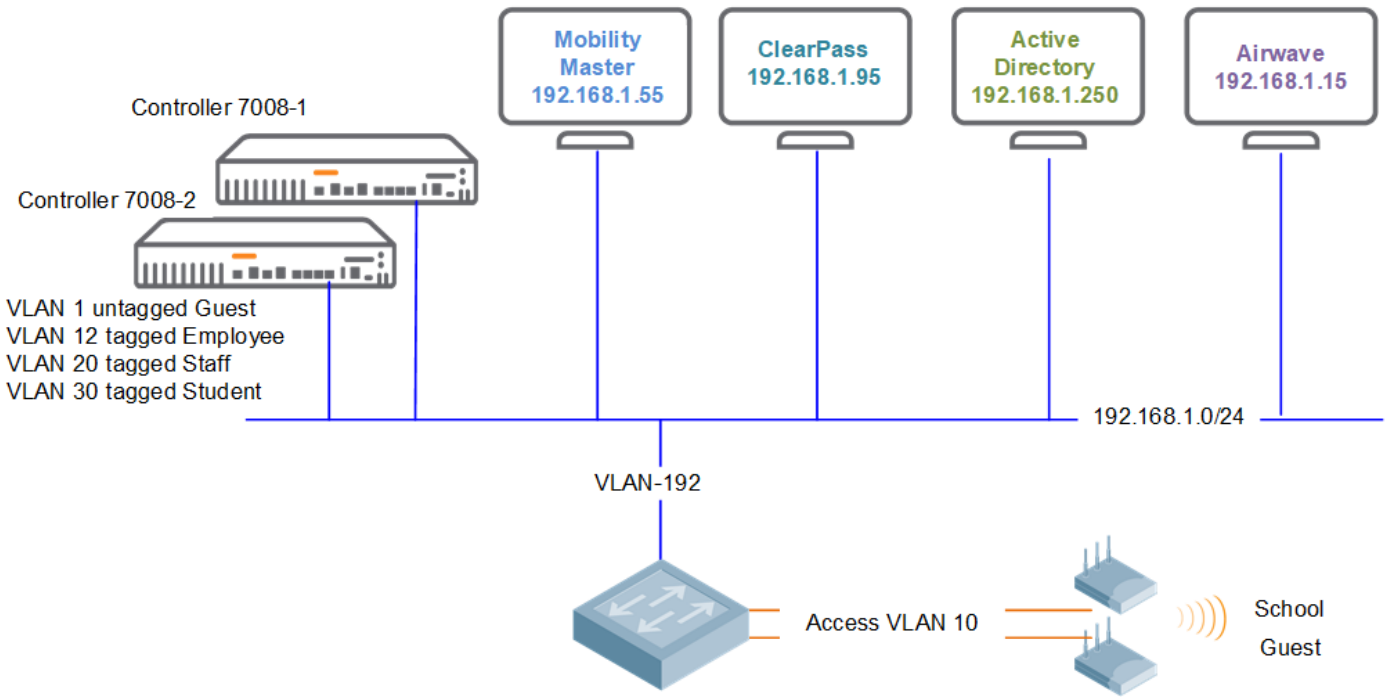
Contents

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.



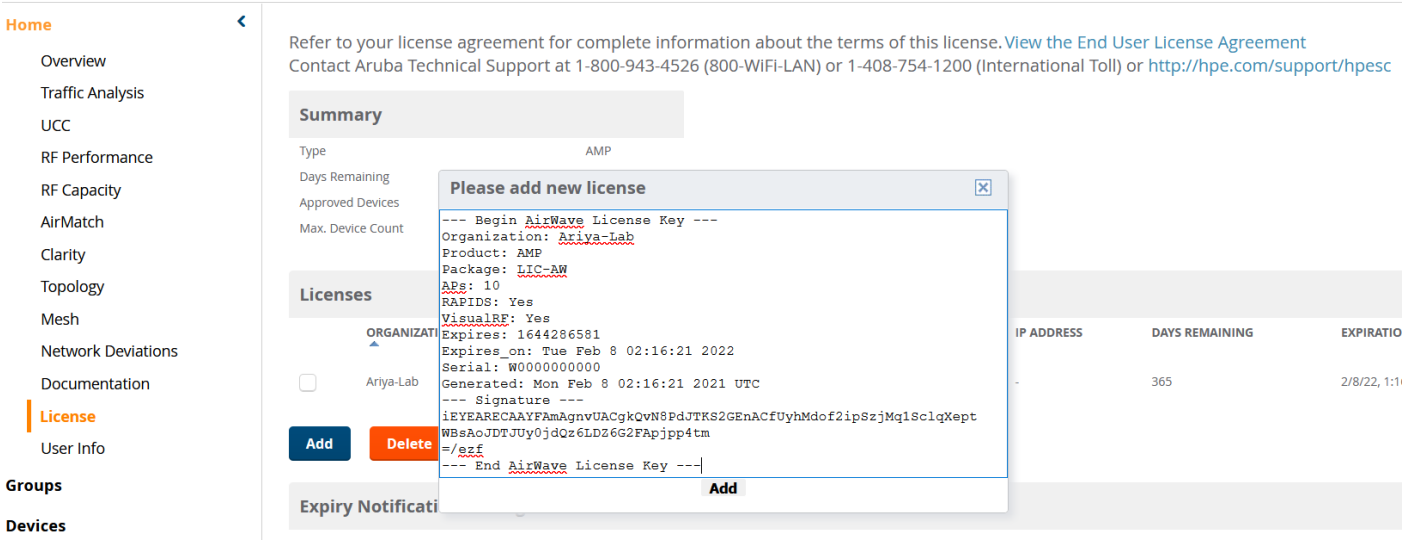
This is the part 3 of the three parts series guide.

11 Airwave Configuration

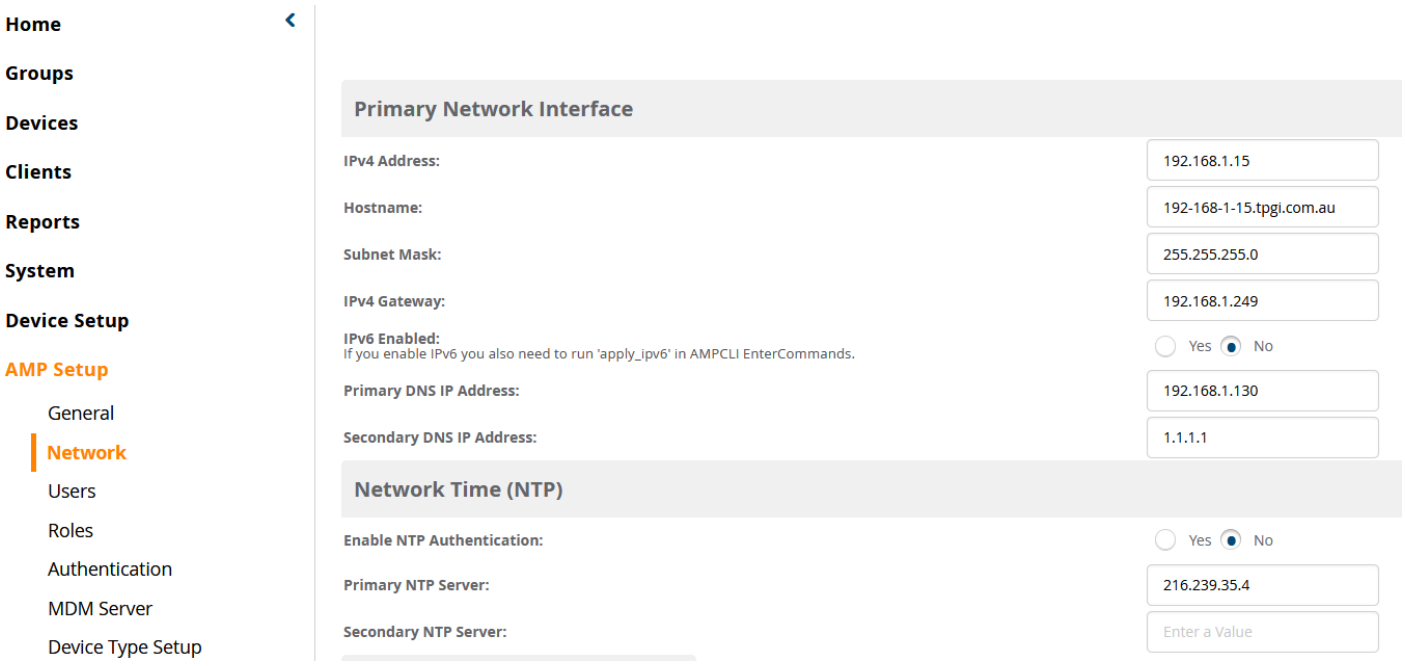
Once Airwave (AW) is installed, you can browse to its IP address.

11.1 Basic Configuration

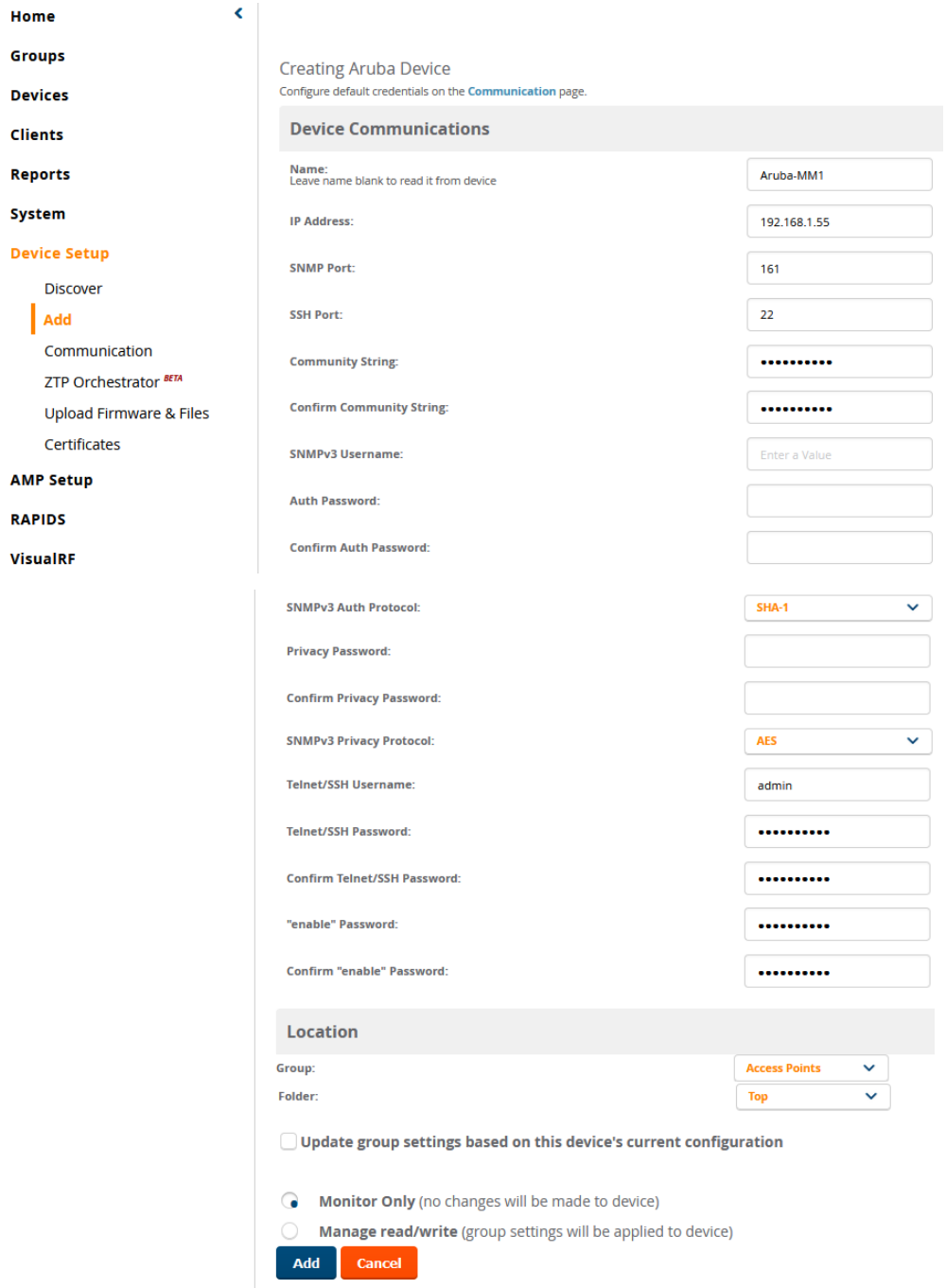
We'll start with adding the evaluation licenses. Before getting this evaluation license from your Aruba SE, you need to send them the IP address of the AW server.



Ensure you have the correct IP addressing and NTP configured.

