DEPLOYMENT GUIDE – ARUBA MESH WITH CENTRAL

USING ARUBA CENTRAL WITH INSTANT ACCESS POINTS

When needing to stand up a quick, easy to deploy temporary, tactical, or permanent deployment of Wi-Fi over an open area that is lacking wired connectivity for the coverage area required, Aruba Central with Instant Access Points (APs) can be implemented. Using Central for cloud management and Instant Mesh within a Virtual Controller (VC), it's easy to wirelessly extend coverage to remote areas that are outside of the wired range of the network or to areas that are difficult to pull wired network drops to. Central and Instant Mesh can be used just to extend wireless coverage to clients in and around the areas where the APs are deployed or can provide wired connectivity using the mesh radios to backhaul traffic over the mesh back to the LAN. Additionally, the APs reporting up to Central allow for remote monitoring and management of the deployed networks via the cloud.

TABLE OF CONTENTS

WHAT IS MESH?

Aruba's mesh solution is a technology that allows APs to talk to other APs for the purpose of providing Wi-Fi links over the APs to carry wired or wireless client traffic from Mesh Points located away from the wired network, back to the Mesh Portal which is connected to the LAN.

Figure 1

Aruba's Mesh supports several topologies, where a mesh portal can support one or more mesh points if necessary. Figure 1 shows a simple Point-to-Point with a single mesh portal and a single mesh point. However, other topologies are supported with Instant Mesh, including Point to Multi-Point in both a hub and spoke (Figure 2) as well as linear multi-hop mesh (Figure 3) below.

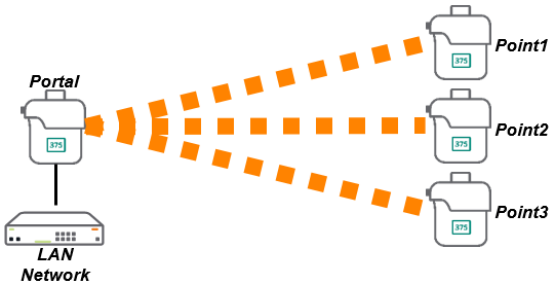


Figure 2

Figure 3

With Central and Aruba Instant, it is recommended that there be no more than 3-4 mesh points per portal for general applications, with no more than 2 hops in the mesh topology design. Aruba Instant has a hard limit of up to 8 mesh points per portal and 2 hops in the mesh topology, but each mesh point in the cluster adds latency and lowers overall throughput, so keeping the mesh point count low helps ensure adequate performance.

HOW TO SET INSTANT MESH WITHIN A VIRTUAL CLUSTER (VC) MANAGED BY CENTRAL

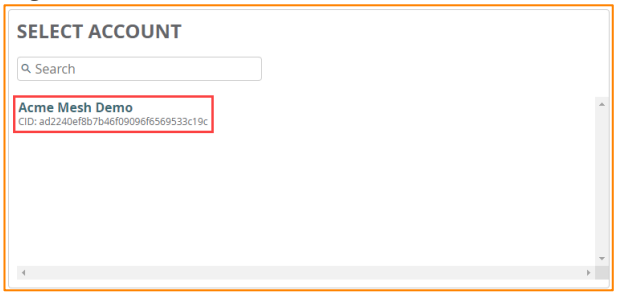
The following process makes a few assumptions necessary to support an Instant mesh solution under Central. Other considerations can be taken into account but are outside the scope of this document. Assumptions include:

- On the network where these new APs are deployed, these are the only Instant APs on that L2 network/VLAN, and the APs will have access to Central in the cloud.
- All APs within the same Virtual Controller (VC) are of the same platform and family (AP-360 family, AP-370 family, AP-387 Point-to-Point solution, etc.)
- All APs configured are part of the mesh and are in the same group within Central. This mesh network will not be able to backhaul other Instant APs not part of the mesh and should be handled with a specific design to accommodate that requirement. Please consult your Aruba SE or Partner.
- DHCP services are available, either to/from the main LAN/network, or provided via the gateway or routers for this network, and all devices have access to the Internet for Central management
- Instant OS version 8.5 or 8.6 or later under Central
- If there are any other deviations or accommodations that need to be made, please consult your Aruba SE or Partner

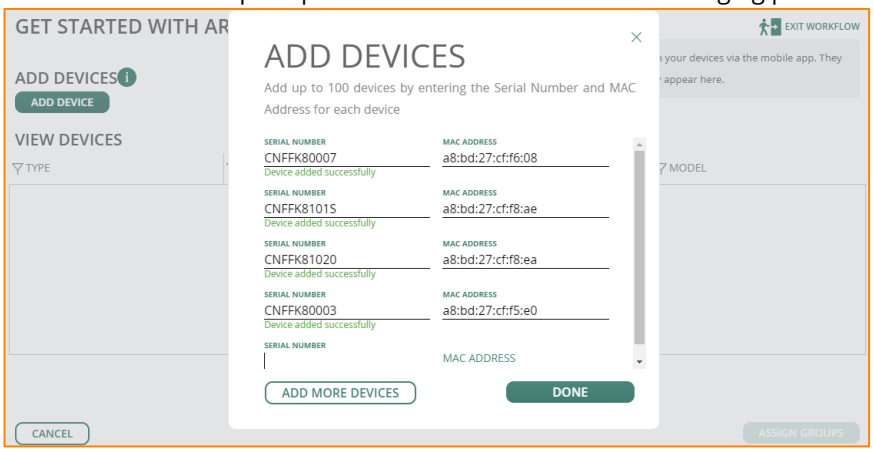
INITIAL STAGING OF CENTRAL

While this deployment guide is starting from the assumption of a new deployment, the following steps can be taken if this is to extend, grow, or modify an existing Central with Instant AP deployment. Because this guide is assuming a new deployment in Central, there are some steps to follow first within Central before connecting and configuring the APs. In addition, Central allows for most of the configuration to be deployed before the APs are brought up, allowing for more rapid staging of hardware once on site.

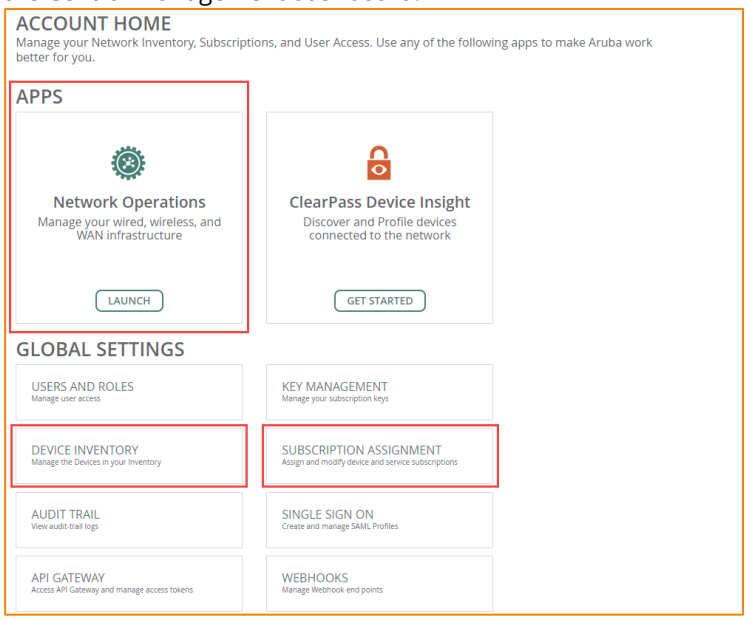
1. Log in to Central and click on the account where the new APs will be deployed



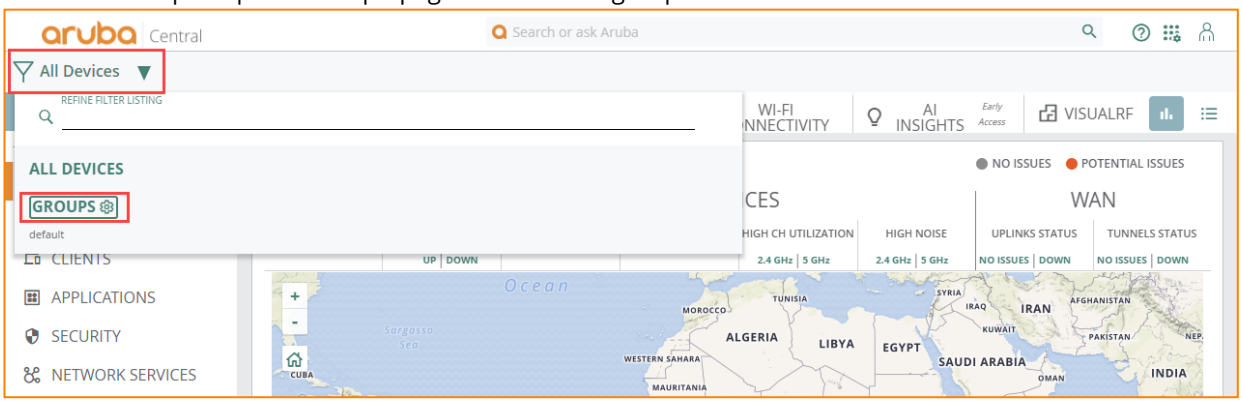
2. When logging in for the first time, there will be a prompt to add new devices to the Central account. This can be done now within the prompt or can wait until later on in the staging process.



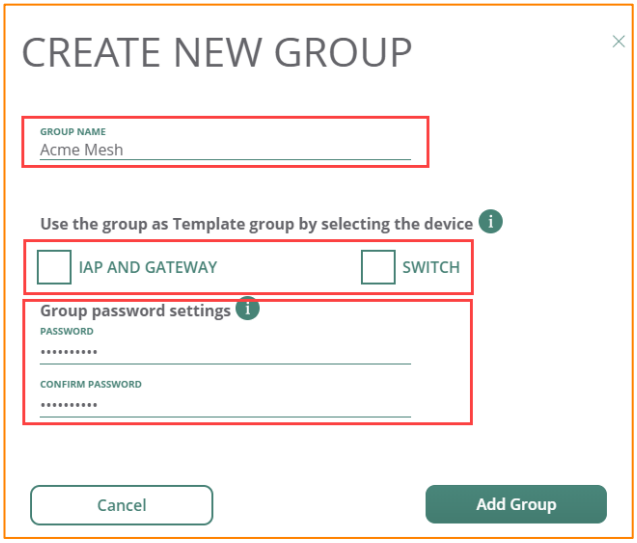
3. After adding devices, or after skipping this step to add the devices later, the 'Account Home' page will be displayed. This is the main page used for adding licenses, subscriptions and devices to the Central account. Assuming the Subscriptions and the Device Inventory has been added, click on 'Network Operations' to log into the Central management dashboard.



