

## Contents

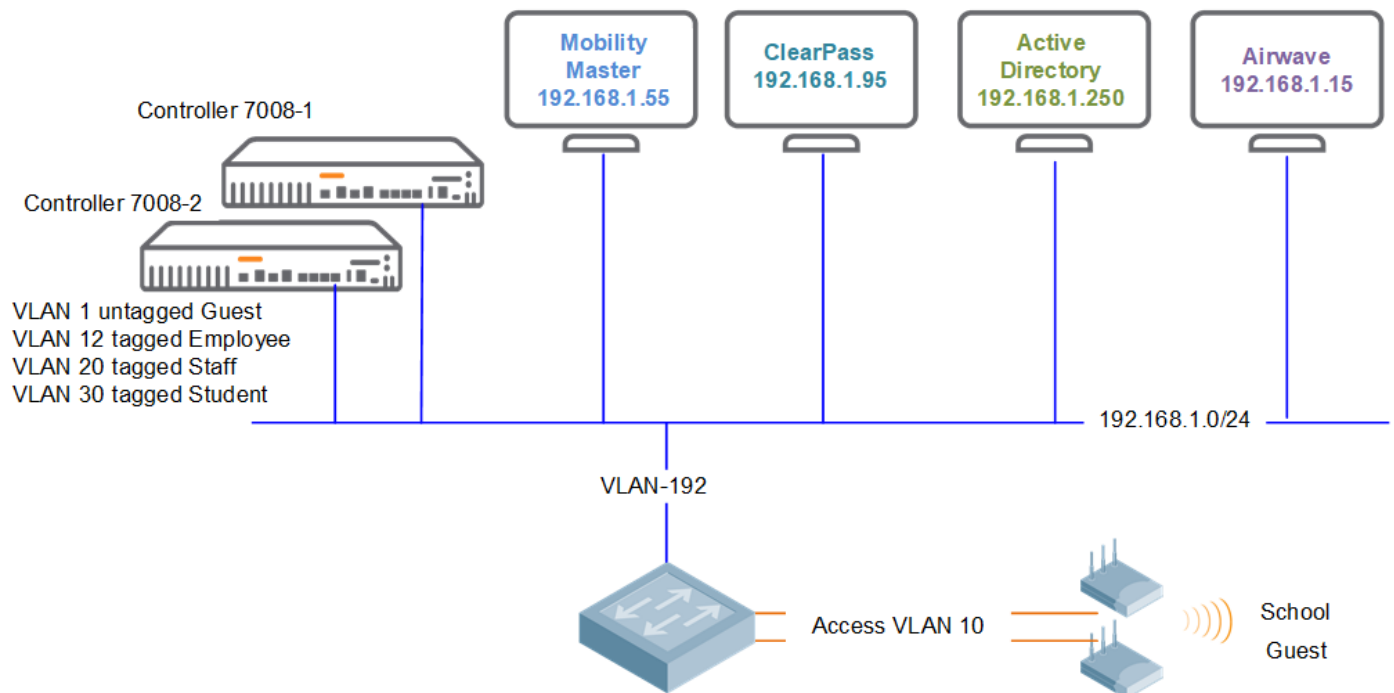
1.1	Revision History .....	1
2	Demo Topology .....	2
3	Setting up the OVA for Mobility Master .....	3
4	Mobility Master Basic Configuration .....	5
5	Controller Configuration .....	11
6	Mobility Master Configuration .....	13
6.1	Dot1x Wireless Configuration .....	15
6.2	ClearPass Basic Configuration .....	23
6.3	Joining AD Domain .....	24
6.4	ClearPass dot1x Service .....	26
6.5	ClearPass Access tracker .....	28

### 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.

The screenshot shows the 'New virtual machine - MM-1' wizard in VMware vSphere. The 'Ready to complete' step is active, showing a summary of the configuration. On the left, a progress bar indicates that step 5, 'Ready to complete', is the current step. The summary table lists the following details:

Property	Value
Product	ArubaOS_MM_8.7.1.1_78245
VM Name	MM-1
Disks	ArubaOS_MM_8.7.1.1_78245-disk1.vmdk, ArubaOS_MM_8.7.1.1_78245-disk2.vmdk
Datastore	datastore1
Provisioning type	Thick
Network mappings	VM Network: VM Network
Guest OS Name	Unknown

Below the table, a yellow warning icon is displayed with the text: 'Do not refresh your browser while this VM is being deployed.' At the bottom right, there are buttons for 'Back', 'Next', 'Finish', and 'Cancel'.

The screenshot shows the 'Edit settings - MM-1 (ESXi 5.0 virtual machine)' window. The 'Virtual Hardware' tab is selected. The settings are as follows:

Device	Configuration
CPU	3
Memory	6144 MB
Hard disk 1	4 GB
Hard disk 2	6 GB
SCSI Controller 0	LSI Logic Parallel
Network Adapter 1	VM Network, <input type="checkbox"/> Connect
Network Adapter 2	VM Network, <input checked="" type="checkbox"/> Connect
Network Adapter 3	VM Network, <input type="checkbox"/> Connect
Floppy drive 1	Use existing floppy image

Just enable the correct VLAN/adaptor 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.

```
Aruba Networks
ArubaOS Version 8.7.1.1 (build 78245 / label #78245)
Built by p4build@hp-hpn-build05 on 2020-12-14 at 20:40:11 UTC (gcc version 4.9.4)
(c) Copyright 2020 Hewlett Packard Enterprise Development LP.

[09:18:08]:Starting device manager [ OK ]

Device Open Failed...Creating New device
<----- Welcome to Aruba Networks - Aruba MM-UA ----->

[09:18:11]:Probing for real-time clock [ OK ]
[09:18:11]:Uncompressing core image files [ OK ]
[09:18:26]:Extracting corefs [ OK ]

[09:18:27]:Waiting for storage device ... [ OK ]
Performing partition fast test... [ DONE ]
Checking for file system... [ OK ]
[09:18:29]:Scanning storage device filesystem [ OK ]
[09:18:34]:Mounting flash [ OK ]
[09:18:34]:Mounting disk1 [ OK ]
[09:18:35]:Mounting disk2 [ OK ]
[09:18:35]:Initializing 256MB as swap on zRam0 [ OK ]
[09:18:37]:Turning swap ON on zRam0 [ OK ]
[09:18:37]:Installing factory image
```

```

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_aimatch_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-UA 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-UA_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

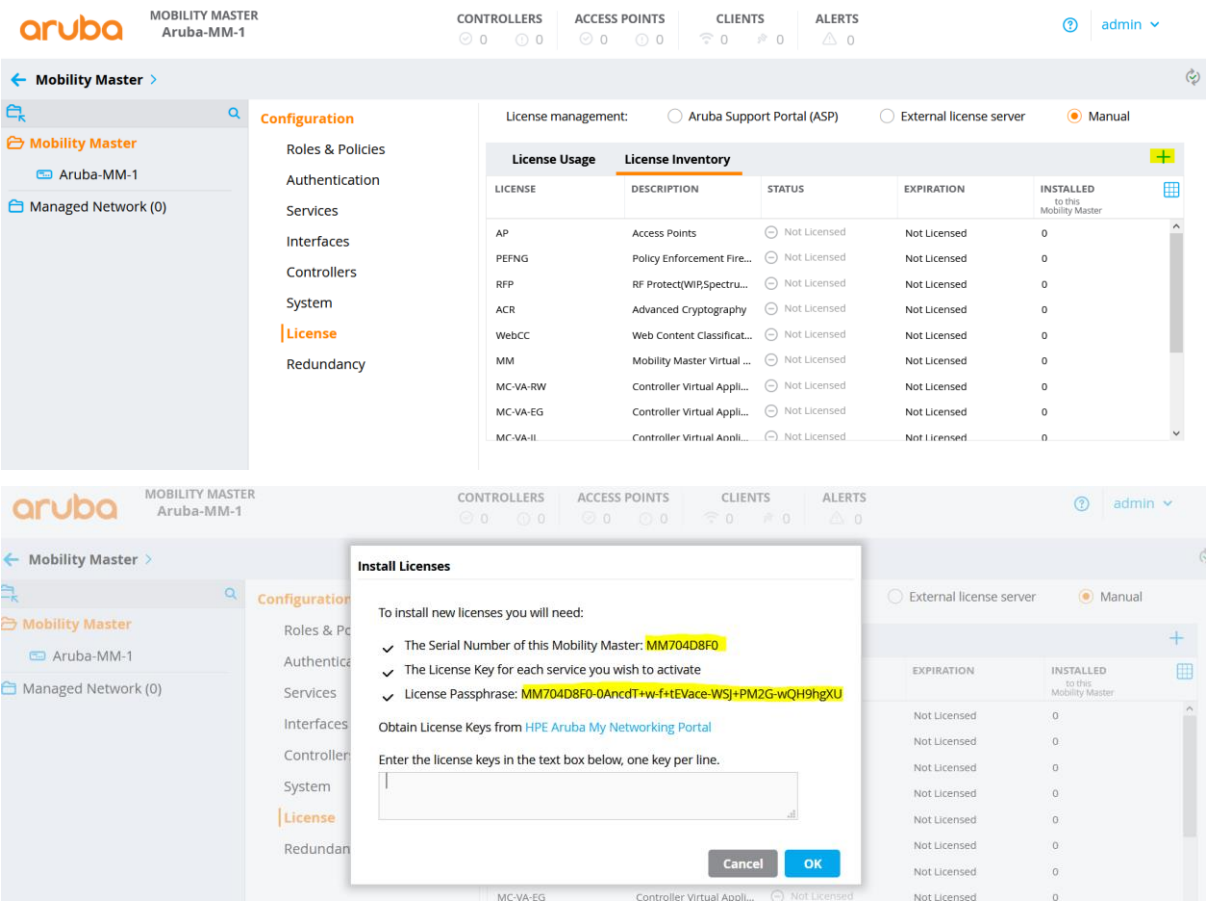
If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no)

