

Contents

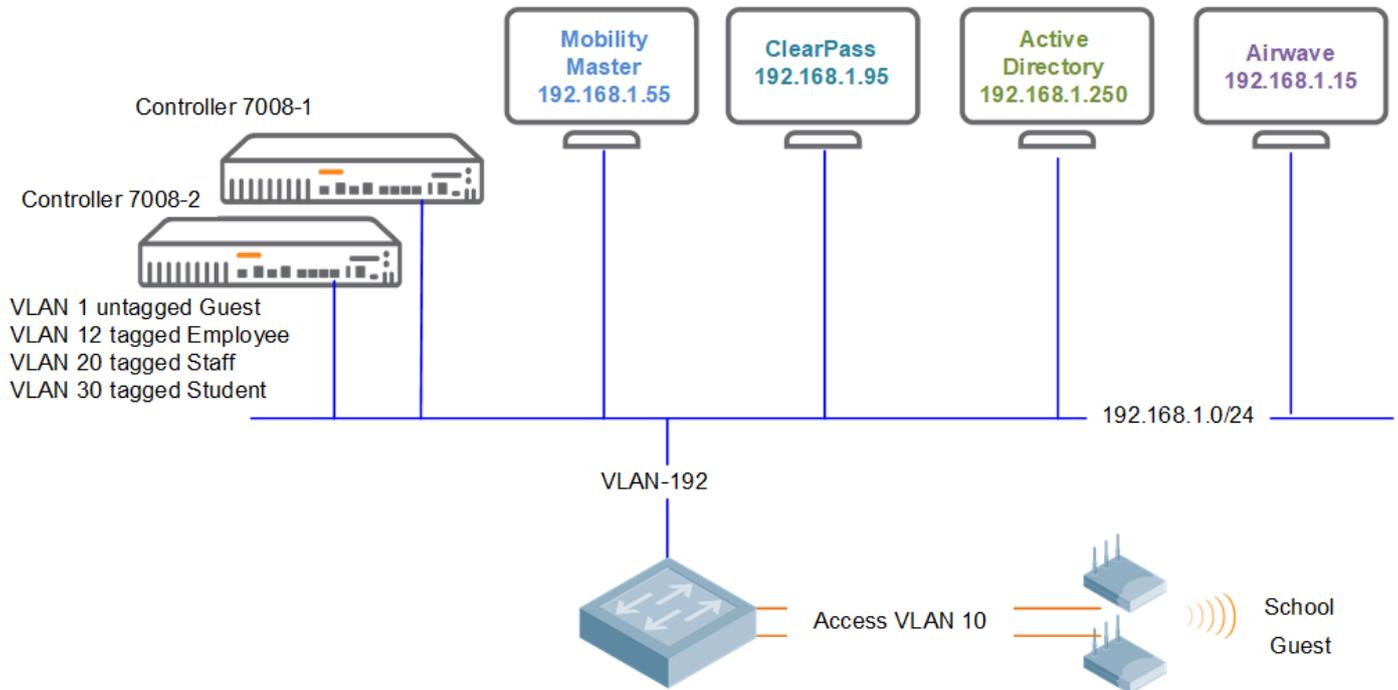
1.1	Revision History	1
2	Demo Topology	2
11	Airwave Configuration	3
11.1	Basic Configuration	3
11.2	VisualRF	8
11.3	Triggers and Alerts	12
12	MD Clustering.....	15
12.1	Cluster Configuration	15
12.2	Cluster Monitoring with Airwave	19
12.3	AP Node List	20
12.4	Live Cluster Upgrade.....	22

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 3 of the three parts series guide.

11 Airwave Configuration

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

11.1 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.

Refer to your license agreement for complete information about the terms of this license. [View the End User License Agreement](#)
Contact Aruba Technical Support at 1-800-943-4526 (800-WIFI-LAN) or 1-408-754-1200 (International Toll) or <http://hpe.com/support/hpesc>

Summary

Type: AMP

Days Remaining: 365

Approved Devices: 0

Max. Device Count: 10

Licenses

ORGANIZATION	IP ADDRESS	DAYS REMAINING	EXPIRATION
Ariya-Lab		365	2/8/22, 1:11

Please add new license

```
--- Begin AirWave License Key ---  
Organization: Ariya-Lab  
Product: AMP  
Package: LIC-AW  
Age: 10  
RAPIDS: Yes  
VisualRF: Yes  
Expires: 1644286581  
Expires_on: Tue Feb 8 02:16:21 2022  
Serial: W000000000  
Generated: Mon Feb 8 02:16:21 2021 UTC  
--- Signature ---  
iEYEAReCAAYFAMagnvUACgkQvN8PdJTRKs2GEnACfUyhMdoF2ipSzjMq1Sc1qXept  
WBSAoJDTUy0jdQz6LDZ6G2Fapjpp4tm  
~/szf  
--- End AirWave License Key ---
```

Add **Delete**

Expiry Notification

Ensure you have the correct IP addressing and NTP configured.

Primary Network Interface

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

IPv6 Enabled: Yes No
If you enable IPv6 you also need to run 'apply_ipv6' in AMPCLI EnterCommands.

