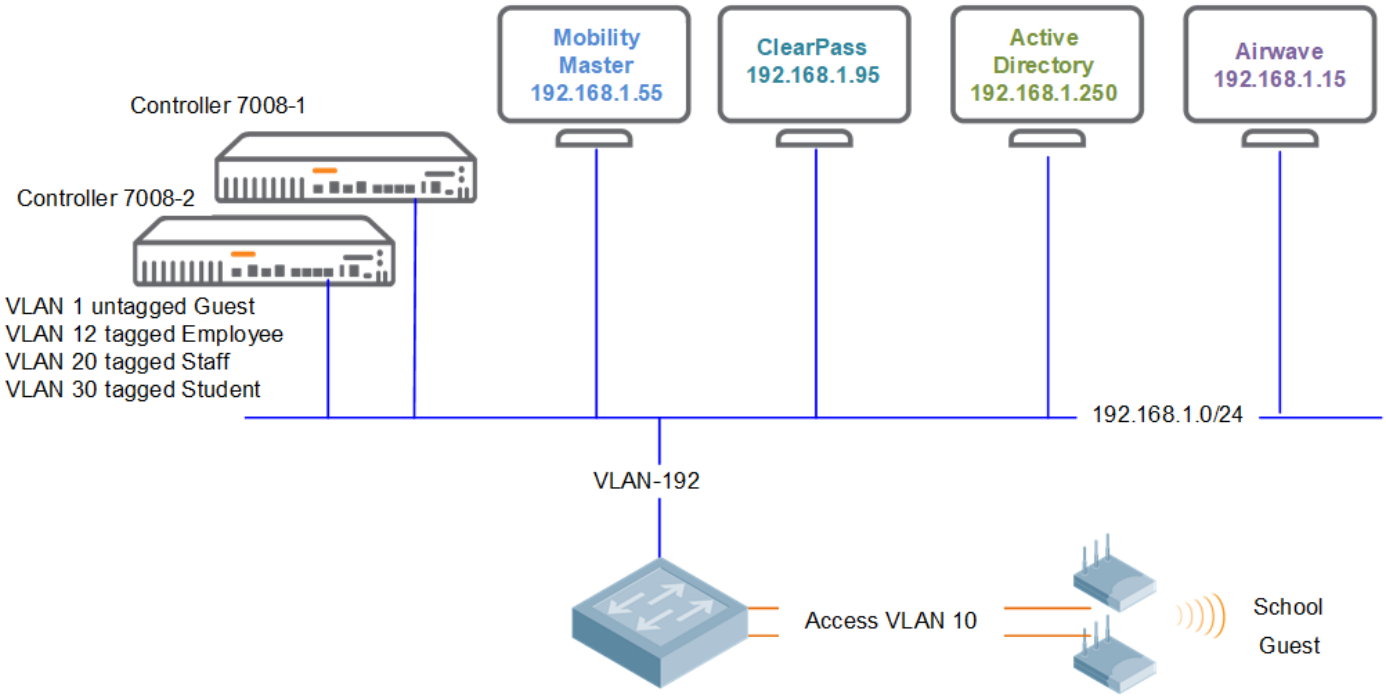
Contents

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
02 Feb 2021	0.1	Ariya Parsamanesh	Initial creation
08 Feb 2021	0.2	Ariya Parsamanesh	Added section 5-6
15 Feb 2021	0.3	Ariya Parsamanesh	Minor modifications

2 Demo Topology

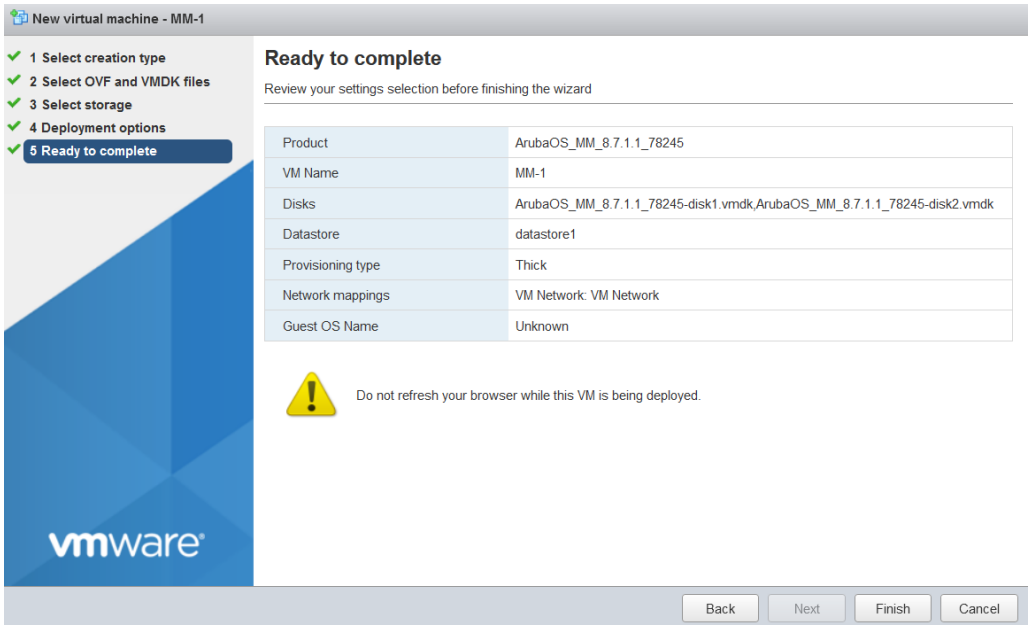
Here is the topology we'll be implementing. The aim here is to provide the starting point to put together a solution that include the Mobility conductor (formally known as mobility master), controllers, APs, ClearPass and Airwave.

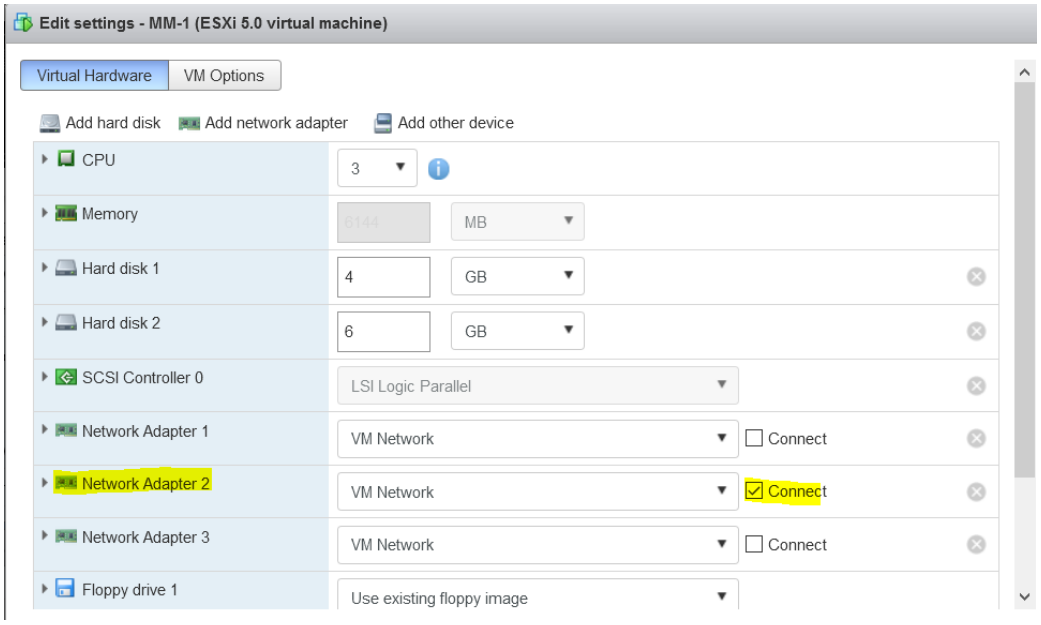


This is the part 1 of the three parts series.

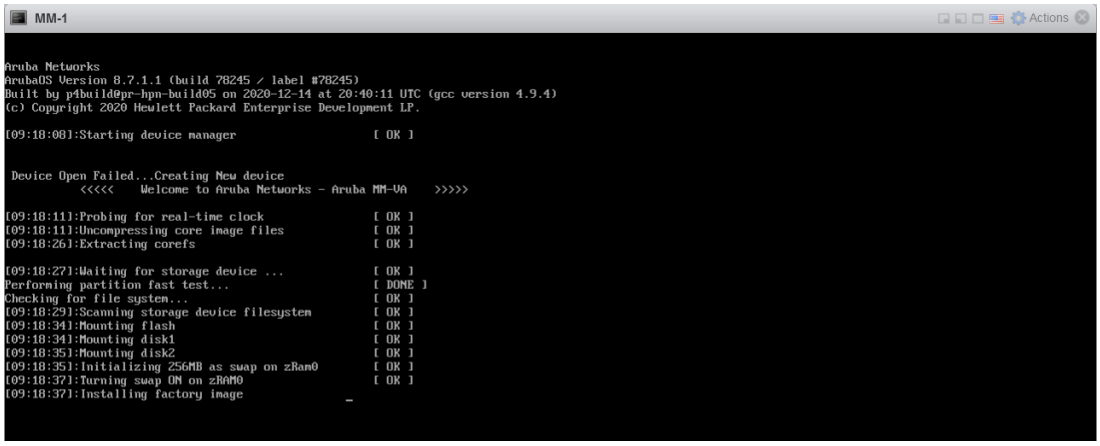
3 Setting up the OVA for Mobility Master

For the details please refer to the ArubaOS 8.7.1.0 virtual appliance installation guide. Here I just want to highlight the areas that some might forget to follow.





Just enable the correct VLAN/adapter to be assigned to network adapter 2 and power that one up. Next, connect to the console of the VM, as you need to setup the IP addressing, etc.



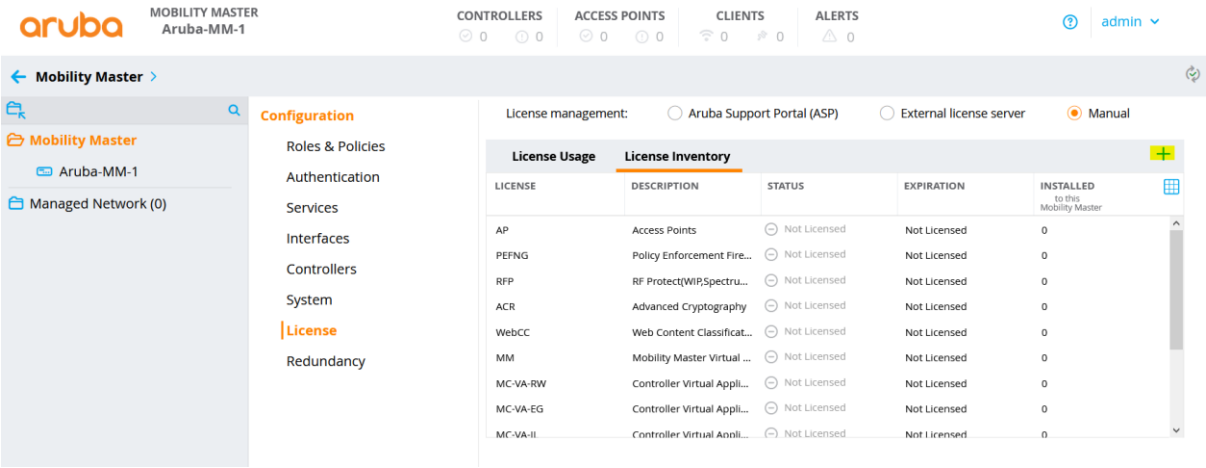
```
Success: Package default_airgroup_pkg installed successfully
Success: Package default_ucm_pkg installed successfully
Success: Package default_wms_pkg installed successfully
Success: Package default_arm_cm_pkg installed successfully
Success: Package default_web_cc_pkg installed successfully
Success: Package default_nbapi_helper_pkg installed successfully
Success: Package default_airmatch_pkg installed successfully
Success: Package default_appRF_pkg installed successfully
[09:46:06]:Verify the bootloader                    [ OK ]
[09:46:07]:rcS Done(32 sec)

[09:46:07]:Initializing CA bundle                   [ OK ]
[09:46:07]:Starting OS services                     [ OK ]

Starting ztp
Starting ztp auto provision

****************** Welcome to the ArubaMM-VA 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 [ArubaMM-VA_04_D8_FA]: Aruba-MM1
Enter Controller VLAN ID [1]:
Enter Controller VLAN port [GE 0/0/0]:
Enter Controller VLAN port mode (access|trunk) [access]:
Do you wish to configure IPV4 address on vlan (yes|no) [yes]:
Enter VLAN interface IP address [172.16.0.254]: 192.168.1.55
Enter VLAN interface subnet mask [255.255.255.0]:
Enter IP Default gateway [none]: 192.168.1.249
Enter DNS IP address [none]: 1.1.1.1
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no_
```

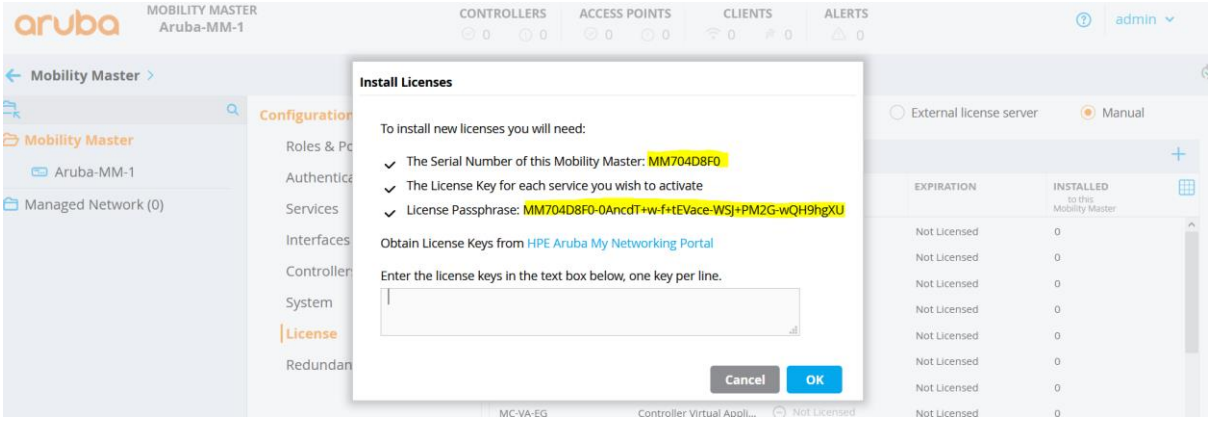
```
Enter Country code (ISO-3166), <ctrl-I> for supported list: AU
You have chosen Country code AU for Australia (yes|no)?: yes
Enter the controller's IANA Time zone [America/Los_Angeles]: Australia/Melbourne
Enter Time in UTC [09:47:23]:
Enter Date (MM/DD/YYYY) [2/1/2021]:
Enter Password for admin login (up to 32 chars): ********
Re-type Password for admin login: ********

Current choices are:

System name: Aruba-MM1
Controller VLAN id: 1
Controller VLAN port: GE 0/0/0
Controller VLAN port mode: access
Option to configure VLAN interface IPV4 address: yes
VLAN interface IP address: 192.168.1.55
VLAN interface subnet mask: 255.255.255.0
IP Default gateway: 192.168.1.249
Domain Name Server to resolve FQDN: 1.1.1.1
Option to configure VLAN interface IPV6 address: no
Country code: AU
IANA Time Zone: Australia/Melbourne

If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no)
```

Once you have accepted the changes, MM will reboot and then you can browse to that IP address which you just configured. Once you login with the new credentials, you need to add the licenses. To be able to add the license, you need to get the license passphrase and send it to Aruba in which they can activate the evaluation licenses for it.

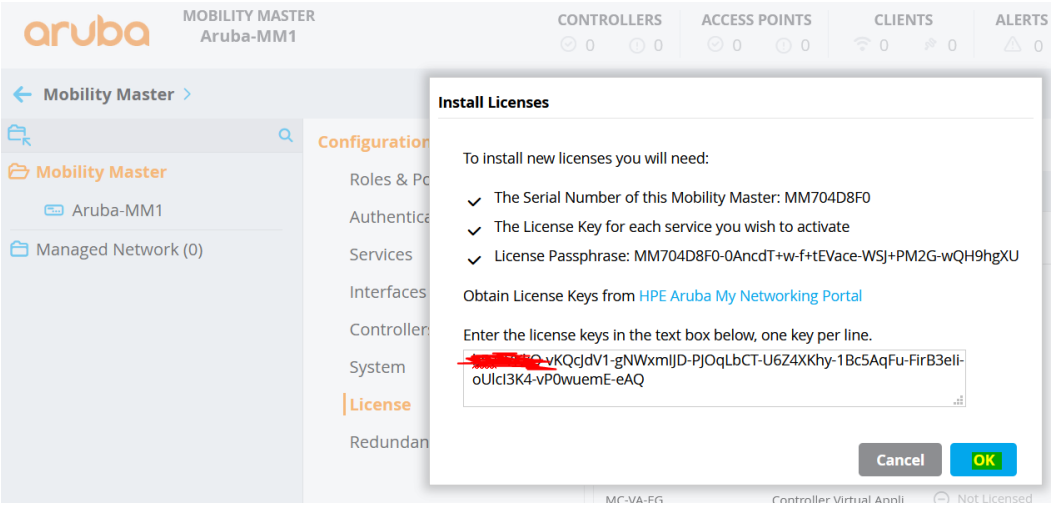
4 Mobility Master Basic Configuration

Here we'll cover the basic configuration starting with evaluation licensing.