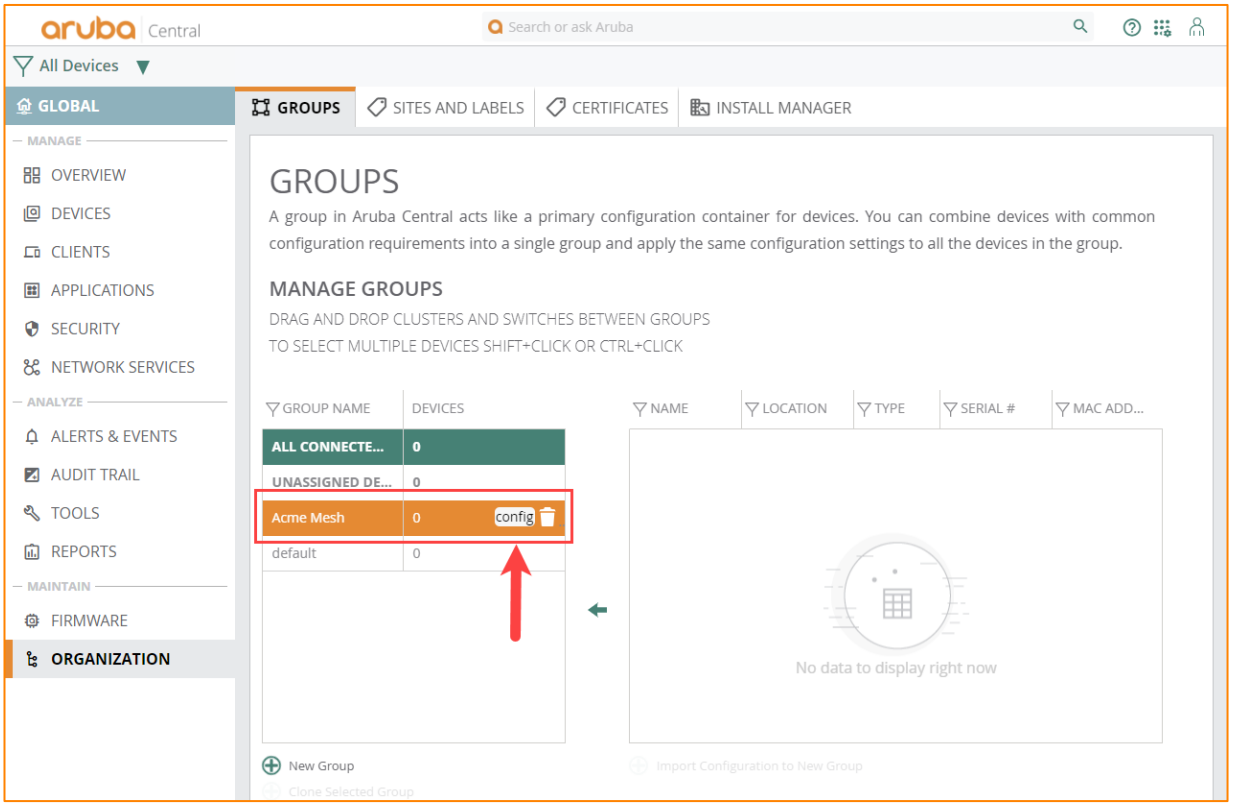
4. Once logged in to the main page, in the top-left, click on 'All Groups' and click on the 'Groups' link with the gear icon. This will open up the 'Groups' page where a new group will be created for the new mesh APs.



5. In the 'Create New Group' prompt, enter a name for the new mesh AP group, uncheck 'IAP and Gateway' as well as 'Switches' as we are not creating any template groups. Enter a password for the new group as this will be the password applied to the individual devices within that group should they need to be accessed.



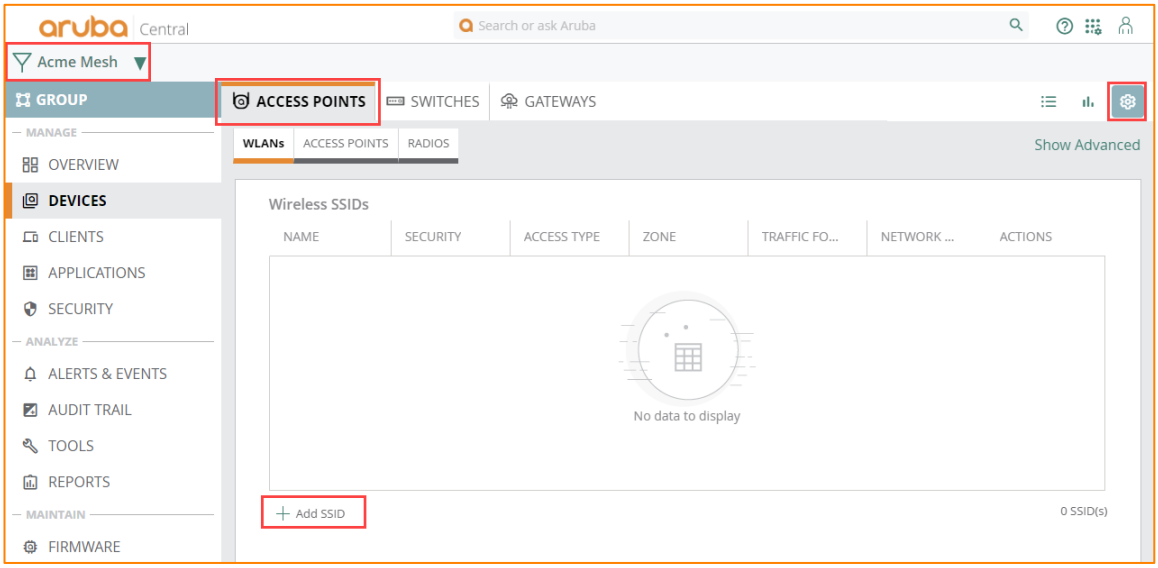
6. With the new mesh AP group created, mouse over the new mesh AP group and click on the 'Config' button to open the Group Configuration page.



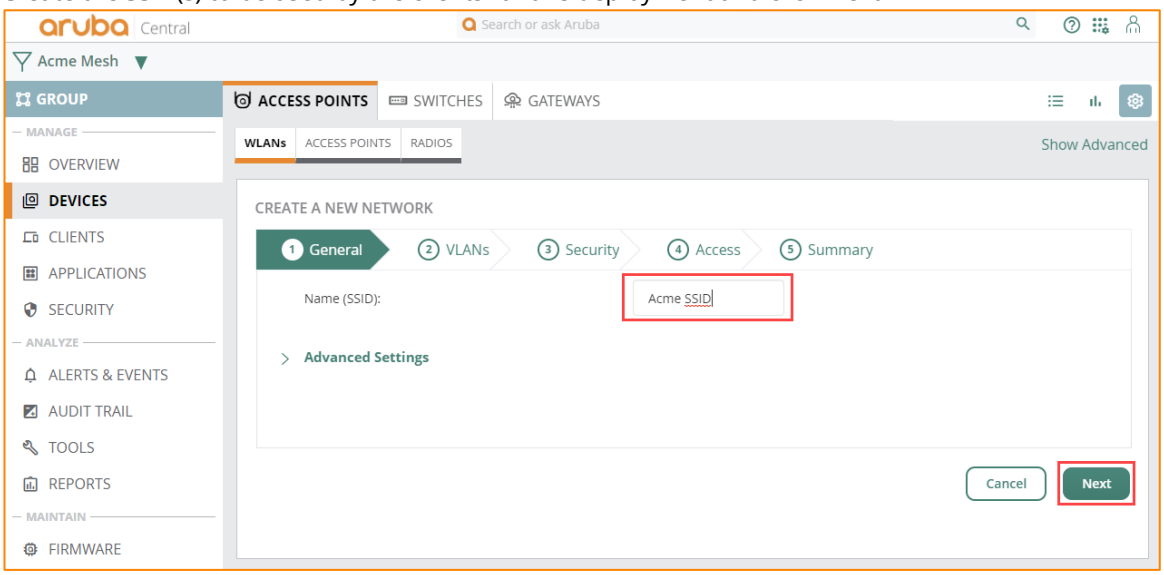
CONFIGURE THE NEW MESH AP GROUP SETTINGS

With the new mesh AP group created under Central, the following steps will go through creating the group settings so that once the new APs are brought up in Central and assigned to the mesh AP group, it can more quickly inherit the settings to make the deployment go faster.