```

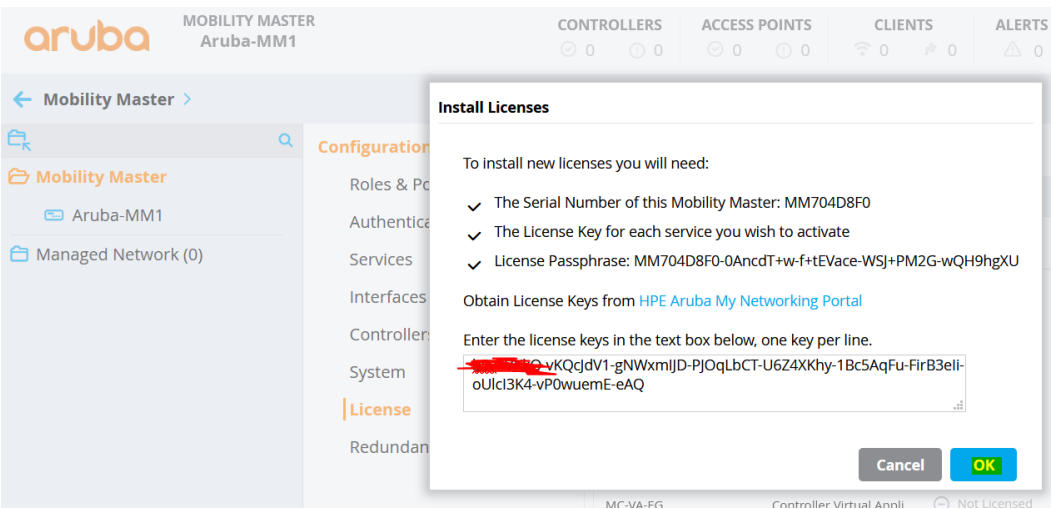
Once you have accepted the changes, MM will reboot and then you can browse to that IP address which you just configured. Once you login with the new credentials, you need to add the licenses. To be able to add the license, you need to get the license passphrase and send it to Aruba in which they can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

# 4 Mobility Master Basic Configuration

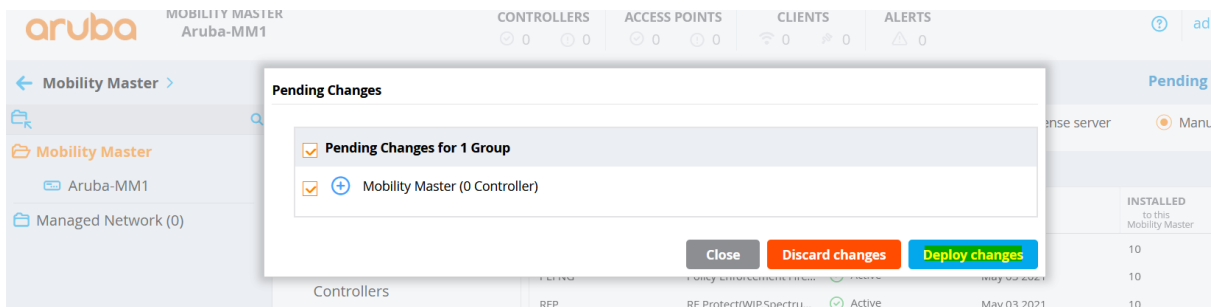
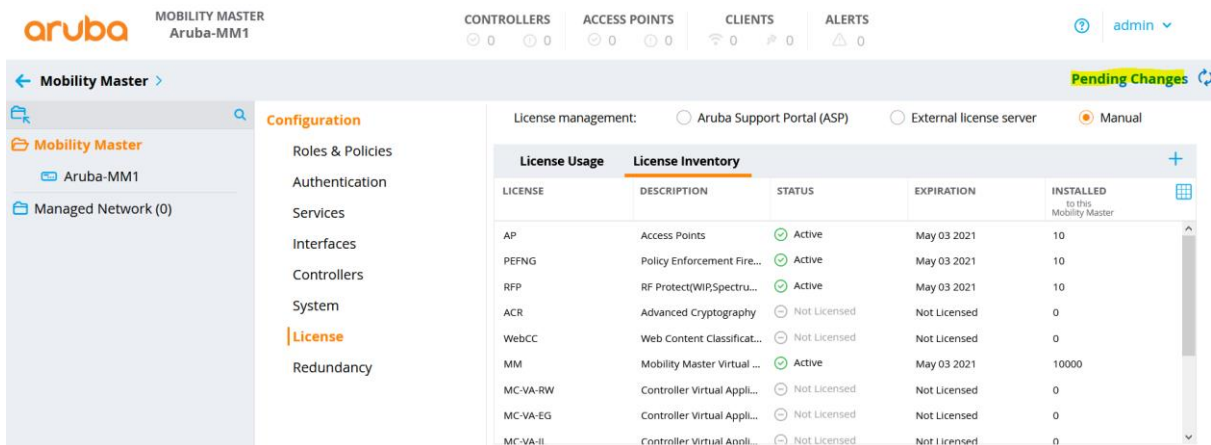
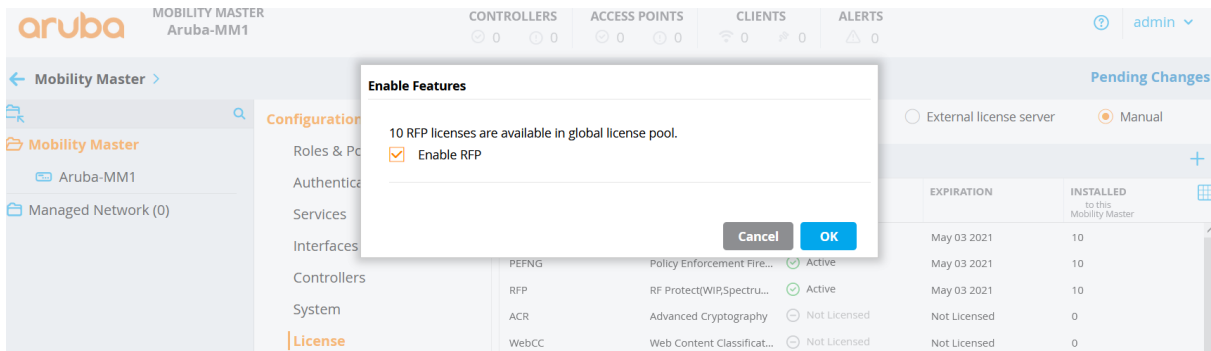
Here we'll cover the basic configuration starting with evaluation licensing.



