

Contents

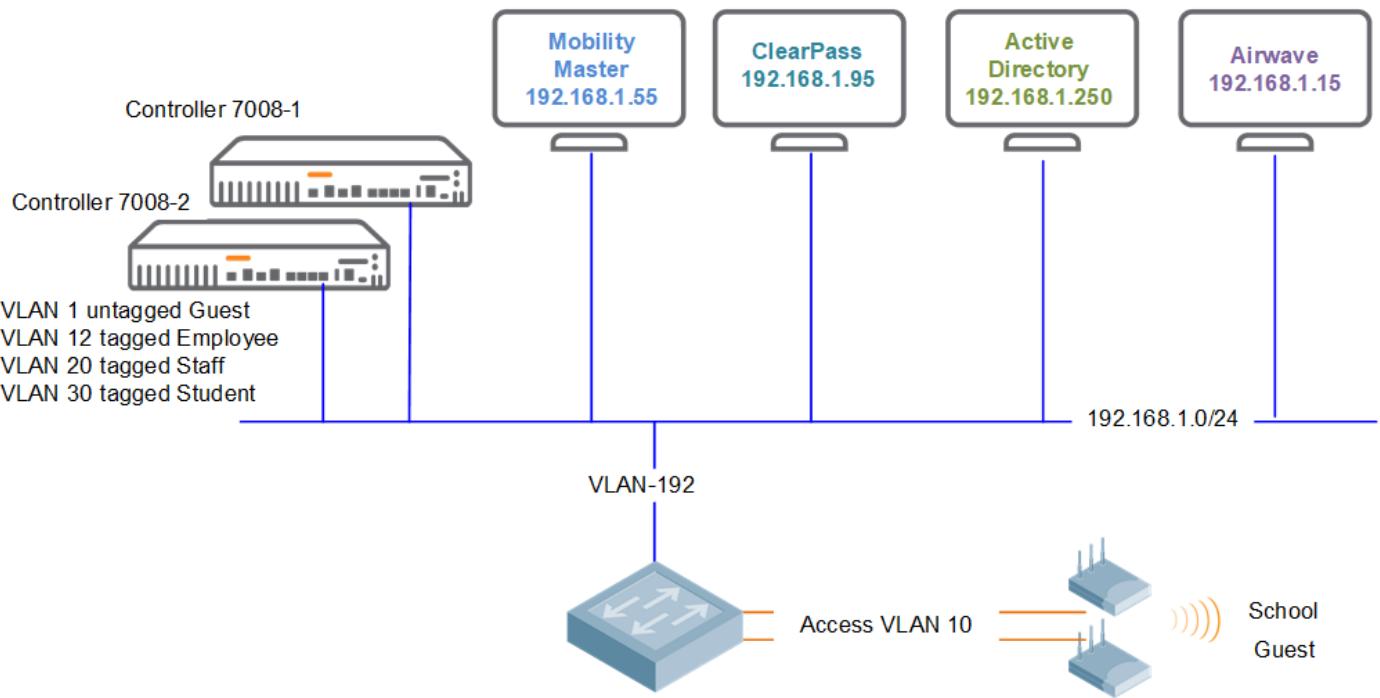
1.1	Revision History	1
2	Demo Topology	2
3	Airwave Configuration.....	3
3.1	Basic Configuration.....	3
3.2	VisualRF	8
3.3	Triggers and Alerts.....	12
4	MD Clustering	15
4.1	Cluster Configuration.....	15
4.2	Cluster Monitoring with Airwave	19
4.3	AP Node List	20
4.4	Live Cluster Upgrade.....	22

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
02 Feb 2021	0.1	Ariya Parsamanesh	Initial creation
12 Feb 2021	0.2	Ariya Parsamanesh	Added Clustering section
15 Feb 2021	0.3	Ariya Parsamanesh	Minor modification

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.



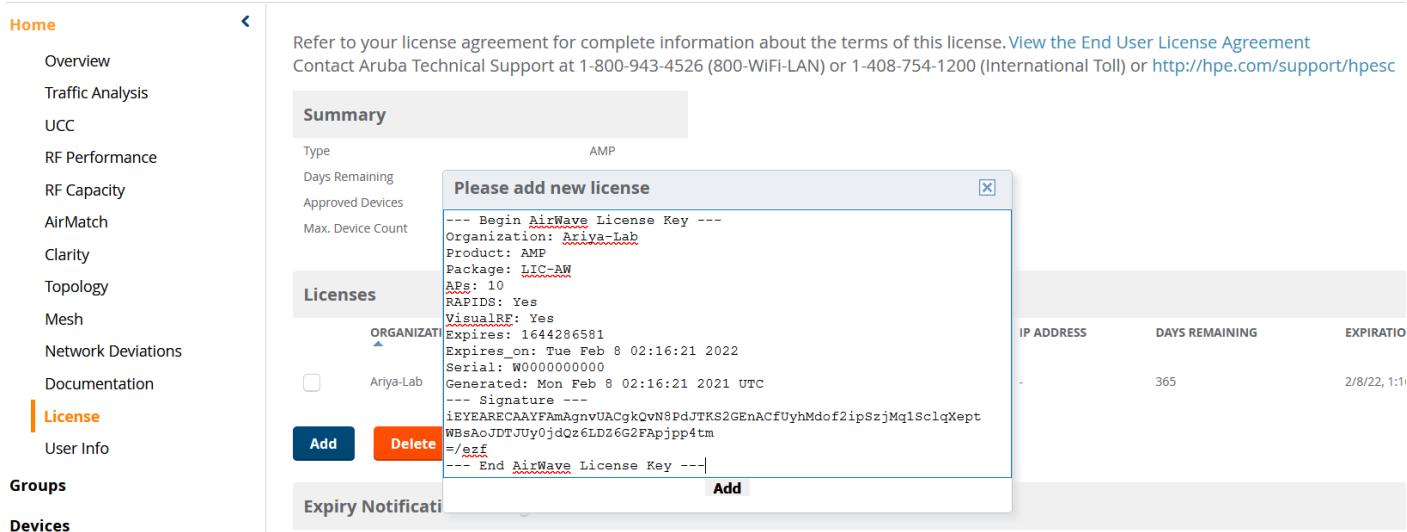
This is the part 4 of the four parts series guide.

3 Airwave Configuration

Once Airwave (AW) is installed, you can browse to its IP address.

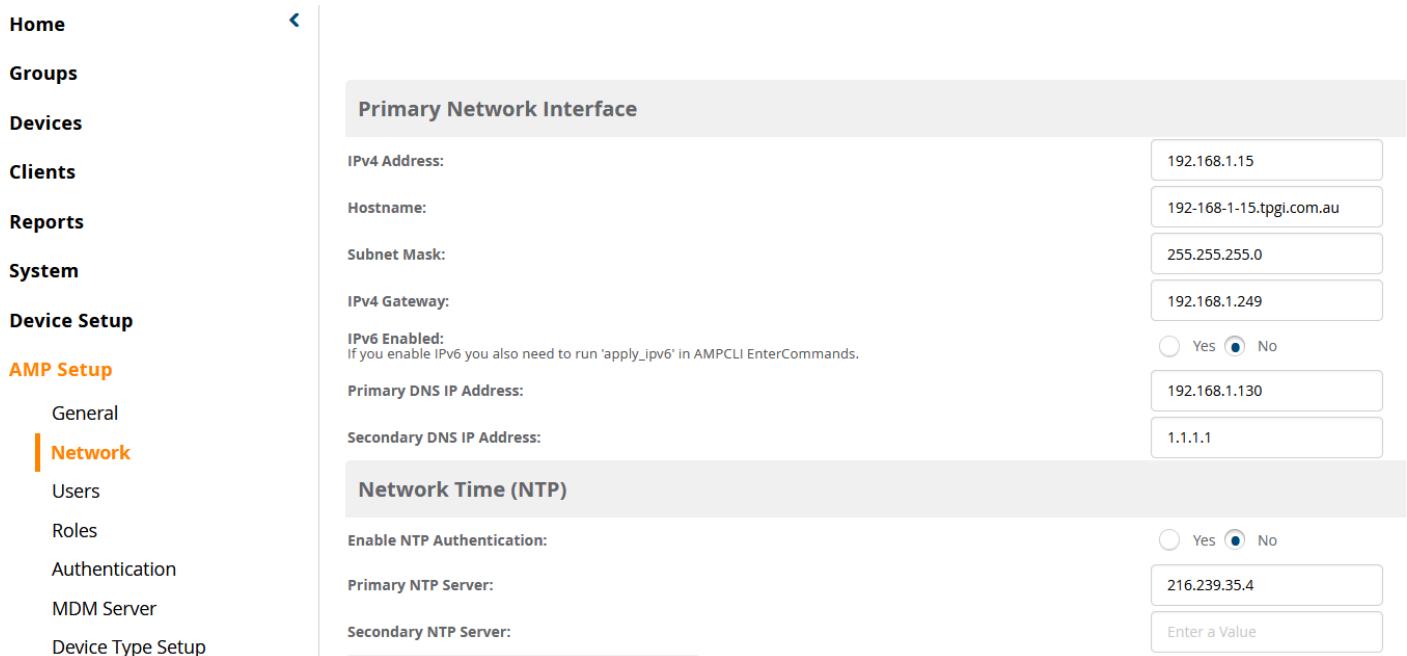
3.1 Basic Configuration

We'll start with adding the evaluation licenses. Before getting this evaluation license from your Aruba SE, you need to send them the IP address of the AW server.



The screenshot shows the Aruba Airwave License Management interface. On the left, a sidebar lists various management categories: Home, Overview, Traffic Analysis, UCC, RF Performance, RF Capacity, AirMatch, Clarity, Topology, Mesh, Network Deviations, Documentation, License (which is selected), and User Info. The main panel has a 'Summary' section with a note about the license agreement and a 'Licenses' section. In the 'Licenses' section, there is a table with columns for IP ADDRESS, DAYS REMAINING, and EXPIRATION DATE. A modal dialog box titled 'Please add new license' is open, showing a block of text representing an AirWave License Key. The key includes fields like Organization (Ariva-Lab), Product (AMP), Package (LIC-AW), and various timestamps and serial numbers.

Ensure you have the correct IP addressing and NTP configured.