Primary DNS IP Address: 192.168.1.130

Secondary DNS IP Address: 1.1.1.1

Network Time (NTP)

Enable NTP Authentication: Yes No

Primary NTP Server: 216.239.35.4

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: <small>Leave name blank to read it from device</small>	<input type="text" value="Aruba-MM1"/>
IP Address:	<input type="text" value="192.168.1.55"/>
SNMP Port:	<input type="text" value="161"/>
SSH Port:	<input type="text" value="22"/>
Community String:	<input type="text" value="*****"/>
Confirm Community String:	<input type="text" value="*****"/>
SNMPv3 Username:	<input type="text" value="Enter a Value"/>
Auth Password:	<input type="text"/>
Confirm Auth Password:	<input type="text"/>
SNMPv3 Auth Protocol:	<input type="text" value="SHA-1"/>
Privacy Password:	<input type="text"/>
Confirm Privacy Password:	<input type="text"/>
SNMPv3 Privacy Protocol:	<input type="text" value="AES"/>
Telnet/SSH Username:	<input type="text" value="admin"/>
Telnet/SSH Password:	<input type="text" value="*****"/>
Confirm Telnet/SSH Password:	<input type="text" value="*****"/>
"enable" Password:	<input type="text" value="*****"/>
Confirm "enable" Password:	<input type="text" value="*****"/>

Location

Group:	<input type="text" value="Access Points"/>
Folder:	<input type="text" value="Top"/>
<input type="checkbox"/> Update group settings based on this device's current configuration	
<input checked="" type="radio"/> Monitor Only (no changes will be made to device)	
<input type="radio"/> Manage read/write (group settings will be applied to device)	
<input type="button" value="Add"/> <input type="button" value="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: Group: Folder: Management Level:

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

DEVICES	TYPE	LAN MAC ADDRESS	IP ADDRESS	DISCOVERED	CONTROLLER	FOLDER	GROUP	ARUBA AP GROUP	DISCOVERY METHOD	SERIAL NUMBER	DEVICE STATE
<input checked="" type="checkbox"/> (id: 2)	Aruba Device	-	192.168.1.57	2/8/21, 1:58 PM	-	-	Access Points	-	SNMP	CNDRJSP06J	-
<input checked="" type="checkbox"/> (id: 3)	Aruba Device	-	192.168.1.58	2/8/21, 1:58 PM	-	-	Access Points	-	SNMP	CNDRJSP06L	-

25 per page Page: 1

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

<p>Name: Status: Configuration: Last Contacted: Type: Firmware: Group: Template: Folder: Management Mode: Enable Planned Downtime Mode:</p>	<p>(id: 3) Down (SNMP get failed) Unknown (Settings not yet read from device) Never Aruba Device unknown Controllers Add a Template Top <input checked="" type="radio"/> Monitor Only <input type="radio"/> Manage Read/Write <input type="radio"/> Yes <input checked="" type="radio"/> No</p>
--	--

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:	<input type="text" value="192.168.1.58"/>
SNMP Port (1-65535):	<input type="text" value="161"/>
SSH Port (1-65535):	<input type="text" value="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:	<input type="text" value="....."/>
Confirm Community String:	<input type="text" value="....."/>
SNMPv3 Username:	<input type="text" value="Enter a Value"/>
Auth Password:	<input type="text"/>
Confirm Auth Password:	<input type="text"/>
SNMPv3 Auth Protocol:	<input type="text" value="SHA-1"/>
Privacy Password:	<input type="text"/>
Confirm Privacy Password:	<input type="text"/>
SNMPv3 Privacy Protocol:	<input type="text" value="AES"/>
Telnet/SSH Username:	<input type="text" value="admin"/>
Telnet/SSH Password:	<input type="text" value="....."/>
Confirm Telnet/SSH Password:	<input type="text" value="....."/>
"enable" Password:	<input type="text" value="....."/>
Confirm "enable" Password:	<input type="text" value="....."/>

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	XXXXXXXXXX	➔	XXXXXXXXXX
Telnet/SSH Password	XXXXXXXXXX	➔	XXXXXXXXXX

Scheduling Options

Occurs:

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:

Home

Groups

Devices

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

Folder: Top (3 Devices) Expand folders to show all Devices

Go to folder: Top (3 Devices)

TOTAL DEVICES: 3 ↑ 3 ↓ 0 MISMATCHED: 0 CLIENTS: 0 USAGE: - VPN SESSIONS: 0

2h 1d 1w 1y

Clients Sources Max Avg Usage Sources Max Avg

DEVICES LIST

Default View: Devices [Total Row Count: 3]

DEVICE	STATUS	CONFIGURATION	CONTROLLER	FOLDER	GROUP	CLIENTS	APS	USAGE	IP ADDRESS	TYPE	CONDUCTOR CONTROLLER	SWITCH ROLE
7008-1	Up	Good	-	Top	Controllers	0	0	0 bps	192.168.1.57	Aruba 7008	Aruba-MM1	-
7008-2	Up	Good	-	Top	Controllers	0	0	0 bps	192.168.1.58	Aruba 7008	Aruba-MM1	-
Aruba-MM1	Up	Good	-	Top	Access Points	0	0	0 bps	192.168.1.55	Aruba MM-VA	-	-

25 per page Page: 1 Go

Alert Summary updated at 2/8/2021 2:36 PM AEDT

TYPE	LAST 2 HOURS	LAST DAY	TOTAL	LAST EVENT
AMP Alerts	0	0	0	-
IDS Events	0	0	0	-
RADIUS Accounting Issues	0	0	0	-
RADIUS Authentication Issues	0	0	0	-

Add New Folder

Then the APs will be automatically discovered from the controllers

aruba | AirWave NEW DEVICES UP 3 DOWN 0 ROGUE 0 CLIENTS 0 ALERTS 0 Log out admin

Home

Groups

Devices

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

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]

DEVICE	TYPE	LAN MAC ADDRESS	IP ADDRESS	DISCOVERED	CONTROLLER	FOLDER	GROUP	ARUBA AP GROUP	DISCOVERY METHOD	SERIAL N
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	-

Home

Groups

Devices

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

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]

DEVICE	TYPE	LAN MAC ADDRESS	IP ADDRESS	DISCOVERED	CONTROLLER	FOLDER	GROUP	ARUBA AP GROUP	DISCOVERY METH
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