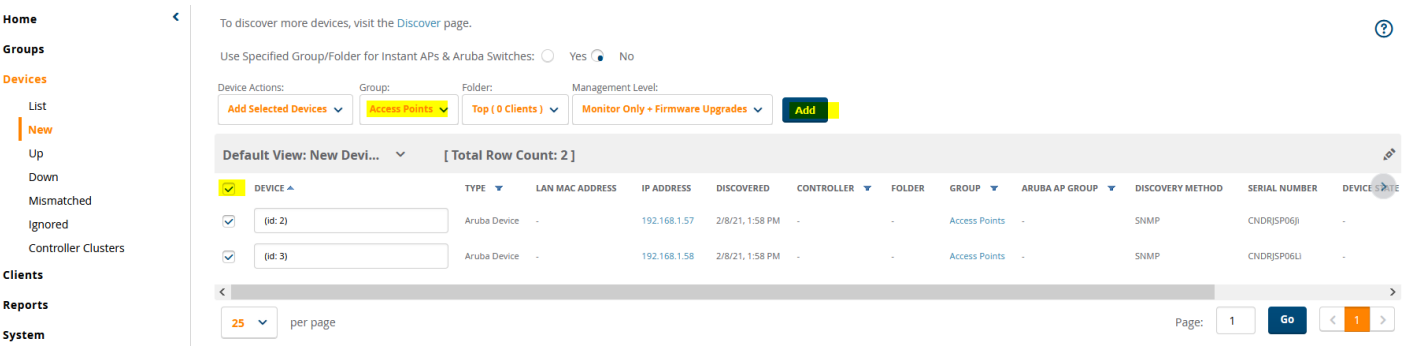


Then we add the MM to AW

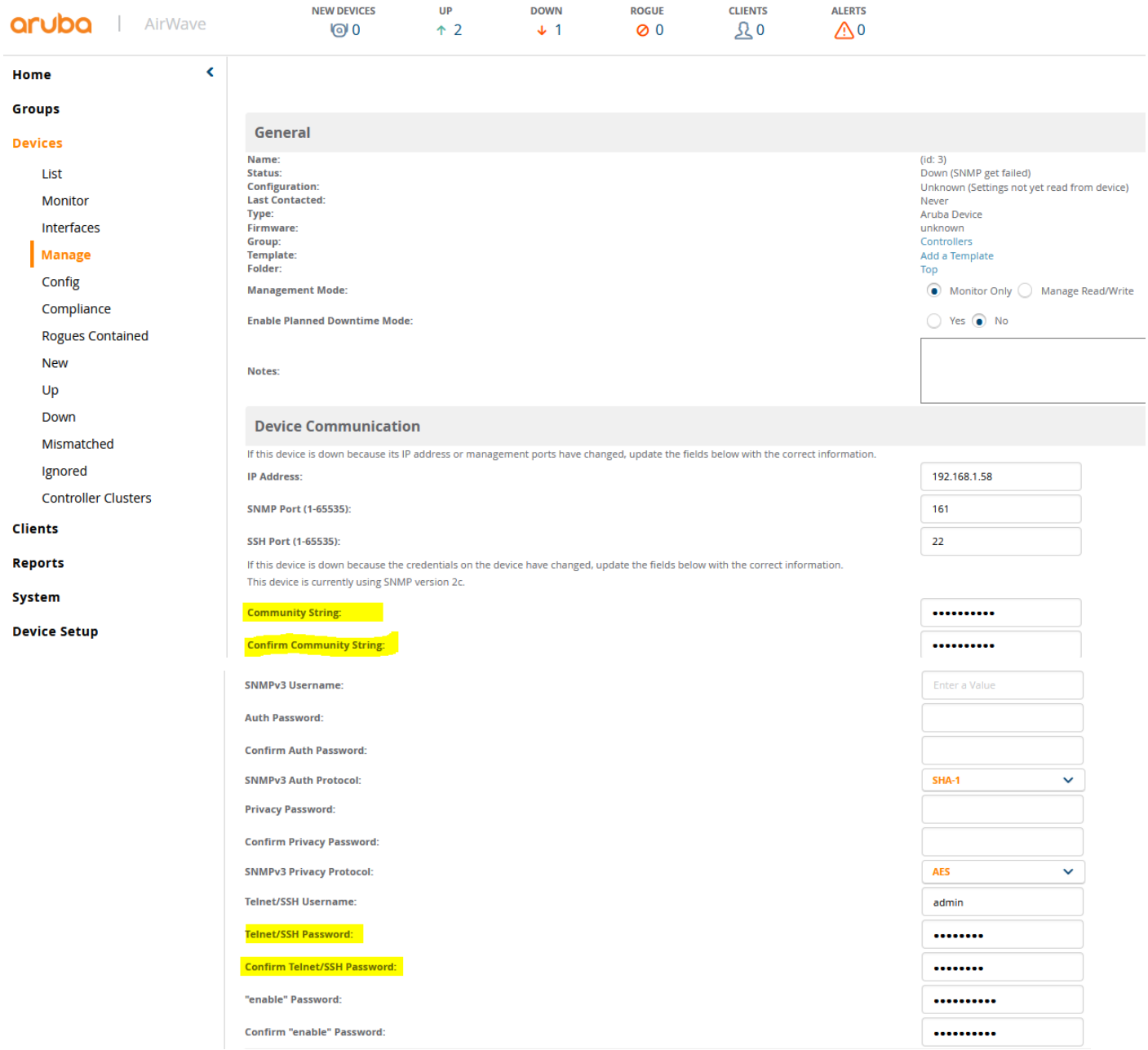


Then after a while you should see MM1 up and AW will discover the 2x controllers.

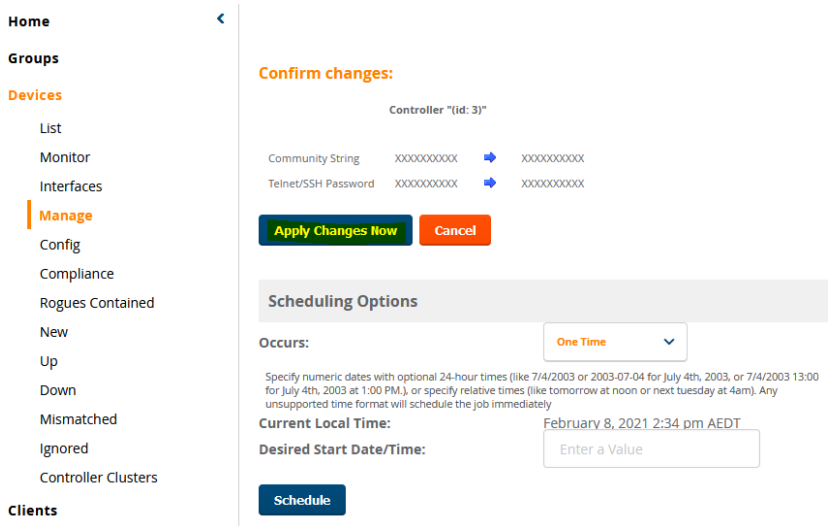
You can then select them and add them to a new group called controllers

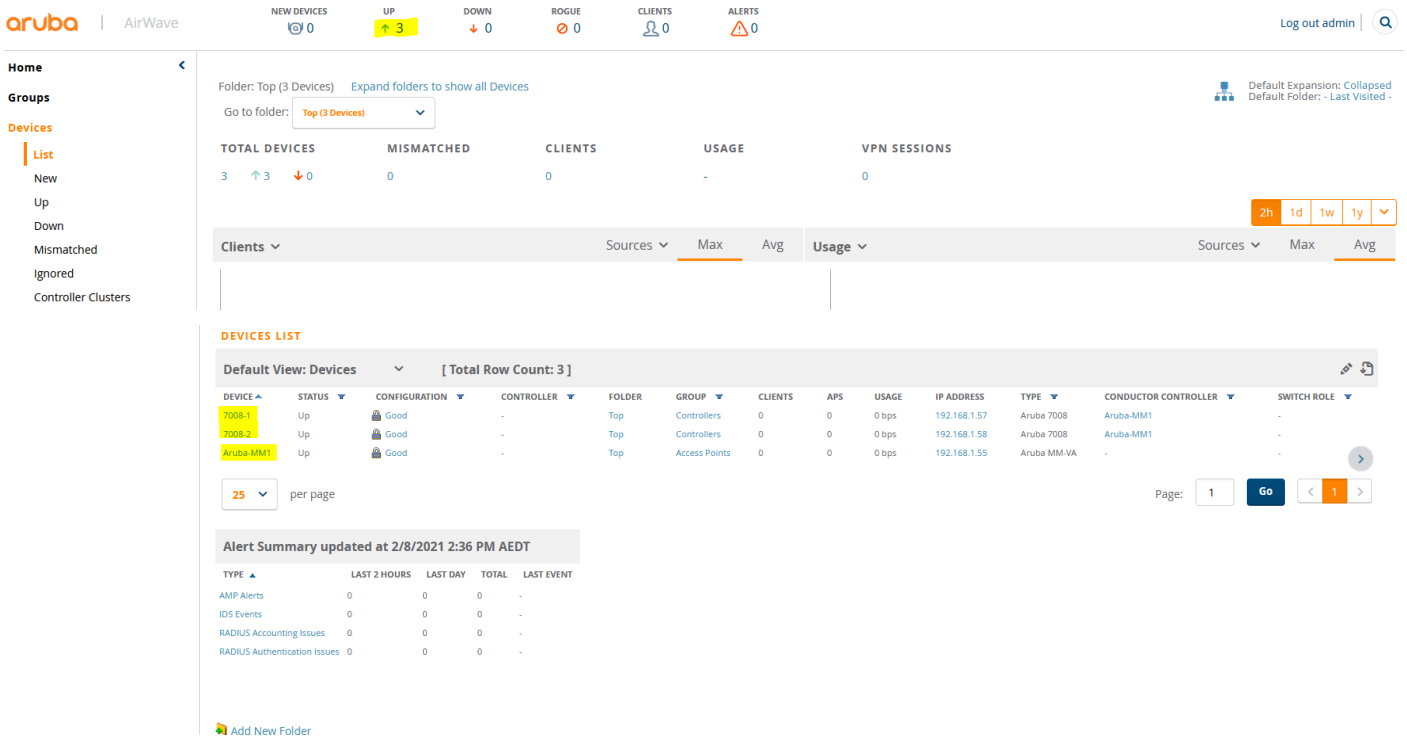


After that click on the down controllers and then manage and add the community strings and admin SSH passwords

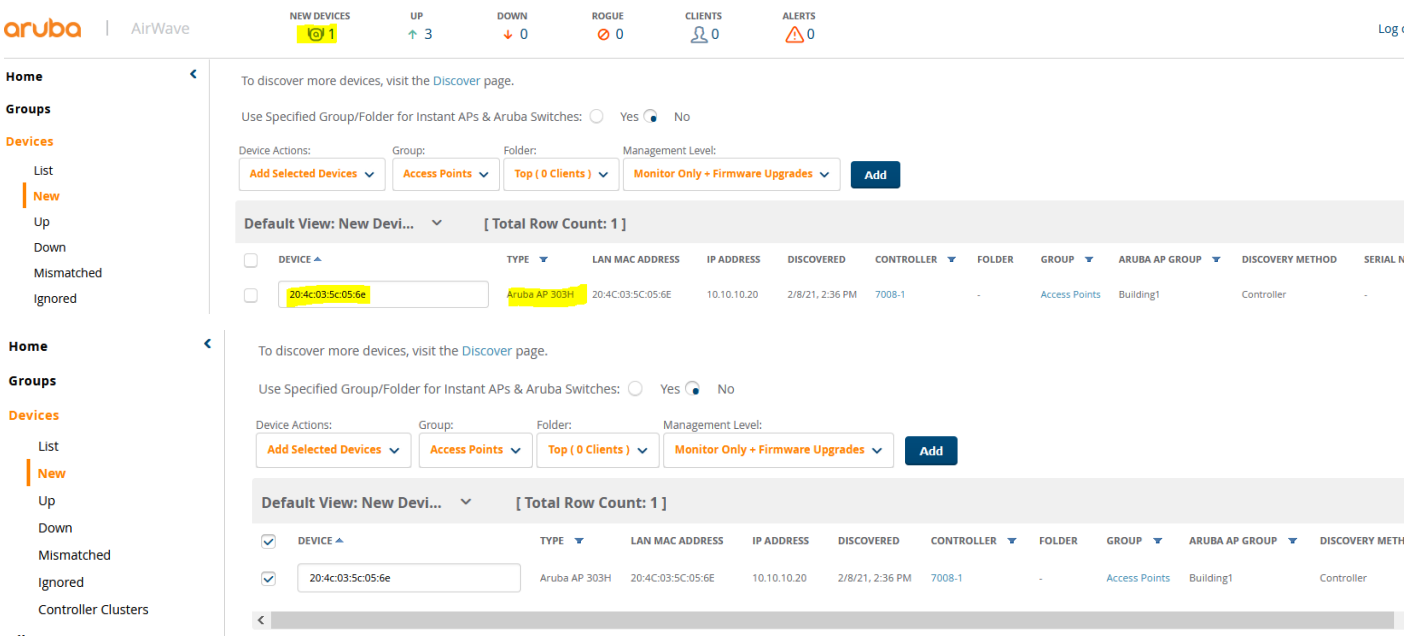


Don’t worry about the enable password it is not used for Aruba devices.