The screenshot shows the Aruba Airwave Device Setup interface. The left sidebar includes categories: Home, Groups, Devices, Clients, Reports, System, Device Setup (which is selected), and AMP Setup. Under Device Setup, the 'Network' section is selected. The main panel has two configuration sections: 'Primary Network Interface' and 'Network Time (NTP)'. In the 'Primary Network Interface' section, fields are filled with values: IPv4 Address (192.168.1.15), Hostname (192-168-1-15.tpgi.com.au), Subnet Mask (255.255.255.0), IPv4 Gateway (192.168.1.249), and IPv6 Enabled (No). In the 'Network Time (NTP)' section, fields are filled with values: Primary NTP Server (216.239.35.4) and Secondary NTP Server (Enter a Value).

Then we add the MM to AW

Home <

Groups

Devices

Clients

Reports

System

Device Setup

- Discover
- Add**
- Communication
- ZTP Orchestrator BETA
- Upload Firmware & Files
- Certificates

AMP Setup

RAPIDS

VisualRF

Creating Aruba Device
Configure default credentials on the [Communication](#) page.

Device Communications

Name:	Aruba-MM1
IP Address:	192.168.1.55
SNMP Port:	161
SSH Port:	22
Community String:	*****
Confirm Community String:	*****
SNMPv3 Username:	Enter a Value
Auth Password:	
Confirm Auth Password:	
SNMPv3 Auth Protocol:	SHA-1
Privacy Password:	
Confirm Privacy Password:	
SNMPv3 Privacy Protocol:	AES
Telnet/SSH Username:	admin
Telnet/SSH Password:	*****
Confirm Telnet/SSH Password:	*****
"enable" Password:	*****
Confirm "enable" Password:	*****

Location

Group:	Access Points
Folder:	Top

Update group settings based on this device's current configuration

Monitor Only (no changes will be made to device)

Manage read/write (group settings will be applied to device)

Add **Cancel**

Then after a while you should see MM1 up and AW will discover the 2x controllers.

You can then select them and add them to a new group called controllers

Home <

Groups

Devices

- List
- New**
- Up
- Down
- Mismatched
- Ignored
- Controller Clusters

Clients

Reports

System

To discover more devices, visit the [Discover](#) page.

Use Specified Group/Folder for Instant APs & Aruba Switches: Yes No

Device Actions: **Add Selected Devices** Group: **Access Points** Folder: **Top (0 Clients)** Management Level: **Monitor Only + Firmware Upgrades** **Add**

Default View: New Devi... [Total Row Count: 2]

DEVICE	TYPE	LAN MAC ADDRESS	IP ADDRESS	DISCOVERED	CONTROLLER	FOLDER	GROUP	ARUBA AP GROUP	DISCOVERY METHOD	SERIAL NUMBER	DEVICE STATE
(Id: 2)	Aruba Device	-	192.168.1.57	2/8/21, 1:58 PM	-	-	Access Points	-	SNMP	CNDRJSP06J	-
(Id: 3)	Aruba Device	-	192.168.1.58	2/8/21, 1:58 PM	-	-	Access Points	-	SNMP	CNDRJSP06U	-

25 per page

Page: 1 **Go** < > < >

After that click on the down controllers and then manage and add the community strings and admin SSH passwords

Home**Groups****Devices**

List

Monitor

Interfaces

Manage

Config

Compliance

Rogues Contained

New

Up

Down

Mismatched

Ignored

Controller Clusters

Clients**Reports****System****Device Setup****General**

Name:

(id: 3)

Down (SNMP get failed)

Unknown (Settings not yet read from device)

Never

Aruba Device

unknown

Controllers

Add a Template

Top

 Monitor Only Manage Read/Write Yes No

Status:

Configuration:

Last Contacted:

Type:

Firmware:

Group:

Template:

Folder:

Management Mode:

Enable Planned Downtime Mode:

Notes:

Device Communication

If this device is down because its IP address or management ports have changed, update the fields below with the correct information.

IP Address:

192.168.1.58

SNMP Port (1-65535):

161

SSH Port (1-65535):

22

If this device is down because the credentials on the device have changed, update the fields below with the correct information.

This device is currently using SNMP version 2c.

Community String:

Confirm Community String:

SNMPv3 Username:

Enter a Value

Auth Password:

Confirm Auth Password:

SNMPv3 Auth Protocol:

SHA-1

Privacy Password:

Confirm Privacy Password:

SNMPv3 Privacy Protocol:

AES

Telnet/SSH Username:

admin

Telnet/SSH Password:

Confirm Telnet/SSH Password:

"enable" Password:

Confirm "enable" Password:

Don't worry about the enable password it is not used for Aruba devices.

Home**Groups****Devices**

List

Monitor

Interfaces

Manage

Config

Compliance

Rogues Contained

New

Up

Down

Mismatched

Ignored

Controller Clusters

Clients**Confirm changes:**

Controller "(id: 3)"

Community String: X000000000



X000000000

Telnet/SSH Password: XXXXXXXXXX



XXXXXXX

Apply Changes Now

Cancel

Scheduling Options

Occurs:

One Time



Specify numeric dates with optional 24-hour times (like 7/4/2003 or 2003-07-04 for July 4th, 2003, or 7/4/2003 13:00 for July 4th, 2003 at 1:00 PM.), or specify relative times (like tomorrow at noon or next tuesday at 4am). Any unsupported time format will schedule the job immediately

Current Local Time:

February 8, 2021 2:34 pm AEDT

Desired Start Date/Time:

Enter a Value

Schedule

The screenshot shows the Aruba AirWave management interface. The top navigation bar includes 'aruba' logo, 'AirWave', and 'Log out admin'. The top right corner shows 'NEW DEVICES' (0), 'UP' (3), 'DOWN' (0), 'ROGUE' (0), 'CLIENTS' (0), and 'ALERTS' (0). The left sidebar has a 'Devices' section with 'List' selected, showing 'New', 'Up', 'Down', 'Mismatched', 'Ignored', and 'Controller Clusters' options. The main content area displays a summary of 'TOTAL DEVICES' (3), 'MISMATCHED' (0), 'CLIENTS' (0), 'USAGE' (0), and 'VPN SESSIONS' (0). A 'Clients' table is shown with columns: Sources, Max, Avg, Usage, Sources, Max, Avg. The table lists three devices: '7008-1', '7008-2', and 'Aruba-MM1', all marked as 'Up' and 'Good'. Below the table are buttons for '2h', '1d', '1w', and '1y'. The 'DEVICES LIST' section shows a table with columns: DEVICE, STATUS, CONFIGURATION, CONTROLLER, FOLDER, GROUP, CLIENTS, APS, USAGE, IP ADDRESS, TYPE, CONDUCTOR CONTROLLER, and SWITCH ROLE. The table data is identical to the one above. At the bottom, there are buttons for '25' items per page, a 'Page' selector (1), and 'Go' buttons for navigating to the next or previous page.

Then the APs will be automatically discovered from the controllers

To discover more devices, visit the [Discover](#) page.

Use Specified Group/Folder for Instant APs & Aruba Switches: Yes No

Device Actions: [Add Selected Devices](#) Group: [Access Points](#) Folder: [Top \(0 Clients\)](#) Management Level: [Monitor Only + Firmware Upgrades](#) [Add](#)

Default View: New Devi... [Total Row Count: 1]

<input type="checkbox"/> DEVICE ▲	TYPE ▼	LAN MAC ADDRESS	IP ADDRESS	DISCOVERED	CONTROLLER ▼	FOLDER	GROUP ▼	ARUBA AP GROUP ▼	DISCOVERY METHOD	SERIAL N
<input type="checkbox"/> 20:4c:03:5c:05:6e	Aruba AP 303H	20:4c:03:5c:05:6E	10.10.10.20	2/8/21, 2:36 PM	7008-1	-	Access Points	Building1	Controller	-

To discover more devices, visit the [Discover](#) page.

Use Specified Group/Folder for Instant APs & Aruba Switches: Yes No

Device Actions: [Add Selected Devices](#) Group: [Access Points](#) Folder: [Top \(0 Clients\)](#) Management Level: [Monitor Only + Firmware Upgrades](#) [Add](#)

Default View: New Devi... [Total Row Count: 1]

<input checked="" type="checkbox"/> DEVICE ▲	TYPE ▼	LAN MAC ADDRESS	IP ADDRESS	DISCOVERED	CONTROLLER ▼	FOLDER	GROUP ▼	ARUBA AP GROUP ▼	DISCOVERY METH
<input checked="" type="checkbox"/> 20:4c:03:5c:05:6e	Aruba AP 303H	20:4c:03:5c:05:6E	10.10.10.20	2/8/21, 2:36 PM	7008-1	-	Access Points	Building1	Controller
<input checked="" type="checkbox"/> 20:4c:03:5c:05:6f	Aruba AP 303H	20:4c:03:5c:05:6F	10.10.10.21	2/8/21, 2:36 PM	7008-1	-	Access Points	Building1	Controller

Once we have clients connected to the wireless networks, we should see them appear in Airwave as well.

aruba | AirWave

NEW DEVICES UP DOWN ROGUE CLIENTS ALERTS

0 4 0 4 2 24

Log out admin |

Home Overview Traffic Analysis UCC RF Performance RF Capacity AirMatch Clarity Topology Mesh Network Deviations Documentation License User Info Groups Devices Clients