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

aruba | AirWave NEW DEVICES UP 4 DOWN 0 ROGUE 4 CLIENTS 2 ALERTS 24 Days Remaining: 362

Home

Overview

Traffic Analysis

UCC

RF Performance

RF Capacity

AirMatch

Clarity

Topology

Mesh

Network Deviations

Documentation

License

User Info

Groups

Devices

Clients

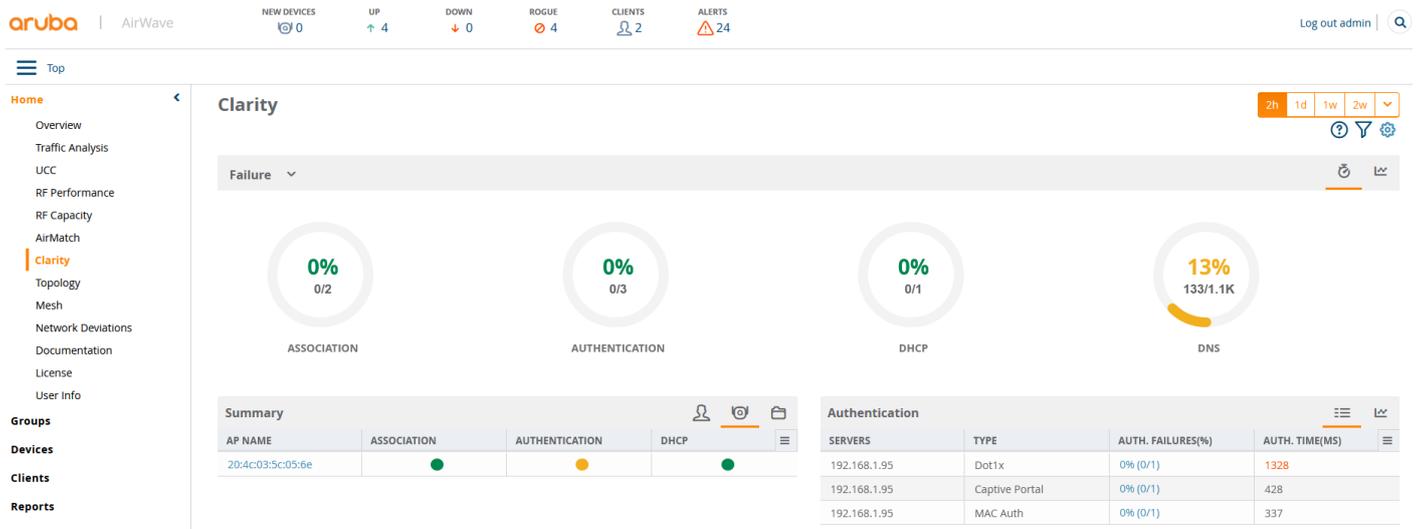
AirWave Management Platform 8.2.12.0

AW-Lab - Ariya-Lab

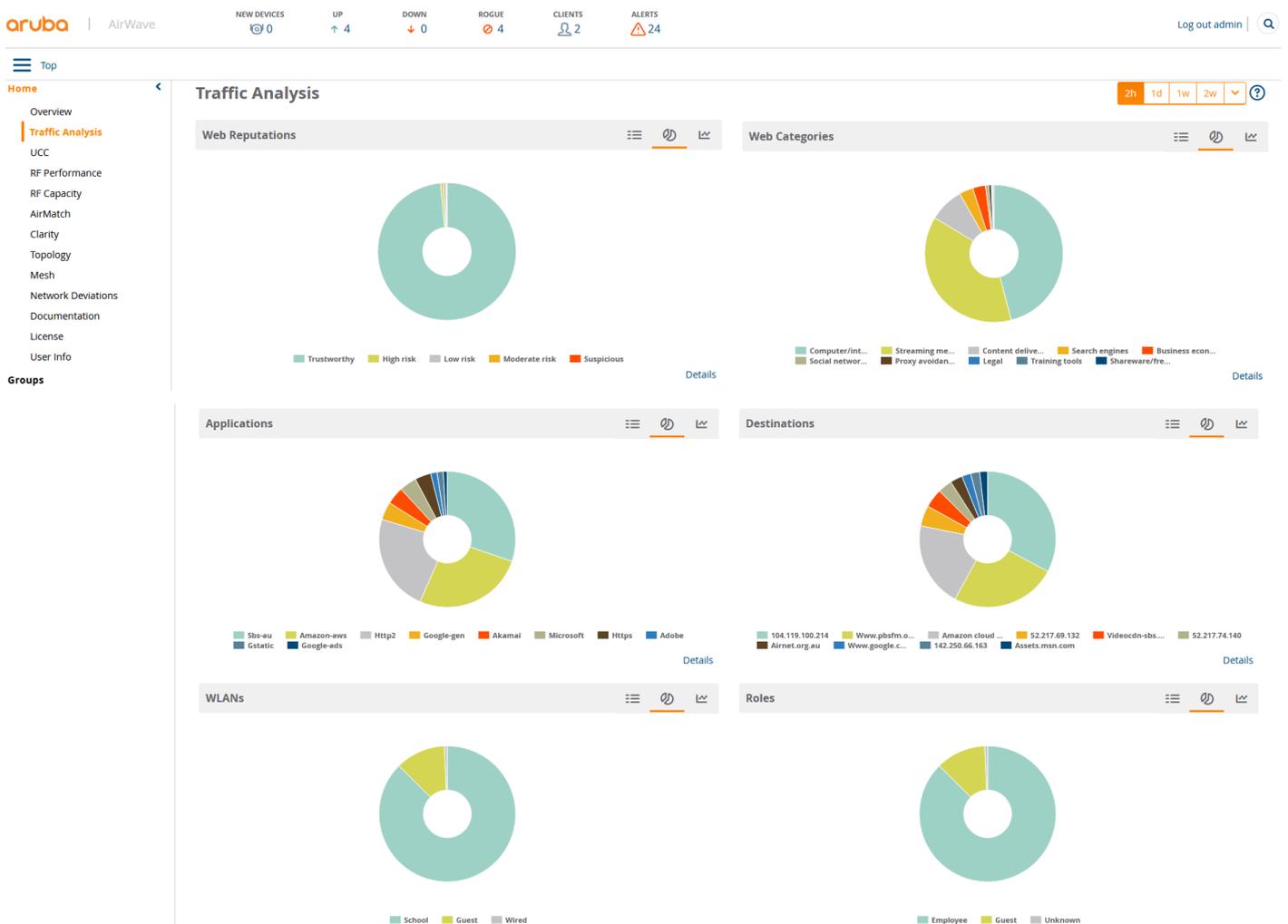
2h 1d 1w 1y

Clients Sources Max Avg Usage Sources Max Avg

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.

11.2 VisualRF

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

aruba | AirWave

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

Home

Groups

Devices

Clients

Reports

System

Device Setup

AMP Setup

RAPIDS

VisualRF

Floor Plans

Setup

Import

Audit Log

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

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

Home

Groups

Devices

Clients

Reports

System

Device Setup

AMP Setup

RAPIDS

VisualRF

Floor Plans

Setup

Import

Audit Log

Network | Map | List | Locate

Default Campus

Network

Properties View **Edit**

Actions

Select All

Undo

