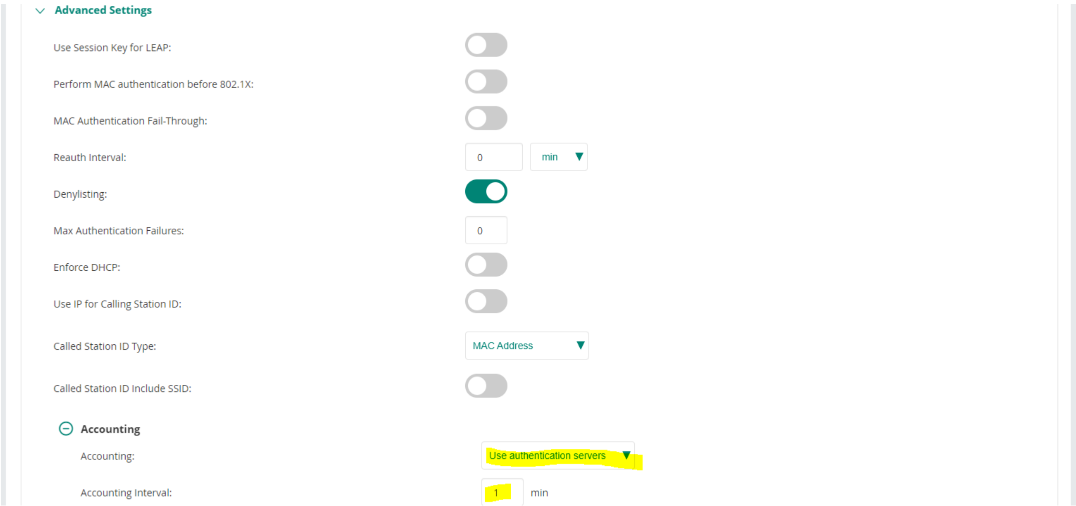
Use IP for Calling Station ID: ○

Called Station ID Type: MAC Address

Called Station ID Include SSID: ○

Accounting

Accounting: Use authentication servers



Advanced Settings

Use Session Key for LEAP: ○

Perform MAC authentication before 802.1X: ○

MAC Authentication Fail-Through: ○

Reauth Interval: 0 min

Denylisting: ●

Max Authentication Failures: 0

Enforce DHCP: ○

Use IP for Calling Station ID: ○

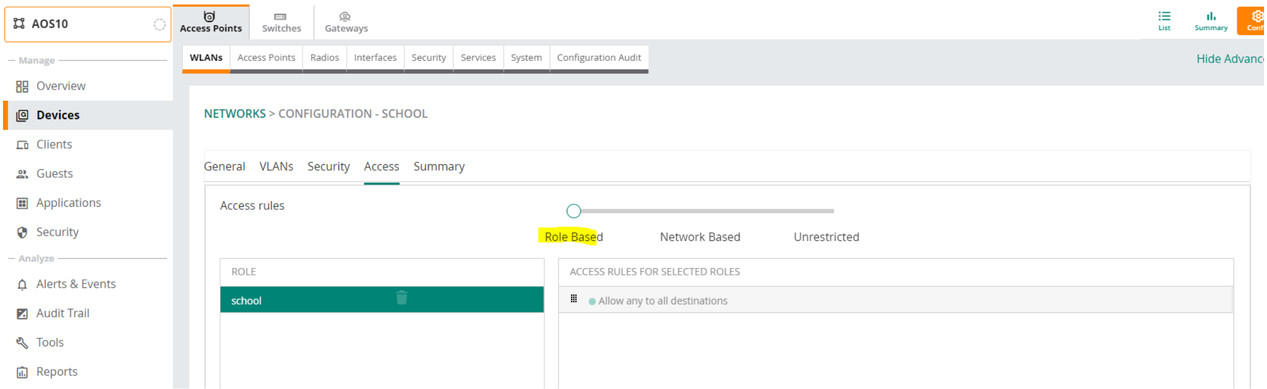
Called Station ID Type: MAC Address

Called Station ID Include SSID: ○

Accounting

Accounting: Use authentication servers

Accounting Interval: 1 min



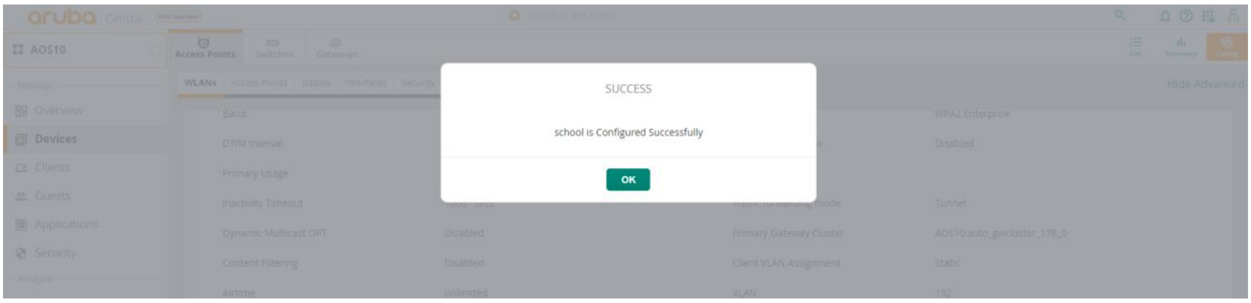
NETWORKS > CONFIGURATION - SCHOOL

Access rules

Role Based | Network Based | Unrestricted

ROLE	ACCESS RULES FOR SELECTED ROLES
school	Allow any to all destinations

And save the configuration.



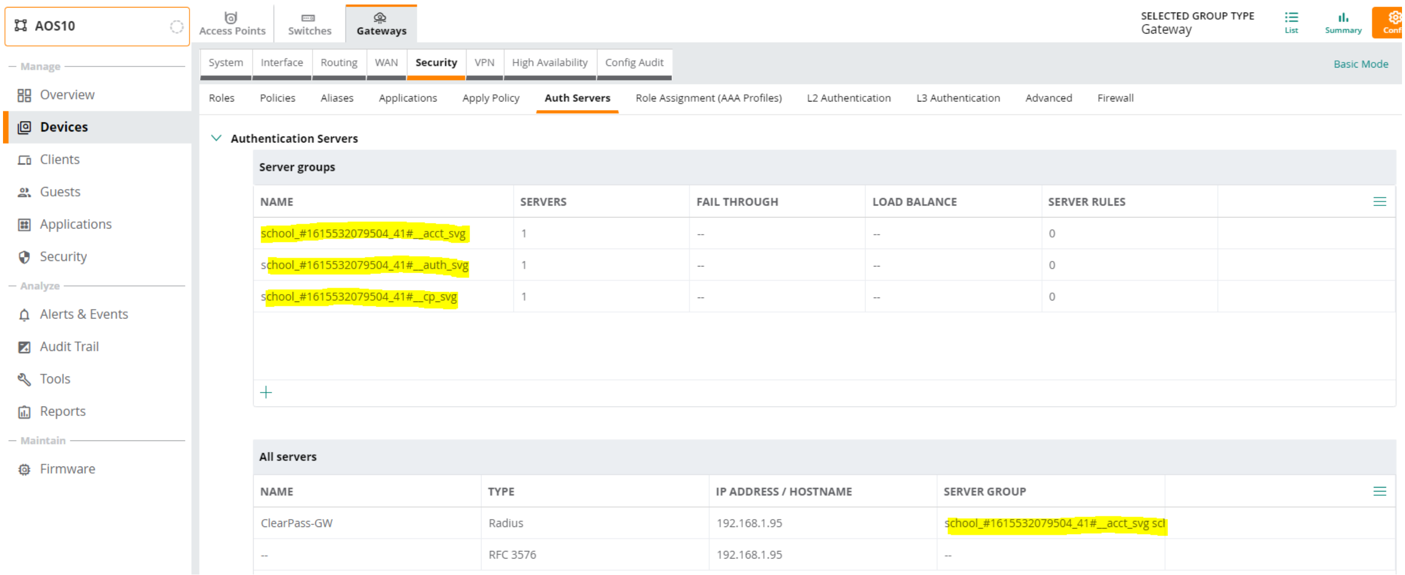
SUCCESS

school is Configured Successfully

OK

6.2 Tunnelled Mode Wireless dot1x Testing

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



Authentication Servers

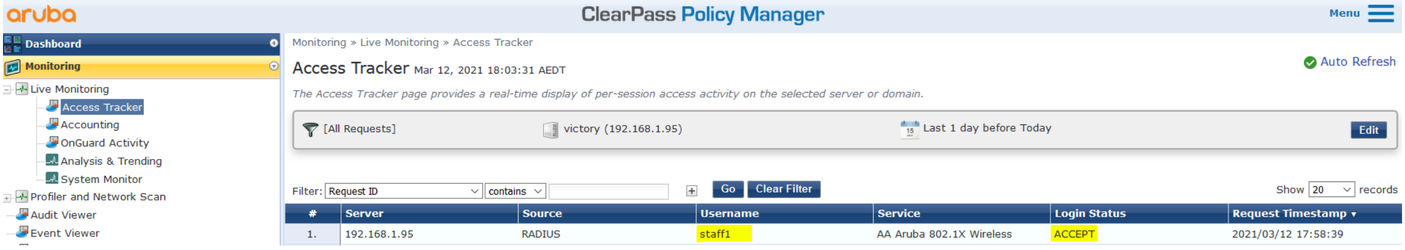
Server groups

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 scl
--	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



Monitoring » Live Monitoring » Access Tracker

Access Tracker Mar 12, 2021 18:03:31 AEDT

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

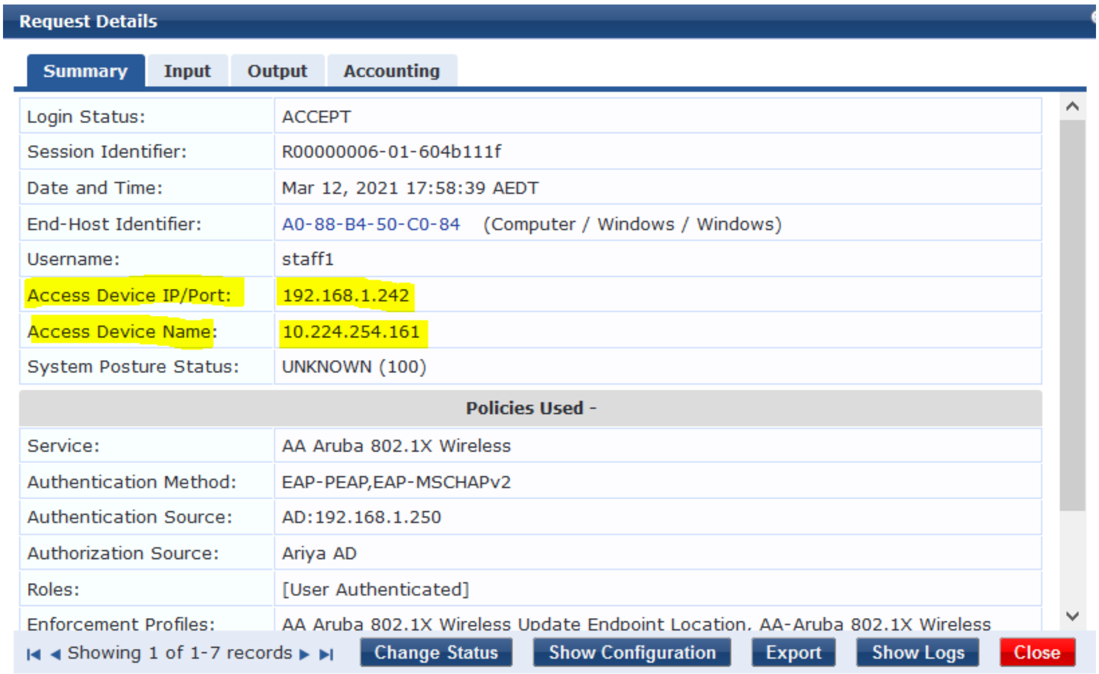
[All Requests] victory (192.168.1.95) Last 1 day before Today

Filter: Request ID contains

Show 20 records

#	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

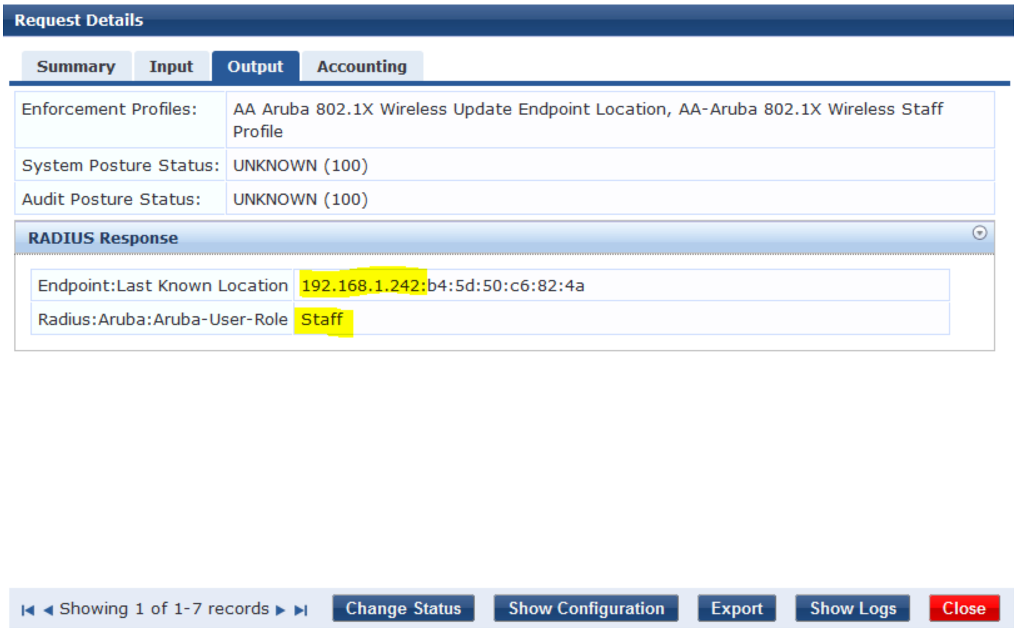
Note that 192.168.1.242 is the IP address of the gateway-1 and 10.224.254.161 is the IP address of the AP.



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

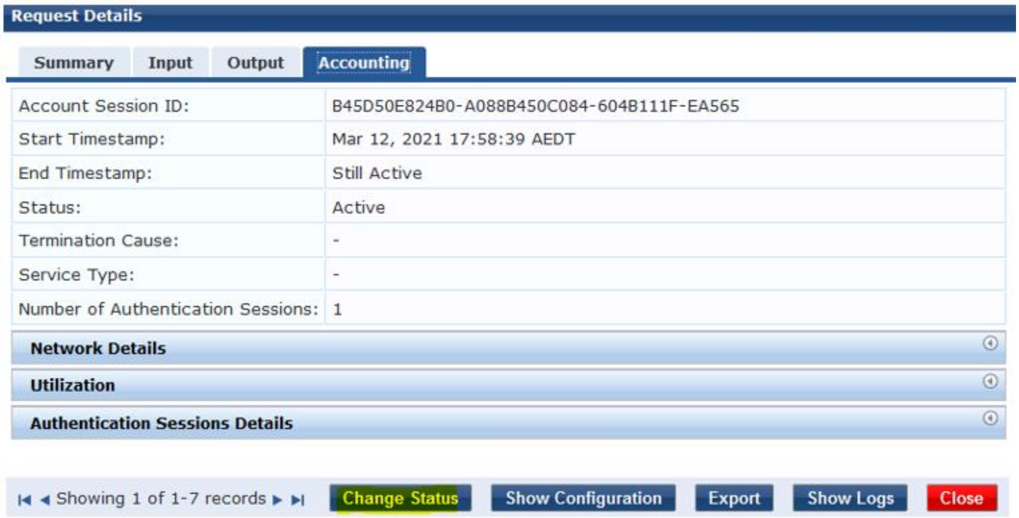


Enforcement Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless Staff Profile
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

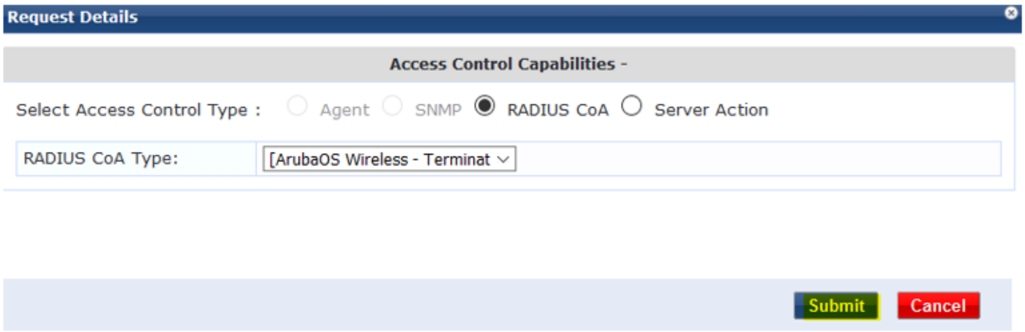
Endpoint:Last Known Location	192.168.1.242:b4:5d:50:c6:82:4a
Radius:Aruba:Aruba-User-Role	Staff

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



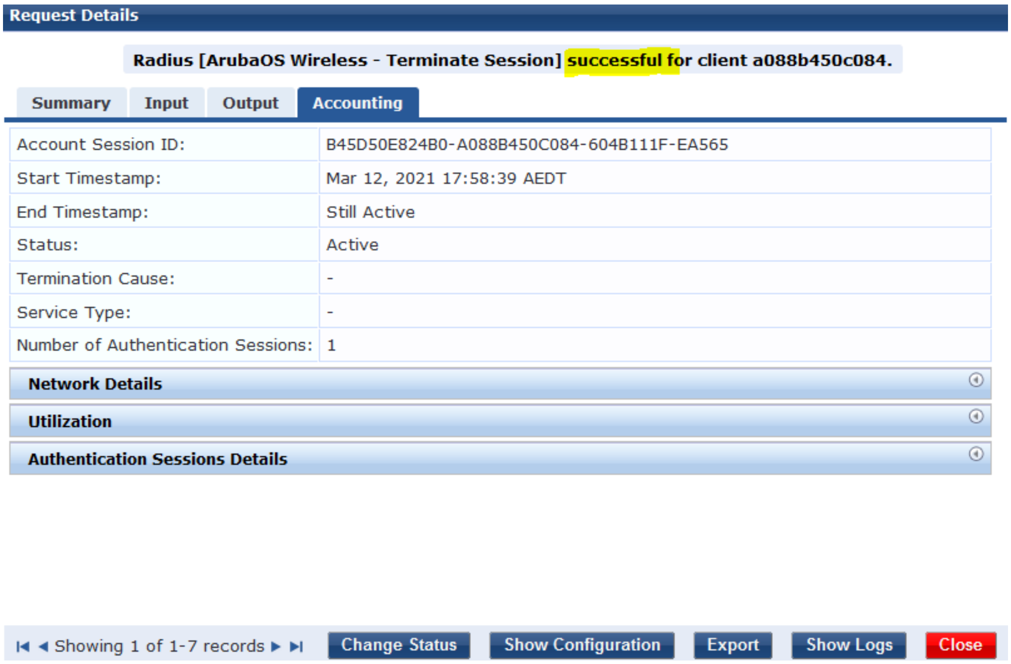
Account Session ID:	B45D50E824B0-A088B450C084-604B111F-EA565
Start Timestamp:	Mar 12, 2021 17:58:39 AEDT
End Timestamp:	Still Active
Status:	Active
Termination Cause:	-
Service Type:	-
Number of Authentication Sessions:	1

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



Select Access Control Type : ○ Agent ○ SNMP ● RADIUS CoA ○ Server Action

RADIUS CoA Type:	[ArubaOS Wireless - Terminat

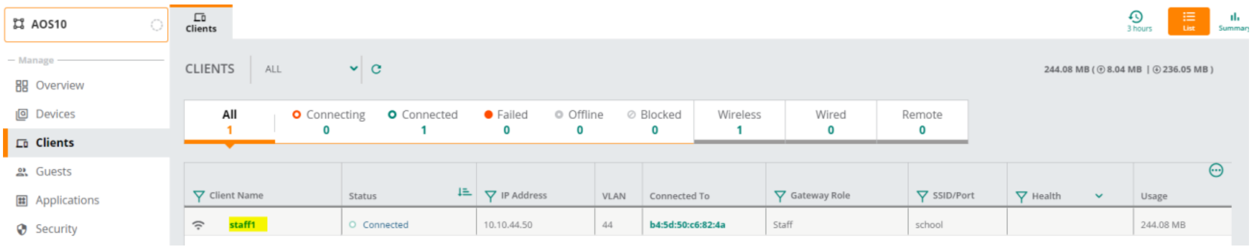


Request Details

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

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

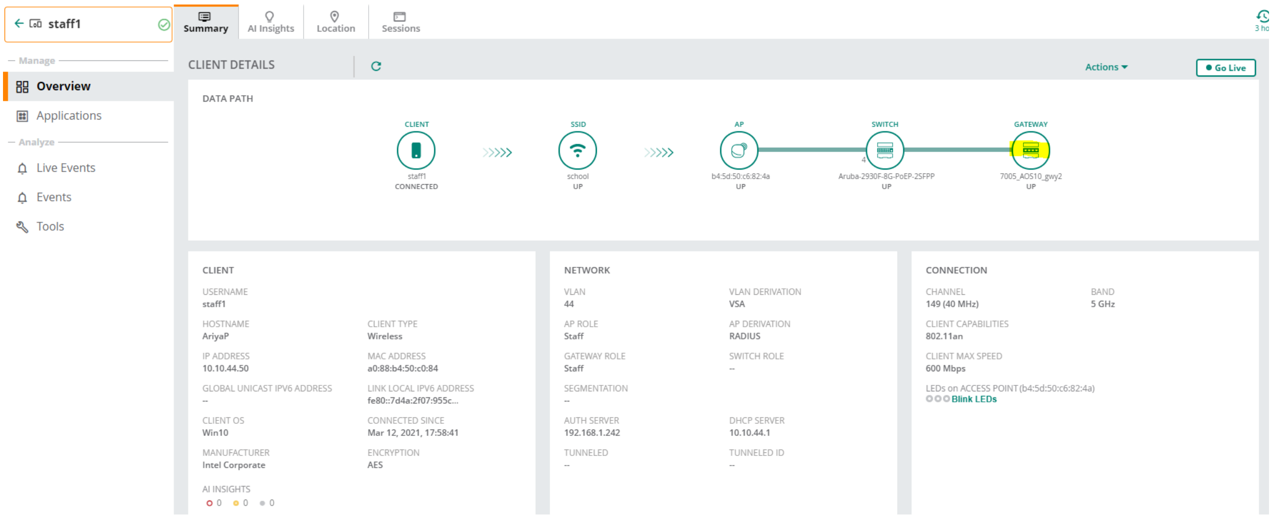
Now looking at Aruba Central pages.



244.08 MB (⊕ 8.04 MB | ⊕ 236.05 MB)

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

Client Name	Status	IP Address	VLAN	Connected To	Gateway Role	SSID/Port	Health	Usage
staff1	Connected	10.10.44.50	44	b4:5d:50:c6:82:4a	Staff	school		244.08 MB



CLIENT

USERNAME
staff1

HOSTNAME
AriyaP

CLIENT TYPE
Wireless

IP ADDRESS
10.10.44.50

MAC ADDRESS
a0:88:b4:50:c0:84

GLOBAL UNICAST IPV6 ADDRESS
--

LINK LOCAL IPV6 ADDRESS
fe80::7d4a:2f07:955c...

CLIENT OS
Win10

CONNECTED SINCE
Mar 12, 2021, 17:58:41

MANUFACTURER
Intel Corporate

ENCRYPTION
AES

AI INSIGHTS
○ 0 ● 0 ● 0

NETWORK

VLAN
44

VLAN DERIVATION
VSA

AP ROLE
Staff

AP DERIVATION
RADIUS

GATEWAY ROLE
Staff

SWITCH ROLE
--

SEGMENTATION
--

AUTH SERVER
192.168.1.242

DHCP SERVER
10.10.44.1

TUNNELED
--

TUNNELED ID
--

CONNECTION

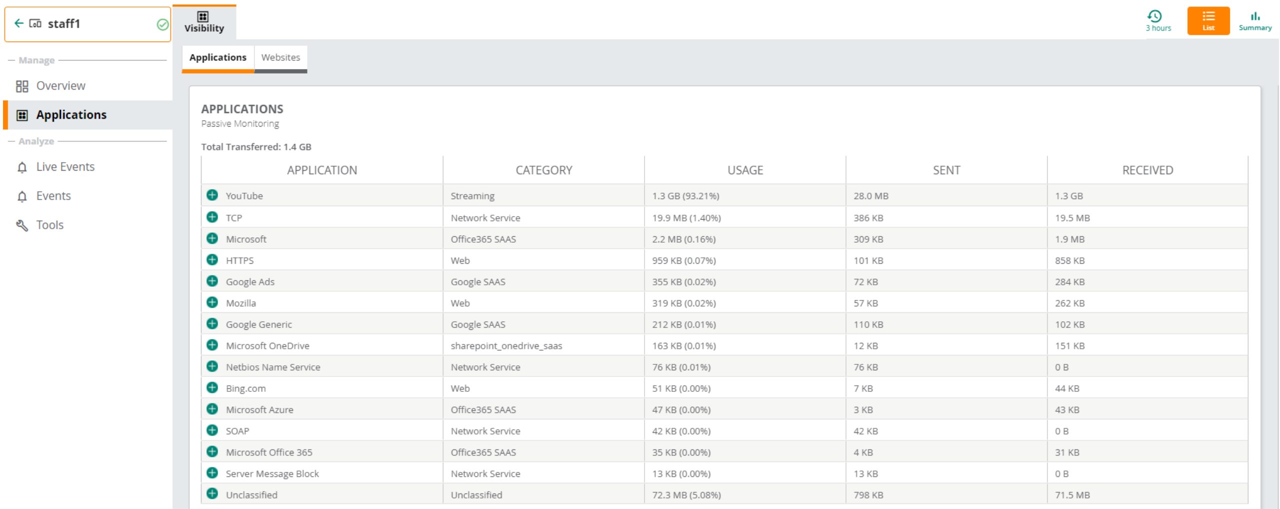
CHANNEL
149 (40 MHz)

BAND
5 GHz

CLIENT CAPABILITIES
802.11an

CLIENT MAX SPEED
600 Mbps

LEDs on ACCESS POINT (b4:5d:50:c6:82:4a)
○○○ Blink LEDs



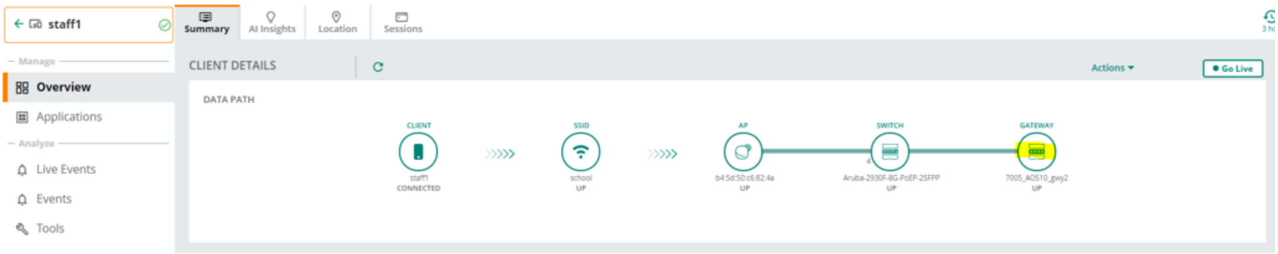
APPLICATIONS

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

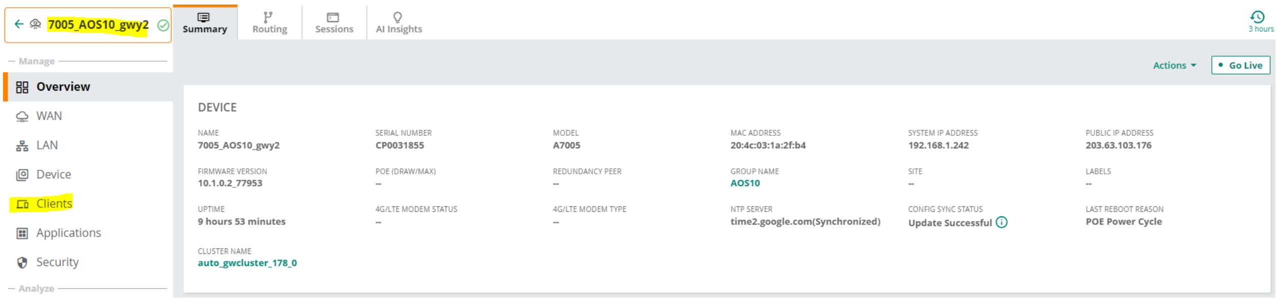
Clicking on the gateway symbol takes us to the gateway that is terminating the user traffic



CLIENT DETAILS

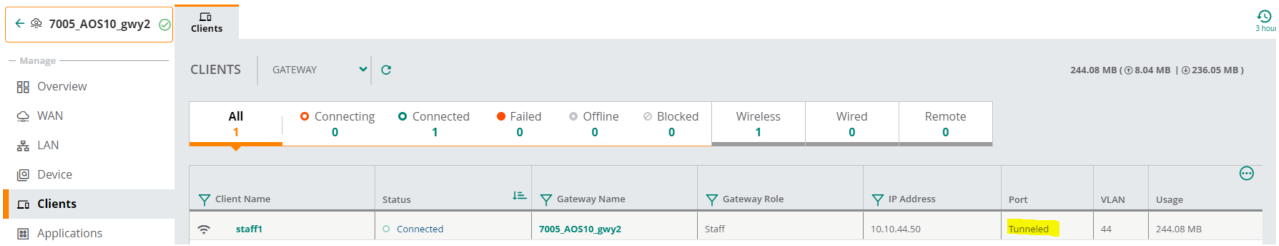
DATA PATH

CLIENT	SSID	AP	SWITCH	GATEWAY
staff1 CONNECTED	school UP	b4:5d:50:c6:82:4a UP	Aruba-2930F-8G-PoEP-2SFPP UP	7005_AOS10_gwy2 UP



DEVICE

NAME	SERIAL NUMBER	MODEL	MAC ADDRESS	SYSTEM IP ADDRESS	PUBLIC IP ADDRESS
7005_AOS10_gwy2	CP0031855	A7005	20:4c:03:1a:2f:b4	192.168.1.242	203.63.103.176
FIRMWARE VERSION	**POE (DRAW/MAX)**	**REDUNDANCY PEER**	**GROUP NAME**	**SITE**	**LABELS**
10.1.0.2_77953	--	--	AOS10	--	--
UPTIME	**4G/LTE MODEM STATUS**	**4G/LTE MODEM TYPE**	**NTP SERVER**	**CONFIG SYNC STATUS**	**LAST REBOOT REASON**
9 hours 53 minutes	--	--	time2.google.com(Synchronized)	Update Successful	POE Power Cycle
CLUSTER NAME					
auto_gwcluster_178_0					



CLIENTS

244.08 MB (8.04 MB | 236.05 MB)

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

	Client Name	Status	Gateway Name	Gateway Role	IP Address	Port	VLAN	Usage
	staff1	Connected	7005_AOS10_gwy2	Staff	10.10.44.50	Tunneled	44	244.08 MB

Now we'll run a few CLI commands.

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

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

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

Num APs:6
Num Associations:2
```

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

Now, checking the IPSEC tunnels from the AP

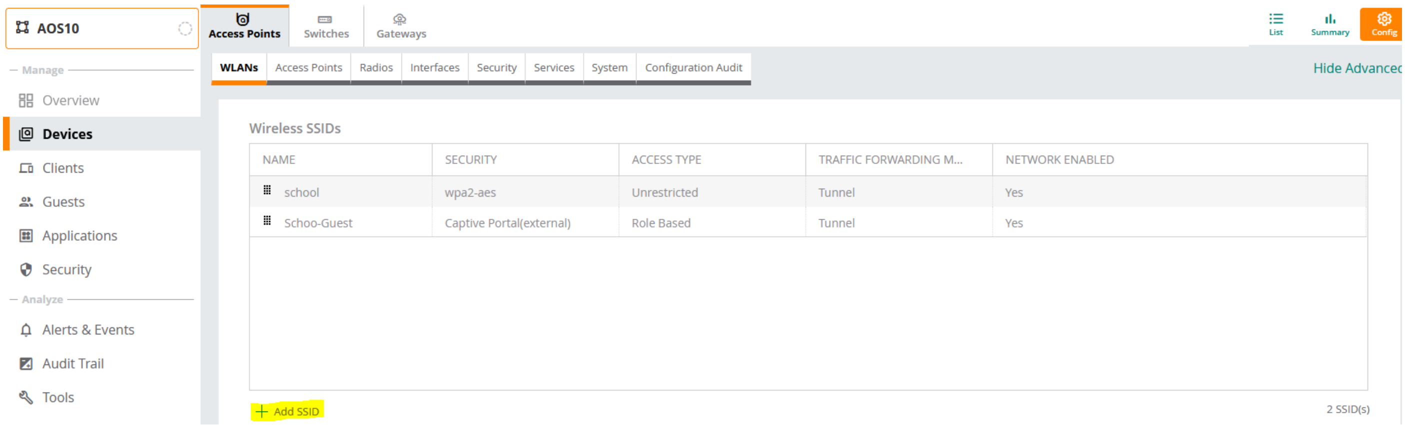
```
b4:5d:50:c6:82:4a# sh ata endpoint