AirWave Management Platform 8.2.12.0

AW-Lab - Aranya-Lab

Days Remaining: 360

2h 1d 1w 1y

Clients Sources Max Avg Usage Sources Max Avg

3 2.38 M

2 1.91 M

1 1.43 M

0 977 K

488 K

0 488 K

0 488 K

10:45 11:00 11:15 11:30 11:45 12:00 12:15 12:30 12:45

10:45 11:00 11:15 11:30 11:45 12:00 12:15 12:30 12:45

— Guest — school — Total Clients

Total In Total Out VPN Total In VPN Total Out

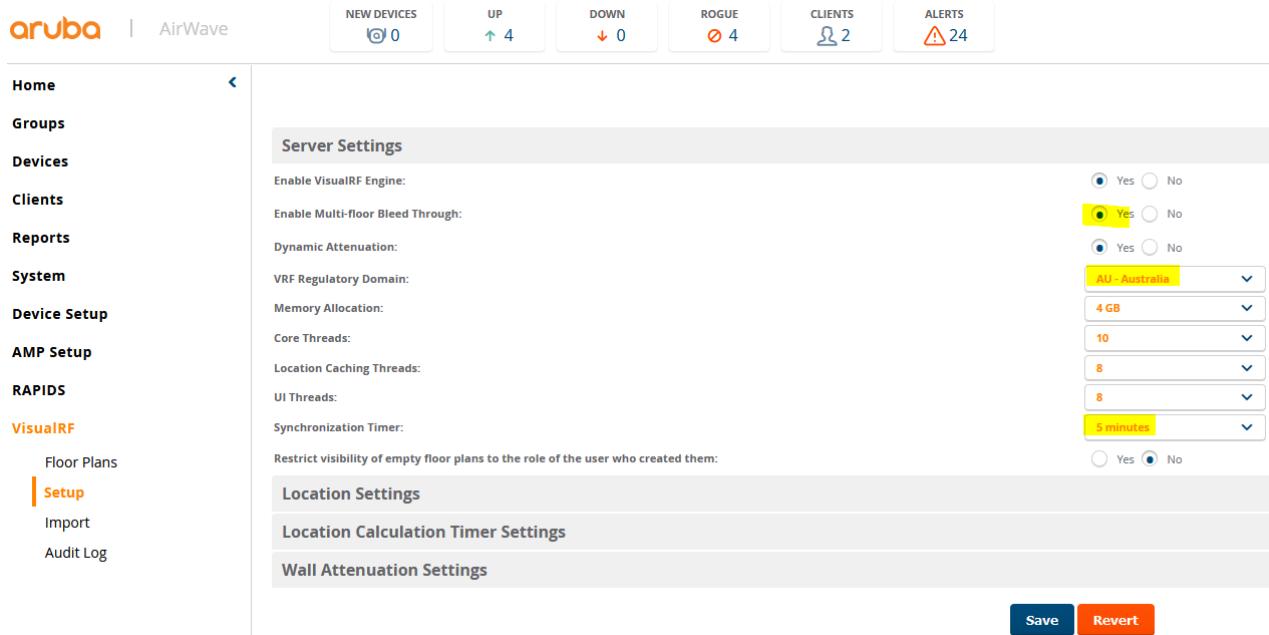
Looking at the Clarity dashboard that gives the amount of time it takes to associate, authenticate, get an IP address from DHCP and DNS resolution.

Next, is the Traffic analysis Dashboard.

Note that all the wireless configuration will be done on Mobility Master and Airwave is just used for monitoring and reporting.

3.2 VisualRF

If you want to see the heatmaps for your APs, then you need to enable VisualRF and import floor plans.



Aruba | AirWave

Home Groups Devices Clients Reports System Device Setup AMP Setup RAPIDS VisualRF

NEW DEVICES UP DOWN ROGUE CLIENTS ALERTS

Server Settings

Enable VisualRF Engine: Yes No

Enable Multi-floor Bleed Through: Yes No

Dynamic Attenuation: Yes No

VRF Regulatory Domain: AU - Australia

Memory Allocation: 4 GB

Core Threads: 10

Location Caching Threads: 8

UI Threads: 8

Synchronization Timer: 5 minutes

Restrict visibility of empty floor plans to the role of the user who created them: Yes No

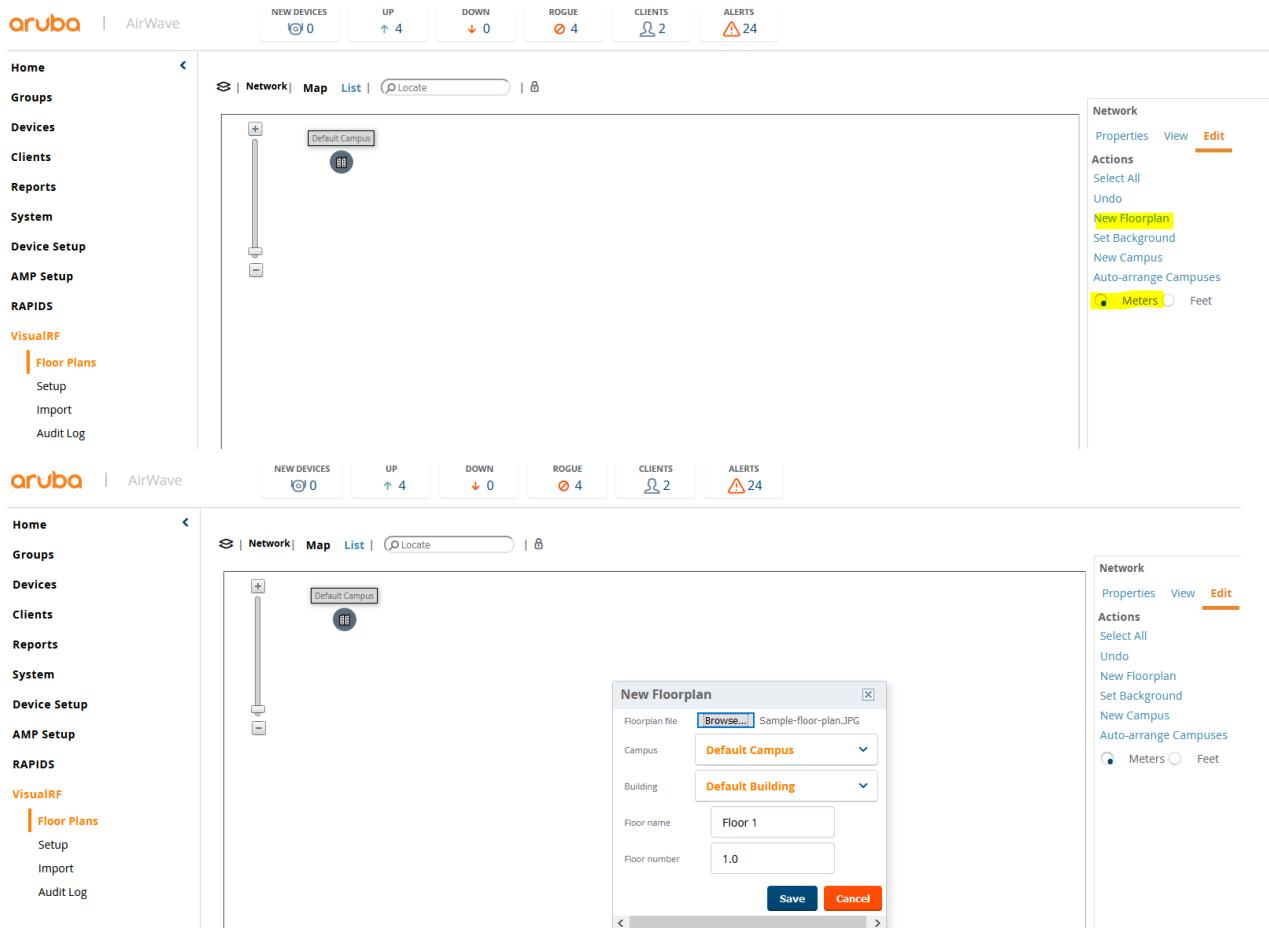
Location Settings

Location Calculation Timer Settings

Wall Attenuation Settings

Save Revert

Then you need to go to the floor plans and import your floor plan



Aruba | AirWave

Home Groups Devices Clients Reports System Device Setup AMP Setup RAPIDS VisualRF

NEW DEVICES UP DOWN ROGUE CLIENTS ALERTS

Floor Plans

Setup Import Audit Log

Network

Properties View Edit

Actions

Select All Undo New Floorplan Set Background New Campus Auto-arrange Campuses

Meters Feet

Network

Properties View Edit

Actions

Select All Undo New Floorplan Set Background New Campus Auto-arrange Campuses

Meters Feet

New Floorplan

Floorplan file: Sample-floor-plan.JPG

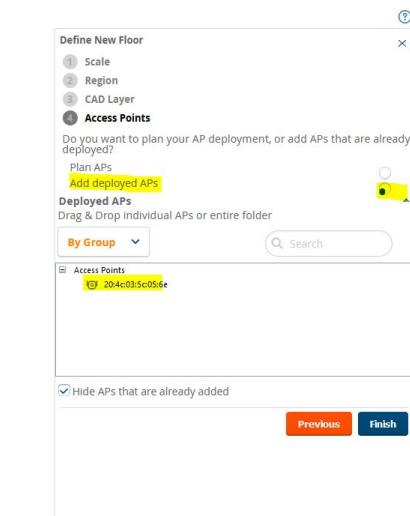
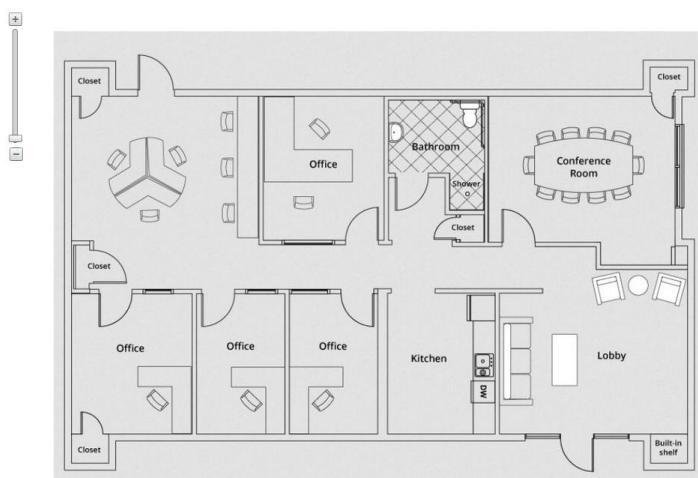
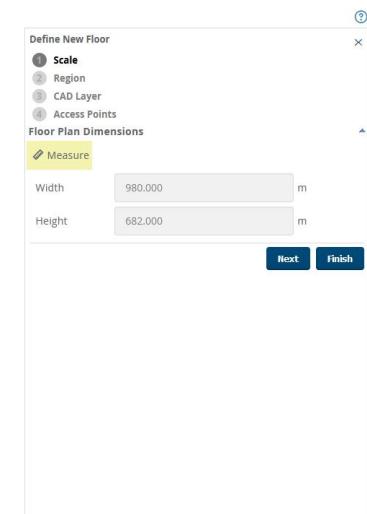
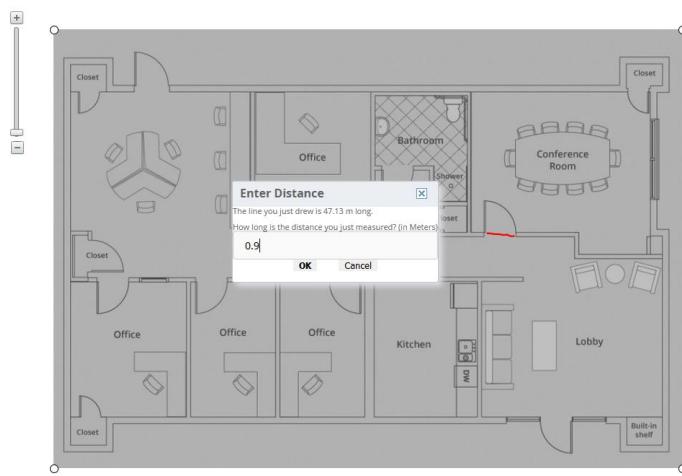
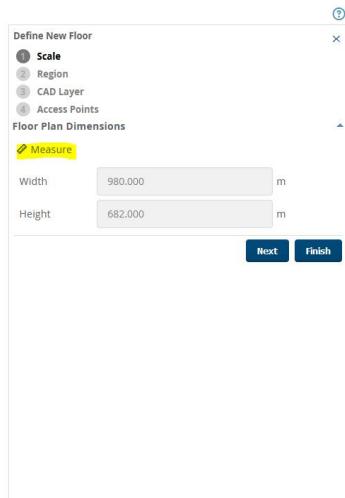
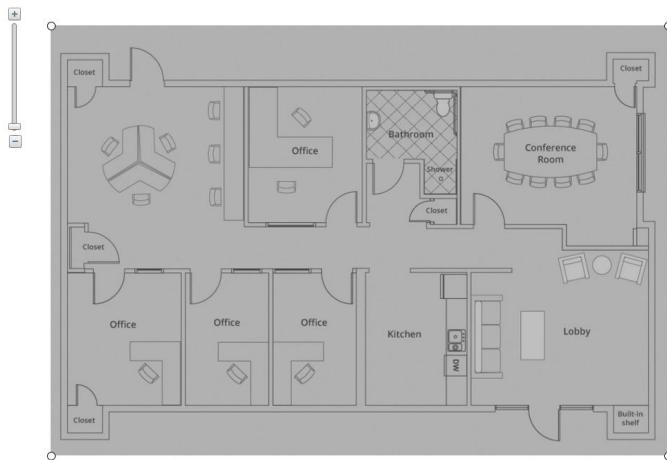
Campus: Default Campus