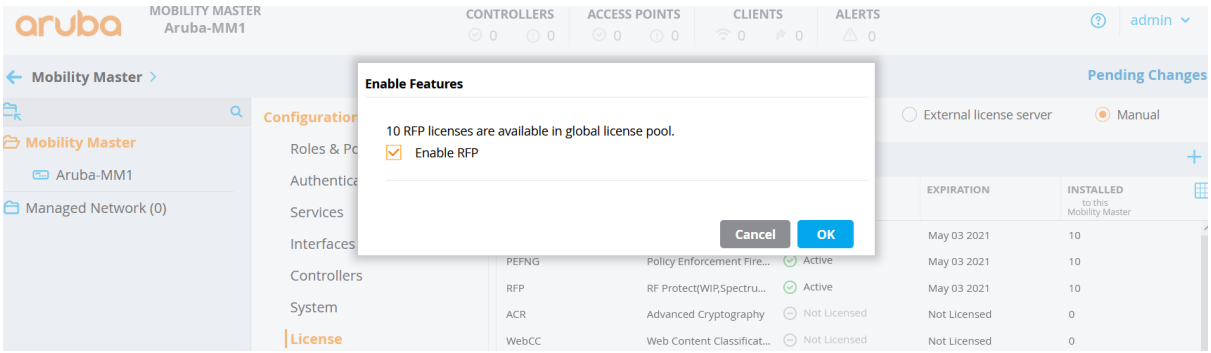


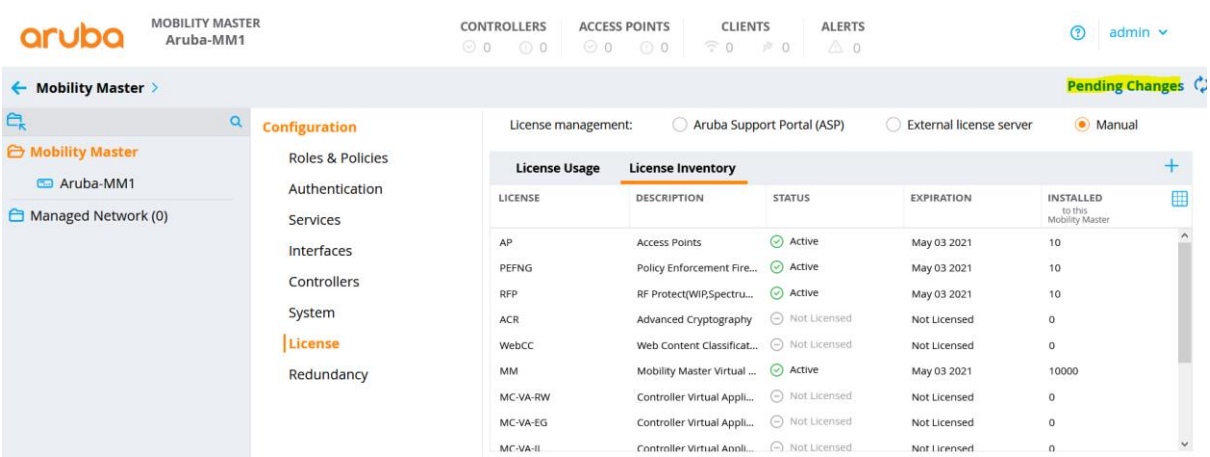


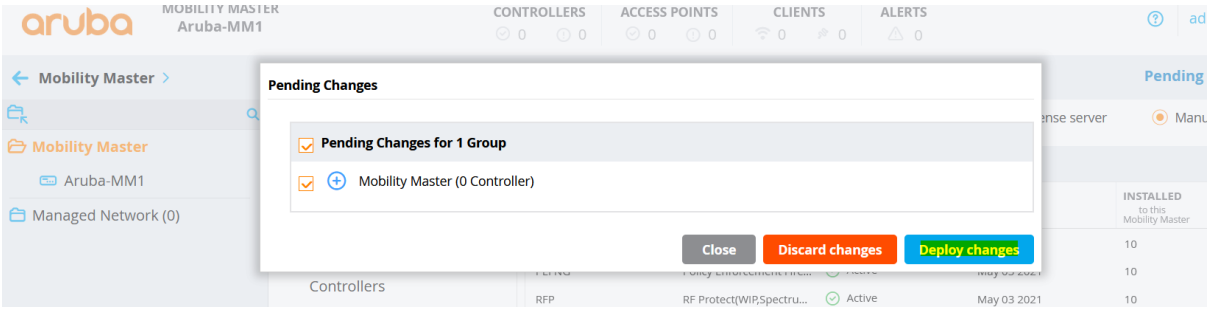
Here is the passphrase which is highlighted. This needs to be sent to your Aruba contact or SE, they should be able to generate and send you the license key to be copy and pasted into the following dialog.



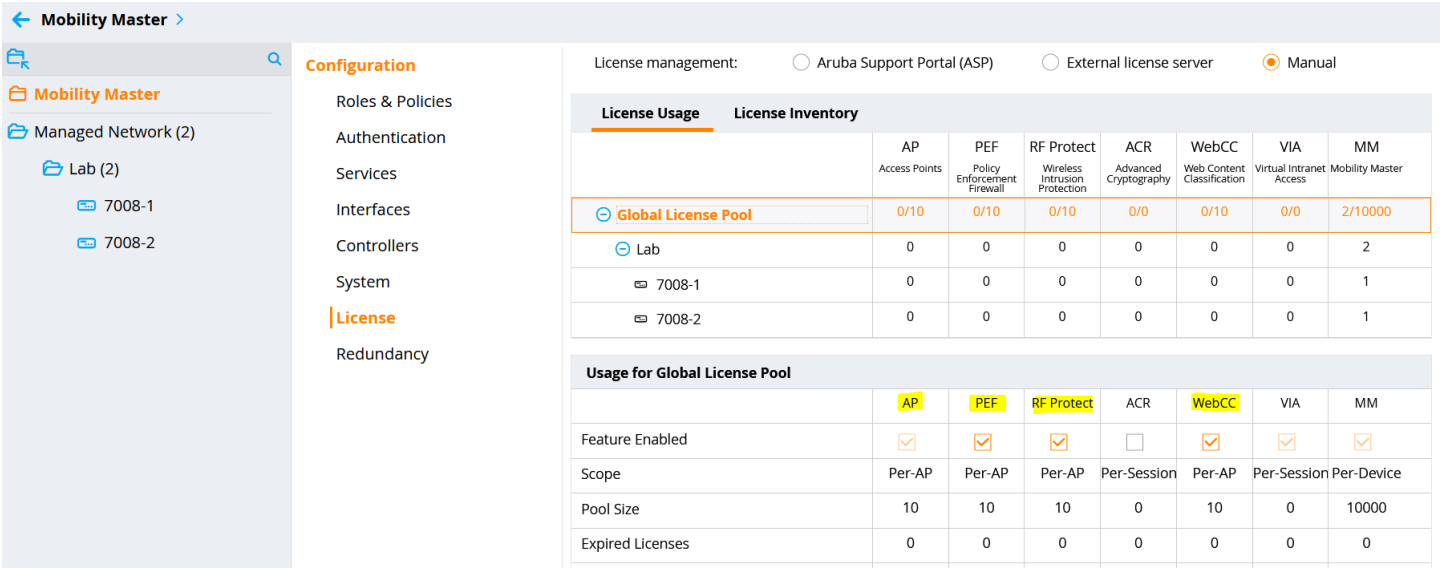
And some of the licenses like PEFNG and RFP will prompt to enable them as shown below.



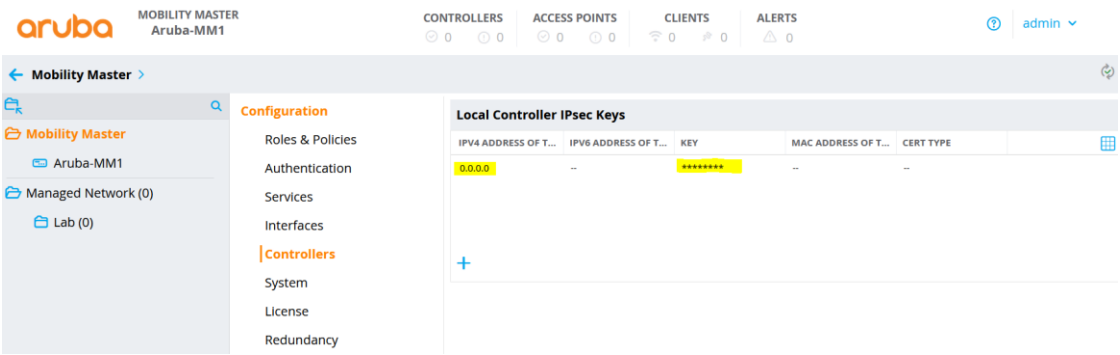




Once you have added your licenses, you should see all four license types (AP, PEF, RFP, WebCC) enabled.

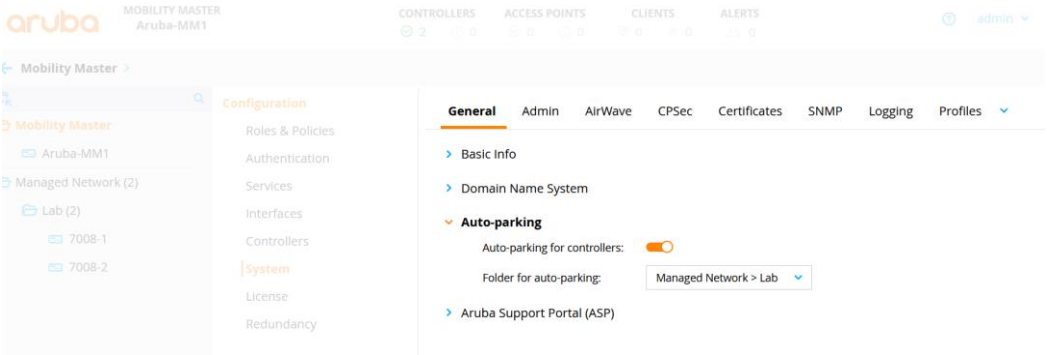


Now we'll add the controllers/ managed devices (MDs). This configuration is for Local controller IPSec keys that all the controllers use to connect to MM. Otherwise you need to specify them individually.

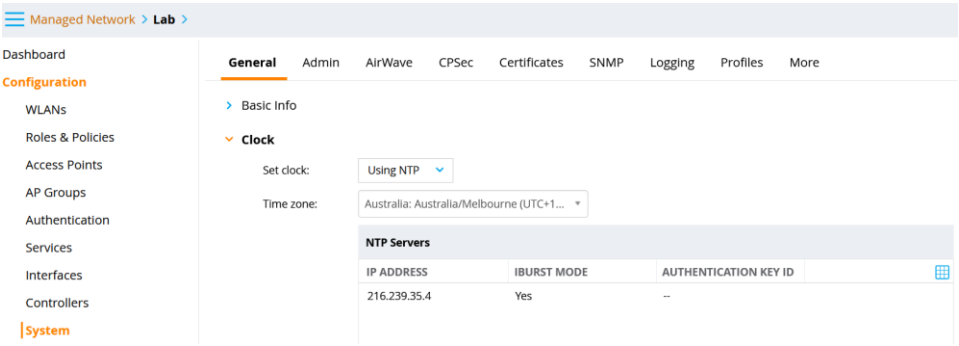


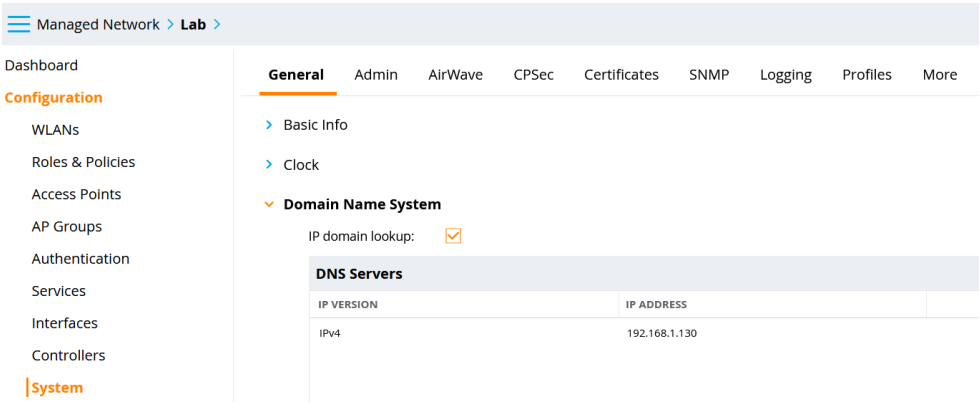
Also note that we have created a folder under Managed Network called Lab. There is a feature called autopark which when enabled makes MD adoption much easier, especially if you have a task of bringing up multiple MDs into the MM. This feature automatically parks the MDs under any node below /md

So now when the controllers get adopted by the MM, it will be added under "/md/Lab"

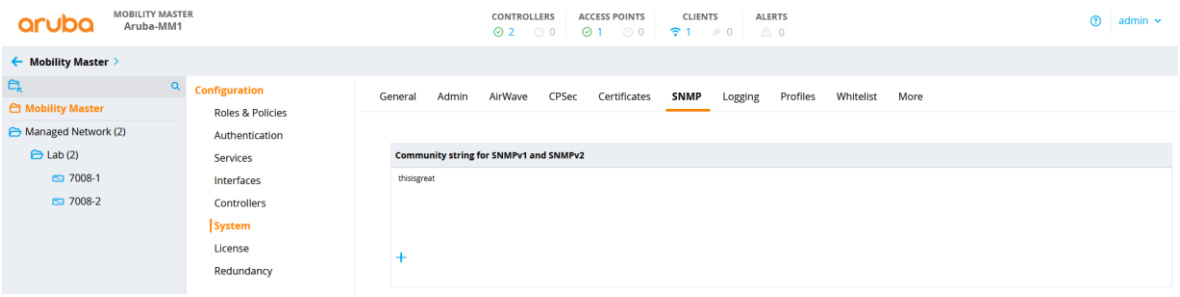


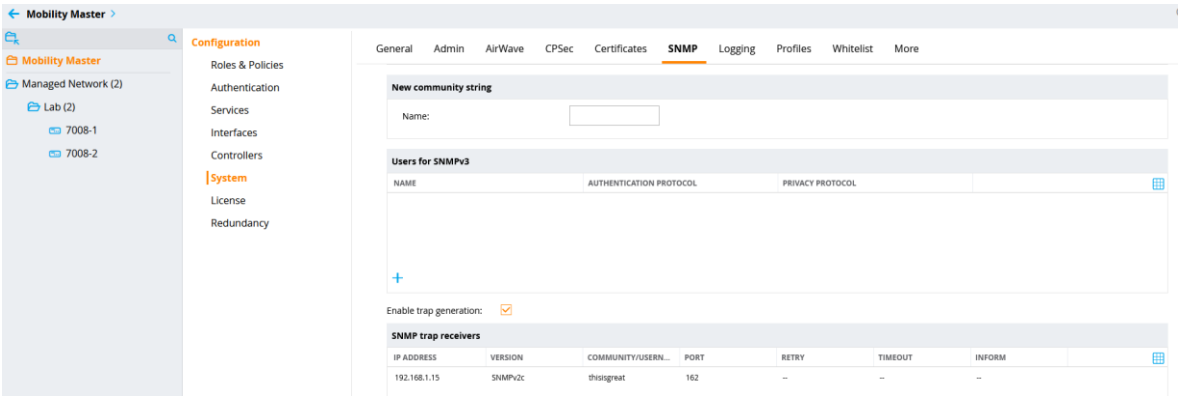
Next, we'll configure NTP and DNS for the Lab folder



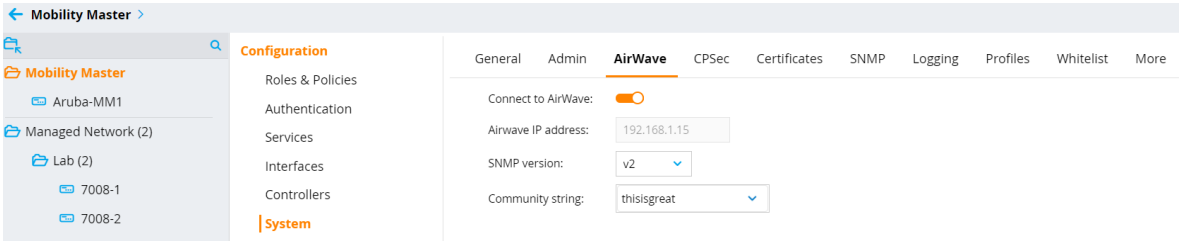


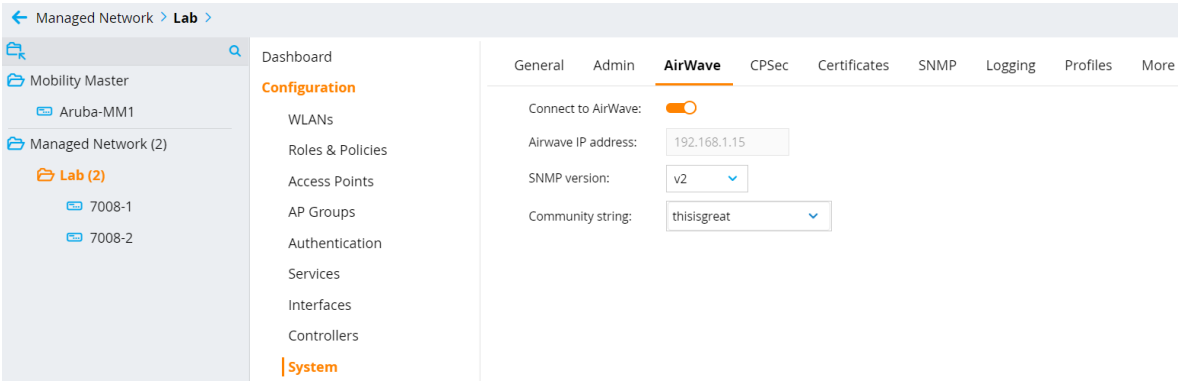
We'll also configure SNMP, so Airwave can manage/monitor it



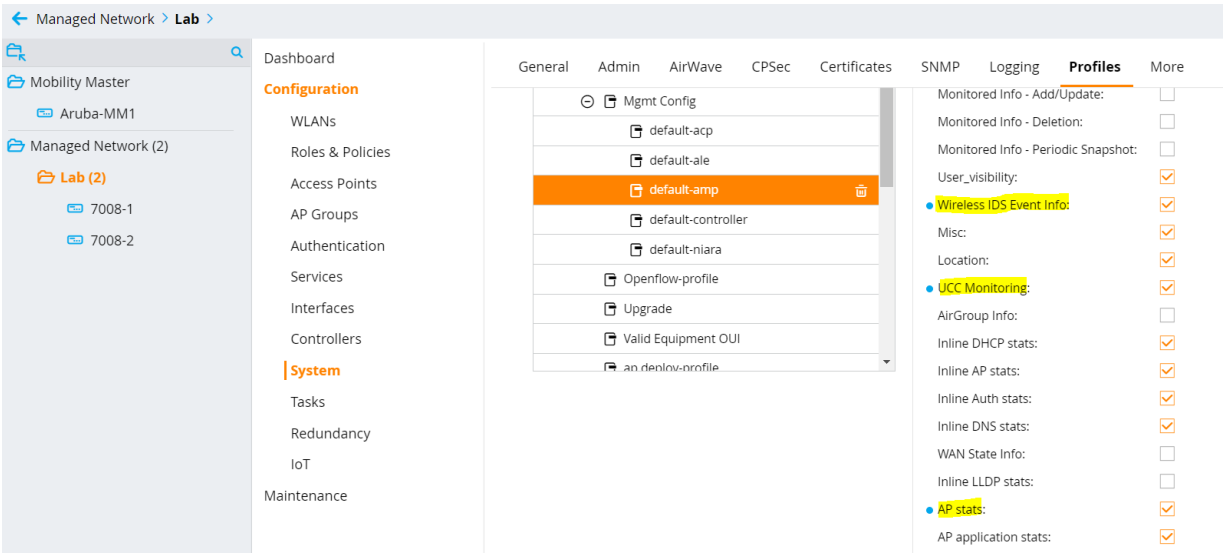


And then enabling the AirWave connectivity for MM and MDs



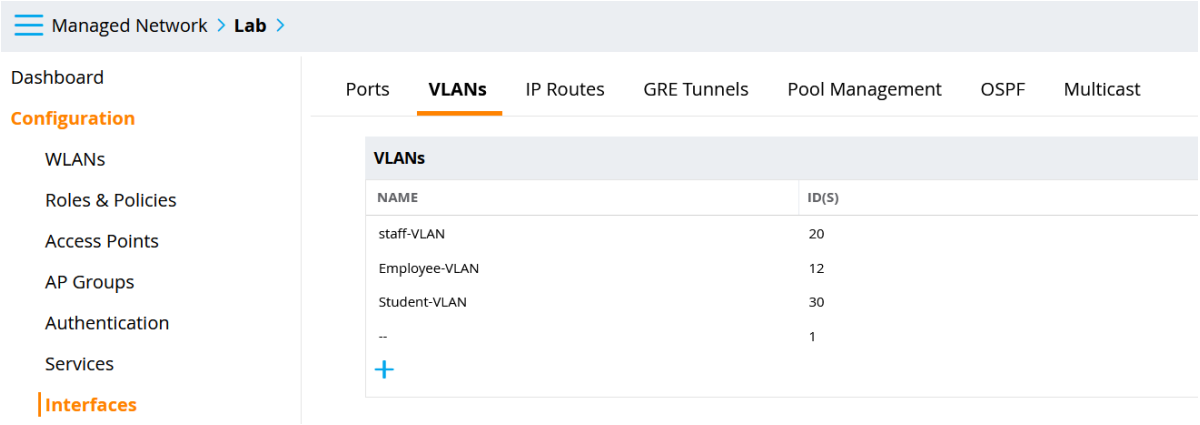


And enabling a few services to send their data to Airwave.