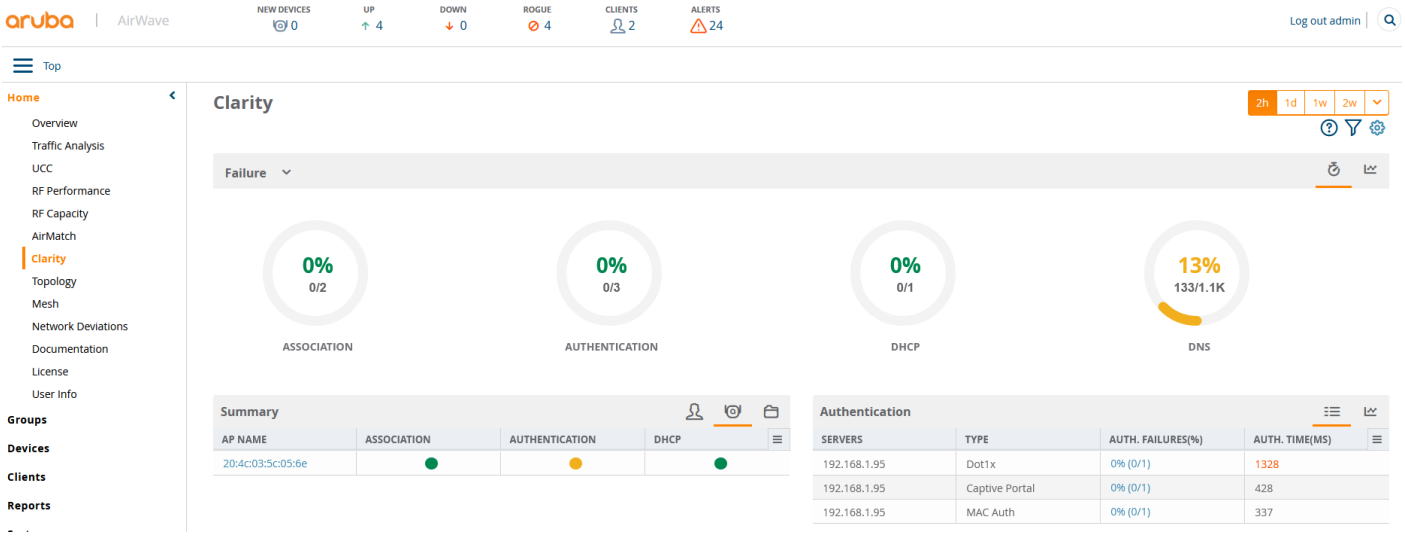


Then the APs will be automatically discovered from the controllers

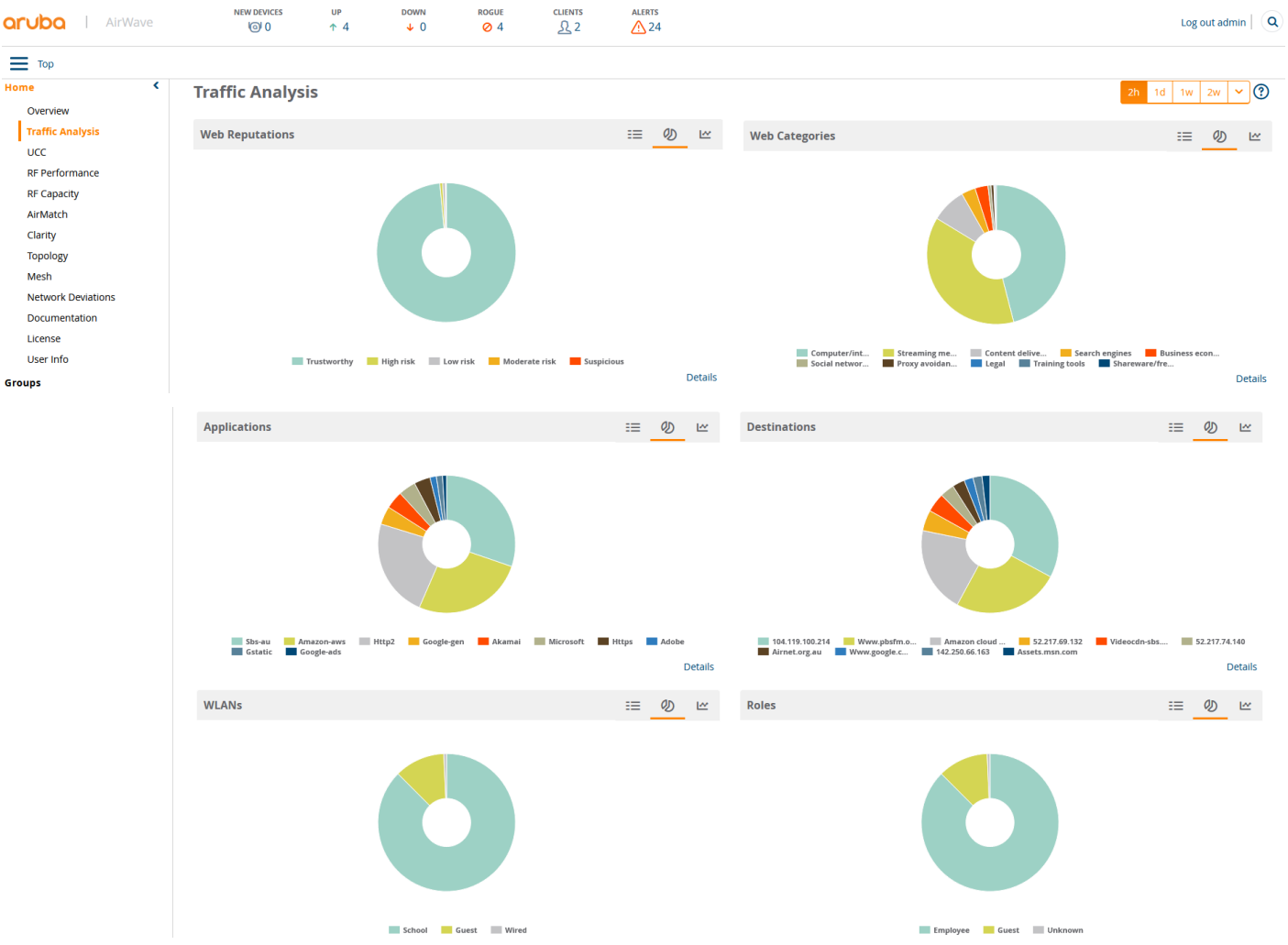


Once we have clients connected to the wireless networks, we should see them appear in Airwave as well.

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



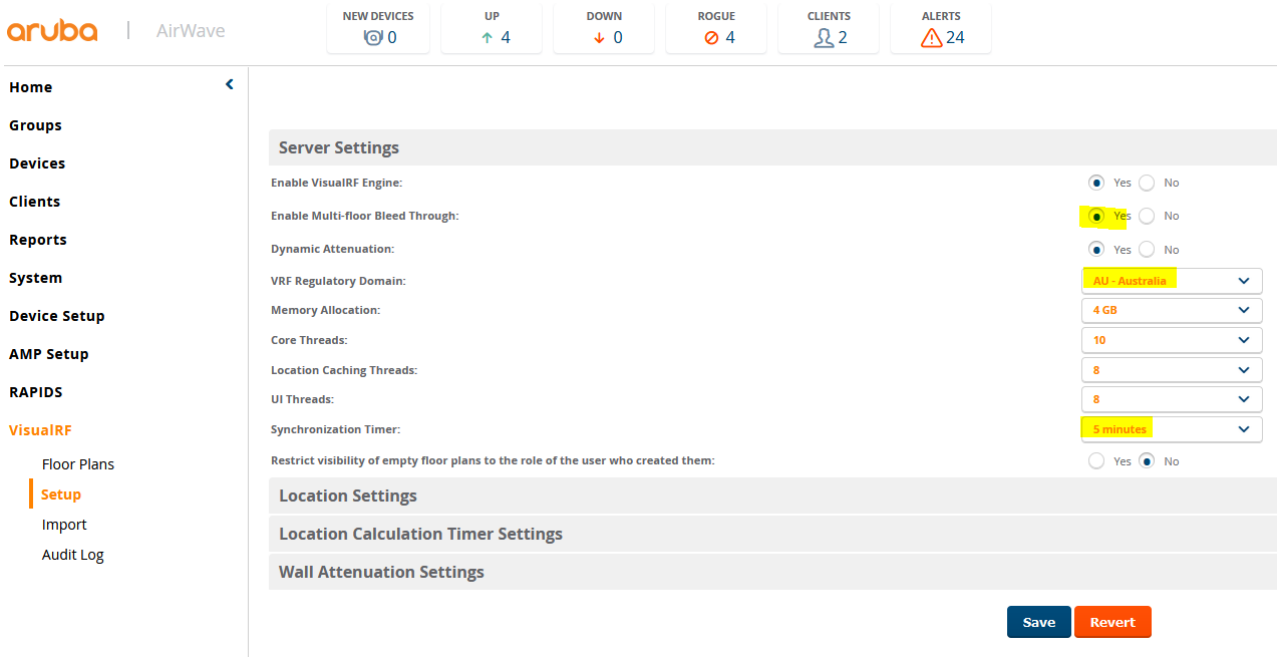
Next, is the Traffic analysis Dashboard.



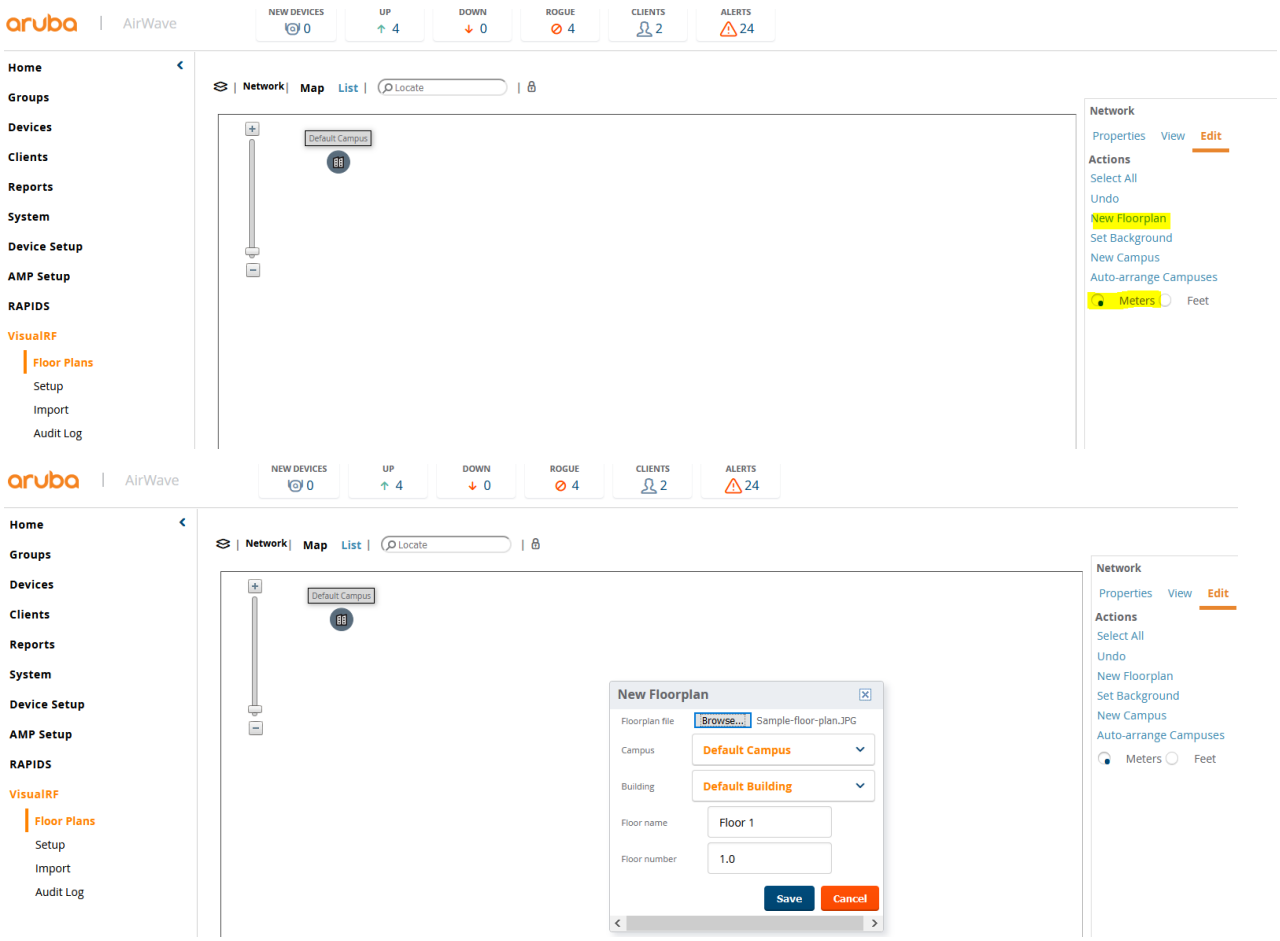
Note that all the wireless configuration will be done on Mobility Master and Airwave is just used for monitoring and reporting.