Building: Default Building

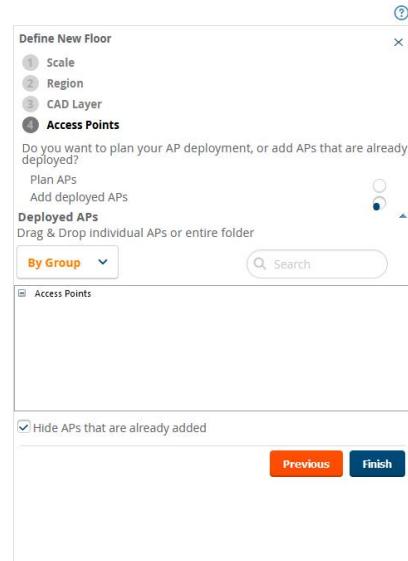
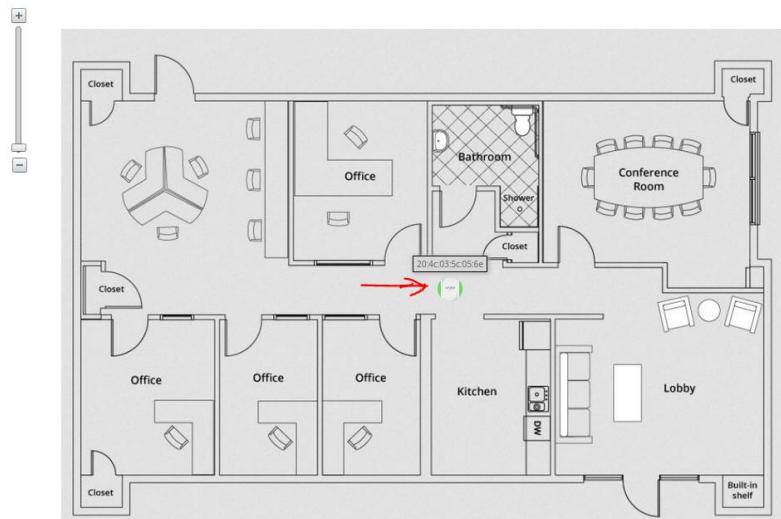
Floor name: Floor 1

Floor number: 1.0

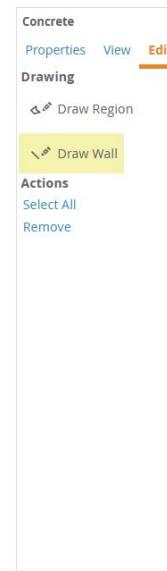
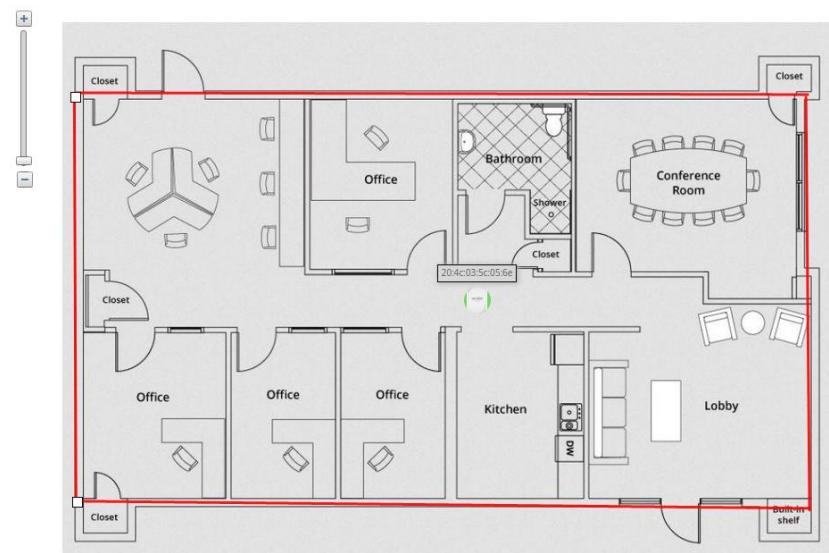
Save Cancel



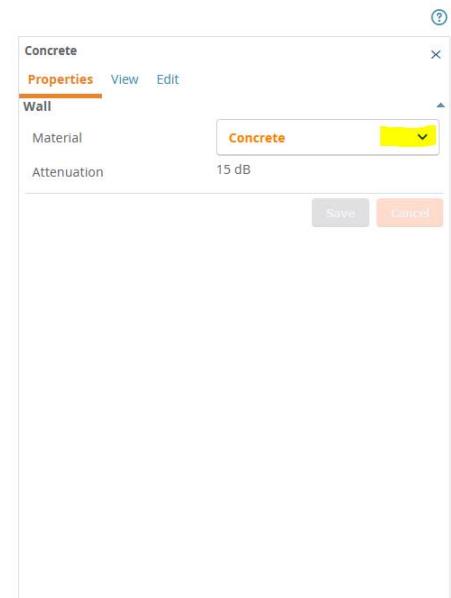
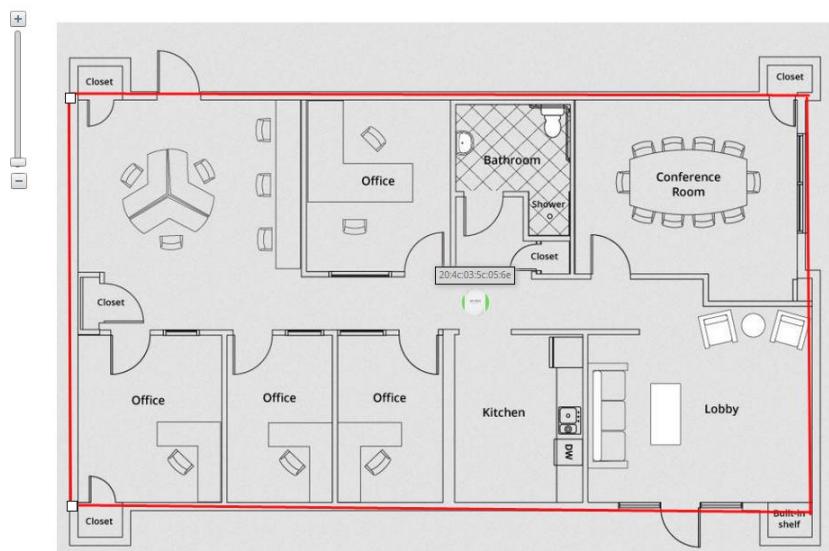
You need to drag the AP on to the floor plan and click on Finish



After this, you need to draw a perimeter wall, also ensure you click on the pad lock to unlock the floor plan.



The red line is concrete wall type and by clicking on properties, you can change it according to your environment



Now you can go back to the VisualRF floor plans and you'll see "Default Campus". Here you can add any background you want to show where that floor plan in that building is located.

Default Campus

Select All Undo Ctrl+A Ctrl+Z New Floorplan Set Background New Campus Auto-arrange Campuses

Network Properties View Edit

Network

APs 1

Buildings 1

Clients 0

Controllers 0

Floors 1

Racks 0

Switches 0

Wiring Closets 0

You can then do the same thing with the campus background

Default Building

Properties View Edit

Building

APs 1 Total, 0 Planned, 0 Down, 4 Rogues

Clients 2

Floors 1

Name Library

Campus Default Campus

Address

Latitude

Longitude

Ceiling Height 3.05 m

Attenuation 20.00 dBm

Save Cancel

Now when you double click on the building, you'll see the floor. We have only added one floor.