New Floorplan

Set Background

New Campus

Auto-arrange Campuses

Meters Feet

aruba | AirWave

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

Home

Groups

Devices

Clients

Reports

System

Device Setup

AMP Setup

RAPIDS

VisualRF

Floor Plans

Setup

Import

Audit Log

Network | Map | List | Locate

Default Campus

New Floorplan

Floorplan file: Sample-floor-plan.JPG

Campus: Default Campus

Building: Default Building

Floor name: Floor 1

Floor number: 1.0

Save Cancel

Network

Properties View **Edit**

Actions

Select All

Undo

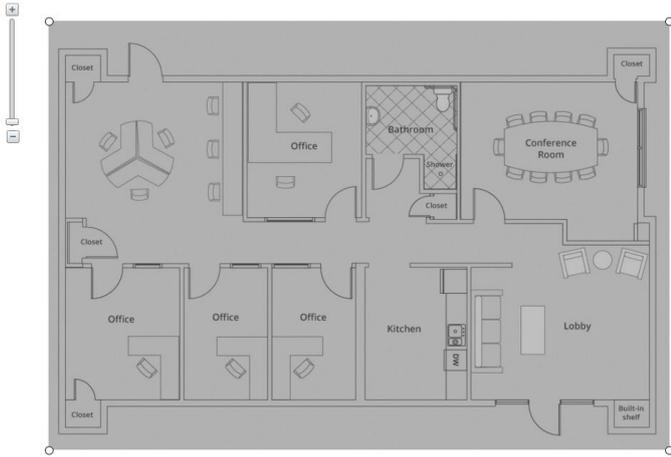
New Floorplan

Set Background

New Campus

Auto-arrange Campuses

Meters Feet



Define New Floor

- 1 Scale
- 2 Region
- 3 CAD Layer
- 4 Access Points

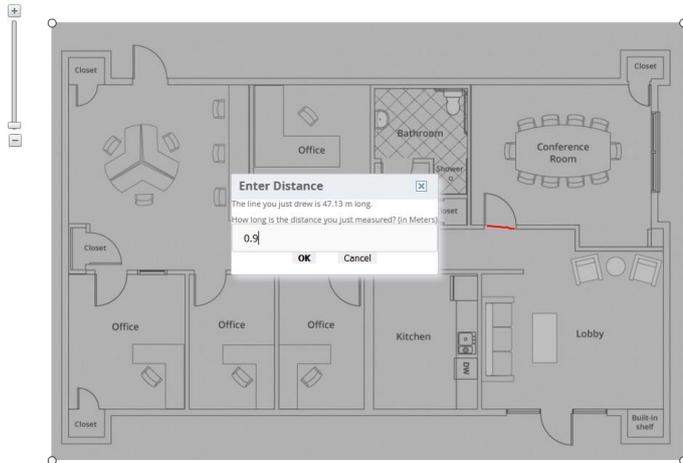
Floor Plan Dimensions

Measure

Width: 980.000 m

Height: 682.000 m

Next Finish



Define New Floor

- 1 Scale
- 2 Region
- 3 CAD Layer
- 4 Access Points

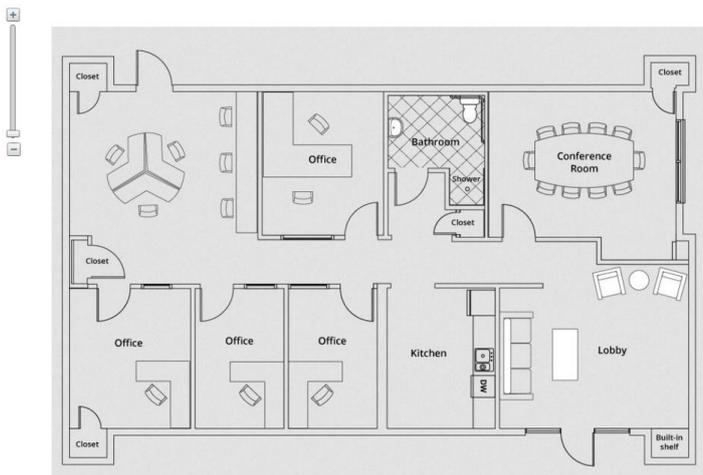
Floor Plan Dimensions

Measure

Width: 980.000 m

Height: 682.000 m

Next Finish



Define New Floor

- 1 Scale
- 2 Region
- 3 CAD Layer
- 4 Access Points

Do you want to plan your AP deployment, or add APs that are already deployed?