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#
```

6.3 Bridge Mode Wireless Configuration

For this mode we have VLAN 22 which will be set aside for Student that will be connecting to this SSID. The LAN switch that the APs are connected to will have VLAN 22 as tagged as well as providing DHCP service for it.

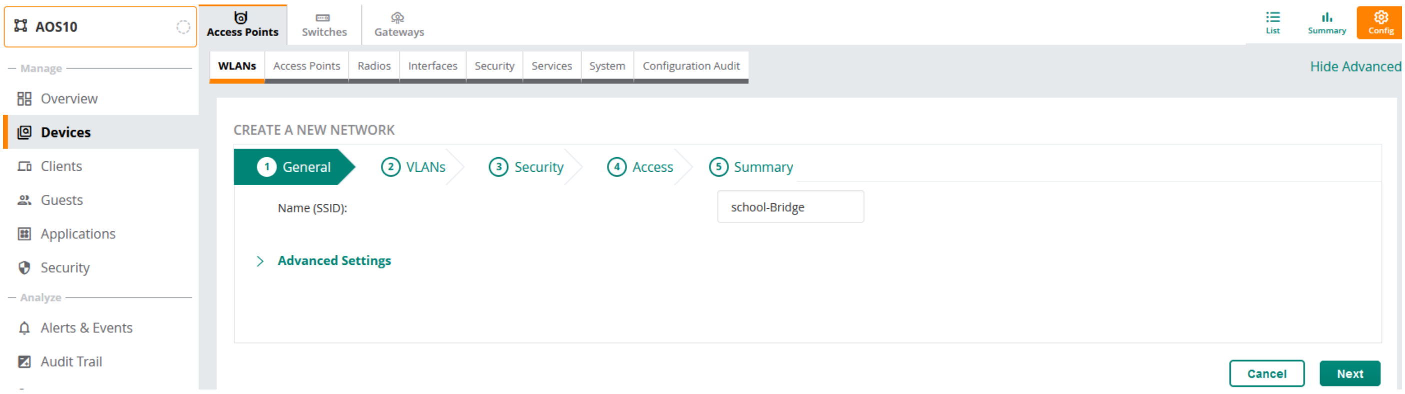
```
!
vlan 22
   name "Student-Bridge-VLAN"
   untagged 2
   tagged 3-4
   ip address 10.10.22.1 255.255.255.0
   dhcp-server
   exit
!
dhcp-server pool "Student-Bridge-VLAN"
   default-router "10.10.22.1"
   dns-server "1.1.1.1"
   lease 00:04:00
   network 10.10.22.0 255.255.255.0
   range 10.10.22.50 10.10.22.59
   exit
!
```

Now, we'll start the configuration of the Bridge mode WLAN.



Wireless SSIDs

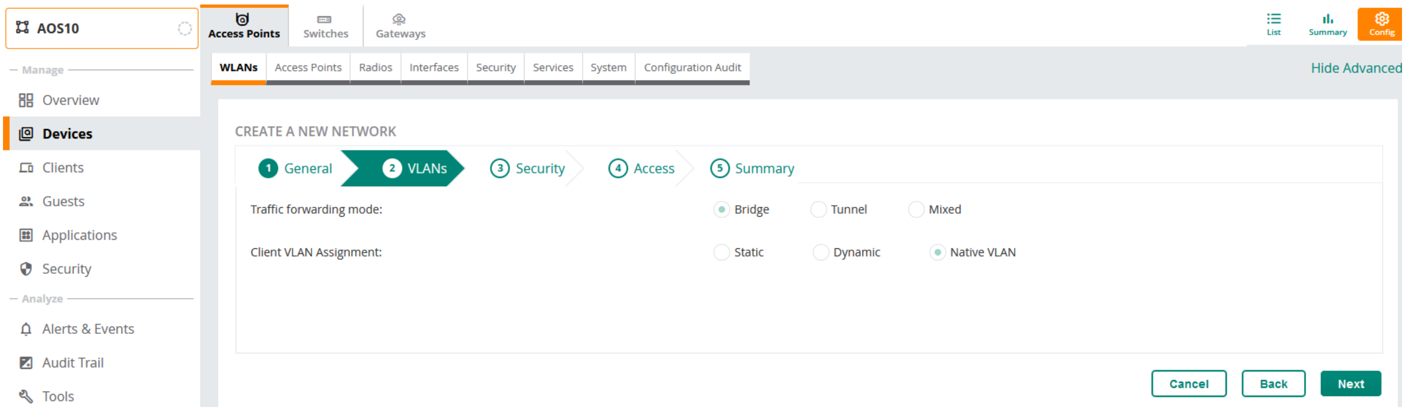
NAME	SECURITY	ACCESS TYPE	TRAFFIC FORWARDING M...	NETWORK ENABLED
school	wpa2-aes	Unrestricted	Tunnel	Yes
Schoo-Guest	Captive Portal(external)	Role Based	Tunnel	Yes



CREATE A NEW NETWORK

Name (SSID): school-Bridge

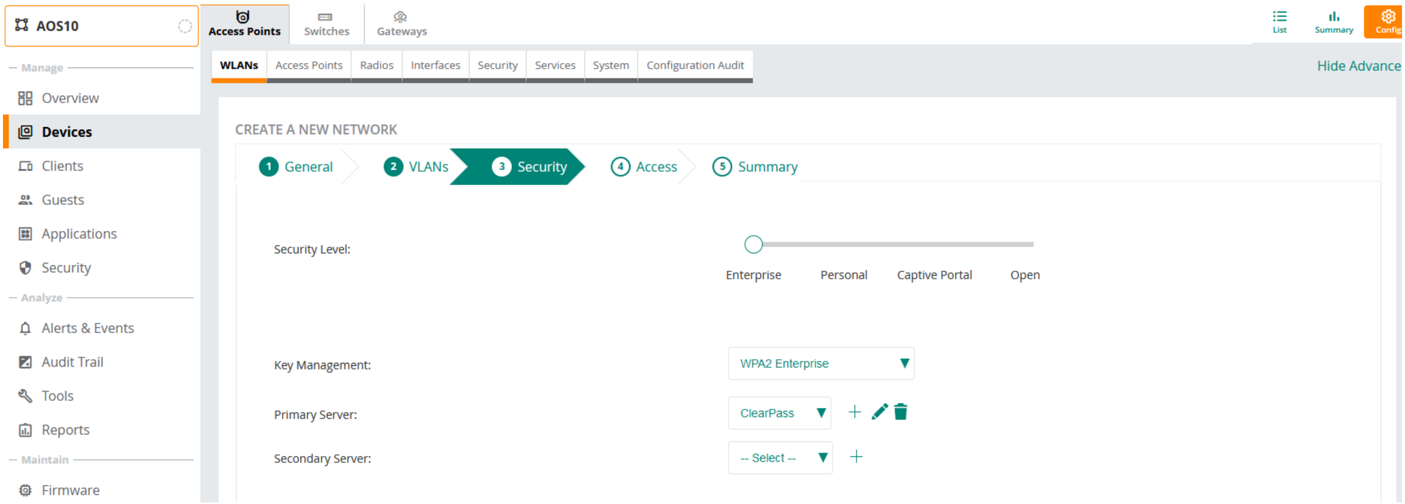
> Advanced Settings



CREATE A NEW NETWORK

Traffic forwarding mode: ● Bridge ○ Tunnel ○ Mixed

Client VLAN Assignment: ○ Static ○ Dynamic ● Native VLAN



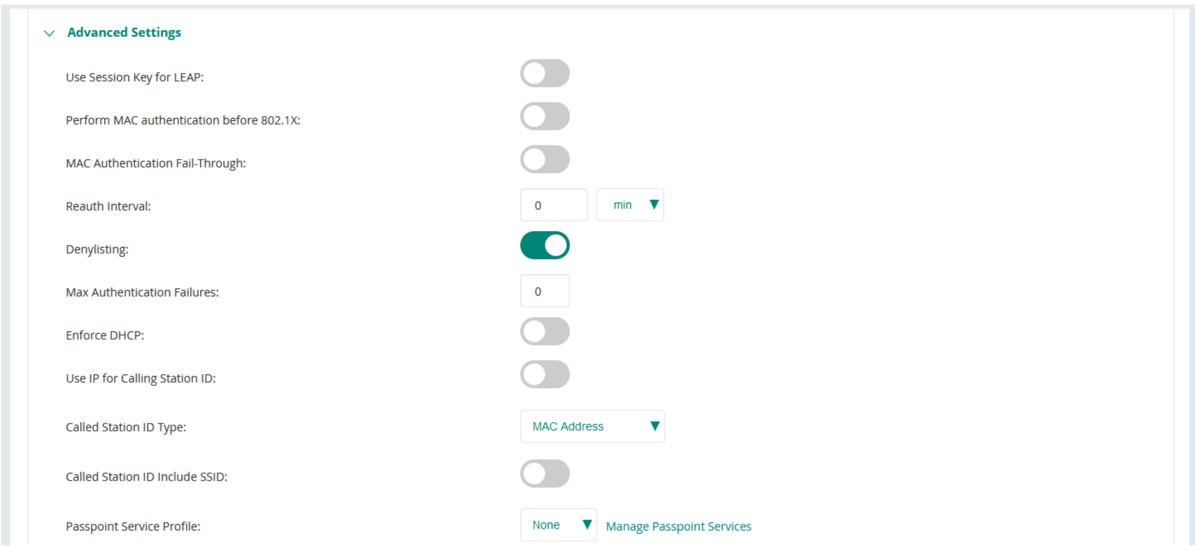
CREATE A NEW NETWORK

Security Level: Enterprise | Personal | Captive Portal | Open

Key Management: WPA2 Enterprise

Primary Server: ClearPass

Secondary Server: -- Select --



Advanced Settings

Use Session Key for LEAP: Off

Perform MAC authentication before 802.1X: Off

MAC Authentication Fail-Through: Off

Reauth Interval: 0 min

Denylisting: On

Max Authentication Failures: 0

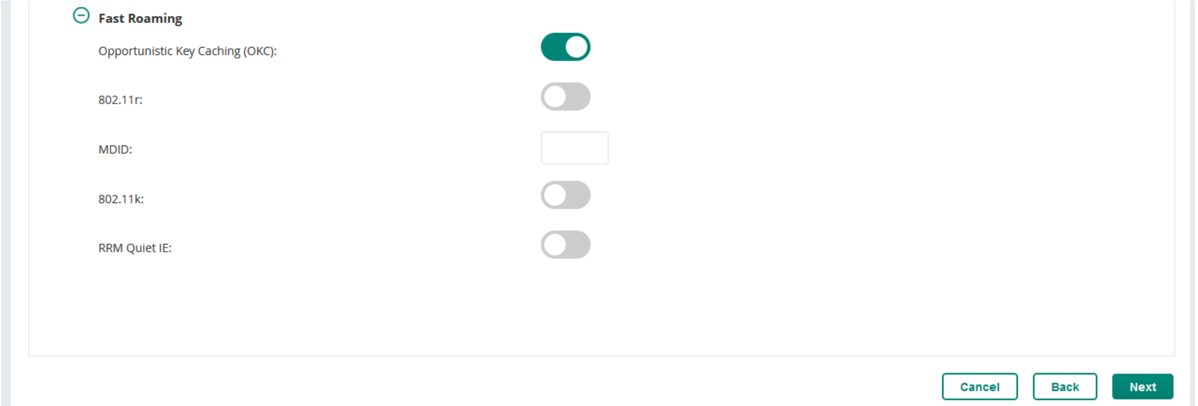
Enforce DHCP: Off

Use IP for Calling Station ID: Off

Called Station ID Type: MAC Address

Called Station ID Include SSID: Off

Passpoint Service Profile: None Manage Passpoint Services



Fast Roaming

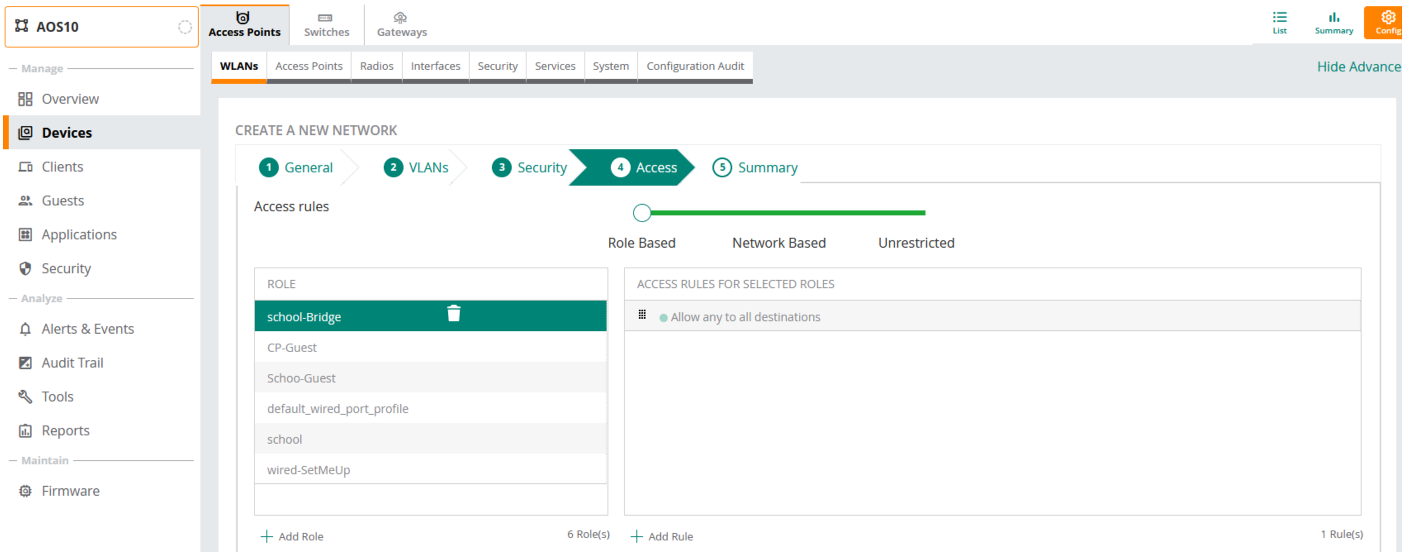
Opportunistic Key Caching (OKC): ● on

802.11r: ○ off

MDID:

802.11k: ○ off

RRM Quiet IE: ○ off



CREATE A NEW NETWORK

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

Access rules

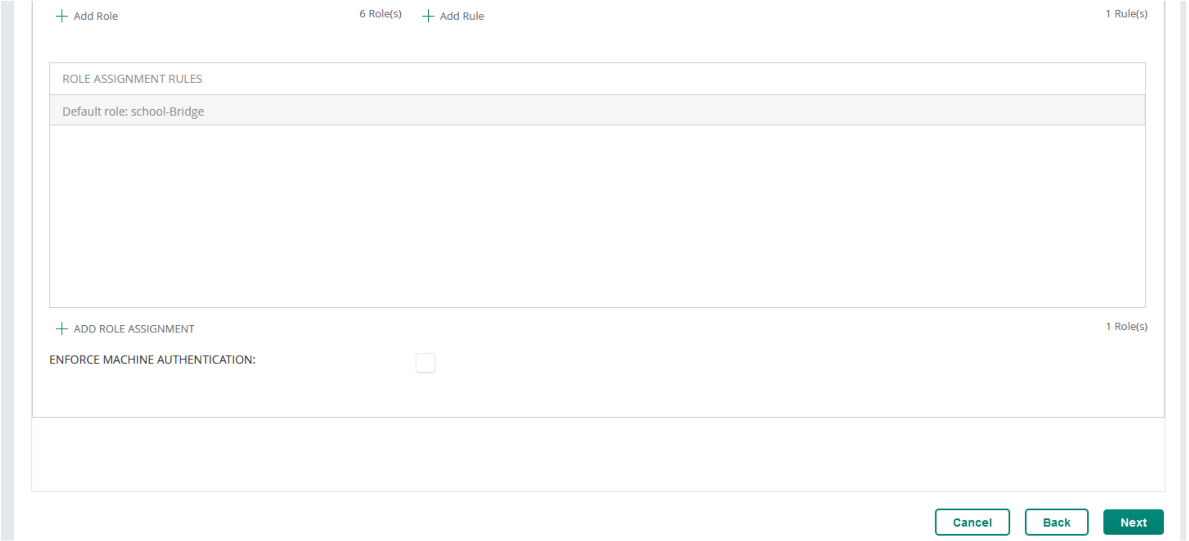
○ Role Based | Network Based | Unrestricted

ROLE
school-Bridge
CP-Guest
Schoo-Guest
default_wired_port_profile
school
wired-SetMeUp

+ Add Role — 6 Role(s)

ACCESS RULES FOR SELECTED ROLES
Allow any to all destinations

+ Add Rule — 1 Rule(s)



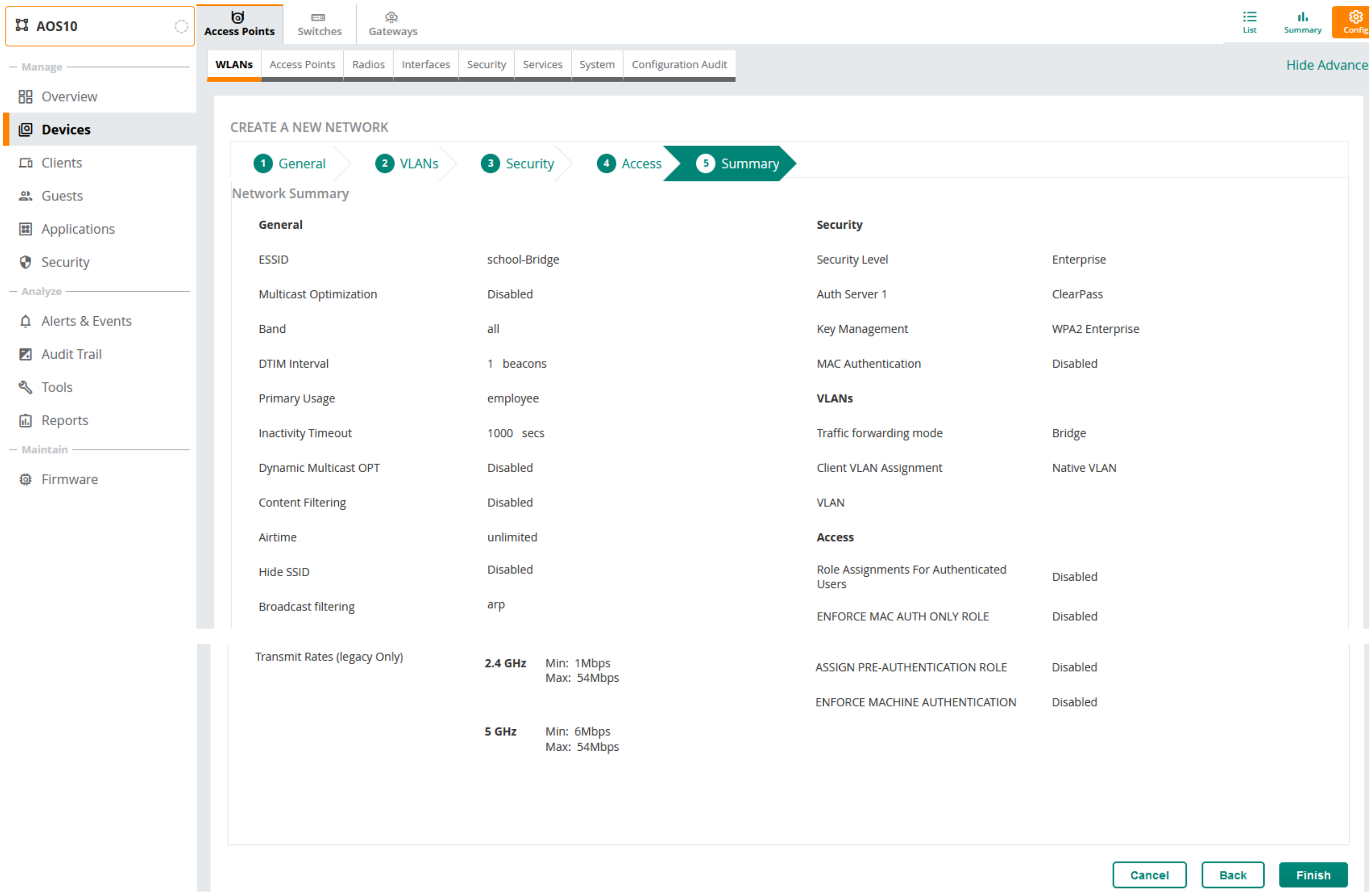
+ Add Role — 6 Role(s)

+ Add Rule — 1 Rule(s)

ROLE ASSIGNMENT RULES
Default role: school-Bridge

+ ADD ROLE ASSIGNMENT — 1 Role(s)

ENFORCE MACHINE AUTHENTICATION: □

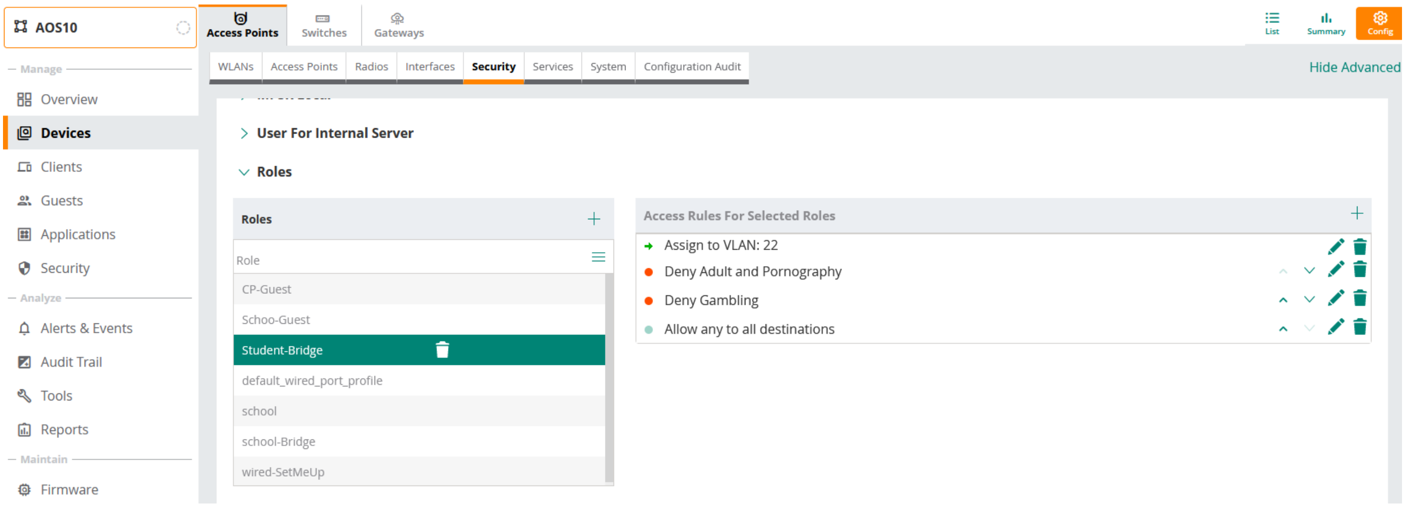


CREATE A NEW NETWORK

Network Summary

General		Security	
ESSID	school-Bridge	Security Level	Enterprise
Multicast Optimization	Disabled	Auth Server 1	ClearPass
Band	all	Key Management	WPA2 Enterprise
DTIM Interval	1 beacons	MAC Authentication	Disabled
Primary Usage	employee	**VLANs**	
Inactivity Timeout	1000 secs	Traffic forwarding mode	Bridge
Dynamic Multicast OPT	Disabled	Client VLAN Assignment	Native VLAN
Content Filtering	Disabled	VLAN	
Airtime	unlimited	**Access**	
Hide SSID	Disabled	Role Assignments For Authenticated Users	Disabled
Broadcast filtering	arp	ENFORCE MAC AUTH ONLY ROLE	Disabled
Transmit Rates (legacy Only)	2.4 GHz Min: 1Mbps Max: 54Mbps	ASSIGN PRE-AUTHENTICATION ROLE	Disabled
		ENFORCE MACHINE AUTHENTICATION	Disabled
	5 GHz Min: 6Mbps Max: 54Mbps		

Now since we are planning to send back user-role “Student-Bridge” from ClearPass, we’ll create a local user at the group level for the AOS10 APs.



User For Internal Server

Roles

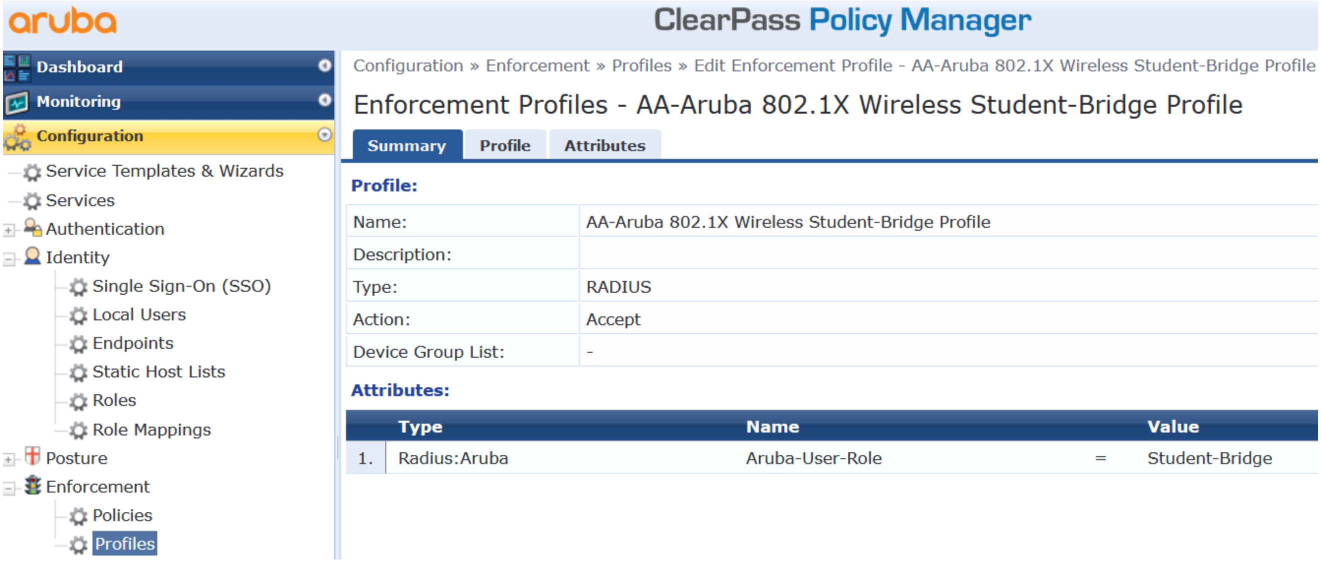
Roles
Role
CP-Guest
Schoo-Guest
Student-Bridge
default_wired_port_profile
school
school-Bridge
wired-SetMeUp

Access Rules For Selected Roles

- Assign to VLAN: 22
- Deny Adult and Pornography
- Deny Gambling
- Allow any to all destinations

6.4 ClearPass Service Modifications

I am planning to use the same ClearPass dot1x service that was used for tunnelled mode WLAN. So, I’ll just need a specific enforcement profile for the bridge mode to send back the user-role and then I’ll modify the service.



Configuration » Enforcement » Profiles » Edit Enforcement Profile - AA-Aruba 802.1X Wireless Student-Bridge Profile

Enforcement Profiles - AA-Aruba 802.1X Wireless Student-Bridge Profile

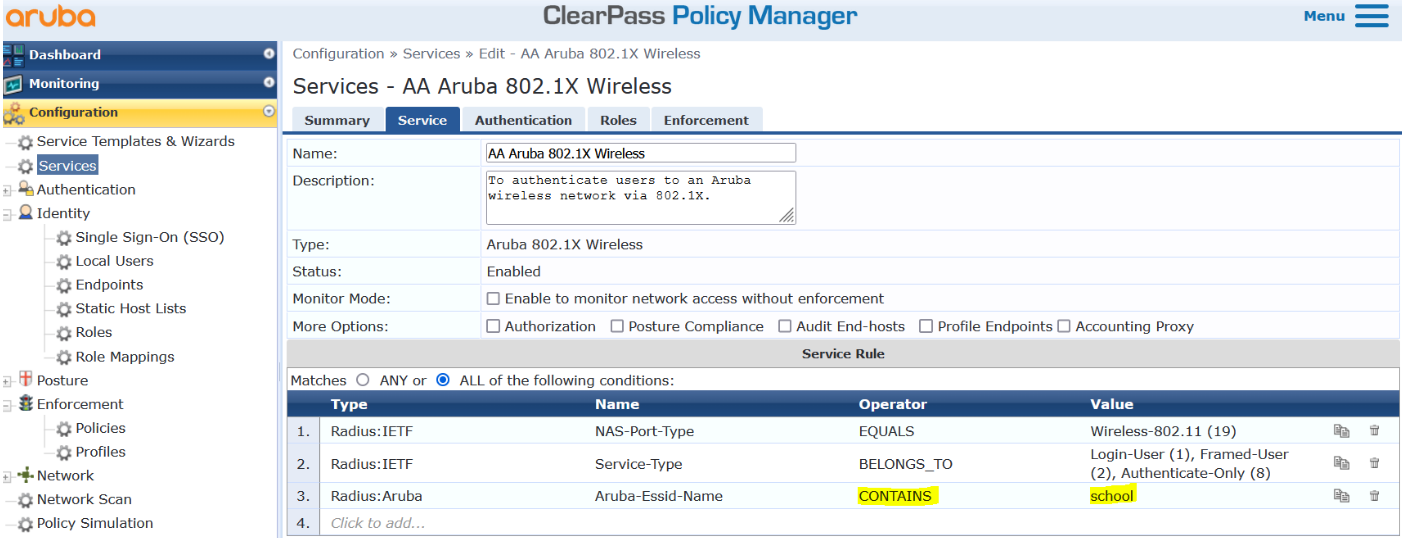
Profile:

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

Attributes:

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

Now, I'll just change the service rule for matching the ESSID name.



Configuration » Services » Edit - AA Aruba 802.1X Wireless

Services - AA Aruba 802.1X Wireless

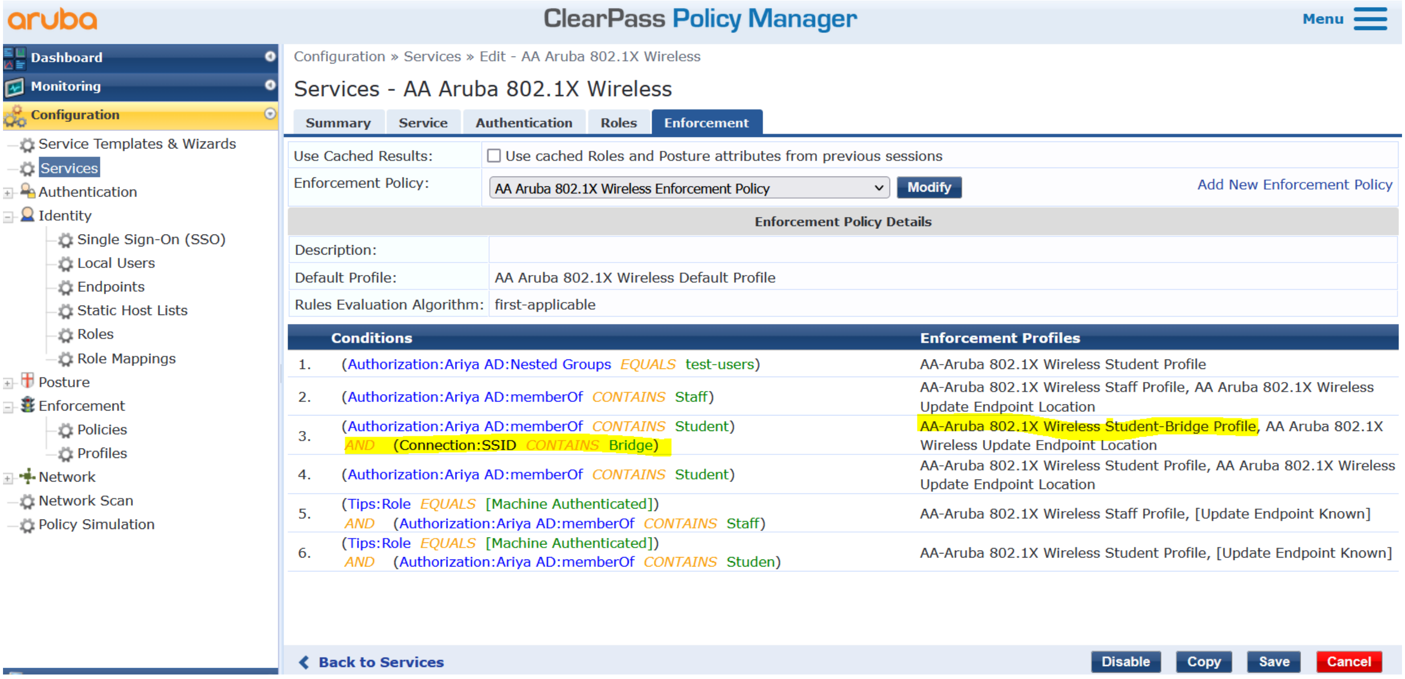
Name:	AA Aruba 802.1X Wireless
Description:	To authenticate users to an Aruba wireless network via 802.1X.
Type:	Aruba 802.1X Wireless
Status:	Enabled
Monitor Mode:	☐ Enable to monitor network access without enforcement
More Options:	☐ Authorization ☐ Posture Compliance ☐ Audit End-hosts ☐ Profile Endpoints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

And add a logic in the enforcement policy.



Configuration » Services » Edit - AA Aruba 802.1X Wireless

Services - AA Aruba 802.1X Wireless

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

Enforcement Policy Details

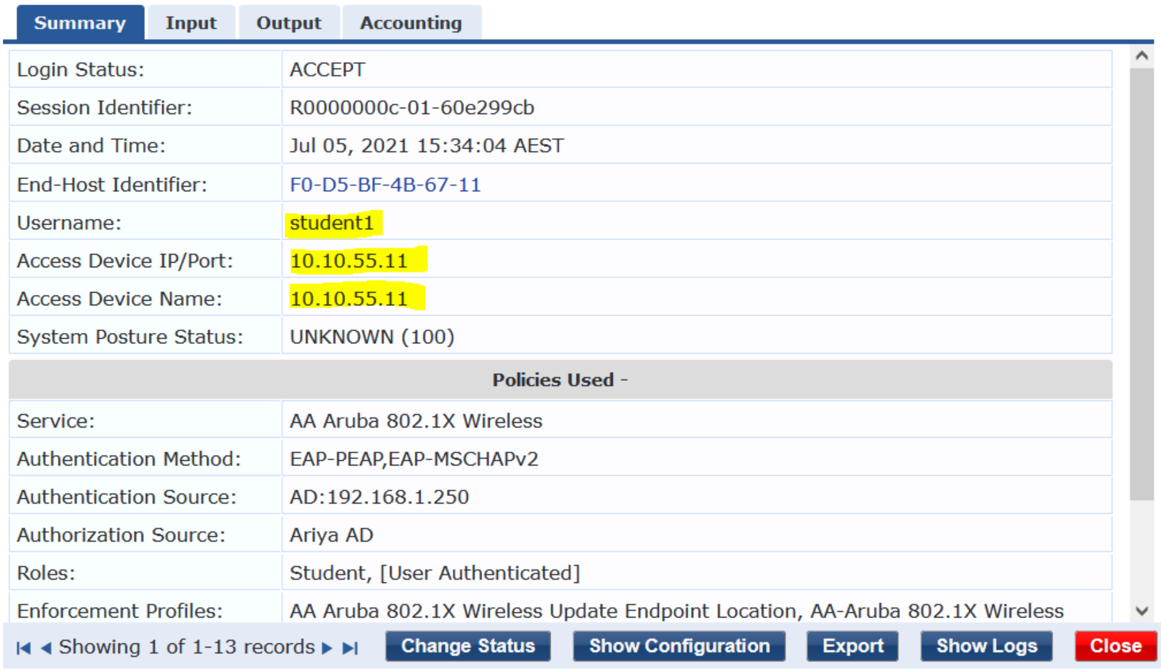
Description:	
Default Profile:	AA Aruba 802.1X Wireless Default Profile
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:Ariya AD:Nested Groups EQUALS test-users)	AA-Aruba 802.1X Wireless Student Profile
2.	(Authorization:Ariya AD:memberOf CONTAINS Staff)	AA-Aruba 802.1X Wireless Staff Profile, AA Aruba 802.1X Wireless Update Endpoint Location
3.	(Authorization:Ariya AD:memberOf CONTAINS Student) AND (Connection:SSID CONTAINS Bridge)	AA-Aruba 802.1X Wireless Student-Bridge Profile, AA Aruba 802.1X Wireless Update Endpoint Location
4.	(Authorization:Ariya AD:memberOf CONTAINS Student)	AA-Aruba 802.1X Wireless Student Profile, AA Aruba 802.1X Wireless Update Endpoint Location
5.	(Tips:Role EQUALS [Machine Authenticated]) AND (Authorization:Ariya AD:memberOf CONTAINS Staff)	AA-Aruba 802.1X Wireless Staff Profile, [Update Endpoint Known]
6.	(Tips:Role EQUALS [Machine Authenticated]) AND (Authorization:Ariya AD:memberOf CONTAINS Studen)	AA-Aruba 802.1X Wireless Student Profile, [Update Endpoint Known]

Now we are ready to test.

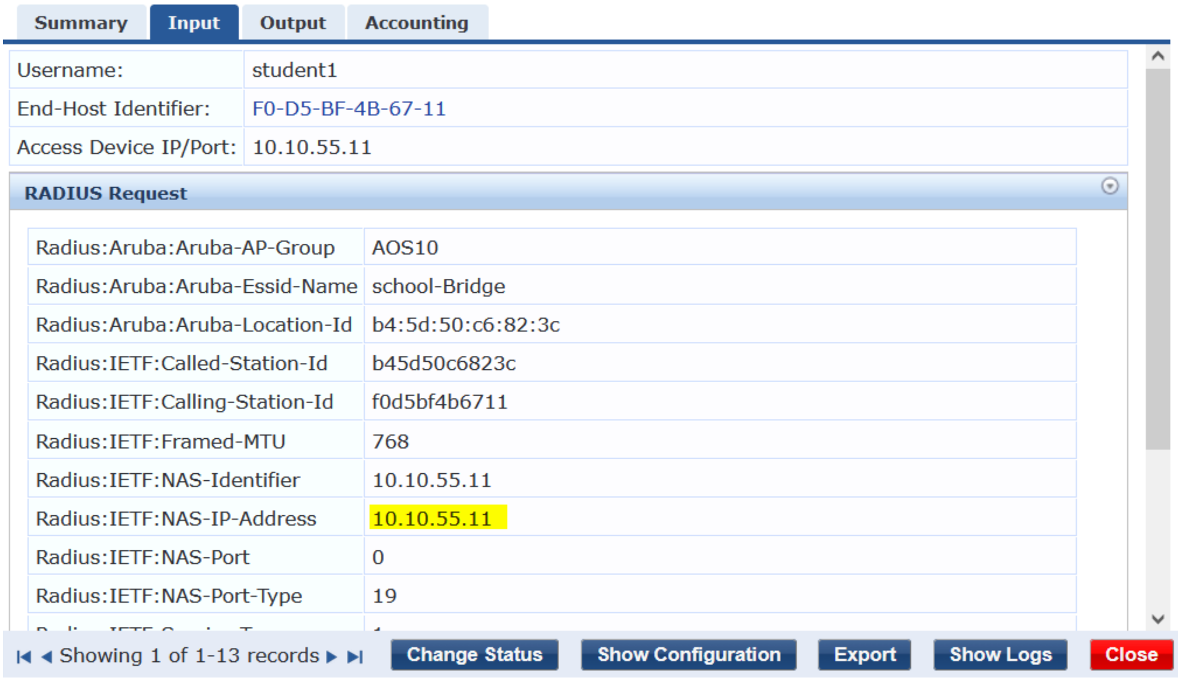
6.5 Bridge Mode Wireless dot1x Testing

Here are the access tracker screenshots.



Login Status:	ACCEPT
Session Identifier:	R0000000c-01-60e299cb
Date and Time:	Jul 05, 2021 15:34:04 AEST
End-Host Identifier:	F0-D5-BF-4B-67-11
Username:	student1
Access Device IP/Port:	10.10.55.11
Access Device Name:	10.10.55.11
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:	Student, [User Authenticated]
Enforcement Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless

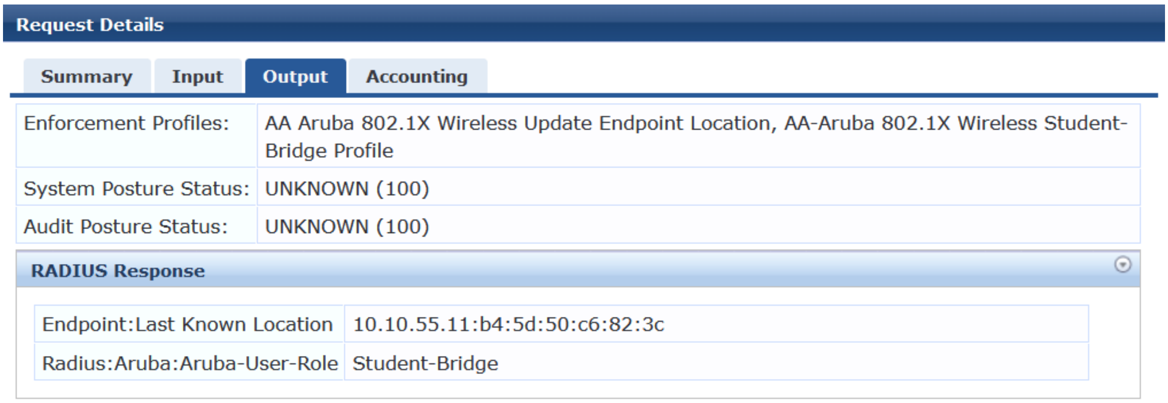
Note that the RADIUS authentication is coming directly for the AP's IP addresses.



Username:	student1
End-Host Identifier:	F0-D5-BF-4B-67-11
Access Device IP/Port:	10.10.55.11

RADIUS Request

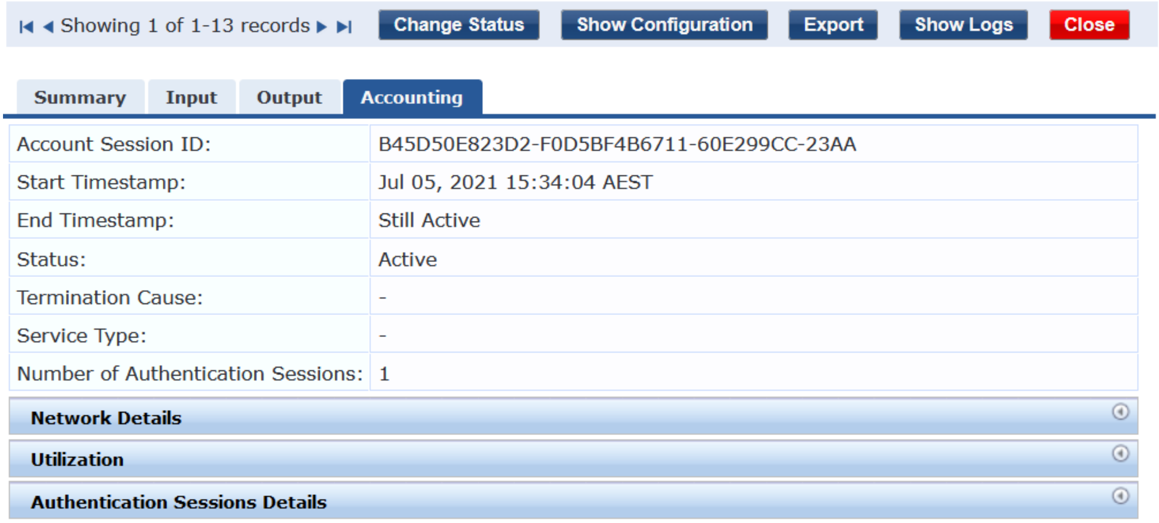
Radius:Aruba:Aruba-AP-Group	AOS10
Radius:Aruba:Aruba-Essid-Name	school-Bridge
Radius:Aruba:Aruba-Location-Id	b4:5d:50:c6:82:3c
Radius:IETF:Called-Station-Id	b45d50c6823c
Radius:IETF:Calling-Station-Id	f0d5bf4b6711
Radius:IETF:Framed-MTU	768
Radius:IETF:NAS-Identifier	10.10.55.11
Radius:IETF:NAS-IP-Address	10.10.55.11
Radius:IETF:NAS-Port	0
Radius:IETF:NAS-Port-Type	19



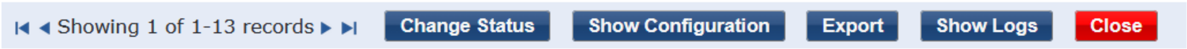
Enforcement Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless Student-Bridge Profile
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

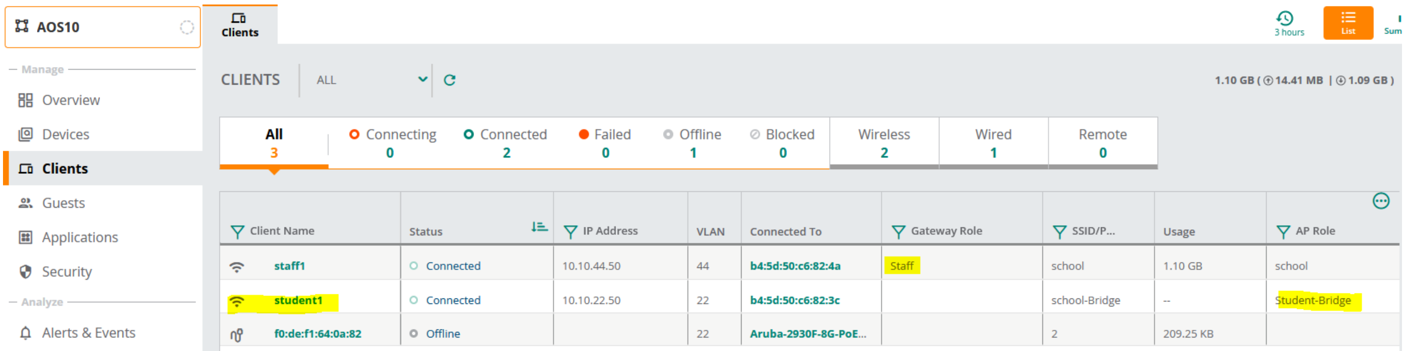
Endpoint:Last Known Location	10.10.55.11:b4:5d:50:c6:82:3c
Radius:Aruba:Aruba-User-Role	Student-Bridge



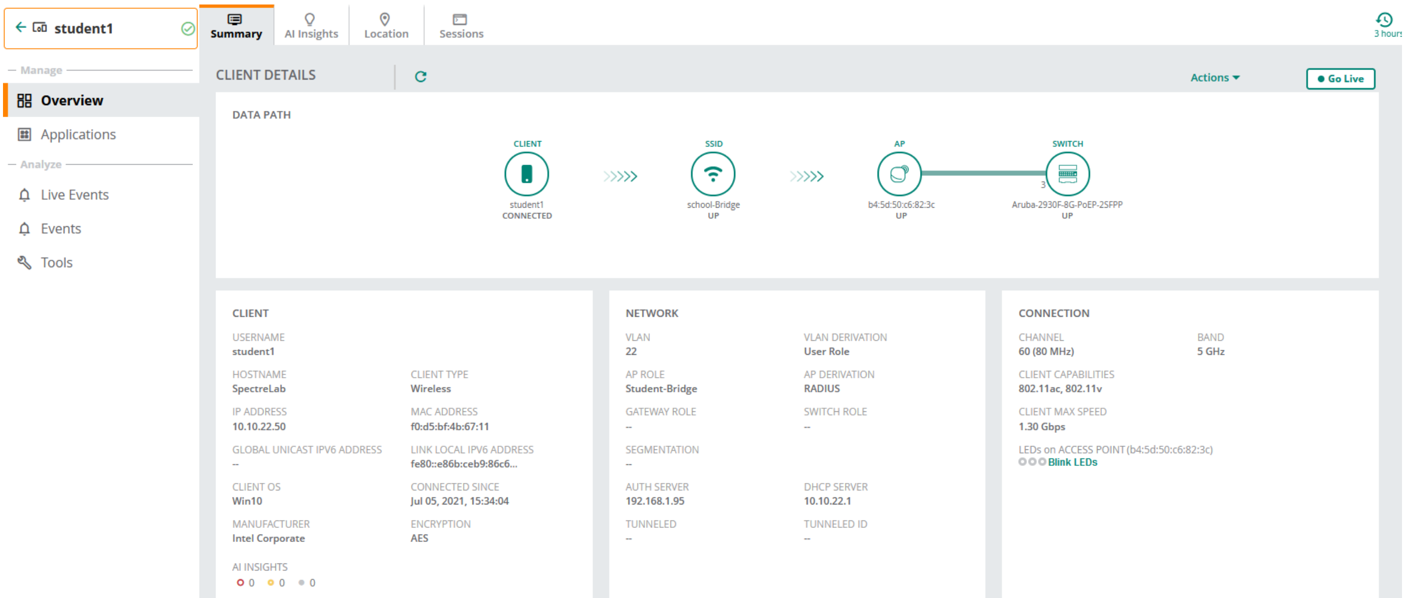
Account Session ID:	B45D50E823D2-F0D5BF4B6711-60E299CC-23AA
Start Timestamp:	Jul 05, 2021 15:34:04 AEST
End Timestamp:	Still Active
Status:	Active
Termination Cause:	-
Service Type:	-
Number of Authentication Sessions:	1



Checking Aruba Central side.



Client Name	Status	IP Address	VLAN	Connected To	Gateway Role	SSID/P...	Usage	AP Role
staff1	Connected	10.10.44.50	44	b4:5d:50:c6:82:4a	Staff	school	1.10 GB	school
student1	Connected	10.10.22.50	22	b4:5d:50:c6:82:3c		school-Bridge	--	Student-Bridge
f0:de:f1:64:0a:82	Offline		22	Aruba-2930F-8G-PoE...		2	209.25 KB	



CLIENT

USERNAME
student1

HOSTNAME
SpectreLab

CLIENT TYPE
Wireless

IP ADDRESS
10.10.22.50

MAC ADDRESS
f0:d5:bf:4b:67:11

GLOBAL UNICAST IPV6 ADDRESS
--

LINK LOCAL IPV6 ADDRESS
fe80::e86b:ceb9:86c6...

CLIENT OS
Win10

CONNECTED SINCE
Jul 05, 2021, 15:34:04

MANUFACTURER
Intel Corporate

ENCRYPTION
AES

AI INSIGHTS
○ 0 ● 0 ● 0

NETWORK

VLAN
22

VLAN DERIVATION
User Role

AP ROLE
Student-Bridge

AP DERIVATION
RADIUS

GATEWAY ROLE
--

SWITCH ROLE
--

SEGMENTATION
--

AUTH SERVER
192.168.1.95

DHCP SERVER
10.10.22.1

TUNNELED
--

TUNNELED ID
--

CONNECTION

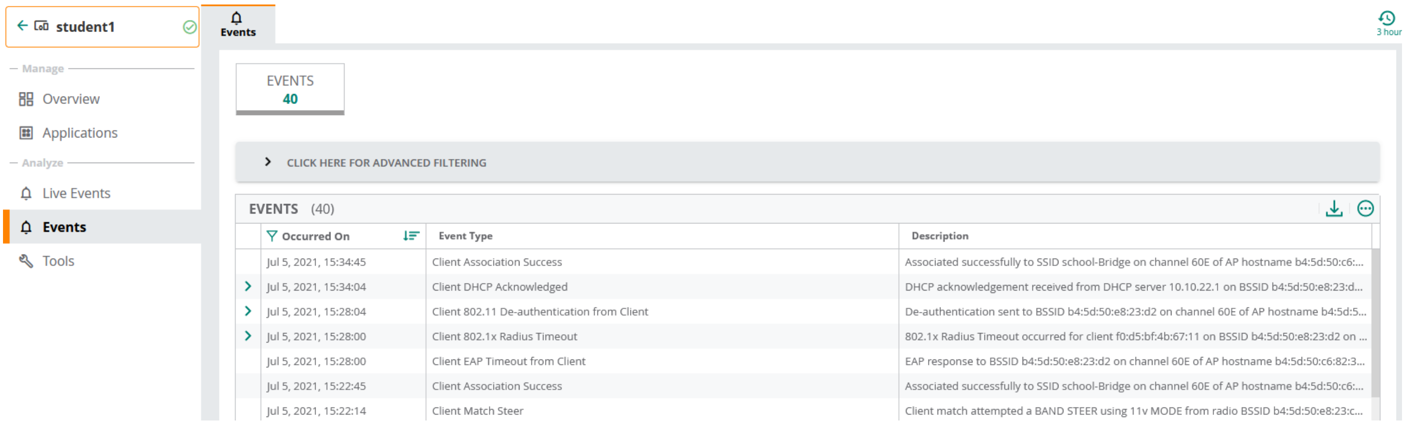
CHANNEL
60 (80 MHz)

BAND
5 GHz

CLIENT CAPABILITIES
802.11ac, 802.11v

CLIENT MAX SPEED
1.30 Gbps

LEDs on ACCESS POINT (b4:5d:50:c6:82:3c)
○○○ Blink LEDs



EVENTS (40)

Occurred On	Event Type	Description
Jul 5, 2021, 15:34:45	Client Association Success	Associated successfully to SSID school-Bridge on channel 60E of AP hostname b4:5d:50:c6:...
Jul 5, 2021, 15:34:04	Client DHCP Acknowledged	DHCP acknowledgement received from DHCP server 10.10.22.1 on BSSID b4:5d:50:e8:23:d...
Jul 5, 2021, 15:28:04	Client 802.11 De-authentication from Client	De-authentication sent to BSSID b4:5d:50:e8:23:d2 on channel 60E of AP hostname b4:5d:5...
Jul 5, 2021, 15:28:00	Client 802.1x Radius Timeout	802.1x Radius Timeout occurred for client f0:d5:bf:4b:67:11 on BSSID b4:5d:50:e8:23:d2 on ...
Jul 5, 2021, 15:28:00	Client EAP Timeout from Client	EAP response to BSSID b4:5d:50:e8:23:d2 on channel 60E of AP hostname b4:5d:50:c6:82:3...
Jul 5, 2021, 15:22:45	Client Association Success	Associated successfully to SSID school-Bridge on channel 60E of AP hostname b4:5d:50:c6:...