Floor 1

Properties View Edit

Floor

APs 1 Total, 0 Planned, 0 Down, 4 Rogues

Clients 2

Campus Default Campus

Building Library

Floor name Floor 1

Floor number 1.0

Width 18.72 m

Height 13.02 m

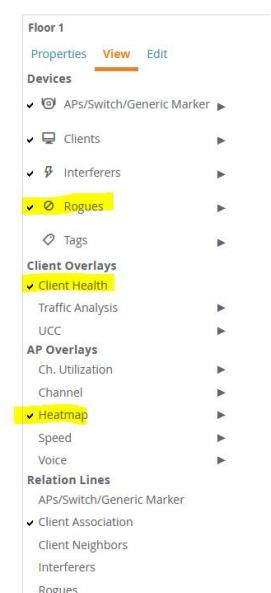
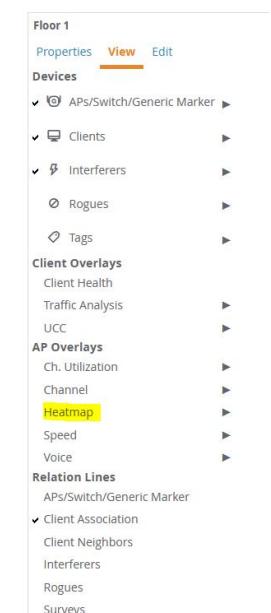
Gridsize 0.6x0.6 m

Advanced

Save Cancel



You can selectively enable a few information like heatmap, rogue APs to overlay the floor plan.



3.3 Triggers and Alerts

Here are some interesting system triggers that you can configure to alert you about your environment.

aruba | AirWave

NEW DEVICES 0 UP 4 DOWN 0 ROGUE 4 CLIENTS 2 ALERTS 24

Log out admin |

Home **Groups** **Devices** **Clients** **Reports** **System** **Triggers** **Alerts** **Backups** **Configuration Change Jobs** **Firmware Upgrade Jobs** **DRT Upgrade Jobs** **Performance** **Download Log Files**

Add New Trigger

Triggers

TYPE	TRIGGER	ADDITIONAL NOTIFICATION OPTIONS	NMS TRAP DESTINATIONS	CEF SYSLOG DESTINATIONS	SEVERITY	FOLDER	GROUP	INCLUDE SUBFOLDERS	LOGGED ALERT
<input type="checkbox"/>	Device Event - SNMP Trap Category is Hardware or SNMP Trap Category is Software	-	-	-	Normal	Top	-	Yes	By Triggering Age
<input type="checkbox"/>	Device Event - Event Type is Syslog and Syslog Severity >= Critical	-	-	-	Normal	Top	-	Yes	By Triggering Age
<input type="checkbox"/>	Device Event - Event Type is Syslog and Syslog Category is Hardware Monitor	-	-	-	Warning	Top	-	Yes	By Triggering Age
<input type="checkbox"/>	Disk Usage - Partition Percent Used >= 80%	-	-	-	Warning	-	-	-	-

4 Triggers
Select All - Unselect All
Delete

No triggers for other roles found

Here we'll add a trigger for channel util of over 70% for 15 minute and if the AP radio is 5GHz.

Trigger

Type: Channel Utilization

Severity: Warning

Duration: 15 min

Conditions

Matching conditions: All

Add New Trigger Condition

OPTION	CONDITION	VALUE
Time Busy (%)	>=	70
Radio Type	is	5GHz (802.11 a/n)

Trigger Restrictions

Folder: Top

Include Subfolders: Yes

Group: - All Groups -

Alert Notifications

And you can combine any of the trigger type

Trigger

Type: Device Down

Severity: Devices

Limit by number of events: Device Down

Send Alerts for Thin APs when Controller is Down: Device Up

Send Alerts when Upstream Device is Down: Configuration Mismatch

Send Alerts on Reboot: AP Usage

Include reboots detected by uptime reset or reboot count increase

Conditions

Matching conditions: Radio Up

Add New Trigger Condition

Trigger Restrictions

Folder: Top

Include Subfolders: Yes

Group: - All Groups -

There are many trigger types which you can use, for the full list of trigger types you should refer to the user guide.

Stolen device

If a device (laptop/tablet) is missing, you can set up a trigger with its MAC address, and this will send an alert whenever the device is seen on the network.

Trigger

Type: Connected Clients

Filter on connection mode: Wireless

MAC Addresses: Enter a list of MAC addresses separated by spaces, commas, or semicolons that should trigger this alert or empty for all clients.

Severity: Normal

Trigger Restrictions

Folder: Top

Include Subfolders: Yes

Group: - All Groups -

Alert Notifications

Client RADIUS Authentication Issues

A Client RADIUS auth trigger can help identify devices that are failing authentication over and over, possibly impacting the performance of the auth server.

The screenshot shows the configuration for a 'Client RADIUS Authentication' trigger. The 'Type' is set to 'Client RADIUS Authentication' with 'Severity' as 'Minor' and a 'Duration' of '15 mins'. The 'Conditions' section is set to 'All' matching conditions. A single condition is defined with 'OPTION' as 'Count', 'CONDITION' as '>', and 'VALUE' as '10'. The 'Trigger Restrictions' section includes a 'Folder' of 'Top', 'Include Subfolders' as 'Yes', and a 'Group' of '- All Groups -'. The 'Alert Notifications' section is empty.

Checking for Radar type when using DFS channels.

Here we can check for the word "Radar" in the events messages that is sent to AW from the controllers.

The screenshot shows the configuration for a 'Device Event' trigger. The 'Type' is set to 'Device Event' with 'Severity' as 'Normal'. The 'Conditions' section is set to 'All' matching conditions. A single condition is defined with 'OPTION' as 'Event Contents', 'CONDITION' as 'matches', and 'VALUE' as 'Radar'. The 'Trigger Restrictions' section includes a 'Folder' of 'Top', 'Include Subfolders' as 'Yes', and a 'Group' of '- All Groups -'. The 'Alert Notifications' section is empty.

4 MD Clustering

Cluster is a combination of multiple MDs working together to provide high availability to all the clients and ensure service continuity when a failover occurs. ArubaOS 8.x supports a 12-node cluster. The managed devices need not be identical and can be either L2-connected or L3-connected with a mixed configuration. In case of failover, the client SSO works for the L2-connected managed devices and the clients are de-authenticated for L3-connected managed devices in a cluster.

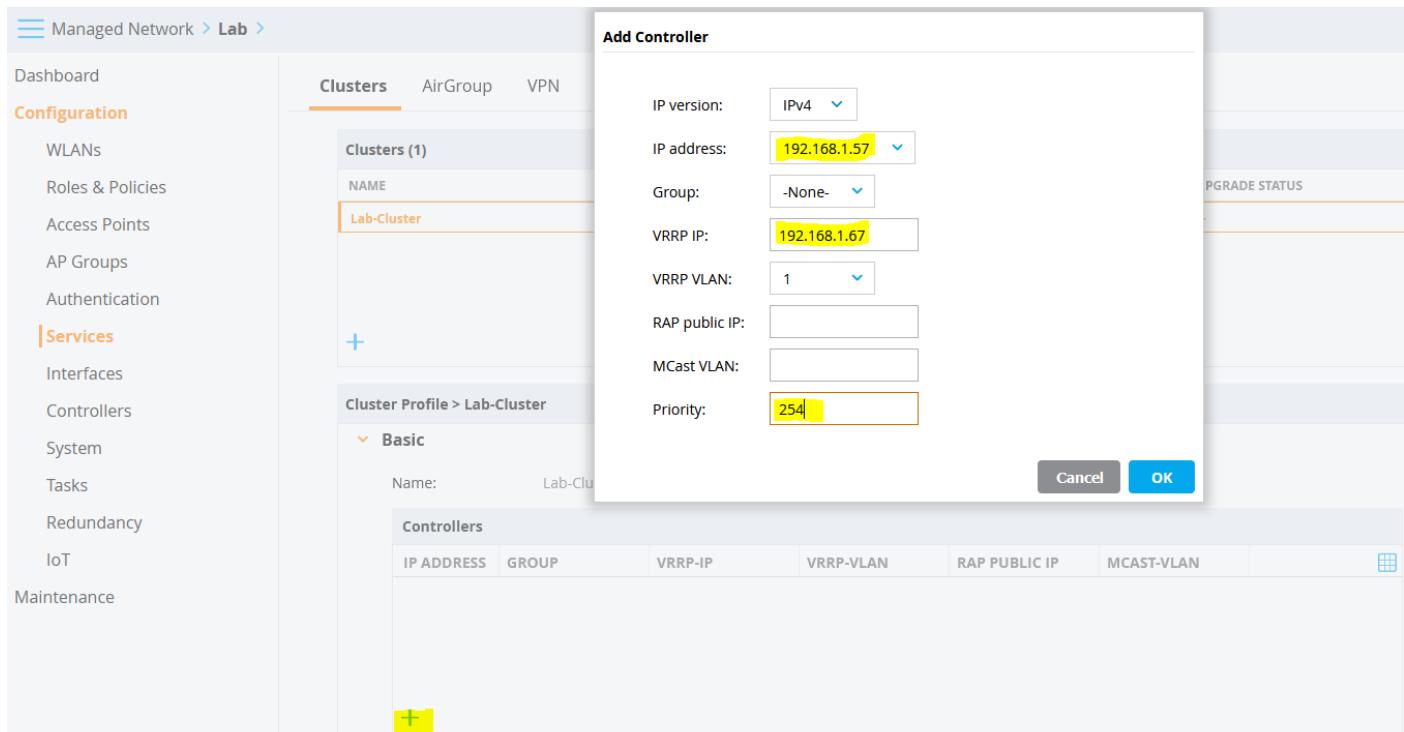
The aims of clustering are

- **seamless Campus Roaming:** When a client roams between APs of different managed devices within a large L2 domain, the client retains the same subnet and IP address to ensure seamless roaming. The clients remain anchored to a single managed device in a cluster throughout their roaming area which makes their roaming experience seamless because their L2 or L3 information and sessions remain on the same managed device.
- **Hitless Client Failover:** When a managed device fails, all the users fail over to their standby managed device seamlessly without any disruption to their wireless connectivity or existing high-value sessions.
- **Client and AP Load Balancing:** When there is excessive workload among the managed devices, the client and AP load is evenly balanced among the cluster members. Both clients and APs are load balanced seamlessly.

4.1 Cluster Configuration

Here we'll be configuring a L2 connected cluster which is the most common type of deployment. The client load is shared by all the managed devices and there is a larger roaming domain with smaller fault domain which helps in faster recovery.

All the managed devices that are part of a cluster are collectively known as cluster members. The workload of serving APs and clients is divided or partitioned among cluster members. All managed devices that are part of the cluster are managed by the same Mobility Master.