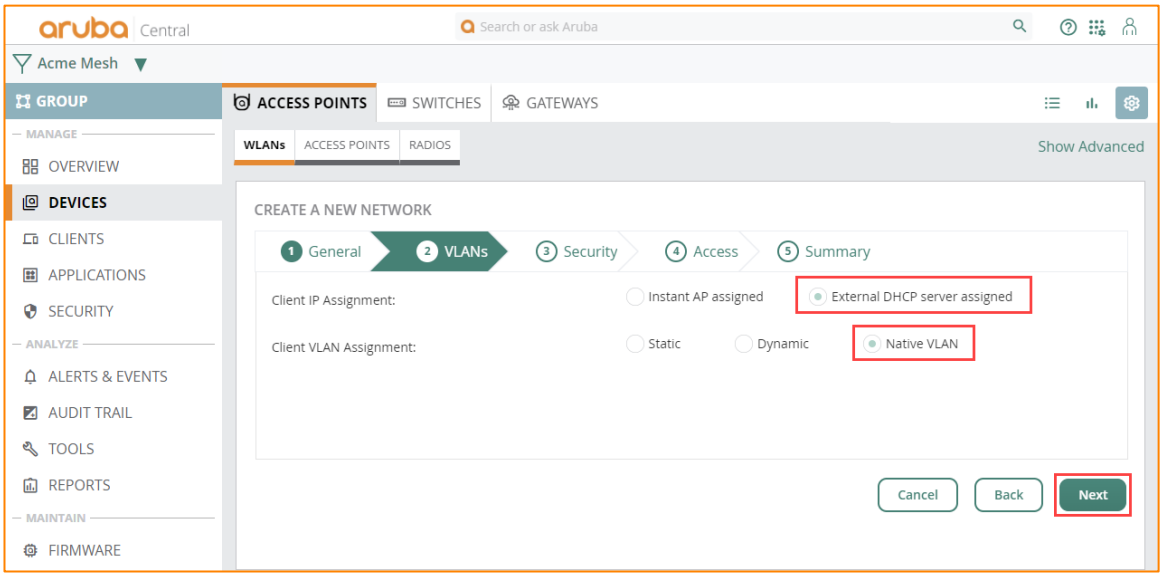
1. Inside the new AP group, under Access Points, click on the 'WLANs' tab and click the "+ Add SSID" button in the lower-left



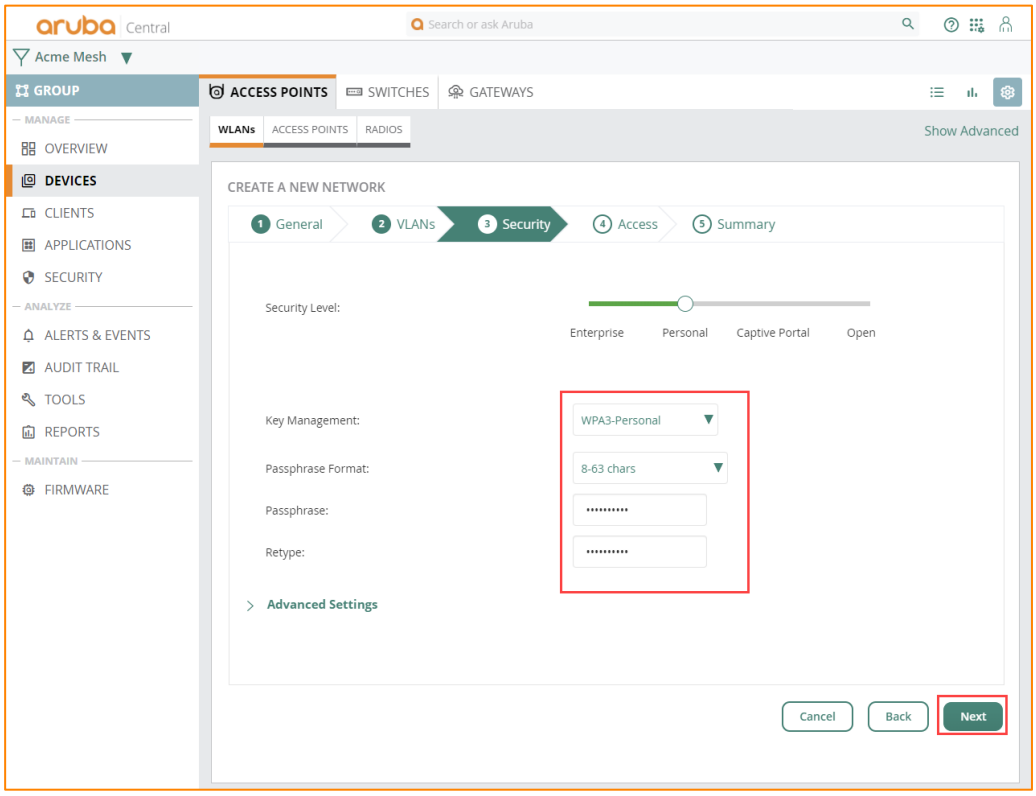
2. Create the SSID(s) to be used by the clients for this deployment and click 'Next'



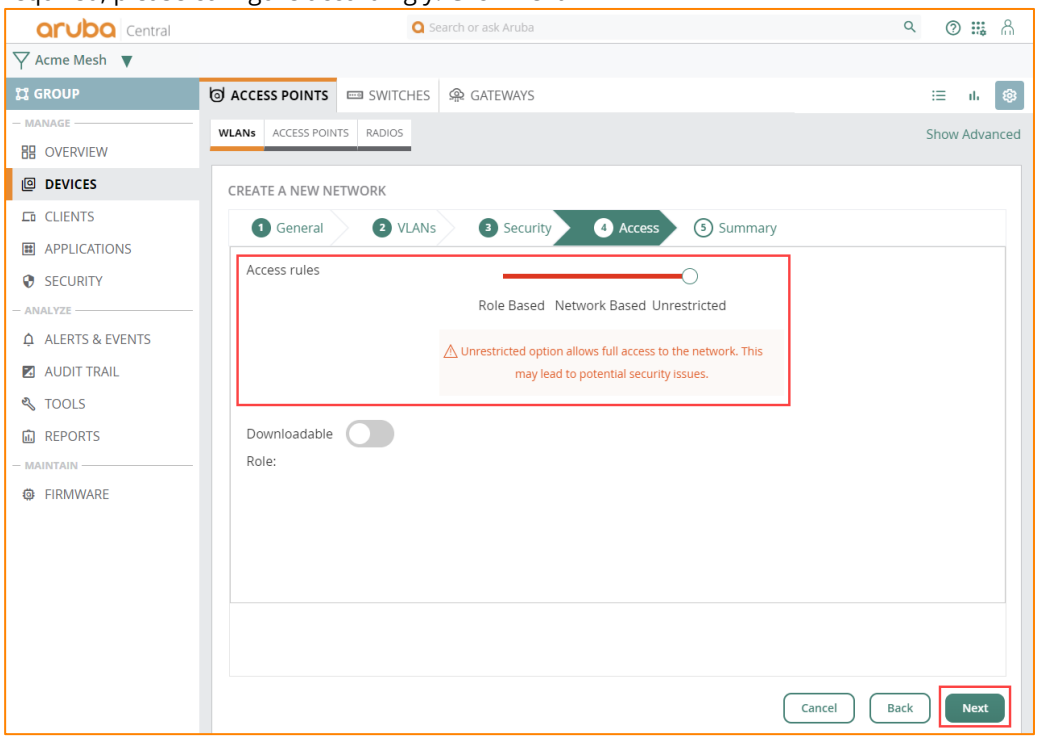
3. Configure the VLAN and network settings for the user SSID being created. Note this configuration is ultimately decided by how the APs are uplinked to the network. If an SSID needs to be in a trunked VLAN on the AP's uplink port, then the appropriate VLAN settings should be applied. In this example, the users will be on the same flat VLAN as the APs. Click 'Next' when done.



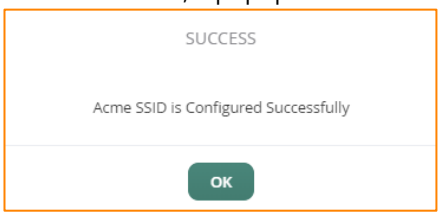
4. Configure the appropriate security settings required for this new SSID. The below example is a WPA3-PSK SSID, but if other security settings are required (Open, WPA2-PSK, RADIUS-based solutions, etc.), please set accordingly. Click 'Next'



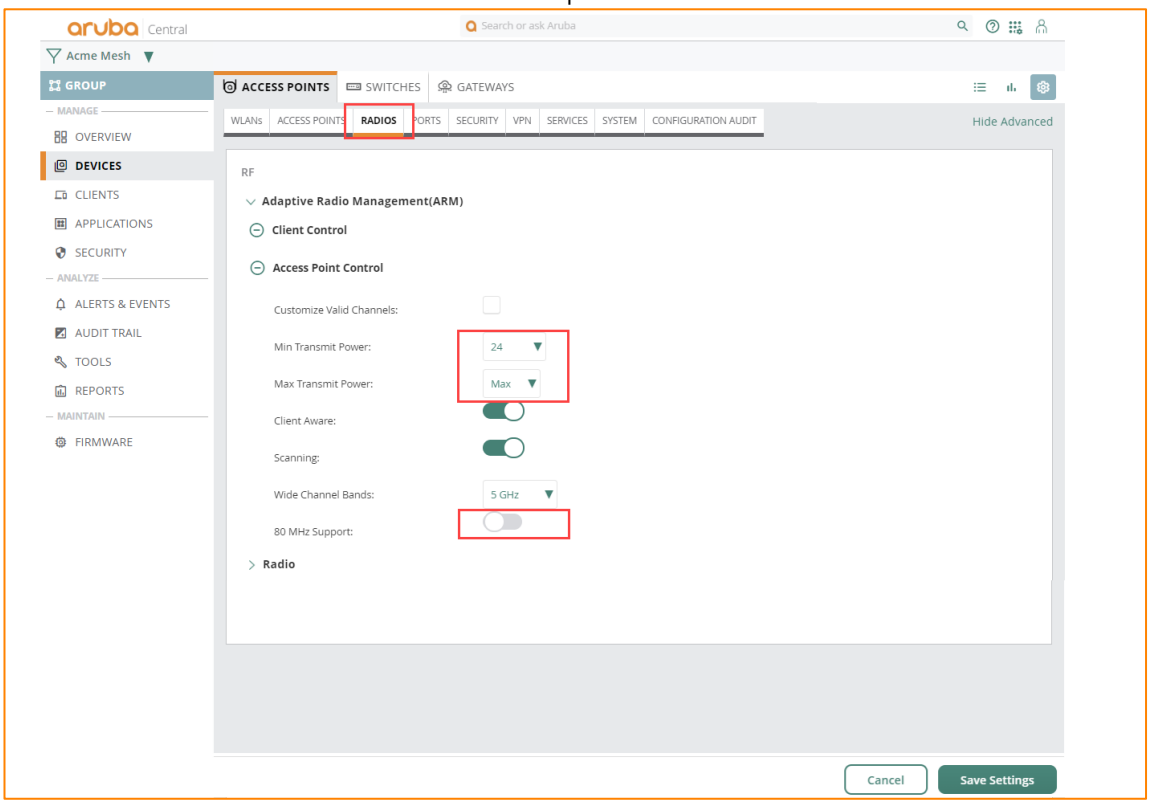
5. Apply any SSID Access Rules required. The below example is open to all traffic, but if a specific security policy is required, please configure accordingly. Click 'Next'