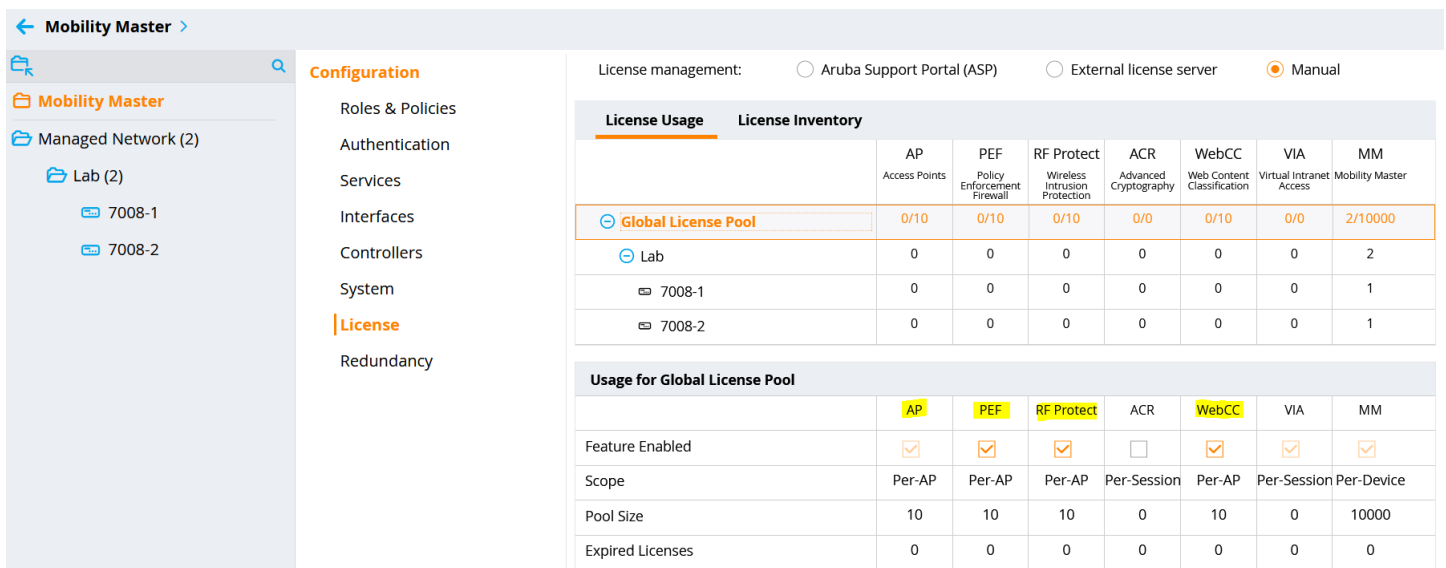
Here is the passphrase which is highlighted. This needs to be sent to your Aruba contact or SE, they should be able to generate and send you the license key to be copy and pasted into the following dialog.



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.

The screenshot shows the Aruba Mobility Master interface. The top navigation bar includes 'CONTROLLERS' (0), 'ACCESS POINTS' (0), 'CLIENTS' (0), and 'ALERTS' (0). The left sidebar shows the 'Configuration' menu with 'Controllers' selected. The main content area displays 'Local Controller IPsec Keys' with a table showing one entry with IP address 0.0.0.0 and a key of \*\*\*\*\*.

IPV4 ADDRESS OF T...	IPV6 ADDRESS OF T...	KEY	MAC ADDRESS OF T...	CERT TYPE
0.0.0.0	--	*****	--	--

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"

The screenshot shows the 'General' configuration page for the 'Lab' folder. The 'Auto-parking' section is expanded, showing 'Auto-parking for controllers' is enabled (toggle switch) and 'Folder for auto-parking' is set to 'Managed Network > Lab'. Other sections like 'Basic Info', 'Domain Name System', and 'Aruba Support Portal (ASP)' are also visible.

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

The screenshot shows the 'NTP Servers' configuration page for the 'Lab' folder. The 'Clock' section is expanded, showing 'Set clock' is set to 'Using NTP' and 'Time zone' is set to 'Australia: Australia/Melbourne (UTC+1...)'. The 'NTP Servers' table shows one entry with IP address 216.239.35.4 and IBURST MODE set to 'Yes'.

IP ADDRESS	IBURST MODE	AUTHENTICATION KEY ID
216.239.35.4	Yes	--

The screenshot shows the 'DNS Servers' configuration page for the 'Lab' folder. The 'Domain Name System' section is expanded, showing 'IP domain lookup' is checked. The 'DNS Servers' table shows one entry with IP version 'IPv4' and IP address '192.168.1.130'.

IP VERSION	IP ADDRESS
IPv4	192.168.1.130

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

aruba MOBILITY MASTER Aruba-MM1

CONTROLLERS 2 ACCESS POINTS 1 CLIENTS 1 ALERTS 0

admin

← Mobility Master >

Configuration

Roles & Policies  
Authentication  
Services  
Interfaces  
Controllers  
System  
License  
Redundancy

General Admin AirWave CPsec Certificates **SNMP** Logging Profiles Whitelist More

Community string for SNMPv1 and SNMPv2

thisisgreat

+

← Mobility Master >

Configuration

Roles & Policies  
Authentication  
Services  
Interfaces  
Controllers  
System  
License  
Redundancy

General Admin AirWave CPsec Certificates **SNMP** Logging Profiles Whitelist More

New community string

Name:

Users for SNMPv3

NAME	AUTHENTICATION PROTOCOL	PRIVACY PROTOCOL
+		

Enable trap generation: ☒

SNMP trap receivers

IP ADDRESS	VERSION	COMMUNITY/USER...	PORT	RETRY	TIMEOUT	INFORM
192.168.1.15	SNMPv2c	thisisgreat	162	-	-	-

And then enabling the AirWave connectivity for MM and MDs

← Mobility Master >

Configuration

Roles & Policies  
Authentication  
Services  
Interfaces  
Controllers  
System  
License  
Redundancy

General Admin **AirWave** CPsec Certificates SNMP Logging Profiles Whitelist More

Connect to AirWave: ☒

Airwave IP address:

SNMP version:

Community string:

← Managed Network > Lab >

Dashboard

Configuration

WLANs  
Roles & Policies  
Access Points  
AP Groups  
Authentication  
Services  
Interfaces  
Controllers  
System  
Tasks  
Redundancy  
IoT  
Maintenance

General Admin **AirWave** CPsec Certificates SNMP Logging Profiles More

Connect to AirWave: ☒

Airwave IP address:

SNMP version:

Community string:

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

← Managed Network > Lab >

Dashboard

Configuration

WLANs  
Roles & Policies  
Access Points  
AP Groups  
Authentication  
Services  
Interfaces  
Controllers  
System  
Tasks  
Redundancy  
IoT  
Maintenance

General Admin AirWave CPsec Certificates SNMP Logging **Profiles** More

Mgmt Config

- default-acp
- default-ale
- default-amp**
- default-controller
- default-niara
- Openflow-profile
- Upgrade
- Valid Equipment OUI
- an.denov-profile

Monitored Info - Add/Update: ☐

Monitored Info - Deletion: ☐

Monitored Info - Periodic Snapshot: ☐

User\_visibility: ☒

Wireless IDS Event Info: ☒

Misc: ☒

Location: ☒

UCC Monitoring: ☒

AirGroup Info: ☐

Inline DHCP stats: ☒

Inline AP stats: ☒

Inline Auth stats: ☒

Inline DNS stats: ☒

WAN State Info: ☐

Inline LLDP stats: ☐

AP stats: ☒

AP application stats: ☒



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

Managed Network > Lab >

Dashboard
Configuration
WLANs
Roles & Policies
Access Points
AP Groups
Authentication
Services
Interfaces