Plan APs

Add deployed APs

Deployed APs

Drag & Drop individual APs or entire folder

By Group

Search

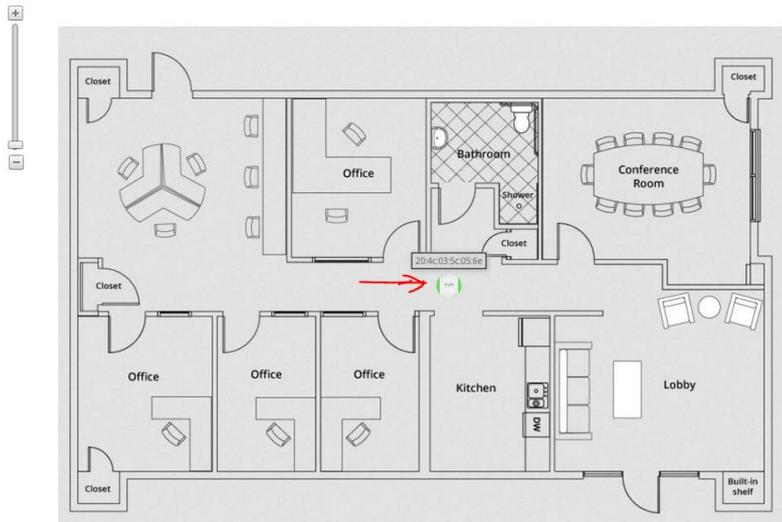
Access Points

- 204c033c058

Hide APs that are already added

Previous Finish

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



Define New Floor

- 1 Scale
- 2 Region
- 3 CAD Layer
- 4 Access Points

Do you want to plan your AP deployment, or add APs that are already deployed?

Plan APs

Add deployed APs

Deployed APs
Drag & Drop individual APs or entire folder

By Group

Access Points

Hide APs that are already added

Previous Finish

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



Concrete

Properties View Edit

Drawing

- Draw Region
- Draw Wall

Actions

- Select All
- Remove

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



Concrete

Properties View Edit

Wall

Material

Attenuation 15 dB

Save Cancel

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.

- Home
- Groups
- Devices
- Clients
- Reports
- System
- Device Setup
- AMP Setup
- RAPIDS
- VisualRF
- Floor Plans
- Setup
- Import
- Audit Log

- Home
- Groups
- Devices
- Clients
- Reports
- System
- Device Setup
- AMP Setup
- RAPIDS
- VisualRF
- Floor Plans
- Setup
- Import
- Audit Log

You can then do the same thing with the campus background

- Home
- Groups
- Devices
- Clients
- Reports
- System
- Device Setup
- AMP Setup
- RAPIDS
- VisualRF
- Floor Plans
- Setup
- Import
- Audit Log

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

Network > Default Campus > Library | Map List | Locate



Floor 1
 Properties View Edit
Devices
 APs/Switch/Generic Marker
 Clients
 Interferers
 Rogues
 Tags
Client Overlays
 Client Health
 Traffic Analysis
 UCC
AP Overlays
 Ch. Utilization
 Channel
 Heatmap
 Speed
 Voice
Relation Lines
 APs/Switch/Generic Marker
 Client Association
 Client Neighbors
 Interferers
 Rogues
 Surveys

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



Floor 1
 Properties View Edit
Devices
 APs/Switch/Generic Marker
 Clients
 Interferers
 Rogues
 Tags
Client Overlays
 Client Health
 Traffic Analysis
 UCC
AP Overlays
 Ch. Utilization
 Channel
 Heatmap
 Speed
 Voice
Relation Lines
 APs/Switch/Generic Marker
 Client Association
 Client Neighbors
 Interferers
 Rogues

11.3 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

Status Syslog & Traps Event Log Triggers Alerts Backups Configuration Change Jobs Firmware Upgrade Jobs DRT Upgrade Jobs Performance Download Log Files

Add New Trigger

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 S...	-	-	-	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
e.g. '15 minutes', '75 seconds', '1 hr 15 mins'

Conditions

Matching conditions: All Any

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 No

Group: - All Groups -

Alert Notifications

And you can combine any of the trigger type

Trigger

Type: Device Down

Severity: Warning

Limit by number of events: 1

Send Alerts for Thin APs when Controller is Down:

Send Alerts when Upstream Device is Down:

Send Alerts on Reboot:
Include reboots detected by uptime reset or reboot count increase

Conditions

Matching conditions: All Any

Add New Trigger Condition

Trigger Restrictions

Folder: Top

Include Subfolders: Yes No

Group: - All Groups -

- Devices**
- Device Down
- Device Up
- Configuration Mismatch
- AP Usage
- Device Resources
- Device Event
- Device Uplink Status
- AP Uplink Speed
- Controller Cluster Trigger
- Interfaces/Radios**
- Radio Down
- Radio Up
- 802.11 Frame Counters
- 802.11 QoS Counters
- Interface Usage
- Interface Errors
- Channel Utilization
- Radio Noise Floor
- Channel Change

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 No

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.

Trigger

Type: Client RADIUS Authentica

Severity: Minor

Duration: 15 mins
e.g. '15 minutes', '75 seconds', '1 hr 15 mins'

Conditions

Matching conditions: All Any

Add New Trigger Condition

OPTION	CONDITION	VALUE
Count	>=	<input type="text" value="10"/>

Trigger Restrictions

Folder: Top

Include Subfolders: Yes No

Group: - All Groups -

Alert Notifications

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.