Jul 5, 2021, 15:22:14	Client Match Steer	Client match attempted a BAND STEER using 11v MODE from radio BSSID b4:5d:50:e8:23:c...

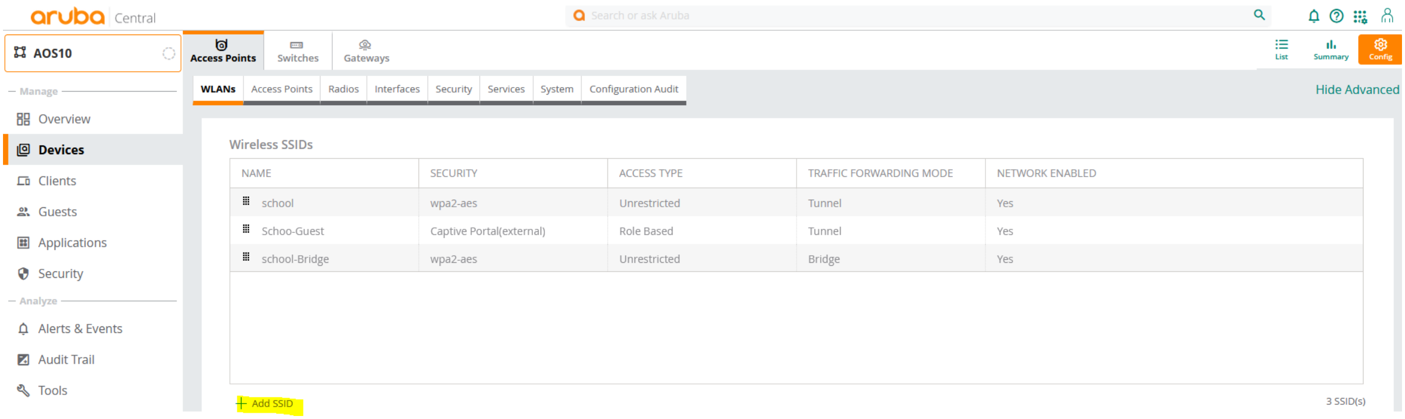
6.6 Mixed Mode Wireless Configuration

In this mode for the same SSID allows both bridging of the user traffic as well as tunnelling it to a cluster of gateways based on the attributes it receives by the RADIUS server. It should be noted that currently mixed Mode SSID is only supported for 802.1X authentication.

We'll be making use of Server Derivation Rule (SDR) to decide which user role that ClearPass sends will be bridged.

In mixed mode the default VLAN is a tunnel VLAN. So, a bridged mode Rule must be defined.

Now we'll start the configuration of the mixed mode WLAN.

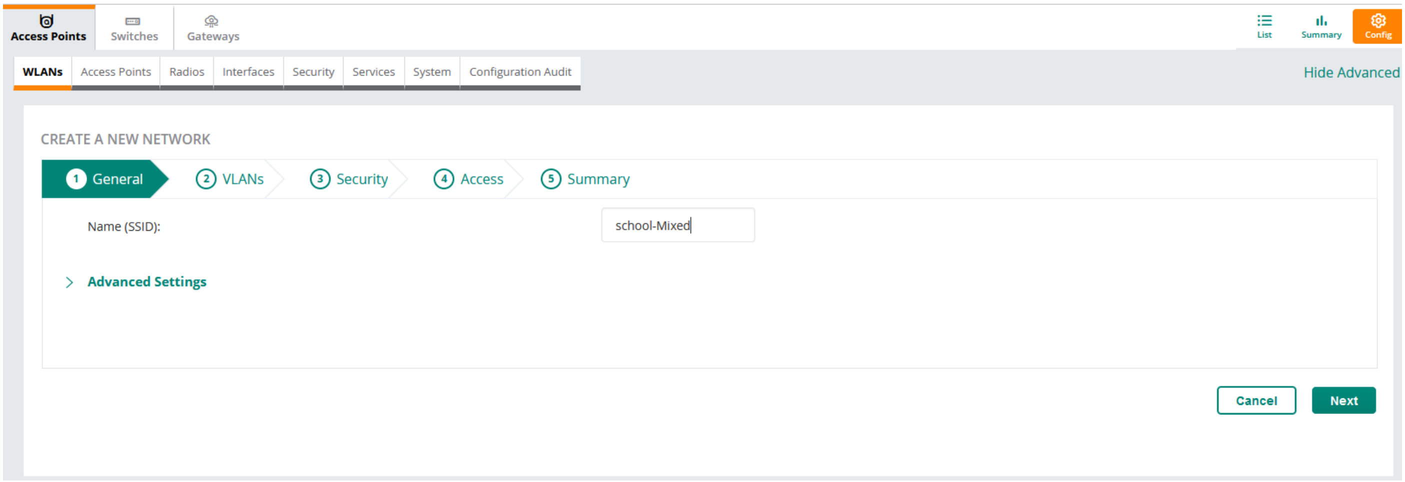


Wireless SSIDs

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

+ Add SSID

3 SSID(s)



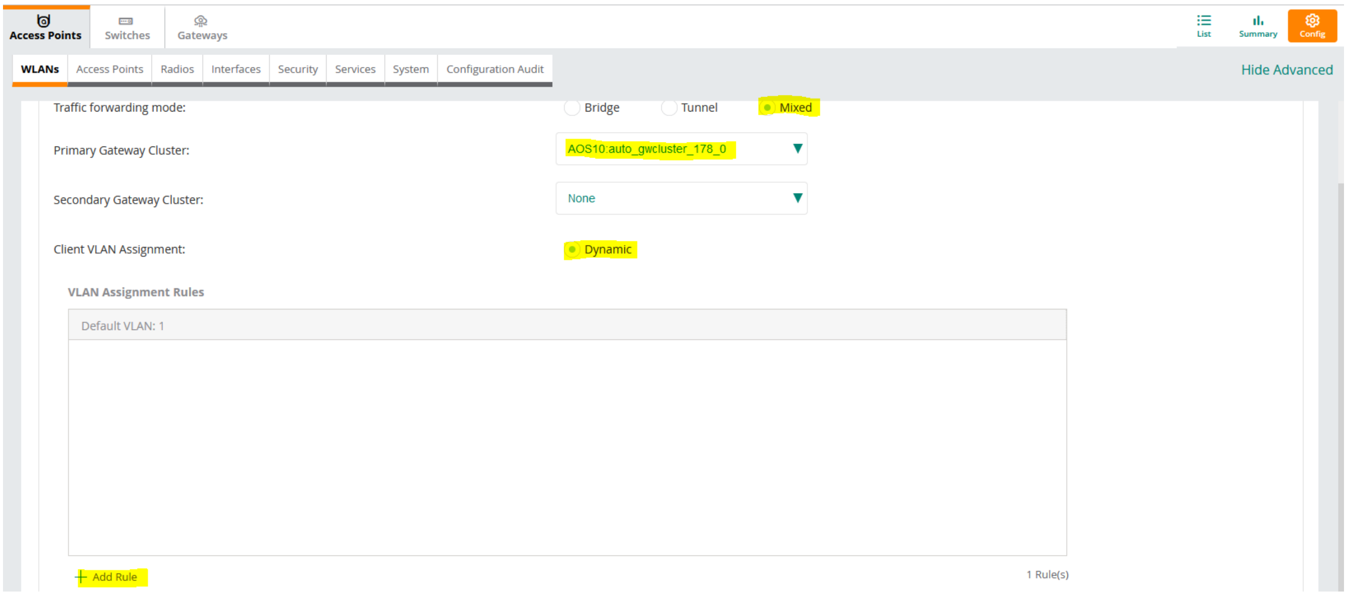
CREATE A NEW NETWORK

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

Name (SSID): school-Mixed

> Advanced Settings

Cancel | Next



Traffic forwarding mode: ○ Bridge ○ Tunnel ● Mixed

Primary Gateway Cluster: AOS10:auto_gwcluster_178_0

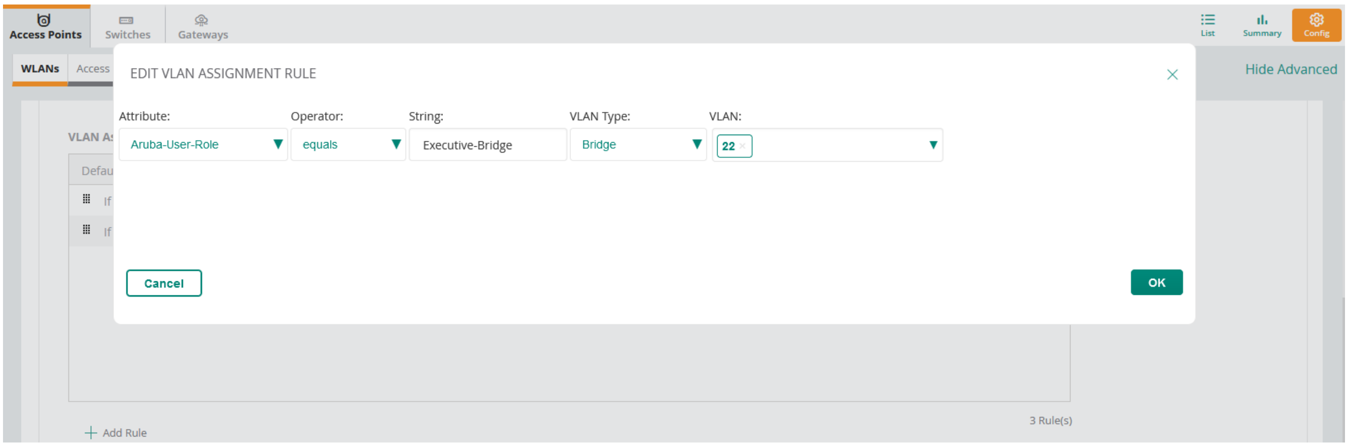
Secondary Gateway Cluster: None

Client VLAN Assignment: ● Dynamic

VLAN Assignment Rules

Default VLAN: 1

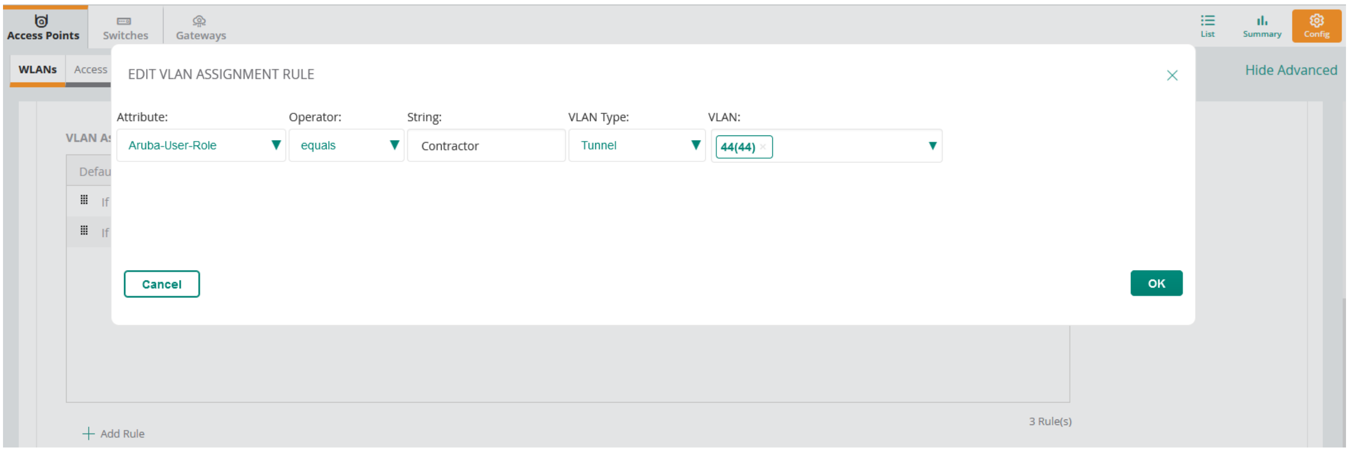
1 Rule(s)



EDIT VLAN ASSIGNMENT RULE

Attribute:	Operator:	String:	VLAN Type:	VLAN:
Aruba-User-Role	equals	Executive-Bridge	Bridge	22

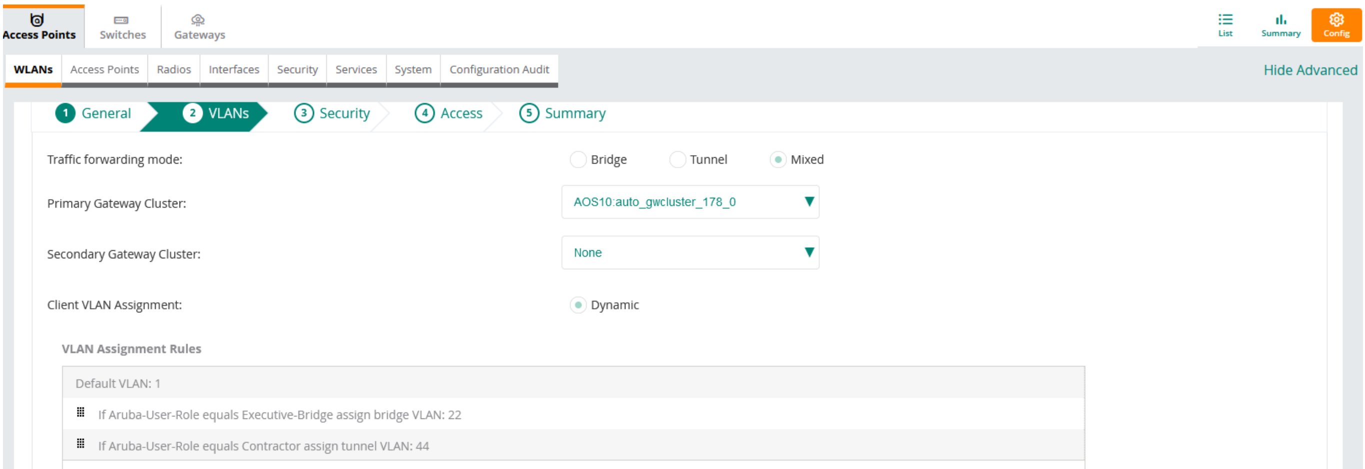
3 Rule(s)



EDIT VLAN ASSIGNMENT RULE

Attribute:	Operator:	String:	VLAN Type:	VLAN:
Aruba-User-Role	equals	Contractor	Tunnel	44(44)

3 Rule(s)



Traffic forwarding mode: ○ Bridge ○ Tunnel ● Mixed

Primary Gateway Cluster: AOS10:auto_gwcluster_178_0

Secondary Gateway Cluster: None

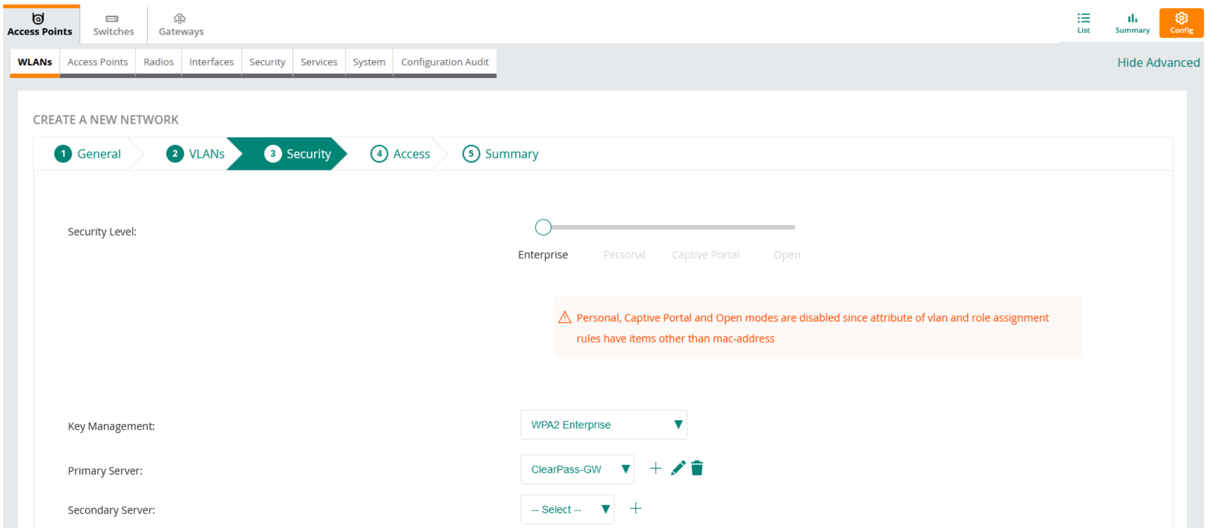
Client VLAN Assignment: ● Dynamic

VLAN Assignment Rules

Default VLAN: 1

If Aruba-User-Role equals Executive-Bridge assign bridge VLAN: 22

If Aruba-User-Role equals Contractor assign tunnel VLAN: 44



CREATE A NEW NETWORK

1 General 2 VLANs 3 Security 4 Access 5 Summary

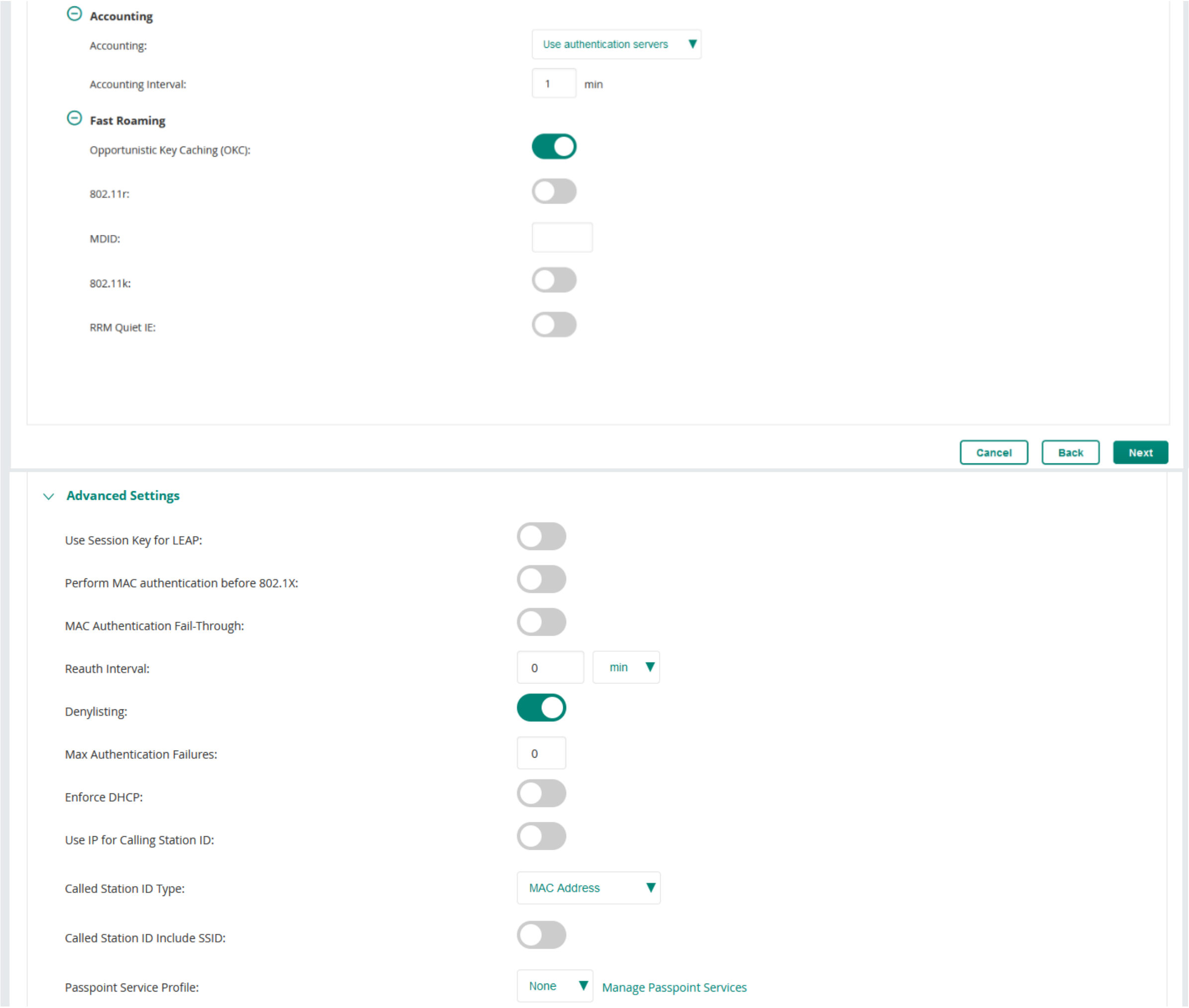
Security Level: Enterprise | Personal | Captive Portal | Open

⚠ Personal, Captive Portal and Open modes are disabled since attribute of vlan and role assignment rules have items other than mac-address

Key Management: WPA2 Enterprise

Primary Server: ClearPass-GW

Secondary Server: -- Select --



⊖ **Accounting**

Accounting: Use authentication servers

Accounting Interval: 1 min

⊖ **Fast Roaming**

Opportunistic Key Caching (OKC): ●

802.11r: ○

MDID:

802.11k: ○

RRM Quiet IE: ○

Advanced Settings

Use Session Key for LEAP: ○

Perform MAC authentication before 802.1X: ○

MAC Authentication Fail-Through: ○

Reauth Interval: 0 min

Denylisting: ●

Max Authentication Failures: 0

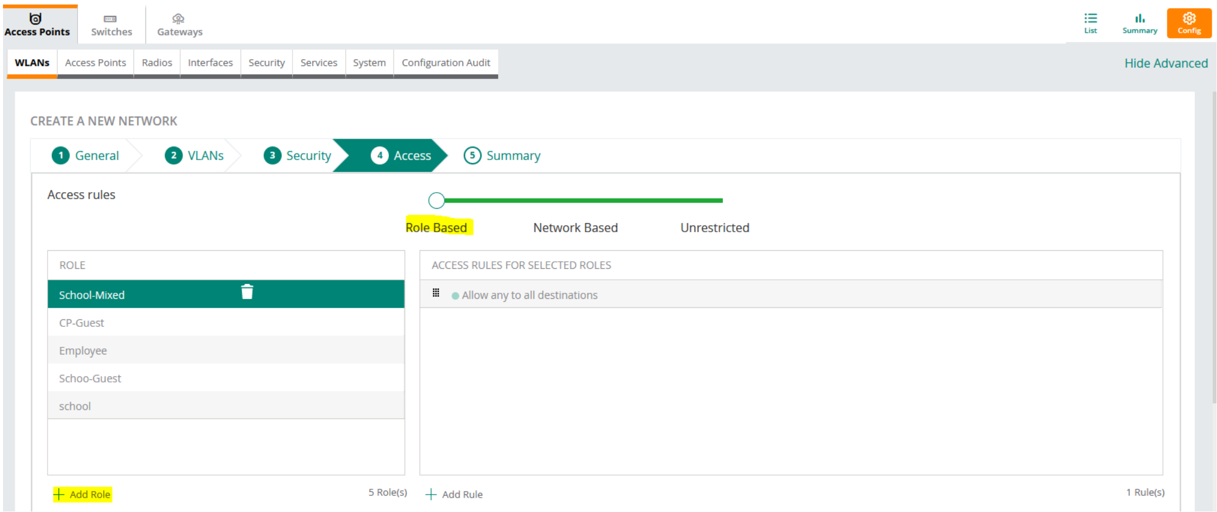
Enforce DHCP: ○

Use IP for Calling Station ID: ○

Called Station ID Type: MAC Address

Called Station ID Include SSID: ○

Passpoint Service Profile: None Manage Passpoint Services



CREATE A NEW NETWORK

1 General 2 VLANs 3 Security 4 Access 5 Summary

Access rules

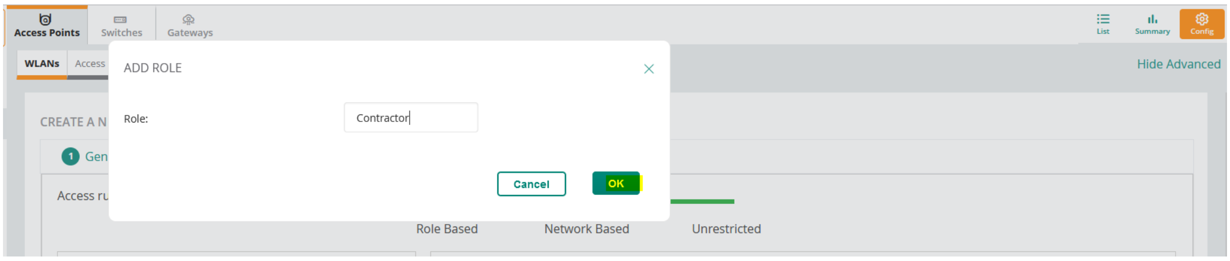
Role Based | Network Based | Unrestricted

ROLE
School-Mixed
CP-Guest
Employee
Schoo-Guest
school

+ Add Role 5 Role(s)

ACCESS RULES FOR SELECTED ROLES
Allow any to all destinations

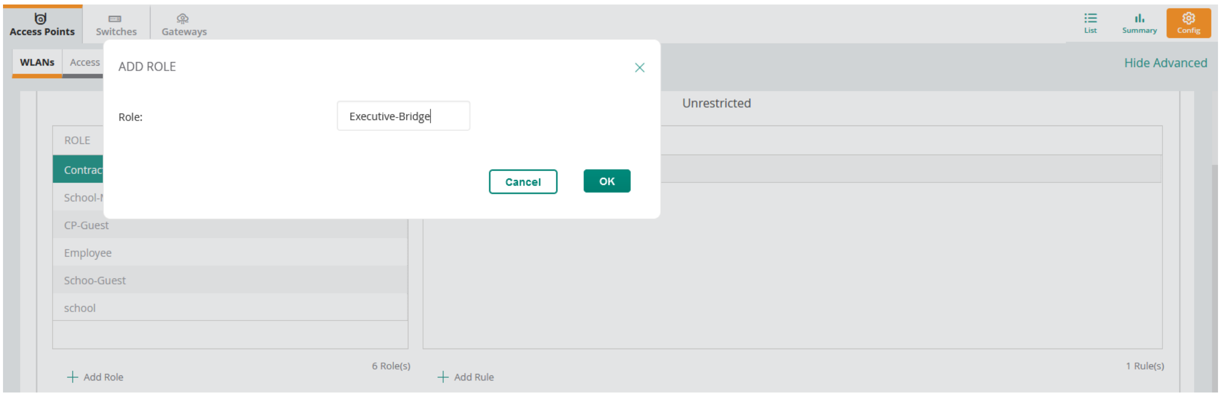
+ Add Rule 1 Rule(s)



ADD ROLE

Role: Contractor

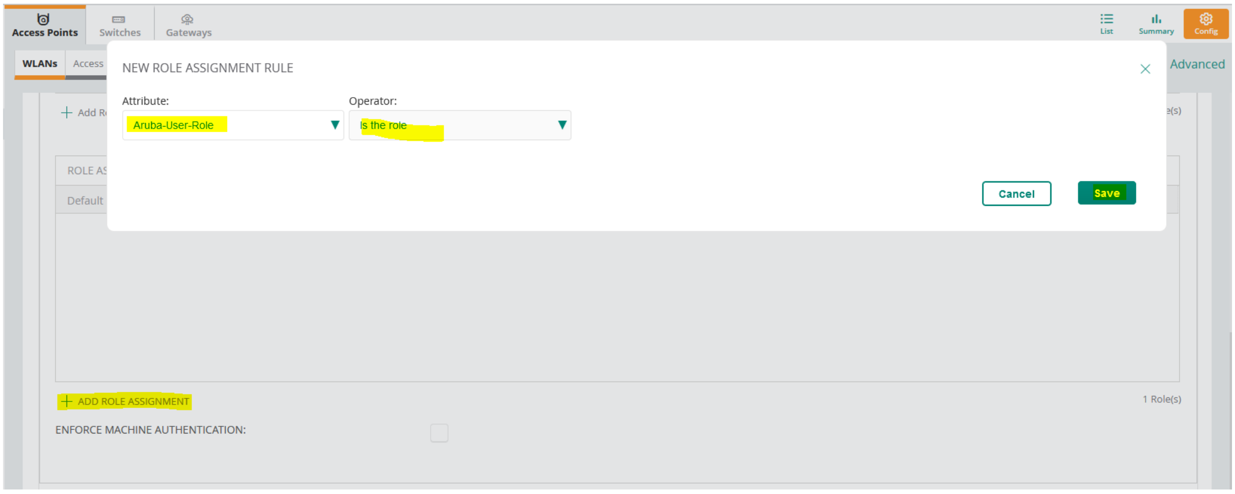
Cancel OK



ADD ROLE

Role: Executive-Bridge

Cancel OK



NEW ROLE ASSIGNMENT RULE

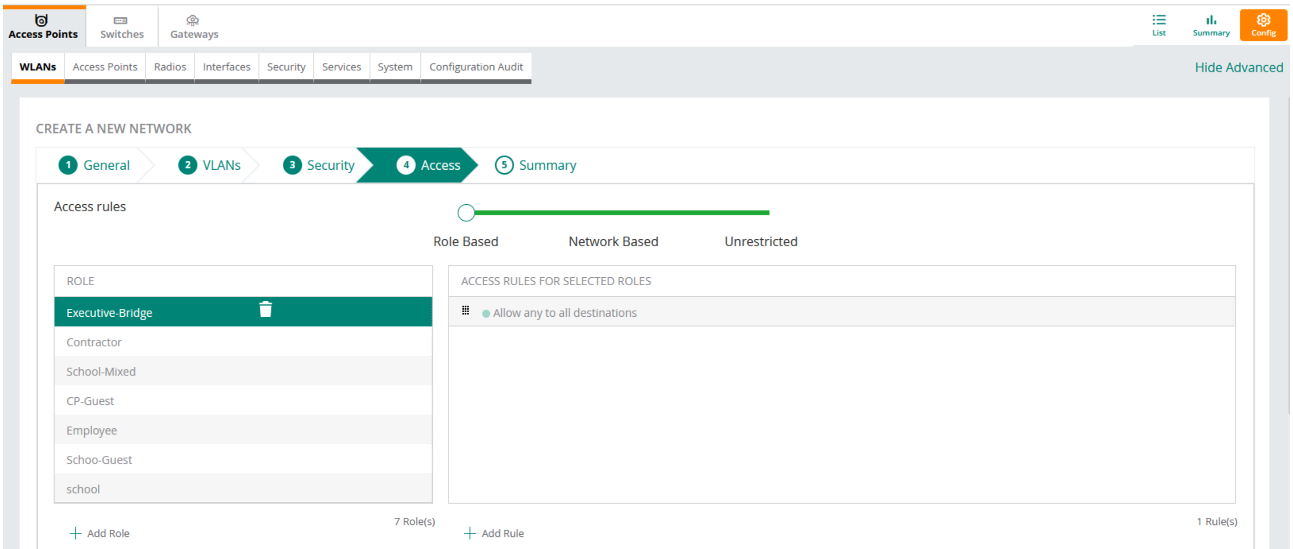
Attribute: Aruba-User-Role

Operator: is the role

Cancel Save

+ ADD ROLE ASSIGNMENT

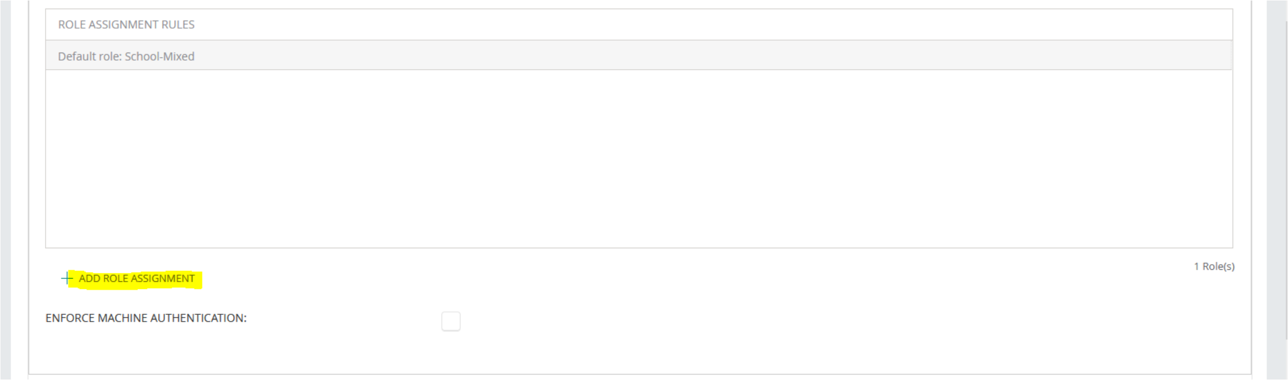
ENFORCE MACHINE AUTHENTICATION: □



CREATE A NEW NETWORK

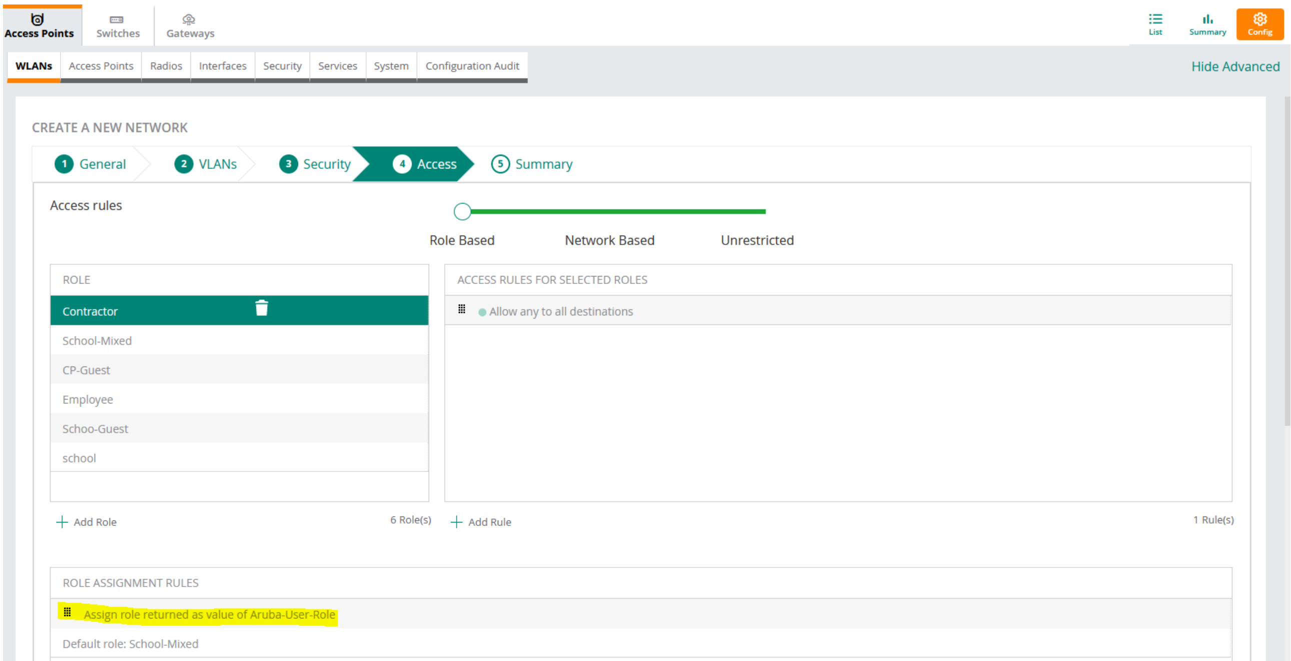
Access rules

ROLE	ACCESS RULES FOR SELECTED ROLES
Executive-Bridge	Allow any to all destinations
Contractor	
School-Mixed	
CP-Guest	
Employee	
Schoo-Guest	
school	


ROLE ASSIGNMENT RULES

Default role: School-Mixed

ENFORCE MACHINE AUTHENTICATION: □



CREATE A NEW NETWORK

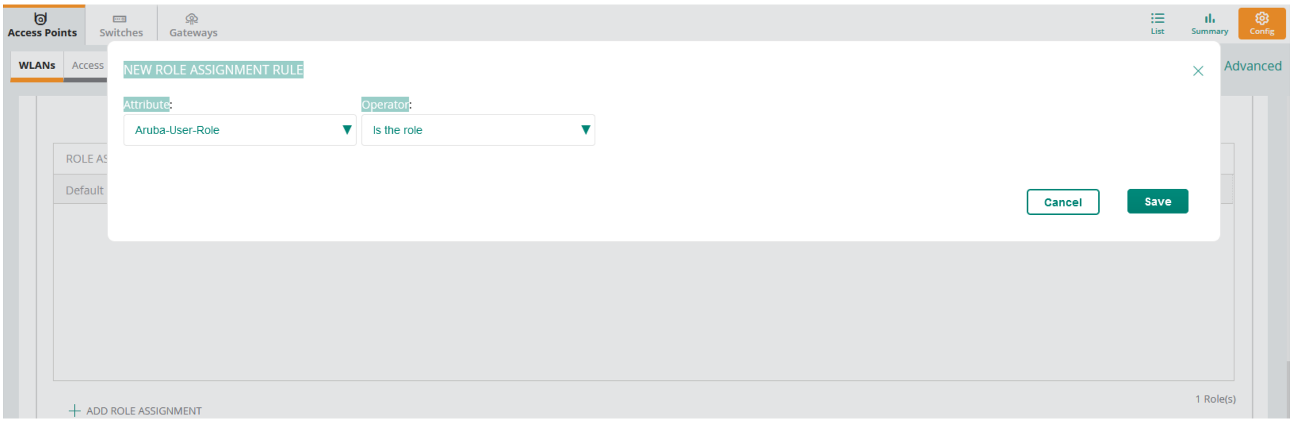
Access rules

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

ROLE ASSIGNMENT RULES

Assign role returned as value of Aruba-User-Role

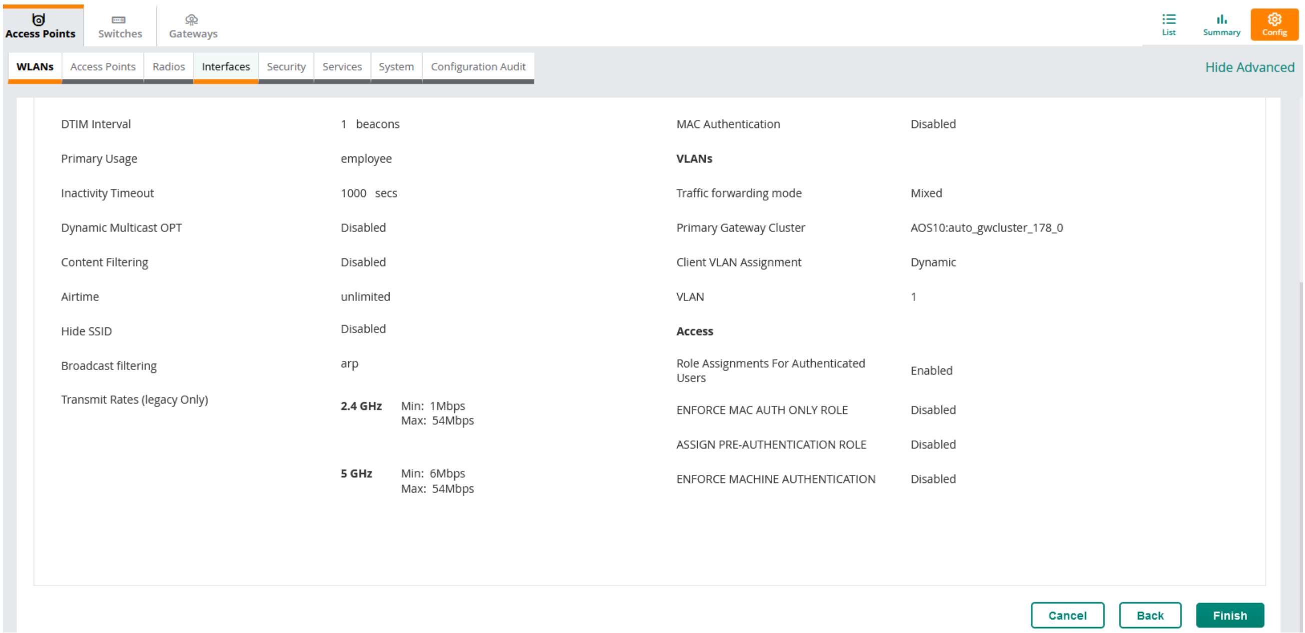
Default role: School-Mixed



NEW ROLE ASSIGNMENT RULE

Attribute: Aruba-User-Role

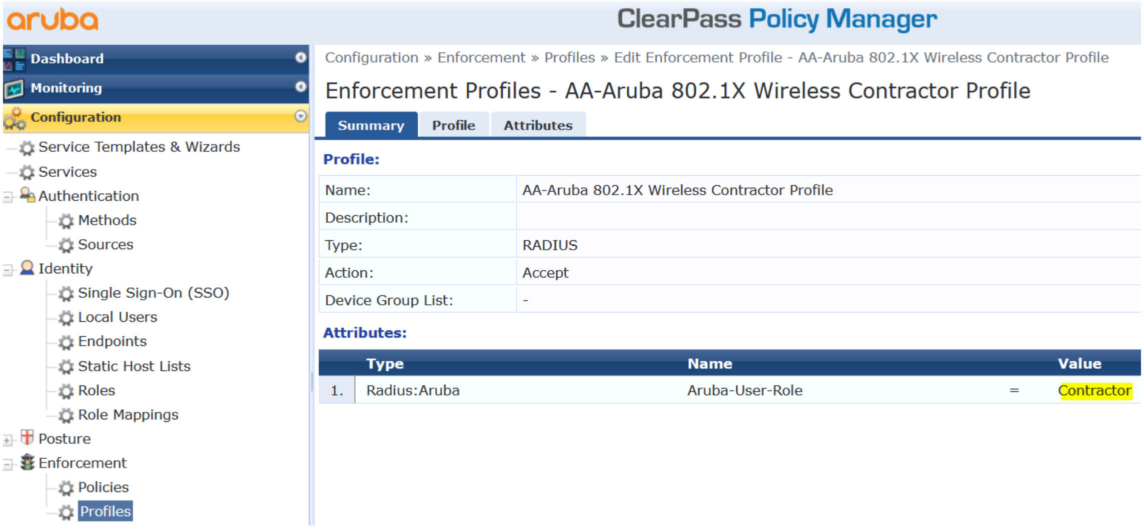
Operator: Is the role



DTIM Interval	1 beacons	MAC Authentication	Disabled
Primary Usage	employee	**VLANs**	
Inactivity Timeout	1000 secs	Traffic forwarding mode	Mixed
Dynamic Multicast OPT	Disabled	Primary Gateway Cluster	AOS10:auto_gwcluster_178_0
Content Filtering	Disabled	Client VLAN Assignment	Dynamic
Airtime	unlimited	VLAN	1
Hide SSID	Disabled	**Access**	
Broadcast filtering	arp	Role Assignments For Authenticated Users	Enabled
Transmit Rates (legacy Only)	**2.4 GHz** Min: 1Mbps Max: 54Mbps	ENFORCE MAC AUTH ONLY ROLE	Disabled
		ASSIGN PRE-AUTHENTICATION ROLE	Disabled
	5 GHz Min: 6Mbps Max: 54Mbps	ENFORCE MACHINE AUTHENTICATION	Disabled

6.7 ClearPass Service Modifications

We'll use the same ClearPass dot1x service that was used for tunnelled and bridge mode WLAN. So, I'll just need a specific enforcement profile for the mixed mode to send back the user-role and then I'll modify the service.



Configuration » Enforcement » Profiles » Edit Enforcement Profile - AA-Aruba 802.1X Wireless Contractor Profile

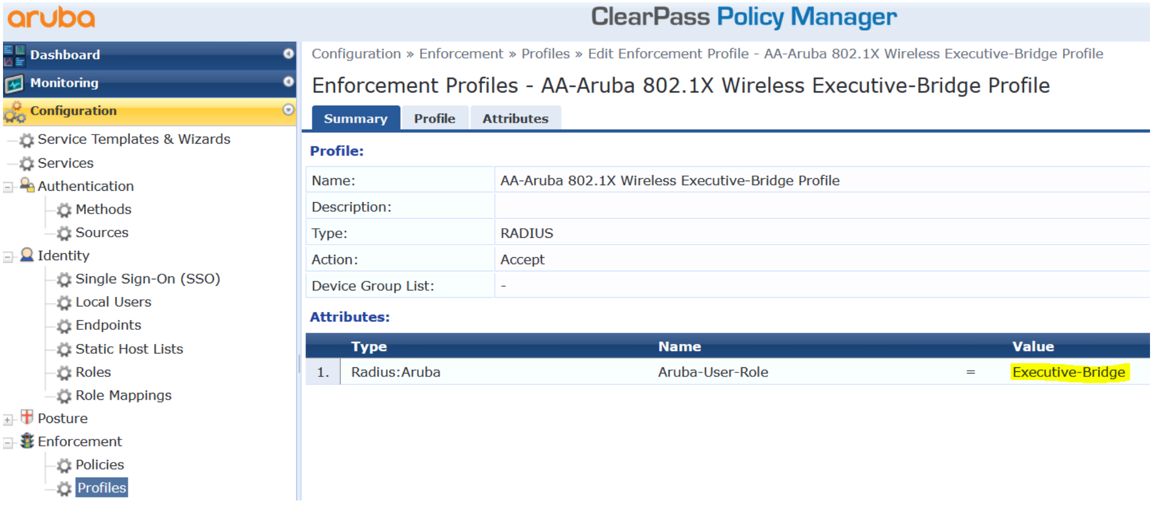
Enforcement Profiles - AA-Aruba 802.1X Wireless Contractor Profile

Profile:

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

Attributes:

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



Configuration » Enforcement » Profiles » Edit Enforcement Profile - AA-Aruba 802.1X Wireless Executive-Bridge Profile

Enforcement Profiles - AA-Aruba 802.1X Wireless Executive-Bridge Profile

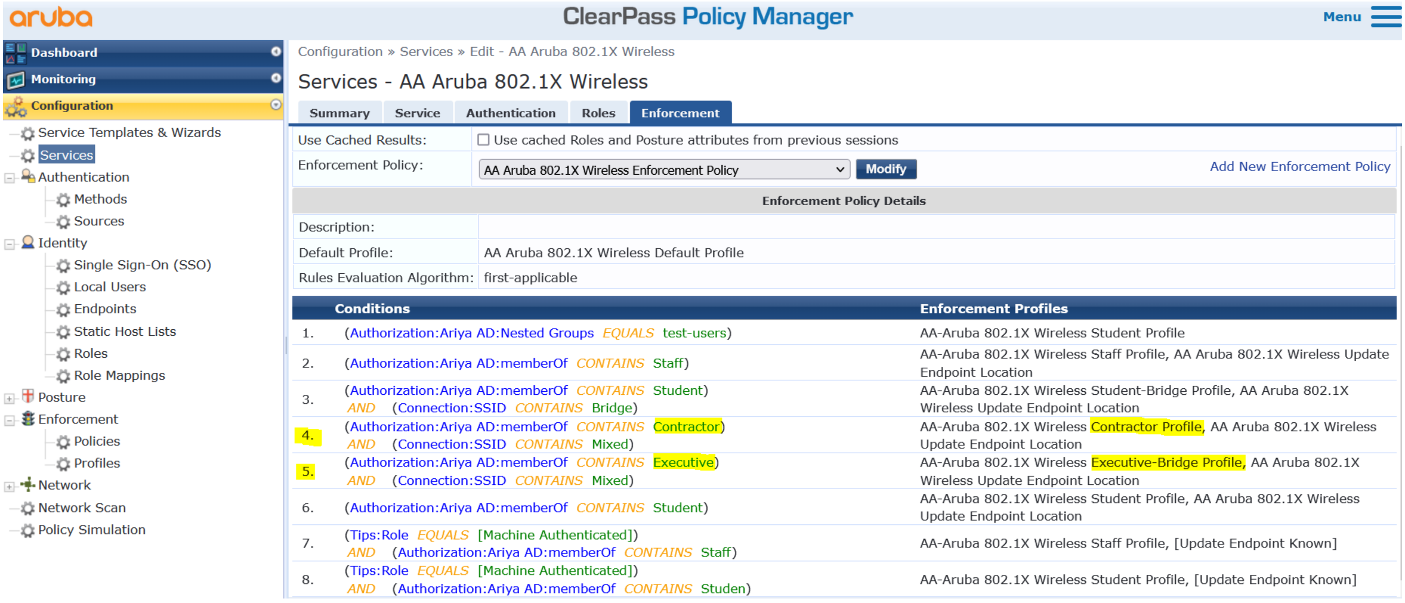
Profile:

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

Attributes:

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

And now we'll add a logic in the enforcement policy.



Configuration » Services » Edit - AA Aruba 802.1X Wireless

Services - AA Aruba 802.1X Wireless

Use Cached Results:	□ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	AA Aruba 802.1X Wireless Enforcement Policy

Enforcement Policy Details

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

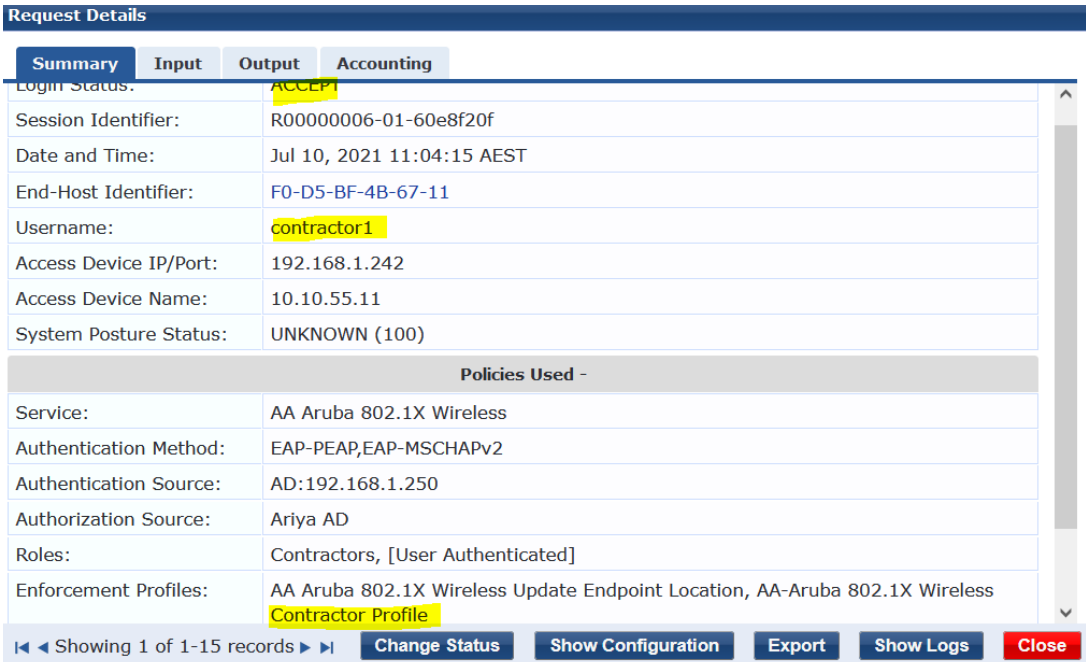
	Conditions	Enforcement Profiles
1.	(Authorization:Ariya AD:Nested Groups *EQUALS* test-users)	AA-Aruba 802.1X Wireless Student Profile
2.	(Authorization:Ariya AD:memberOf *CONTAINS* Staff)	AA-Aruba 802.1X Wireless Staff Profile, AA Aruba 802.1X Wireless Update Endpoint Location
3.	(Authorization:Ariya AD:memberOf *CONTAINS* Student) *AND* (Connection:SSID *CONTAINS* Bridge)	AA-Aruba 802.1X Wireless Student-Bridge Profile, AA Aruba 802.1X Wireless Update Endpoint Location
4.	(Authorization:Ariya AD:memberOf *CONTAINS* Contractor) *AND* (Connection:SSID *CONTAINS* Mixed)	AA-Aruba 802.1X Wireless Contractor Profile, AA Aruba 802.1X Wireless Update Endpoint Location
5.	(Authorization:Ariya AD:memberOf *CONTAINS* Executive) *AND* (Connection:SSID *CONTAINS* Mixed)	AA-Aruba 802.1X Wireless Executive-Bridge Profile, AA Aruba 802.1X Wireless Update Endpoint Location
6.	(Authorization:Ariya AD:memberOf *CONTAINS* Student)	AA-Aruba 802.1X Wireless Student Profile, AA Aruba 802.1X Wireless Update Endpoint Location
7.	(Tips:Role *EQUALS* [Machine Authenticated]) *AND* (Authorization:Ariya AD:memberOf *CONTAINS* Staff)	AA-Aruba 802.1X Wireless Staff Profile, [Update Endpoint Known]
8.	(Tips:Role *EQUALS* [Machine Authenticated]) *AND* (Authorization:Ariya AD:memberOf *CONTAINS* Studen)	AA-Aruba 802.1X Wireless Student Profile, [Update Endpoint Known]

Now we are ready to test it out.

6.8 Mixed Mode Wireless dot1x Testing

The contractor credentials should get tunnelled to the gateway clusters and should get VLAN 44 while the Executive credentials should get bridged to VLAN 22.

Here are the access tracker screenshots.



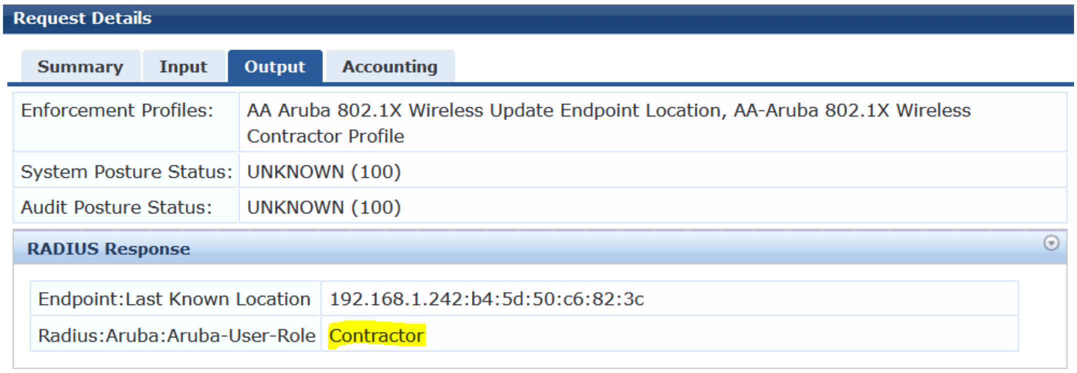
Request Details

Login Status:	ACCEPT
Session Identifier:	R00000006-01-60e8f20f
Date and Time:	Jul 10, 2021 11:04:15 AEST
End-Host Identifier:	F0-D5-BF-4B-67-11
Username:	contractor1
Access Device IP/Port:	192.168.1.242
Access Device Name:	10.10.55.11
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:	Contractors, [User Authenticated]
Enforcement Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless Contractor Profile

Showing 1 of 1-15 records



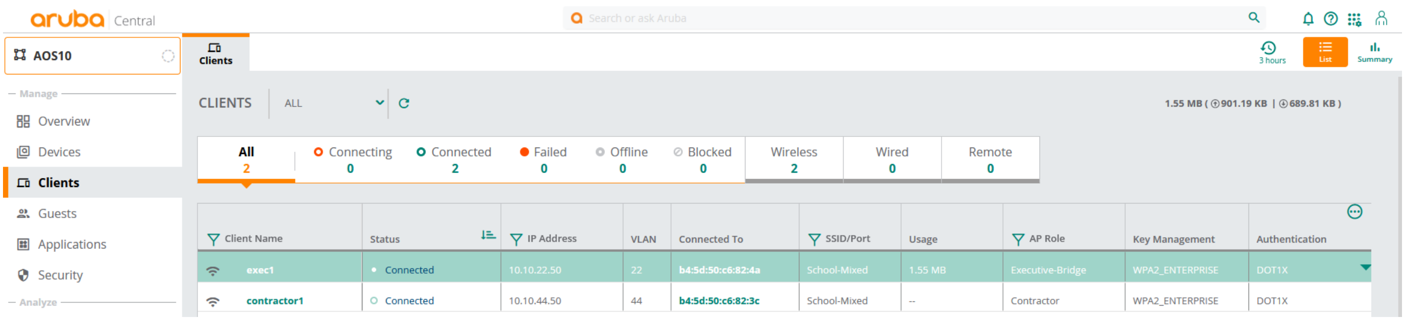
Request Details

Enforcement Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless Contractor Profile
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Endpoint:Last Known Location	192.168.1.242:b4:5d:50:c6:82:3c
Radius:Aruba:Aruba-User-Role	Contractor

Looking at the Clients from Aruba Central we see that both clients are in the respective VLANs.

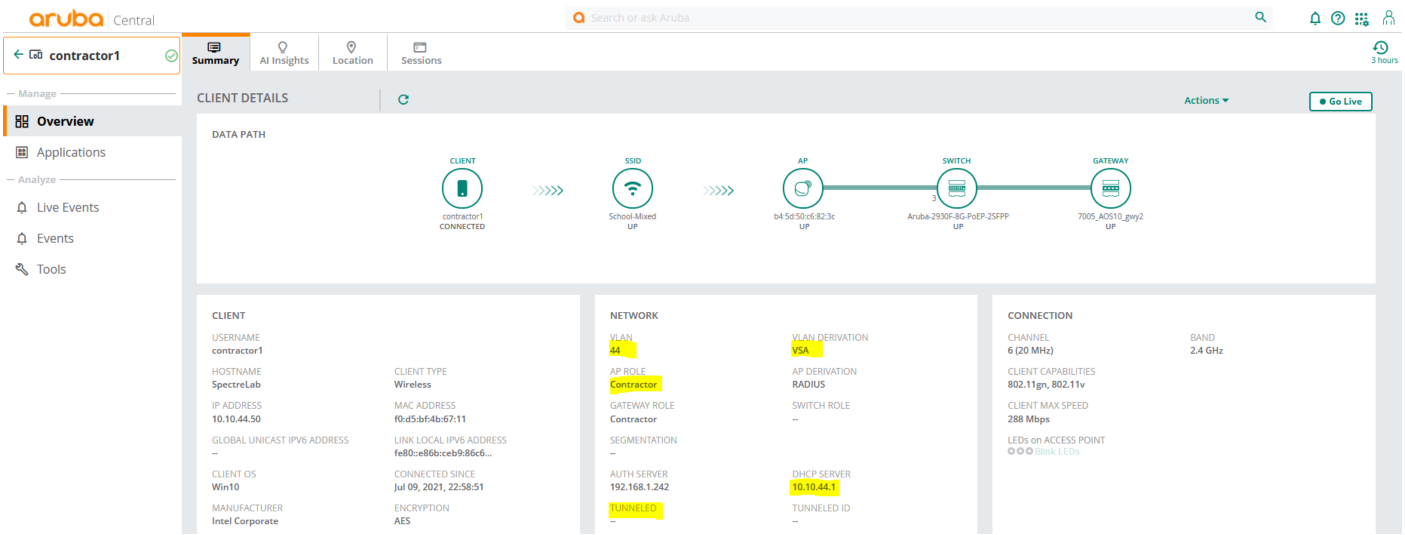


CLIENTS ALL

1.55 MB (901.19 KB | 689.81 KB)

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

Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	Usage	AP Role	Key Management	Authentication
exec1	Connected	10.10.22.50	22	b4:5d:50:c6:82:4a	School-Mixed	1.55 MB	Executive-Bridge	WPA2_ENTERPRISE	DOT1X
contractor1	Connected	10.10.44.50	44	b4:5d:50:c6:82:3c	School-Mixed	--	Contractor	WPA2_ENTERPRISE	DOT1X



CLIENT DETAILS

DATA PATH

CLIENT

USERNAME contractor1	
HOSTNAME SpectreLab	CLIENT TYPE Wireless
IP ADDRESS 10.10.44.50	MAC ADDRESS f0:d5:bf:4b:67:11
GLOBAL UNICAST IPV6 ADDRESS --	LINK LOCAL IPV6 ADDRESS fe80::e86b:ceb9:86c6...
CLIENT OS Win10	CONNECTED SINCE Jul 09, 2021, 22:58:51
MANUFACTURER Intel Corporate	ENCRYPTION AES

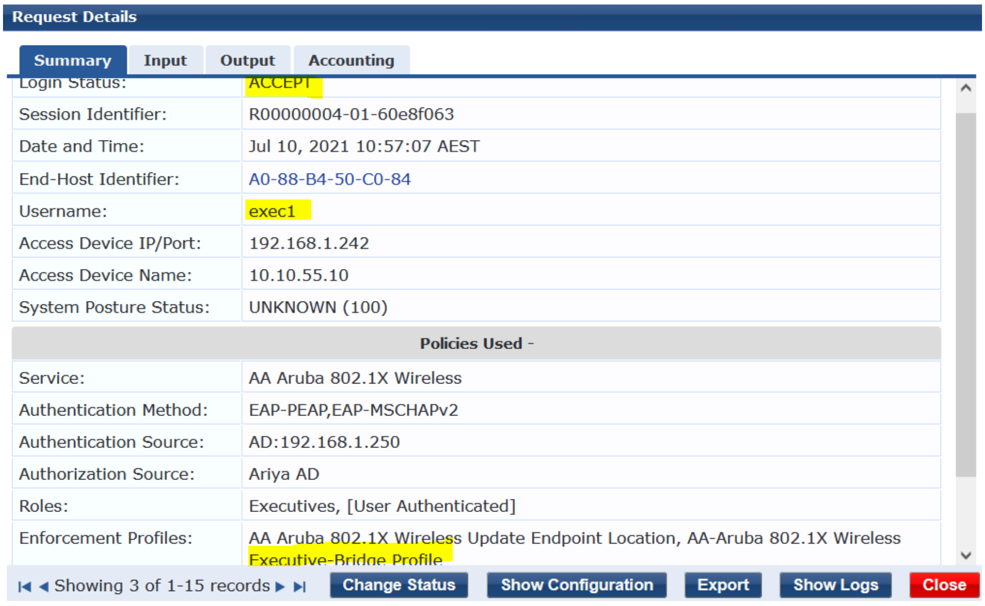
NETWORK

VLAN 44	VLAN DERIVATION VSA
AP ROLE Contractor	AP DERIVATION RADIUS
GATEWAY ROLE Contractor	SWITCH ROLE --
SEGMENTATION --	
AUTH SERVER 192.168.1.242	DHCP SERVER 10.10.44.1
TUNNELED --	TUNNELED ID --

CONNECTION

CHANNEL 6 (20 MHz)	BAND 2.4 GHz
CLIENT CAPABILITIES 802.11gn, 802.11v	