The screenshot shows the ArubaOS interface for managing a network. On the left, a sidebar lists various configuration options like WLANs, Roles & Policies, and Services. The main area is focused on 'Clusters', showing a list of 'Clusters (1)' with 'Lab-Cluster' selected. A modal dialog titled 'Add Controller' is open, allowing the configuration of a new cluster member. The 'Basic' profile for 'Lab-Cluster' is selected. The 'Add Controller' dialog fields are as follows:

- IP version: IPv4
- IP address: 192.168.1.57
- Group: -None-
- VRRP IP: 192.168.1.67
- VRRP VLAN: 1
- RAP public IP: (empty)
- MCast VLAN: (empty)
- Priority: 254

At the bottom of the dialog are 'Cancel' and 'OK' buttons. The background shows the 'Clusters' tab in the 'Lab' configuration section, with 'Clusters (1)' and 'NAME' listed.

And we'll add the second MD as well

Add Controller

IP version:	IPv4
IP address:	192.168.1.58
Group:	-None-
VRRP IP:	192.168.1.68
VRRP VLAN:	1
RAP public IP:	
MCast VLAN:	
Priority:	253

Cancel **OK**

Dashboard

Clusters AirGroup VPN Firewall IP Mobility External Services DHCP WAN

Clusters (1)

NAME	CONTROLLERS	FIRMWARE VERSION	UPGRADE STATUS
Lab-Cluster	2	--	--

+

Cluster Profile > Lab-Cluster

Basic

Name:	Lab-Cluster
-------	-------------

Controllers

IP ADDRESS	GROUP	VRRP-IP	VRRP-VLAN	RAP PUBLIC IP	MCAST-VLAN
192.168.1.57	--	192.168.1.67	1	--	--
192.168.1.58	--	192.168.1.68	1	--	--

Now we need to go to individual MDs and assigned them to this cluster

Managed Network > Lab > 7008-1 Version 8.6.0.7

Clusters AirGroup VPN Firewall IP Mobility External Services DHCP WAN

Cluster Profile

Cluster group-membership:	Lab-Cluster
Exclude VLANs:	

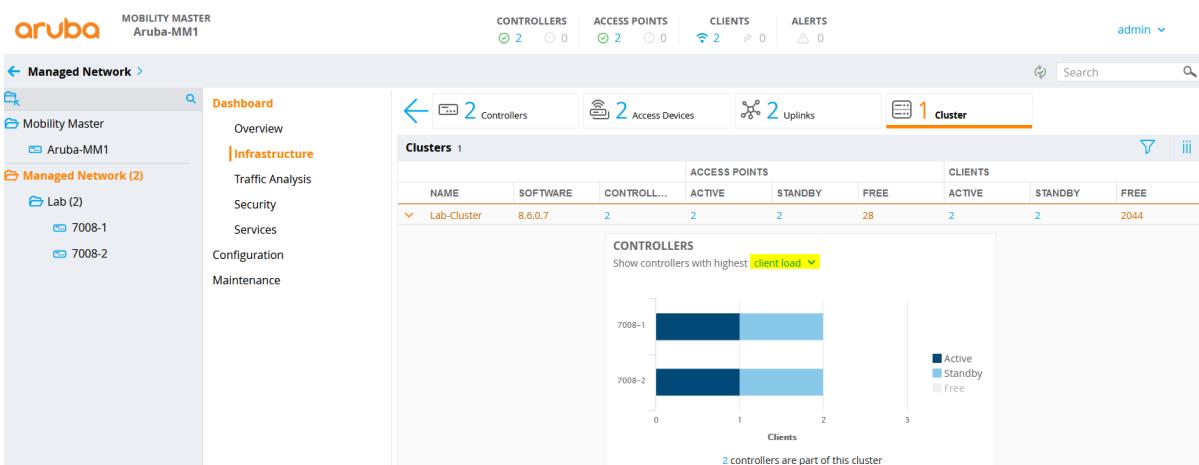
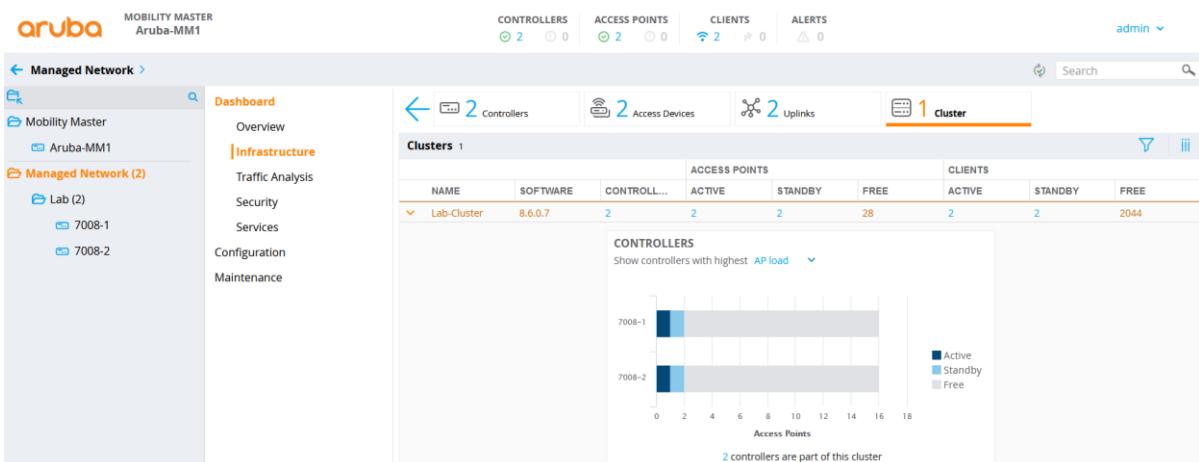
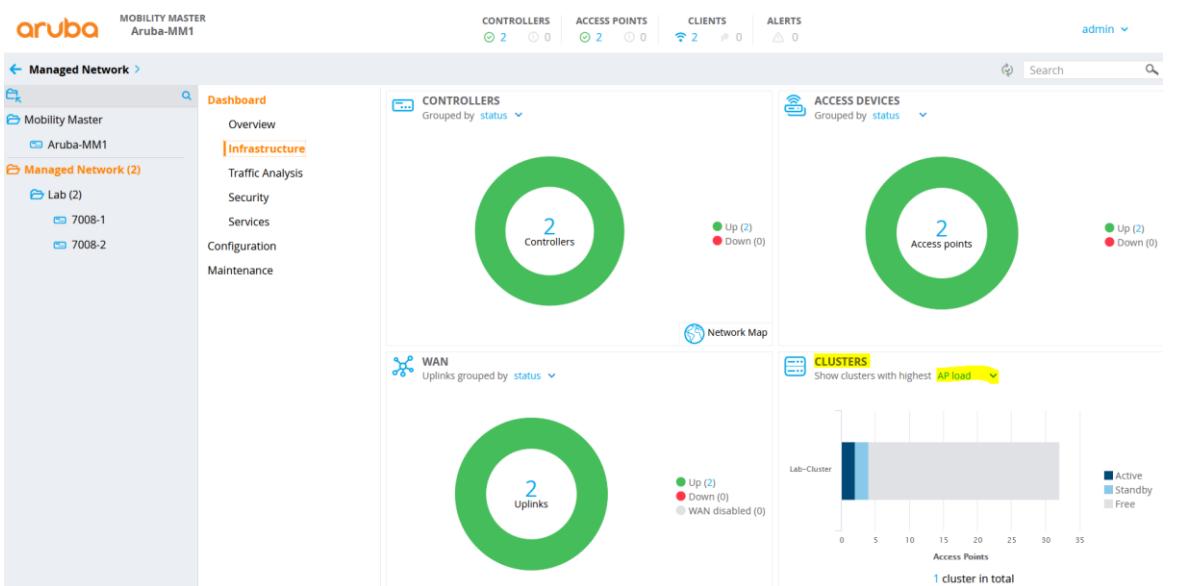
Managed Network > Lab > 7008-2 Version 8.6.0.7

Clusters AirGroup VPN Firewall IP Mobility External Services DHCP WAN

Cluster Profile

Cluster group-membership:	Lab-Cluster
Exclude VLANs:	

Once you submitted the configuration, you can check the dashboard.