Trigger

Type: Device Event

Severity: Normal

Conditions

Matching conditions: All Any

Add New Trigger Condition

OPTION	CONDITION	VALUE
Event Contents	matches	<input type="text" value="Radar"/>

Trigger Restrictions

Folder: Top

Include Subfolders: Yes No

Group: - All Groups -

Alert Notifications

12 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.

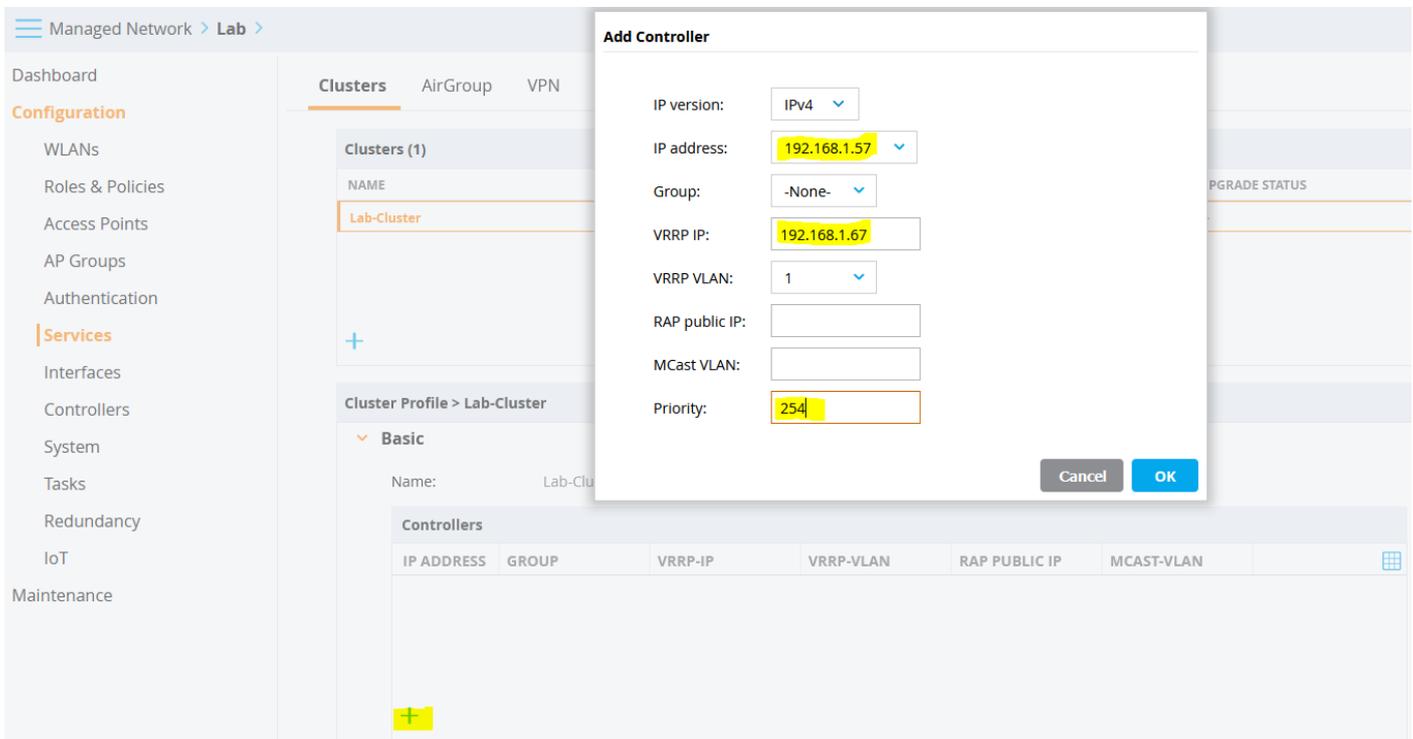
The aims of clustering are

- 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.

12.1 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.



And we'll add the second MD as well

Add Controller

IP version:

IP address:

Group:

VRRP IP:

VRRP VLAN:

RAP public IP:

MCast VLAN:

Priority:

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

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:

Exclude VLANs:

Managed Network > Lab > 7008-2 Version 8.6.0.7

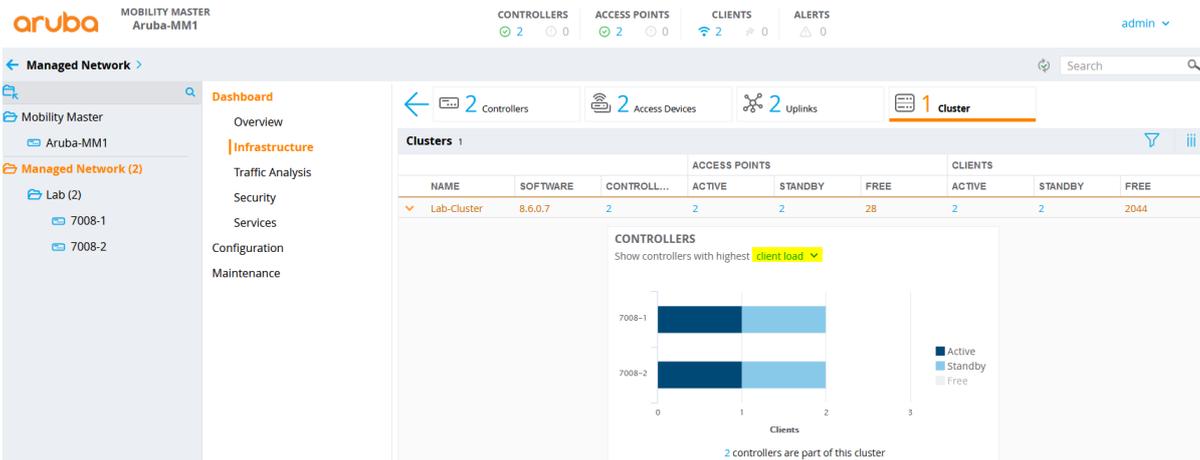
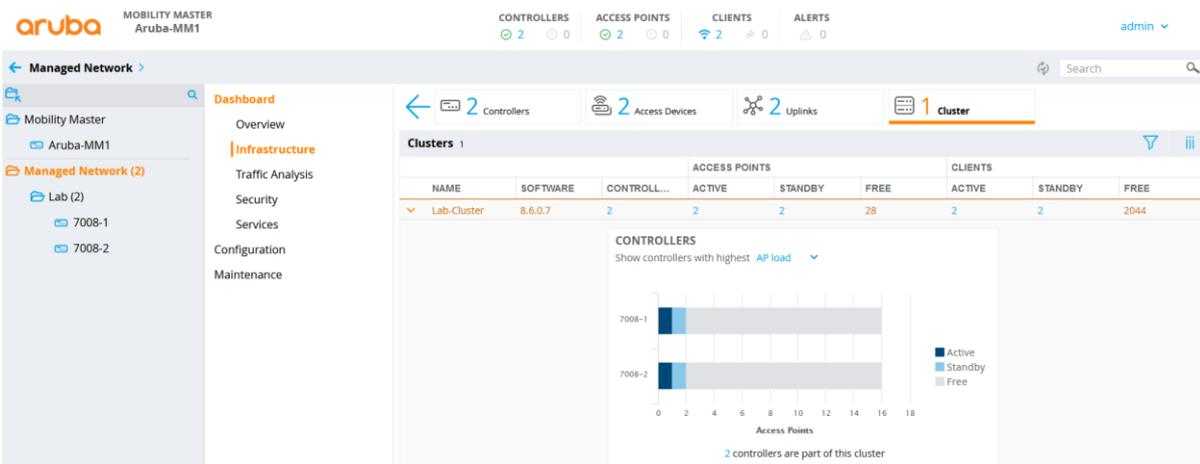
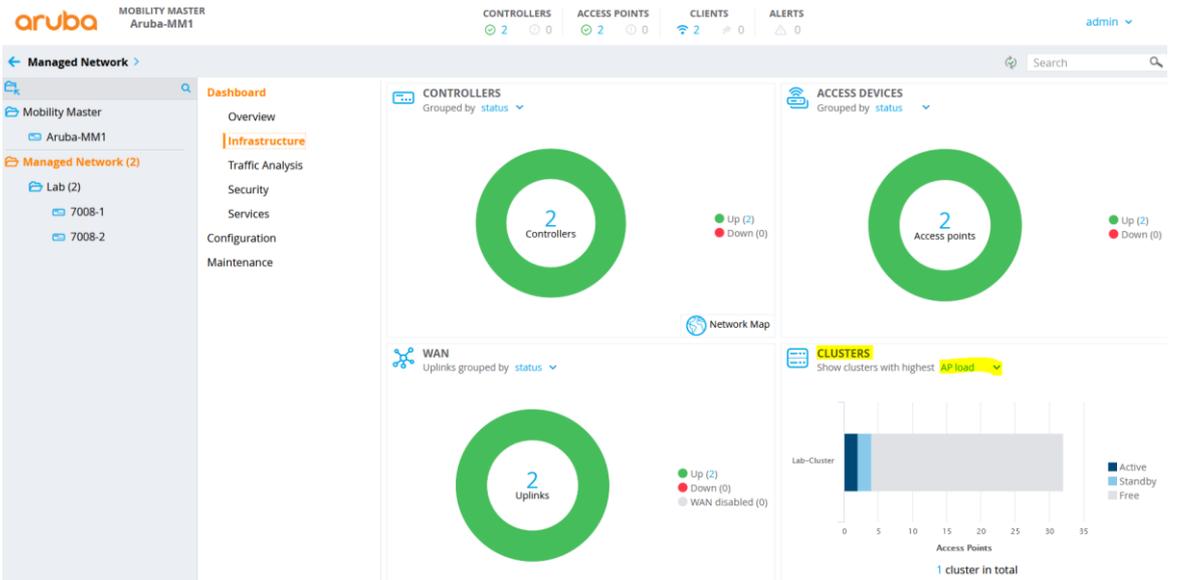
Clusters AirGroup VPN Firewall IP Mobility External Services DHCP WAN

Cluster Profile

Cluster group-membership:

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) #  
(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.

Configuration » Network » Devices

Network Devices

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

Filter: Name contains [] Go Clear Filter Show 20 records

#	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	

Showing 1-5 of 5

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.

[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	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

12.2 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 1 UP 4 DOWN 0 ROGUE 6 CLIENTS 2 ALERTS 24 Log out admin

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 Control...	Mobility Ma...	ACTION
Lab-Cluster		2	2	●	●	●	8.6.0.7	14	POSSIBLE	1	Aruba-MM1	Delete

Clicking on the "Lab-Cluster".

aruba | AirWave

NEW DEVICES 1 UP 4 DOWN 0 ROGUE 6 CLIENTS 2 ALERTS 24 Log out admin

Controller Clusters > Cluster Monitoring (Lab-Cluster)