CLIENT MAX SPEED 288 Mbps	
LEDs on ACCESS POINT	

Note that Auth server shown above is the IP address of one of the gateways. Now we’ll use another client and login with exec1 credentials. First checking ClearPass Access tracker



Request Details

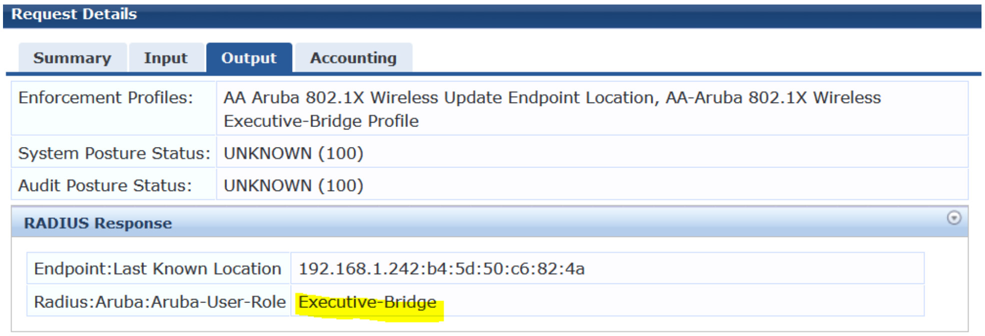
Login Status:	ACCEPT
Session Identifier:	R00000004-01-60e8f063
Date and Time:	Jul 10, 2021 10:57:07 AEST
End-Host Identifier:	A0-88-B4-50-C0-84
Username:	exec1
Access Device IP/Port:	192.168.1.242
Access Device Name:	10.10.55.10
System Posture Status:	UNKNOWN (100)

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:	Executives, [User Authenticated]
Enforcement Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless Executive-Bridge Profile

Showing 3 of 1-15 records

Change Status



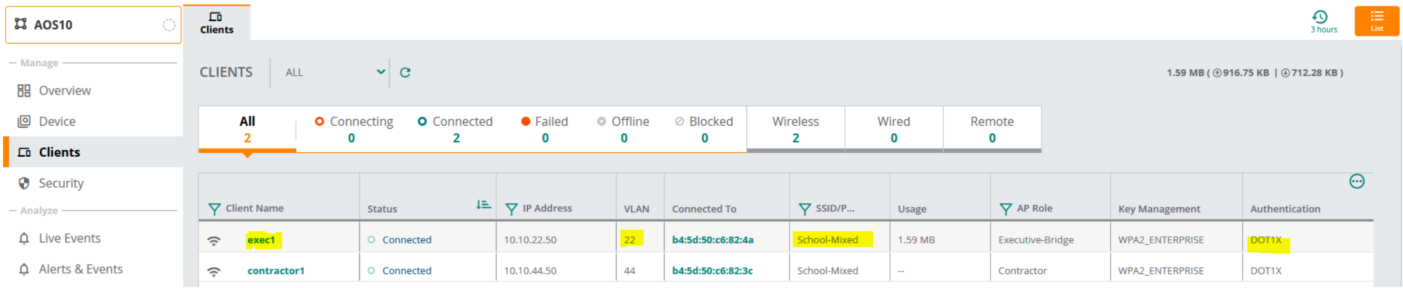
Request Details

Enforcement Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless Executive-Bridge 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	Executive-Bridge

Checking the client dashboard on Aruba Central

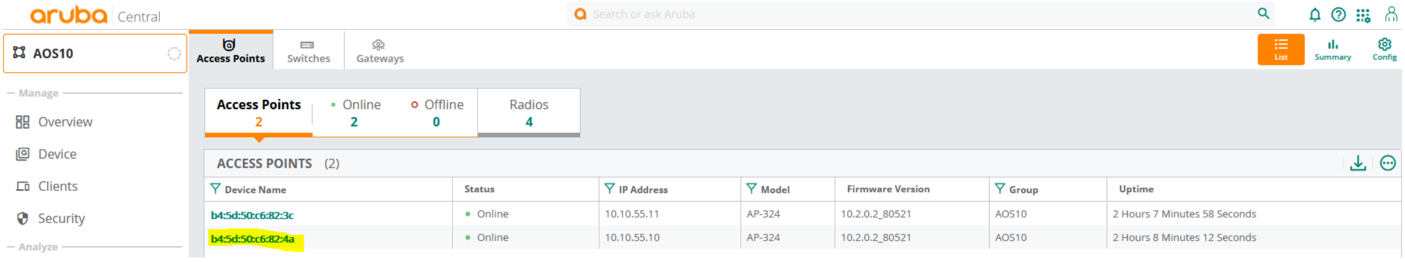


1.59 MB (⊕916.75 KB | ⊕712.28 KB)

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

Client Name	Status	IP Address	VLAN	Connected To	SSID/P...	Usage	AP Role	Key Management	Authentication
exec1	Connected	10.10.22.50	22	b4:5d:50:c6:82:4a	School-Mixed	1.59 MB	Executive-Bridge	WPA2_ENTERPRISE	DOT1X
contractor1	Connected	10.10.44.50	44	b4:5d:50:c6:82:3c	School-Mixed	--	Contractor	WPA2_ENTERPRISE	DOT1X

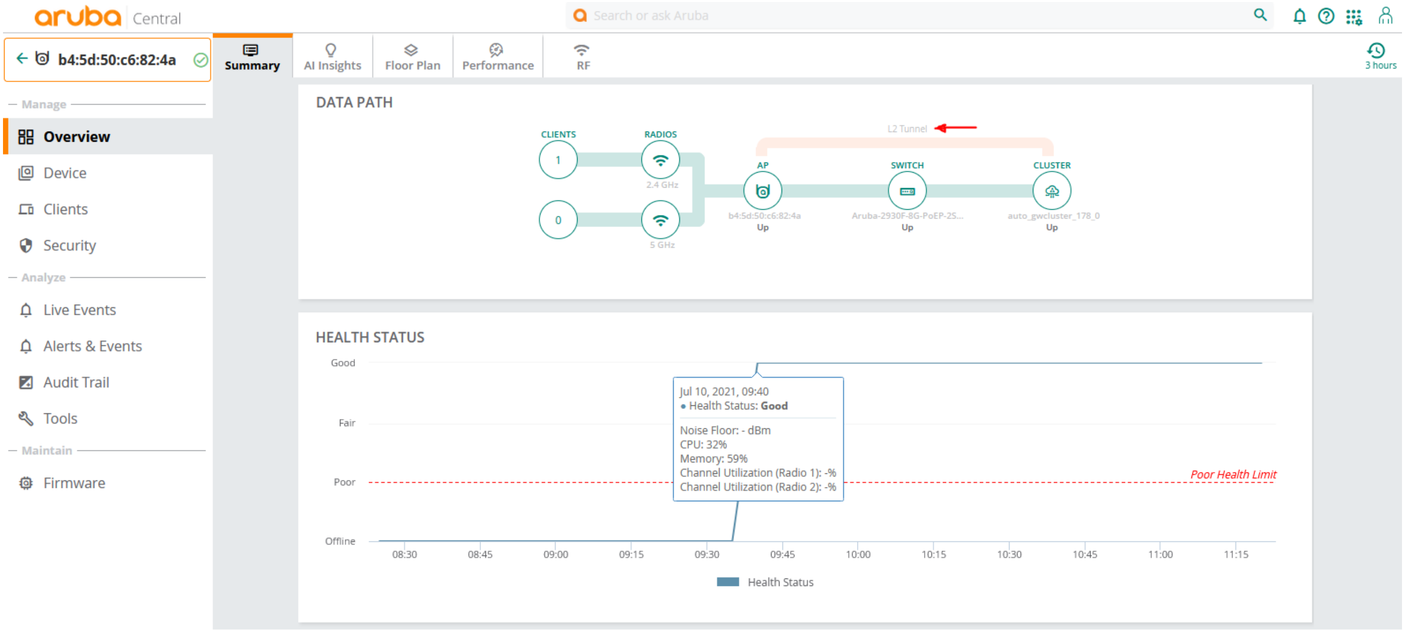
Checking the AP view to see the graphical tunnel for



Access Points	Online	Offline	Radios
2	2	0	4

ACCESS POINTS (2)

Device Name	Status	IP Address	Model	Firmware Version	Group	Uptime
b4:5d:50:c6:82:3c	Online	10.10.55.11	AP-324	10.2.0.2_80521	AOS10	2 Hours 7 Minutes 58 Seconds
b4:5d:50:c6:82:4a	Online	10.10.55.10	AP-324	10.2.0.2_80521	AOS10	2 Hours 8 Minutes 12 Seconds

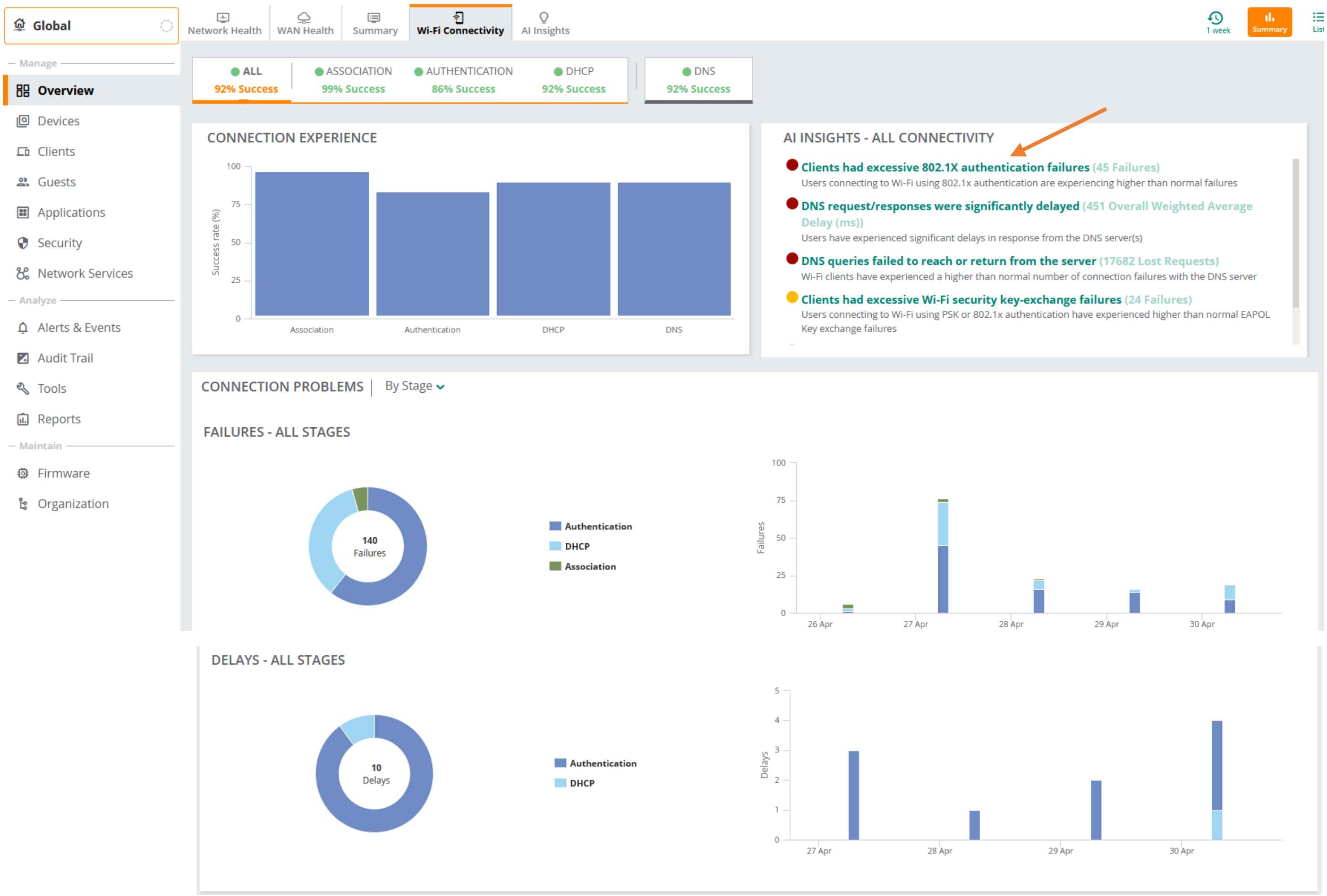


Jul 10, 2021, 09:40
• Health Status: **Good**

Noise Floor: - dBm
CPU: 32%
Memory: 59%
Channel Utilization (Radio 1): -%
Channel Utilization (Radio 2): -%

7 RF Monitoring

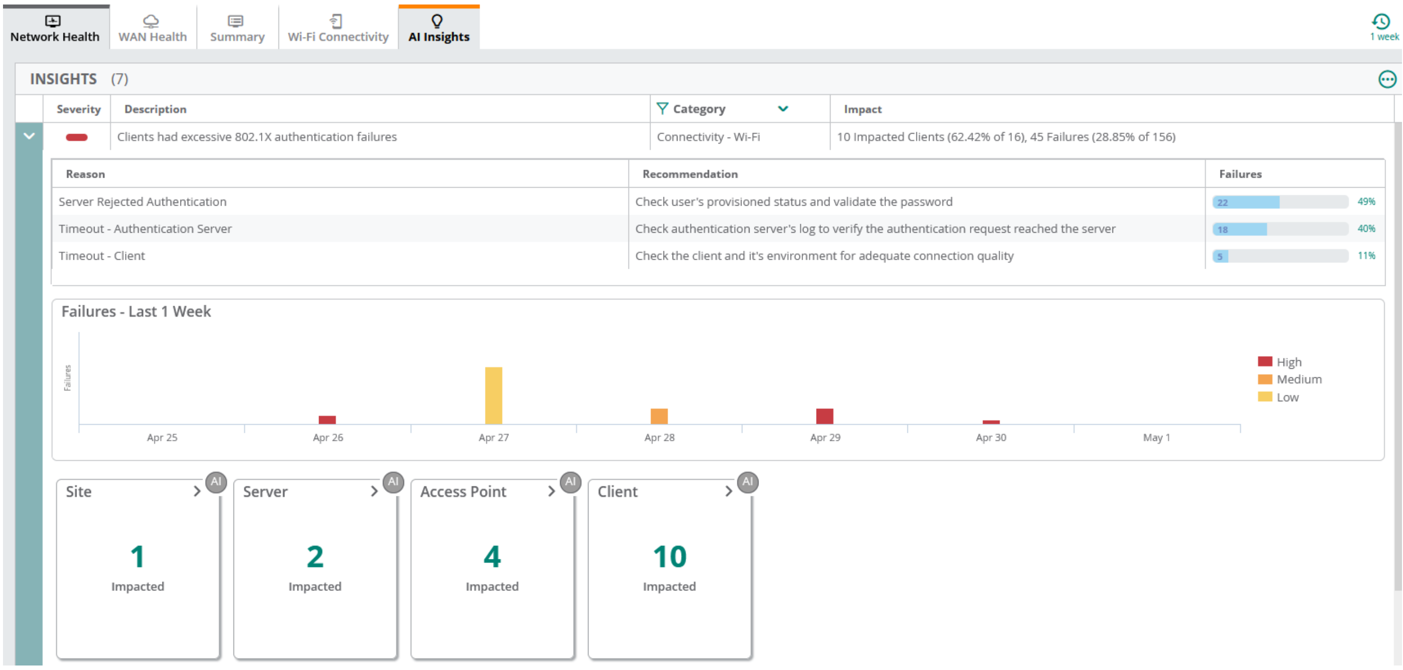
Here we’ll just touch on some of the RF mgmt. info that are available in Central. To start with at the global level, you can check the WiFi connectivity and then drill down on any specifics, like AI insights, associations, authentication , etc.



AI INSIGHTS - ALL CONNECTIVITY

- **Clients had excessive 802.1X authentication failures** (45 Failures)
  Users connecting to Wi-Fi using 802.1x authentication are experiencing higher than normal failures
- **DNS request/responses were significantly delayed** (451 Overall Weighted Average Delay (ms))
  Users have experienced significant delays in response from the DNS server(s)
- **DNS queries failed to reach or return from the server** (17682 Lost Requests)
  Wi-Fi clients have experienced a higher than normal number of connection failures with the DNS server
- **Clients had excessive Wi-Fi security key-exchange failures** (24 Failures)
  Users connecting to Wi-Fi using PSK or 802.1x authentication have experienced higher than normal EAPOL Key exchange failures

Clicking on “clients had excessive 802.1.x failures”



INSIGHTS (7)

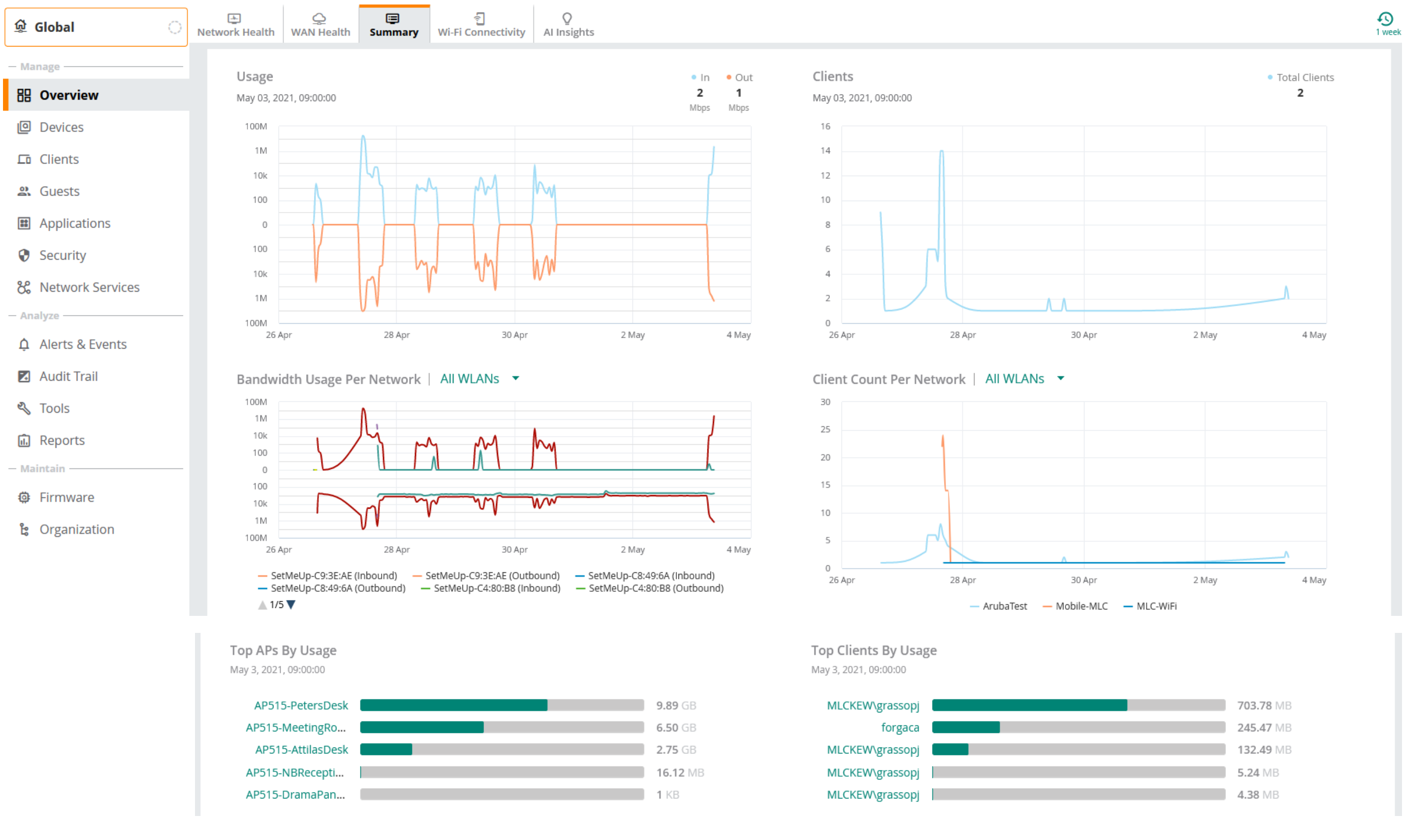
Severity	Description	Category	Impact
🟥	Clients had excessive 802.1X authentication failures	Connectivity - Wi-Fi	10 Impacted Clients (62.42% of 16), 45 Failures (28.85% of 156)

Reason	Recommendation	Failures
Server Rejected Authentication	Check user's provisioned status and validate the password	22 49%
Timeout - Authentication Server	Check authentication server's log to verify the authentication request reached the server	18 40%
Timeout - Client	Check the client and it's environment for adequate connection quality	5 11%

Failures - Last 1 Week

Site	Server	Access Point	Client
1 Impacted	2 Impacted	4 Impacted	10 Impacted

Next, we can check the usage summary



Top APs By Usage

May 3, 2021, 09:00:00

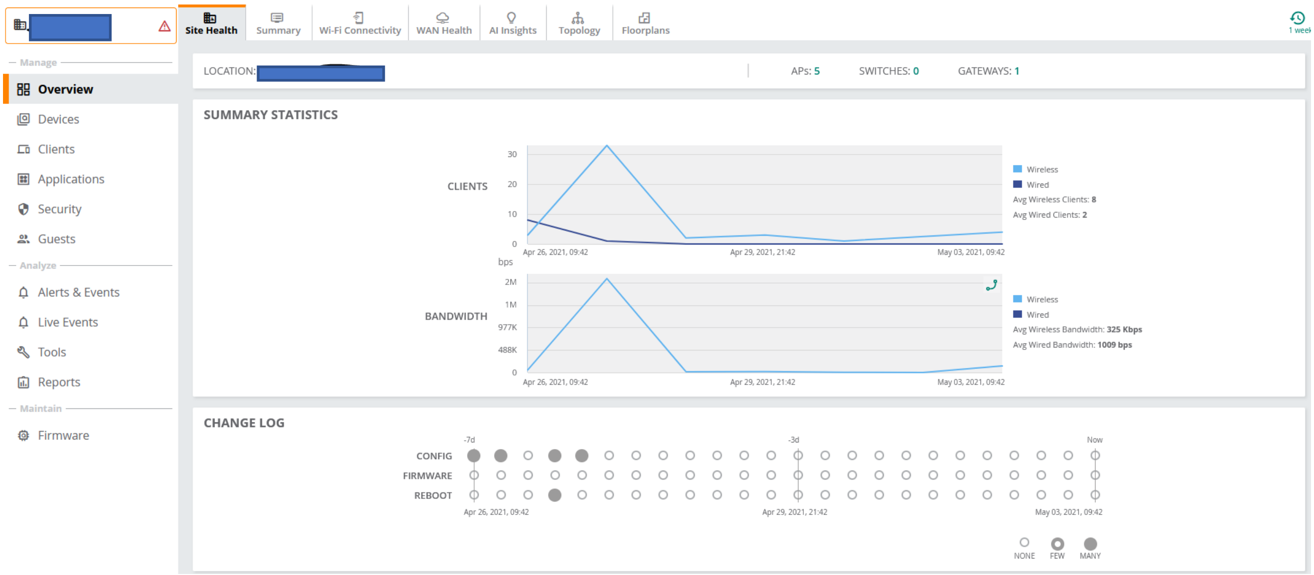
AP515-PetersDesk	9.89 GB
AP515-MeetingRo...	6.50 GB
AP515-AttilasDesk	2.75 GB
AP515-NBRecepti...	16.12 MB
AP515-DramaPan...	1 KB

Top Clients By Usage

May 3, 2021, 09:00:00

MLCKEW\grassopj	703.78 MB
forgaca	245.47 MB
MLCKEW\grassopj	132.49 MB
MLCKEW\grassopj	5.24 MB
MLCKEW\grassopj	4.38 MB

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



LOCATION: [redacted]

APs: 5 SWITCHES: 0 GATEWAYS: 1

SUMMARY STATISTICS

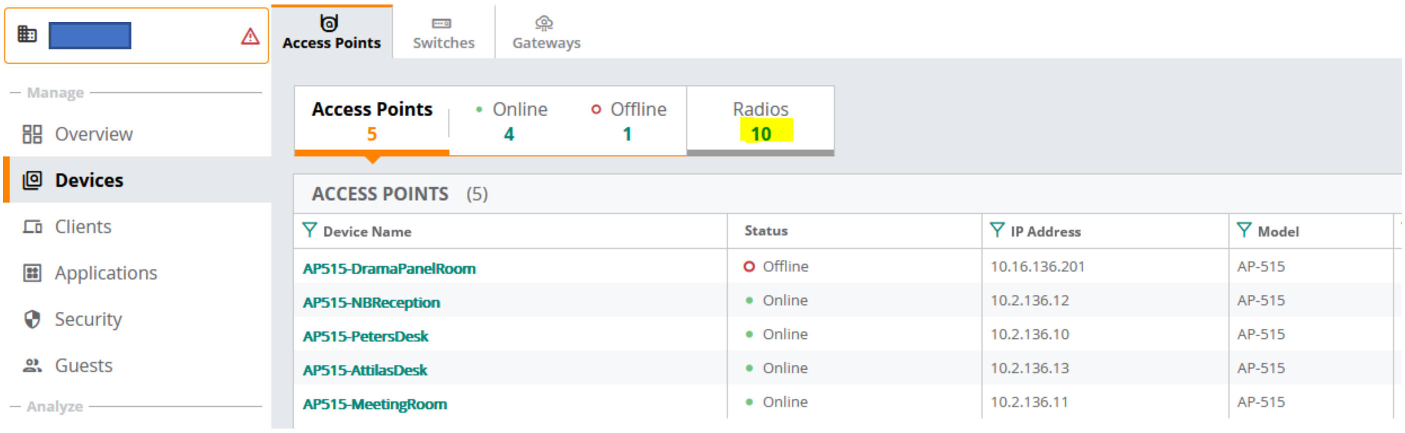
Avg Wireless Clients: 8

Avg Wired Clients: 2

Avg Wireless Bandwidth: 325 Kbps

Avg Wired Bandwidth: 1009 bps

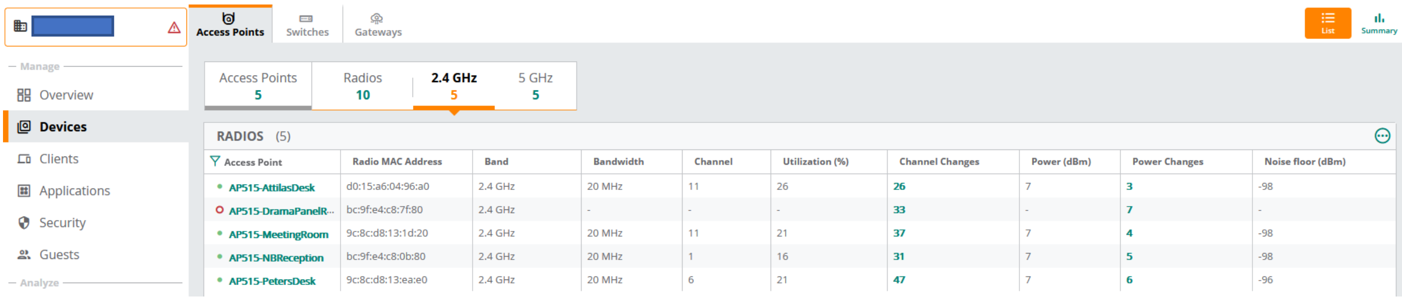
CHANGE LOG



Access Points 5 · Online 4 · Offline 1 · Radios 10

ACCESS POINTS (5)

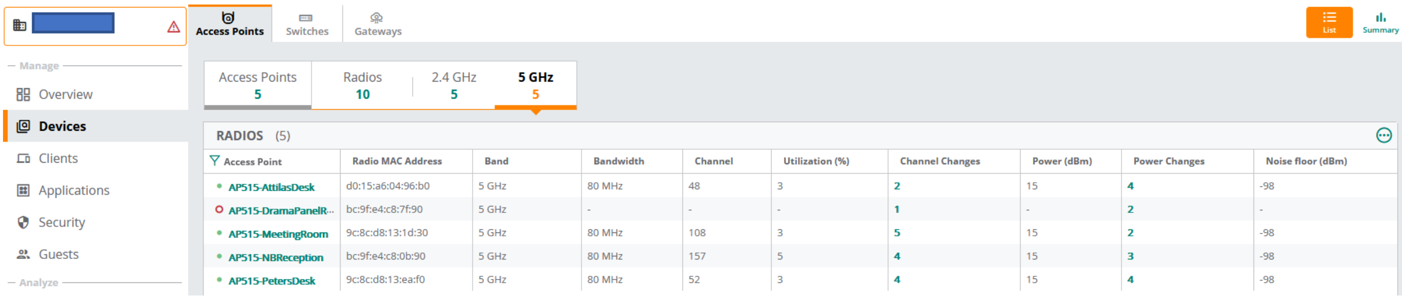
Device Name	Status	IP Address	Model
AP515-DramaPanelRoom	○ Offline	10.16.136.201	AP-515
AP515-NBReception	● Online	10.2.136.12	AP-515
AP515-PetersDesk	● Online	10.2.136.10	AP-515
AP515-AttilasDesk	● Online	10.2.136.13	AP-515
AP515-MeetingRoom	● Online	10.2.136.11	AP-515


[redacted]

Access Points	Radios	2.4 GHz	5 GHz
5	10	5	5

RADIOS (5)

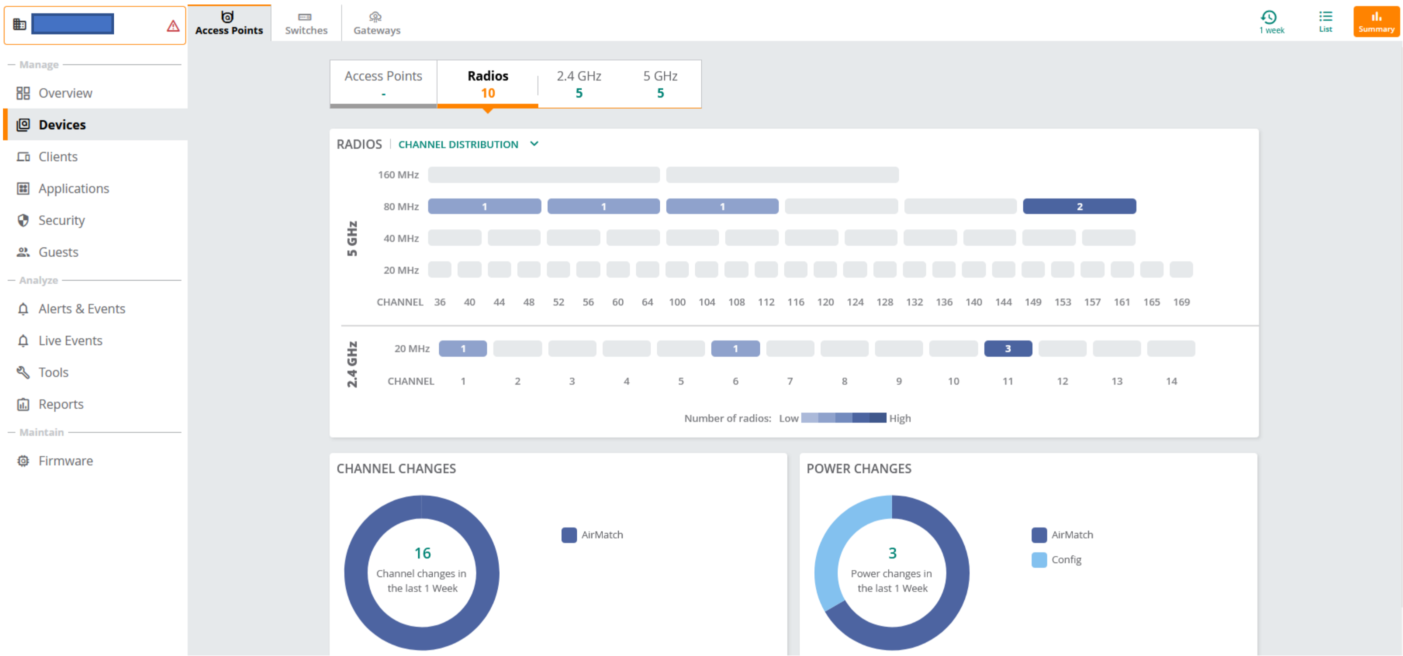
Access Point	Radio MAC Address	Band	Bandwidth	Channel	Utilization (%)	Channel Changes	Power (dBm)	Power Changes	Noise floor (dBm)
● AP515-AttilasDesk	d0:15:a6:04:96:a0	2.4 GHz	20 MHz	11	26	26	7	3	-98
○ AP515-DramaPanelR...	bc:9f:e4:c8:7f:80	2.4 GHz	-	-	-	33	-	7	-
● AP515-MeetingRoom	9c:8c:d8:13:1d:20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


[redacted]

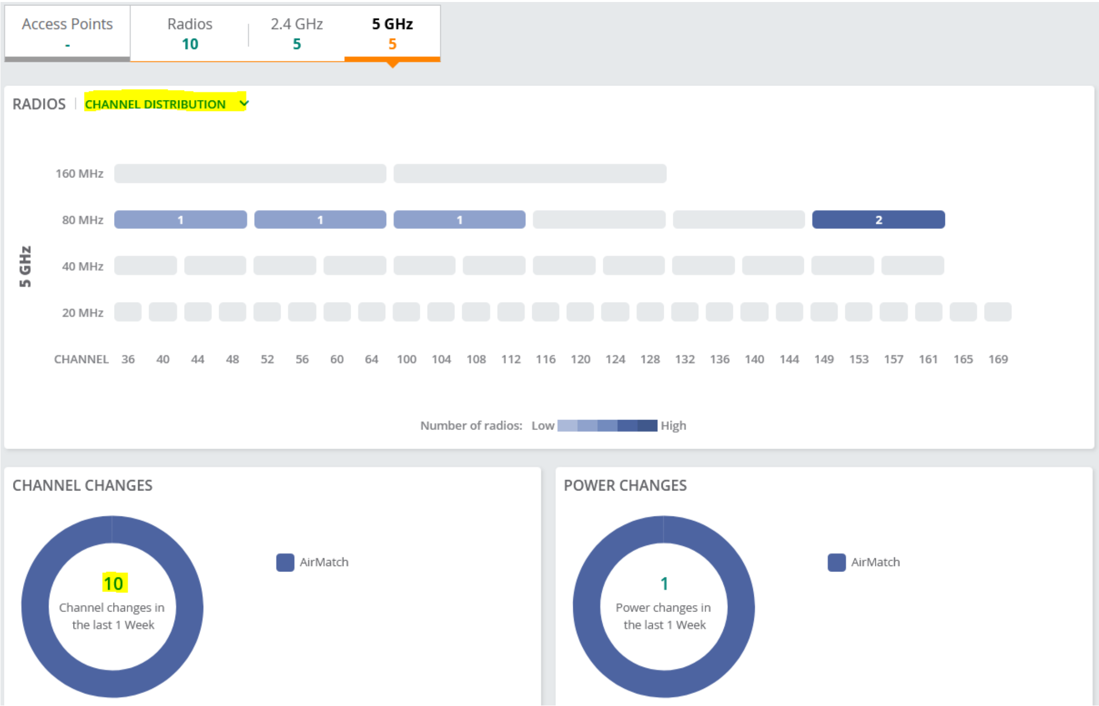
Access Points	Radios	2.4 GHz	5 GHz
5	10	5	5

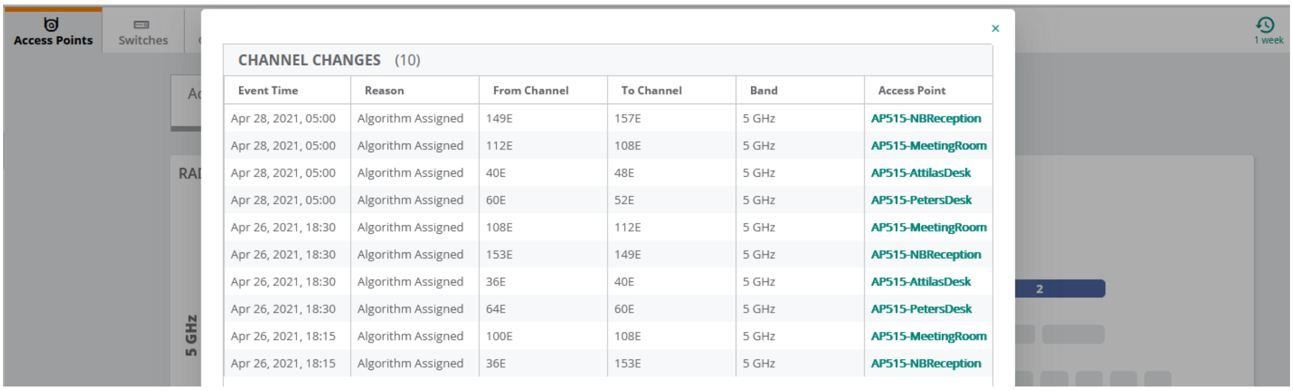
RADIOS (5)

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


[redacted]

Looking at 5GHz band

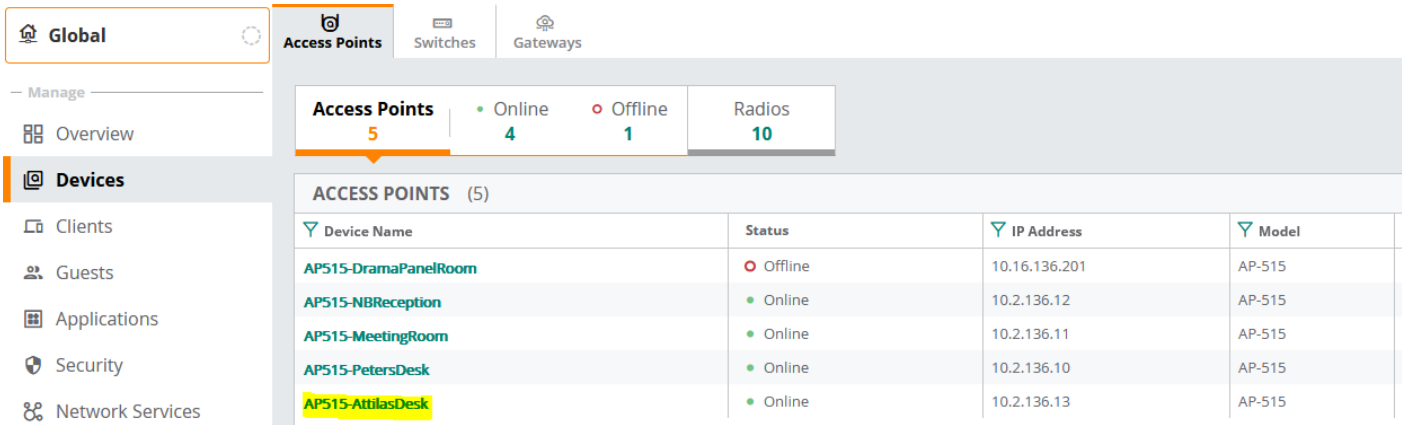

Access Points
-
Radios
10
2.4 GHz
5
5 GHz
5
RADIOS
CHANNEL DISTRIBUTION
5 GHz
160 MHz
80 MHz
1
1
1
2
40 MHz
20 MHz
CHANNEL 36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140 144 149 153 157 161 165 169
Number of radios: Low High
CHANNEL CHANGES
10
Channel changes in the last 1 Week
AirMatch
POWER CHANGES
1
Power changes in the last 1 Week
AirMatch



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

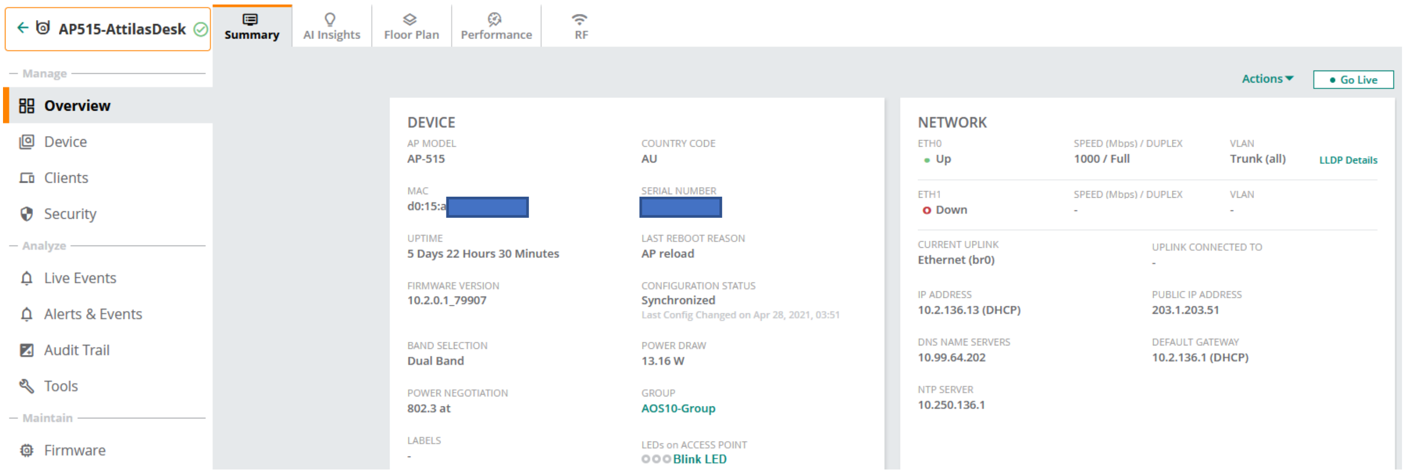
Next, we can have a look at the Live view, for that we'll choose a specific AP.



Access Points 5 | ● Online 4 | ○ Offline 1 | Radios 10

ACCESS POINTS (5)

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



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: ○○○ Blink LED

NETWORK

	SPEED (Mbps) / DUPLEX	VLAN	
ETH0 ● Up	1000 / Full	Trunk (all)	LLDP Details
ETH1 ○ Down	-	-	

CURRENT UPLINK: Ethernet (br0)

UPLINK CONNECTED TO: -

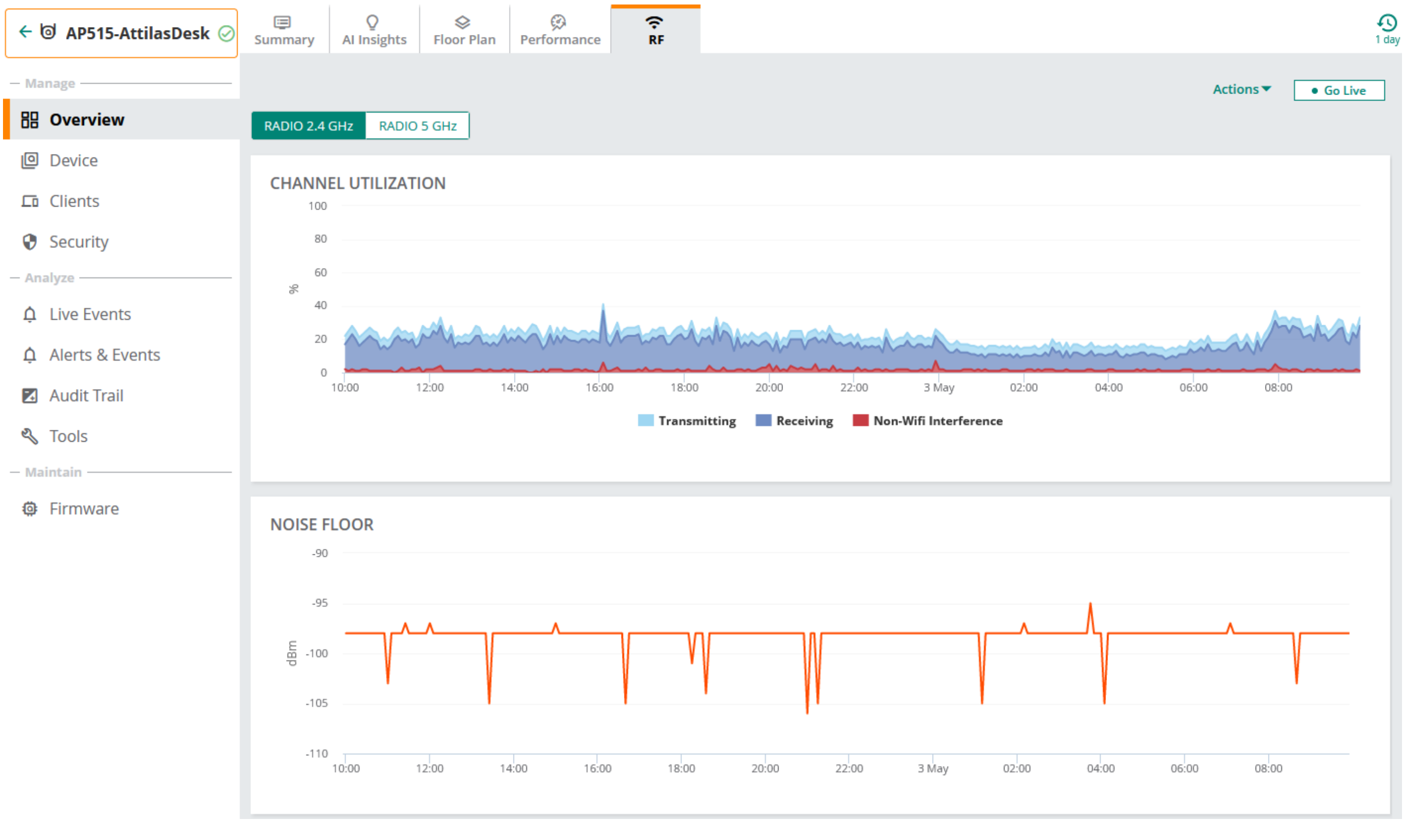
IP ADDRESS: 10.2.136.13 (DHCP)

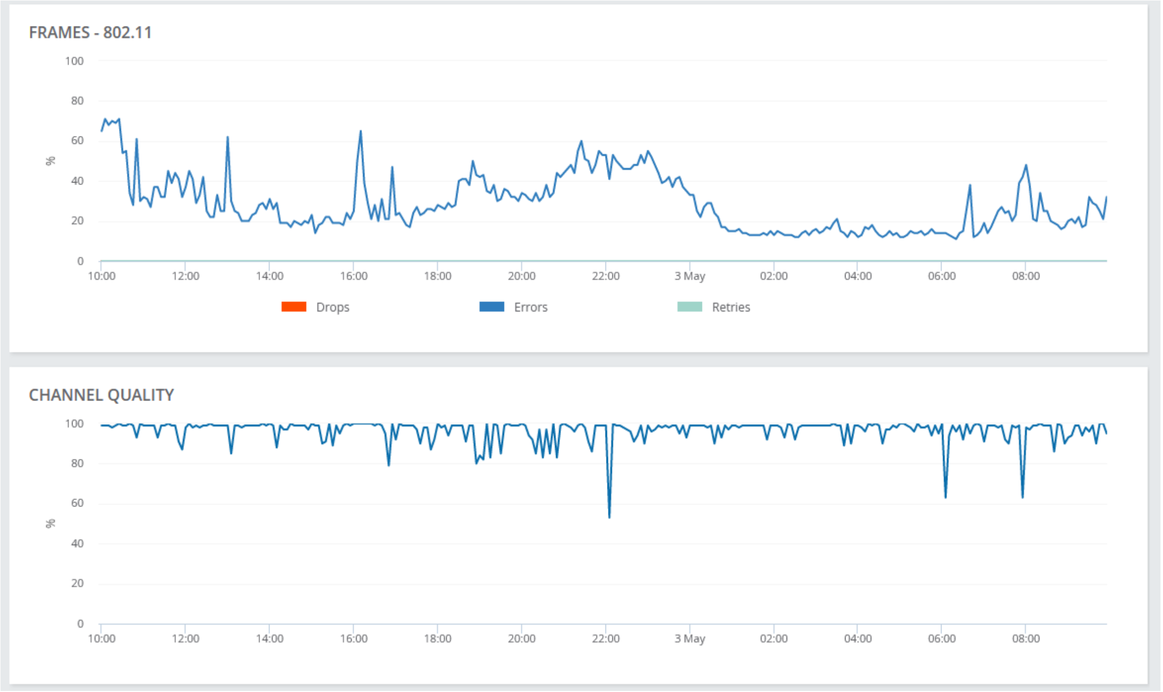
PUBLIC IP ADDRESS: 203.1.203.51

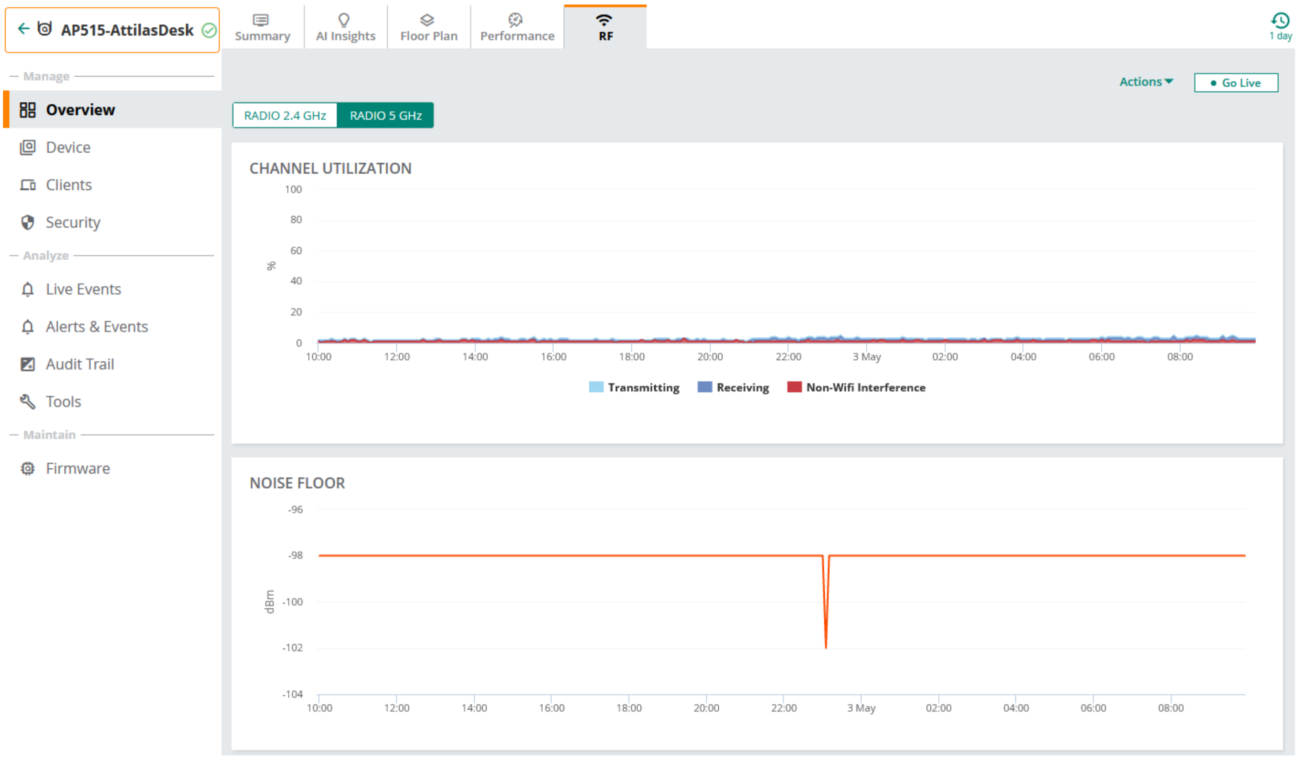
DNS NAME SERVERS: 10.99.64.202

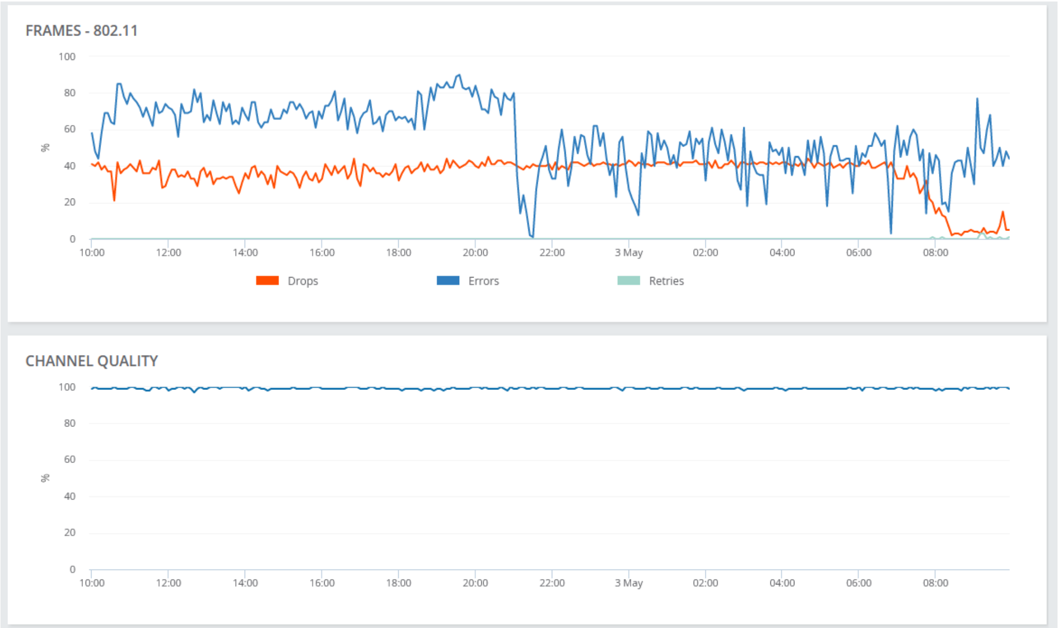
DEFAULT GATEWAY: 10.2.136.1 (DHCP)

NTP SERVER: 10.250.136.1

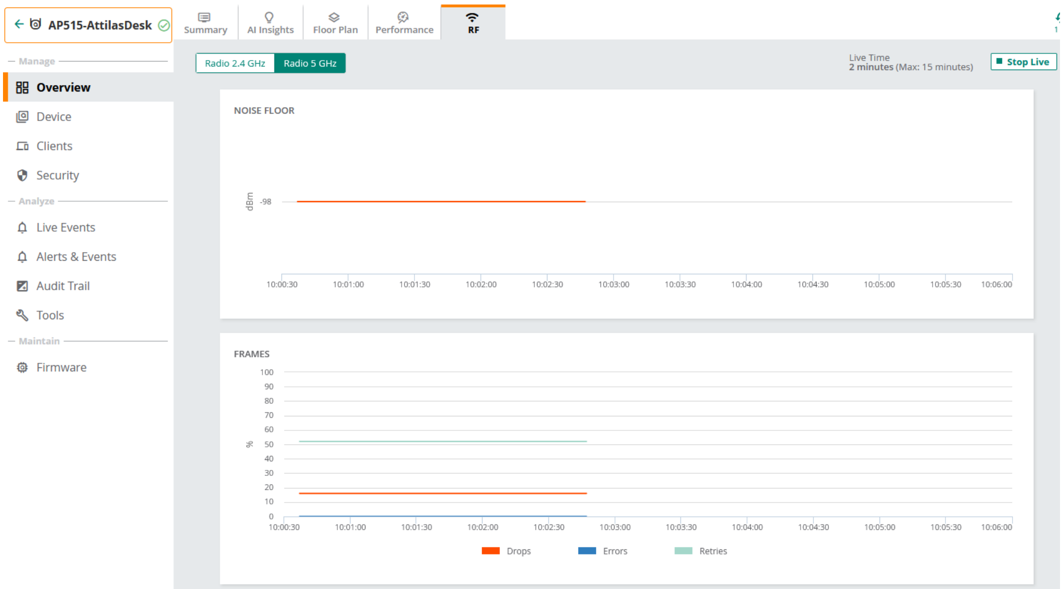

AP515-AttilasDesk
Summary
AI Insights
Floor Plan
Performance
RF
1 day
Manage
Overview
Device
Clients
Security
Analyze
Live Events
Alerts & Events
Audit Trail
Tools
Maintain
Firmware
Actions
● Go Live
RADIO 2.4 GHz
RADIO 5 GHz
CHANNEL UTILIZATION
100
80
60
40
20
0
%
10:00
12:00
14:00
16:00
18:00
20:00
22:00
3 May
02:00
04:00
06:00
08:00
Transmitting
Receiving
Non-Wifi Interference
NOISE FLOOR
-90
-95
-100
-105
-110
dBm
10:00
12:00
14:00
16:00
18:00
20:00
22:00
3 May
02:00
04:00
06:00
08:00


FRAMES - 802.11
100
80
60
40
20
0
%
10:00
12:00
14:00
16:00
18:00
20:00
22:00
3 May
02:00
04:00
06:00
08:00
Drops
Errors
Retries
CHANNEL QUALITY
100
80
60
40
20
0
%
10:00
12:00
14:00
16:00
18:00
20:00
22:00
3 May
02:00
04:00
06:00
08:00





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

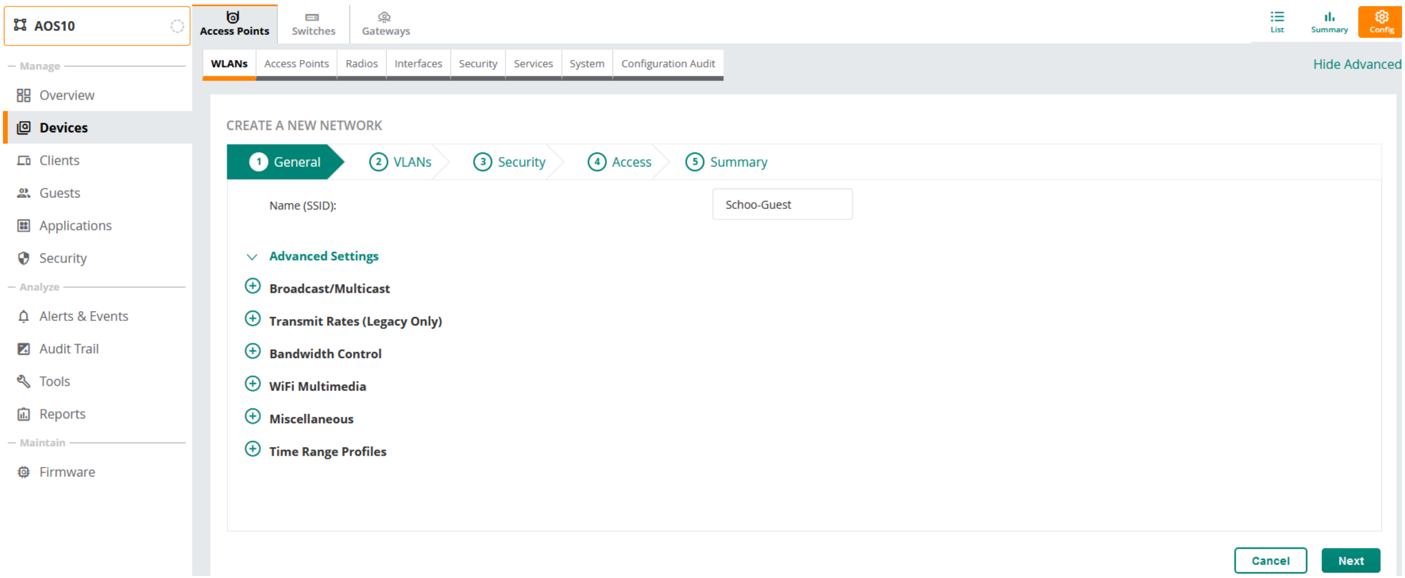


8 Guest Access Configuration

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.

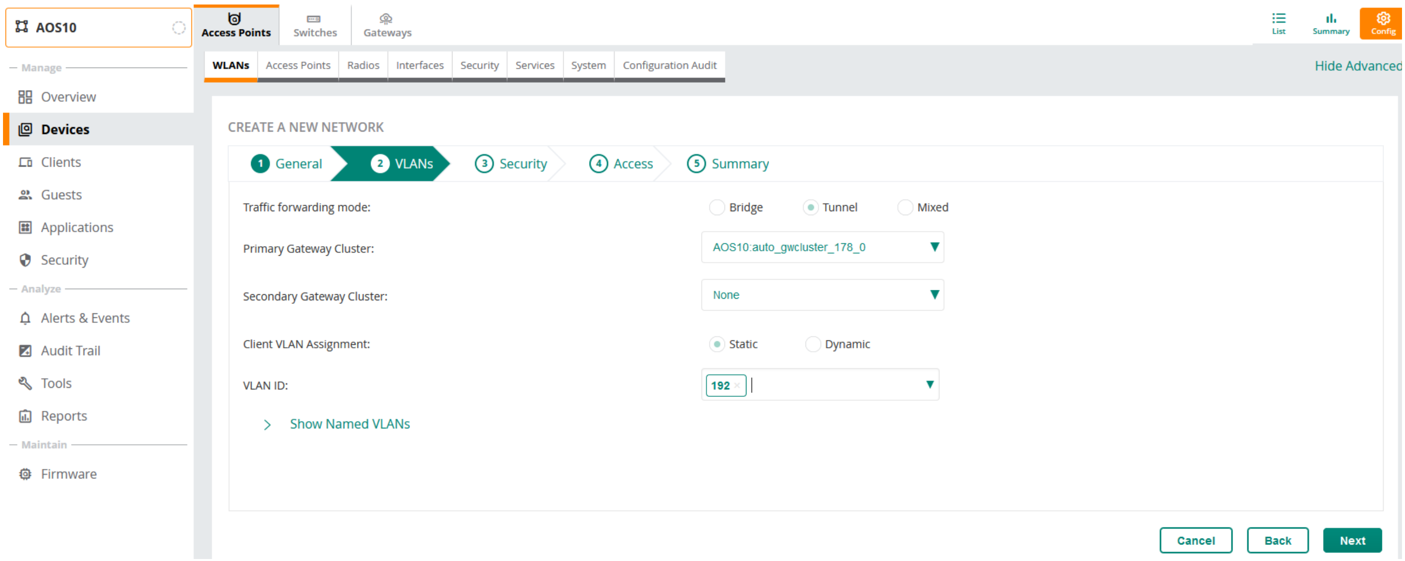


CREATE A NEW NETWORK

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

Name (SSID): Schoo-Guest

Advanced Settings
- Broadcast/Multicast
- Transmit Rates (Legacy Only)
- Bandwidth Control
- WiFi Multimedia
- Miscellaneous
- Time Range Profiles



CREATE A NEW NETWORK

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

Traffic forwarding mode: ○ Bridge ● Tunnel ○ Mixed

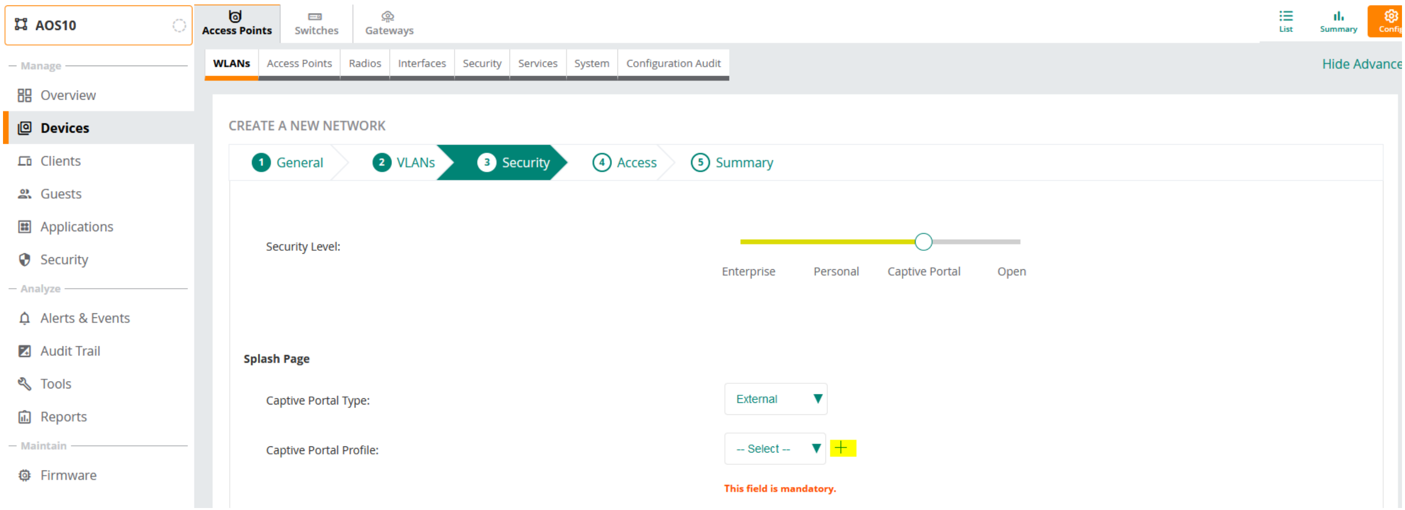
Primary Gateway Cluster: AOS10:auto_gwcluster_178_0

Secondary Gateway Cluster: None

Client VLAN Assignment: ● Static ○ Dynamic

VLAN ID: 192

Show Named VLANs



CREATE A NEW NETWORK

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

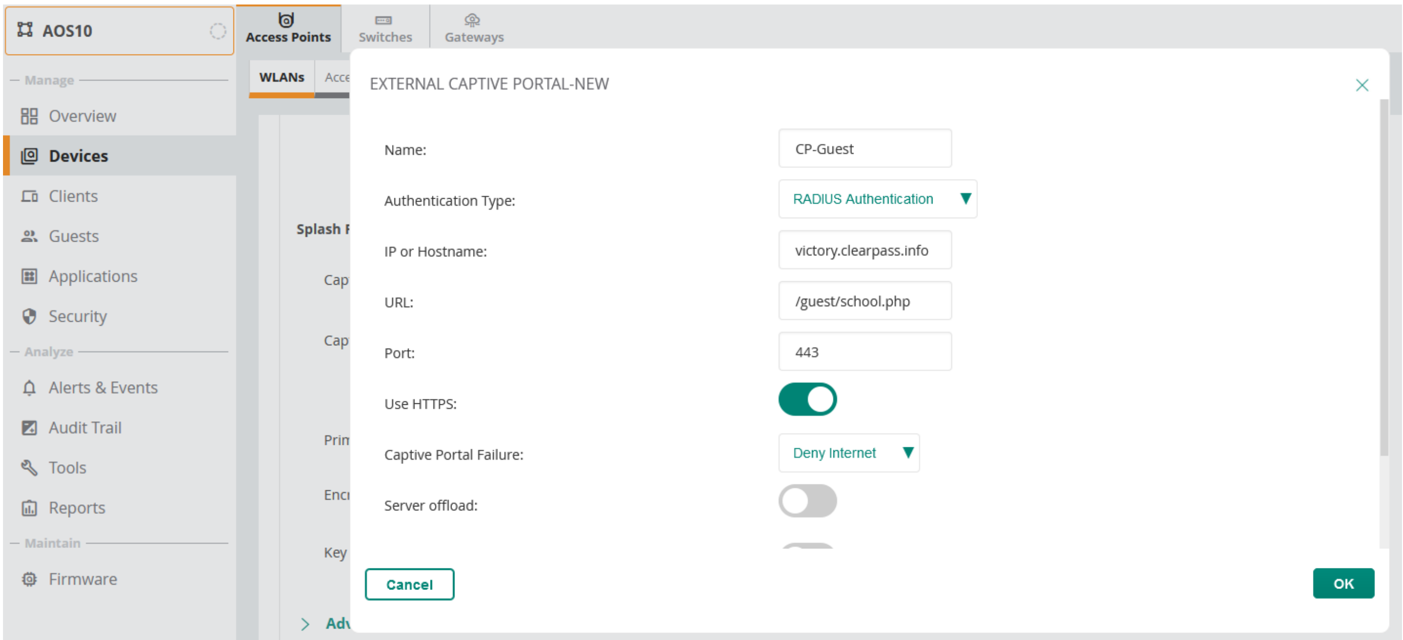
Security Level: Enterprise | Personal | Captive Portal | Open

Splash Page

Captive Portal Type: External

Captive Portal Profile: -- Select --

This field is mandatory.



EXTERNAL CAPTIVE PORTAL-NEW

Name: CP-Guest

Authentication Type: RADIUS Authentication

IP or Hostname: victory.clearpass.info

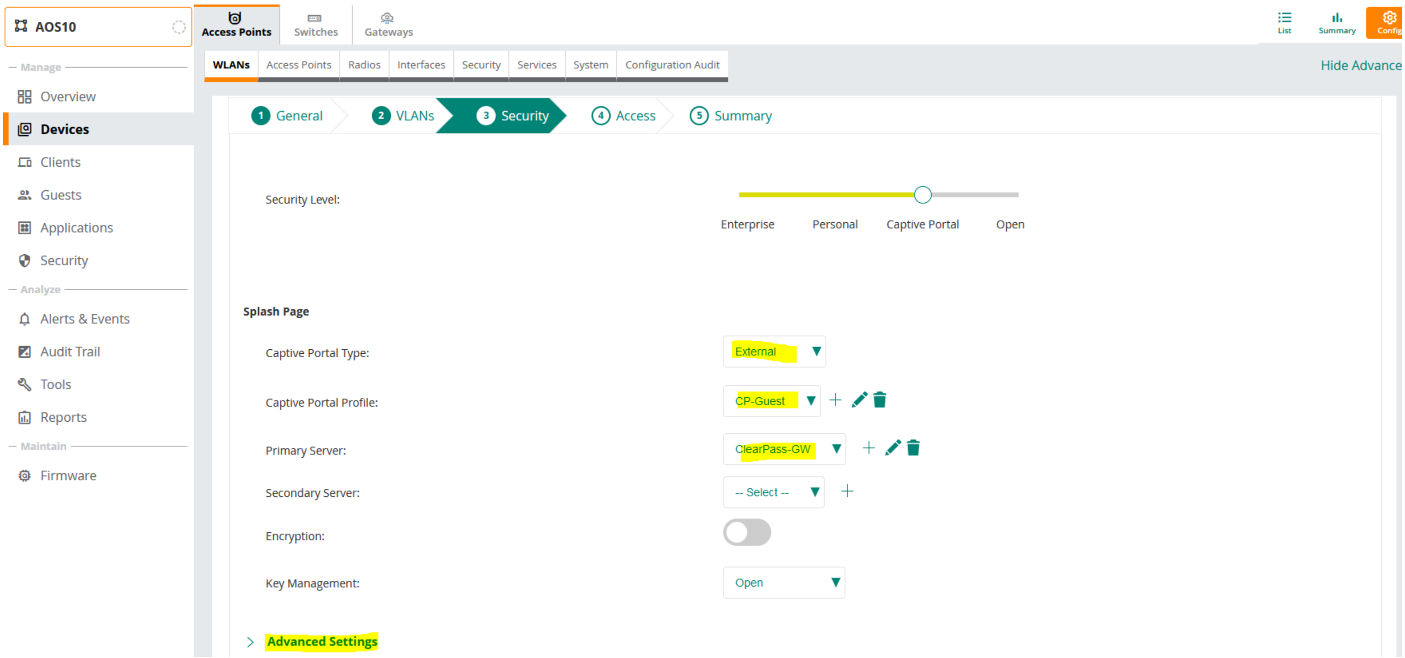
URL: /guest/school.php

Port: 443

Use HTTPS: On

Captive Portal Failure: Deny Internet

Server offload: Off



Security Level: Captive Portal

Enterprise Personal Captive Portal Open

Splash Page

Captive Portal Type: External

Captive Portal Profile: CP-Guest

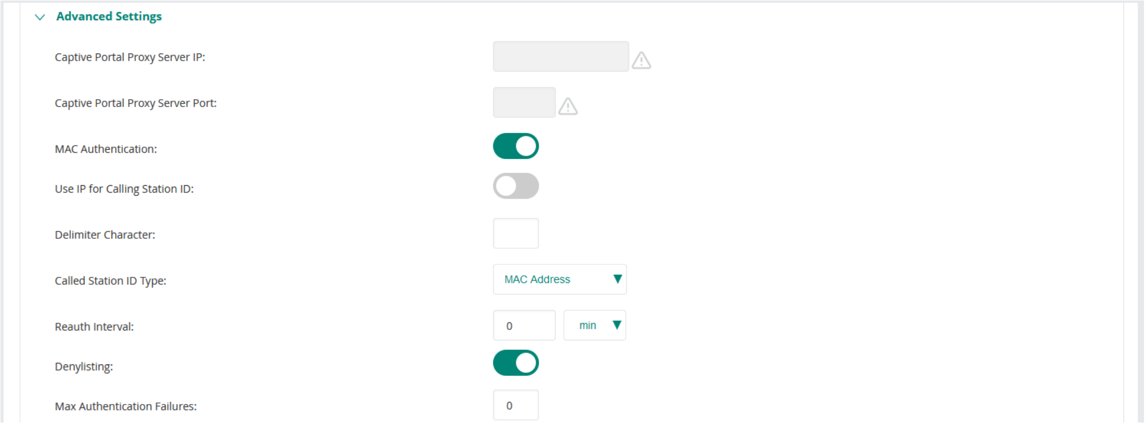
Primary Server: ClearPass-GW

Secondary Server: -- Select --

Encryption: Off

Key Management: Open

> Advanced Settings



Advanced Settings

Captive Portal Proxy Server IP:

Captive Portal Proxy Server Port:

MAC Authentication: On

Use IP for Calling Station ID: Off

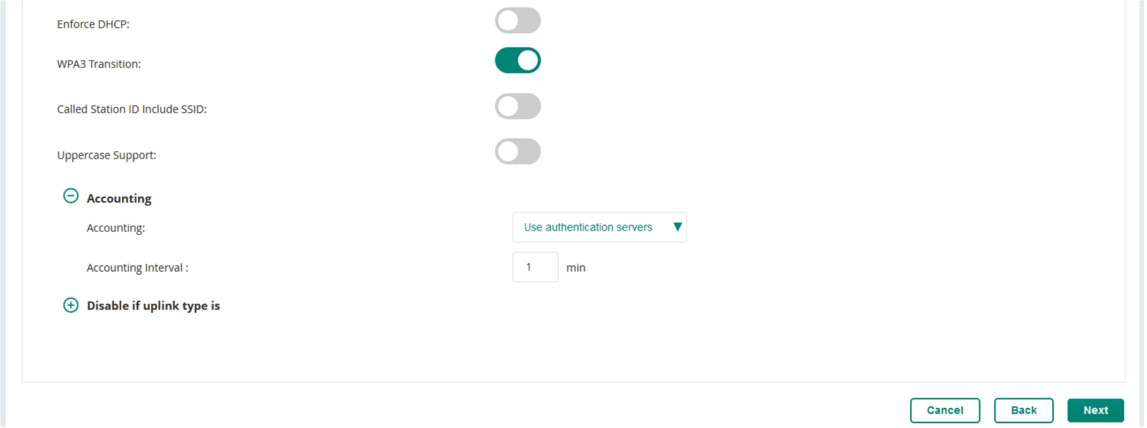
Delimiter Character:

Called Station ID Type: MAC Address

Reauth Interval: 0 min

Denylisting: On

Max Authentication Failures: 0



Enforce DHCP: Off

WPA3 Transition: On

Called Station ID Include SSID: Off

Uppercase Support: Off

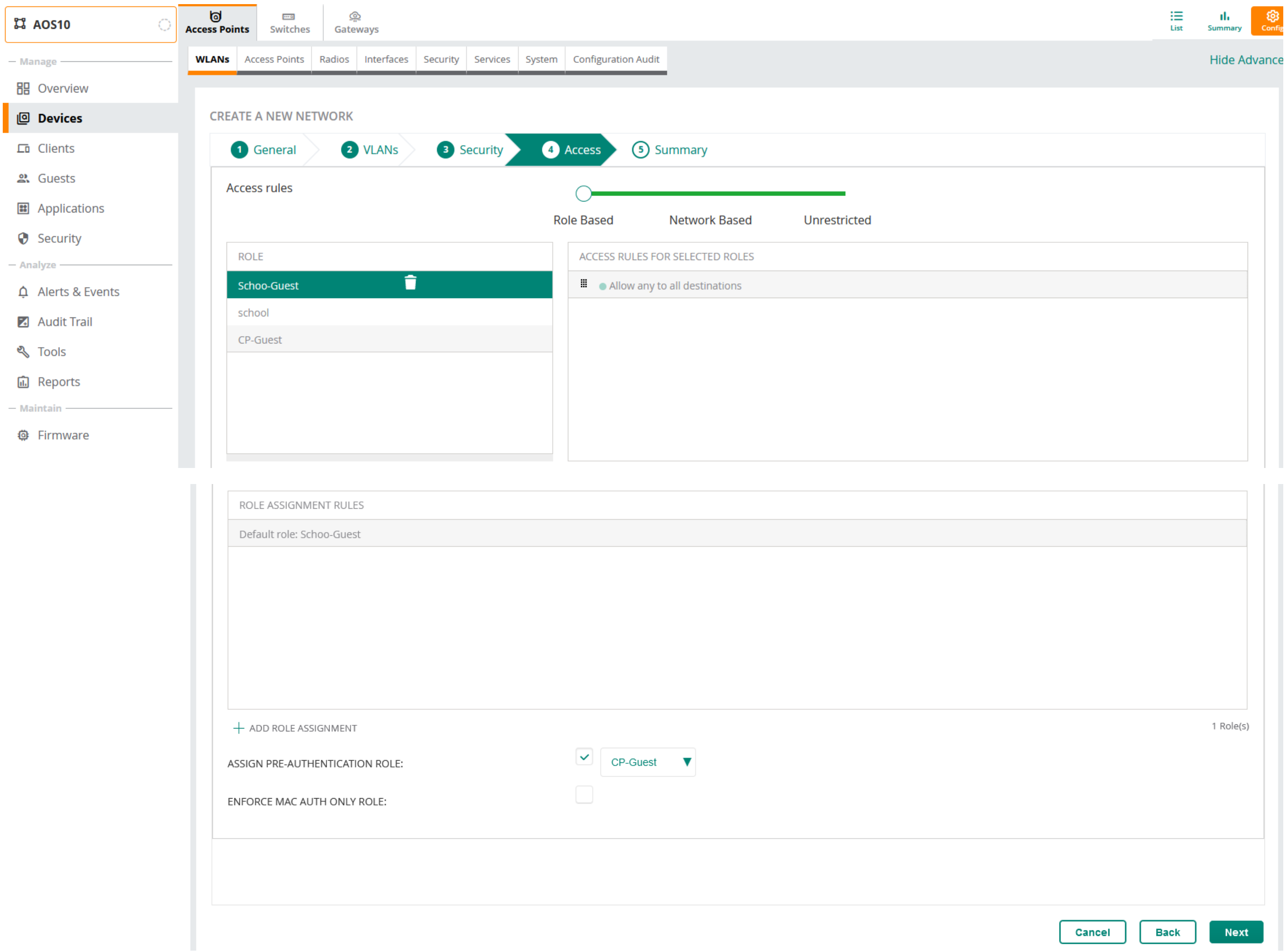
Accounting

Accounting: Use authentication servers

Accounting Interval : 1 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.



CREATE A NEW NETWORK

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