Here is the CLI command to check the operation of the cluster.

```
(7008-1) #show lc-cluster group-membership
```

```
Cluster Enabled, Profile Name = "Lab-Cluster"
Redundancy Mode On
Active Client Rebalance Threshold = 50%
Standby Client Rebalance Threshold = 75%
Unbalance Threshold = 5%
AP Load Balancing: Enabled
Active AP Rebalance Threshold = 20%
Active AP Unbalance Threshold = 5%
Active AP Rebalance AP Count = 50
```

```

Active AP Rebalance Timer = 1 minutes
Cluster Info Table
-----
Type IPv4 Address      Priority Connection-Type STATUS
-----
self    192.168.1.57      254          N/A CONNECTED (Leader)
peer    192.168.1.58      253          L2-Connected CONNECTED (Member, last HBT_RSP 10ms ago, RTD =
1.003 ms)
(7008-1) #
(7008-1) #
(7008-1) #
(7008-1) #
(7008-1) #show lc-cluster load distribution client

Cluster Load Distribution for Clients
-----
Type IPv4 Address      Active Clients Standby Clients
-----
self    192.168.1.57      1          1
peer    192.168.1.58      1          1
Total: Active Clients 2 Standby Clients 2
(7008-1) #
(7008-1) #show lc-cluster load distribution ap

Cluster Load Distribution for APs
-----
Type IPv4 Address      Active APs      Standby APs
-----
self    192.168.1.57      1          1
peer    192.168.1.58      1          1
Total: Active APs 2 Standby APs 2
(7008-1) #

(7008-2) #show lc-cluster group-membership

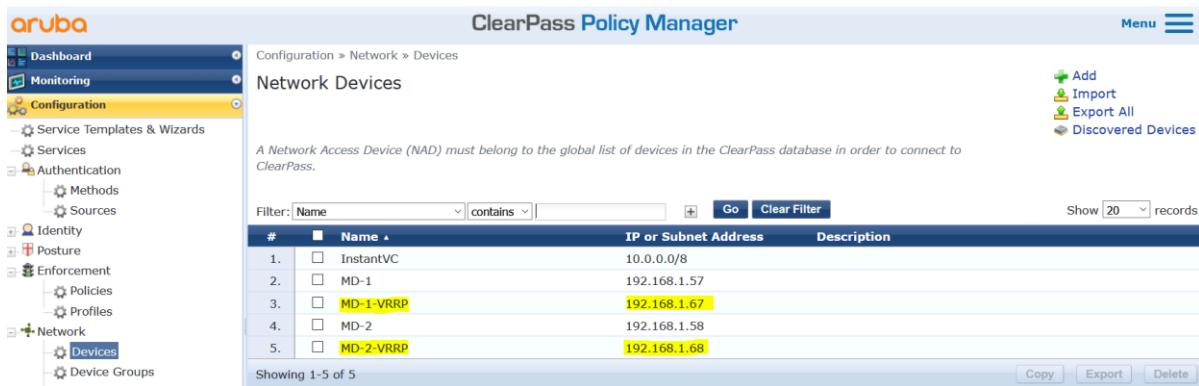
Cluster Enabled, Profile Name = "Lab-Cluster"
Redundancy Mode On
Active Client Rebalance Threshold = 50%
Standby Client Rebalance Threshold = 75%
Unbalance Threshold = 5%
AP Load Balancing: Enabled
Active AP Rebalance Threshold = 20%
Active AP Unbalance Threshold = 5%
Active AP Rebalance AP Count = 50
Active AP Rebalance Timer = 1 minutes
Cluster Info Table
-----
Type IPv4 Address      Priority Connection-Type STATUS
-----
peer    192.168.1.57      254          L2-Connected CONNECTED (Leader, last HBT_RSP 36ms ago, RTD =
0.000 ms)
self    192.168.1.58      253          N/A CONNECTED (Member)
(7008-2) #
(7008-2) #show lc-cluster load distribution ap

Cluster Load Distribution for APs
-----
Type IPv4 Address      Active APs      Standby APs
-----
peer    192.168.1.57      1          1
self    192.168.1.58      1          1
Total: Active APs 2 Standby APs 2
(7008-2) #
(7008-2) #show lc-cluster load distribution client

Cluster Load Distribution for Clients
-----
Type IPv4 Address      Active Clients Standby Clients
-----
peer    192.168.1.57      1          1
self    192.168.1.58      1          1
Total: Active Clients 2 Standby Clients 2
(7008-2) #

```

Now we need to add the VRRP IP addresses of the MDs for the cluster as NADs to ClearPass otherwise CoA will not work. The VRRP IP used to service all requests initiated by external authentication servers such as CoA.



ClearPass Policy Manager

Network Devices

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

#	Name	IP or Subnet Address	Description
1.	InstantVC	10.0.0.0/8	
2.	MD-1	192.168.1.57	
3.	MD-1-VRRP	192.168.1.67	
4.	MD-2	192.168.1.58	
5.	MD-2-VRRP	192.168.1.68	

Here we'll check the access tracker for a new client authentication

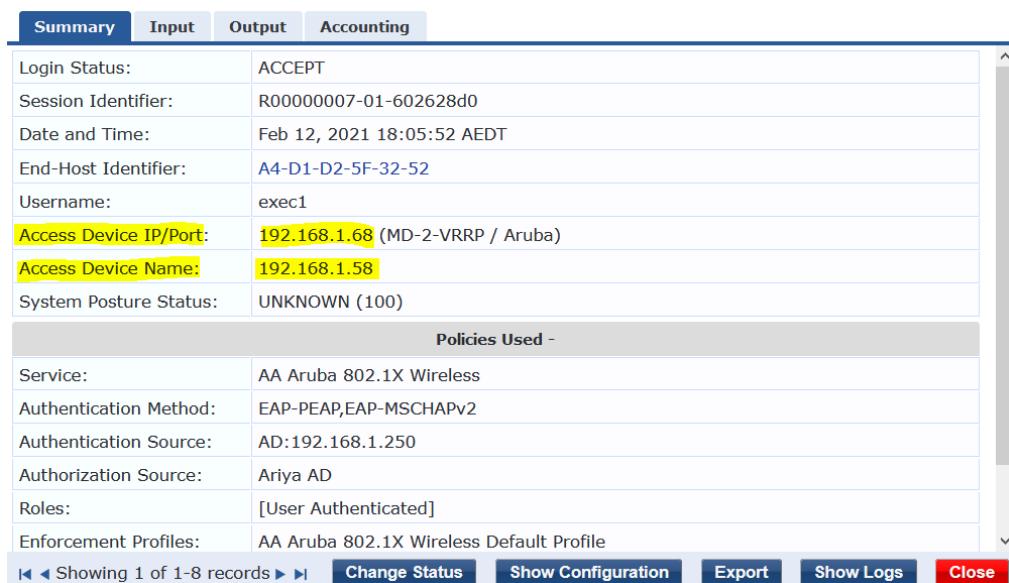


Monitoring > Live Monitoring > Access Tracker

Access Tracker Feb 12, 2021 18:08:41 AEDT

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

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.95	RADIUS	exec1	AA Aruba 802.1X Wireless	ACCEPT	2021/02/12 18:05:52
2.	192.168.1.95	RADIUS	exec1	AA Aruba 802.1X Wireless	ACCEPT	2021/02/12 18:05:28
3.	192.168.1.95	RADIUS	exec1	AA Aruba 802.1X Wireless	ACCEPT	2021/02/12 18:03:10
4.	192.168.1.95	RADIUS	anonyguest	GG MAC Authentication	ACCEPT	2021/02/12 18:00:54



Summary Input Output Accounting

Login Status:	ACCEPT
Session Identifier:	R00000007-01-602628d0
Date and Time:	Feb 12, 2021 18:05:52 AEDT
End-Host Identifier:	A4-D1-D2-5F-32-52
Username:	exec1
Access Device IP/Port:	192.168.1.68 (MD-2-VRRP / Aruba)
Access Device Name:	192.168.1.58
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 Default Profile

◀ ▶ Showing 1 of 1-8 records ▶ ▶ Change Status Show Configuration Export Show Logs Close

4.2 Cluster Monitoring with Airwave

You can get a quick cluster status on the Controller Clusters dashboard. You will find a count of the controllers, APs and clients are associated with these clusters at the top of the page and cluster information, including fault tolerance in the table beneath the counters.

aruba | AirWave

NEW DEVICES UP 4 DOWN 0 ROGUE 6 CLIENTS 2 ALERTS 24

Home Groups Devices Clients Reports

Controller Clusters

1 Clusters 2 Controllers 2 APs 2 Clients

Cluster Name	Controller C...	APs	Clients	Cluster Status	AP Capacity	Client Capac...	Version	Free AP Count	HitLess_Failo...	Max Controll...	Mobility Ma...	ACTION
Lab-Cluster	2	2	2	AI	AI	AI	8.6.0.7	14	POSSIBLE	1	Aruba-MM1	

Clicking on the “Lab-Cluster”.

aruba | AirWave

NEW DEVICES UP 4 DOWN 0 ROGUE 6 CLIENTS 2 ALERTS 24

Home Groups Devices Clients Reports System Device Setup AMP Setup RAPIDS VisualRF

Controller Clusters > Cluster Monitoring (Lab-Cluster)

AP Capacity Client Capacity

Controllers

Name	IP	Status	AP Capacity	Client Capacity	Role	Type	Version
7008-1	192.168.1.57	AI	AI	AI	Leader	Aruba 7008	8.6.0.7
7008-2	192.168.1.58	AI	AI	AI	Member	Aruba 7008	8.6.0.7

4.3 AP Node List

When an AP joins a cluster, it learns the IP addresses of all the cluster members. These IP addresses are stored in a Node List, which is saved as an environment variable in the AP's flash memory. Therefore, when the AP reboots and comes back up, the AP checks the Node List, contact the cluster member that is listed first in the Node List. If the cluster member that is first on the Node List is down or not reachable, then the AP dynamically tries the second cluster member listed in the Node List and so forth. The AP always finds a managed device as long as at least one managed device is active in the cluster.

Here is the console log of the AP booting.

```

APBoot 2.1.4.7 (build 57679)
Built: 2016-12-08 at 15:41:41

Model: AP-303H
DRAM: 512 MiB
Flash: Detected MX25L3205D: total 4 MiB
NAND: Detected MX35LFXGE4AB: total 128 MiB
Power: 802.3af POE
Net: eth0
Radio: ipq4029#0, ipq4029#1
Reset: cold
FIPS: passed