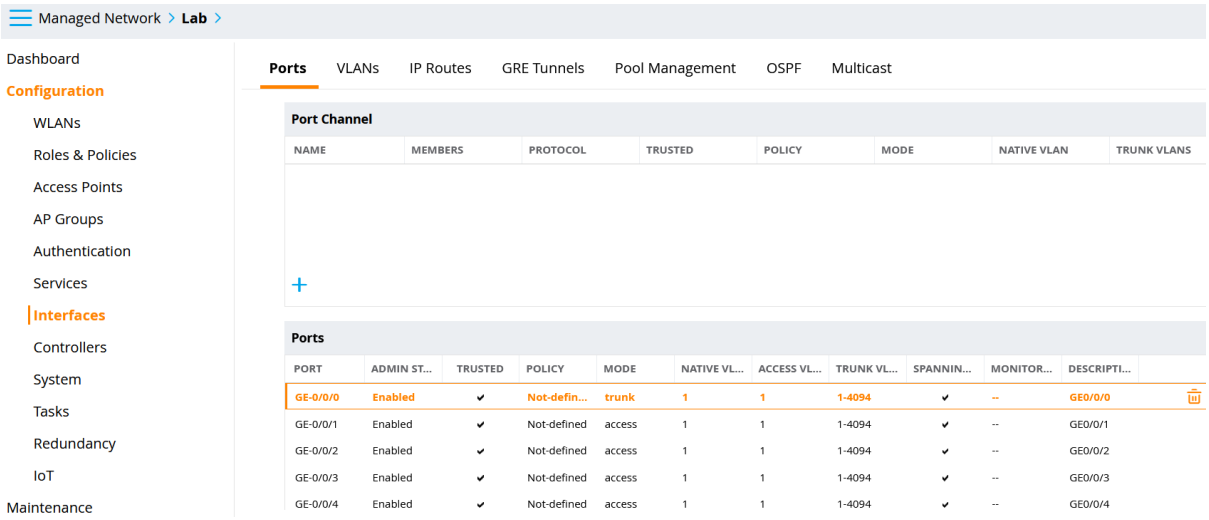


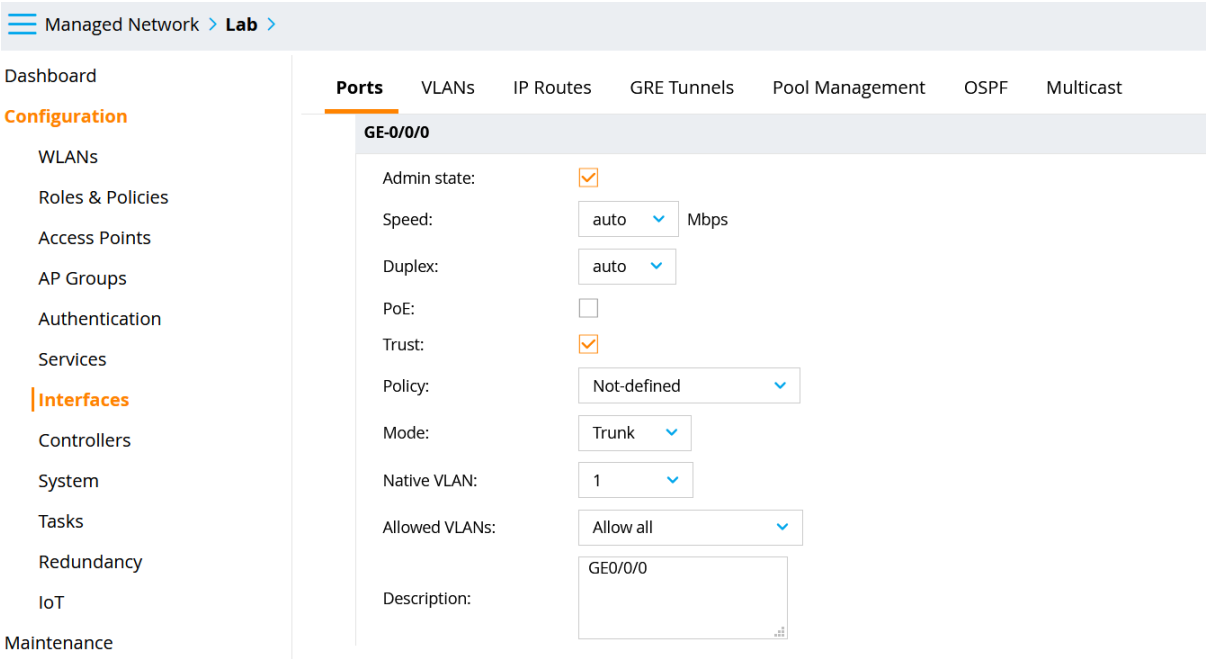
Aruba APs will create a IPSEC tunnels as an overlay to the controller or cluster of controllers. So, you need to ensure all the needed VLANs are configured at the controller end. And the port that connects to the controllers are configured for VLAN trunking.

Configuring employee, staff, and students VLANs. The aim here is that after authentication, if the users don't match the user group of staff or students then they are put into employee VLAN

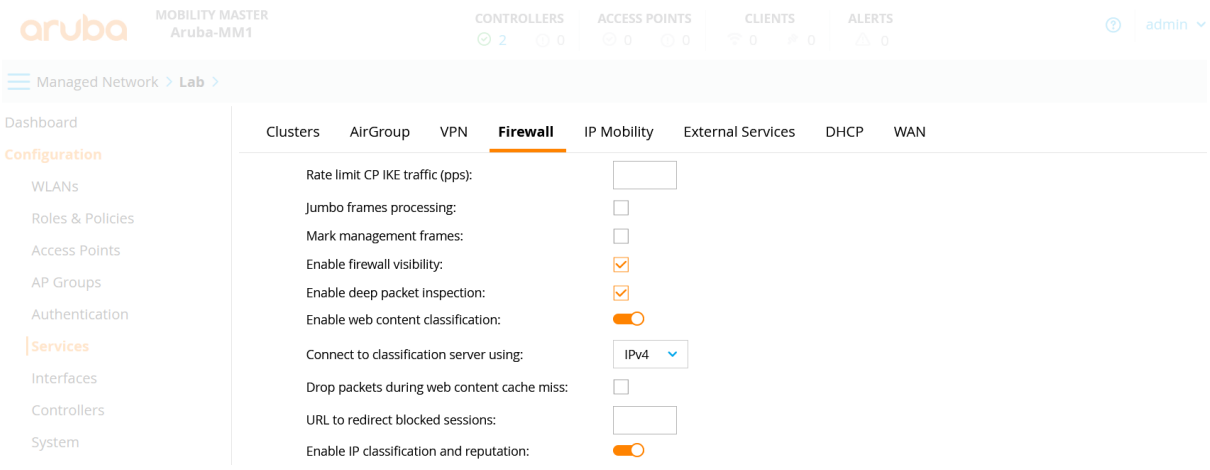


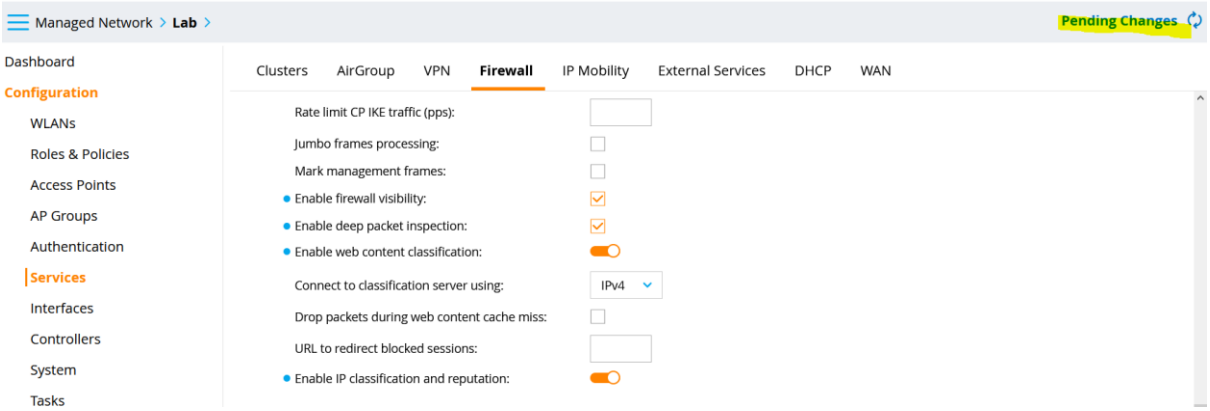
Make the port 0/0/0 as Trunk port with native VLAN as VLAN1





Also note that you can configured LACP and aggregate the two or more interfaces together. This is not shown here. Lastly enable firewall visibility, deep packet inspection and Web content classification.





For this we need to reload the MDs it they are already connected to the MM.

5 Controller Configuration

Once you power up the controllers that are in default state connect through the serial console and you'll see the following starting with "Auto-provisioning". There are many ways to auto provision them, here we'll do the basic configuration so it can join the mobility master and then all the configuration will be done from the MM.