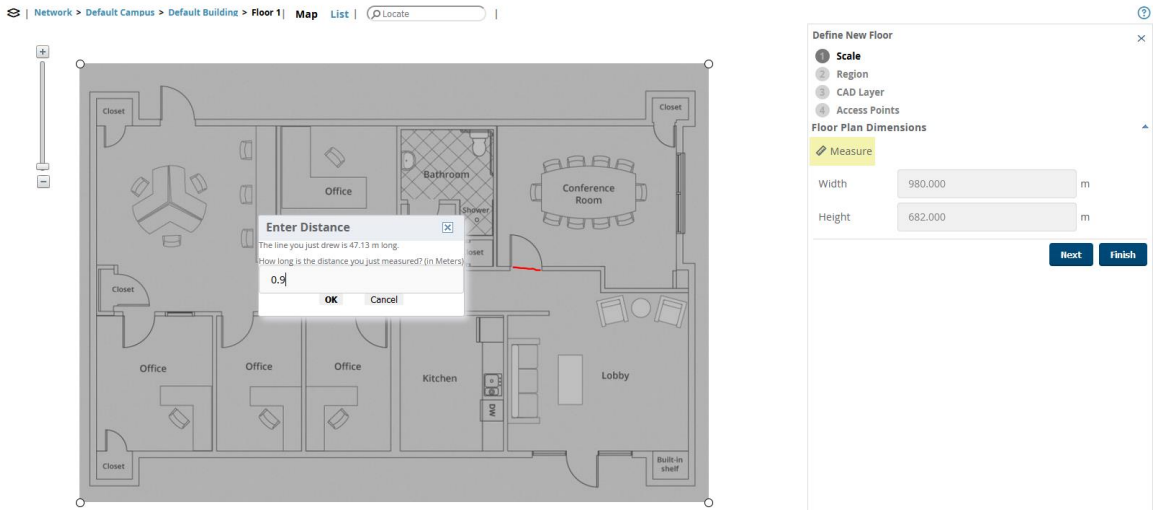
11.2 VisualRF

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

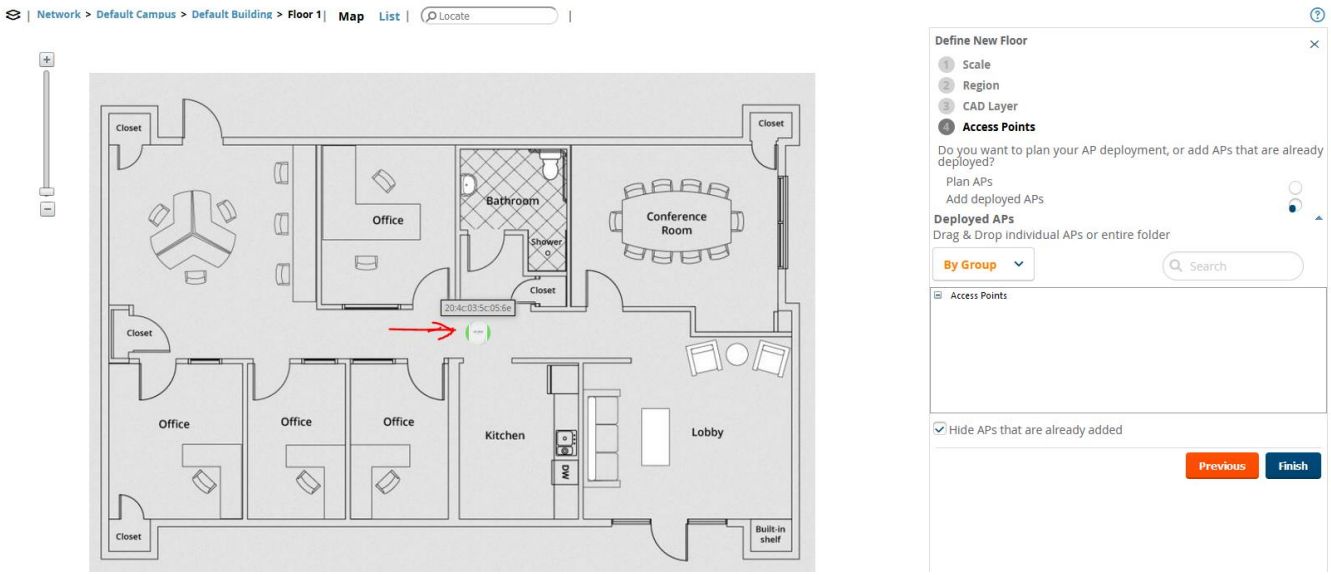


Then you need to go to the floor plans and import your floor plan





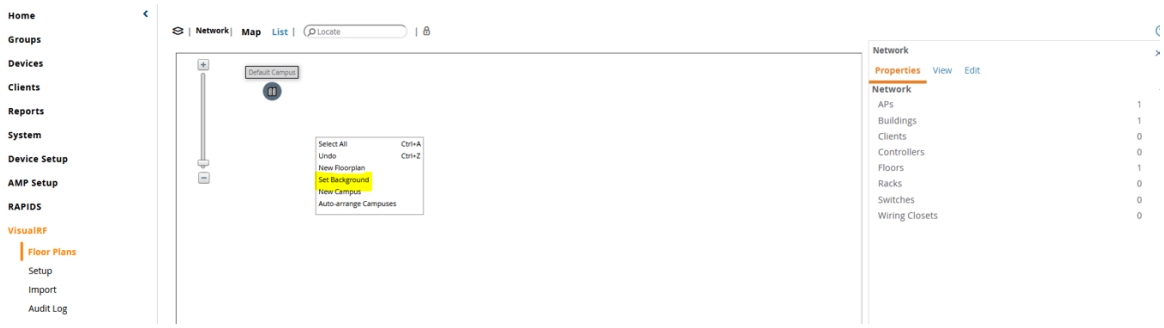
You need to drag he AP on to the floor plan and click on Finish

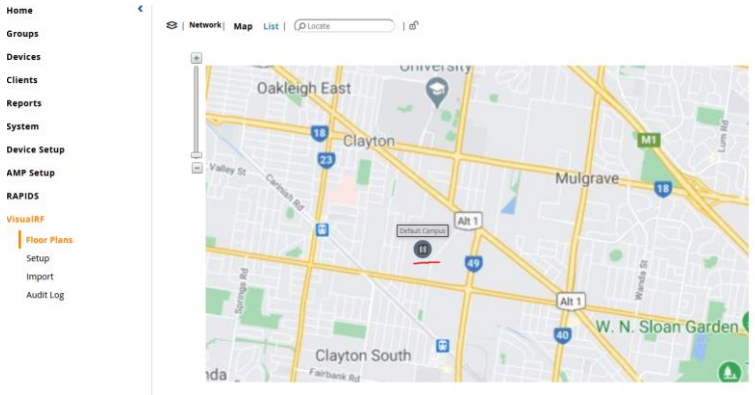


After this, you need to draw a perimeter wall, also ensure you click on the pad lock to unlock the floor plan.

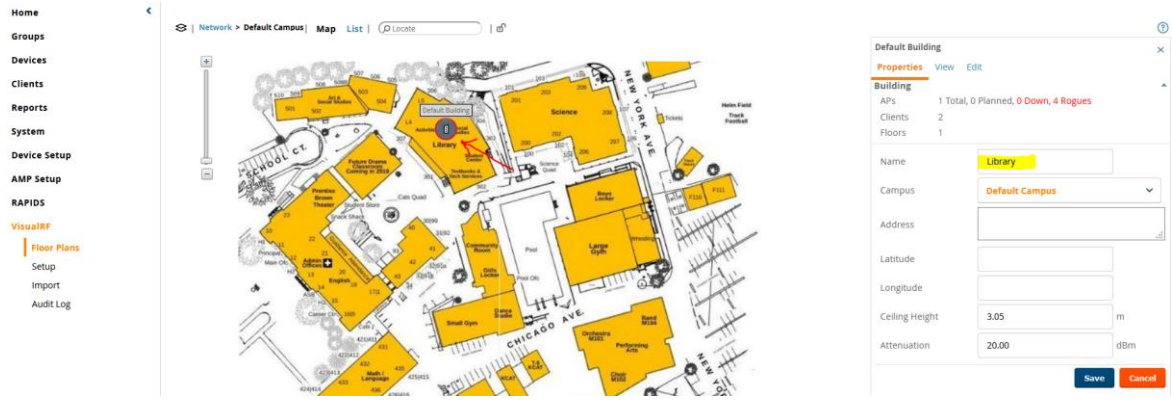
The red line is concrete wall type and by clicking on properties, you can change it according to your environment

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.



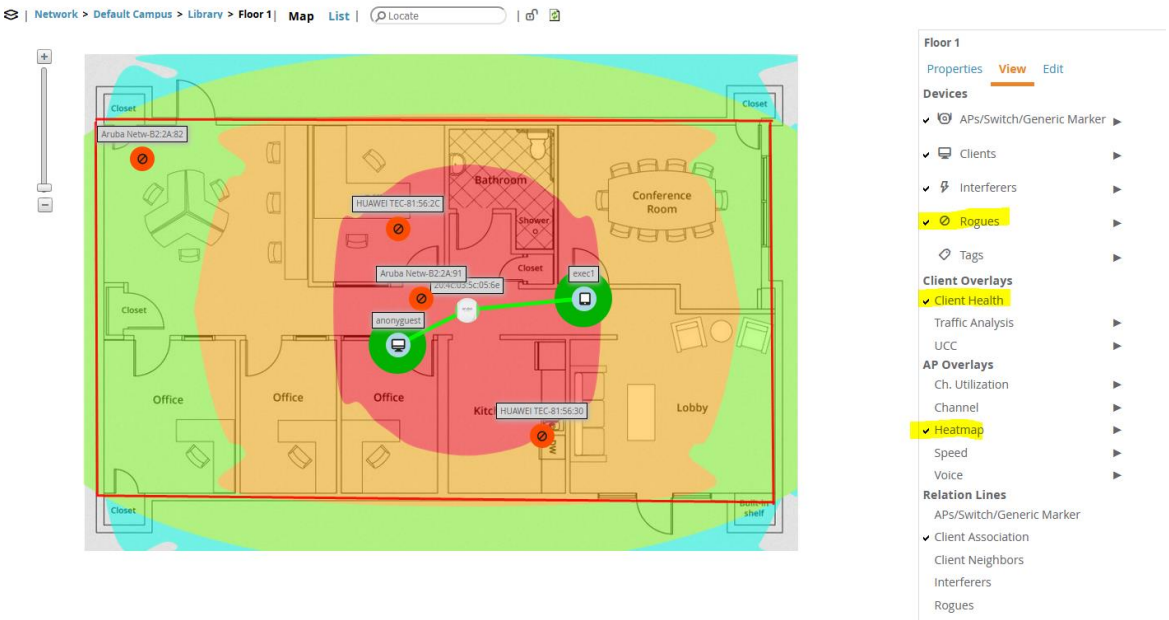


You can then do the same thing with the campus background



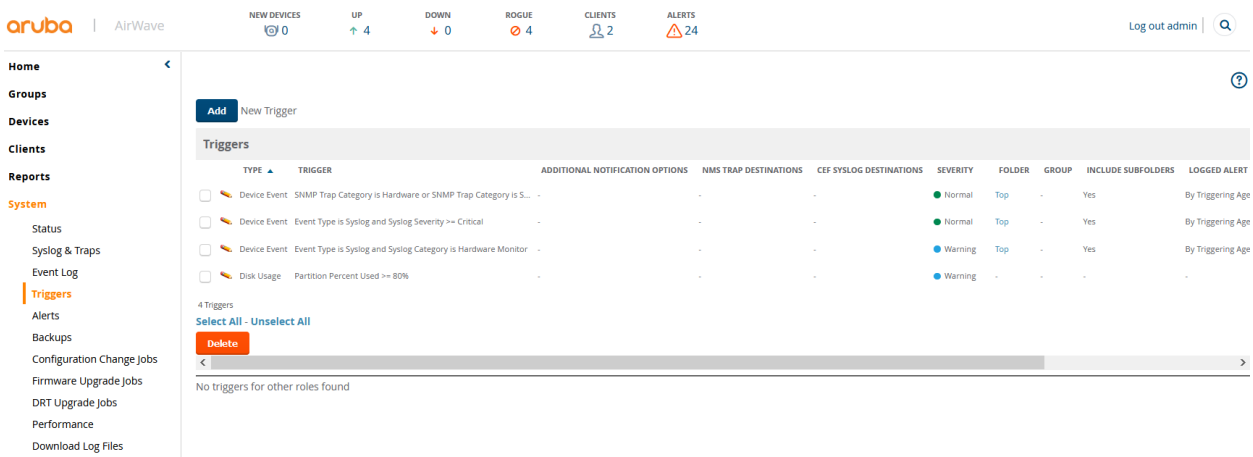
Now when you double click on the building, you'll see the floor. We have only added one floor.

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

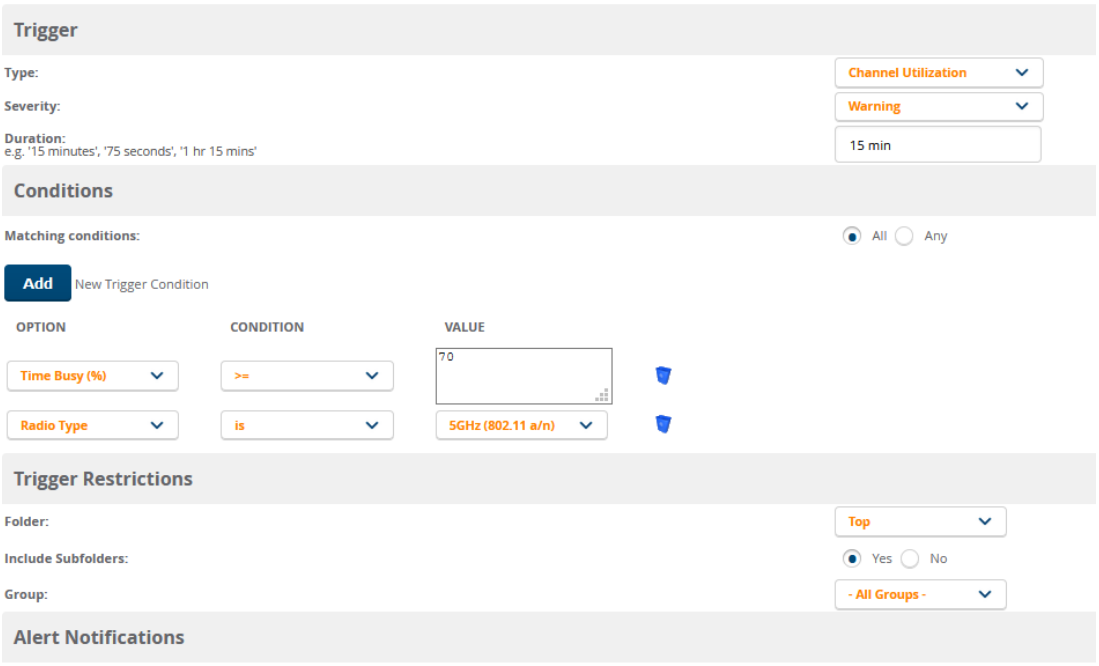


11.3 Triggers and Alerts

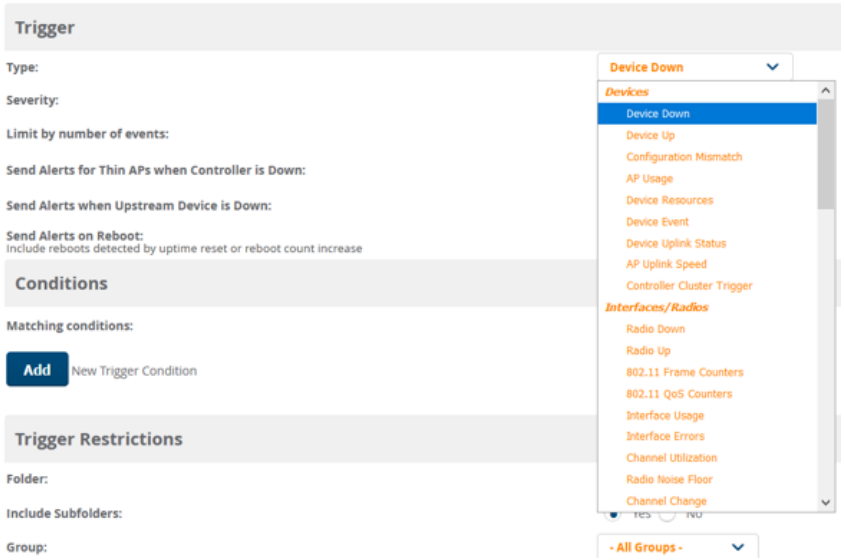
Here are some interesting system triggers that you can configure to alert you about your environment.