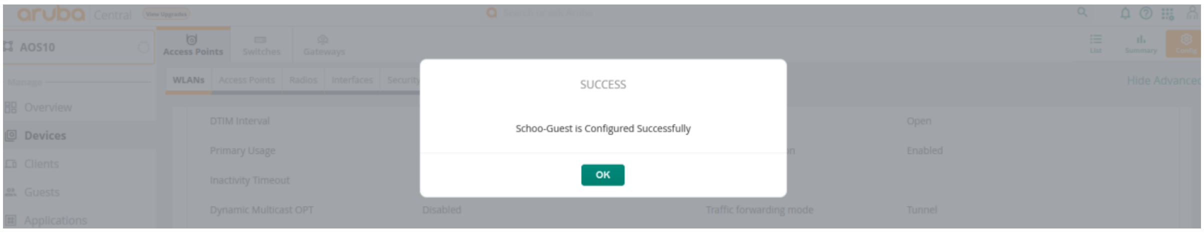
Default role: Schoo-Guest

ADD ROLE ASSIGNMENT

1 Role(s)

ASSIGN PRE-AUTHENTICATION ROLE: ☑ CP-Guest

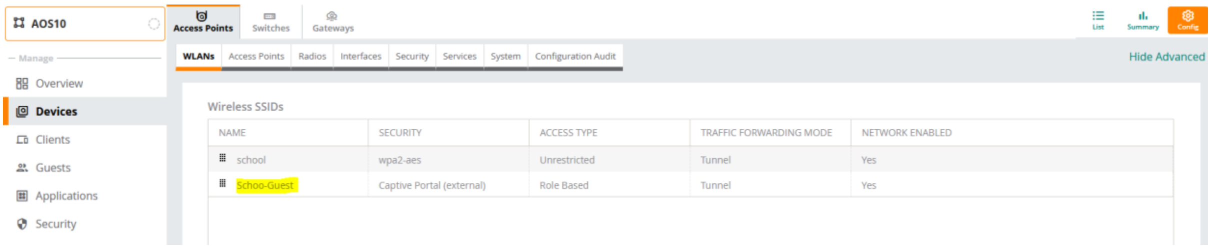
ENFORCE MAC AUTH ONLY ROLE: □



SUCCESS

Schoo-Guest is Configured Successfully

Now we have our Guest SSID configured.

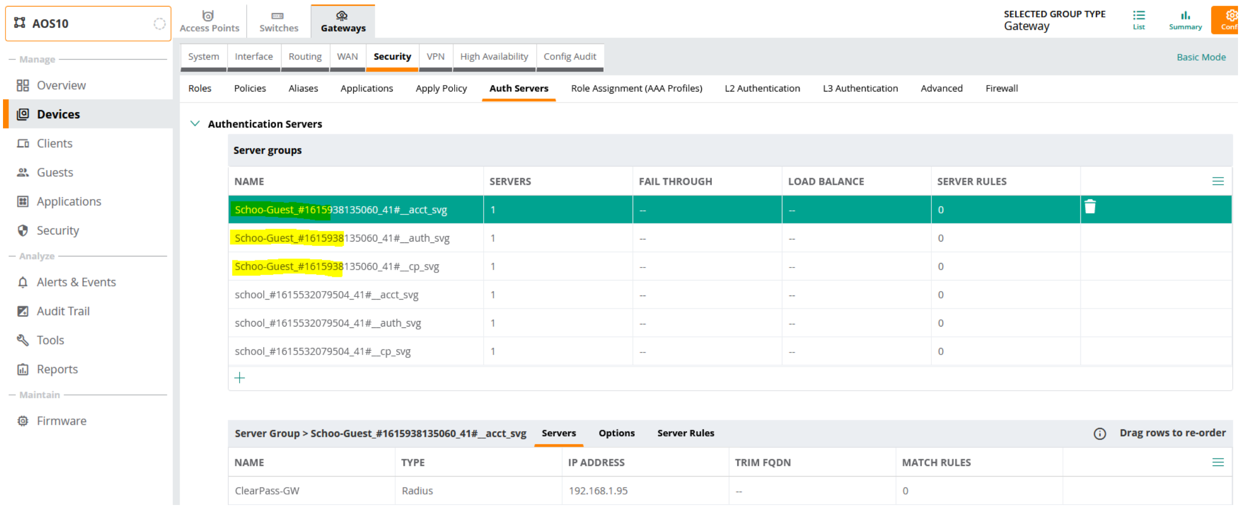


Wireless SSIDs

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



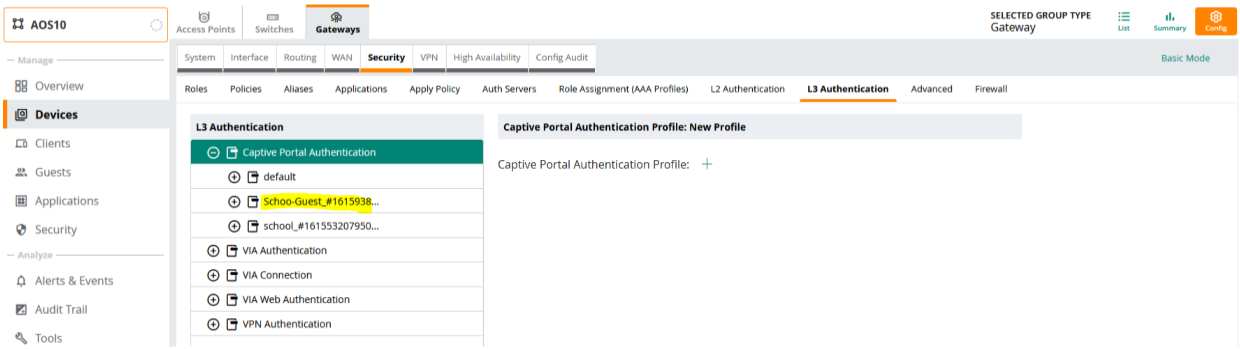
Authentication Servers

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   Servers   Options   Server Rules   Drag rows to re-order

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

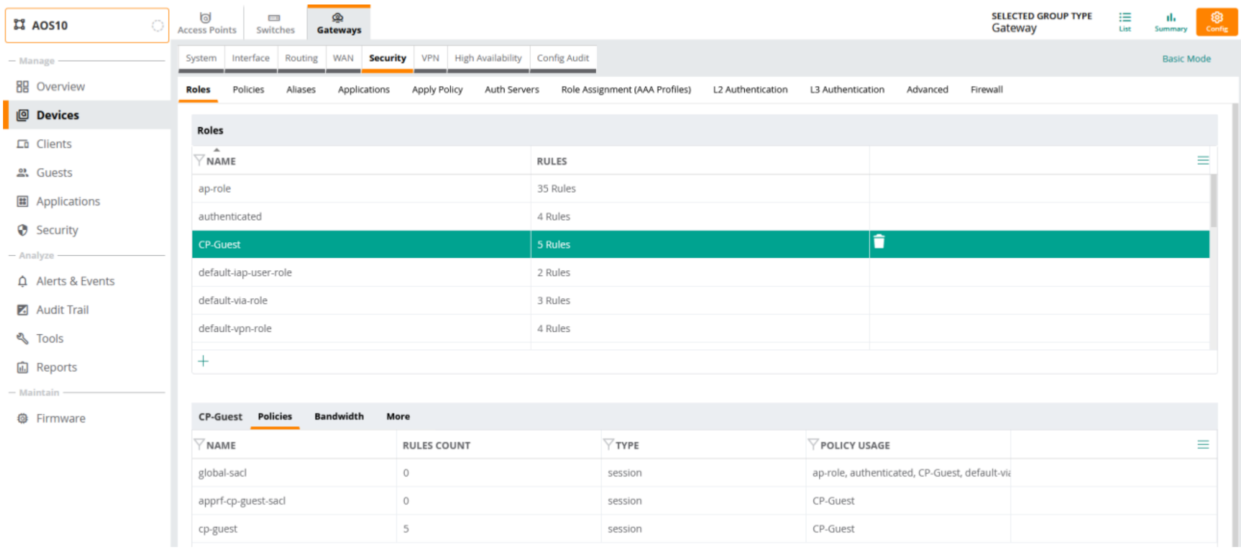


L3 Authentication

- Captive Portal Authentication
  - default
  - Schoo-Guest_#1615938...
  - school_#161553207950...
- VIA Authentication
- VIA Connection
- VIA Web Authentication
- VPN Authentication

Captive Portal Authentication Profile: New Profile

Captive Portal Authentication Profile: +



Roles

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

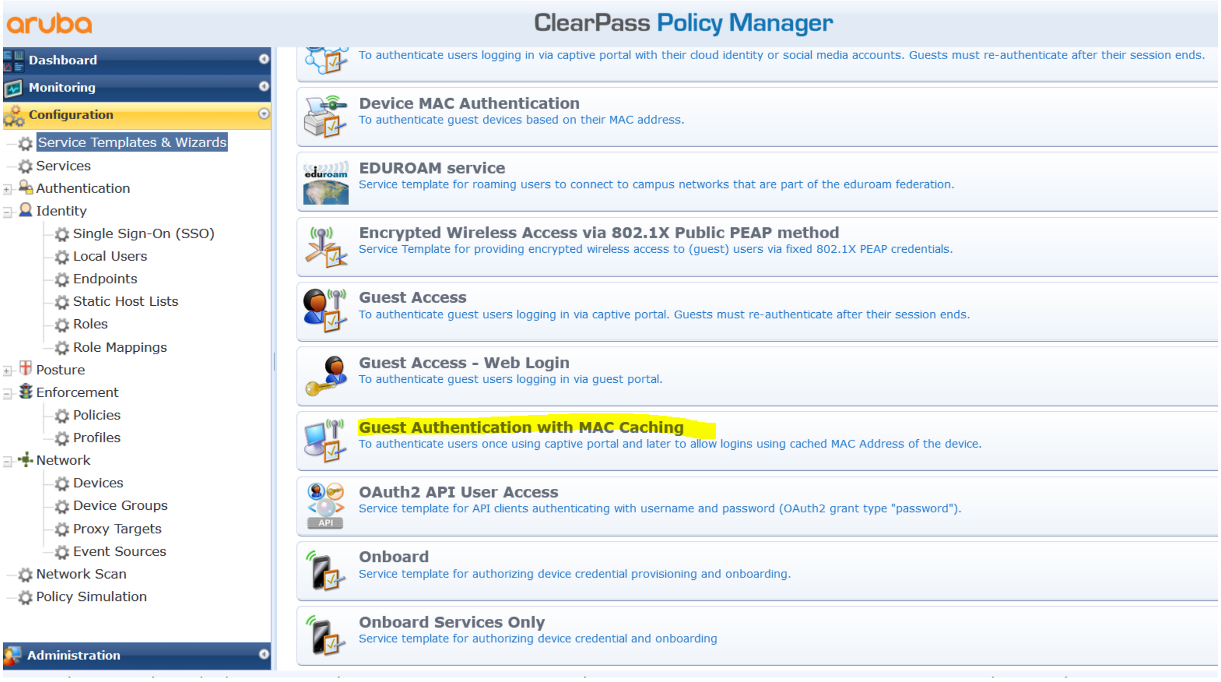
CP-Guest   Policies   Bandwidth   More

NAME	RULES COUNT	TYPE	POLICY USAGE
global-sacl	0	session	ap-role, authenticated, CP-Guest, default-vi
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.



To authenticate users logging in via captive portal with their cloud identity or social media accounts. Guests must re-authenticate after their session ends.

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.

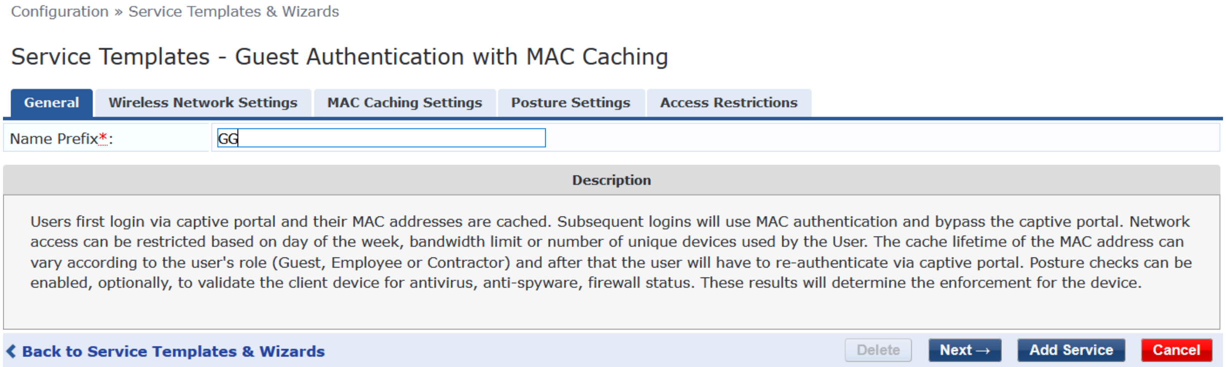
Guest Access - Web Login
To authenticate guest users logging in via guest portal.

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

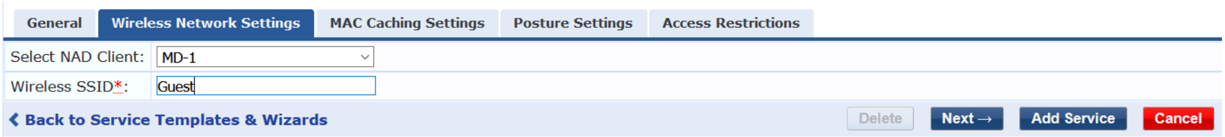

Configuration » Service Templates & Wizards
General
Wireless Network Settings
MAC Caching Settings
Posture Settings
Access Restrictions
Back to Service Templates & Wizards
Delete
Next →
Add Service
Cancel

Service Templates - Guest Authentication with MAC Caching

Name Prefix*: GG

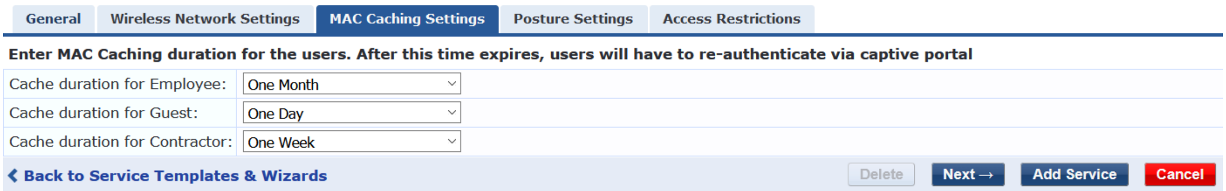
Description

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.



Select NAD Client: MD-1

Wireless SSID*: Guest

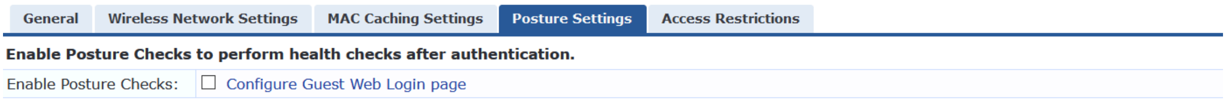


Enter MAC Caching duration for the users. After this time expires, users will have to re-authenticate via captive portal

Cache duration for Employee: One Month

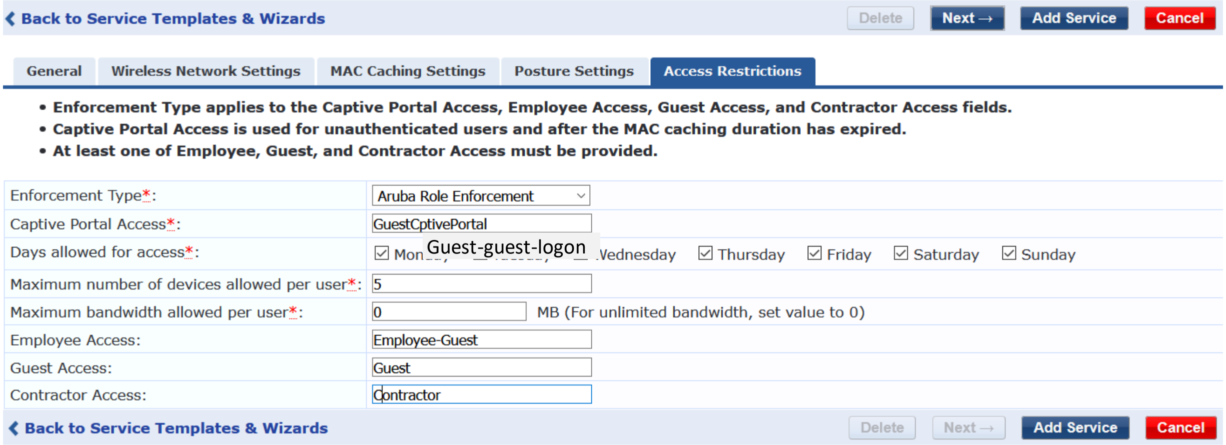
Cache duration for Guest: One Day

Cache duration for Contractor: One Week



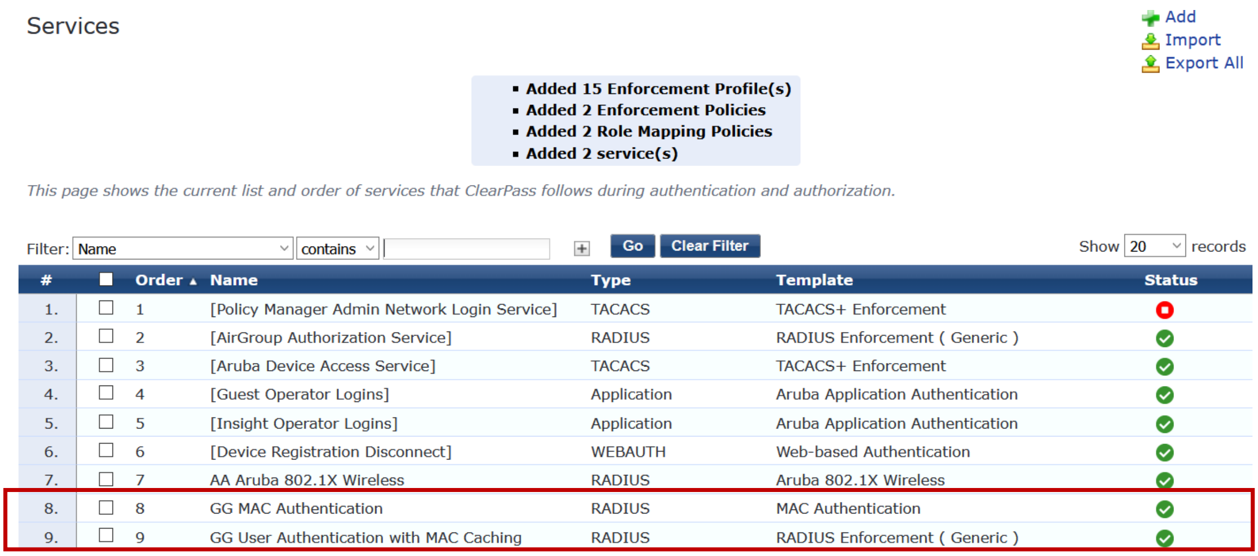
Enable Posture Checks to perform health checks after authentication.

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*:	GuestCptivePortal
Days allowed for access*:	☑ Mon Guest-guest-logon 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

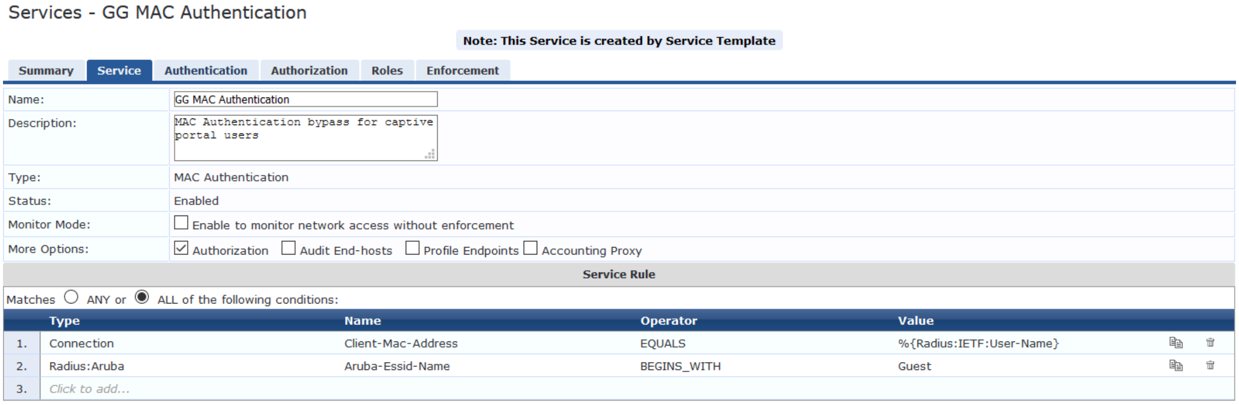
- **Added 15 Enforcement Profile(s)**
- **Added 2 Enforcement Policies**
- **Added 2 Role Mapping Policies**
- **Added 2 service(s)**

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

Filter: Name contains 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

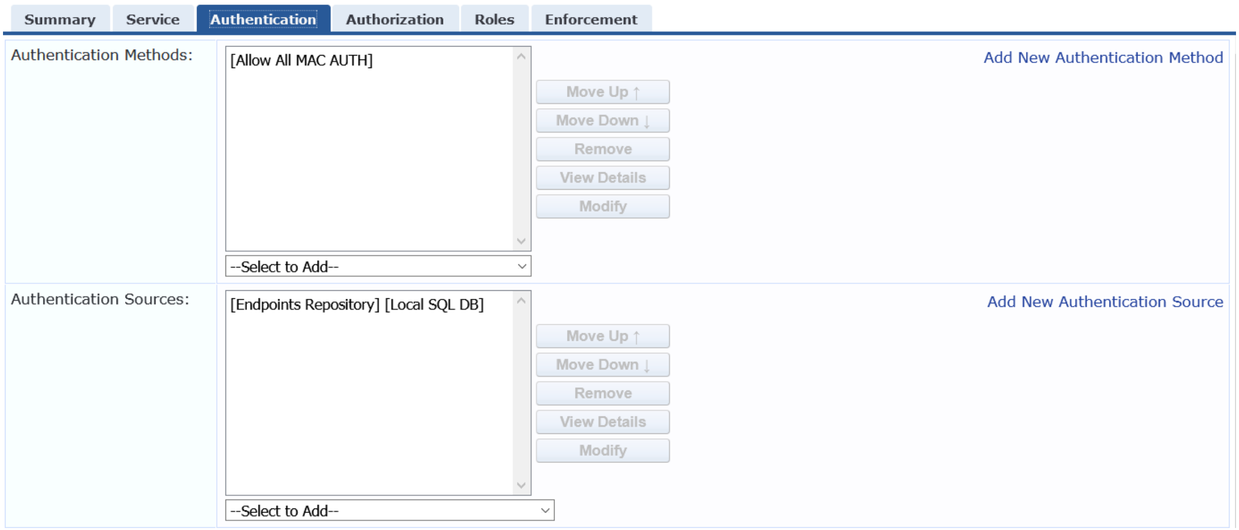
Note: This Service is created by Service Template

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

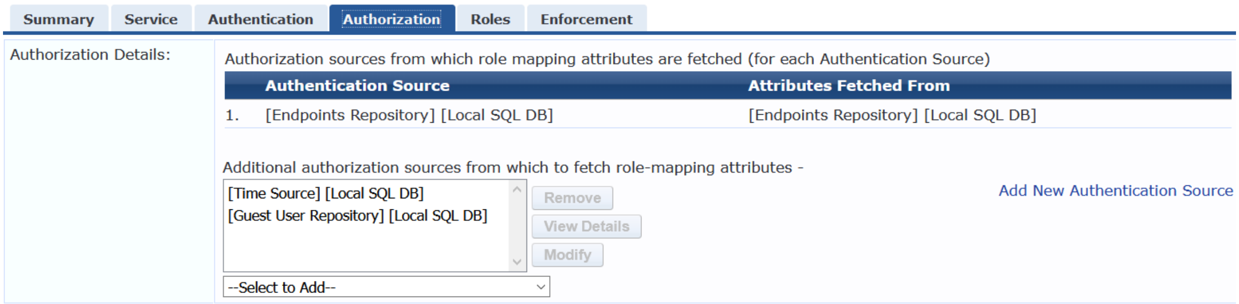
Service Rule

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...*			



Authentication Methods:	[Allow All MAC AUTH] --Select to Add--
Authentication Sources:	[Endpoints Repository] [Local SQL DB] --Select to Add--



Authorization Details:

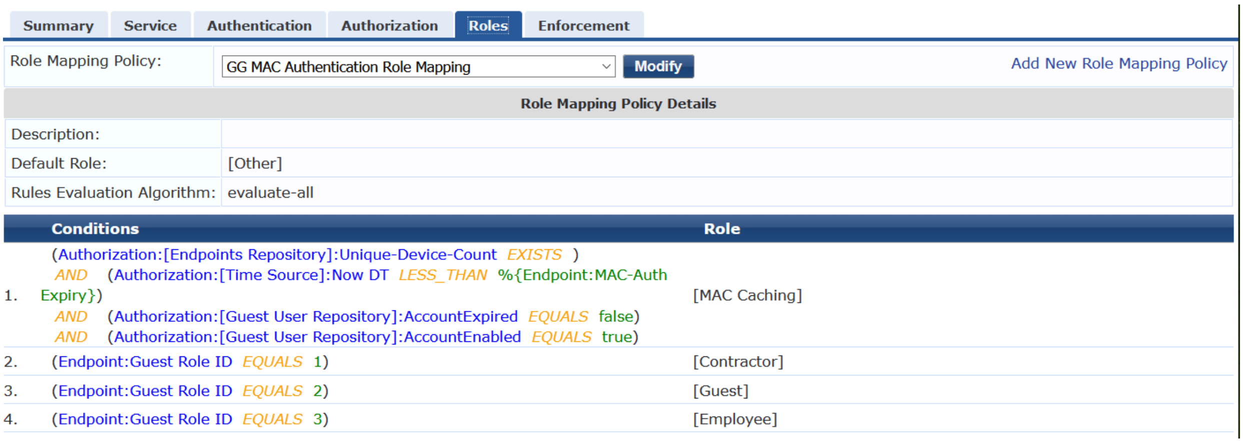
Authorization sources from which role mapping attributes are fetched (for each Authentication Source)

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

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

[Time Source] [Local SQL DB]
[Guest User Repository] [Local SQL DB]

--Select to Add--

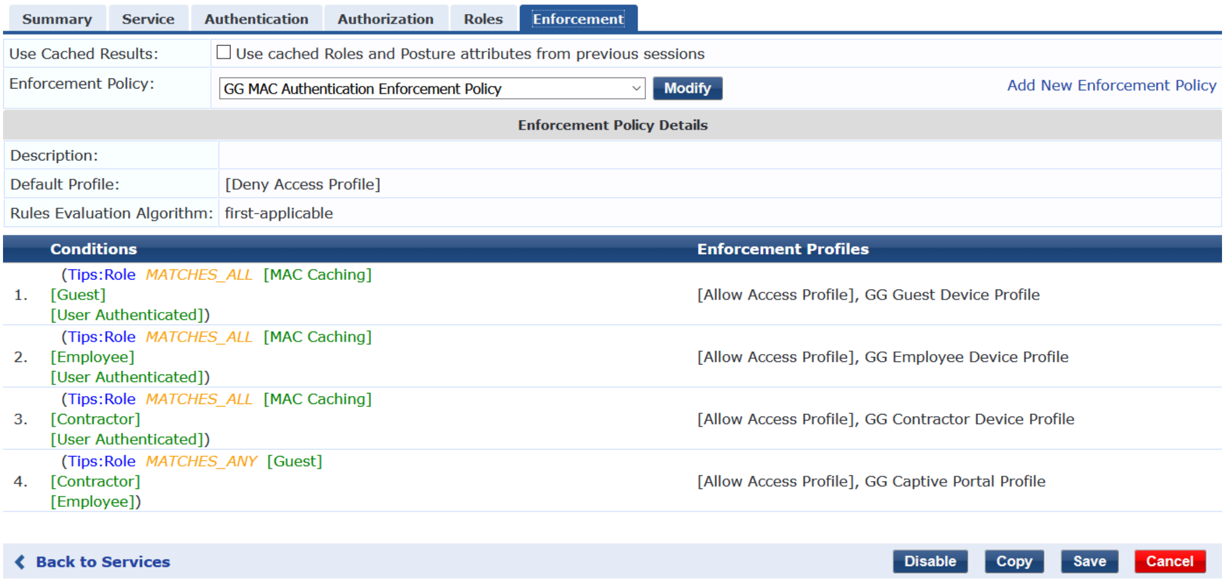


Role Mapping Policy: GG MAC Authentication Role Mapping

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]



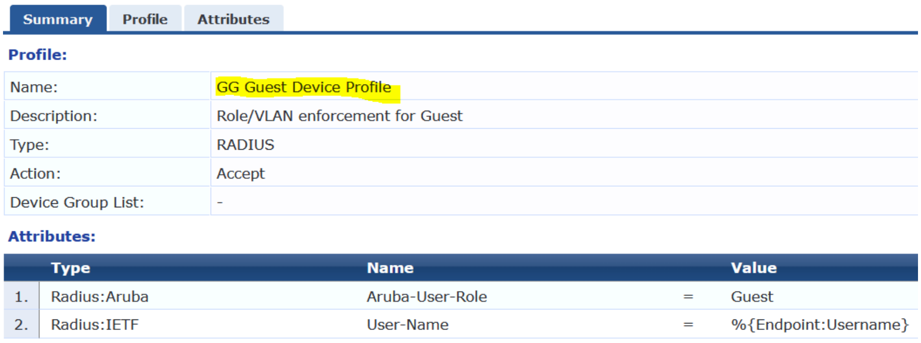
Use Cached Results:	☐ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	GG MAC Authentication Enforcement Policy

Enforcement Policy Details

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

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

And here are the enforcement profiles that are used here

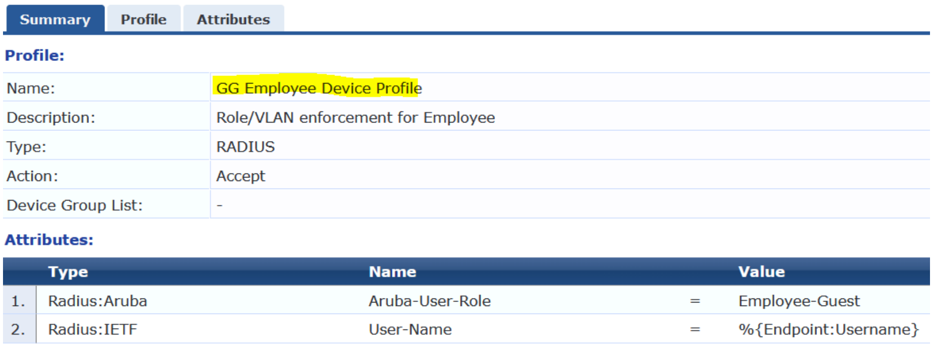


Profile:

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}

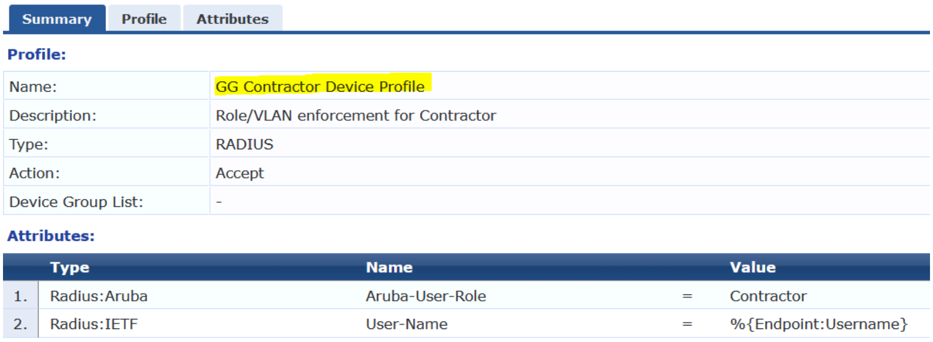


Profile:

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}

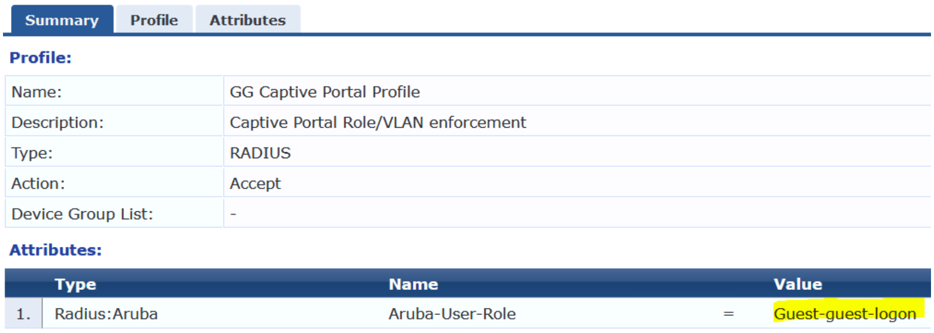


Profile:

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}



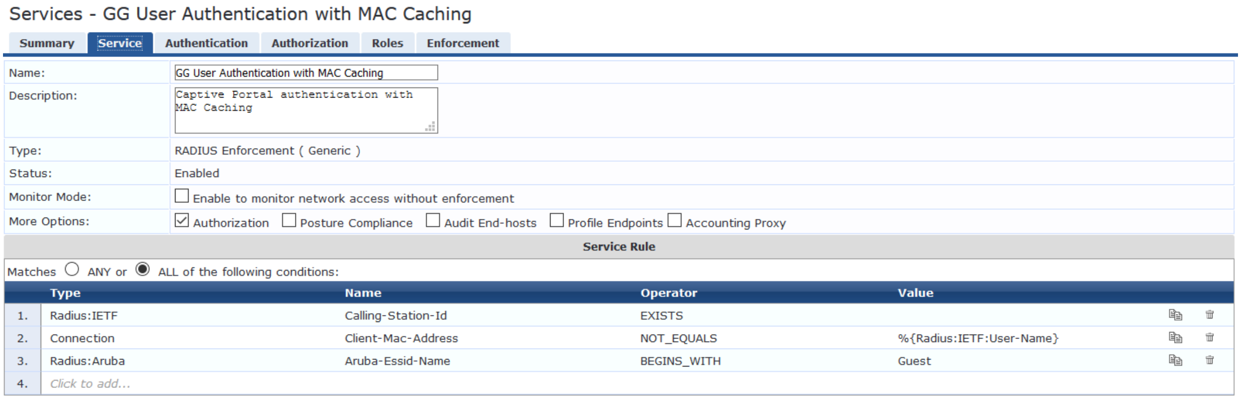
Profile:

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-logon

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

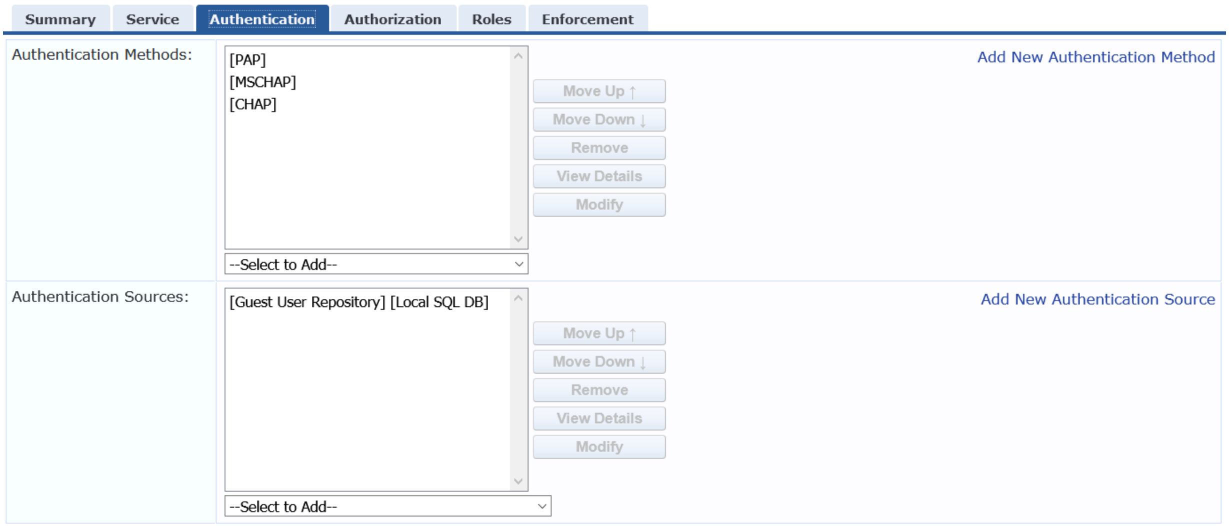

Services - GG User Authentication with MAC Caching

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

Service Rule

Matches ○ ANY or ● ALL of the following conditions:

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

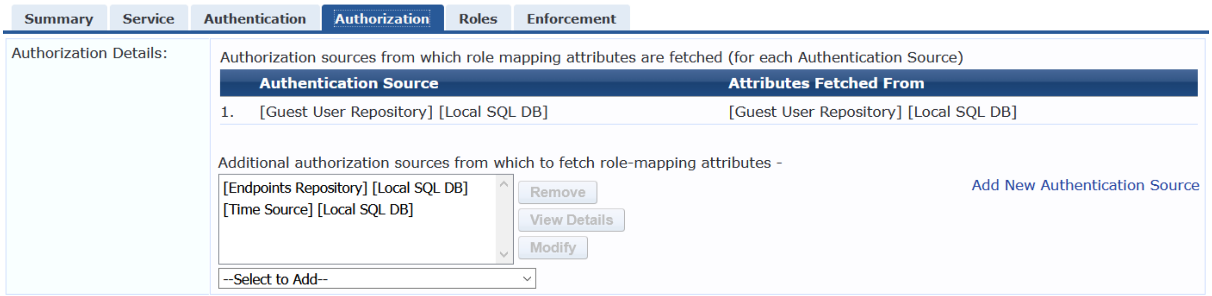


Authentication Methods: [PAP]
[MSCHAP]
[CHAP]

--Select to Add--

Authentication Sources: [Guest User Repository] [Local SQL DB]

--Select to Add--



Authorization Details:

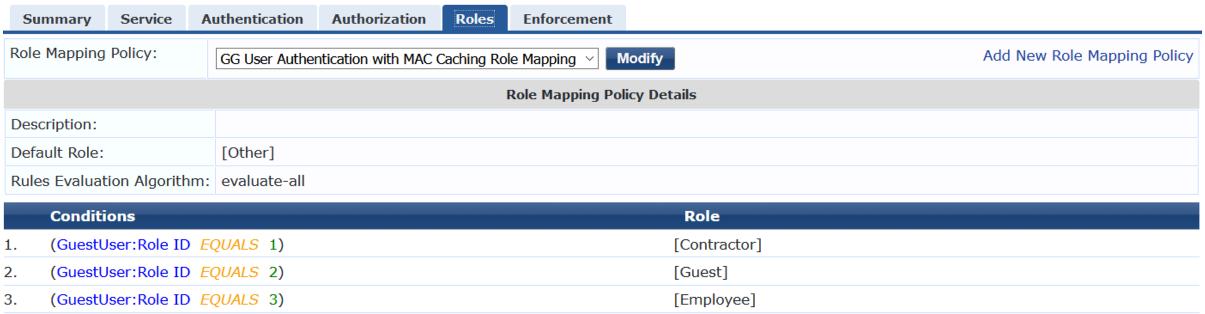
Authorization sources from which role mapping attributes are fetched (for each Authentication Source)

	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]

--Select to Add--

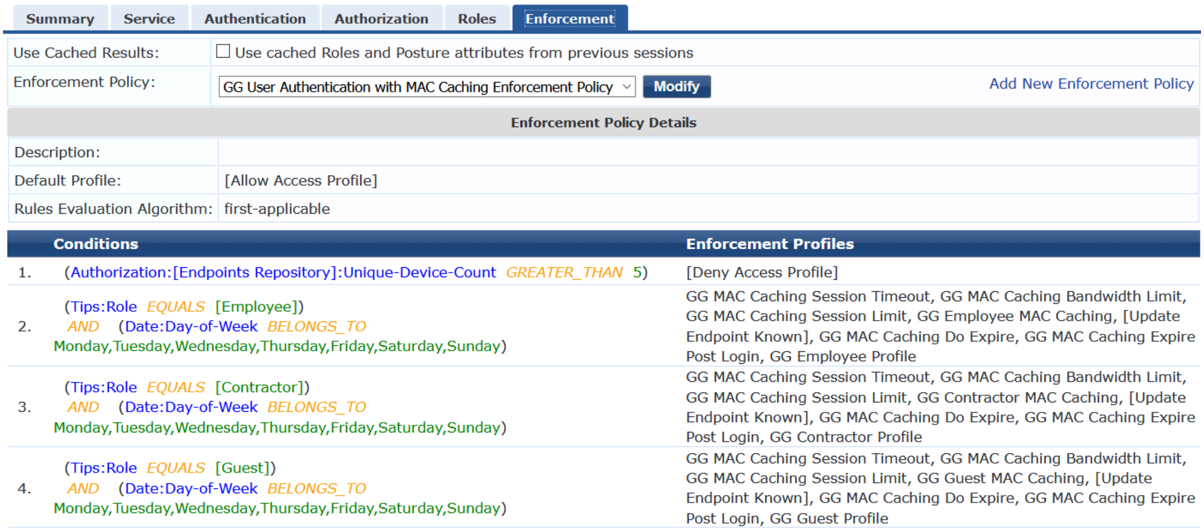


Role Mapping Policy: GG User Authentication with MAC Caching Role Mapping

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]



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

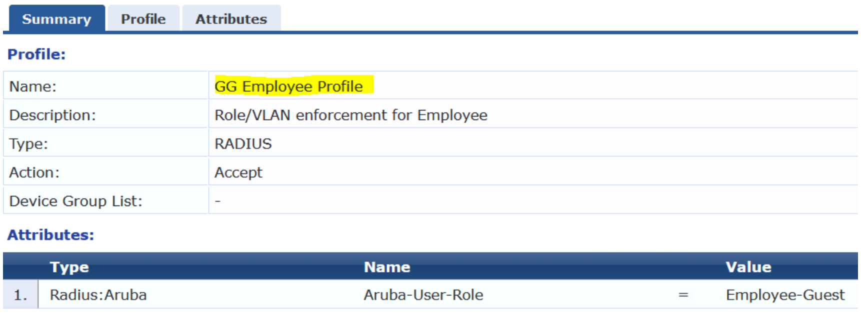
Enforcement Policy: GG User Authentication with MAC Caching Enforcement Policy

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

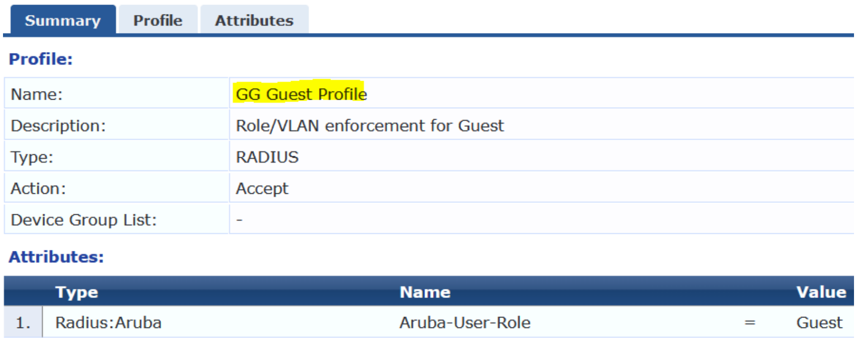


Profile:

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

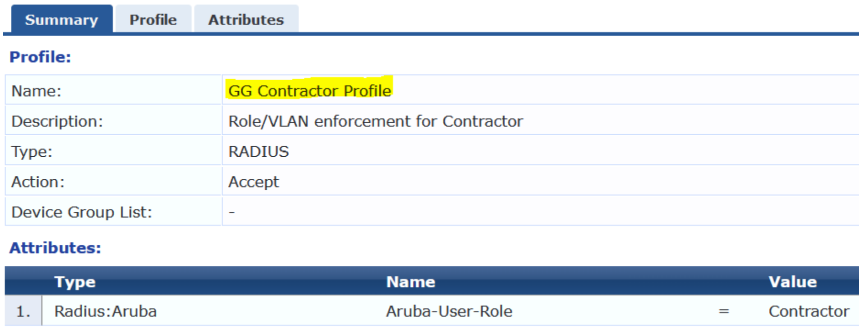


Profile:

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:

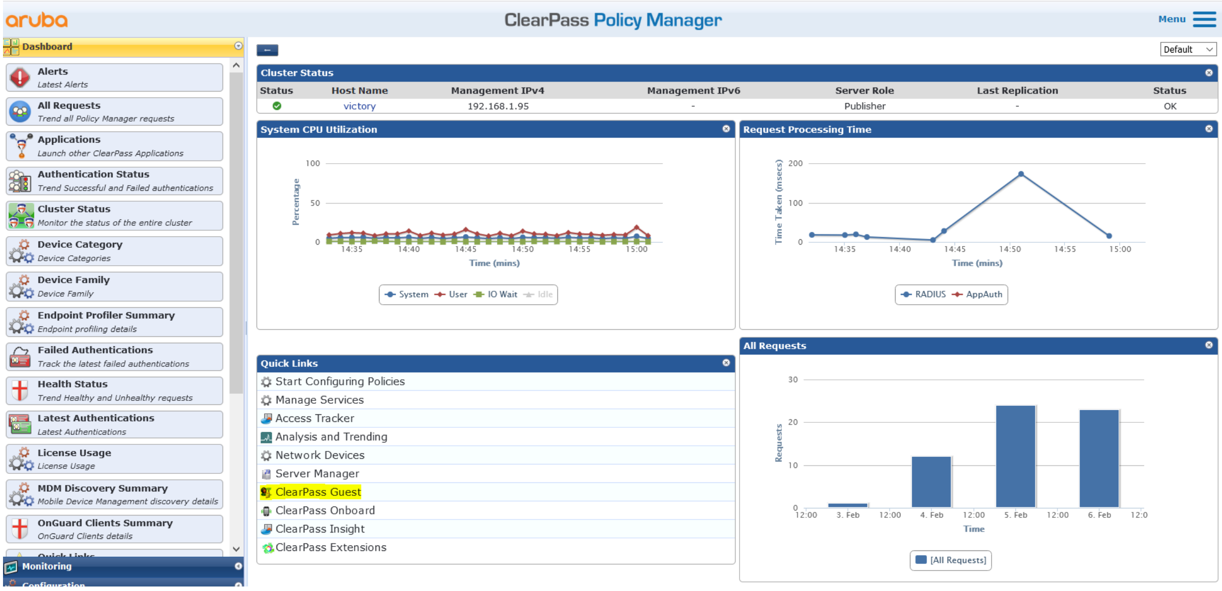
Name:	GG Contractor Profile
Description:	Role/VLAN enforcement for Contractor
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

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

8.3 ClearPass Guest Portal Configuration

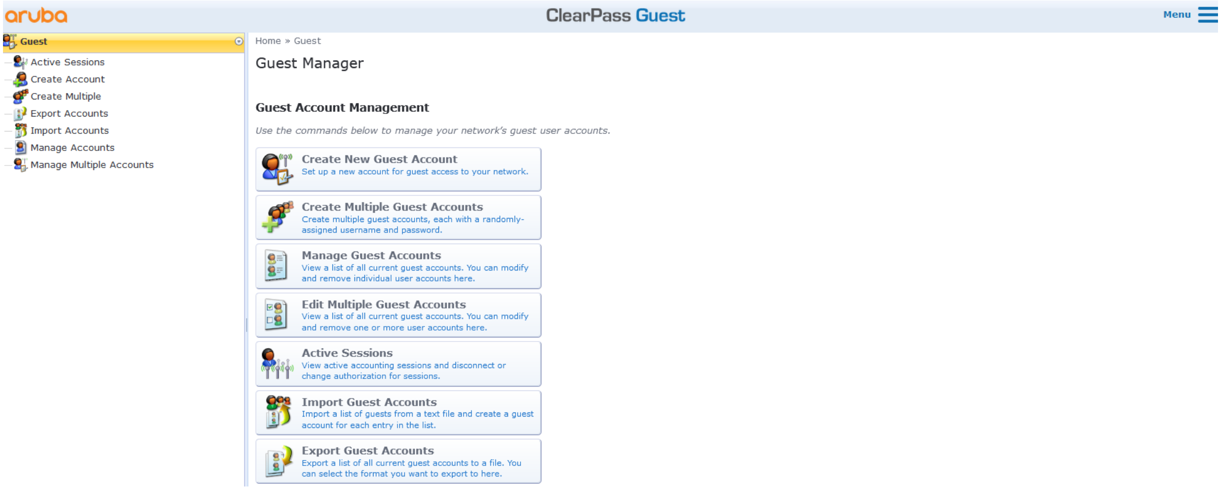
Here we'll configure the portal pages.



Cluster Status

Status	Host Name	Management IPv4	Management IPv6	Server Role	Last Replication	Status
✓	victory	192.168.1.95	-	Publisher	-	OK

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



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.

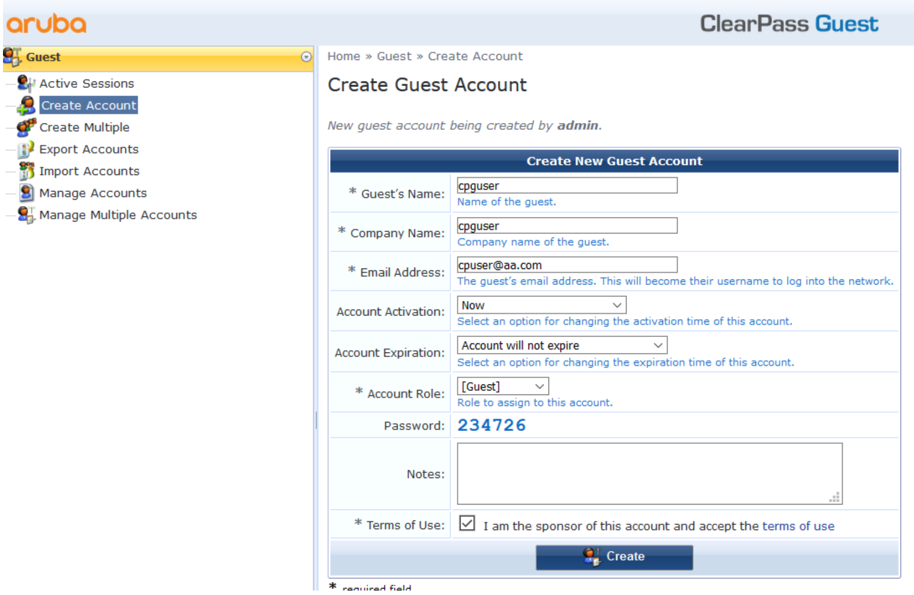
Manage Guest Accounts
View a list of all current guest accounts. You can modify and remove individual user accounts here.

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.

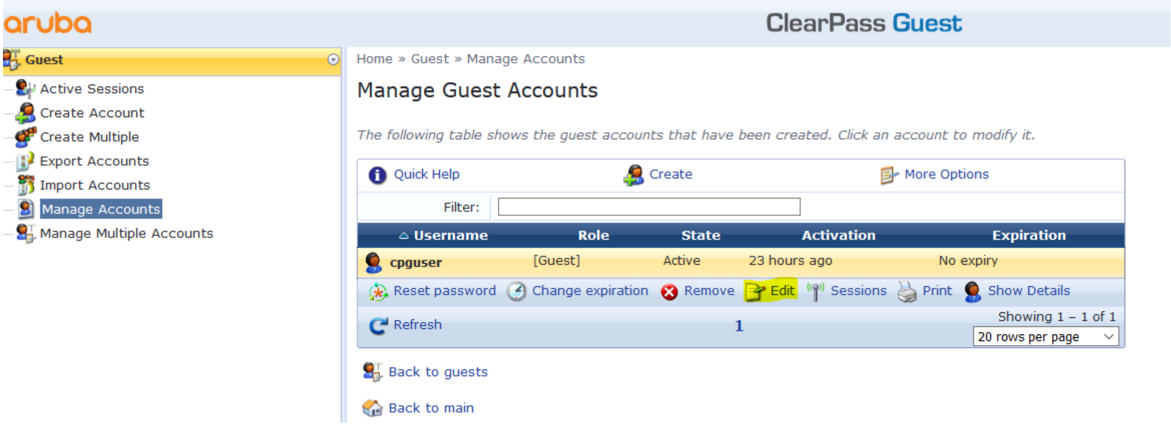


Create Guest Account

*New guest account being created by **admin**.*

Create New Guest Account	
* Guest's Name:	cpguser Name of the guest.
* Company Name:	cpguser Company name of the guest.
* Email Address:	cpuser@aa.com The guest's email address. This will become their username to log into the network.
Account Activation:	Now Select an option for changing the activation time of this account.
Account Expiration:	Account will not expire Select an option for changing the expiration time of this account.
* Account Role:	[Guest] Role to assign to this account.
Password:	234726
Notes:	
* Terms of Use:	☑ I am the sponsor of this account and accept the terms of use

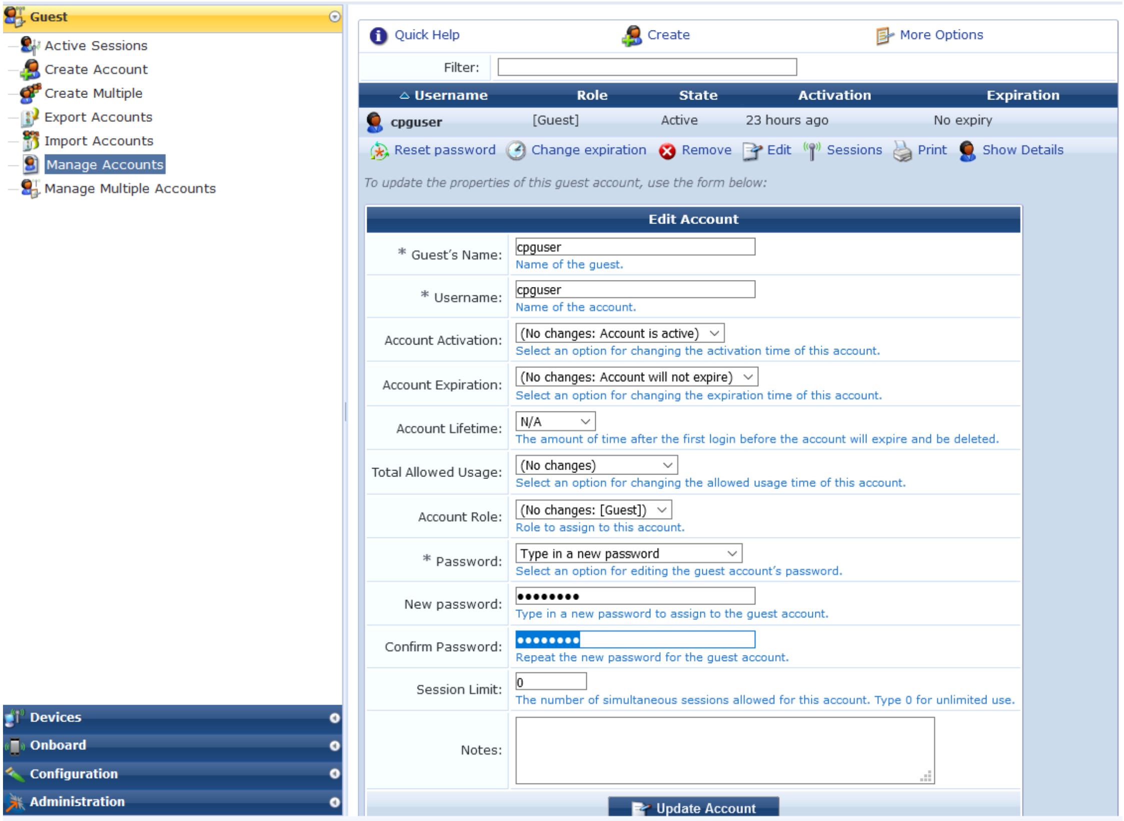
Once created we'll modify it to change the username and password



Manage Guest Accounts

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

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



Filter:

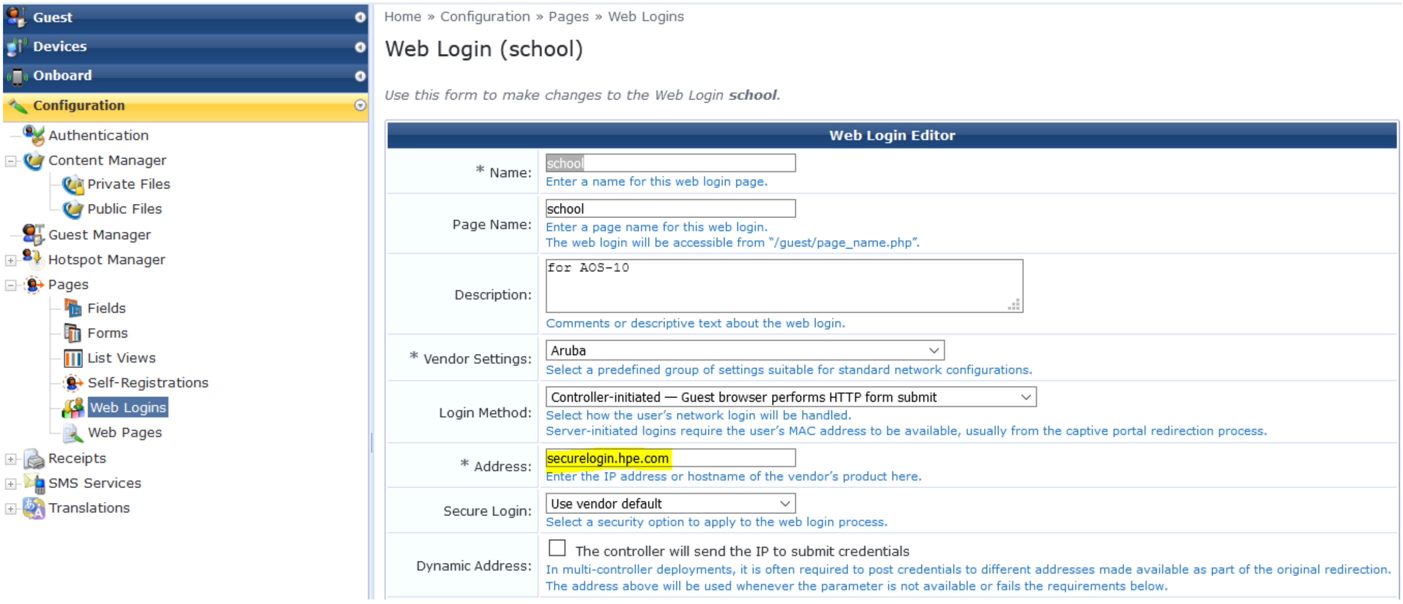
Username	Role	State	Activation	Expiration
cpguser	[Guest]	Active	23 hours ago	No expiry

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:	

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.



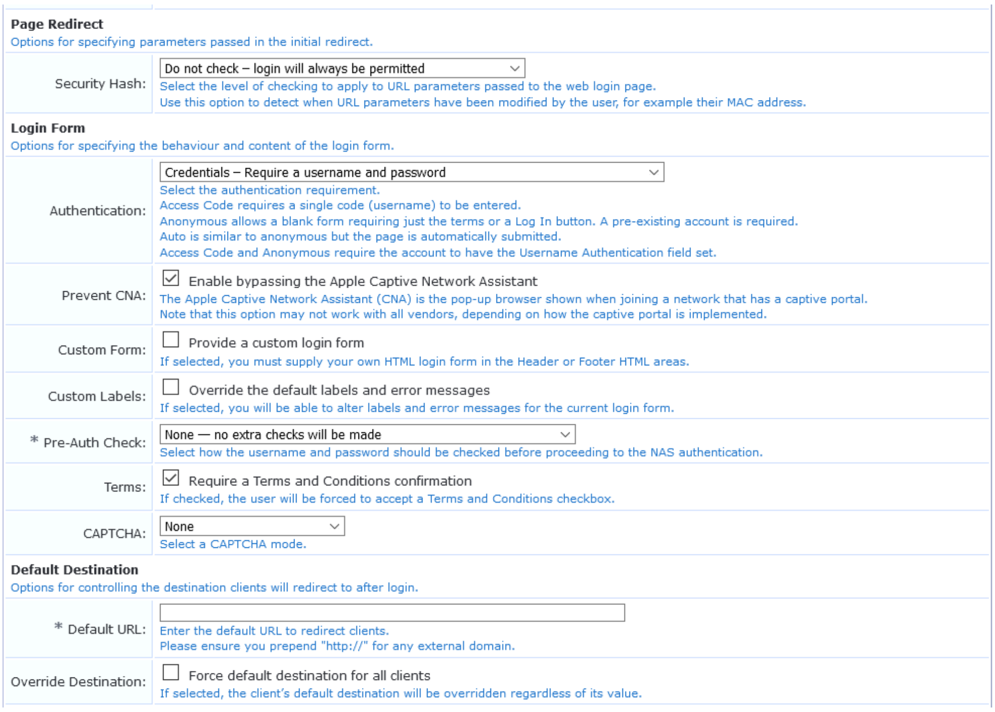
Home » Configuration » Pages » Web Logins

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.

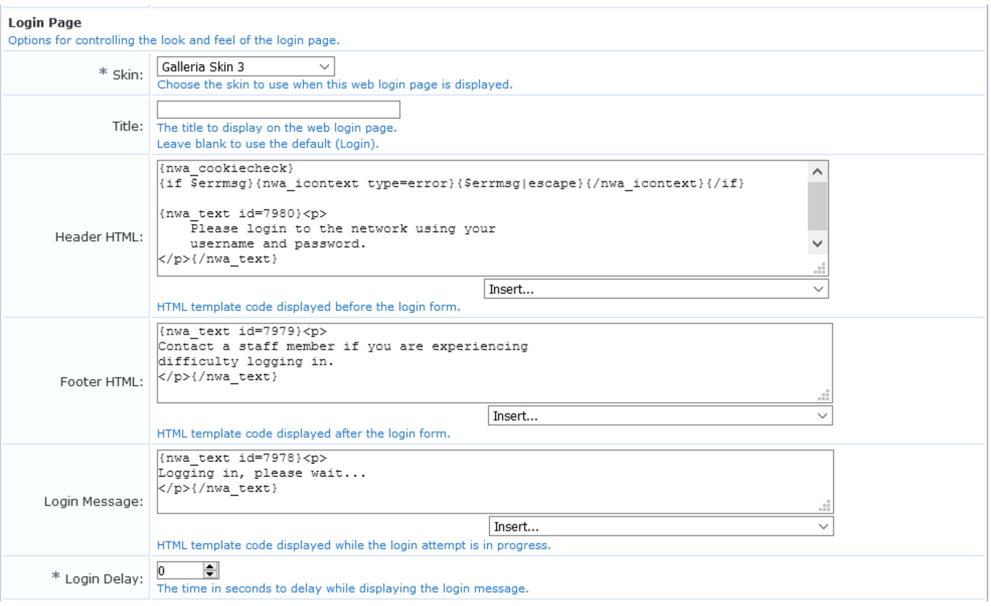
Security Hash:	Do not check – login will always be permitted Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.

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

Authentication:	Credentials – Require a username and password Select the authentication requirement. Access Code requires a single code (username) to be entered. Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required. Auto is similar to anonymous but the page is automatically submitted. Access Code and Anonymous require the account to have the Username Authentication field set.
Prevent CNA:	☑ Enable bypassing the Apple Captive Network Assistant The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.
Custom Form:	□ Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	□ Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.
* Pre-Auth Check:	None — no extra checks will be made Select how the username and password should be checked before proceeding to the NAS authentication.
Terms:	☑ Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.
CAPTCHA:	None Select a CAPTCHA mode.

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

* Default URL:	Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.
Override Destination:	□ Force default destination for all clients If selected, the client's default destination will be overridden regardless of its value.



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

* Skin:	Galleria Skin 3 Choose the skin to use when this web login page is displayed.
Title:	The title to display on the web login page. Leave blank to use the default (Login).

Header HTML:

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

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

Insert...
HTML template code displayed before the login form.

Footer HTML:

```
{nwa_text id=7979}<p>
Contact a staff member if you are experiencing
difficulty logging in.
</p>{/nwa_text}
```

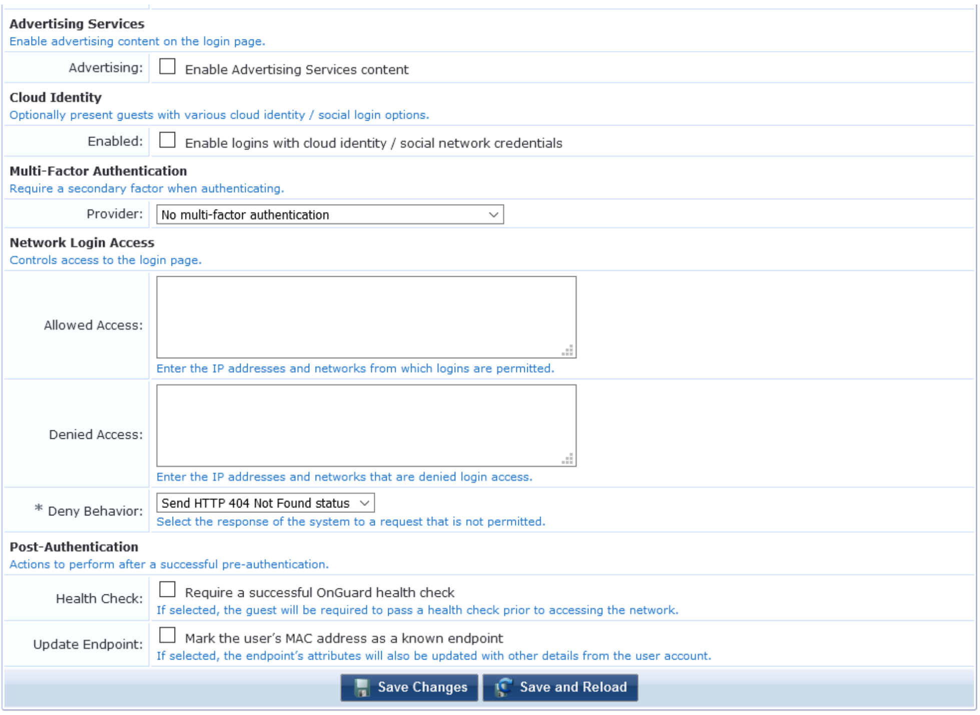
Insert...
HTML template code displayed after the login form.

Login Message:

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

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

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



Advertising Services
Enable advertising content on the login page.

Advertising:	□ Enable Advertising Services content

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

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

Multi-Factor Authentication
Require a secondary factor when authenticating.

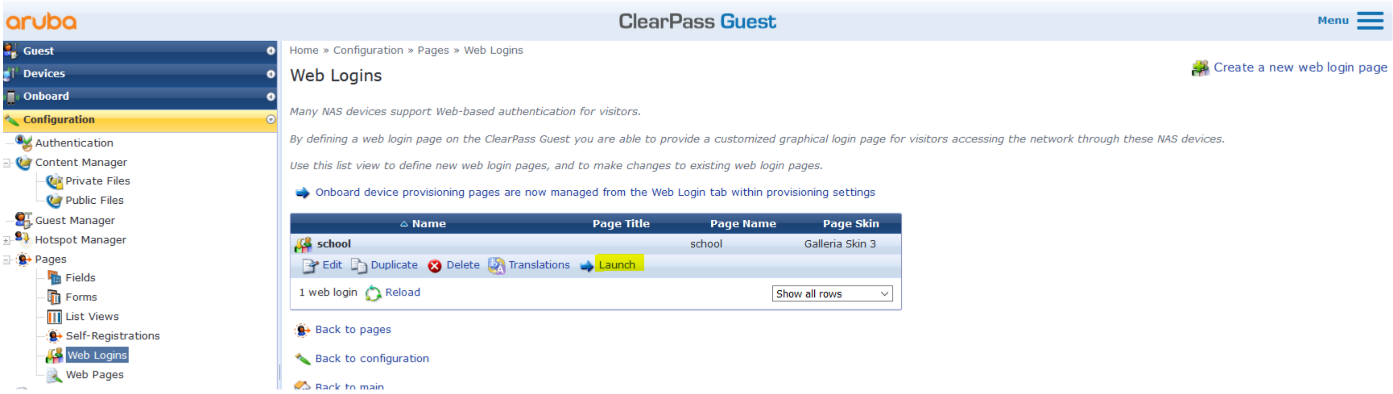
Provider:	No multi-factor authentication

Network Login Access
Controls access to the login page.

Allowed Access:	Enter the IP addresses and networks from which logins are permitted.
Denied Access:	Enter the IP addresses and networks that are denied login access.
* Deny Behavior:	Send HTTP 404 Not Found status Select the response of the system to a request that is not permitted.

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

Health Check:	□ Require a successful OnGuard health check If selected, the guest will be required to pass a health check prior to accessing the network.
Update Endpoint:	□ Mark the user's MAC address as a known endpoint If selected, the endpoint's attributes will also be updated with other details from the user account.



Web Logins

Many NAS devices support Web-based authentication for visitors.

By defining a web login page on the ClearPass Guest you are able to provide a customized graphical login page for visitors accessing the network through these NAS devices.

Use this list view to define new web login pages, and to make changes to existing web login pages.

Onboard device provisioning pages are now managed from the Web Login tab within provisioning settings

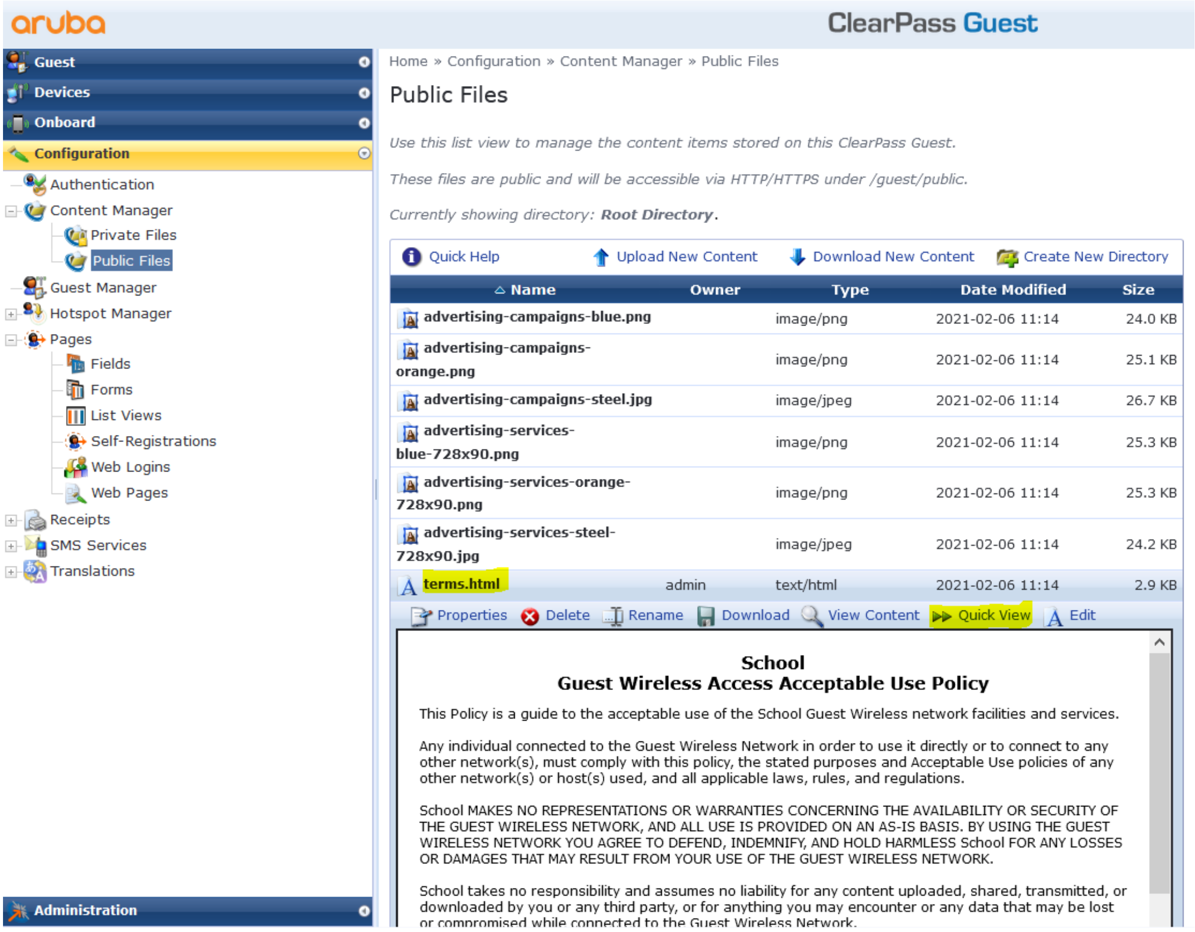
Name	Page Title	Page Name	Page Skin
school		school	Galleria Skin 3

1 web login

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.



Public Files

Use this list view to manage the content items stored on this ClearPass Guest.

These files are public and will be accessible via HTTP/HTTPS under /guest/public.

Currently showing directory: ***Root Directory*.**

Name	Owner	Type	Date Modified	Size
advertising-campaigns-blue.png		image/png	2021-02-06 11:14	24.0 KB
advertising-campaigns-orange.png		image/png	2021-02-06 11:14	25.1 KB
advertising-campaigns-steel.jpg		image/jpeg	2021-02-06 11:14	26.7 KB
advertising-services-blue-728x90.png		image/png	2021-02-06 11:14	25.3 KB
advertising-services-orange-728x90.png		image/png	2021-02-06 11:14	25.3 KB
advertising-services-steel-728x90.jpg		image/jpeg	2021-02-06 11:14	24.2 KB
terms.html	admin	text/html	2021-02-06 11:14	2.9 KB

School
Guest Wireless Access Acceptable Use Policy

This Policy is a guide to the acceptable use of the School Guest Wireless network facilities and services.

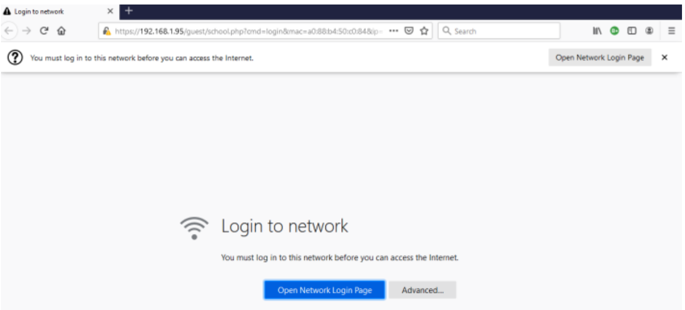
Any individual connected to the Guest Wireless Network in order to use it directly or to connect to any other network(s), must comply with this policy, the stated purposes and Acceptable Use policies of any other network(s) or host(s) used, and all applicable laws, rules, and regulations.

School MAKES NO REPRESENTATIONS OR WARRANTIES CONCERNING THE AVAILABILITY OR SECURITY OF THE GUEST WIRELESS NETWORK, AND ALL USE IS PROVIDED ON AN AS-IS BASIS. BY USING THE GUEST WIRELESS NETWORK YOU AGREE TO DEFEND, INDEMNIFY, AND HOLD HARMLESS School FOR ANY LOSSES OR DAMAGES THAT MAY RESULT FROM YOUR USE OF THE GUEST WIRELESS NETWORK.

School takes no responsibility and assumes no liability for any content uploaded, shared, transmitted, or downloaded by you or any third party, or for anything you may encounter or any data that may be lost or compromised while connected to the Guest Wireless Network.

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

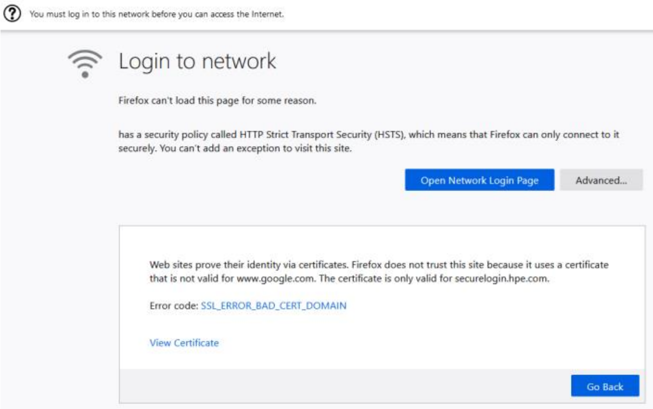


https://192.168.1.95/guest/school.php?cmd=login&mac=a0:88:b4:50:c0:84&ip=

You must log in to this network before you can access the Internet.

Login to network

You must log in to this network before you can access the Internet.



You must log in to this network before you can access the Internet.

Login to network

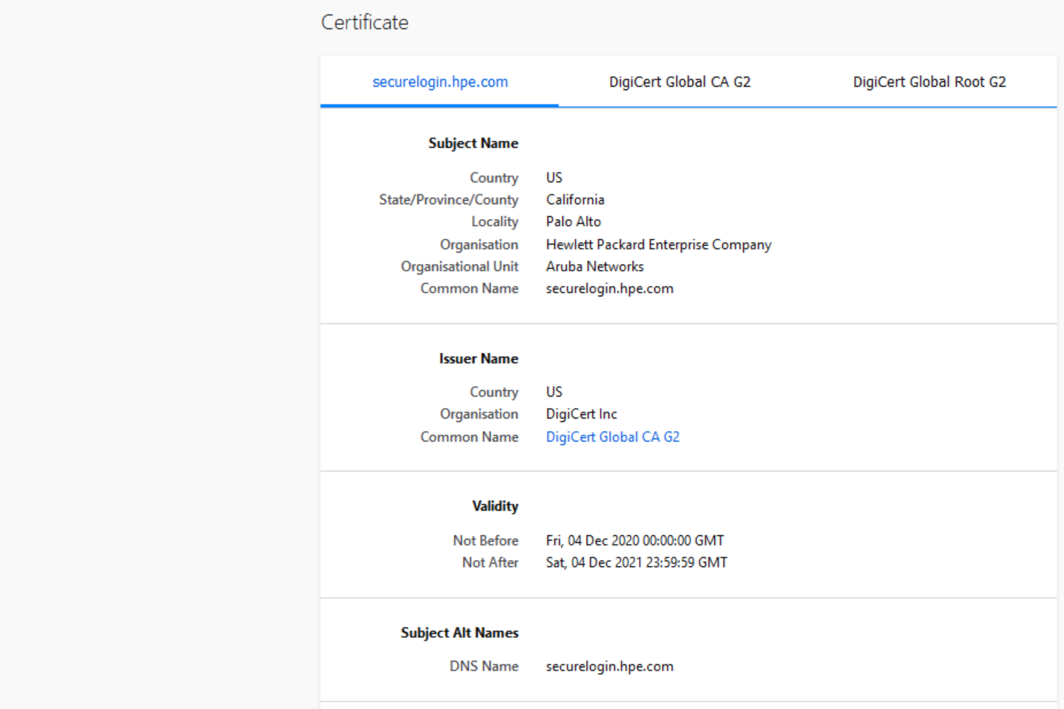
Firefox can't load this page for some reason.

has a security policy called HTTP Strict Transport Security (HSTS), which means that Firefox can only connect to it securely. You can't add an exception to visit this site.

Web sites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for www.google.com. The certificate is only valid for securelogin.hpe.com.

Error code: SSL_ERROR_BAD_CERT_DOMAIN

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



Subject Name

Country US
State/Province/County California
Locality Palo Alto
Organisation Hewlett Packard Enterprise Company
Organisational Unit Aruba Networks
Common Name securelogin.hpe.com

Issuer Name

Country US
Organisation DigiCert Inc
Common Name DigiCert Global CA G2

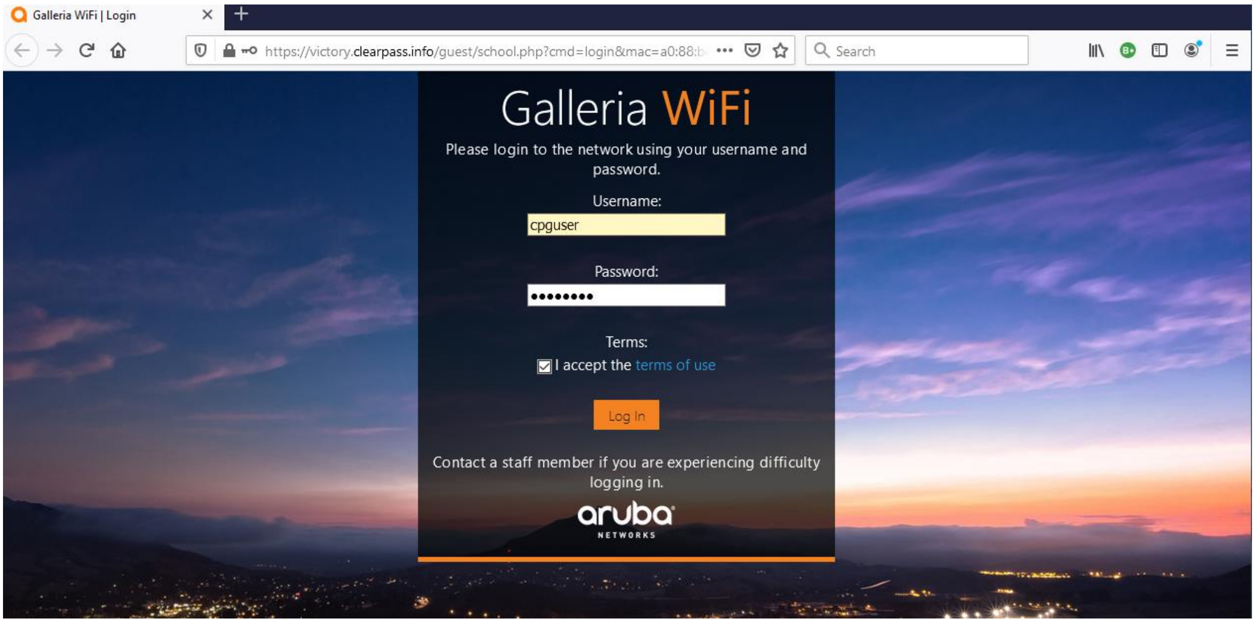
Validity

Not Before Fri, 04 Dec 2020 00:00:00 GMT
Not After Sat, 04 Dec 2021 23:59:59 GMT

Subject Alt Names

DNS Name securelogin.hpe.com

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



https://victory.clearpass.info/guest/school.php?cmd=login&mac=a0:88:b

Galleria WiFi

Please login to the network using your username and password.

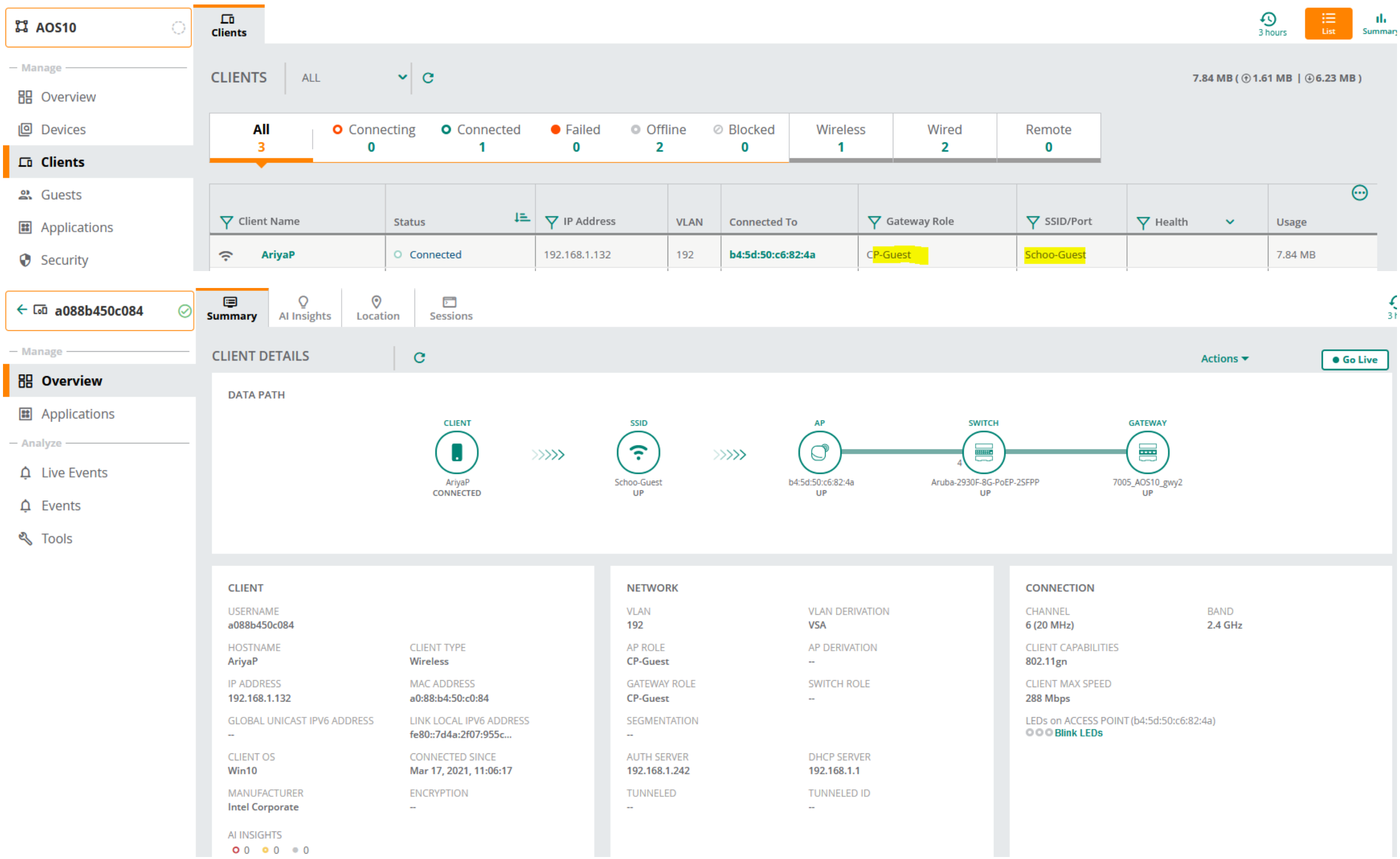
Username: cpguser

Password: ••••••••

Terms:
☑ I accept the terms of use

Contact a staff member if you are experiencing difficulty logging in.

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.



7.84 MB (⊕1.61 MB | ⊕6.23 MB)

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
AriyaP	Connected	192.168.1.132	192	b4:5d:50:c6:82:4a	CP-Guest	Schoo-Guest		7.84 MB

CLIENT

USERNAME
a088b450c084

HOSTNAME
AriyaP

CLIENT TYPE
Wireless

IP ADDRESS
192.168.1.132

MAC ADDRESS
a0:88:b4:50:c0:84

GLOBAL UNICAST IPV6 ADDRESS
--

LINK LOCAL IPV6 ADDRESS
fe80::7d4a:2f07:955c...

CLIENT OS
Win10

CONNECTED SINCE
Mar 17, 2021, 11:06:17

MANUFACTURER
Intel Corporate

ENCRYPTION
--

AI INSIGHTS
○ 0 ● 0 ● 0

NETWORK

VLAN
192

VLAN DERIVATION
VSA

AP ROLE
CP-Guest

AP DERIVATION
--

GATEWAY ROLE
CP-Guest

SWITCH ROLE
--

SEGMENTATION
--

AUTH SERVER
192.168.1.242

DHCP SERVER
192.168.1.1

TUNNELED
--

TUNNELED ID
--

CONNECTION

CHANNEL
6 (20 MHz)

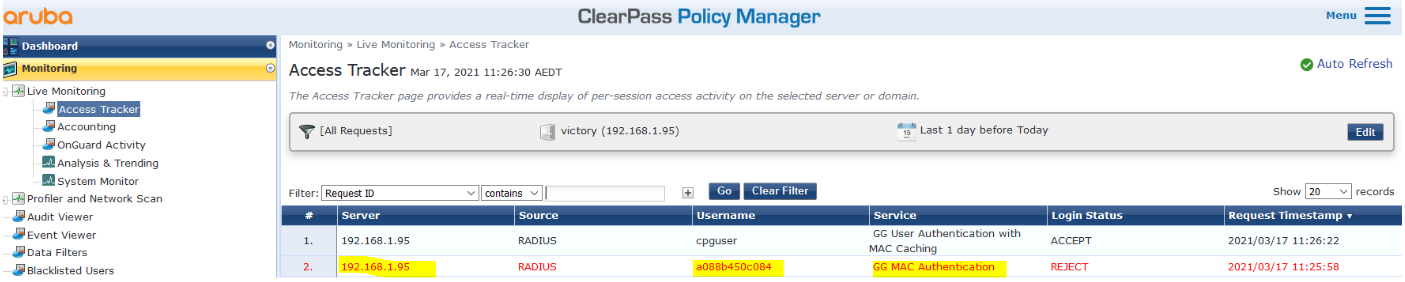
BAND
2.4 GHz

CLIENT CAPABILITIES
802.11gn

CLIENT MAX SPEED
288 Mbps

LEDs on ACCESS POINT (b4:5d:50:c6:82:4a)
○○○ Blink LEDs

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



Monitoring » Live Monitoring » Access Tracker

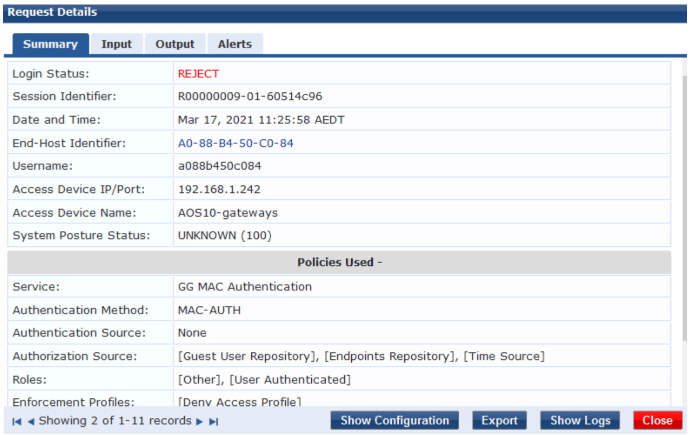
Access Tracker Mar 17, 2021 11:26:30 AEDT

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

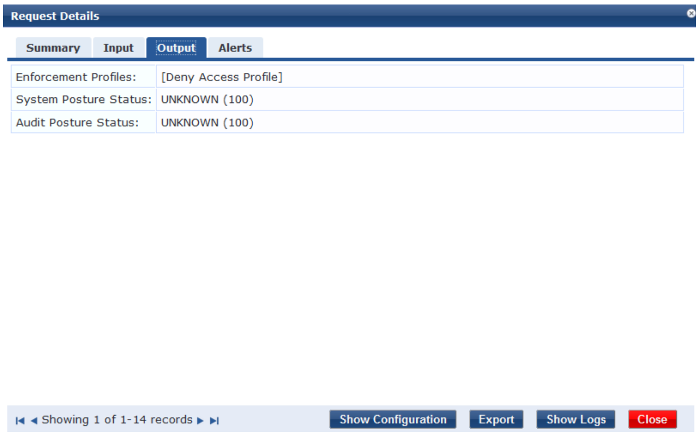
Filter: Request ID contains Show 20 records

#	Server	Source	Username	Service	Login Status	Request Timestamp ▾
1.	192.168.1.95	RADIUS	cpguser	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



Login Status:	REJECT
Session Identifier:	R00000009-01-60514c96
Date and Time:	Mar 17, 2021 11:25:58 AEDT
End-Host Identifier:	A0-88-B4-50-C0-84
Username:	a088b450c084
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:	None
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]
Roles:	[Other], [User Authenticated]
Enforcement Profiles:	[Deny Access Profile]

◂◂ ◂ Showing 2 of 1-11 records ▸ ▸▸



Enforcement Profiles:	[Deny Access Profile]
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

◂◂ ◂ Showing 1 of 1-14 records ▸ ▸▸

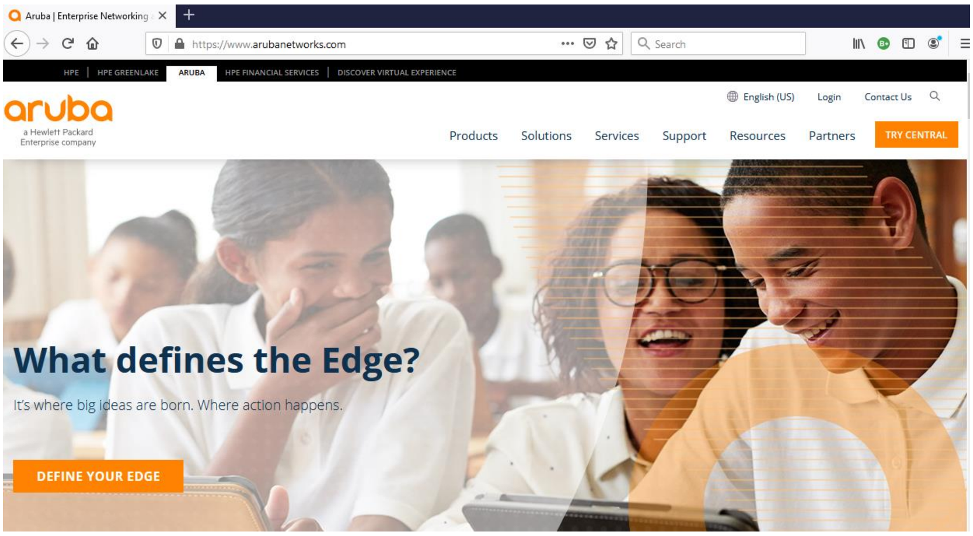
This is normal as this MAC address has not been seen before.

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#
```