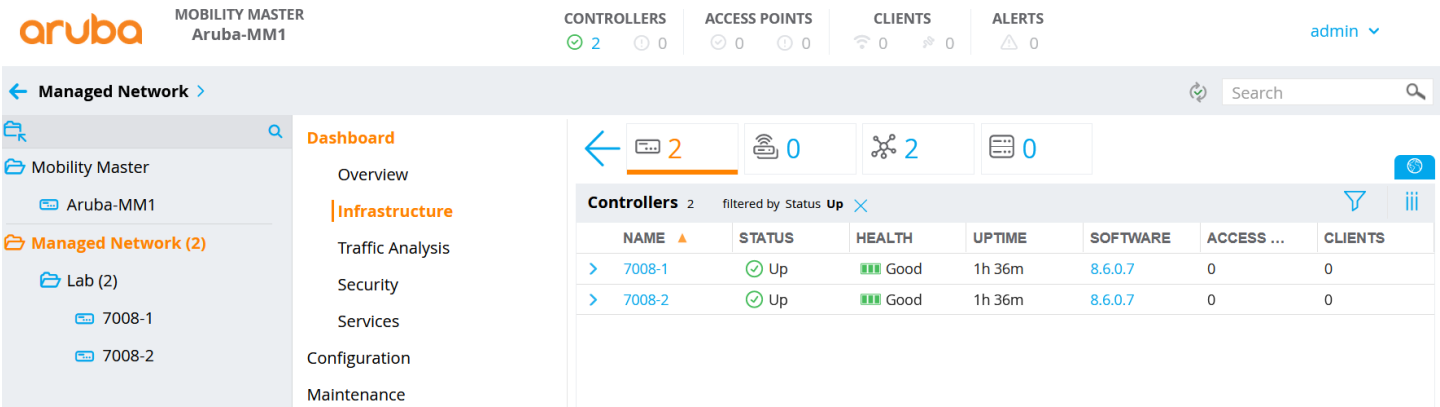
```
Auto-provisioning is in progress. It requires DHCP and Activate servers
Choose one of the following options to override or debug auto-provisioning...
    'enable-debug'      : Enable auto-provisioning debug logs
    'disable-debug'     : Disable auto-provisioning debug logs
    'mini-setup'        : 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 Aruba7008 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 [Aruba7008]: 7008-2
Enter Switch Role (standalone|md) [md]:
Enter IP type to terminate IPSec tunnel (ipv4|ipv6) [ipv4]:
Enter Master switch IP address or FQDN: 192.168.1.55
Is this a VPN concentrator for managed device to reach Master switch (yes|no) [no]:
This device connects to Master switch via VPN concentrator (yes|no) [no]:
Is Master switch Virtual Mobility Master? (yes|no) [yes]:
Master switch Authentication method (PSKwithIP|PSKwithMAC) [PSKwithIP]:
Enter IPSec Pre-shared Key: ********
Re-enter IPSec Pre-shared Key: ********
Do you want to enable L3 Redundancy (yes|no) [no]:
Enter Uplink Vlan ID [1]:
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]: 10.10.10.5
Enter Uplink Vlan Static IP netmask [255.255.255.0]:
Enter IP default gateway [none]: 10.10.10.1
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) [2/2/2021]:
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: ********

Current choices are:
```

```
System name: 7008-2
Switch Role: md
IP type to terminate IPSec tunnel: ipv4
Master switch IP address or FQDN: 192.168.1.55
Is this VPN concentrator: no
Connect via VPN concentrator: no
IPSec authentication method: PSKwithIP
Vlan id for uplink interface: 1
Uplink port: GE 0/0/0
Uplink port mode: access
Uplink Vlan IP assignment method: static
Uplink Vlan static IP Address: 192.168.1.57
Uplink Vlan static IP net-mask: 255.255.255.0
Uplink Vlan IP default gateway: 192.168.1.249
Domain Name Server to resolve FQDN: 192.168.1.130
Option to configure VLAN interface IPV6 address: no
Country code: AU
IANA Time Zone: Australia/Melbourne
Admin account created: yes

Note: These settings require IP-Based-PSK configuration on Master switch

If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no)yes
INFO: Backing up existing config dir.
Creating configuration... Done.

System will now restart!


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

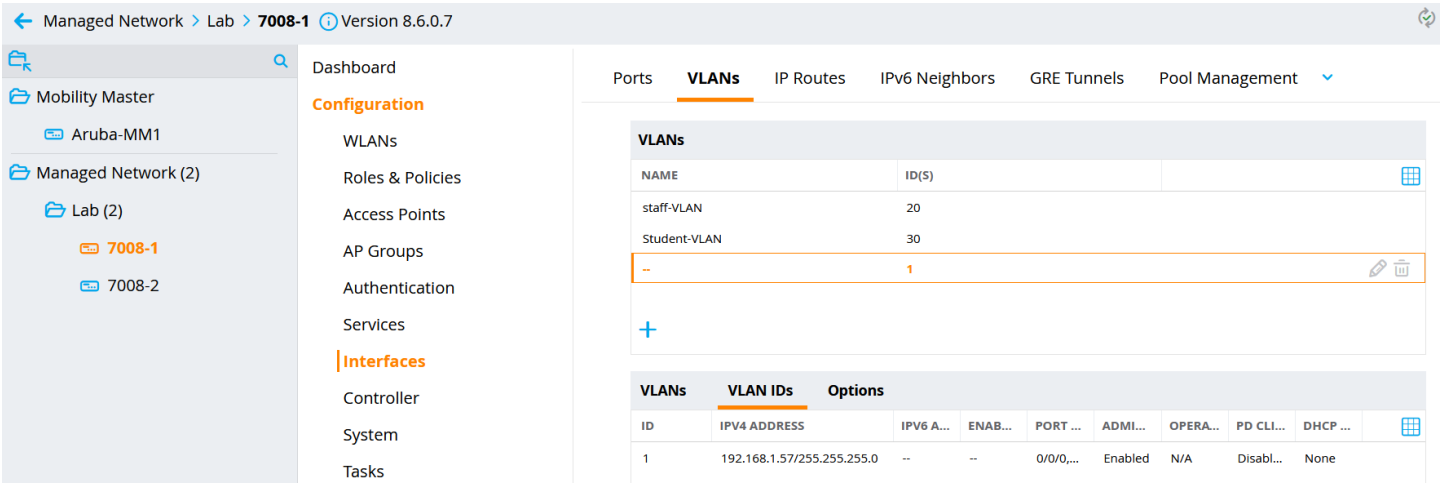
Now we see that both the controllers show up on MM

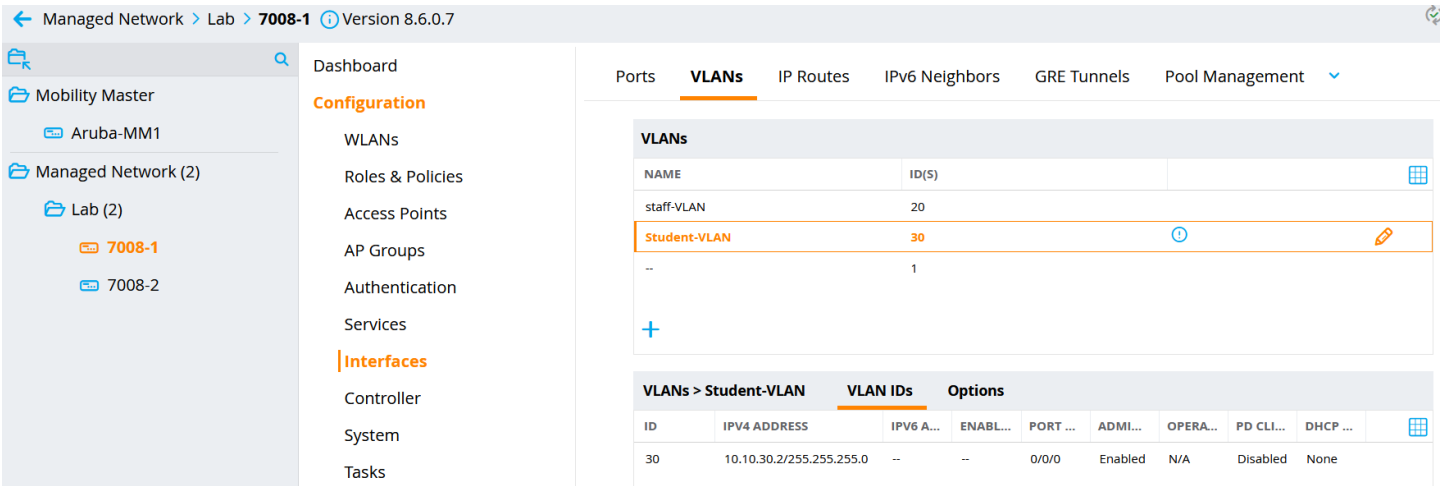
6 Mobility Master Configuration

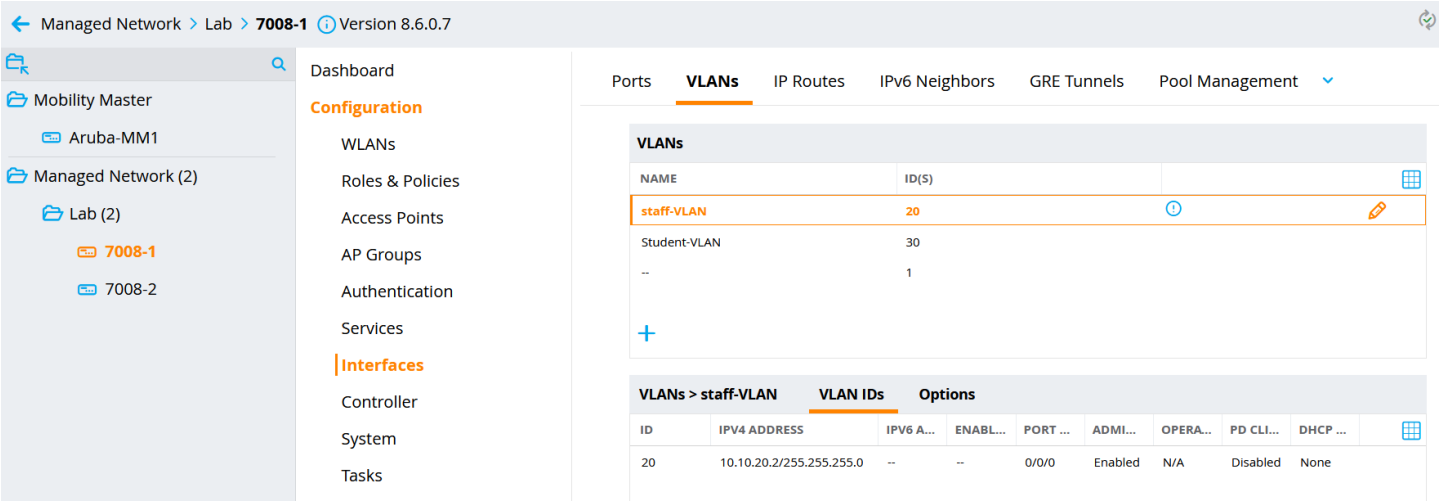
Here we have done the previous process for two MDs and they have end up on the MM dashboard and have now got the basic configuration tat we did earlier for the “Lab” folder.

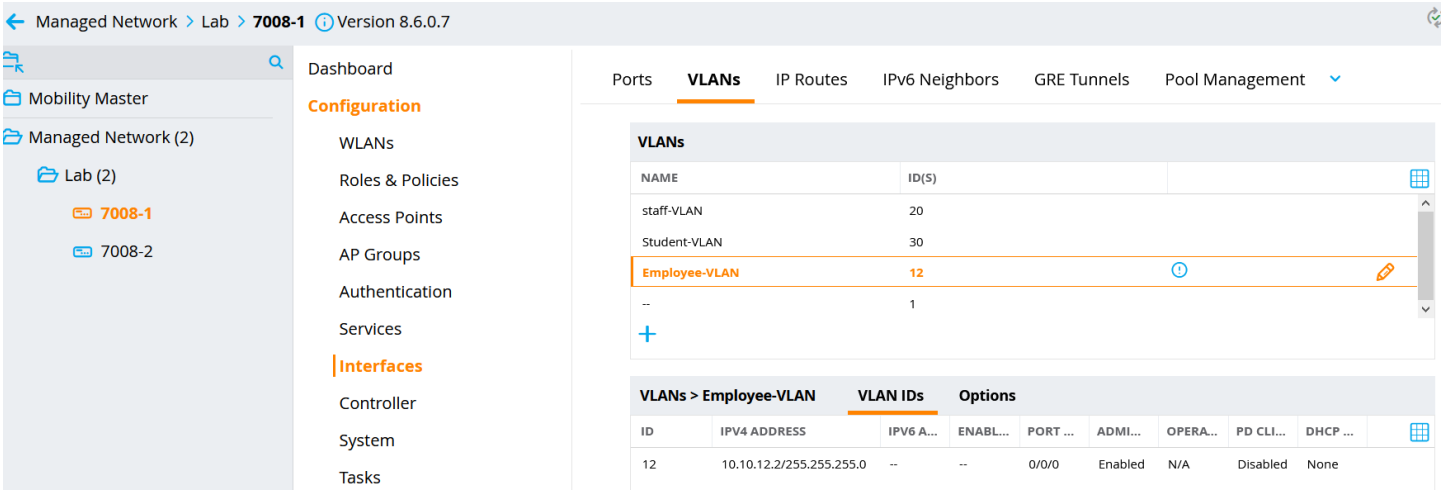


Now from the MM’s device view, we’ll configure the IP addresses for VLAN1, 12, 20 and 30. The aim of hierarchical configuration through folder is that most of the configuration will be done at the folder level and device specific configuration to be done at the device level.

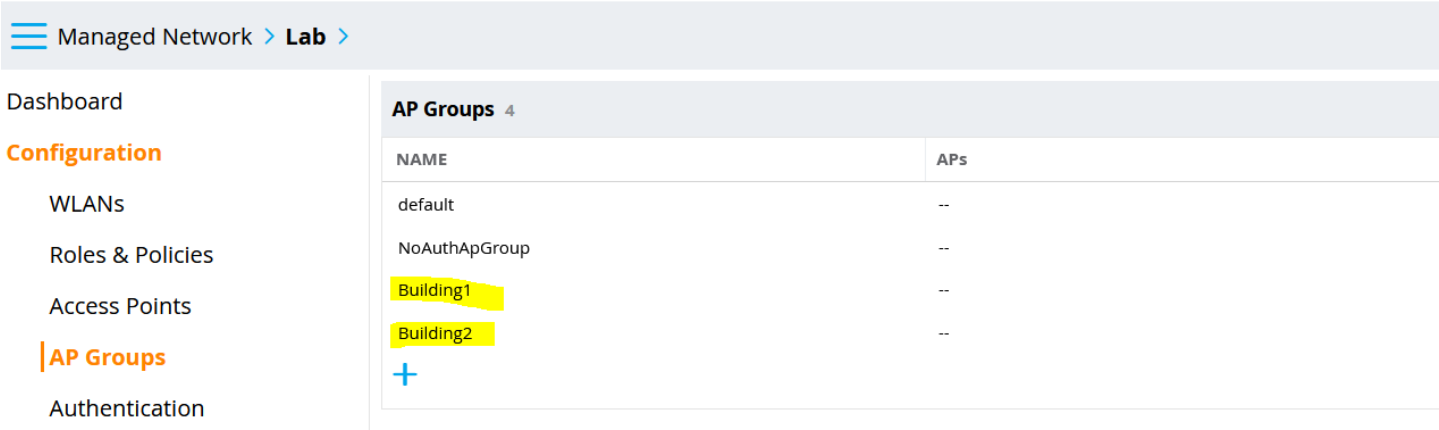




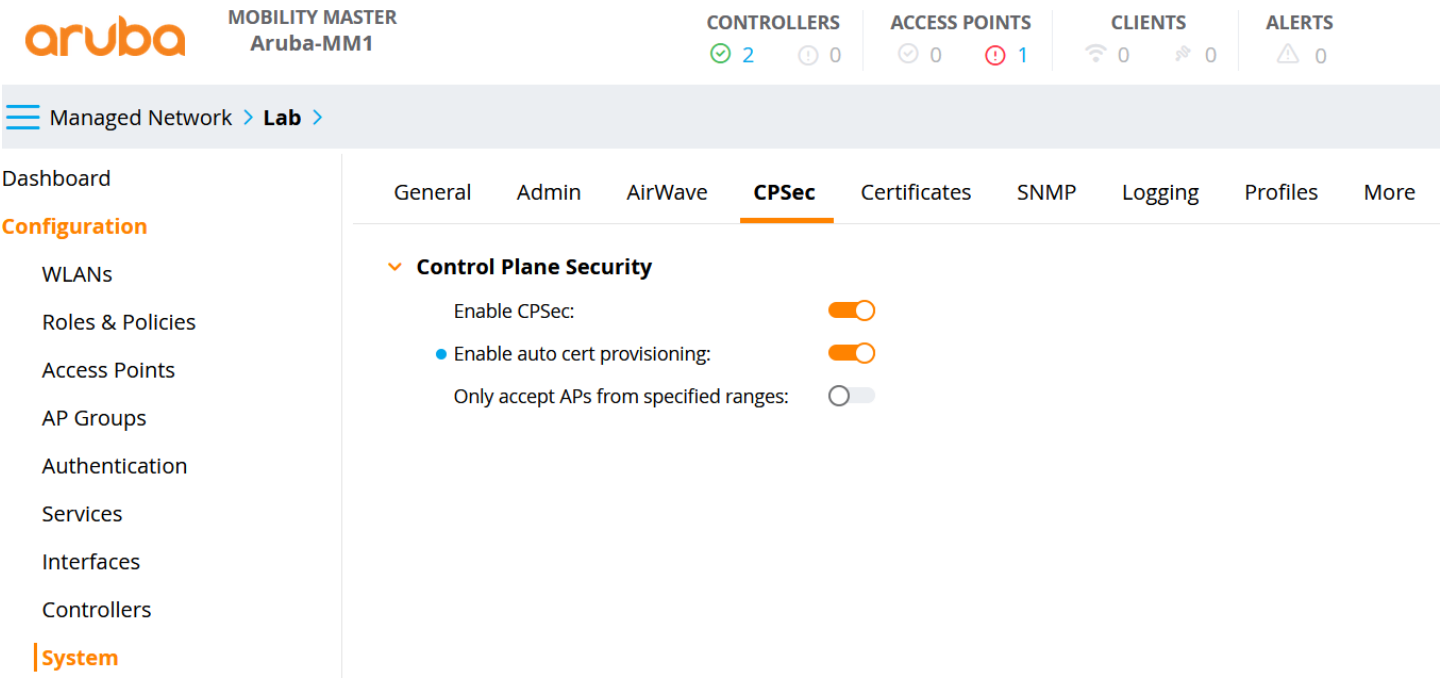




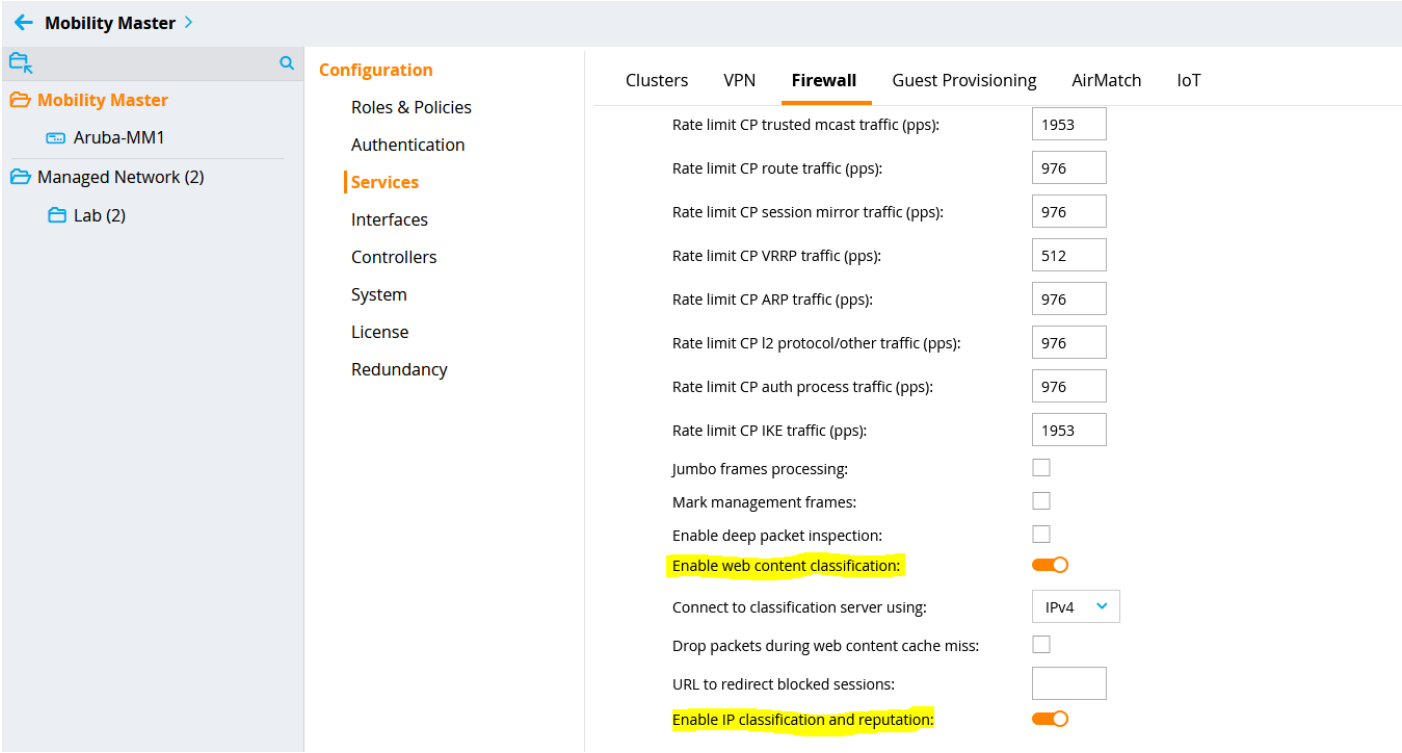
We are going to create couple of AP-groups, you can then put various APs in each group, and they would have their own specific WLAN settings.