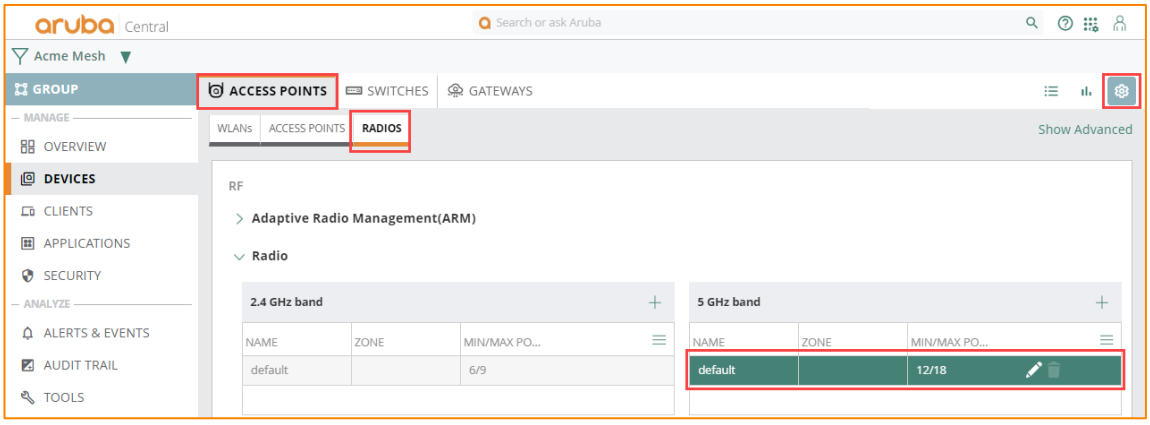
6. Review all elements configured for the new SSID in the 'Summary' page, if it all looks correct, click 'Finish'. Once 'Finish' is clicked, a popup will indicate the SSID was created.



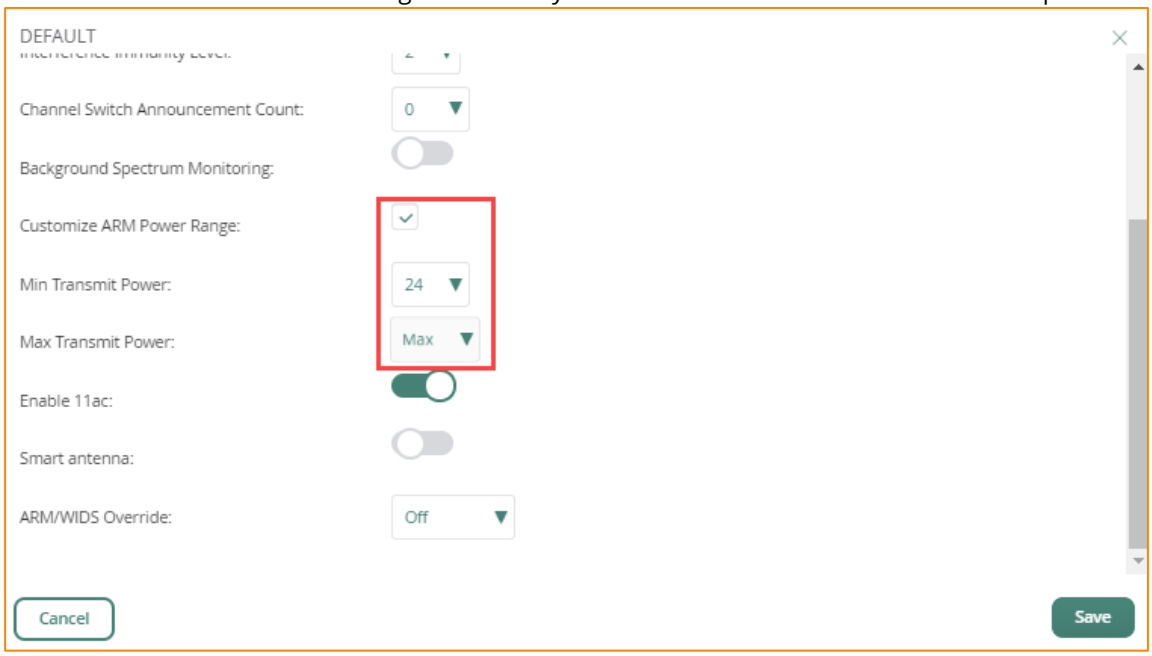
7. Next, click on the 'Radios' tab. Because in most cases for an outdoor AP mesh deployment, the APs being outdoors requires higher power levels to ensure range and coverage. As such, the 'Radio' settings should be modified so that ARM applies a higher power level to the APs radios. On the 'Radios' page, under 'Access Point Control', set the Min Transmit Power to '24' and the Max Transmit Power to 'Max'. Additionally, disable 80Mhz wide channels as well as 160Mhz wide channels if present.



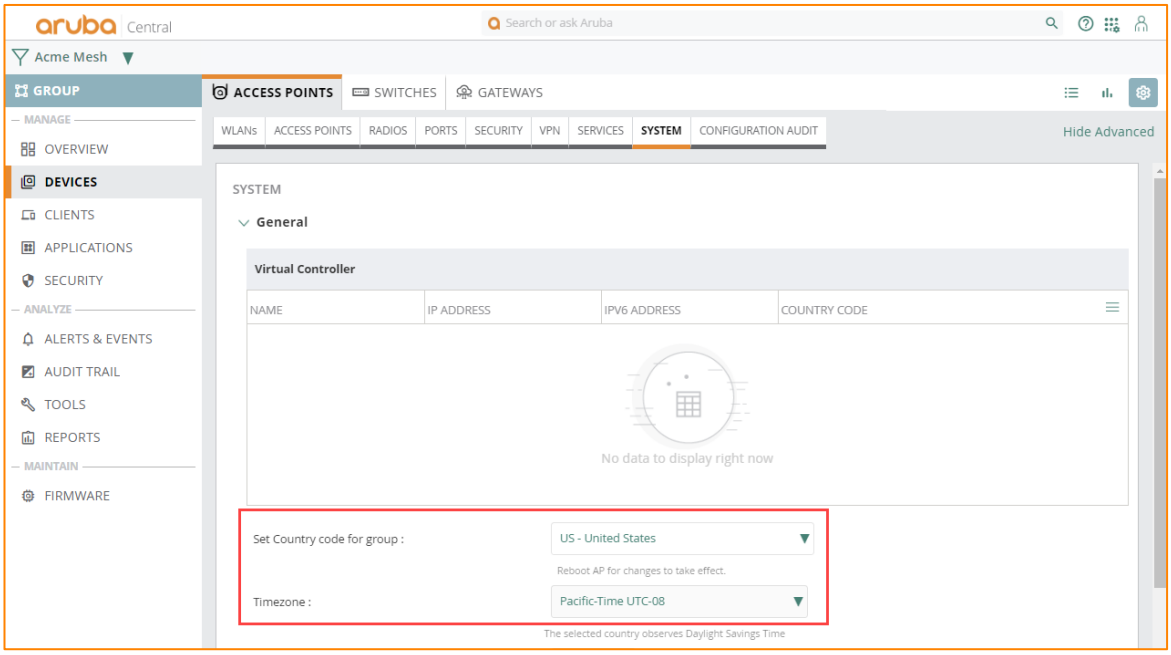
8. Additionally, within the 'Radio' tab, click on 'Radio' tab, and on the 5Ghz band modify the 'default' 5Ghz radio profile by clicking on the pencil icon.

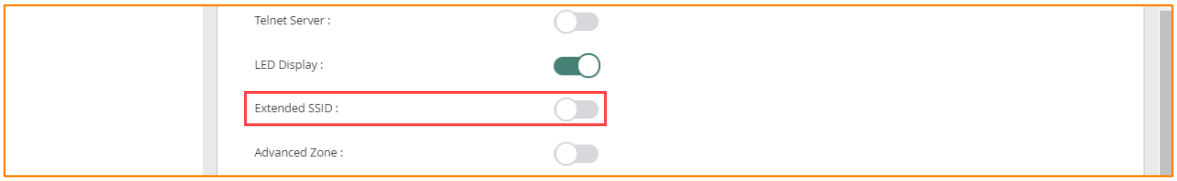


9. Check the 'Custom ARM Power Range' and modify the maximum and minimum to match Step 7.

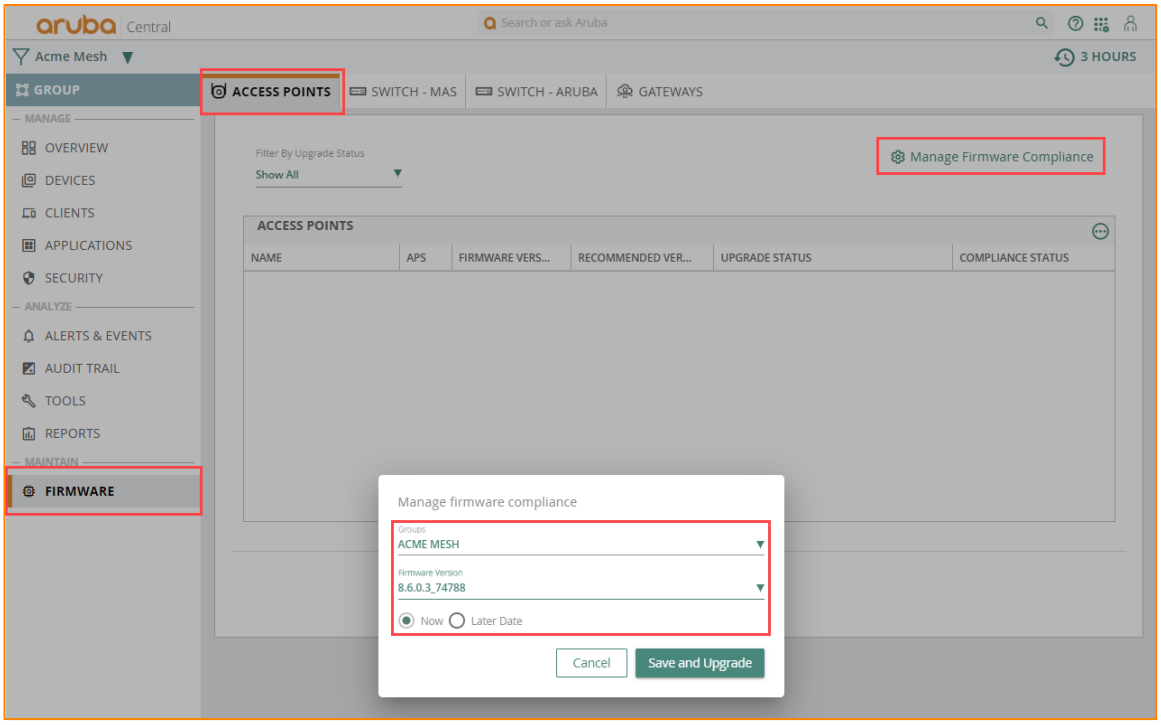


10. Next, the new Group 'System' configurations need to be applied. This consists of assigning a country code and time zone to the 'System' settings in the group. Additionally, because the APs in this group will be doing mesh, the 'Extended SSID' should be disabled. Once done, click 'Save Settings'.