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



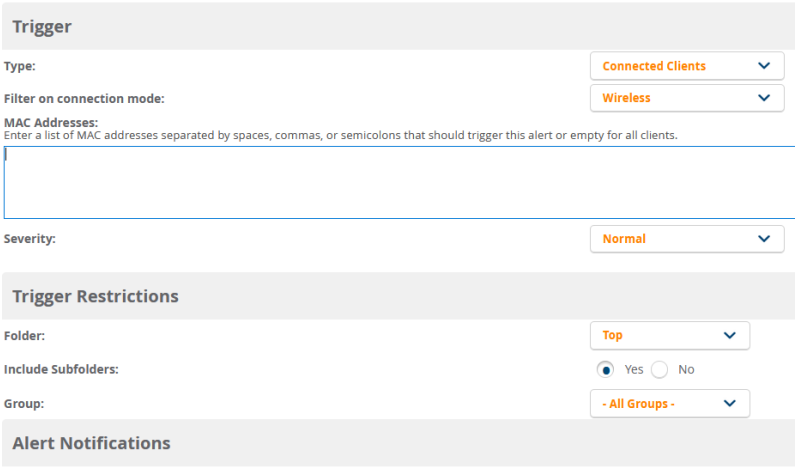
And you can combine any of the trigger type



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

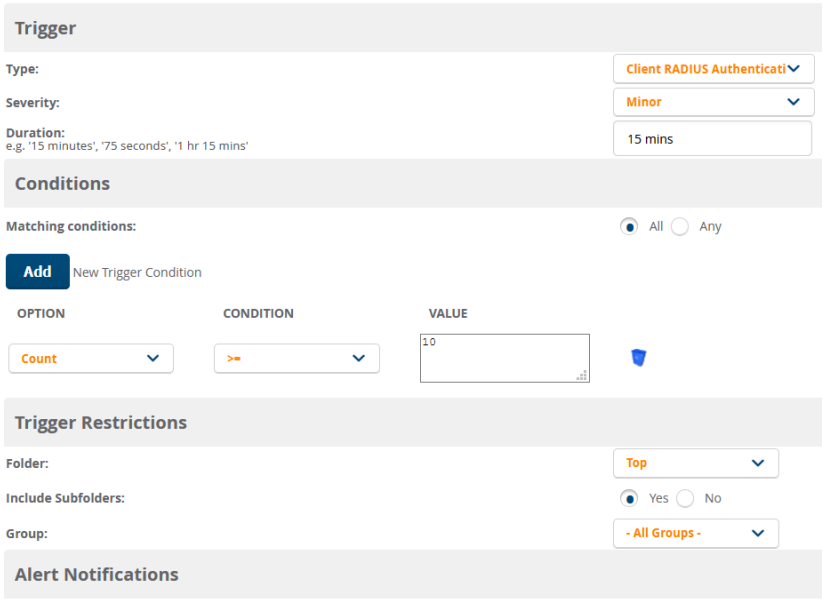
Stolen device

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.



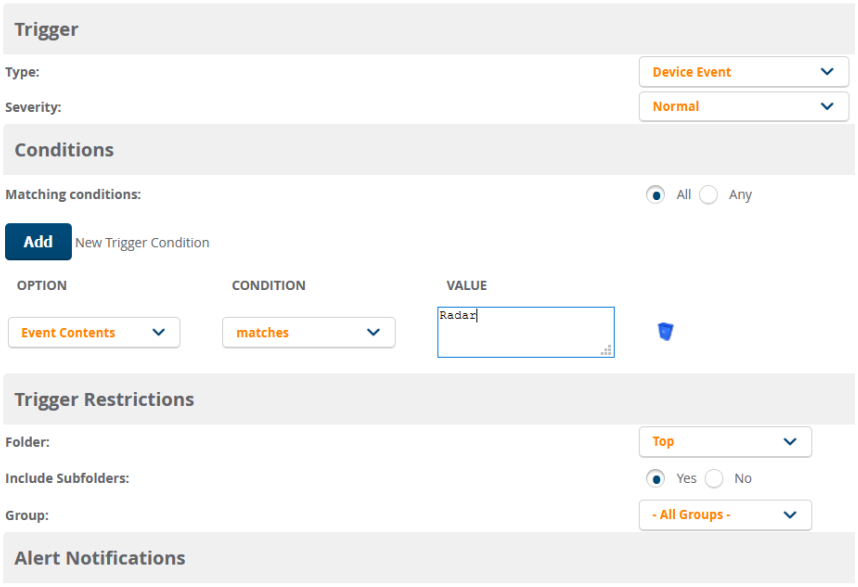
Client RADIUS Authentication Issues

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



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.



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.

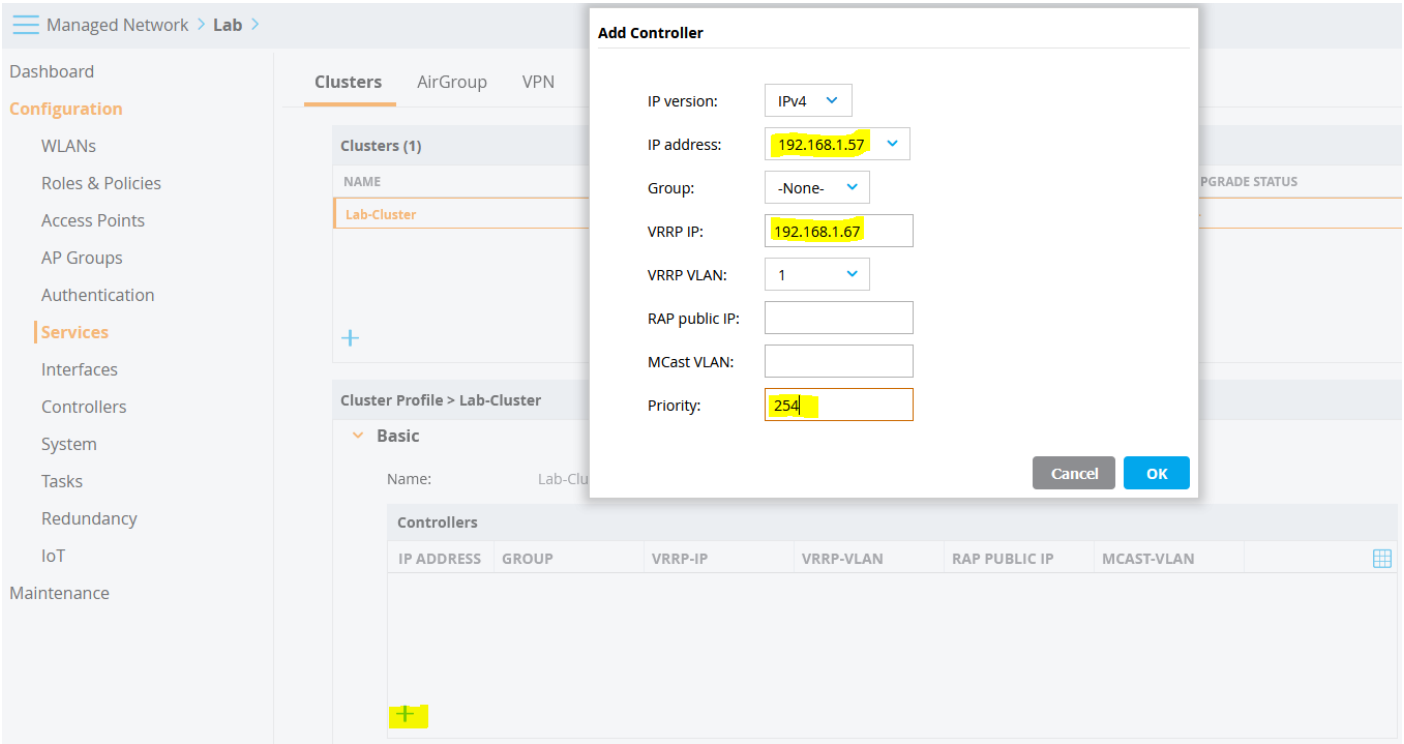
The aims of clustering are

- 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.

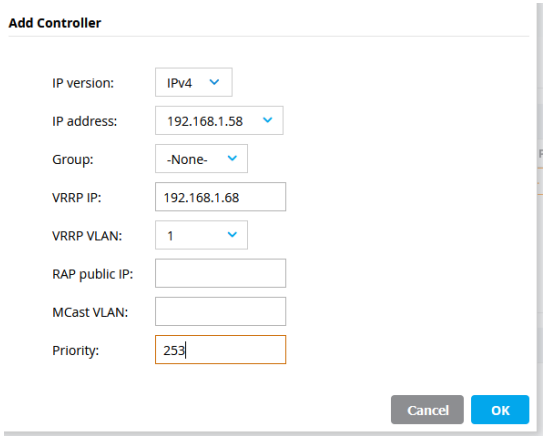
12.1 Cluster Configuration

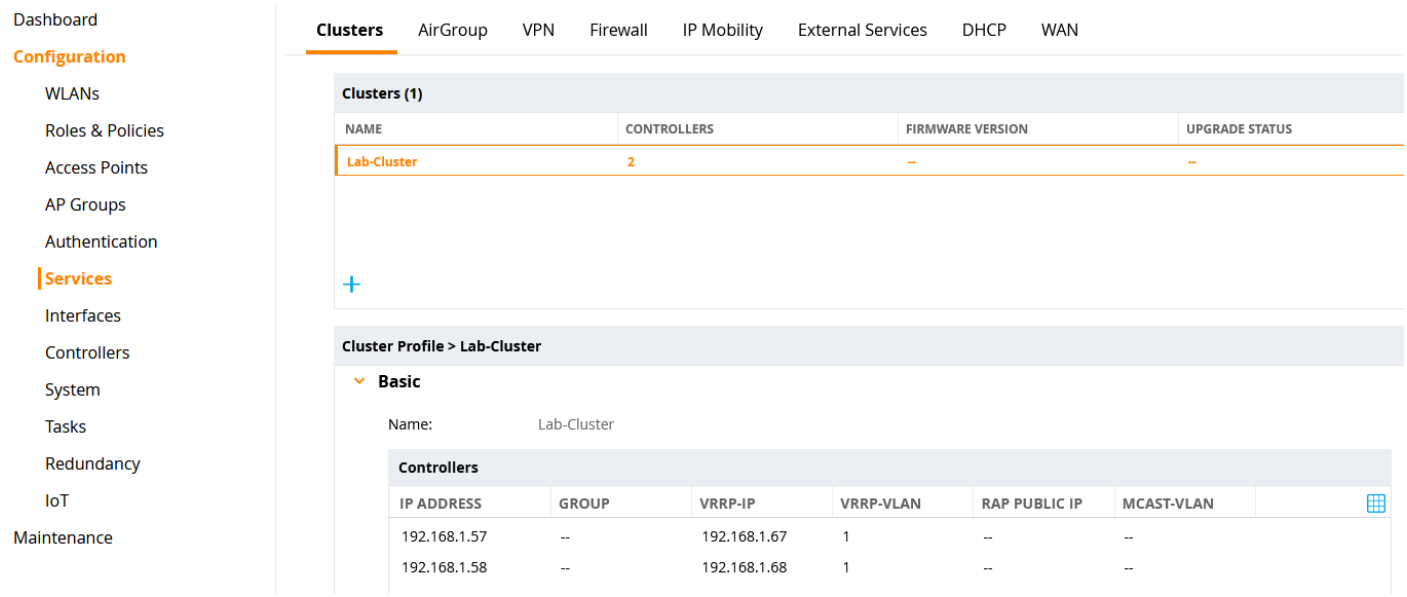
Here we'll be configuring a L2 connected cluster which is the most common type of deployment. The client load is shared by all the managed devices and there is a larger roaming domain with smaller fault domain which helps in faster recovery.

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.