Also enable auto certificate provisioning of the APs.

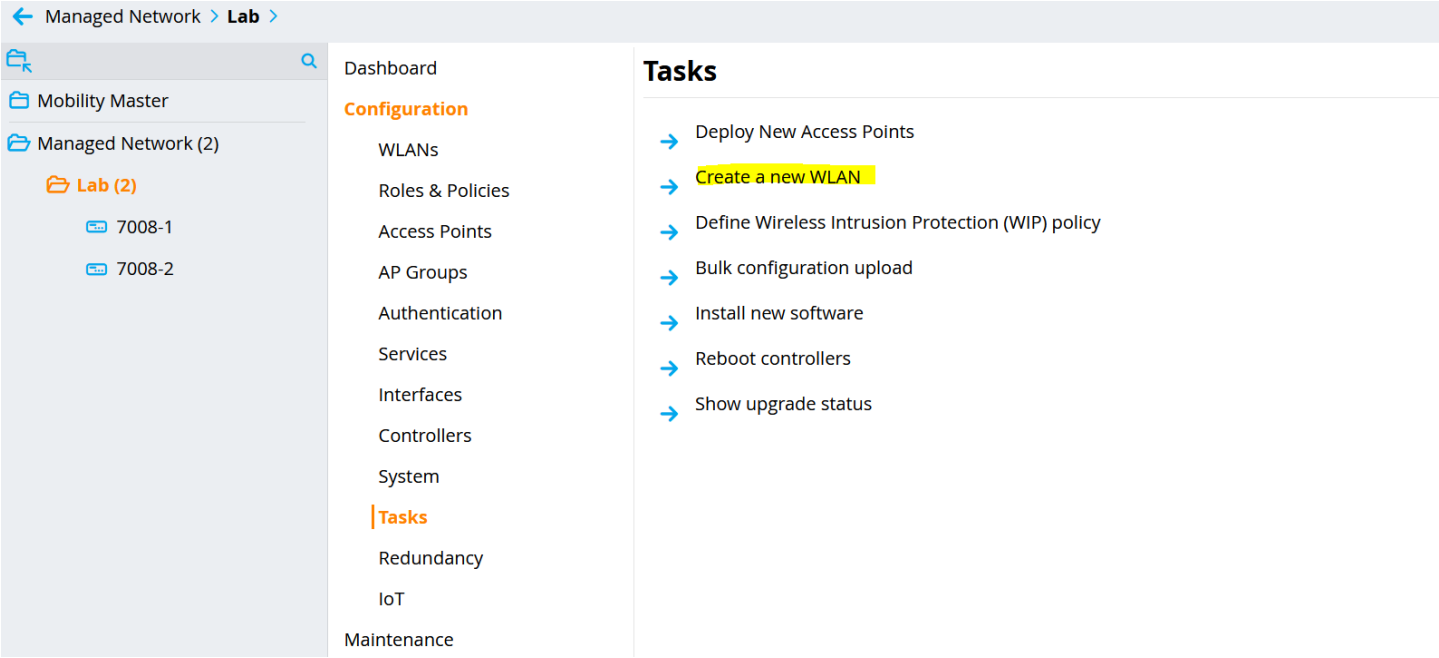


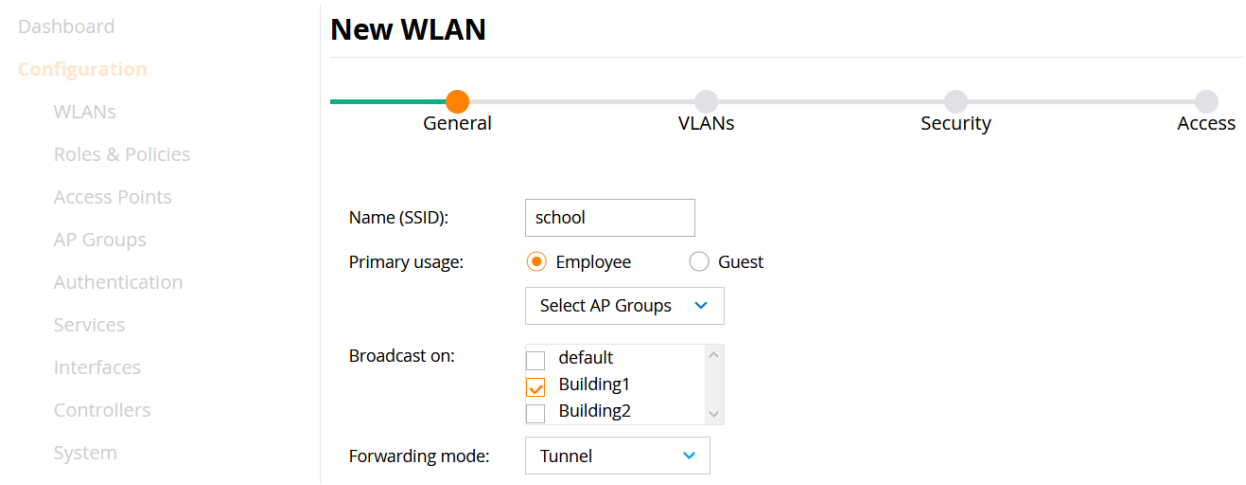
You need to enable the following as well to be able to see the classification and WebCC info in the MD dashboard as well as in Airwave.

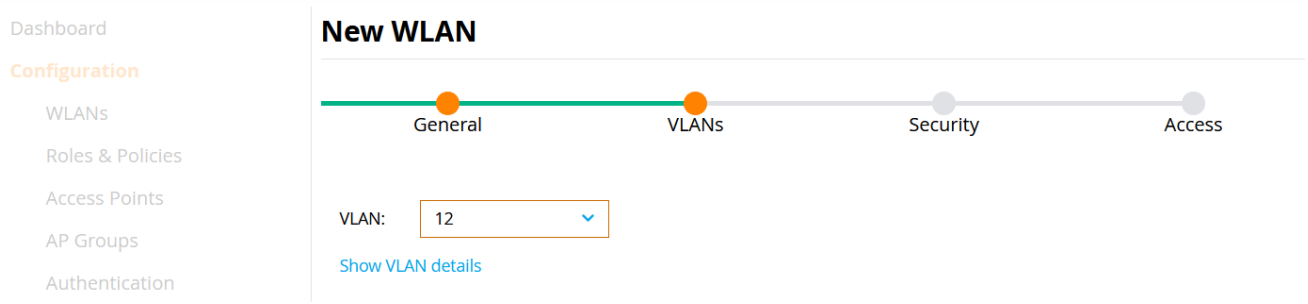


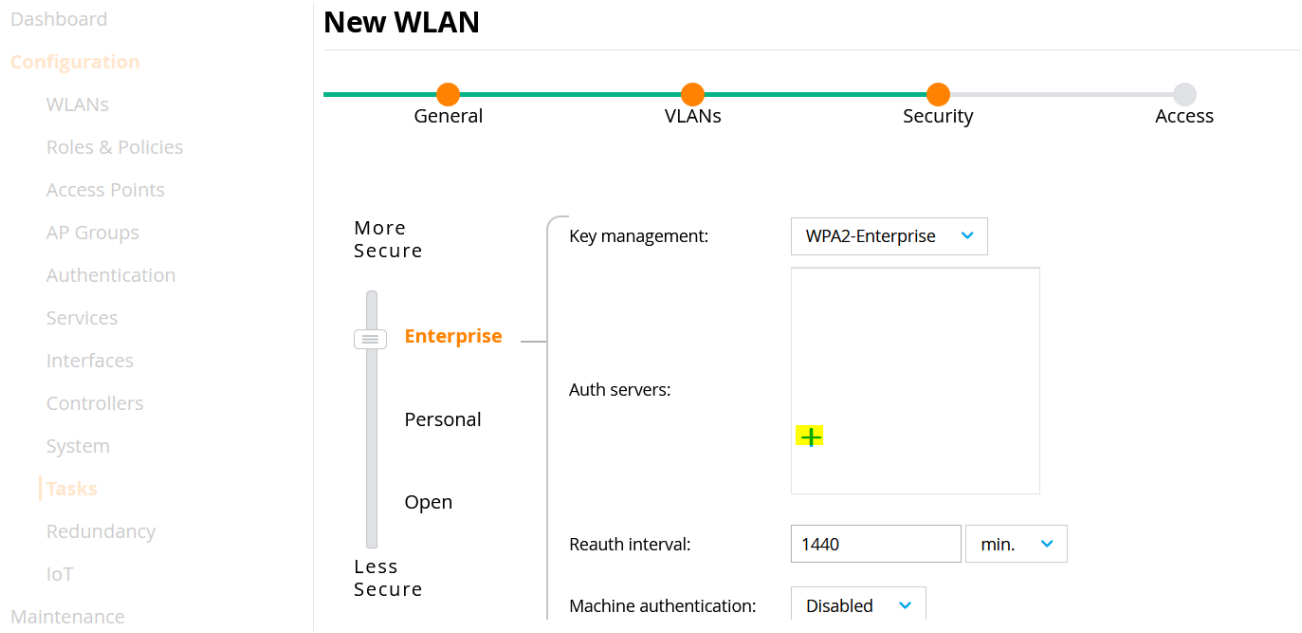
6.1 Dot1x Wireless Configuration

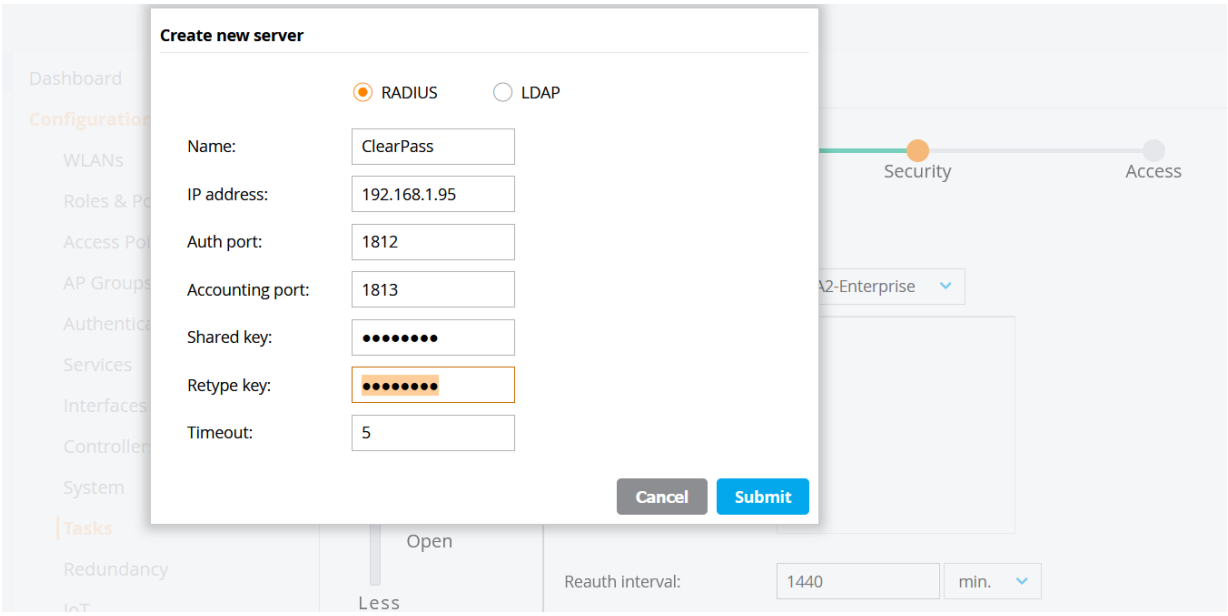
We'll go through the Task wizard to set this up. We are going to create a dot1x WLAN that uses ClearPass as the Authentication server.

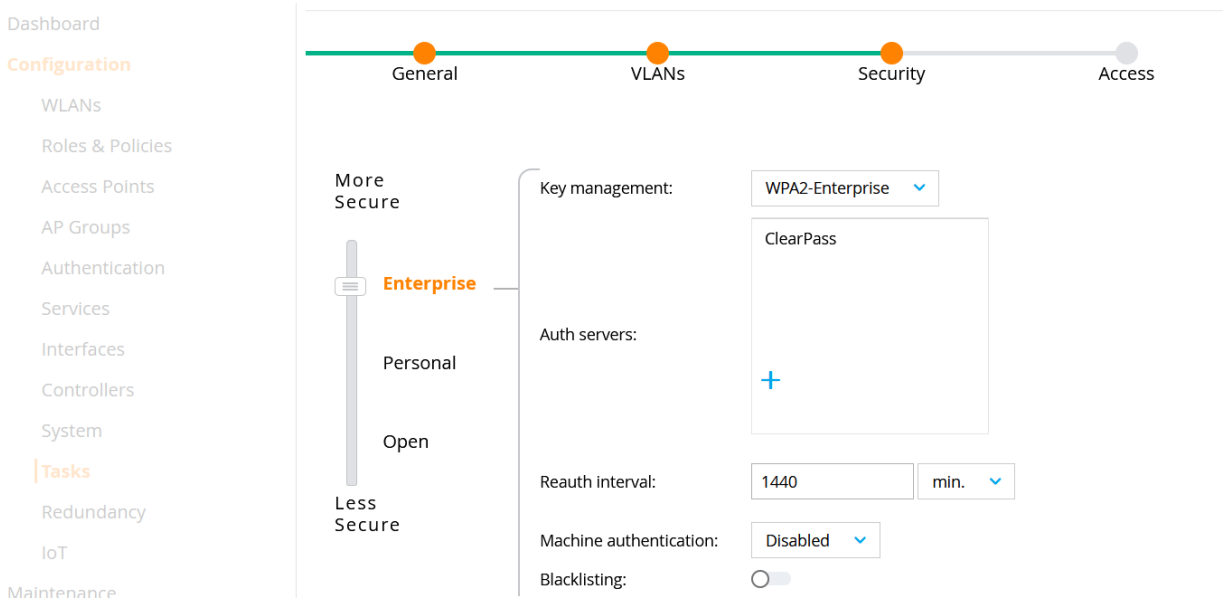

Managed Network > Lab >
Mobility Master
Managed Network (2)
Lab (2)
7008-1
7008-2
Dashboard
Configuration
WLANs
Roles & Policies
Access Points
AP Groups
Authentication
Services
Interfaces
Controllers
System
Tasks
Redundancy
IoT
Maintenance
Tasks
Deploy New Access Points
Create a new WLAN
Define Wireless Intrusion Protection (WIP) policy
Bulk configuration upload
Install new software
Reboot controllers
Show upgrade status

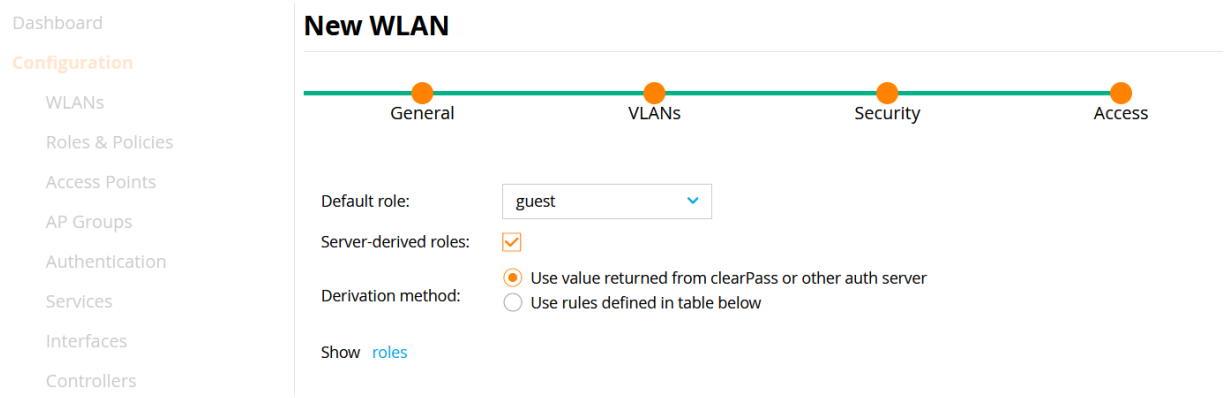

Dashboard
Configuration
WLANs
Roles & Policies
Access Points
AP Groups
Authentication
Services
Interfaces
Controllers
System
New WLAN
General
VLANs
Security
Access
Name (SSID):
school
Primary usage:
Employee
Guest
Select AP Groups
Broadcast on:
default
Building1
Building2
Forwarding mode:
Tunnel

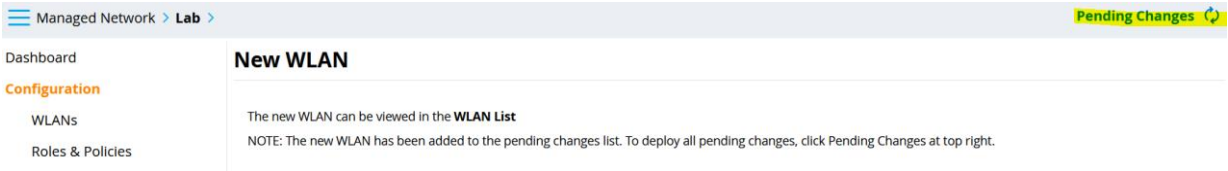

Dashboard
Configuration
WLANs
Roles & Policies
Access Points
AP Groups
Authentication
New WLAN
General
VLANs
Security
Access
VLAN:
12
Show VLAN details

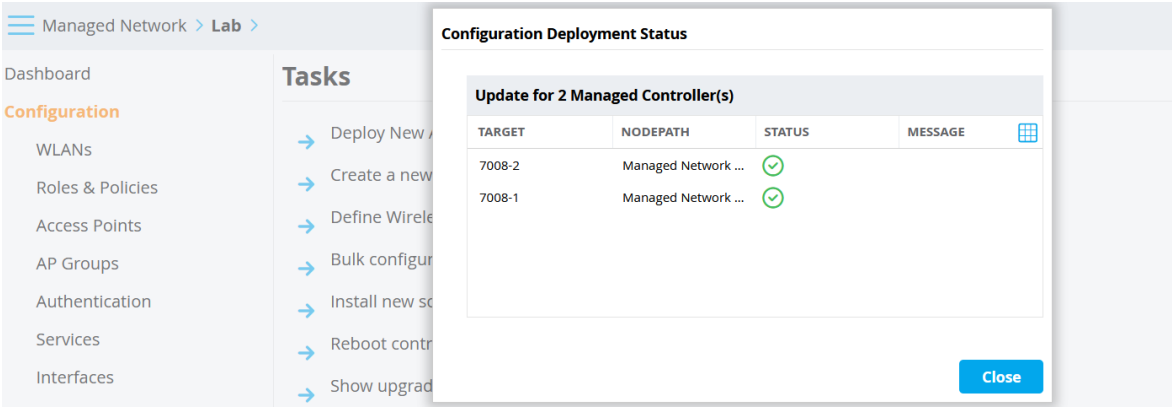

Dashboard
Configuration
WLANs
Roles & Policies
Access Points
AP Groups
Authentication
Services
Interfaces
Controllers
System
Tasks
Redundancy
IoT
Maintenance
New WLAN
General
VLANs
Security
Access
More Secure
Enterprise
Personal
Open
Less Secure
Key management:
WPA2-Enterprise
Auth servers:
Reauth interval:
1440
min.
Machine authentication:
Disabled


Create new server
RADIUS
LDAP
Name:
ClearPass
IP address:
192.168.1.95
Auth port:
1812
Accounting port:
1813
Shared key:
Retype key:
Timeout:
5
Cancel
Submit
Security
Access
Open
Less
Reauth interval:
1440
min.

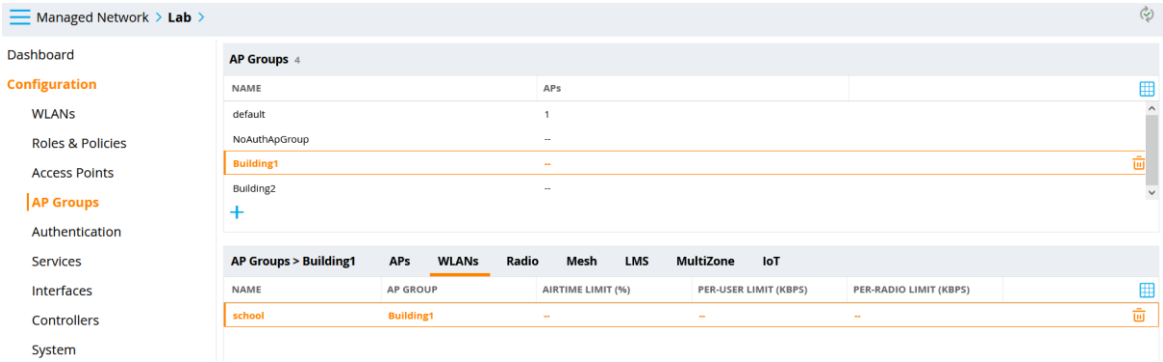

Dashboard
Configuration
WLANs
Roles & Policies
Access Points
AP Groups
Authentication
Services
Interfaces
Controllers
System
Tasks
Redundancy
IoT
Maintenance
General
VLANs
Security
Access
More Secure
Enterprise
Personal
Open
Less Secure
Key management:
WPA2-Enterprise
ClearPass
Auth servers:
Reauth interval:
1440
min.
Machine authentication:
Disabled
Blacklisting:



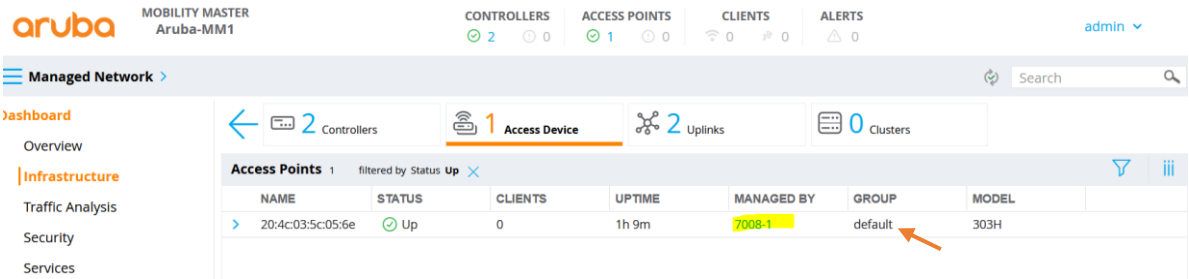




Make sure to submit and apply changes.



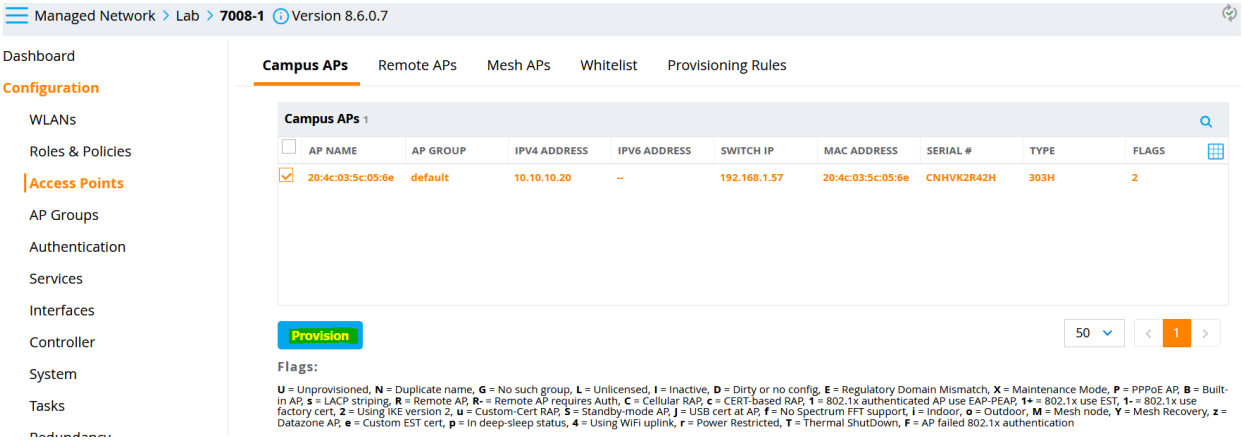
Now you can connect the APs, we'll not be covering the discovery process that APs use, but since the APs are not sharing L2 adjacencies with the controllers, we'll use the DNS method. Here you'll notice that the new AP has ended up in default ap-group.

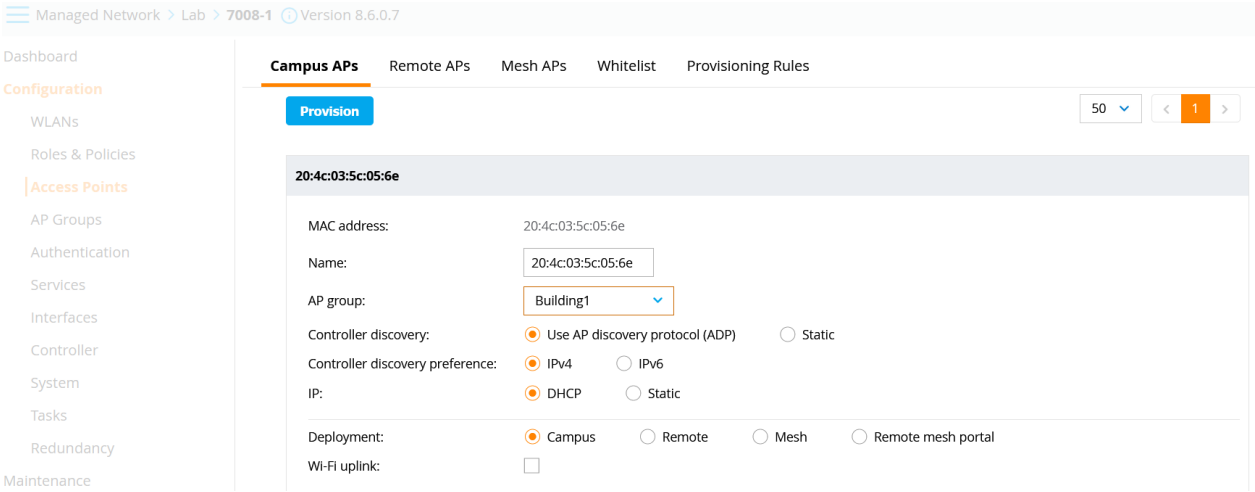


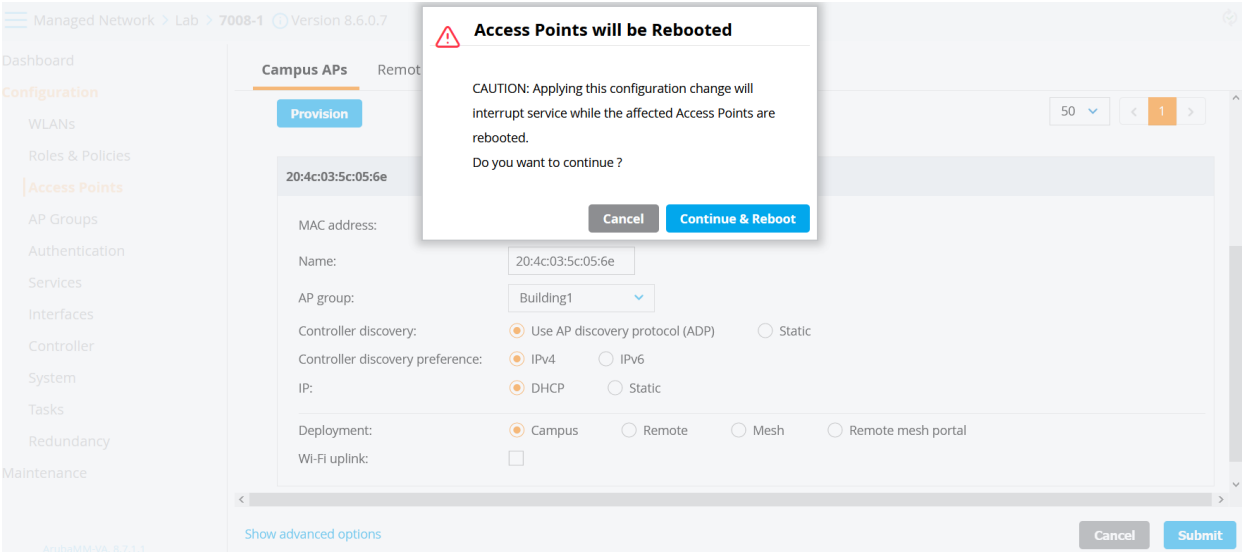
Notice that the AP has landed on 7008-1 because "aruba-master" resolves to that IP address. If we had enabled clustering, then after AP's initial contact to 7008-1 it would also learn the IP address of the 7008-2 controller. More