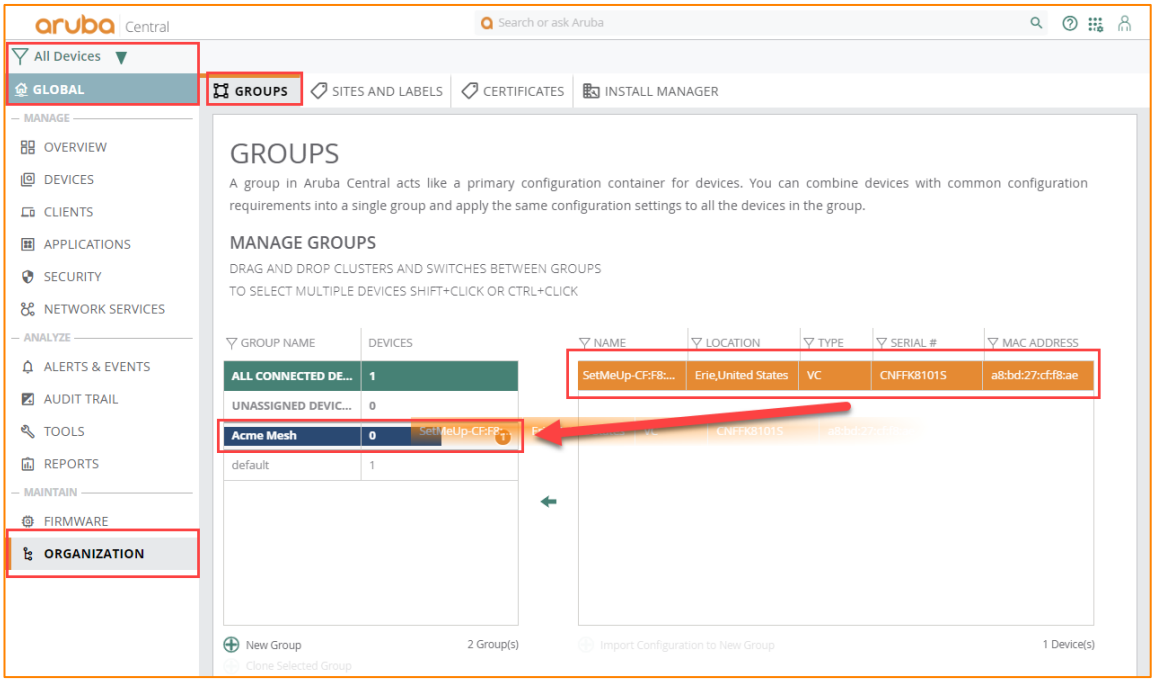
11. The last step in staging the Central group settings is to set 'Manage Firmware Compliance' for the devices assigned to this group. This will save some time so that once APs are assigned to this group, Central will automatically upgrade them to the specified version. Back on the main page under the new Central 'Group', click on 'Firmware', and go to the 'Access Points' tab. In the top-right, there is a 'Manage Firmware Compliance' link and once clicked, a popup will appear to define the group to apply the compliance policy to, as well as which version to apply. Once done, click 'Save and Upgrade'. No APs will be in this group once clicked, so there won't be anything to actually upgrade. But if APs are assigned to that group, they will start to upgrade.



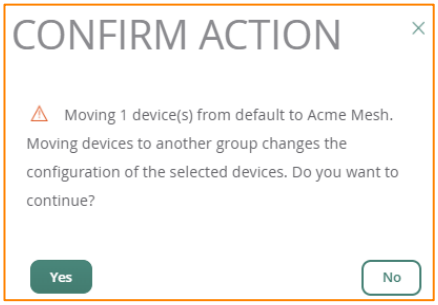
ASSIGNING APS TO THE NEWLY CREATED CENTRAL GROUP

With the new Central group defined and pre-staging settings applied, the APs can now be assigned to the new group from the 'default' group where new APs show up in Central.

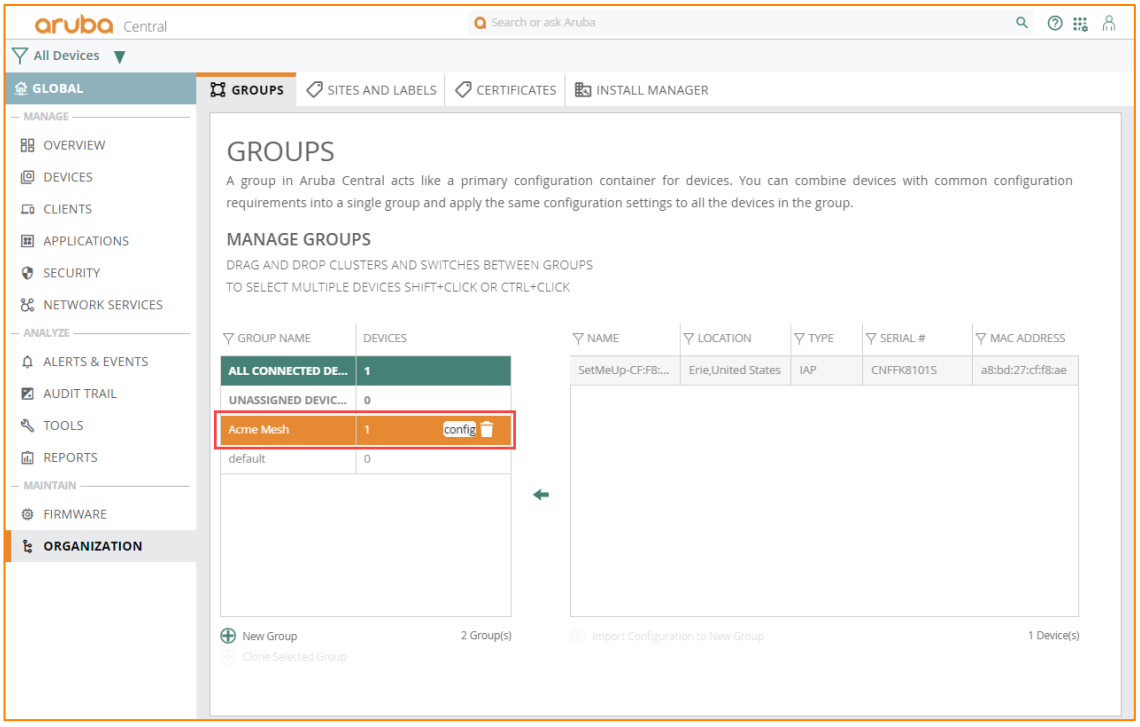
1. From the 'Global > All Devices' page in Central, go to 'Organization' in the lower-left and click on the 'Groups' tab. The newly deployed APs will show up in the 'default' group and will be visible in the right pane. Click and drag the Virtual Controller (VC) from the right pane into the newly created Central group.



2. A confirmation dialogue box will appear to confirm the move.



3. Once moved, the new Central group will reflect the new device(s) in the group. Click on the 'Config' button.

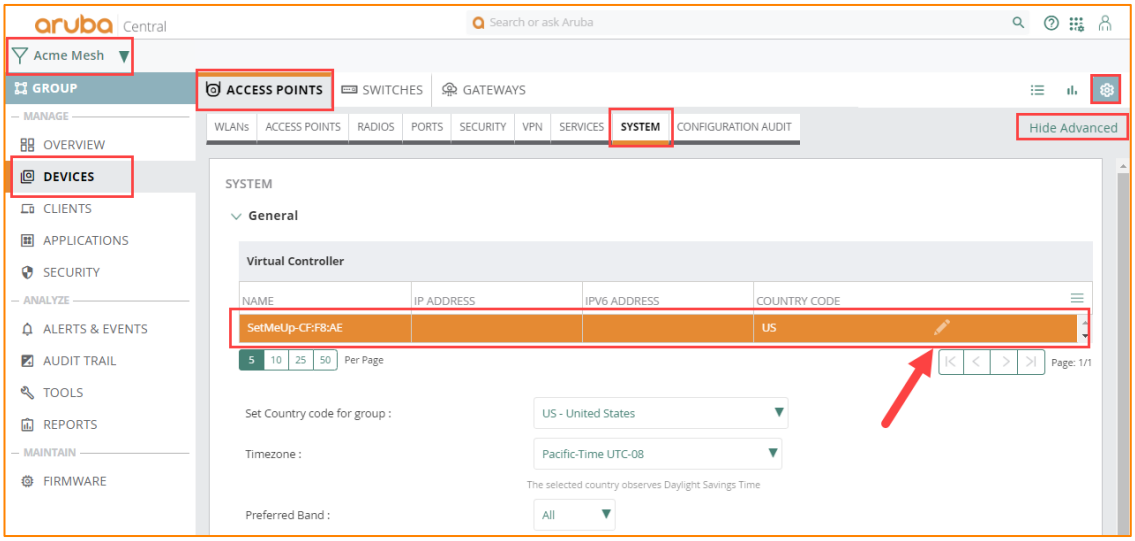


4. Clicking on the 'Firmware' link in the lower left should show the newly added APs upgrading to the firmware version defined in the 'Manage Firmware Compliance' in a previous step. If so, wait for the APs to finish upgrading before moving on.