Ports
**VLANs**
IP Routes
GRE Tunnels
Pool Management
OSPF
Multicast

**VLANs**

NAME	ID(S)
staff-VLAN	20
Employee-VLAN	12
Student-VLAN	30
--	1

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

Managed Network > Lab >

Dashboard
Configuration
WLANs
Roles & Policies
Access Points
AP Groups
Authentication
Services
Interfaces
Controllers
System
Tasks
Redundancy
IoT
Maintenance

Ports
**VLANs**
IP Routes
GRE Tunnels
Pool Management
OSPF
Multicast

**Port Channel**

NAME	MEMBERS	PROTOCOL	TRUSTED	POLICY	MODE	NATIVE VLAN	TRUNK VLANs
+							

**Ports**

PORT	ADMIN ST...	TRUSTED	POLICY	MODE	NATIVE VL...	ACCESS VL...	TRUNK VL...	SPANNIN...	MONITOR...	DESCRIPTI...
GE-0/0/0	Enabled	✓	Not-defin...	trunk	1	1	1-4094	✓	--	GE0/0/0
GE-0/0/1	Enabled	✓	Not-defined	access	1	1	1-4094	✓	--	GE0/0/1
GE-0/0/2	Enabled	✓	Not-defined	access	1	1	1-4094	✓	--	GE0/0/2
GE-0/0/3	Enabled	✓	Not-defined	access	1	1	1-4094	✓	--	GE0/0/3
GE-0/0/4	Enabled	✓	Not-defined	access	1	1	1-4094	✓	--	GE0/0/4

Managed Network > Lab >

Dashboard
Configuration
WLANs
Roles & Policies
Access Points
AP Groups
Authentication
Services
Interfaces
Controllers
System
Tasks
Redundancy
IoT
Maintenance

Ports
**VLANs**
IP Routes
GRE Tunnels
Pool Management
OSPF
Multicast

**GE-0/0/0**

Admin state: ☒
Speed:  Mbps
Duplex: 
PoE: ☐
Trust: ☒
Policy: 
Mode: 
Native VLAN: 
Allowed VLANs: 
Description:

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.

MOBILITY MASTER  
Aruba-MM1

CONTROLLERS

2

ACCESS POINTS

0

CLIENTS

0

ALERTS

0

admin

Managed Network > Lab >

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

Controllers

System

Clusters

AirGroup

VPN

Firewall

IP Mobility

External Services

DHCP

WAN

Rate limit CP IKE traffic (pps):

Jumbo frames processing:

Mark management frames:

Enable firewall visibility:

☒

Enable deep packet inspection:

☒

Enable web content classification:

☒

Connect to classification server using:

IPv4

Drop packets during web content cache miss:

☐

URL to redirect blocked sessions:

Enable IP classification and reputation:

☒

Pending Changes

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

Controllers

System

Tasks

Clusters

AirGroup

VPN

Firewall

IP Mobility

External Services

DHCP

WAN

Rate limit CP IKE traffic (pps):

Jumbo frames processing:

☐

Mark management frames:

☐

Enable firewall visibility:

☒

Enable deep packet inspection:

☒

Enable web content classification:

☒

Connect to classification server using:

IPv4

Drop packets during web content cache miss:

☐

URL to redirect blocked sessions:

Enable IP classification and reputation:

☒

For this we need to reload the MDs if 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.
```

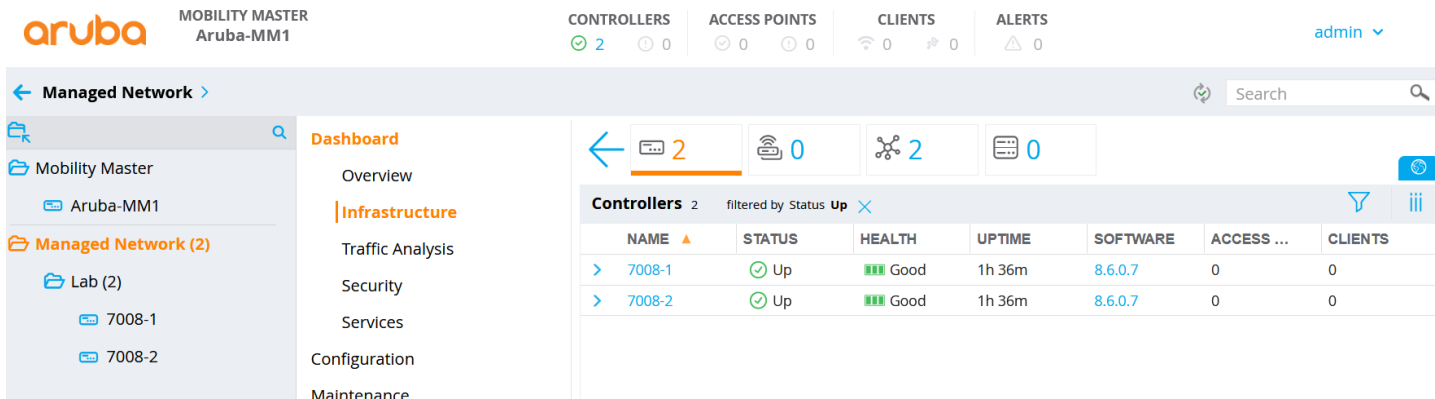
System will now restart!

```
[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

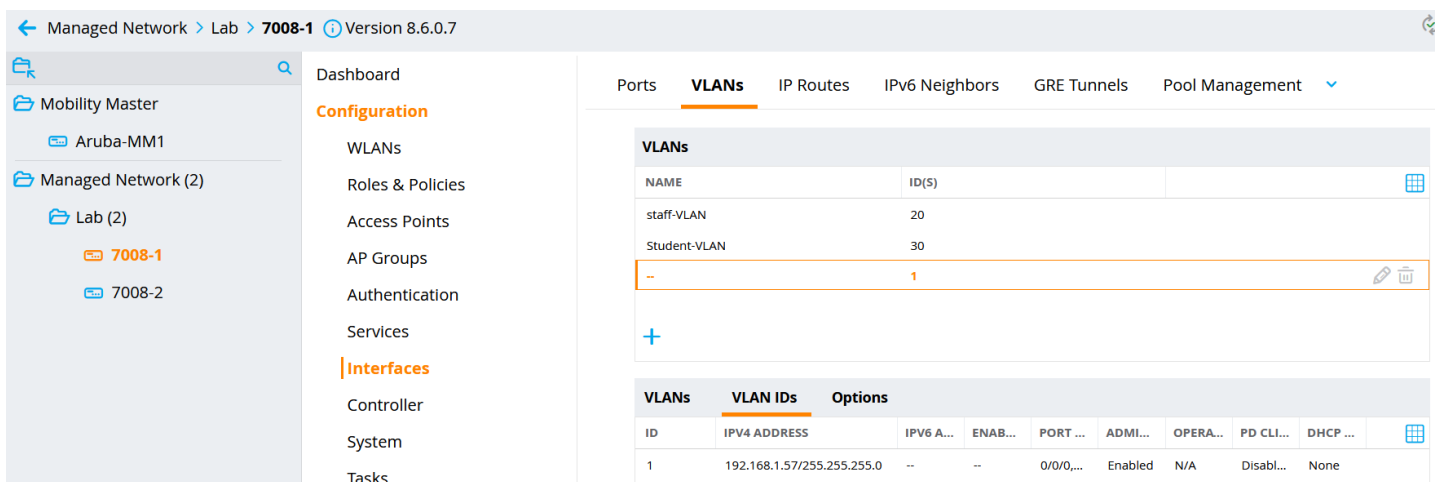
Here we have done the previous process for two MDs and they have end up on the MM dashboard and have now got the basic configuration tat we did earlier for the “Lab” folder.