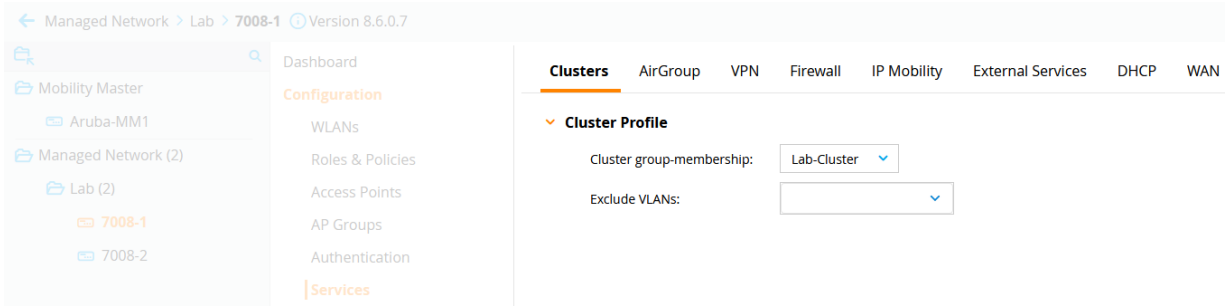


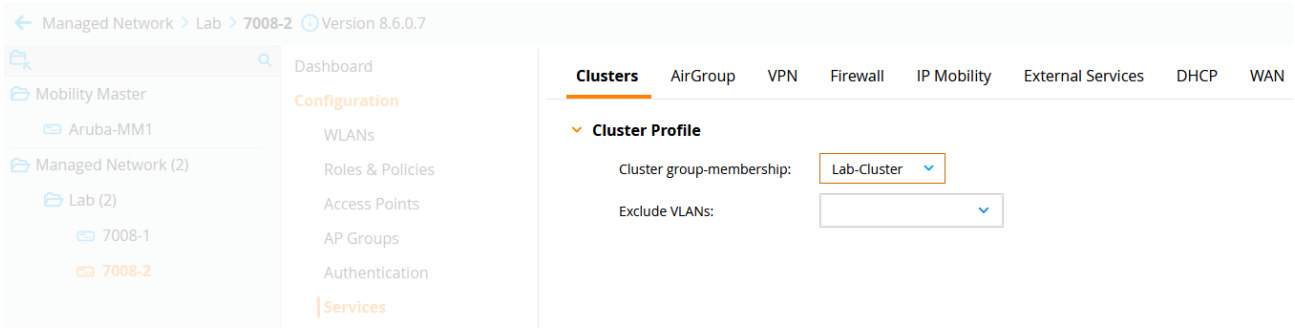
And we'll add the second MD as well



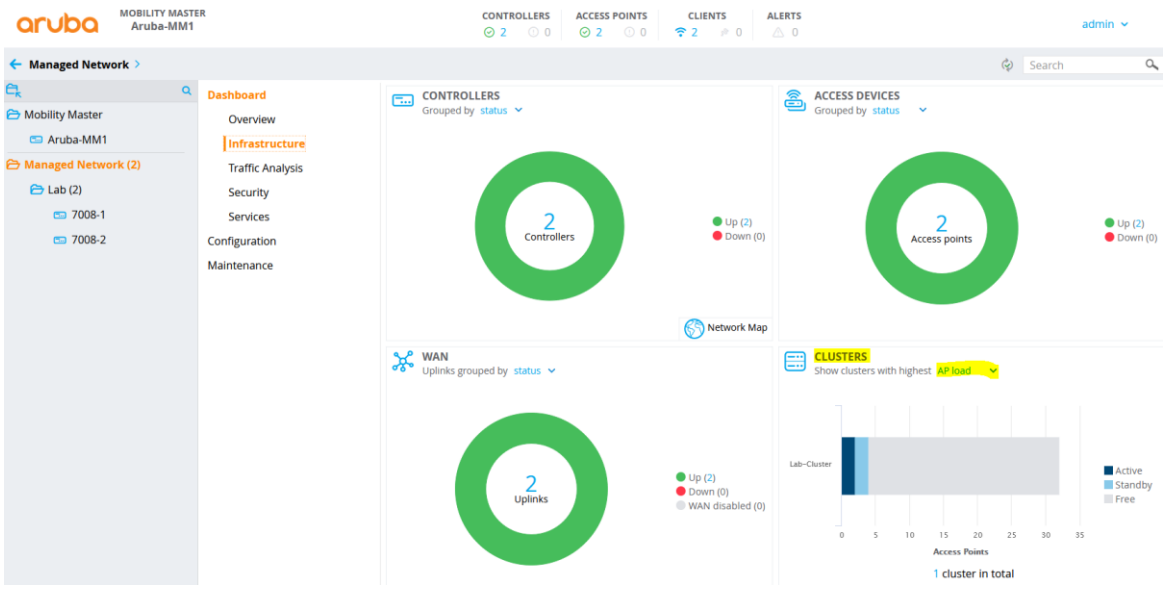


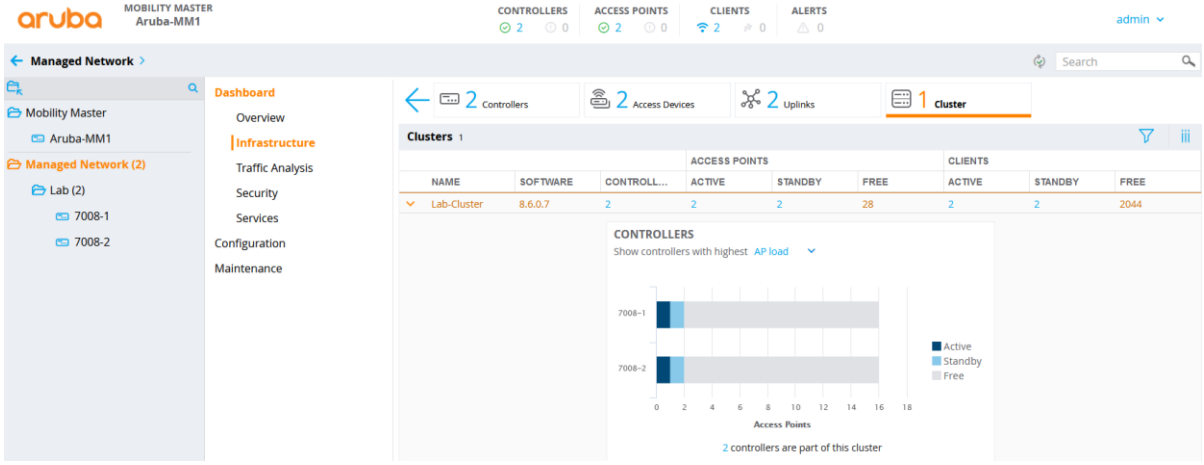
Now we need to go to individual MDs and assigned them to this cluster

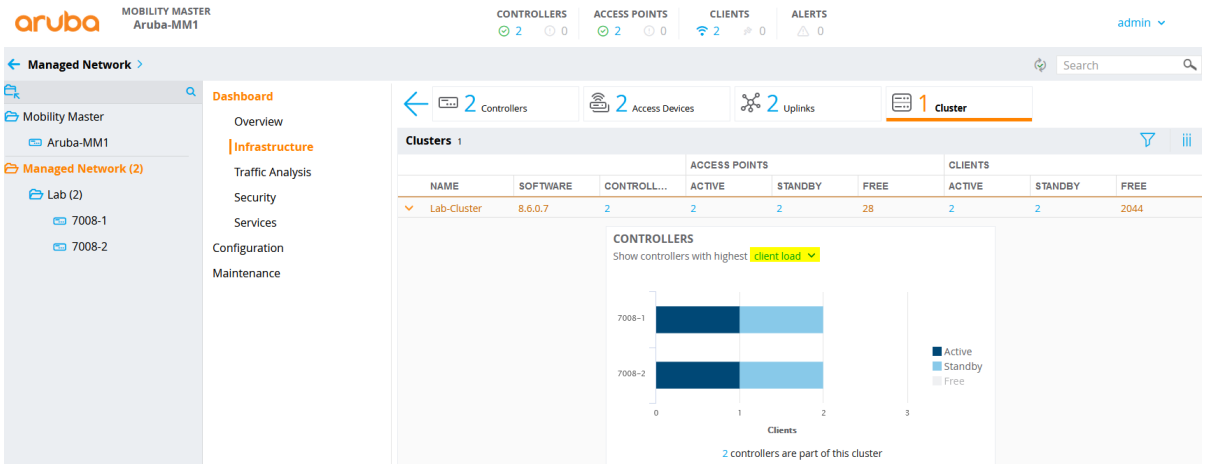




Once you submitted the configuration, you can check the dashboard.





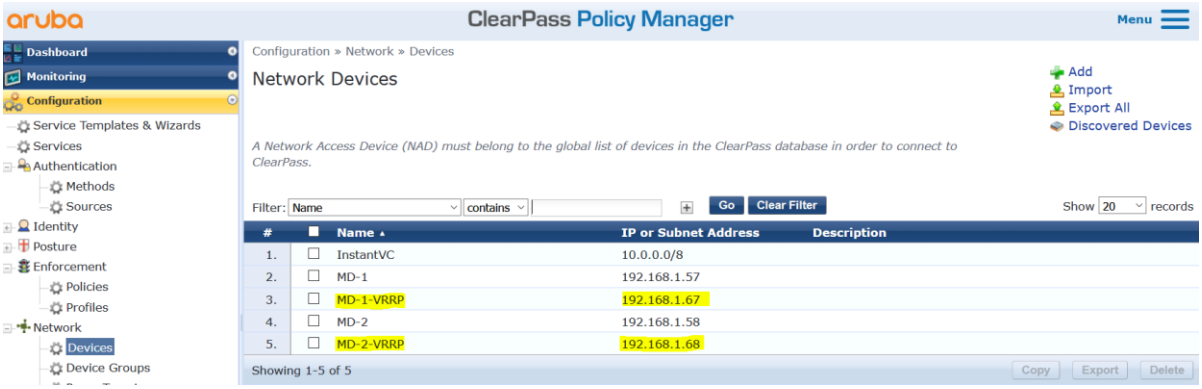


Here is the CLI command to check the operation of the cluster.

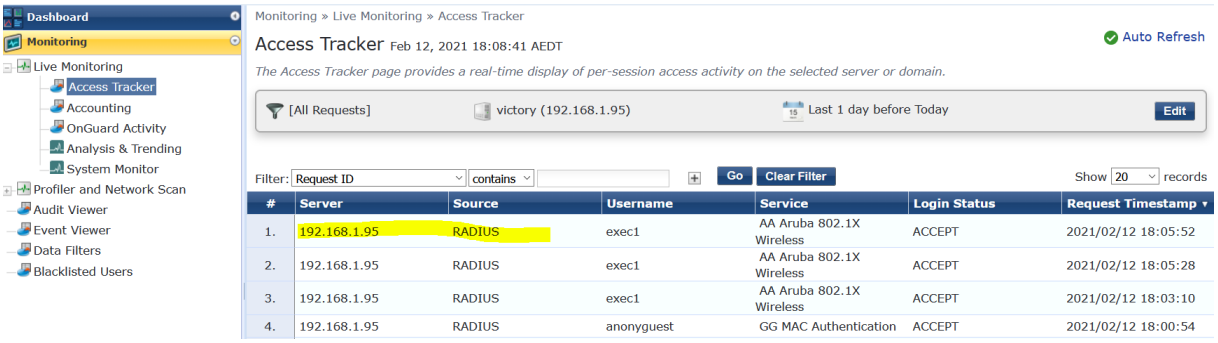
```
(7008-1) #show lc-cluster group-membership

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
```