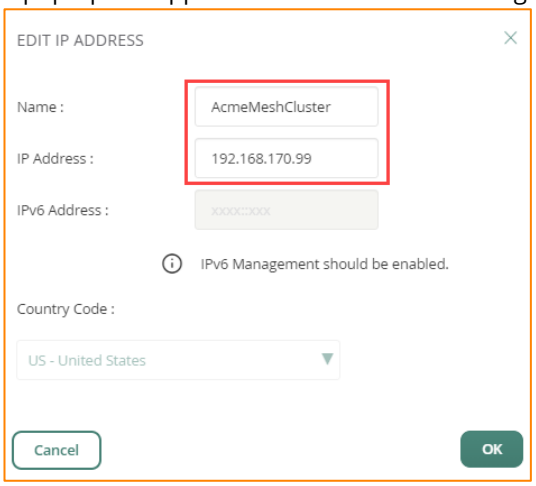
CONFIGURING THE APS IN CENTRAL

After the firmware is finished upgrading to the specified version, the APs are ready to be configured. This includes naming the APs, setting any AP specific configuration elements, and configuring the mesh points.

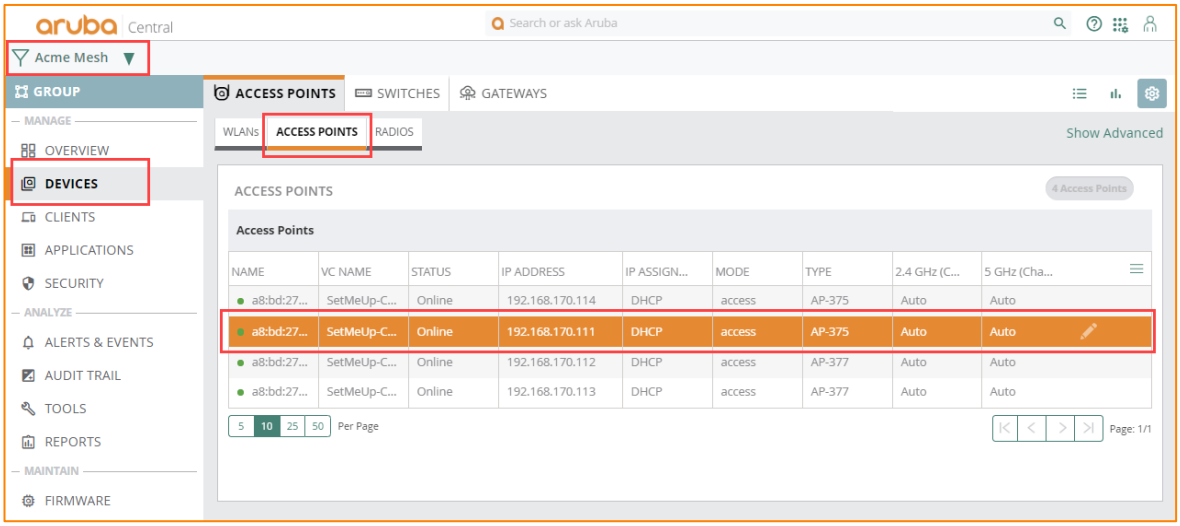
1. Go to the new Central group, click on 'Devices', and under 'Access Points', the new APs should show up with the default Virtual Controller (VC) name and the AP names should be their wired MAC address. To start, click on 'Show Advanced' and click on the 'System' tab. The default 'SetMeUp' Virtual Controller (VC) should be present. Click on the pencil to edit the VC.



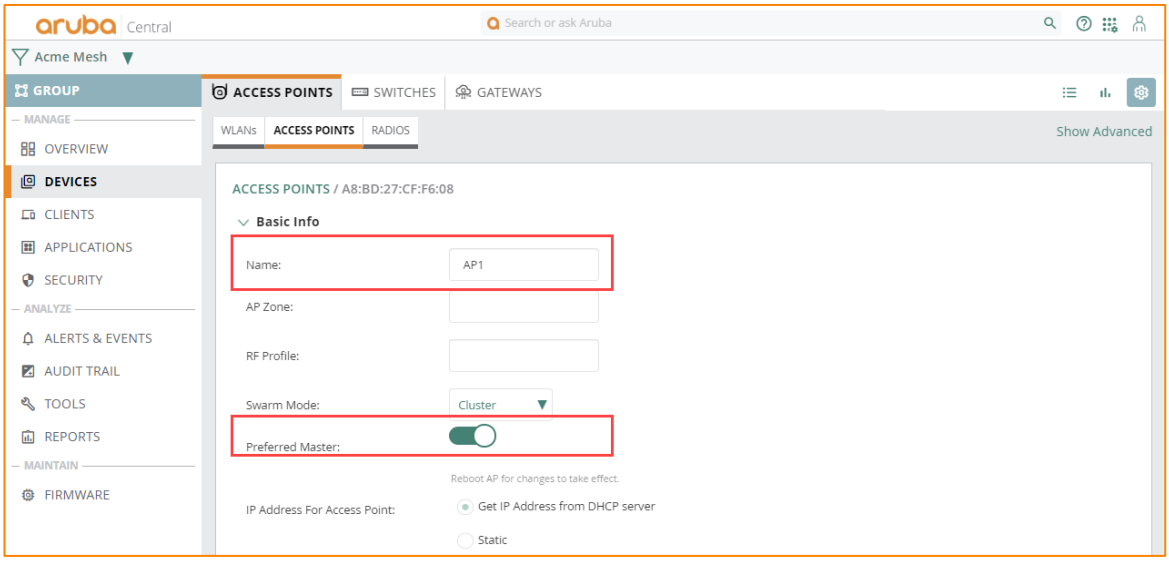
2. A pop-up will appear to name the VC and assign a virtual IP to the cluster (optional). Click 'OK' when done.



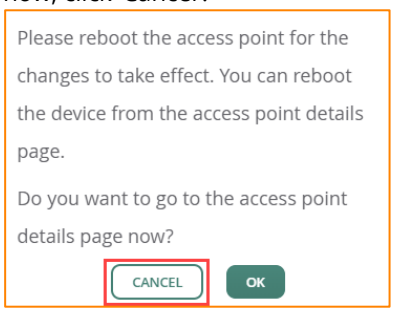
3. Once the 'System' settings are done, go back to the 'Access Points' tab and click on the AP that will be designated the portal. Once highlighted, click the pencil icon.



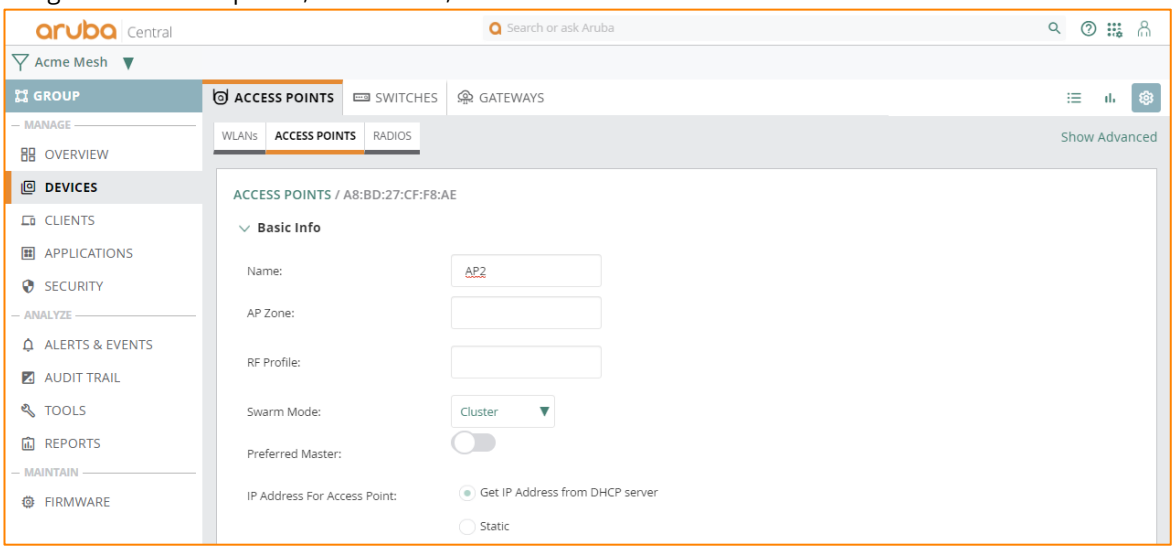
4. Name the portal in accordance with your naming convention to identify this AP as the portal. Additionally, the portal should be defined as the “Preferred Master” to ensure the VC master is on the wired network. Click ‘Submit when done.



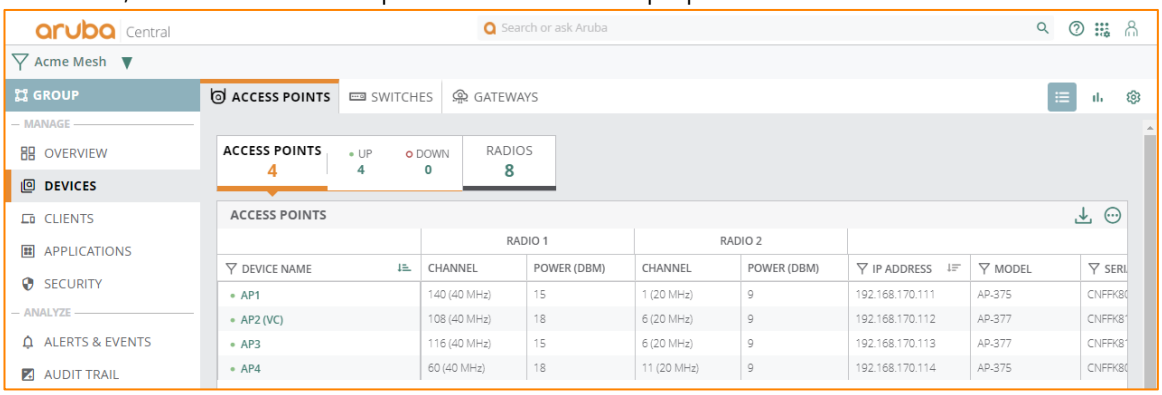
5. There will be a prompt to reboot the AP, and it will ask if it should load the AP details page to reboot the AP. For now, click ‘Cancel’.