```

```

Hit <Enter> to stop autoboot: 0
apboot>

```

```

apboot> print
NEW_SBL1=1
a_ant_pol=0
a_antenna=0
ap1xtls_suffix_domain=aruba.ap
ap_lldp_pse_detect=0
auto_prov_id=0
autoload=n
autostart=yes
backup_vap_band=2
backup_vap_init_master=192.168.1.58
backup_vap_opmode=0
baudrate=9600
boardname=Aberlour
bootargs=console=ttyMSM0,9600n8 rdinit=/sbin/init ubi.mtd-aos0 ubi.mtd-aos1
ubi.mtd=ubifs
bootcmd=boot ap
bootdelay=2
bootfile=ipq40xx.ari
cellular_nw_preference=1
cert_cap=1
cfg_blms=0.0.0.0
cfg_lms=0.0.0.0
ethact=eth0
ethaddr=20:4c:03:17:a0:4c
g_ant_pol=0
g_antenna=0
group=Building1
hw_opmode=0
installation=0
ip6prefix=64
is_rmp_enable=0
machid=8010001
master_preference=2
mesh_role=0
mesh_sae=0
mtdddevname-aos0
mtdddevnum=0
mtddids=nand0=nand0
mtddparts=mtddparts=nand0:0x2000000@0x0(aos0),0x2000000@0x2000000(aos1),0x4000000@0x40000
00(ubifs)
name=20:4c:03:17:a0:4c
nodelist=192.168.1.58,192.168.1.57
num_ipsec_retry=85
num_reboot=49
num_total_bootstrap=7
os_partition=0
partition=nand0,0
previous_lms=0.0.0.0
priority_cellular=0
priority_etherent=0
priority_wifi=0
radio_0_5ghz_ant_pol=0
radio_1_5ghz_ant_pol=0
rap_tftp_upgrade=0
servername=aruba-master
start_type=cold_start
stderr=serial
stdin=serial
stdout=serial
uplink_vlan=0
usb_power_mode=0
usb_type=0

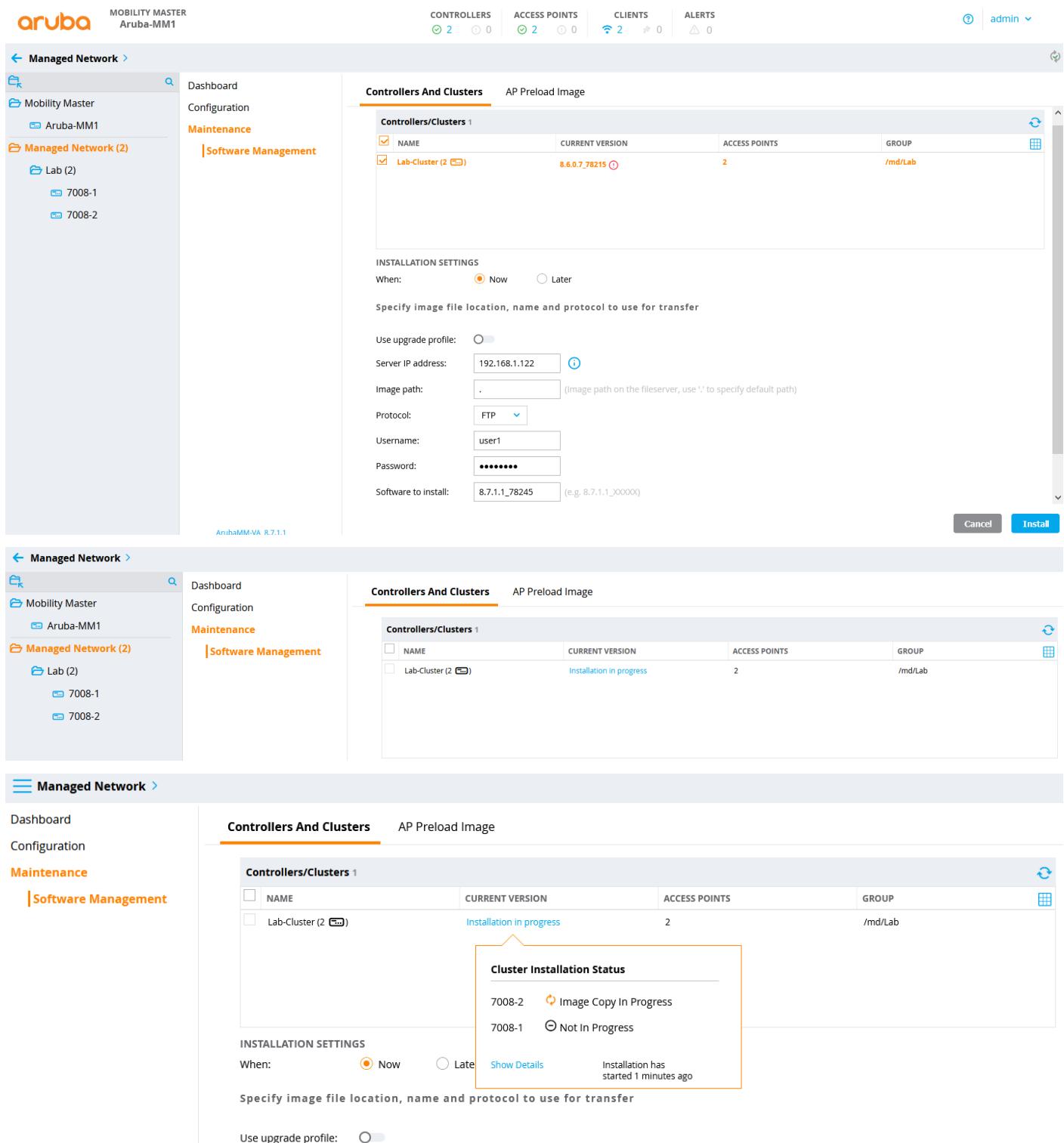
Environment size: 1316/65532 bytes
apboot>

```

4.4 Live Cluster Upgrade

The Live Upgrades feature allows you to upgrade the managed devices and APs in a cluster in real time network upgrade where managed devices and APs upgrade automatically without any planned maintenance downtime. You can also schedule an upgrade to a specified time to avoid manual intervention.

Here we'll upgrade the cluster from 8.6.0.7 to 8.7.1.1



The screenshots illustrate the process of upgrading a Lab-Cluster from version 8.6.0.7 to 8.7.1.1. The interface shows the following steps:

- Initial State:** The 'Controllers And Clusters' table shows the Lab-Cluster (2) with a current version of 8.6.0.7.28215. The 'AP Preload Image' tab is selected.
- Upgrading:** The 'When' field is set to 'Now'. The 'Server IP address' is 192.168.1.122, 'Protocol' is FTP, 'Username' is user1, and 'Password' is masked. The 'Software to install' field is 8.7.1.1_78245. The 'Install' button is visible.
- Progress:** The 'CURRENT VERSION' for the Lab-Cluster is now 'Installation in progress'. The 'AP Preload Image' tab is selected. A 'Cluster Installation Status' box shows the status for two devices:
 - 7008-2: Image Copy In Progress
 - 7008-1: Not In ProgressA note indicates the installation started 1 minute ago.

Managed Network >

Dashboard Configuration Maintenance Software Management

Controllers And Clusters AP Preload Image

Controllers/Clusters 1

NAME	CURRENT VERSION	ACCESS POINTS	GROUP
Lab-Cluster (2)	Installation in progress	2	/md/Lab

Cluster Installation Status

- 7008-2 Image Copy Success
- 7008-1 Image Copy In Progress

INSTALLATION SETTINGS

When: Now Later

Show Details Installation has started 4 minutes ago

Specify image file location, name and protocol to use for transfer

aruba MOBILITY MASTER Aruba-MM1

CONTROLLERS: 1 (1 Green, 0 Yellow, 0 Red) ACCESS POINTS: 2 (2 Green, 0 Yellow, 0 Red) CLIENTS: 2 ALERTS: 0

admin

Managed Network >

Dashboard Configuration Maintenance Software Management

Controllers And Clusters AP Preload Image

Controllers/Clusters 1

NAME	CURRENT VERSION	ACCESS POINTS	GROUP
Lab-Cluster (2)	Installation in progress	2	/md/Lab

Cluster Installation Status

- 7008-2 Reboot In Progress
- 7008-1 Image Copy Success

INSTALLATION SETTINGS

When: Now Later

Show Details Installation has started 10 minutes ago

Specify image file location, name and protocol to use for transfer

You can click on the “show details”



Access Points (2)					
Name	IP Address	Mac Address	Ap Group	Target Contr...	Status
20:4c:03:5c:05:6e	10.10.10.20	20:4c:03:5c:05:6e	Building1	192.168.1.58	Not In Progress
20:4c:03:17:a0:4c	10.10.10.21	20:4c:03:17:a0:4c	Building1	192.168.1.58	Not In Progress

50 < 1 >

Close

aruba MOBILITY MASTER Aruba-MM1

CONTROLLERS 2 / 0 ACCESS POINTS 2 / 0 CLIENTS 2 / 0 ALERTS 0

admin

Managed Network > Lab (2)

Dashboard Configuration Maintenance Software Management

Controllers And Clusters AP Preload Image

Controllers/Clusters 1

NAME	CURRENT VERSION	ACCESS POINTS	GROUP
Lab-Cluster (2)	Installation in progress	2	/md/Lab

Cluster Installation Status

7008-2 Upgrade Complete, AP Move in Progress

7008-1 Image Copy Success

INSTALLATION SETTINGS

When: Now Later

Show Details Installation has started 16 minutes ago

You can also follow the upgrade status from the services tab

aruba MOBILITY MASTER Aruba-MM1

CONTROLLERS 1 / 1 ACCESS POINTS 2 / 0 CLIENTS 2 / 0 ALERTS 0

admin

Managed Network > Lab >

Dashboard Configuration Services

Clusters AirGroup VPN Firewall IP Mobility External Services DHCP WAN

Upgrade Status for cluster Lab-Cluster Status: In Progress

Controllers Status Summary Access Point Status Summary

Controllers 2

NAME	IP ADDRESS	MAC ADDRESS	STATUS
7008-2	192.168.1.58	20:4c:03:0ab9:60	Reboot In Progress
7008-1	192.168.1.57	20:4c:03:0ab9:c0	Image Copy Success

aruba MOBILITY MASTER Aruba-MM1

CONTROLLERS 2 / 0 ACCESS POINTS 2 / 0 CLIENTS 0 / 0 ALERTS 0

admin

Managed Network > Lab >

Dashboard Configuration Services

Clusters AirGroup VPN Firewall IP Mobility External Services DHCP WAN

Clusters (1)

NAME	CONTROLLERS	FIRMWARE VERSION	UPGRADE STATUS
Lab-Cluster	2	8.7.11_78245	Completed

aruba MOBILITY MASTER Aruba-MM1

CONTROLLERS 2 0 ACCESS POINTS 2 0 CLIENTS 0 ALERTS 0

admin

Managed Network > Lab >

Dashboard Configuration

WLANS Roles & Policies Access Points AP Groups Authentication Services

Interfaces Controllers System Tasks Redundancy IoT Maintenance

Lab (2)

7008-1 7008-2

Clusters AirGroup VPN Firewall IP Mobility External Services DHCP WAN

Upgrade Status for cluster Lab-Cluster Status: Completed

Controllers Status Summary

Category	Value
Not in Progress	0
Image Copy in Progress	0
Image Copy Success	0
Image Copy Fail	0
Reboot in Progress	0
Reboot Fail	0
Upgraded Out of Sequence	0
Upgraded, AP Move in Progress	0
Upgrade Success	2

Access Point Status Summary

Category	Value
Not in Progress	0
Image Preload in Progress	0
Image Preload Success	0
Image Preload Fail	0
Move with Reboot in Progress	0
Upgrade Success	2
Upgrade Fail	0
Upgrade Skipped for Mesh APs	0

Controllers

NAME	IP ADDRESS	MAC ADDRESS	STATUS
7008-1	192.168.1.57	20:4c:03:0a:b9:e0	Upgrade Success
7008-2	192.168.1.58	20:4c:03:0a:b9:e0	Upgrade Success

The procedure for upgrade and downgrade is exactly the same. The important thing to note is that MM's firmware version should always be either the same or higher than the version on your MDs.