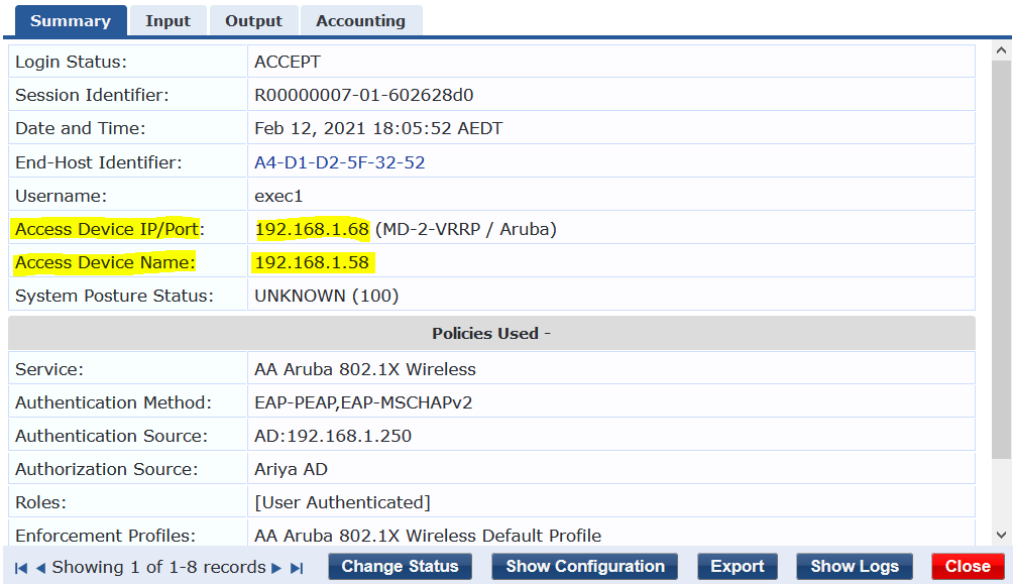
```
Active AP Rebalance Timer = 1 minutes
Cluster Info Table
------------------
Type IPv4 Address    Priority Connection-Type STATUS
---- --------------- -------- --------------- ------
self    192.168.1.57      254             N/A CONNECTED (Leader)
peer    192.168.1.58      253    L2-Connected CONNECTED (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.



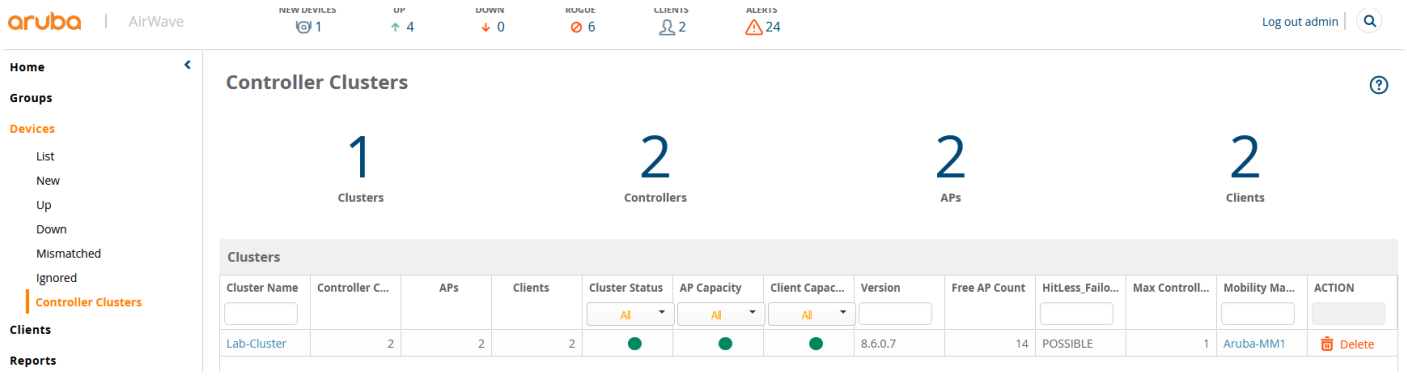
Here we'll check the access tracker for a new client authentication



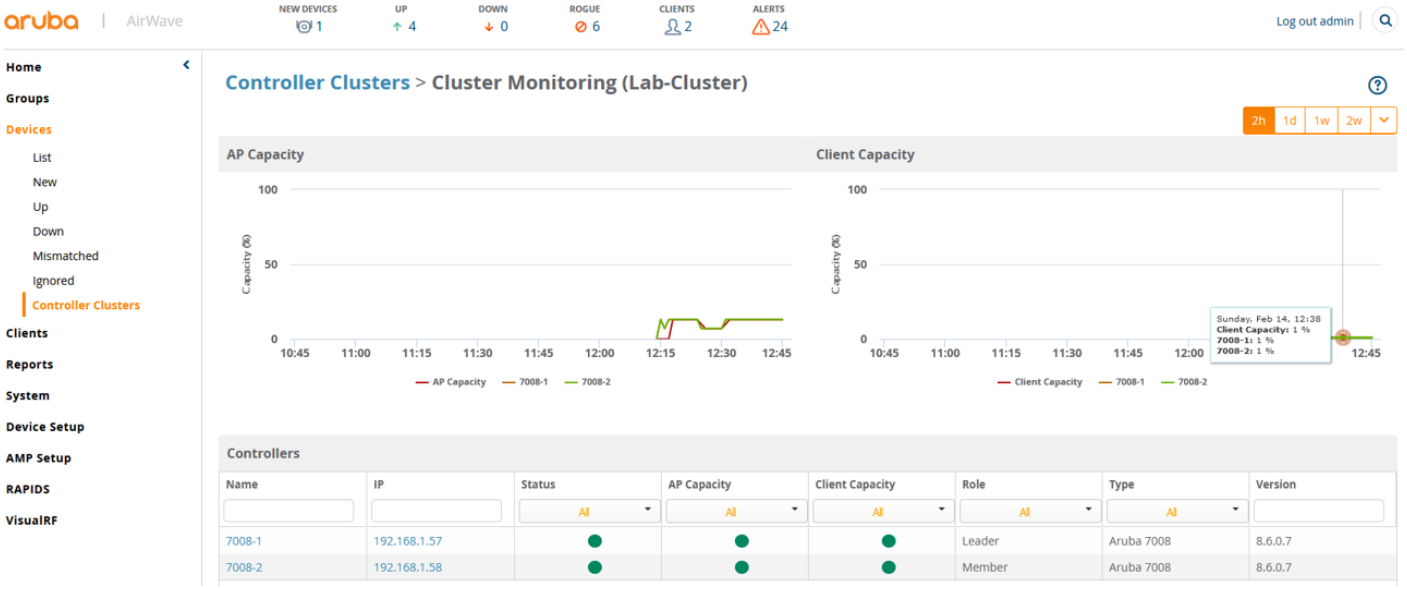


12.2 Cluster Monitoring with Airwave

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.



Clicking on the “Lab-Cluster”.



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.

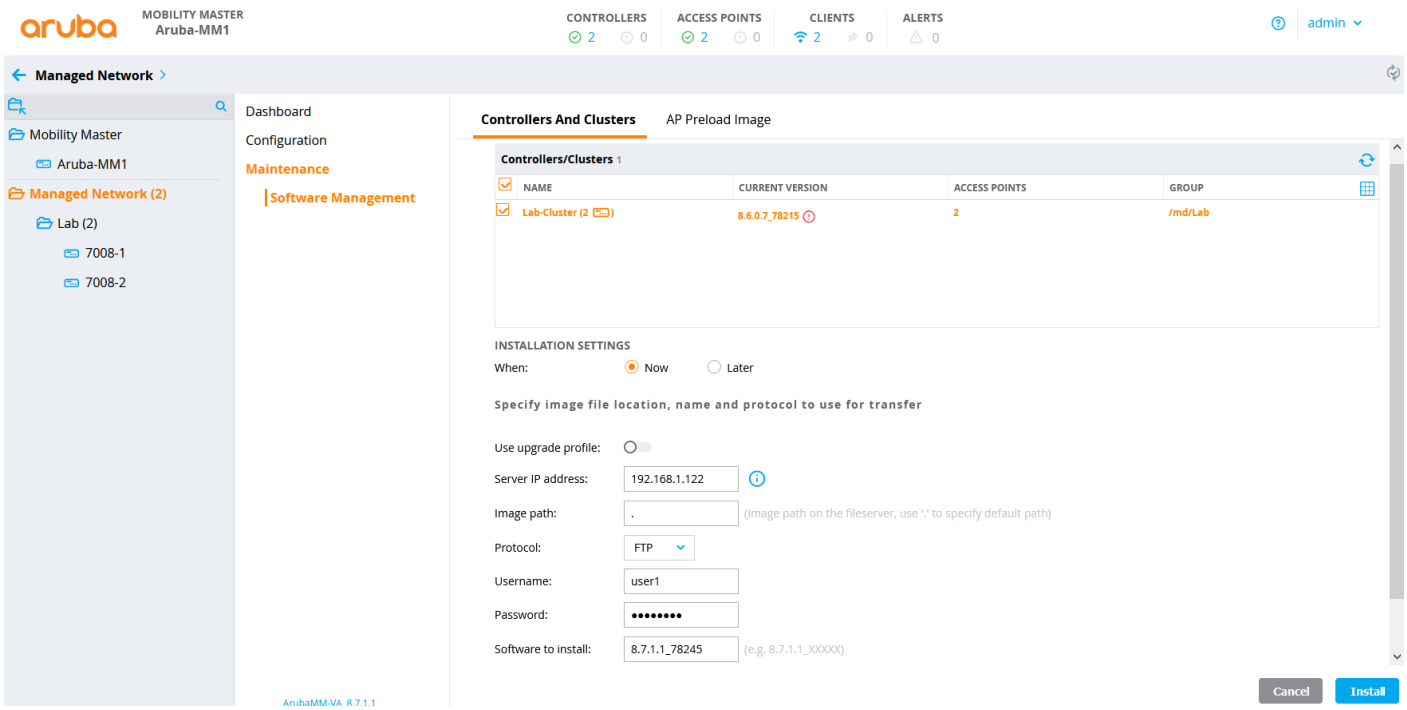
```
APBoot 2.1.4.7 (build 57679)
Built: 2016-12-08 at 15:41:41