2h 1d 1w 2w

AP Capacity

Client Capacity

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

12.3 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
mtddevname=aos0
mtddevnum=0
mtdids=nand0=nand0
mtdparts=mtdparts=nand0:0x2000000@0x0 (aos0),0x2000000@0x2000000 (aos1),0x4000000@0x4000000 (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_ethernet=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>
```

12.4 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 screenshot shows the Aruba Mobility Master interface. At the top, there are status indicators for CONTROLLERS (2), ACCESS POINTS (2), CLIENTS (2), and ALERTS (0). The user is logged in as 'admin'. The main navigation pane on the left shows 'Managed Network (2)' with sub-items 'Lab (2)', '7008-1', and '7008-2'. The main content area is titled 'Controllers And Clusters' and 'AP Preload Image'. It features a table with the following data:

NAME	CURRENT VERSION	ACCESS POINTS	GROUP
Lab-Cluster (2)	8.6.0.7_78215	2	/md/Lab

Below the table, there are 'INSTALLATION SETTINGS' including 'When' (set to 'Now'), 'Specify image file location, name and protocol to use for transfer', 'Use upgrade profile' (disabled), 'Server IP address' (192.168.1.122), 'Image path' (.), 'Protocol' (FTP), 'Username' (user1), 'Password' (masked), and 'Software to install' (8.7.1.1_78245). 'Cancel' and 'Install' buttons are at the bottom right.

This screenshot shows the same 'AP Preload Image' configuration screen after the upgrade process has begun. The table now shows the status of the cluster:

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

The 'INSTALLATION SETTINGS' section remains the same as in the previous screenshot.

This screenshot shows the 'Cluster Installation Status' dialog box overlaid on the configuration screen. The dialog provides a detailed view of the upgrade progress for each device in the cluster:

- 7008-2: Image Copy In Progress
- 7008-1: Not In Progress

At the bottom of the dialog, it states 'Installation has started 1 minutes ago' and includes a 'Show Details' link. The background configuration screen is partially visible behind the dialog.

Managed Network >

Dashboard
Configuration
Maintenance
Software Management

Controllers And Clusters AP Preload Image

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

[Show Details](#) Installation has started 4 minutes ago

INSTALLATION SETTINGS
When: Now Later

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

aruba MOBILITY MASTER Aruba-MM1

CONTROLLERS: 1 (green), 1 (yellow) | ACCESS POINTS: 2 (green), 0 (grey) | CLIENTS: 2 (green), 0 (grey) | ALERTS: 0 (grey)

Managed Network >

Dashboard
Configuration
Maintenance
Software Management

Controllers And Clusters AP Preload Image

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

[Show Details](#) Installation has started 10 minutes ago

INSTALLATION SETTINGS
When: Now Later

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

You can click on the “show details”

Installation Status

Access Points 2

Controllers 2

NAME	IP ADDRESS	MAC ADDRESS	STATUS
7008-2	192.168.1.58	20:4c:03:0a:b9:e0	Reboot In Progress
7008-1	192.168.1.57	20:4c:03:0a:b9:c0	Image Copy Success

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 ACCESS POINTS 2 CLIENTS 2 ALERTS 0

Managed Network >

Dashboard Configuration Maintenance Software Management

Controllers And Clusters AP Preload Image

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

Show Details Installation has started 16 minutes ago

INSTALLATION SETTINGS
When: Now Later

You can also follow the upgrade status from the services tab

aruba MOBILITY MASTER Aruba-MM1

CONTROLLERS 1 ACCESS POINTS 2 CLIENTS 2 ALERTS 0

Managed Network > Lab >

Dashboard Configuration Services Interfaces Controllers System Tasks

Clusters AirGroup VPN Firewall IP Mobility External Services DHCP WAN

Upgrade Status for cluster Lab-Cluster Status: In Progress

Controllers Status Summary 2

NAME	IP ADDRESS	MAC ADDRESS	STATUS
7008-2	192.168.1.58	20:4c:03:0a:b9:e0	Reboot In Progress
7008-1	192.168.1.57	20:4c:03:0a:b9:c0	Image Copy Success

Access Point Status Summary 2

aruba MOBILITY MASTER Aruba-MM1

CONTROLLERS 2 ACCESS POINTS 2 CLIENTS 0 ALERTS 0

Managed Network > Lab >

Dashboard Configuration Services Interfaces

Clusters AirGroup VPN Firewall IP Mobility External Services DHCP WAN

NAME	CONTROLLERS	FIRMWARE VERSION	UPGRADE STATUS
Lab-Cluster	2	8.7.1.1_78245	Completed

Managed Network > Lab >

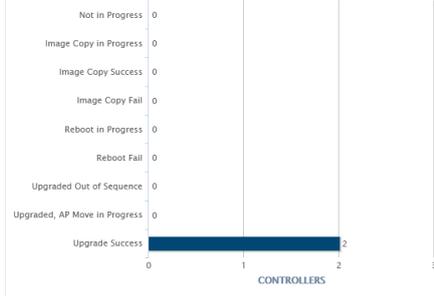
- Dashboard
- Configuration
 - WLANs
 - Roles & Policies
 - Access Points
 - AP Groups
 - Authentication
- Services
 - Interfaces
 - Controllers
 - System
 - Tasks
 - Redundancy
 - IoT
- Maintenance

Clusters AirGroup VPN Firewall IP Mobility External Services DHCP WAN

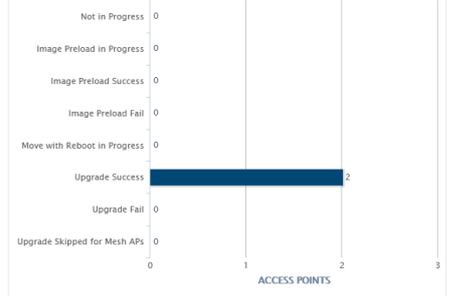
Upgrade Status for cluster Lab-Cluster

Status: **Completed**

Controllers Status Summary 2



Access Point Status Summary 2



Controllers 2

NAME	IP ADDRESS	MAC ADDRESS	STATUS
7008-1	192.168.1.57	20:4c:03:0a:b9:c0	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.