The screenshot shows the Aruba Mobility Master dashboard. At the top, there's a navigation bar with the Aruba logo, 'MOBILITY MASTER Aruba-MM1', and status indicators for CONTROLLERS (2), ACCESS POINTS (0), CLIENTS (0), and ALERTS (0). The user 'admin' is logged in. The left sidebar shows a tree view: Managed Network > Mobility Master > Aruba-MM1 > Managed Network (2) > Lab (2) > 7008-1 and 7008-2. The main content area has a 'Dashboard' tab selected, showing a summary of the network. Below the summary, there's a table for 'Controllers' with 2 entries, filtered by Status 'Up'. The table has columns: NAME, STATUS, HEALTH, UPTIME, SOFTWARE, ACCESS..., and CLIENTS.

NAME	STATUS	HEALTH	UPTIME	SOFTWARE	ACCESS...	CLIENTS
7008-1	Up	Good	1h 36m	8.6.0.7	0	0
7008-2	Up	Good	1h 36m	8.6.0.7	0	0

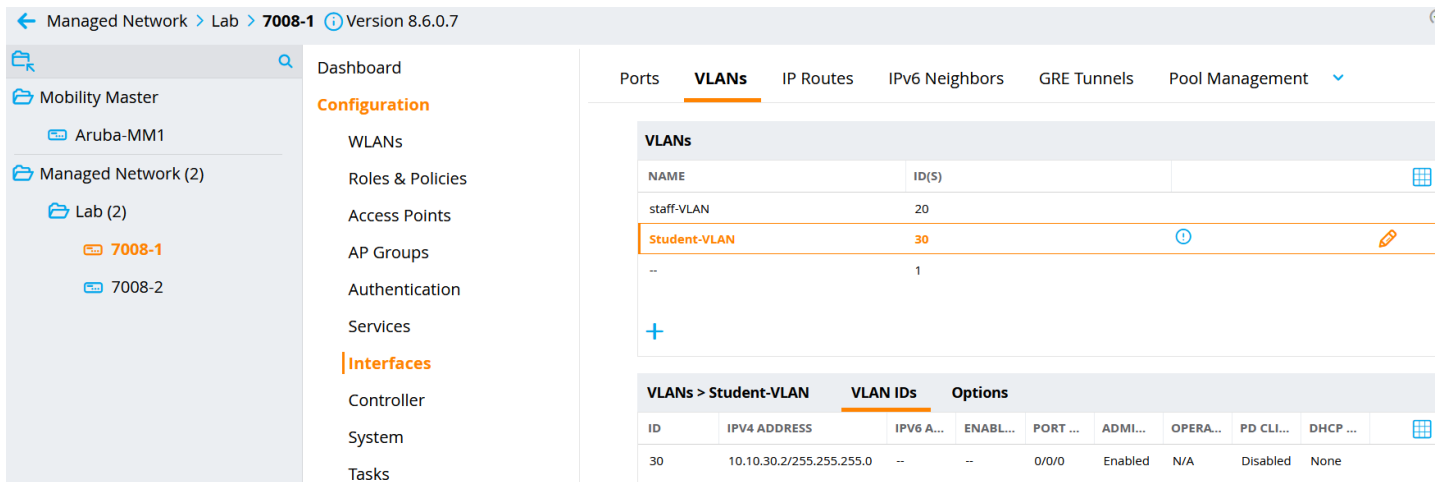
Now from the MM’s device view, we’ll configure the IP addresses for VLAN1, 12, 20 and 30. The aim of hierarchical configuration through folder is that most of the configuration will be done at the folder level and device specific configuration to be done at the device level.



The screenshot shows the 'VLANs' configuration page in the Aruba Mobility Master. The breadcrumb trail is: Managed Network > Lab > 7008-1 > Version 8.6.0.7. The left sidebar shows the configuration tree: Dashboard > Configuration > VLANs. The main content area has tabs for Ports, VLANs, IP Routes, IPv6 Neighbors, GRE Tunnels, and Pool Management. The 'VLANs' tab is active, showing a table with columns: NAME, ID(S), and a grid icon. The table has three rows: staff-VLAN (ID 20), Student-VLAN (ID 30), and a new row with ID 1. Below the table, there's a '+' button to add a new VLAN. At the bottom, there's a table for 'VLANs > Student-VLAN' with columns: ID, IPV4 ADDRESS, IPV6 A..., ENABL..., PORT..., ADML..., OPERA..., PD CLI..., and DHCP... The table has one row for ID 30 with IPV4 ADDRESS 10.10.30.2/255.255.255.0.

NAME	ID(S)
staff-VLAN	20
Student-VLAN	30
--	1

ID	IPV4 ADDRESS	IPV6 A...	ENABL...	PORT...	ADML...	OPERA...	PD CLI...	DHCP...
1	192.168.1.57/255.255.255.0	--	--	0/0/0,...	Enabled	N/A	Disabl...	None



The screenshot shows the 'VLANs' configuration page in the Aruba Mobility Master, similar to the previous one. The breadcrumb trail is: Managed Network > Lab > 7008-1 > Version 8.6.0.7. The left sidebar shows the configuration tree: Dashboard > Configuration > VLANs. The main content area has tabs for Ports, VLANs, IP Routes, IPv6 Neighbors, GRE Tunnels, and Pool Management. The 'VLANs' tab is active, showing a table with columns: NAME, ID(S), and a grid icon. The table has three rows: staff-VLAN (ID 20), Student-VLAN (ID 30), and a new row with ID 1. Below the table, there's a '+' button to add a new VLAN. At the bottom, there's a table for 'VLANs > Student-VLAN' with columns: ID, IPV4 ADDRESS, IPV6 A..., ENABL..., PORT..., ADML..., OPERA..., PD CLI..., and DHCP... The table has one row for ID 30 with IPV4 ADDRESS 10.10.30.2/255.255.255.0.

NAME	ID(S)
staff-VLAN	20
Student-VLAN	30
--	1

ID	IPV4 ADDRESS	IPV6 A...	ENABL...	PORT...	ADML...	OPERA...	PD CLI...	DHCP...
30	10.10.30.2/255.255.255.0	--	--	0/0/0	Enabled	N/A	Disabled	None

Managed Network > Lab > 7008-1 Version 8.6.0.7

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

Controller

System

Tasks

Ports VLANs IP Routes IPv6 Neighbors GRE Tunnels Pool Management

VLANs

NAME	ID(S)
staff-VLAN	20
Student-VLAN	30
--	1

VLANs > staff-VLAN

ID	IPV4 ADDRESS	IPV6 A...	ENABL...	PORT ...	ADMI...	OPERA...	PD CLI...	DHCP ...
20	10.10.20.2/255.255.255.0	--	--	0/0/0	Enabled	N/A	Disabled	None

Managed Network > Lab > 7008-1 Version 8.6.0.7

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

Controller

System

Tasks

Ports VLANs IP Routes IPv6 Neighbors GRE Tunnels Pool Management

VLANs

NAME	ID(S)
staff-VLAN	20
Student-VLAN	30
Employee-VLAN	12
--	1

VLANs > Employee-VLAN

ID	IPV4 ADDRESS	IPV6 A...	ENABL...	PORT ...	ADMI...	OPERA...	PD CLI...	DHCP ...
12	10.10.12.2/255.255.255.0	--	--	0/0/0	Enabled	N/A	Disabled	None

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.

Managed Network > Lab >

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

AP Groups 4

NAME	APs
default	--
NoAuthApGroup	--
Building1	--
Building2	--

Also enable auto certificate provisioning of the APs.

MOBILITY MASTER  
Aruba-MM1

CONTROLLERS

2
 0

ACCESS POINTS

0
 1

CLIENTS

0
 0

ALERTS

0

Managed Network > Lab >

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

Controllers

System

General

Admin

AirWave

CPSec

Certificates

SNMP

Logging

Profiles

More

Control Plane Security

Enable CPSec:

☒

Enable auto cert provisioning:

☒

Only accept APs from specified ranges:

☐

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.