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>
```

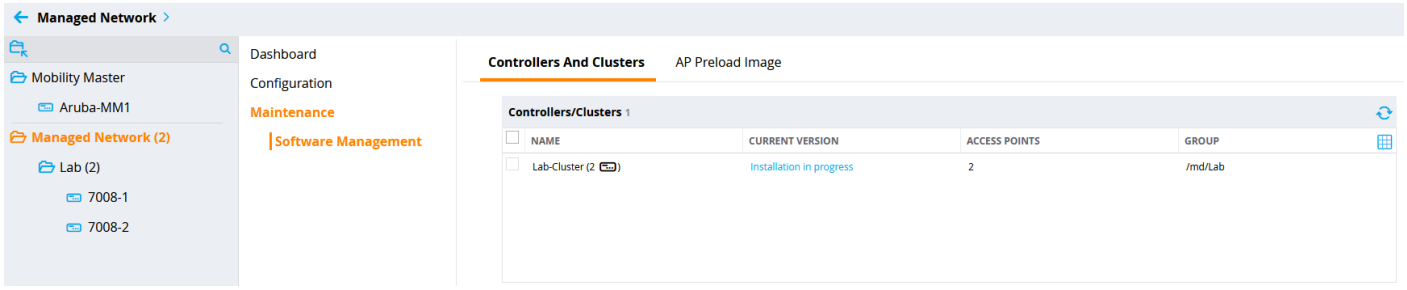
```
apboot> print
NEW_SBL1=1
a_ant_pol=0
a_antenna=0
ap1xtls_suffix_domain=aruba.ap
ap_lldp_pse_detect=0
auto_prov_id=0
autoload=n
autostart=yes
backup_vap_band=2
backup_vap_init_master=192.168.1.58
backup_vap_opmode=0
baudrate=9600
boardname=Aberlour
bootargs=console=ttyMSM0,9600n8 rdinit=/sbin/init 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@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_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>
```

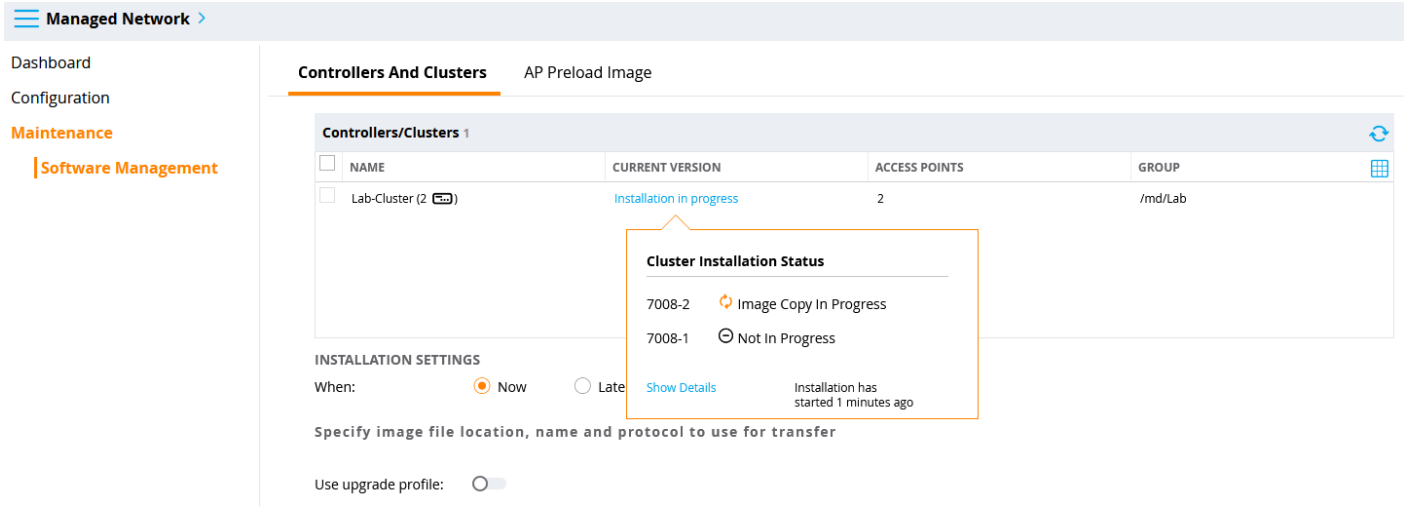
12.4 Live Cluster Upgrade

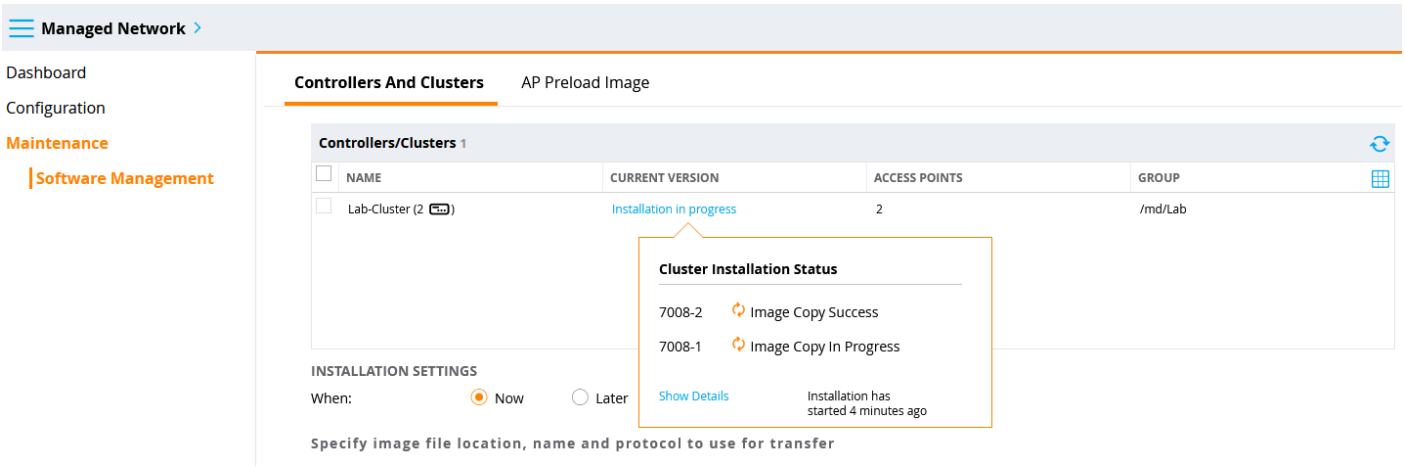
The Live Upgrades feature allows you to upgrade the managed devices and APs in a cluster in real time network upgrade where managed devices and APs upgrade automatically without any planned maintenance downtime. You can also schedule an upgrade to a specified time to avoid manual intervention.

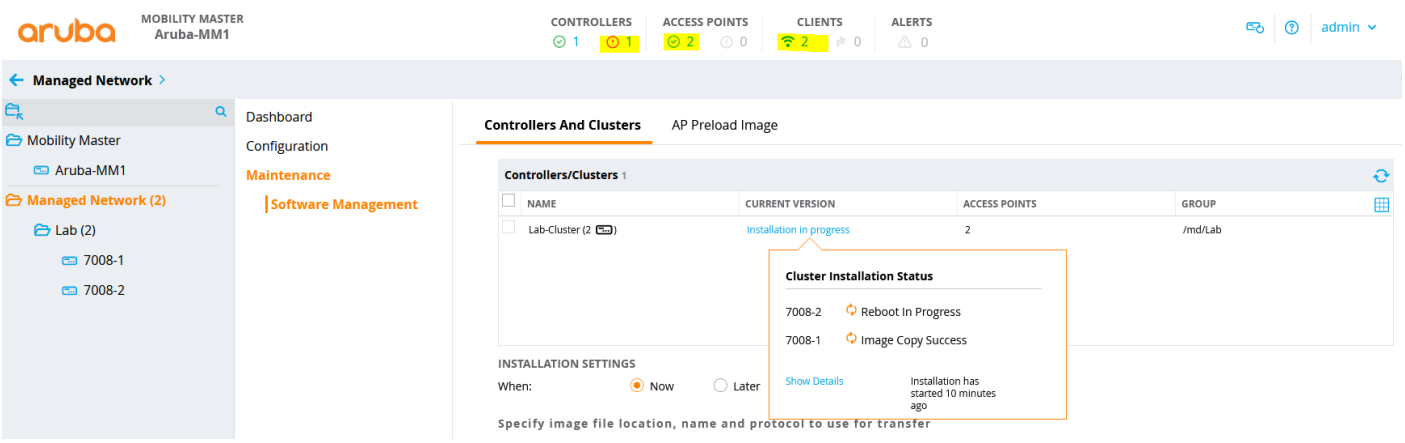
Here we'll upgrade the cluster from 8.6.0.7 to 8.7.1.1



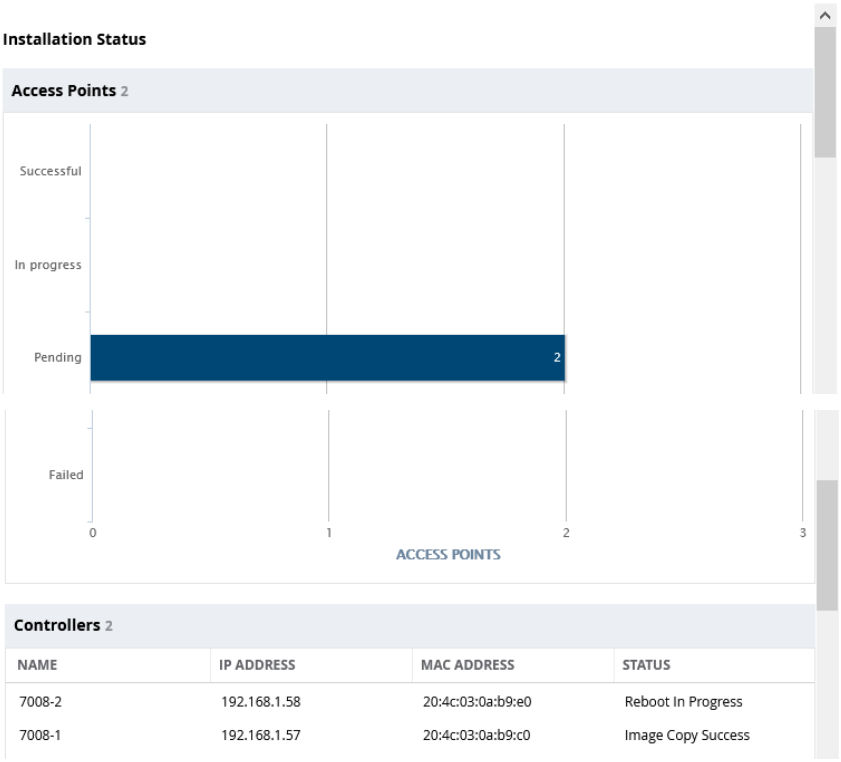


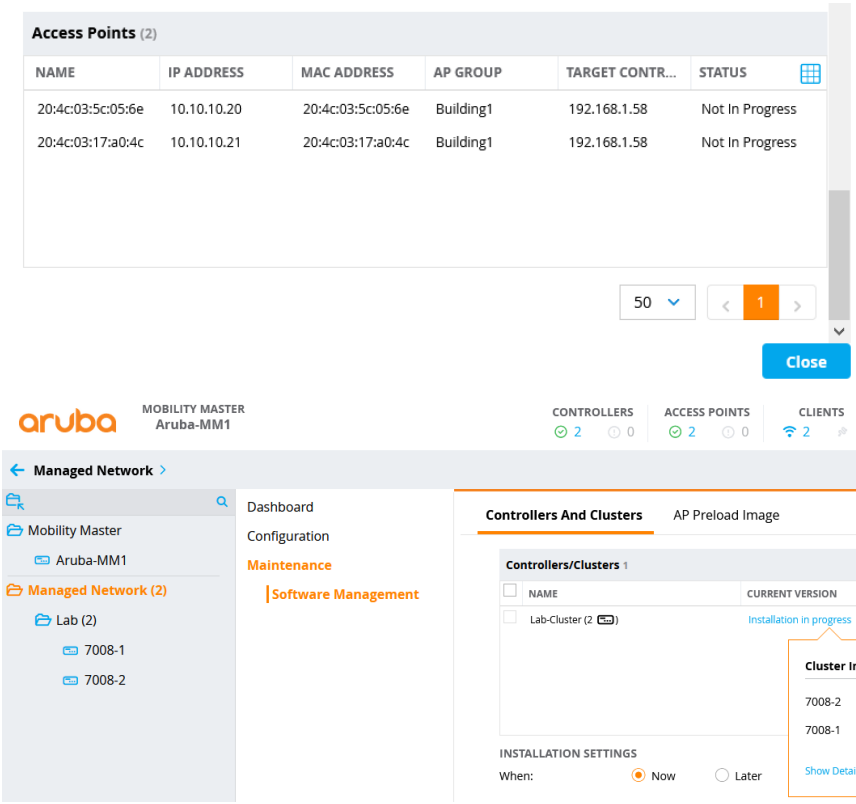




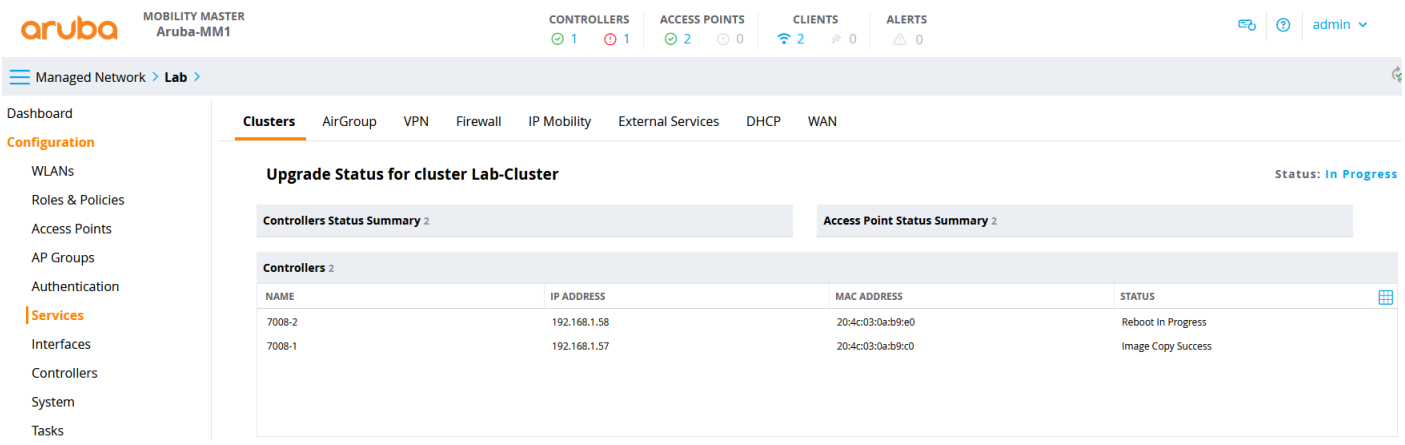


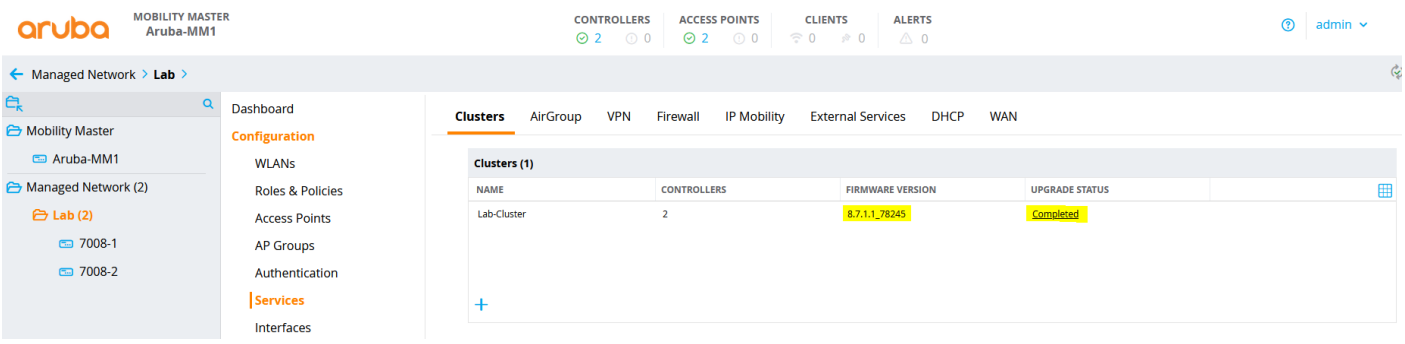
You can click on the “show details”

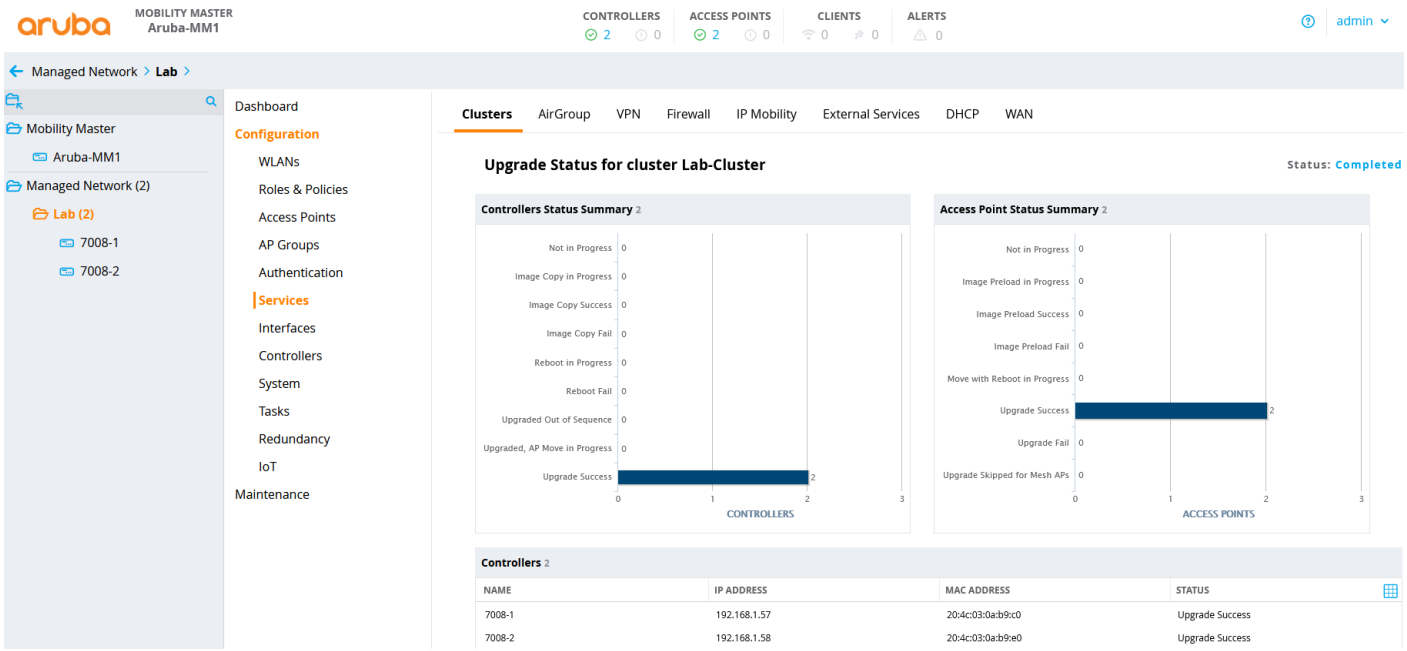




You can also follow the upgrade status from the services tab







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.