about that later. Note that the best practice is to point the “aruba-master” DNS resolution to VRRP VIP address that covers two or more controllers.

Anyway, we’ll select this AP and move to buidling1 AP-group

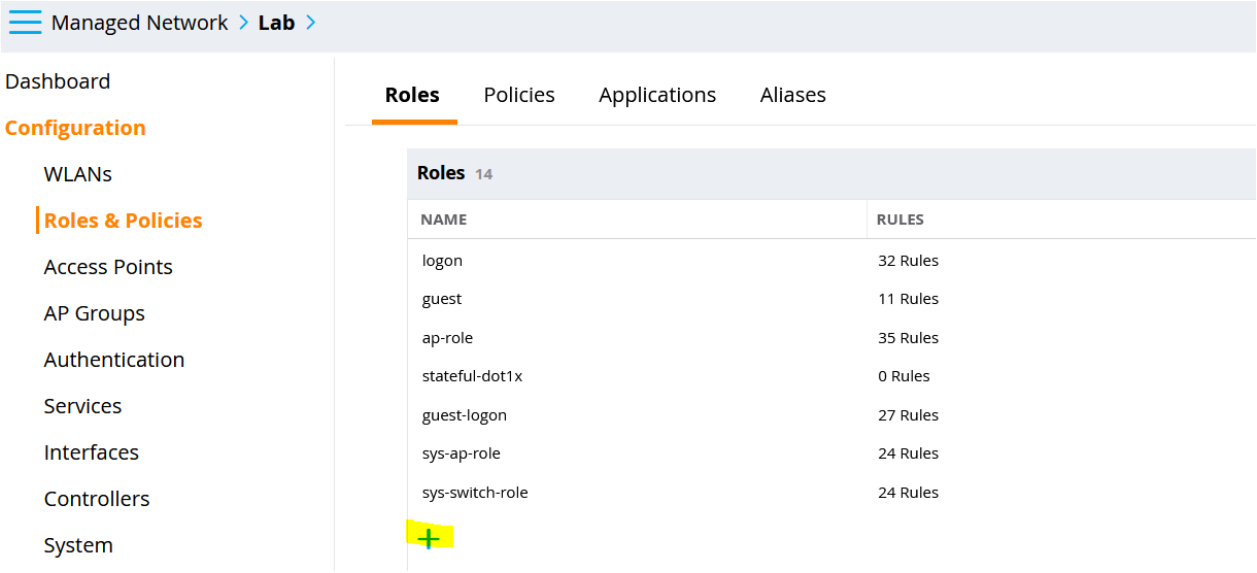


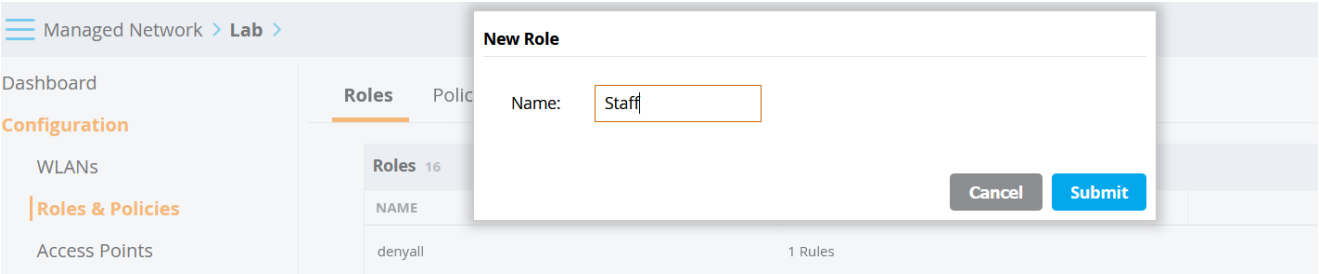


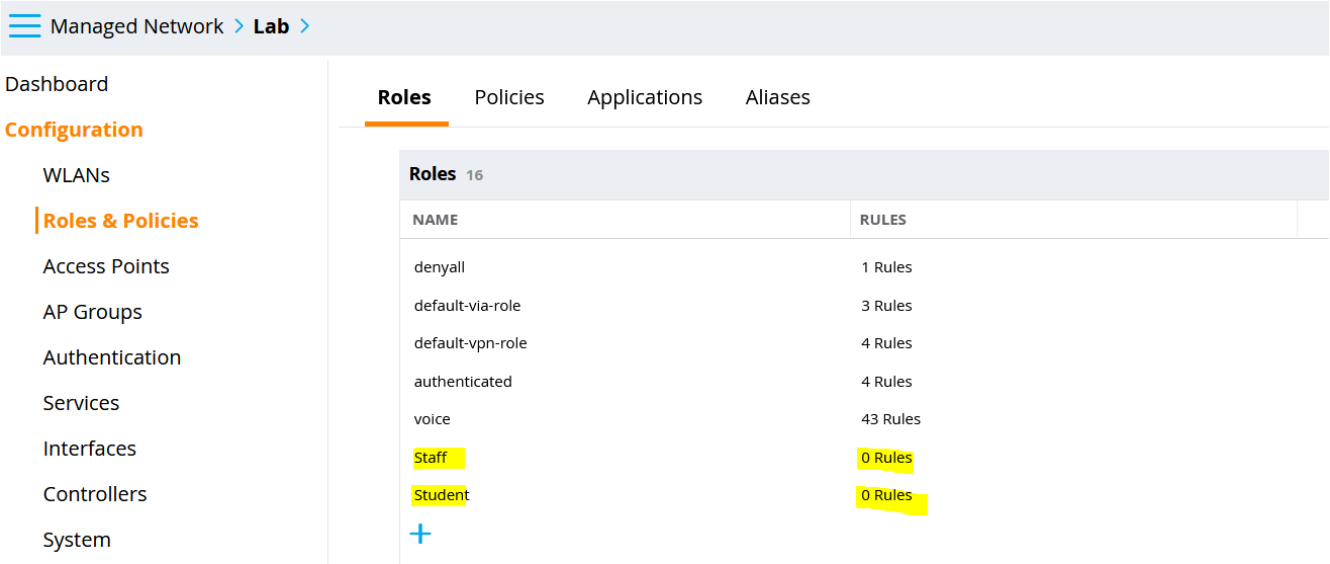


Now when the AP reboots, it will be in building1 ap-group and will broadcast “school” SSID.

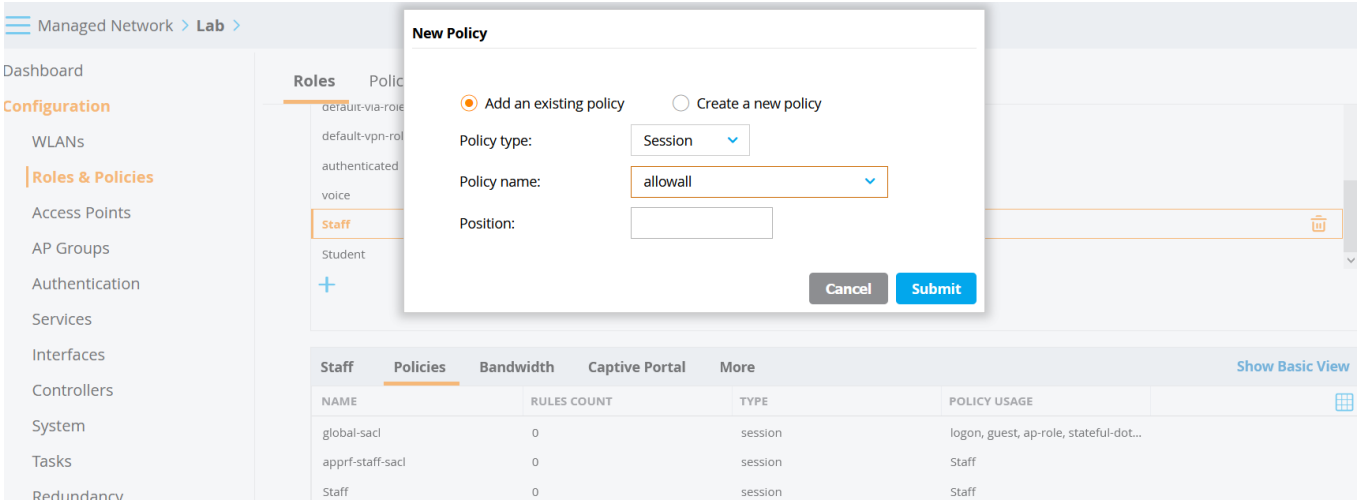
Here we’ll create the user roles that ClearPass will pass to MDs based on the policies that will be configured

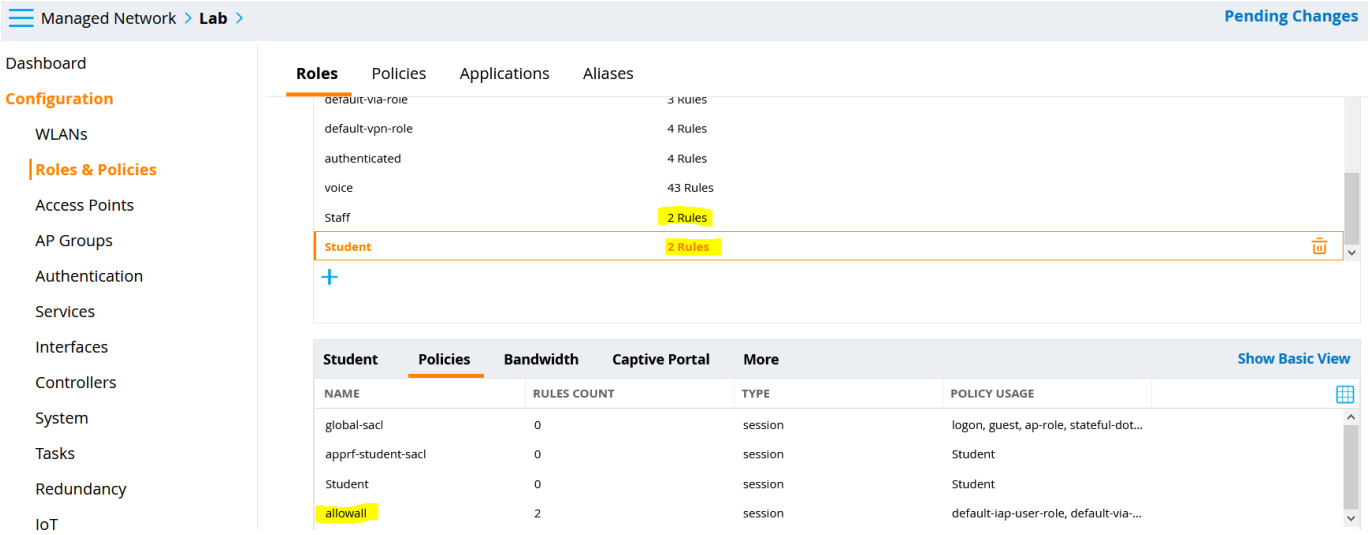




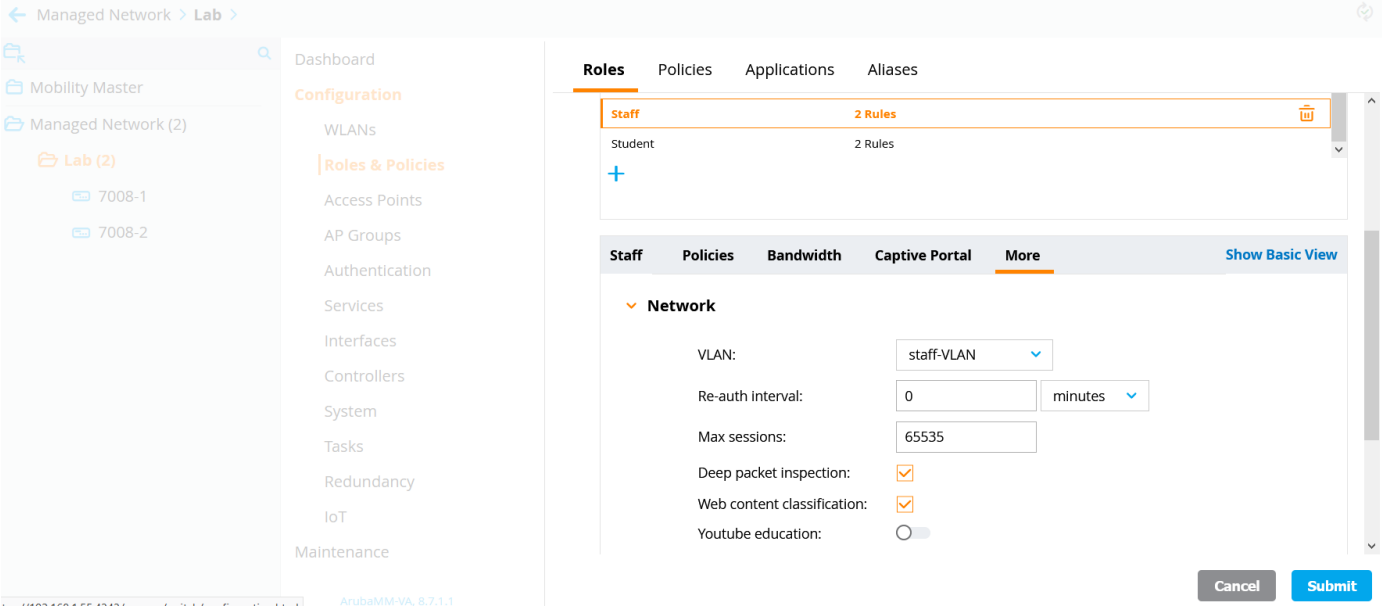


We'll just add a "allow-all" policy to both user roles.



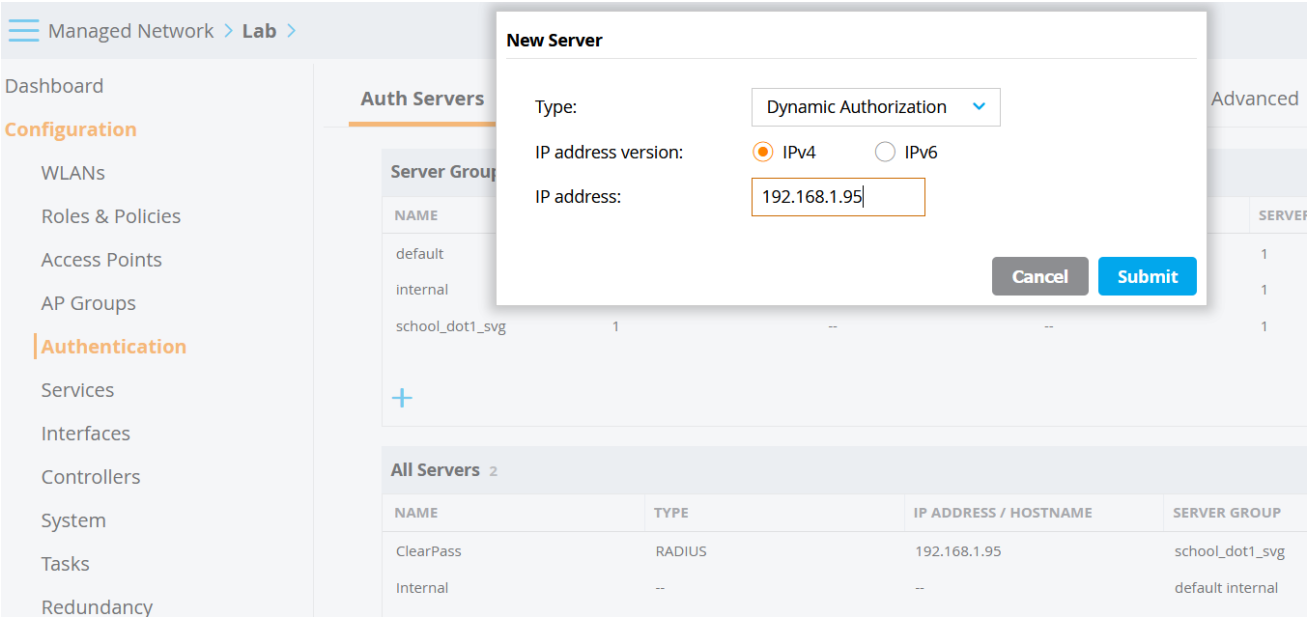


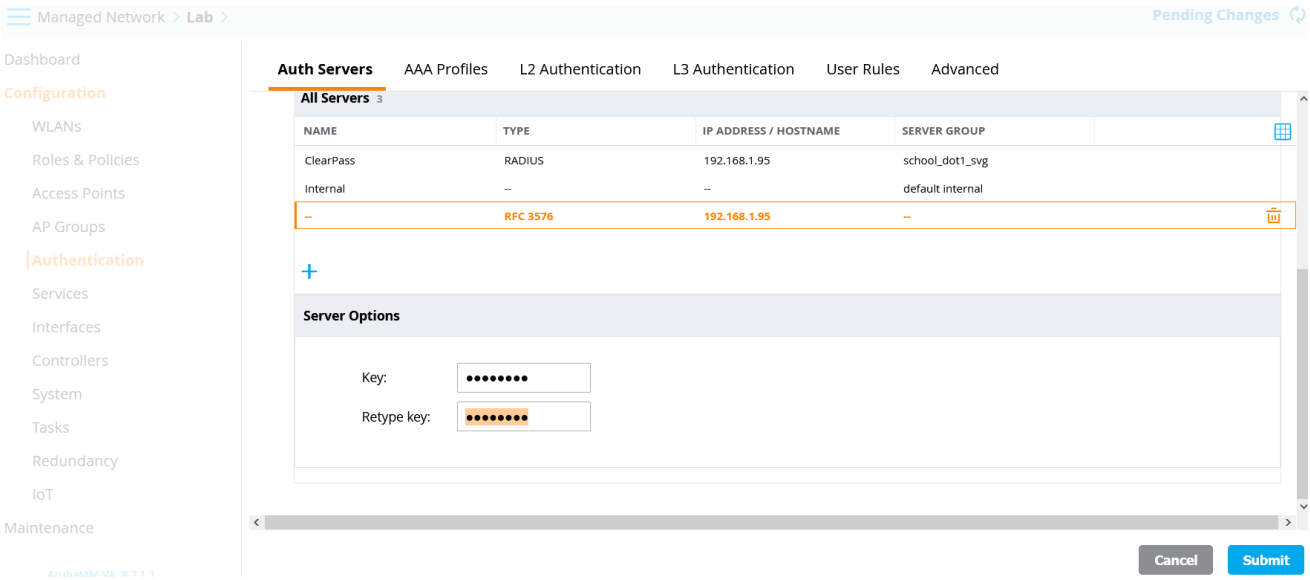
Lastly, we'll also assign a VLAN to each role



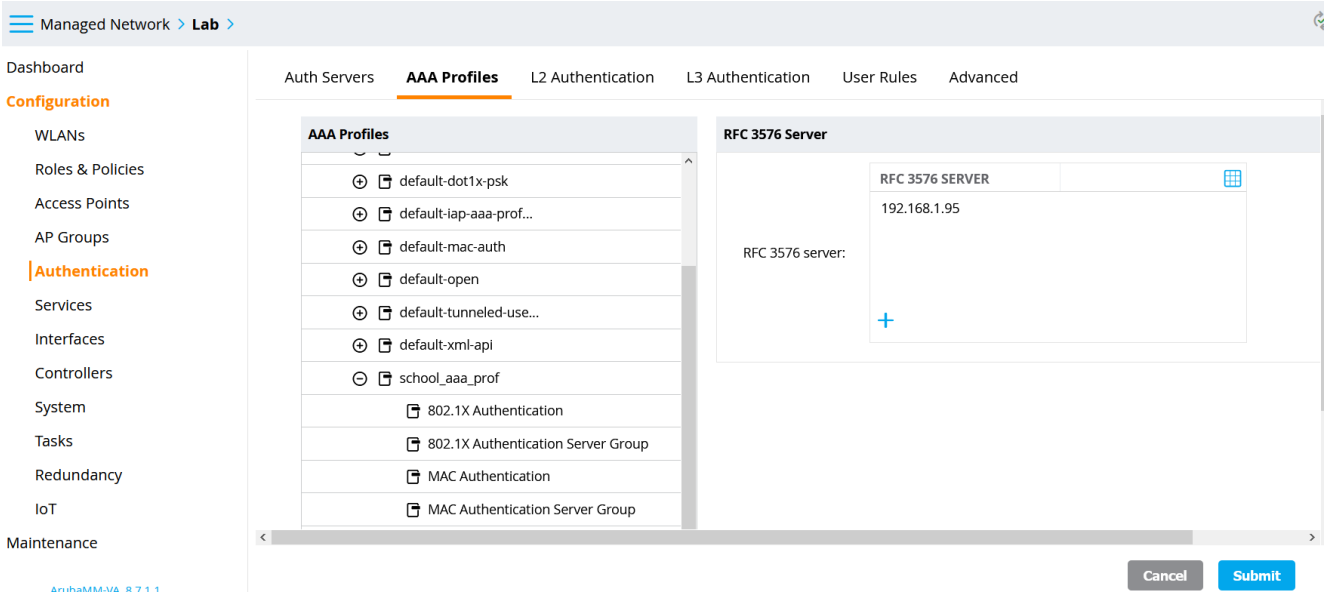
We'll do the same thing for the student user role.

Here we'll configure dynamic authorisation that will use CoA. It is pointing to the same ClearPass

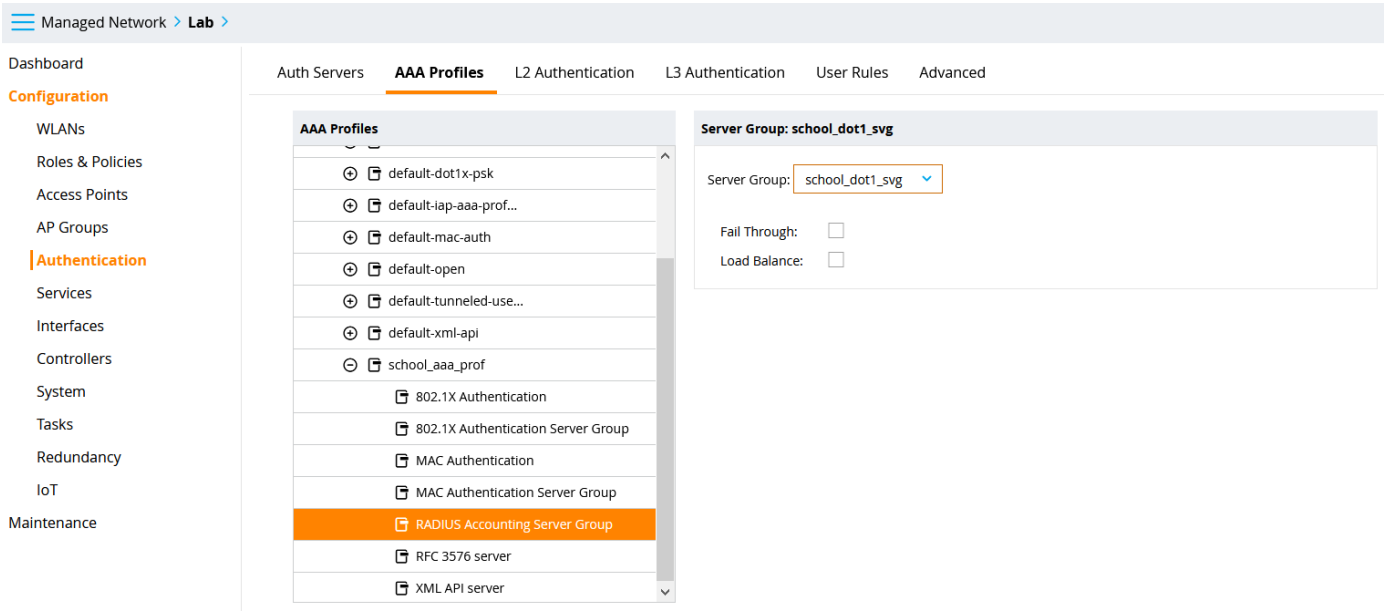




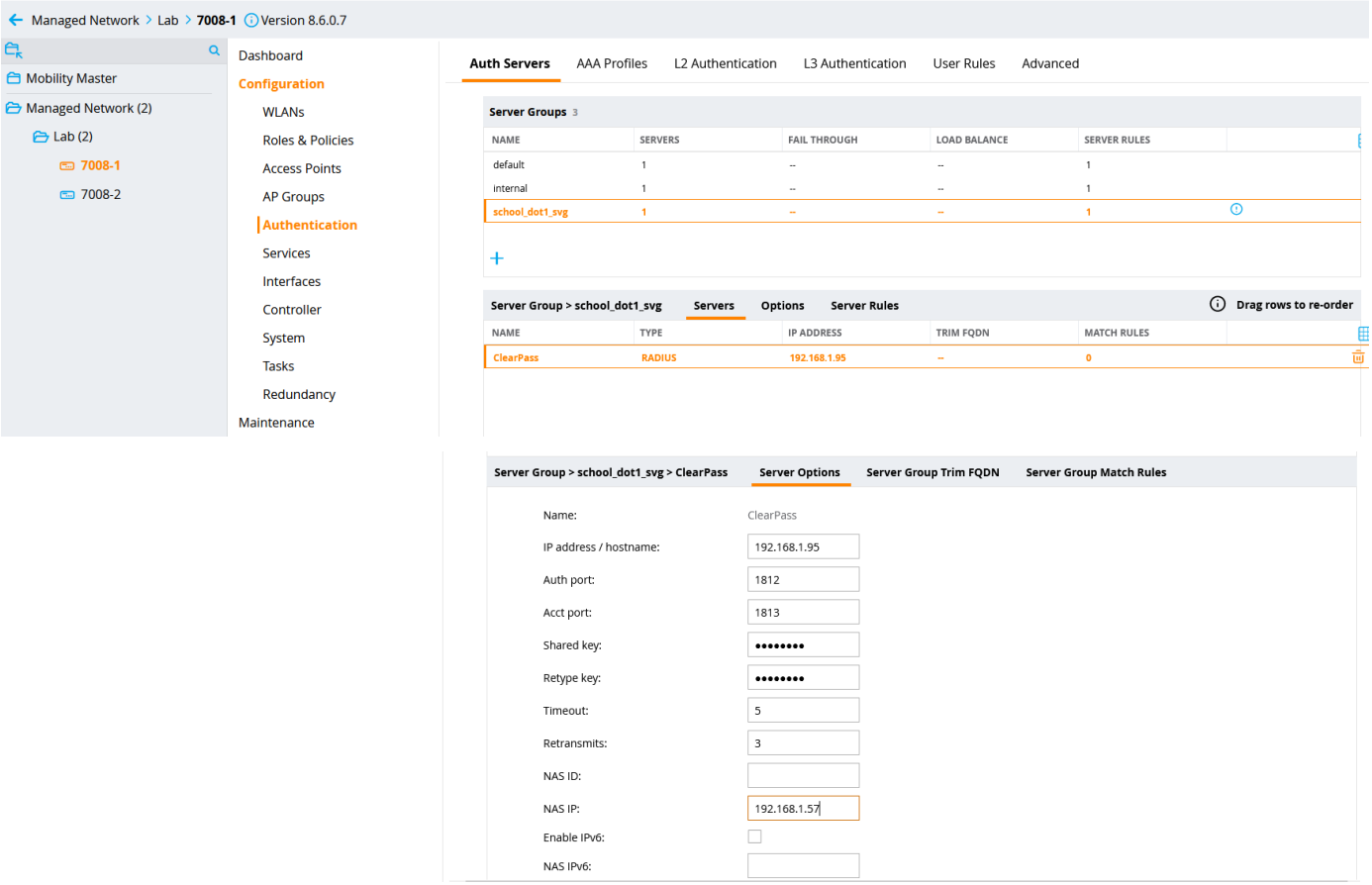
And we'll add rfc3576 sever to the AAA profile for the School WLAN



And enable RADIUS accounting, note that we can create a new accounting server group but here we'll sue the same.



Now because CoA will need to have a specific IP address of MD (controller) , we need to specify that at the device level and as seen here we are assigning 192.168.1.57 as NAS ID.

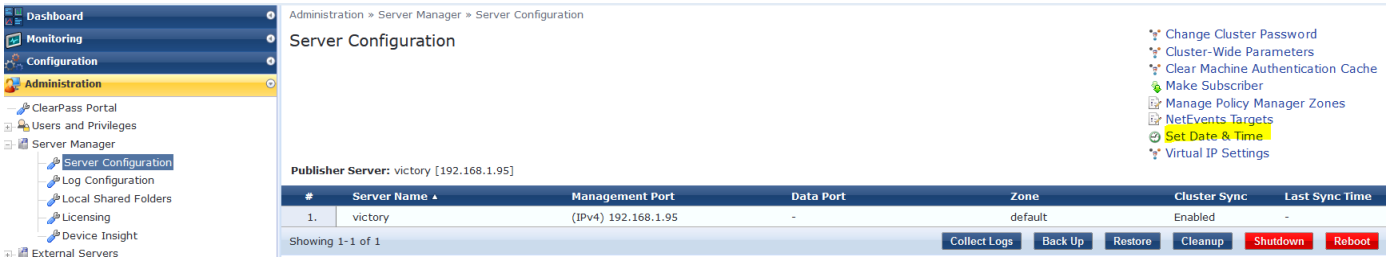


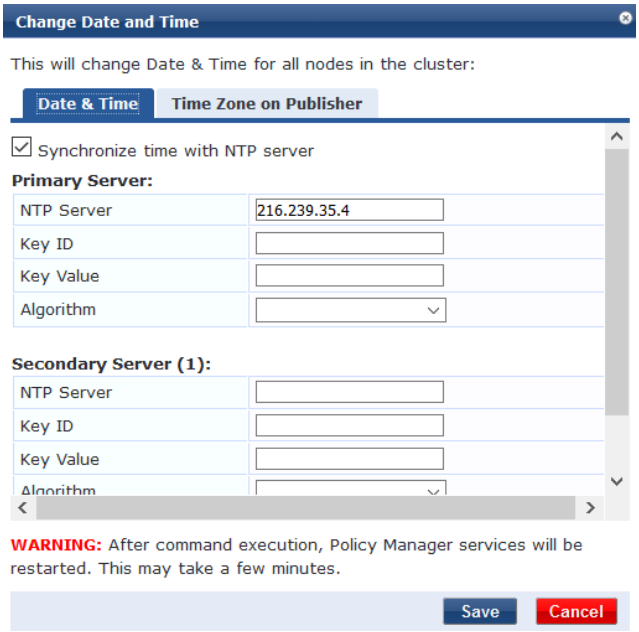
Here is the table outlining the user roles and their corresponding VLAN IDs and subnets.

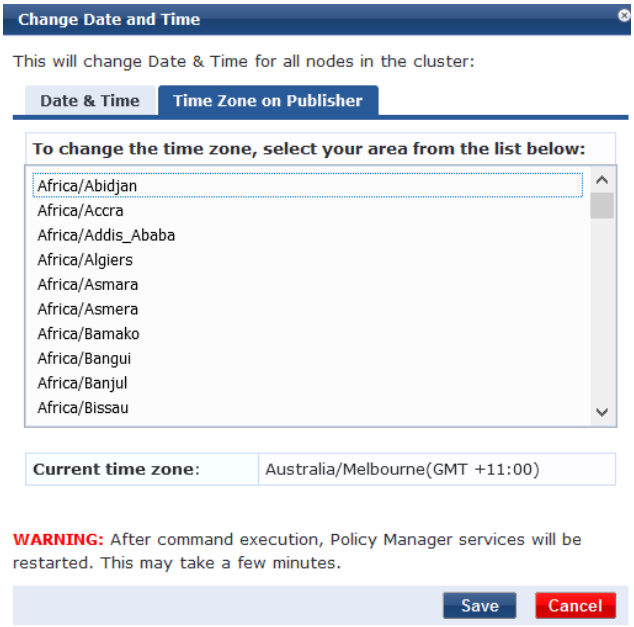
User role	VLAN ID	IP subnet
Staff	20	10.10.20.0/24
Student	30	10.10.30.0/24
Employee	12	10.10.12.0/24

6.2 ClearPass Basic Configuration

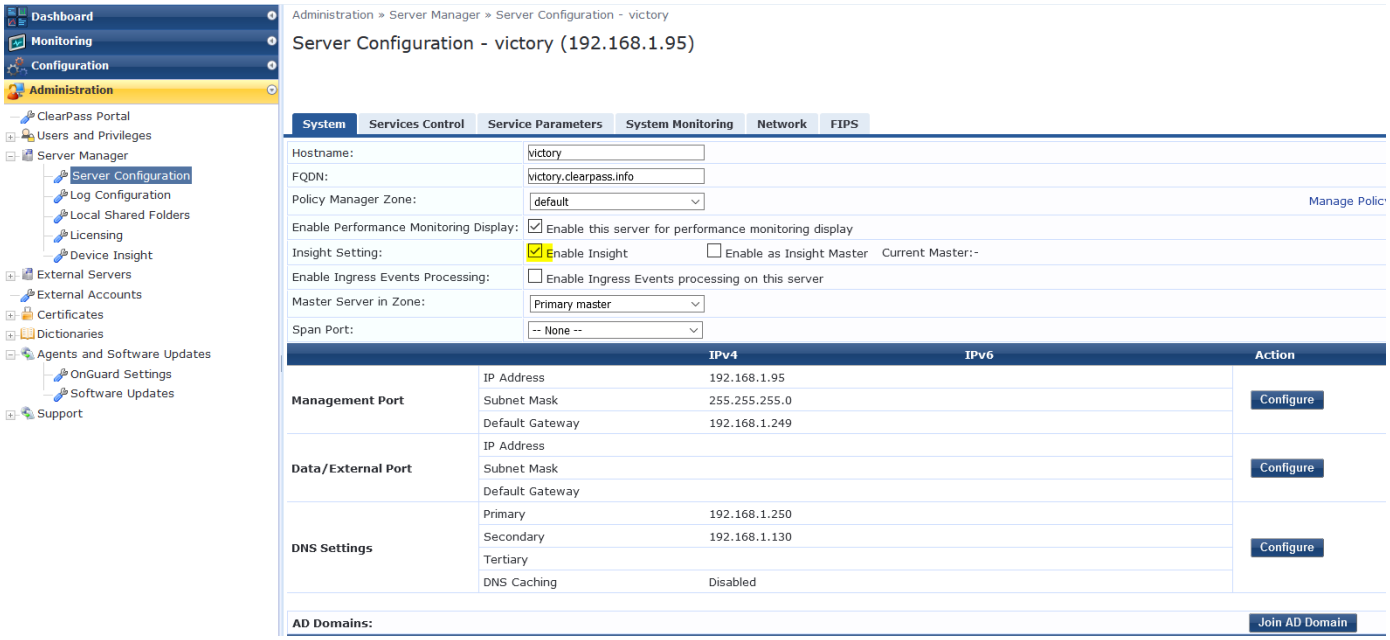
In this section we'll do the basic ClearPass configuration and join it to the AD domain. We'll start with NTP and time zone.





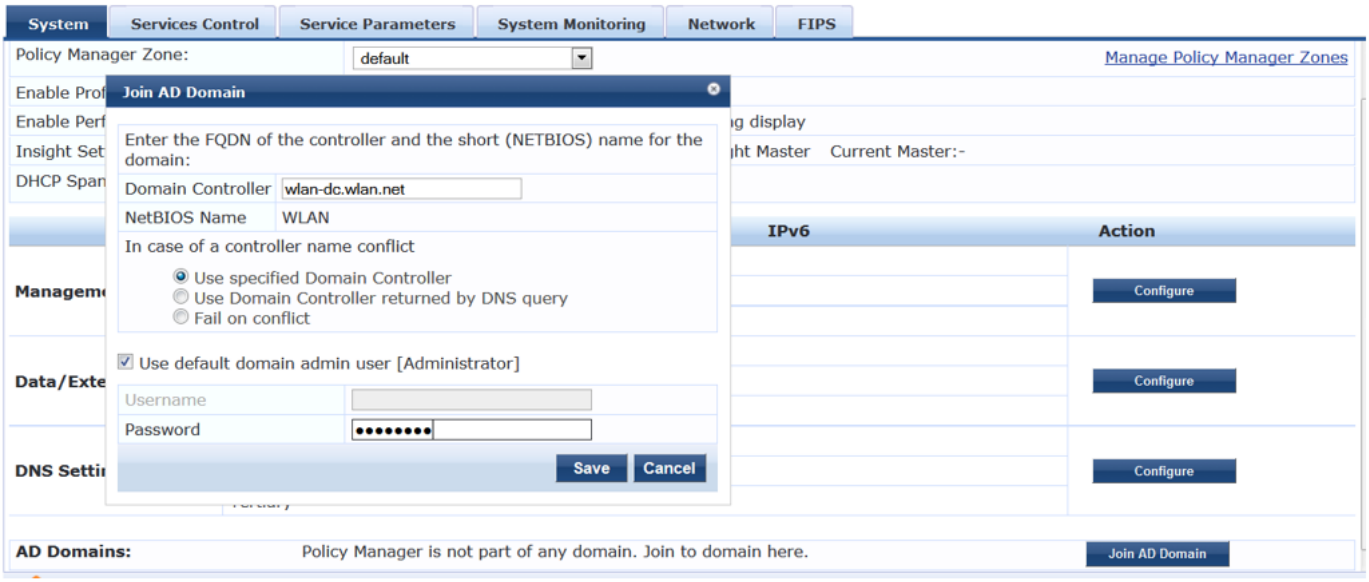


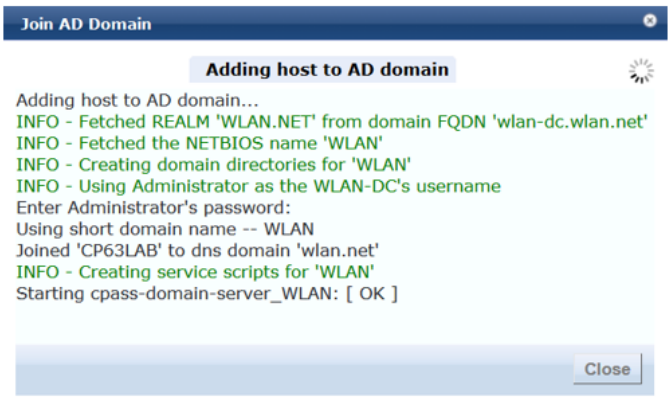
Then enabling Insight which is the reporting module of ClearPass

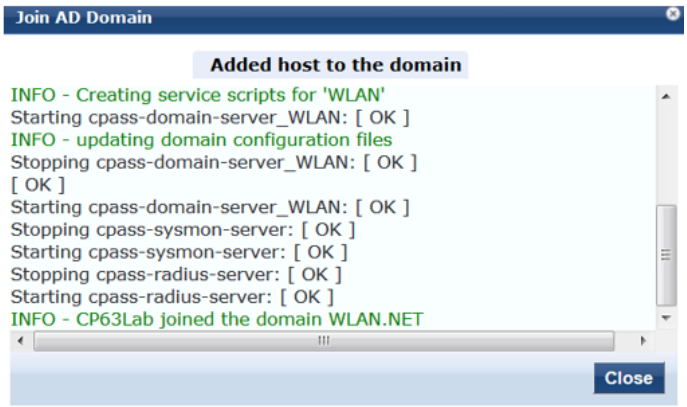


6.3 Joining AD Domain

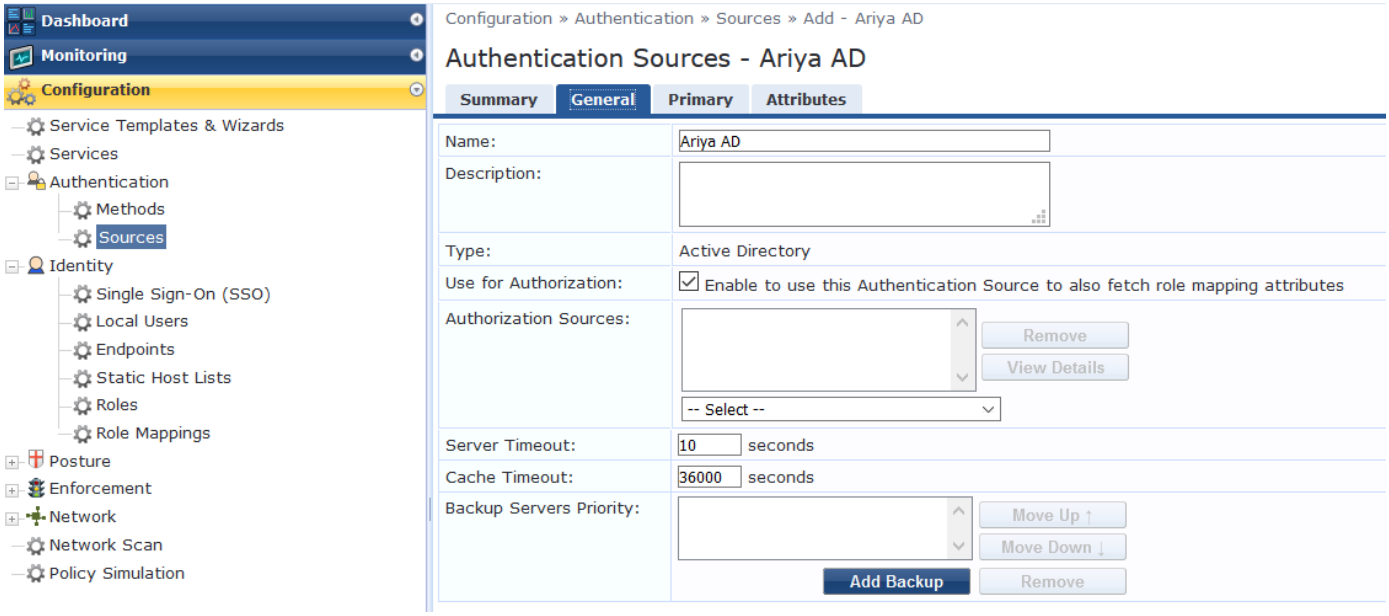
Configure the IP addresses and the rest as per your Lab setup but ensure you have the IP address of your domain controller as the primary DNS. CPPM needs to join the AD domain, in order to authenticate against it. Make sure the clock time for AD and CPPM are almost in sync. It is best to use NTP. If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







Now we need to add the AD as authentication source.



Configuration » Authentication » Sources » Add - Ariya AD

Authentication Sources - Ariya AD

Summary | General | Primary | Attributes

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

Configuration » Authentication » Sources » Add - Ariya AD

Authentication Sources - Ariya AD

Summary | General | Primary | Attributes

Specify filter queries used to fetch authentication and authorization attributes

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

6.4 ClearPass dot1x Service

Here we'll create a dot1x service for wireless access.

ClearPass Policy Manager

Configuration » Services