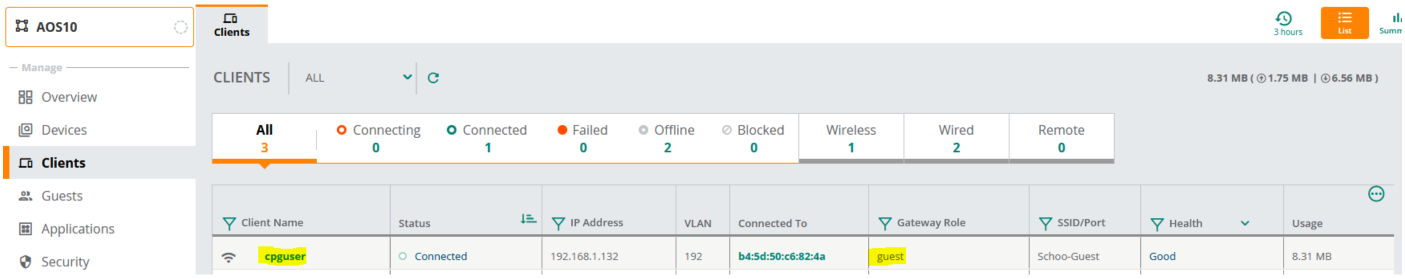
Now when the user performs a successful the login (we are using username cpguser) process, they will be redirected to the “redirect URL” that we specified.