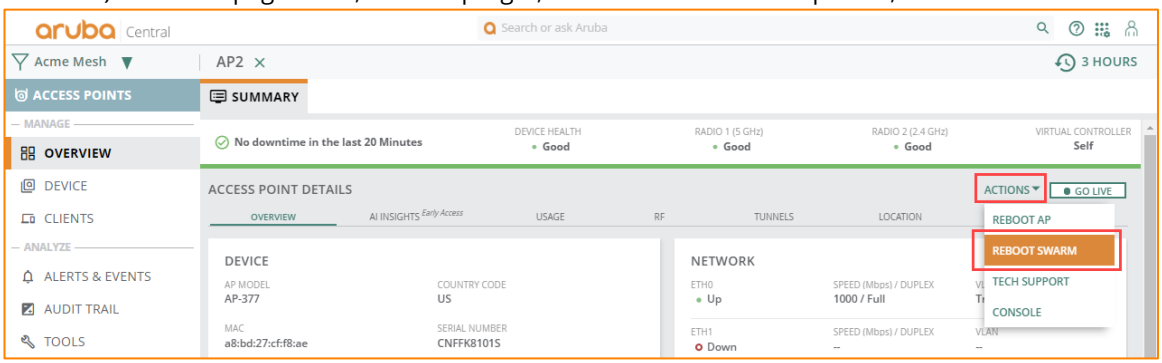
6. Do the same thing for the APs that will be designated as the mesh point(s). Click on the APs that will be designated as mesh points, name them, and click 'Submit'

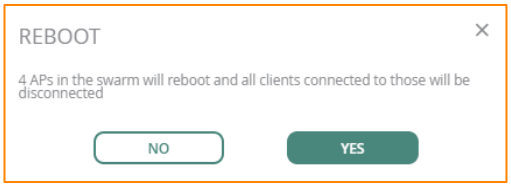


7. Once done, all APs should show up in the AP list with the proper name.

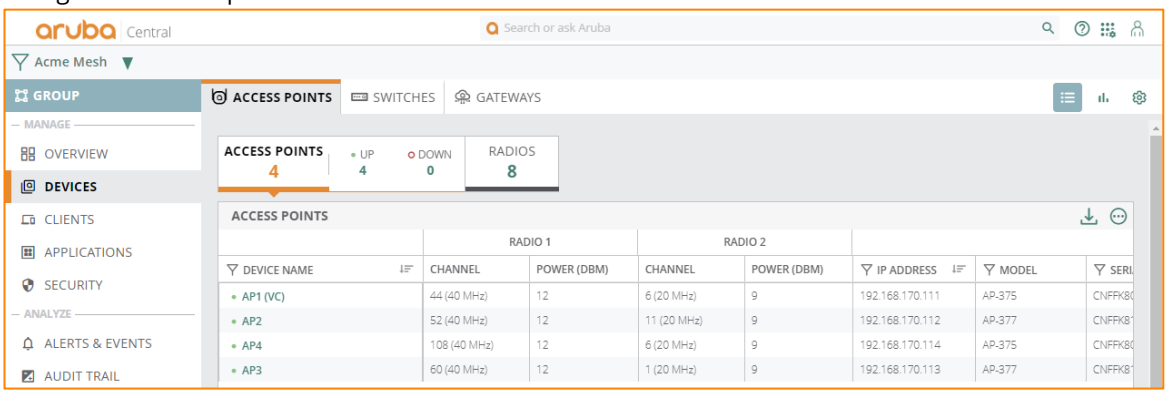


8. Once it's verified that all APs are named correctly, click on the current VC AP (identified by the "(VC)" label next to the AP). Once the page loads, in the top-right, there is an 'Actions' dropdown, select 'Reboot Swarm'.



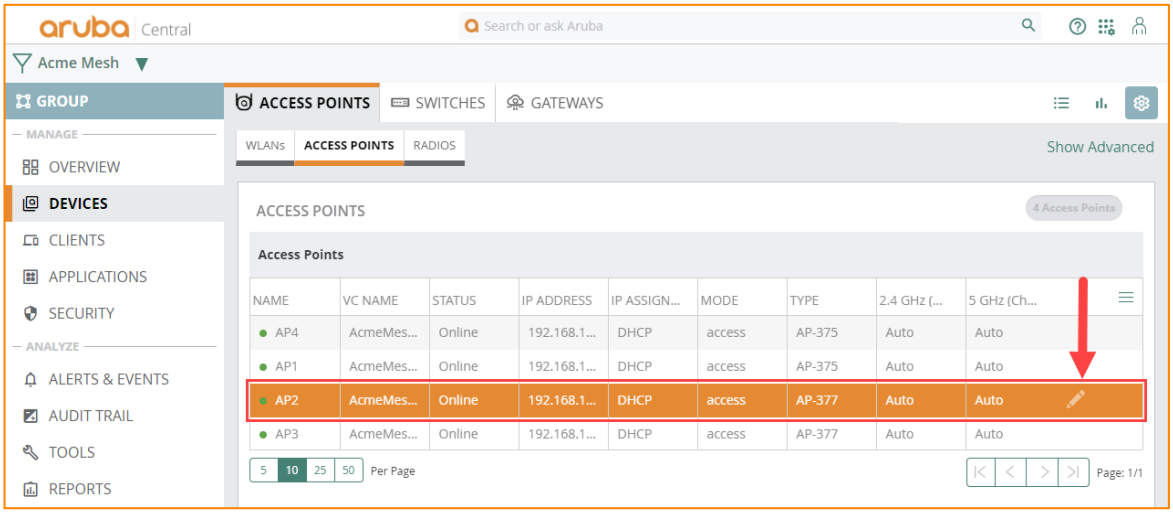


9. Once all the APs have rebooted, the designated VC AP should be identified as the 'VC' AP. The next steps will configure the mesh points.

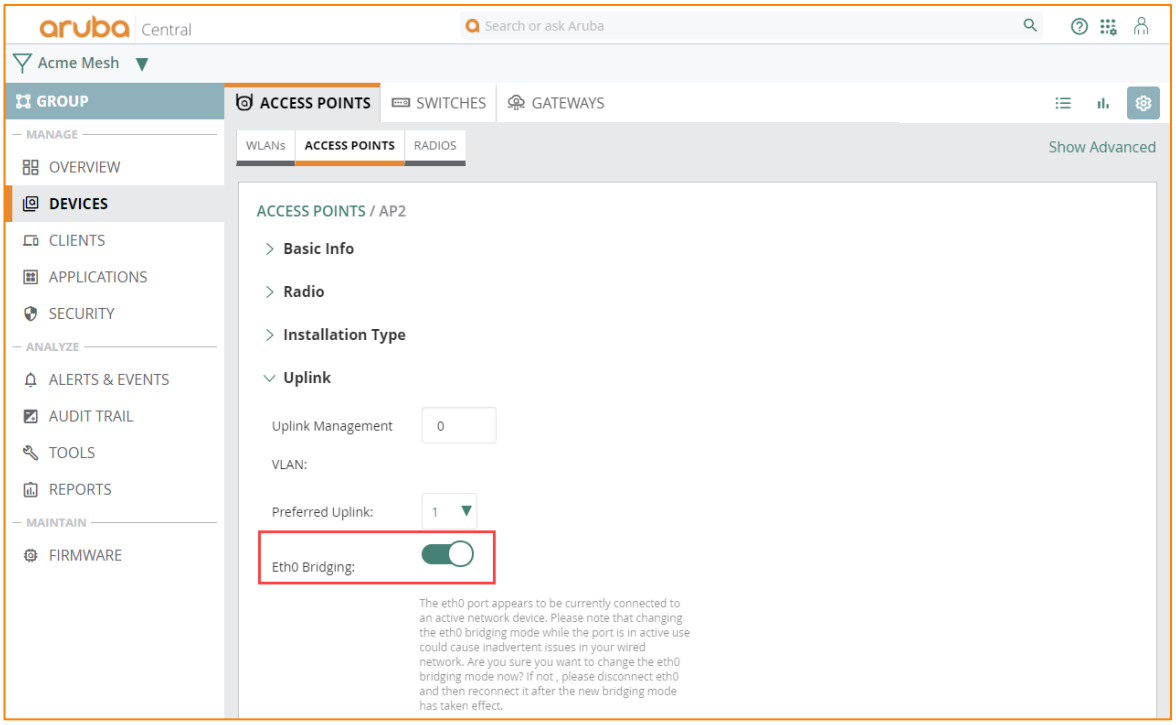


CONFIGURE THE MESH POINTS

1. Once the APs have rebooted, the mesh points are ready to be configured to operate with mesh. For the APs to be configured as mesh points, click on each AP and click the pencil icon to edit the AP.

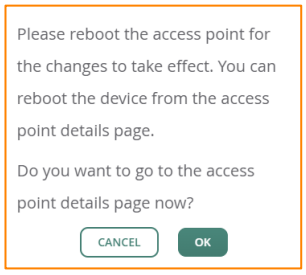


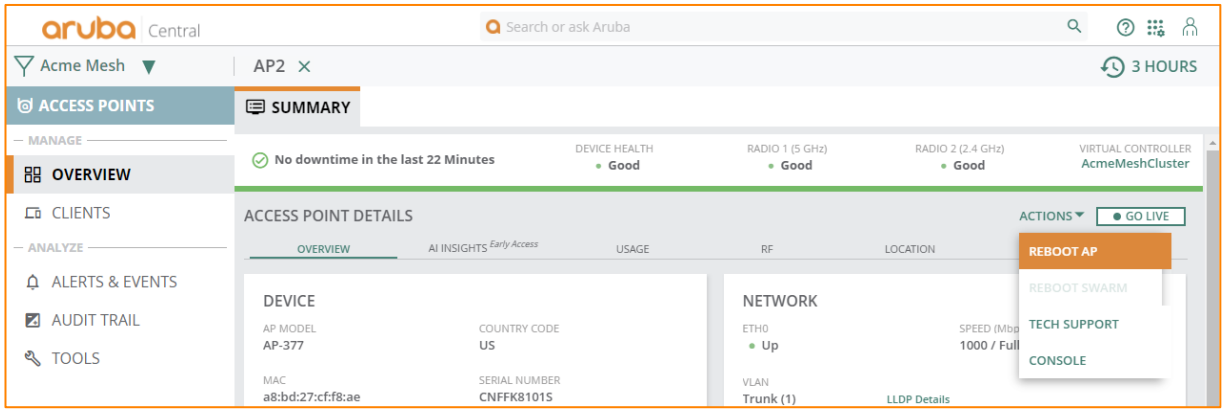
2. Enable 'Eth0 Bridging' on the mesh point and once done click 'Submit'.