Mobility Master >

Mobility Master

Aruba-MM1

Managed Network (2)

Lab (2)

Configuration

Roles & Policies

Authentication

Services

Interfaces

Controllers

System

License

Redundancy

Clusters

VPN

Firewall

Guest Provisioning

AirMatch

IoT

Rate limit CP trusted mcast traffic (pps):

1953

Rate limit CP route traffic (pps):

976

Rate limit CP session mirror traffic (pps):

976

Rate limit CP VRRP traffic (pps):

512

Rate limit CP ARP traffic (pps):

976

Rate limit CP I2 protocol/other traffic (pps):

976

Rate limit CP auth process traffic (pps):

976

Rate limit CP IKE traffic (pps):

1953

Jumbo frames processing:

☐

Mark management frames:

☐

Enable deep packet inspection:

☐

Enable web content classification:

☒

Connect to classification server using:

IPv4

Drop packets during web content cache miss:

☐

URL to redirect blocked sessions:

Enable IP classification and reputation:

☒

## 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

16 | Page



## 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

## 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

Auth servers: ClearPass

Reauth interval: 1440 min.

Machine authentication: Disabled

Blacklisting: ☐

Dashboard
Configuration
WLANs
Roles & Policies
Access Points
AP Groups
Authentication
Services
Interfaces
Controllers

## New WLAN

General
VLANs
Security
Access

Default role: guest

Server-derived roles: ☒

Derivation method:
☒ Use value returned from clearPass or other auth server
☐ Use rules defined in table below

Show [roles](#)

Managed Network > Lab >
Pending Changes

Dashboard
Configuration
WLANs
Roles & Policies

## New WLAN

The new WLAN can be viewed in the **WLAN List**

NOTE: The new WLAN has been added to the pending changes list. To deploy all pending changes, click Pending Changes at top right.

Managed Network > Lab >

Dashboard
Configuration
WLANs
Roles & Policies
Access Points
AP Groups
Authentication
Services
Interfaces

## Tasks

- Deploy New
- Create a new
- Define Wirele
- Bulk configur
- Install new se
- Reboot contr
- Show upgrad

### Configuration Deployment Status

#### Update for 2 Managed Controller(s)

TARGET	NODEPATH	STATUS	MESSAGE
7008-2	Managed Network ...	✓	
7008-1	Managed Network ...	✓	

Close

Make sure to submit and apply changes.

Managed Network > Lab >

Dashboard
Configuration
WLANs
Roles & Policies
Access Points
AP Groups
Authentication
Services
Interfaces
Controllers
System

### AP Groups 4

NAME	APs
default	1
NoAuthApGroup	--
Building1	--
Building2	--

+

#### AP Groups > Building1

NAME	AP GROUP	AIRTIME LIMIT (%)	PER-USER LIMIT (KBPS)	PER-RADIO LIMIT (KBPS)
school	Building1	--	--	--

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.

aruba
MOBILITY MASTER
Aruba-MM1
CONTROLLERS 2 ACCESS POINTS 1 CLIENTS 0 ALERTS 0
admin

Managed Network >

Dashboard
Infrastructure
Traffic Analysis
Security
Services

← 2 Controllers
1 Access Device
2 Uplinks
0 Clusters

### Access Points 1

filtered by Status Up

NAME	STATUS	CLIENTS	UPTIME	MANAGED BY	GROUP	MODEL
20:4c03:5c05:6e	Up	0	1h 9m	7008-1	default	303H

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

Managed Network > Lab > 7008-1 Version 8.6.0.7

Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces
- Controller
- System
- Tasks
- Redundancy

Campus APs Remote APs Mesh APs Whitelist Provisioning Rules

Campus APs 1

<input type="checkbox"/>	AP NAME	AP GROUP	IPv4 ADDRESS	IPv6 ADDRESS	SWITCH IP	MAC ADDRESS	SERIAL #	TYPE	FLAGS
<input checked="" type="checkbox"/>	20:4c:03:5c:05:6e	default	10.10.10.20	--	192.168.1.57	20:4c:03:5c:05:6e	CNHVK2R42H	303H	2

Provision

50 < 1 >

Flags:

U = Unprovisioned, N = Duplicate name, G = No such group, L = Unlicensed, I = Inactive, D = Dirty or no config, E = Regulatory Domain Mismatch, X = Maintenance Mode, P = PPPoE AP, B = Built-in AP, S = LACP stripping, R = Remote AP, R- = Remote AP requires Auth, C = Cellular RAP, c = CERT-based RAP, 1 = 802.1x authenticated AP use EAP-PEAP, 1+ = 802.1x use EST, 1- = 802.1x use factory cert, 2 = Using IKE version 2, u = Custom-Cert RAP, S = Standby-mode AP, J = USB cert at AP, f = No Spectrum FFT support, I = Indoor, O = Outdoor, M = Mesh node, Y = Mesh Recovery, z = Datazone AP, e = Custom EST cert, p = In deep-sleep status, 4 = Using WiFi uplink, r = Power Restricted, T = Thermal ShutDown, F = AP failed 802.1x authentication

Managed Network > Lab > 7008-1 Version 8.6.0.7

Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces
- Controller
- System
- Tasks
- Redundancy
- Maintenance

Campus APs Remote APs Mesh APs Whitelist Provisioning Rules

Provision

50 < 1 >

20:4c:03:5c:05:6e

MAC address: 20:4c:03:5c:05:6e

Name: 20:4c:03:5c:05:6e

AP group: Building1

Controller discovery: ☒ Use AP discovery protocol (ADP) ☐ Static

Controller discovery preference: ☒ IPv4 ☐ IPv6

IP: ☒ DHCP ☐ Static

Deployment: ☒ Campus ☐ Remote ☐ Mesh ☐ Remote mesh portal

Wi-Fi uplink: ☐

Managed Network > Lab > 7008-1 Version 8.6.0.7

Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces
- Controller
- System
- Tasks
- Redundancy
- Maintenance

Campus APs Remote APs Mesh APs Whitelist Provisioning Rules

Provision

50 < 1 >

20:4c:03:5c:05:6e

MAC address: 20:4c:03:5c:05:6e

Name: 20:4c:03:5c:05:6e

AP group: Building1

Controller discovery: ☒ Use AP discovery protocol (ADP) ☐ Static

Controller discovery preference: ☒ IPv4 ☐ IPv6

IP: ☒ DHCP ☐ Static

Deployment: ☒ Campus ☐ Remote ☐ Mesh ☐ Remote mesh portal

Wi-Fi uplink: ☐

Show advanced options

Cancel Submit

**Access Points will be Rebooted**

CAUTION: Applying this configuration change will interrupt service while the affected Access Points are rebooted.

Do you want to continue?

Cancel Continue & Reboot

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

Managed Network > Lab >

Dashboard
Configuration
WLANs
**Roles & Policies**
Access Points
AP Groups
Authentication
Services
Interfaces
Controllers
System

**Roles** Policies Applications Aliases

**Roles** 14

NAME	RULES
logon	32 Rules
guest	11 Rules
ap-role	35 Rules
stateful-dot1x	0 Rules
guest-logon	27 Rules
sys-ap-role	24 Rules
sys-switch-role	24 Rules

Managed Network > Lab >

Dashboard
Configuration
WLANs
**Roles & Policies**
Access Points

**Roles** Policies

**Roles** 16

NAME	RULES
denyall	1 Rules

New Role
Name: Staff
Cancel Submit

Managed Network > Lab >

Dashboard
Configuration
WLANs
**Roles & Policies**
Access Points
AP Groups
Authentication
Services
Interfaces
Controllers
System

**Roles** Policies Applications Aliases

**Roles** 16

NAME	RULES
denyall	1 Rules
default-via-role	3 Rules
default-vpn-role	4 Rules
authenticated	4 Rules
voice	43 Rules
Staff	0 Rules
Student	0 Rules

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

Managed Network > Lab >

Dashboard
Configuration
WLANs
**Roles & Policies**
Access Points
AP Groups
Authentication
Services
Interfaces
Controllers
System
Tasks
Redundancy

**Roles** Policies

**Roles** 16

NAME	RULES
denyall	1 Rules
default-via-role	3 Rules
default-vpn-role	4 Rules
authenticated	4 Rules
voice	43 Rules
Staff	0 Rules
Student	0 Rules

New Policy
Add an existing policy Create a new policy
Policy type: Session
Policy name: allowall
Position:
Cancel Submit

Staff	Policies	Bandwidth	Captive Portal	More
NAME	RULES COUNT	TYPE	POLICY USAGE	
global-sacl	0	session	logon, guest, ap-role, stateful-dot...	
apprf-staff-sacl	0	session	Staff	
Staff	0	session	Staff	

Show Basic View

Managed Network > Lab > Pending Changes

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

Controllers

System

Tasks

Redundancy

IoT

**Roles** Policies Applications Aliases

Role	Rules
default-via-role	3 Rules
default-vpn-role	4 Rules
authenticated	4 Rules
voice	43 Rules
Staff	2 Rules
Student	2 Rules

**Student** Policies Bandwidth Captive Portal More Show Basic View

NAME	RULES COUNT	TYPE	POLICY USAGE
global-sacl	0	session	login, guest, ap-role, stateful-dot...
apprf-student-sacl	0	session	Student
Student	0	session	Student
allowall	2	session	default-iap-user-role, default-via...