Aruba | Enterprise Networking
https://www.arubanetworks.com
Search
HPE | HPE GREENLAKE | ARUBA | HPE FINANCIAL SERVICES | DISCOVER VIRTUAL EXPERIENCE
aruba
a Hewlett Packard Enterprise company
English (US)
Login
Contact Us
Products
Solutions
Services
Support
Resources
Partners
TRY CENTRAL
DEFINE YOUR EDGE

What defines the Edge?

It's where big ideas are born. Where action happens.

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



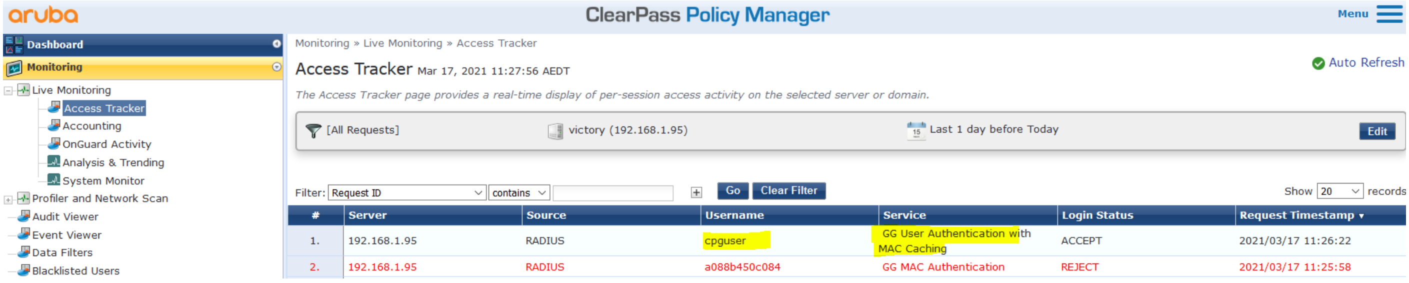
CLIENTS ALL

8.31 MB (1.75 MB | 6.56 MB)

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
cpguser	Connected	192.168.1.132	192	b4:5d:50:c6:82:4a	guest	Schoo-Guest	Good	8.31 MB

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



Monitoring » Live Monitoring » Access Tracker

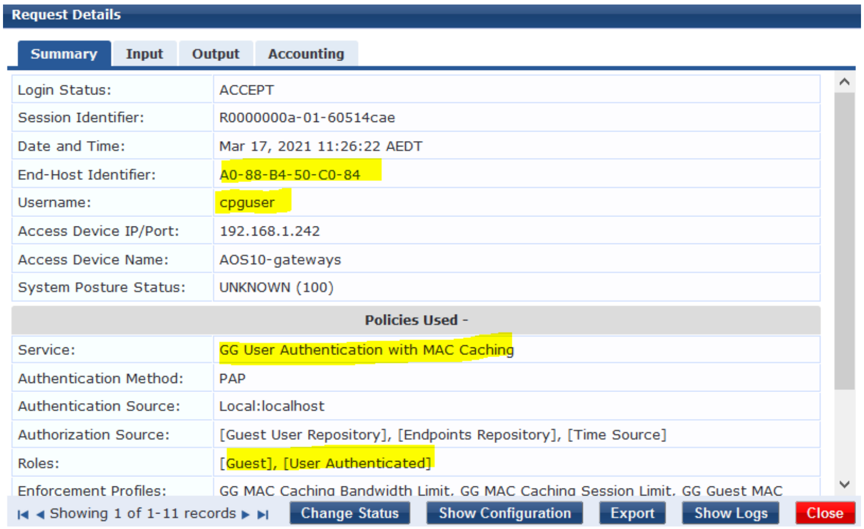
Access Tracker Mar 17, 2021 11:27:56 AEDT

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

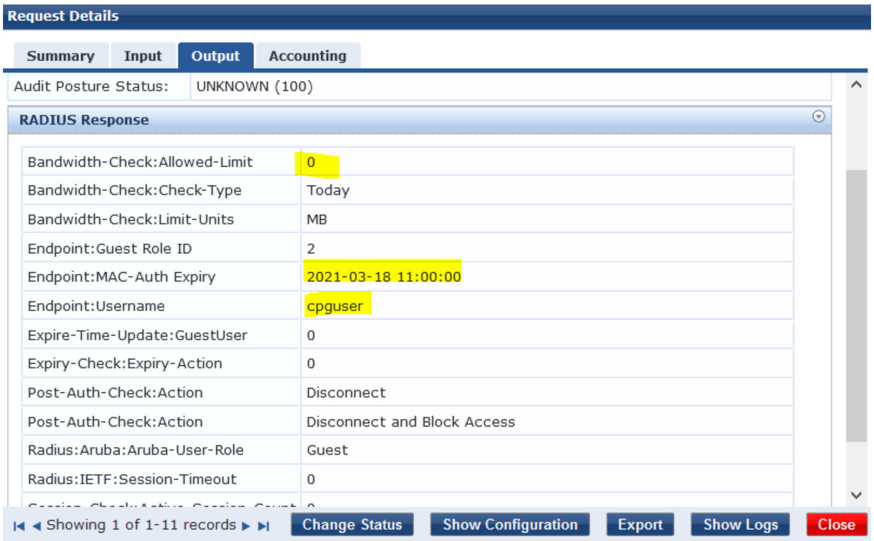
[All Requests]   victory (192.168.1.95)   Last 1 day before Today

Filter: Request ID contains   Show 20 records

#	Server	Source	Username	Service	Login Status	Request Timestamp ▾
1.	192.168.1.95	RADIUS	cpguser	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



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



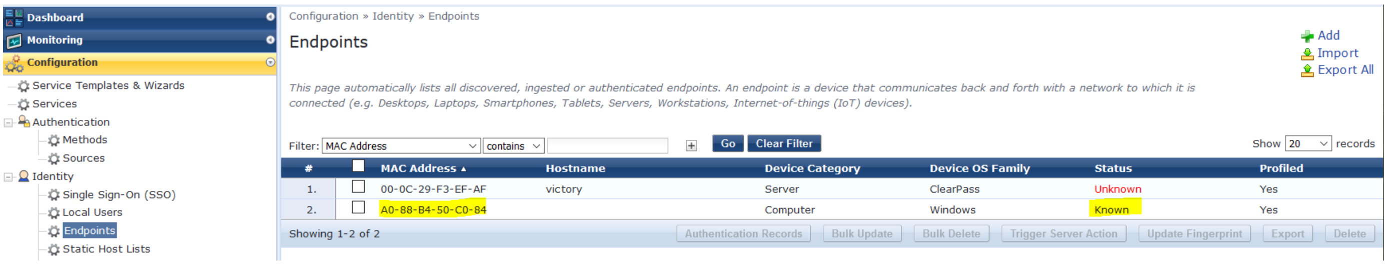
Request Details

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
Session-Check:Active-Session-Count	0

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



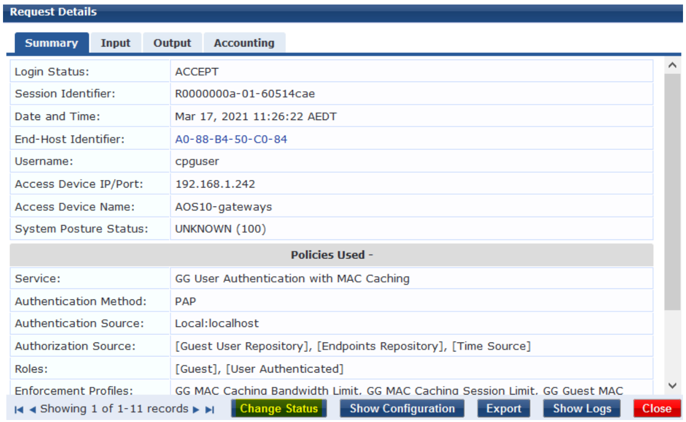
Endpoints

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

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.

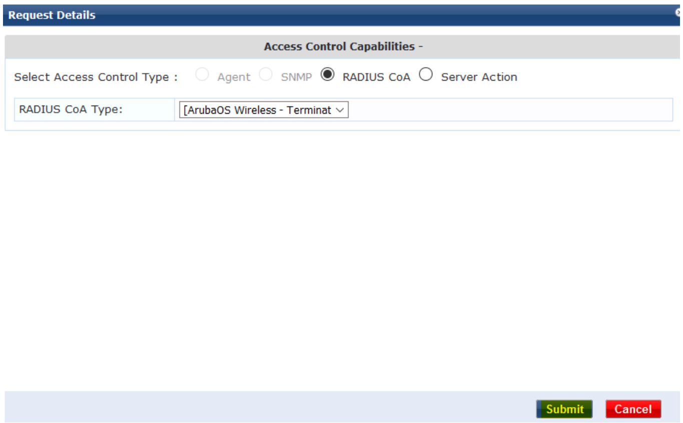


Request Details

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

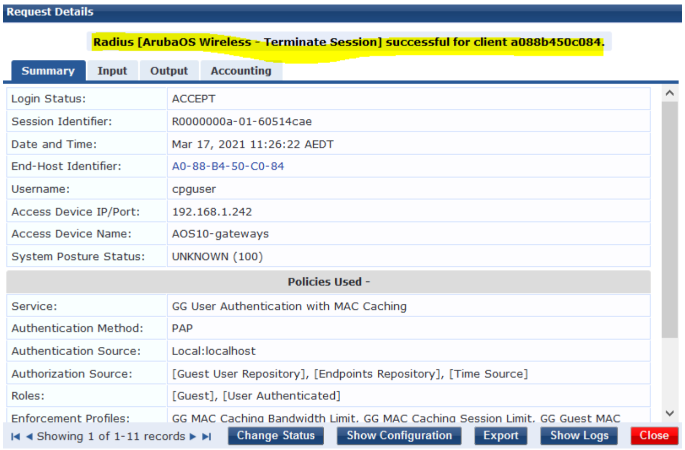


Request Details

Access Control Capabilities -

Select Access Control Type : ○ Agent ○ SNMP ● RADIUS CoA ○ Server Action

RADIUS CoA Type: [ArubaOS Wireless - Terminat



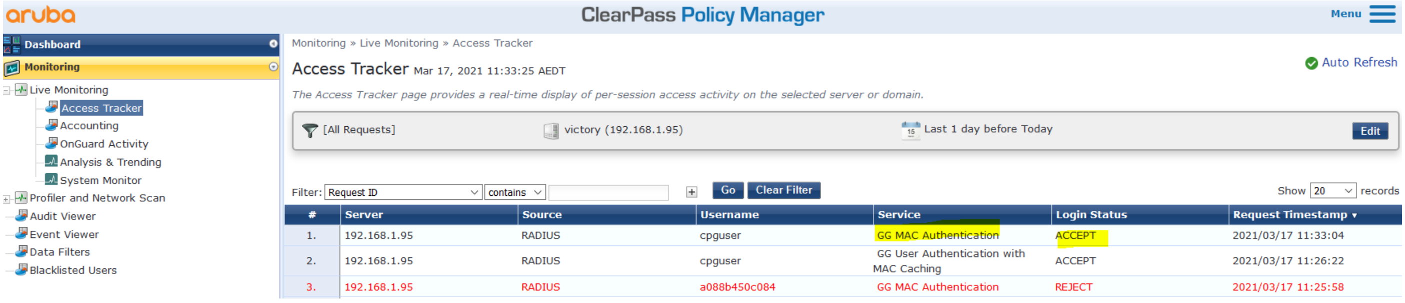
Request Details

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

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



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

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

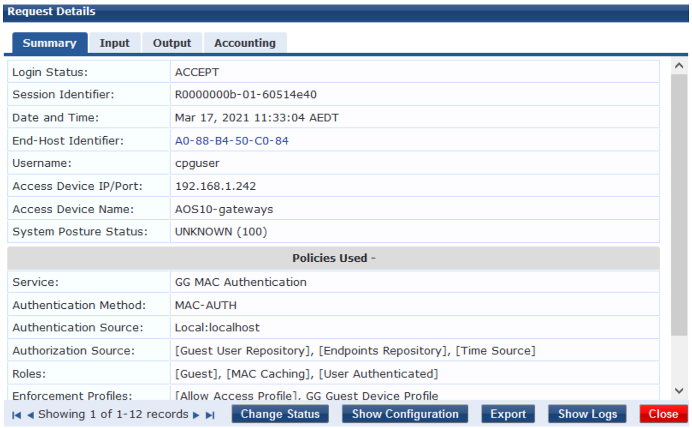
[All Requests] victory (192.168.1.95) Last 1 day before Today

Filter: Request ID contains

Show 20 records

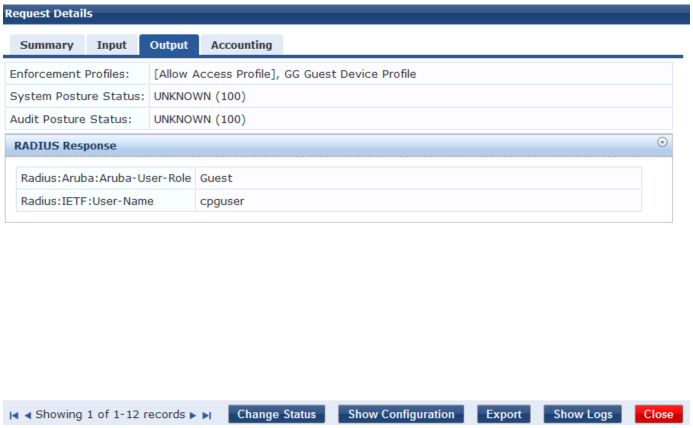
#	Server	Source	Username	Service	Login Status	Request Timestamp ▾
1.	192.168.1.95	RADIUS	cpguser	GG MAC Authentication	ACCEPT	2021/03/17 11:33:04
2.	192.168.1.95	RADIUS	cpguser	GG User Authentication with MAC Caching	ACCEPT	2021/03/17 11:26:22
3.	192.168.1.95	RADIUS	a088b450c084	GG MAC Authentication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

Looking at the details of that session



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:	cpguser
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

Showing 1 of 1-12 records



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	cpguser

Showing 1 of 1-12 records

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

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

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

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