Services

Add | Import | Export All

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

Filter: Name contains Go Clear Filter Show 20 records

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

Summary | Service | Authentication | Roles | Enforcement

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

Service Rule

Matches ○ ANY or ◉ ALL of the following conditions:

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

“school” is the name of the SSID

Summary | Service | Authentication | Roles | Enforcement

Authentication Methods:	[EAP PEAP] [EAP TLS] Move Up ↑ / Move Down ↓ / Remove / View Details / Modify --Select to Add--
Authentication Sources:	Ariya AD [Active Directory] Move Up ↑ / Move Down ↓ / Remove / View Details / Modify --Select to Add--
Strip Username Rules:	☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes
Service Certificate:	--Select to Add--

Summary | Service | Authentication | Roles | Enforcement

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

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

Conditions	Role

Summary | Service | Authentication | Roles | Enforcement

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

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

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

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

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

Enforcement Profiles - AA Aruba 802.1X Wireless Default Profile

Note: This Enforcement Profile is created by Service Template

Summary | Profile | Attributes

Profile:

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

Attributes:

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

Enforcement Profiles - AA-Aruba 802.1X Wireless Staff Profile

Note: This Enforcement Profile is created by Service Template

Summary | Profile | Attributes

Profile:

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

Attributes:

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

Enforcement Profiles - AA-Aruba 802.1X Wireless Student Profile

Note: This Enforcement Profile is created by Service Template

Summary | Profile | Attributes

Profile:

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

Attributes:

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

Enforcement Profiles - AA Aruba 802.1X Wireless Update Endpoint Location

Note: This Enforcement Profile is created by Service Template

Summary | Profile | Attributes

Profile:

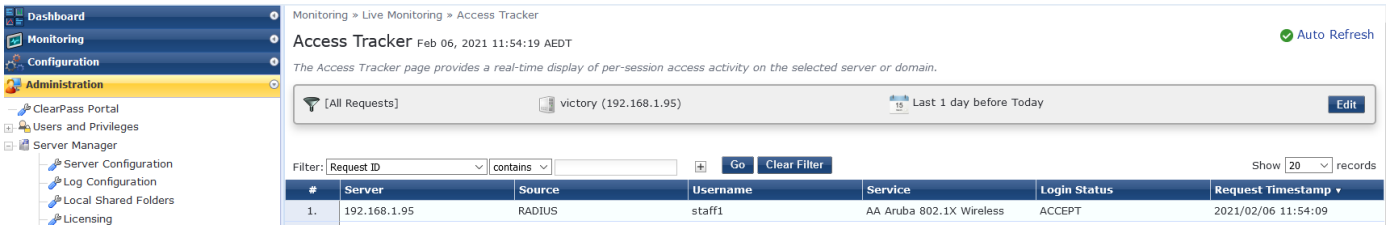
Name:	AA Aruba 802.1X Wireless Update Endpoint Location
Description:	
Type:	Post_Authentication
Action:	
Device Group List:	-

Attributes:

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

6.5 ClearPass Access tracker

Now we'll test by connecting to the school SSID.



Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R00000000-01-601de8a8
Date and Time:	Feb 06, 2021 11:54:09 AEDT
End-Host Identifier:	A0-88-B4-50-C0-84 (Computer / Windows / Windows)
Username:	staff1
Access Device IP/Port:	192.168.1.57 (MD-1 / Aruba)
Access Device Name:	7008-1
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	AA Aruba 802.1X Wireless
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:192.168.1.250
Authorization Source:	Ariya AD
Roles:	[User Authenticated]