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

Managed Network > Lab >

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

Controllers

System

Tasks

Redundancy

IoT

Maintenance

**Roles** Policies Applications Aliases

Staff 2 Rules

Student 2 Rules

**Staff** Policies Bandwidth Captive Portal More Show Basic View

**Network**

VLAN: staff-VLAN

Re-auth interval: 0 minutes

Max sessions: 65535

Deep packet inspection: ☒

Web content classification: ☒

Youtube education: ☐

Cancel Submit

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

Managed Network > Lab >

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

Controllers

System

Tasks

Redundancy

**Auth Servers**

Server Group

NAME

default

internal

school\_dot1\_svg 1 -- --

**New Server**

Type: Dynamic Authorization

IP address version: ☒ IPv4 ☐ IPv6

IP address: 192.168.1.95

Cancel Submit

**All Servers 2**

NAME	TYPE	IP ADDRESS / HOSTNAME	SERVER GROUP
ClearPass	RADIUS	192.168.1.95	school_dot1_svg
Internal	--	--	default internal

Managed Network > Lab > Pending Changes

Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces
- Controllers
- System
- Tasks
- Redundancy
- IoT

Maintenance

Auth Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

All Servers 3

NAME	TYPE	IP ADDRESS / HOSTNAME	SERVER GROUP
ClearPass	RADIUS	192.168.1.95	school_dot1_svg
Internal	--	--	default internal
--	RFC 3576	192.168.1.95	--

Server Options

Key: .....

Retype key: .....

Cancel Submit

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

Managed Network > Lab >

Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces
- Controllers
- System
- Tasks
- Redundancy
- IoT

Maintenance

Auth Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

AAA Profiles

- default-dot1x-psk
- default-iap-aaa-prof...
- default-mac-auth
- default-open
- default-tunneled-use...
- default-xml-api
- school\_aaa\_prof
- 802.1X Authentication
- 802.1X Authentication Server Group
- MAC Authentication
- MAC Authentication Server Group

RFC 3576 Server

RFC 3576 SERVER

192.168.1.95

RFC 3576 server:

+

Cancel Submit

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

Managed Network > Lab >

Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces
- Controllers
- System
- Tasks
- Redundancy
- IoT

Maintenance

Auth Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

AAA Profiles

- default-dot1x-psk
- default-iap-aaa-prof...
- default-mac-auth
- default-open
- default-tunneled-use...
- default-xml-api
- school\_aaa\_prof
- 802.1X Authentication
- 802.1X Authentication Server Group
- MAC Authentication
- MAC Authentication Server Group
- RADIUS Accounting Server Group
- RFC 3576 server
- XML API server

Server Group: school\_dot1\_svg

Server Group: school\_dot1\_svg

Fail Through: ☐

Load Balance: ☐

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.

The screenshot shows the Cisco Mobility Master configuration interface. The left sidebar displays the navigation menu with 'Managed Network' selected. The main panel is titled 'Auth Servers' and shows the configuration for the 'school\_dot1\_svg' server group. The 'Servers' tab is active, showing a table of servers. The 'ClearPass' server is highlighted, and its configuration is shown in the 'Server Options' section.

NAME	SERVICES	FAIL THROUGH	LOAD BALANCE	SERVER RULES
default	1	--	--	1
internal	1	--	--	1
school_dot1_svg	1	--	--	1

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

**Server Group > school\_dot1\_svg > ClearPass**

**Server Options**

Name: ClearPass

IP address / hostname: 192.168.1.95

Auth port: 1812

Acct port: 1813

Shared key: \*\*\*\*\*

Retype key: \*\*\*\*\*

Timeout: 5

Retransmits: 3

NAS ID:

NAS IP: 192.168.1.57

Enable IPv6: ☐

NAS IPv6:

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.

The screenshot shows the Cisco Mobility Master configuration interface. The left sidebar displays the navigation menu with 'Administration' selected. The main panel is titled 'Server Configuration' and shows the configuration for the 'victory' server. The 'Publisher Server' section is active, showing the configuration for the 'victory' server.

**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

Buttons: Collect Logs, Back Up, Restore, Cleanup, Shutdown, Reboot

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

**Change Date and Time**

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

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

☒ Synchronize time with NTP server

**Primary Server:**

NTP Server	216.239.35.4
Key ID	
Key Value	
Algorithm	

**Secondary Server (1):**

NTP Server	
Key ID	
Key Value	
Algorithm	

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

**Save** **Cancel**

**Change Date and Time**

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

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

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

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

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

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

**Save** **Cancel**

Then enabling Insight which is the reporting module of ClearPass

Administration » Server Manager » Server Configuration - victory

**Server Configuration - victory (192.168.1.95)**

**System** **Services Control** **Service Parameters** **System Monitoring** **Network** **FIPS**

Hostname: victory

FQDN: victory.clearpass.info

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

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

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

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

Master Server in Zone: Primary master

Span Port: -- None --

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

AD Domains: [Join AD Domain](#)

## 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.



System Services Control Service Parameters System Monitoring Network FIPS

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

**Join AD Domain**

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

Domain Controller: wlan-dc.wlan.net

NetBIOS Name: WLAN

In case of a controller name conflict

☒ Use specified Domain Controller

☐ Use Domain Controller returned by DNS query

☐ Fail on conflict

☒ Use default domain admin user [Administrator]

Username:

Password:

Save Cancel

**AD Domains:** Policy Manager is not part of any domain. Join to domain here. [Join AD Domain](#)

**Join AD Domain**

**Adding host to AD domain**

Adding host to AD domain...

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

INFO - Fetched the NETBIOS name 'WLAN'

INFO - Creating domain directories for 'WLAN'

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

Enter Administrator's password:

Using short domain name -- WLAN

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

INFO - Creating service scripts for 'WLAN'

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

Close

**Join AD Domain**

**Added host to the domain**

INFO - Creating service scripts for 'WLAN'

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

INFO - updating domain configuration files

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

[ OK ]

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

Stopping cpass-sysmon-server: [ OK ]

Starting cpass-sysmon-server: [ OK ]

Stopping cpass-radius-server: [ OK ]

Starting cpass-radius-server: [ OK ]

INFO - CP63Lab joined the domain WLAN.NET

Close

Now we need to add the AD as authentication source.

Dashboard Monitoring Configuration

Service Templates & Wizards Services Authentication Methods Sources Identity Single Sign-On (SSO) Local Users Endpoints Static Host Lists Roles Role Mappings Posture Enforcement Network Network Scan Policy Simulation

Configuration » Authentication » Sources » Add - Ariya AD

**Authentication Sources - Ariya AD**

Summary General Primary Attributes

Name: Ariya AD

Description:

Type: Active Directory

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

Authorization Sources:

-- Select --

Server Timeout: 10 seconds

Cache Timeout: 36000 seconds

Backup Servers Priority:

Add Backup Move Up ↑ Move Down ↓ Remove

Dashboard

Monitoring

Configuration

Service Templates & Wizards
Services
Authentication
Methods
Sources
Identity
Single Sign-On (SSO)
Local Users
Endpoints
Static Host Lists
Roles
Role Mappings
Posture
Enforcement
Network
Network Scan
Policy Simulation

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

Dashboard

Monitoring

Configuration

Service Templates & Wizards
Services
Authentication
Methods
Sources
Identity
Single Sign-On (SSO)
Local Users
Endpoints
Static Host Lists
Roles
Role Mappings
Posture
Enforcement
Network
Network Scan
Policy Simulation

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.

aruba

ClearPass Policy Manager

Menu

Dashboard

Monitoring

Configuration

Service Templates & Wizards
Services
Authentication
Methods
Sources
Identity
Single Sign-On (SSO)
Local Users
Endpoints
Static Host Lists
Roles
Role Mappings
Posture

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:				
<input type="checkbox"/> 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:				
<input type="checkbox"/> 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 Student)		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.

Dashboard

Monitoring

Configuration

Administration

ClearPass Portal

Users and Privileges

Server Manager

Server Configuration

Log Configuration

Local Shared Folders

Licensing

Monitoring > Live Monitoring > Access Tracker

Access Tracker Feb 06, 2021 11:54:19 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 Go Clear Filter

Show 20 records

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.95	RADIUS	staff1	AA Aruba 802.1X Wireless	ACCEPT	2021/02/06 11:54:09

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

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

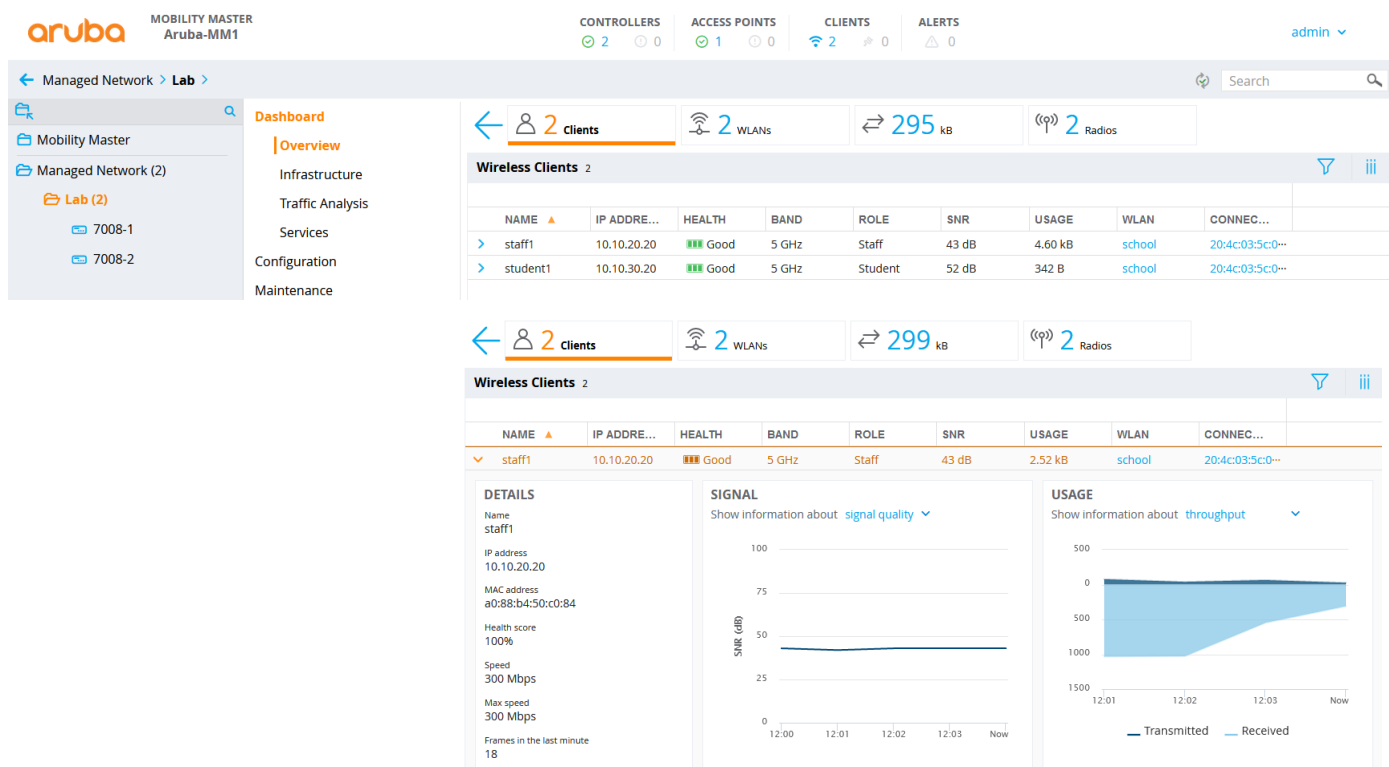
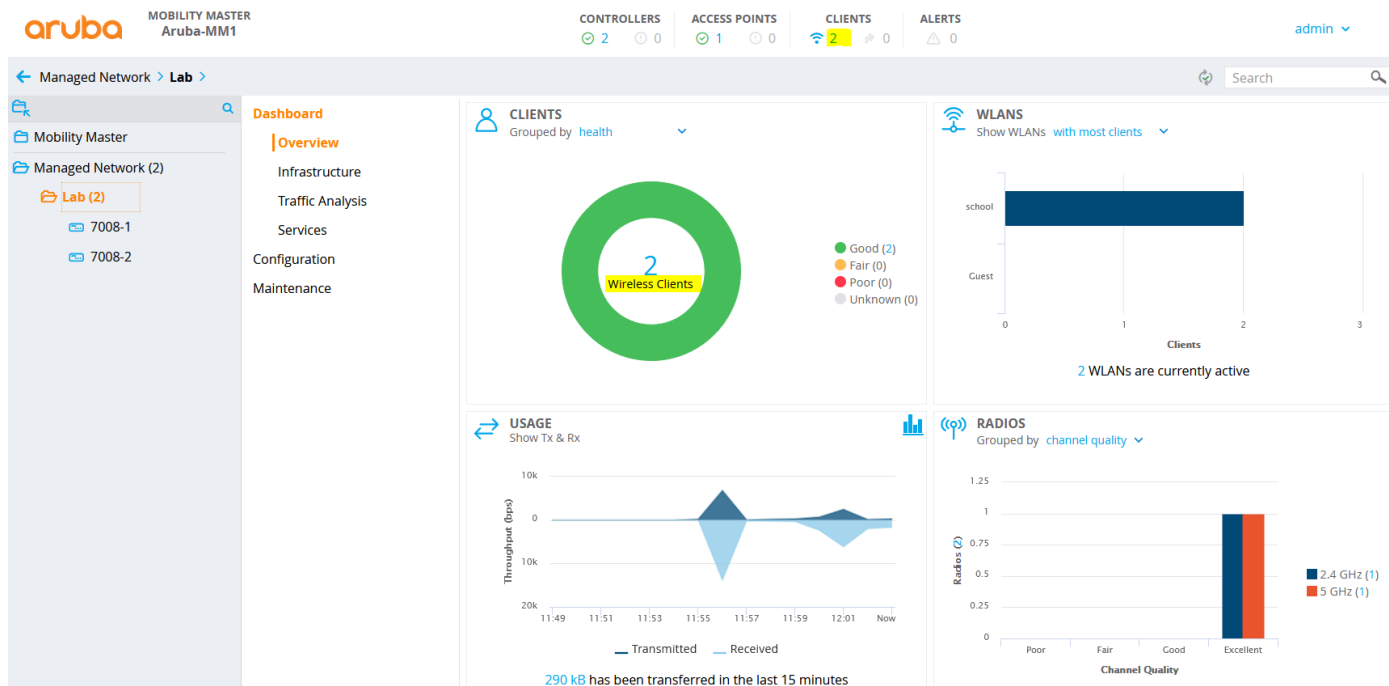
## Summary Input Output Accounting

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.