Enforcement Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless

Showing 1 of 1-20 records | Change Status | Show Configuration | Export | Show Logs | Close

Request Details

Summary | Input | Output | Accounting

Username:	staff1
End-Host Identifier:	A0-88-B4-50-C0-84 (Computer / Windows / Windows)
Access Device IP/Port:	192.168.1.57 (MD-1 / Aruba)

RADIUS Request

Authorization Attributes

Authorization:Ariya AD:Account Expires	9223372036854775807 [30828-09-14 12:48:05 AEST]
Authorization:Ariya AD:memberOf	CN=Administrators,CN=Builtin,DC=wlan,DC=net, CN=Staff,CN=Users,DC=wlan,DC=net
Authorization:Ariya AD:Name	staff1
Authorization:Ariya AD:UserDN	CN=staff1,CN=Users,DC=wlan,DC=net

Computed Attributes

Endpoint Attributes

Summary | Input | Output | Accounting

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

RADIUS Response

Endpoint:Last Known Location	192.168.1.57:20:4c:03:5c:05:6e
Radius:Aruba:Aruba-User-Role	Staff

Summary | Input | Output | Accounting

Account Session ID:	staff1A088B450C084-601DE8B3-C2FE1
Start Timestamp:	Feb 06, 2021 11:54:11 AEDT
End Timestamp:	Still Active
Status:	Active
Termination Cause:	-
Service Type:	-
Number of Authentication Sessions:	1

Network Details

Utilization

Authentication Sessions Details

We'll use another device to connect and login as student1

Access Tracker Feb 06, 2021 11:59:19 AEDT

Auto Refresh

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

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

Filter: Request ID contains Go Clear Filter Show 20 records

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.95	RADIUS	student1	AA Aruba 802.1X Wireless	ACCEPT	2021/02/06 11:59:18
2.	192.168.1.95	RADIUS	staff1	AA Aruba 802.1X Wireless	ACCEPT	2021/02/06 11:59:08

Summary Input Output Accounting

Login Status:	ACCEPT
Session Identifier:	R00000004-01-601de9e6
Date and Time:	Feb 06, 2021 11:59:18 AEDT
End-Host Identifier:	12-65-72-CA-22-BE
Username:	student1
Access Device IP/Port:	192.168.1.57 (MD-1 / Aruba)
Access Device Name:	7008-1
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	AA Aruba 802.1X Wireless
Authentication Method:	EAP-PEAP
Authentication Source:	AD:192.168.1.250
Authorization Source:	Ariya AD
Roles:	[User Authenticated]
Enforcement Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless

Showing 2 of 1-20 records Change Status Show Configuration Export Show Logs Close

Summary Input Output Accounting

Username:	student1	
End-Host Identifier:	12-65-72-CA-22-BE	
Access Device IP/Port:	192.168.1.57	(MD-1 / Aruba)

RADIUS Request

Authorization Attributes

Authorization:Ariya AD:Account Expires	9223372036854775807 [30828-09-14 12:48:05 AEST]
Authorization:Ariya AD:Email	ariyap@hpe.com
Authorization:Ariya AD:memberOf	CN=Student,CN=Users,DC=wlan,DC=net
Authorization:Ariya AD:Name	student1
Authorization:Ariya AD:UserDN	CN=student1,CN=Users,DC=wlan,DC=net

Computed Attributes

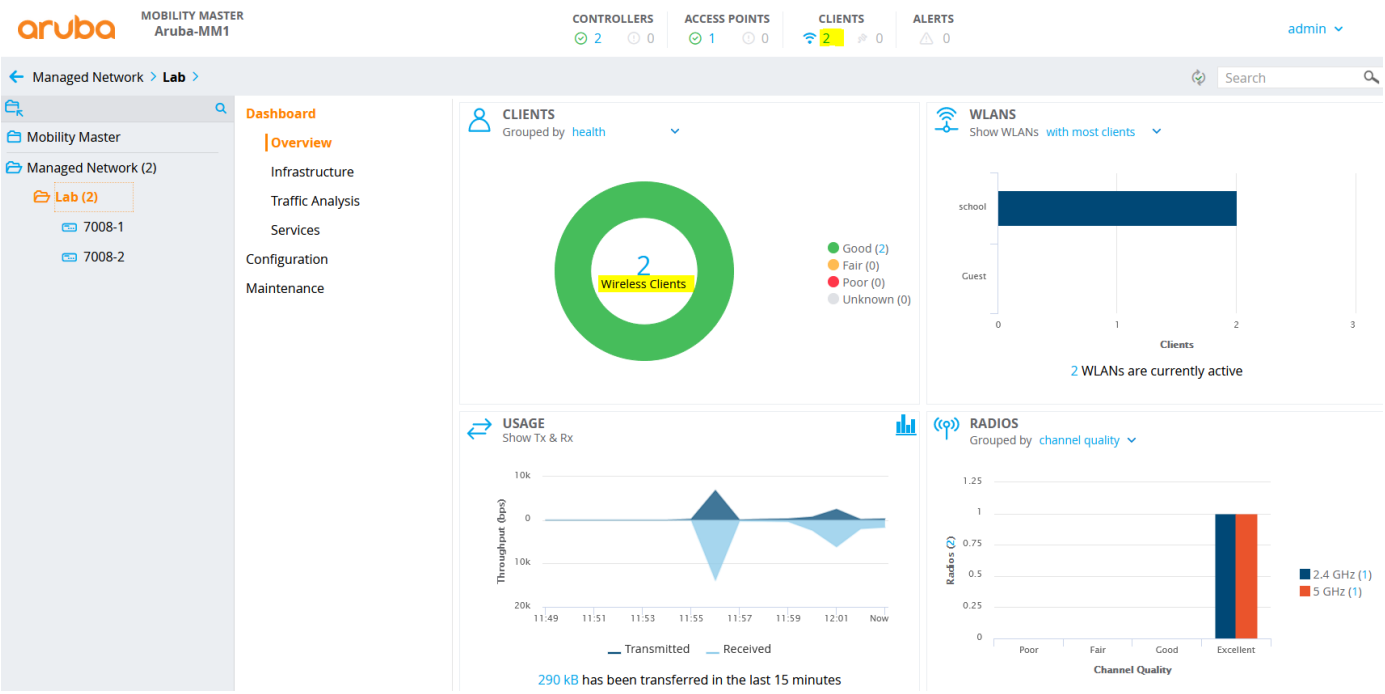
Summary Input Output Accounting

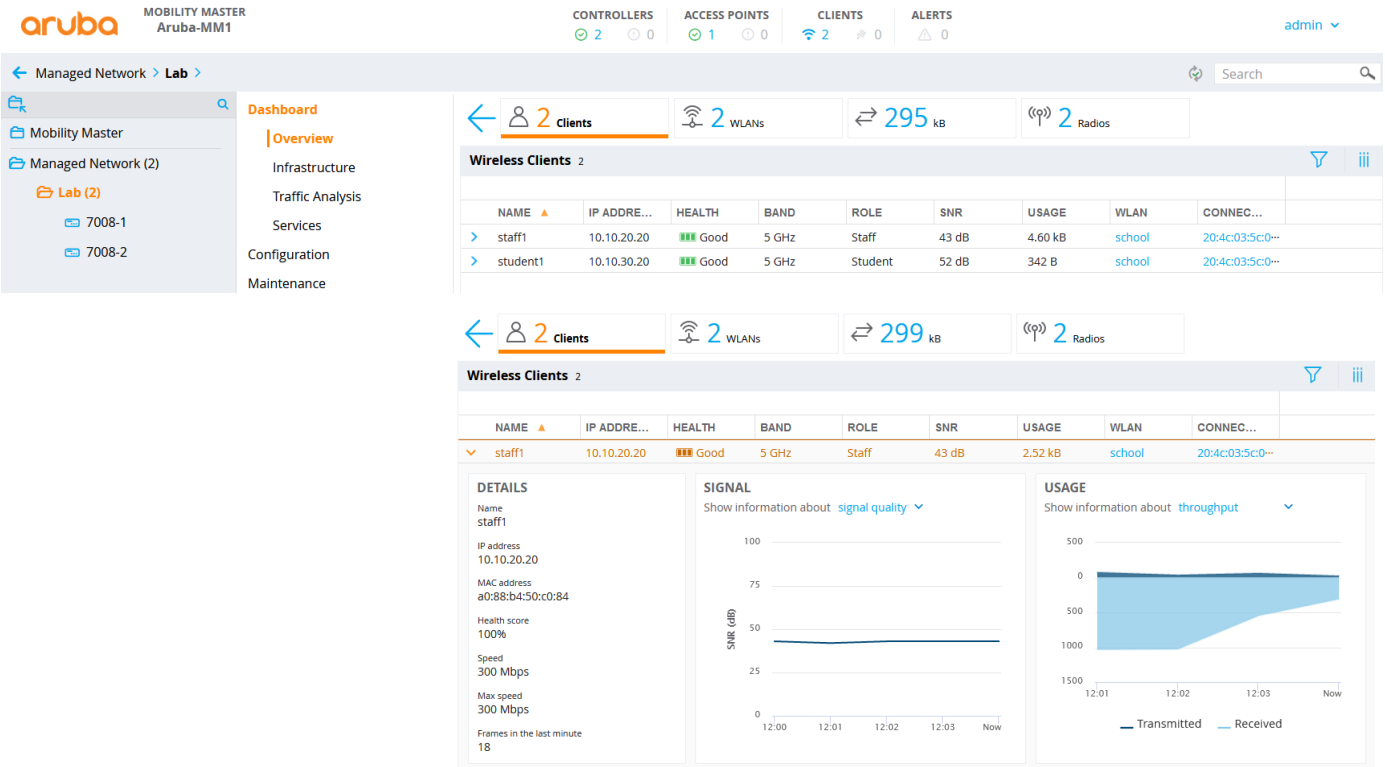
Enforcement Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless Student Profile
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Endpoint:Last Known Location	192.168.1.57:20:4c:03:5c:05:6e
Radius:Aruba:Aruba-User-Role	Student

And here is what we see on the MM dashboard.





Next, check part 2 of this document.