3. Once submitted, a popup will prompt to reboot the AP and will redirect to the AP details page. Click 'Cancel' as we will configure all the points and then reboot them all together. However, if you want to reload the AP to deploy as they are configured one by one, reboot the AP and once it reboots, disconnect from the network and power up off the network to ensure that it comes up as a mesh AP before taking it to its final location.

NOTE: As there can be a slight delay between submitting a change from Central to the AP, and then the AP writing the actual command into its configuration, it is a best practice to wait at least 1-2 minutes after making a configuration change before rebooting and disconnecting the AP from the network. Otherwise, the configuration for 'Eth0 Bridging' may not get written to the AP and as a result, the AP may not come up on mesh until it's reconnected to the network to fully inherit its config.



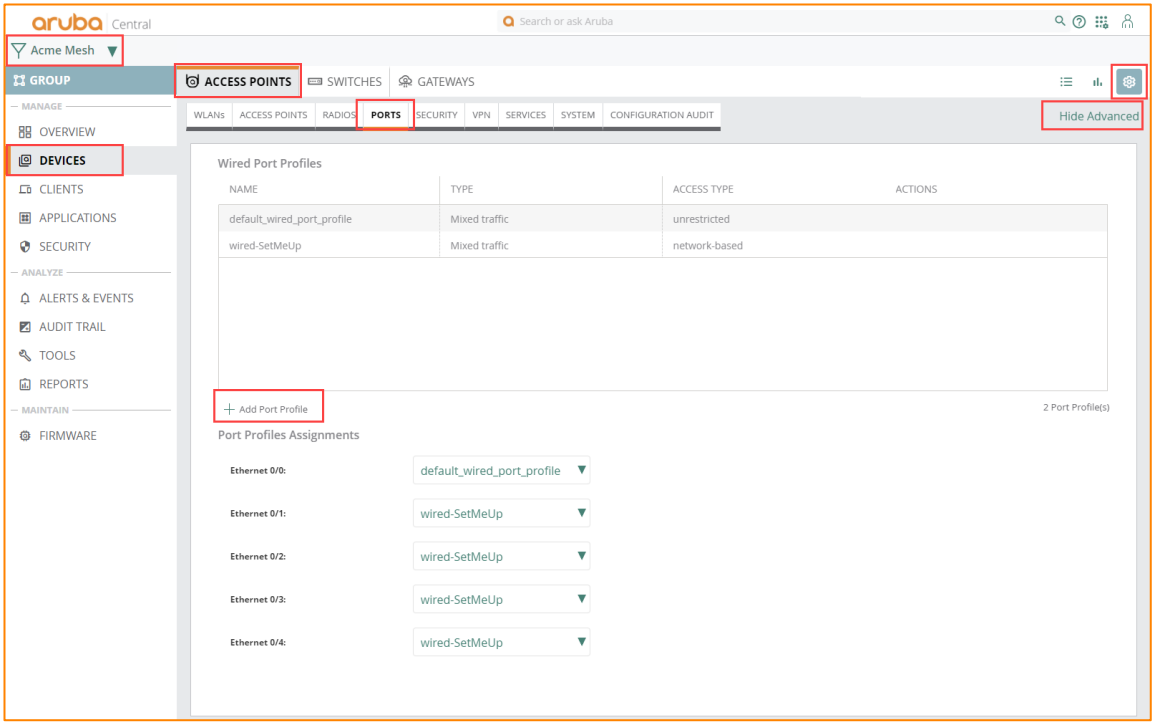


4. Once all the mesh point APs have been configured, the resulting network should have the portal AP up along with all mesh points up in Central.

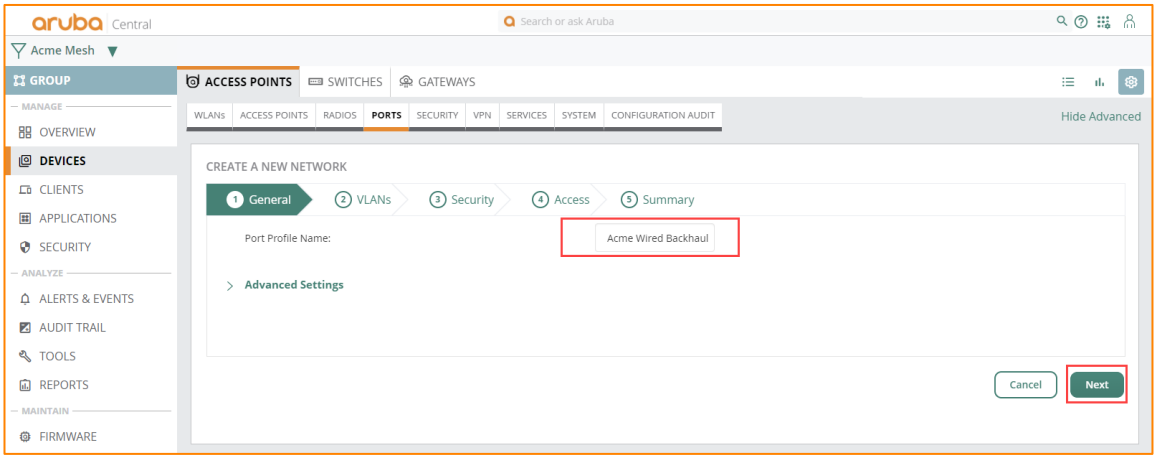
MESH SETUP WITH WIRED BACKHAUL

If there is a need to connect a switch or a wired device to a mesh point to backhaul wired network traffic from the remote switch on the mesh point back to the main LAN or internet, perform the following steps.

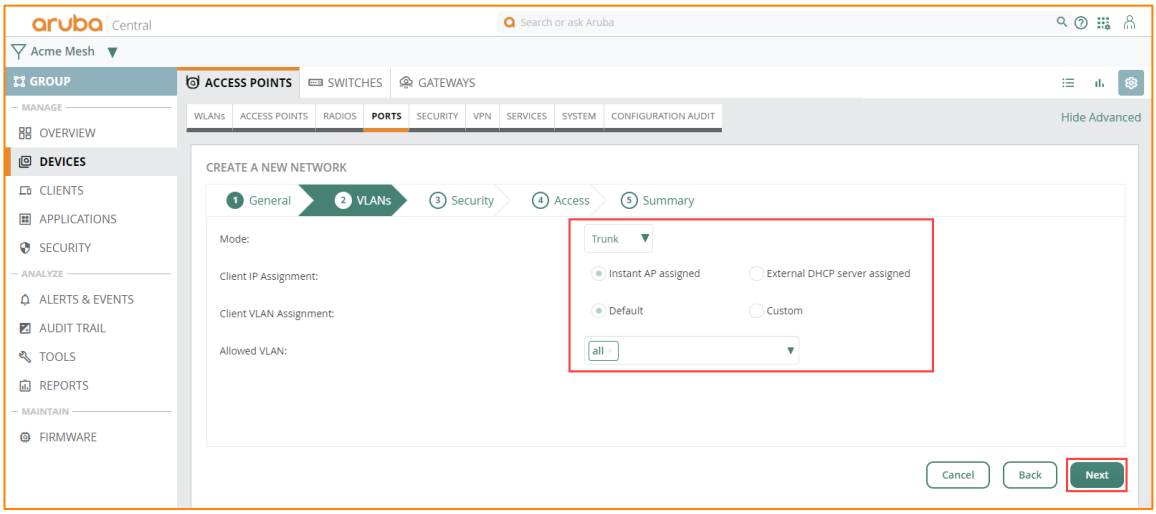
1. In Central, in the newly created Central group, click on 'Devices' and then 'Show Advanced' under 'Access Points' and click on 'Ports' to show the 'Wired Port Profile' settings for the APs.



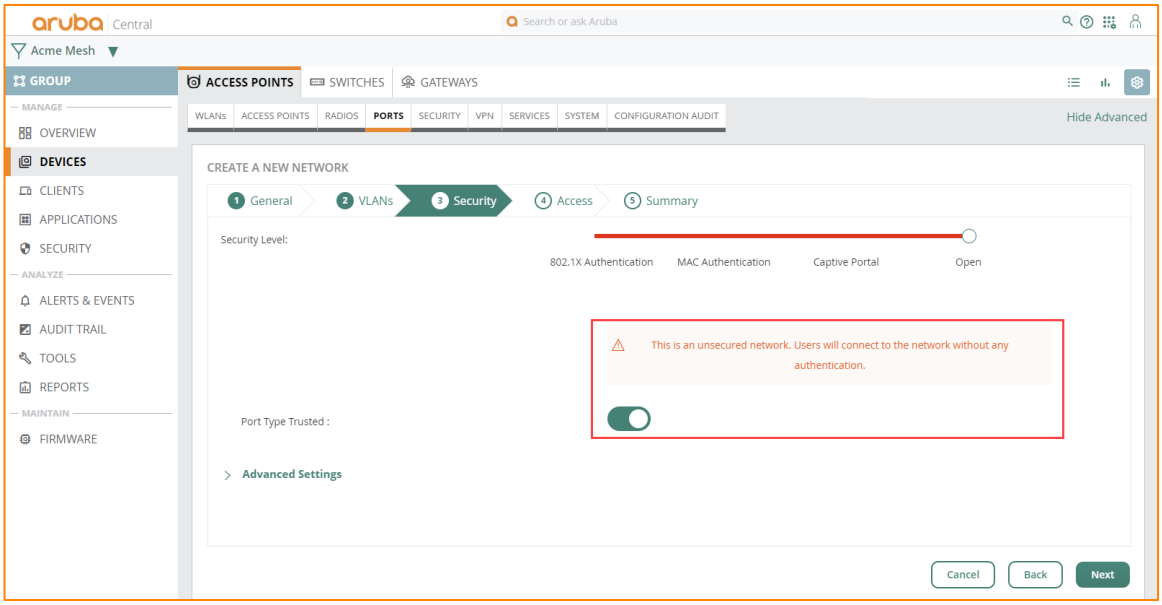
2. Create a new 'Wired Port Profile' that will be assigned to the APs in this Central group. Provide a name to use for this new profile and click 'Next'.



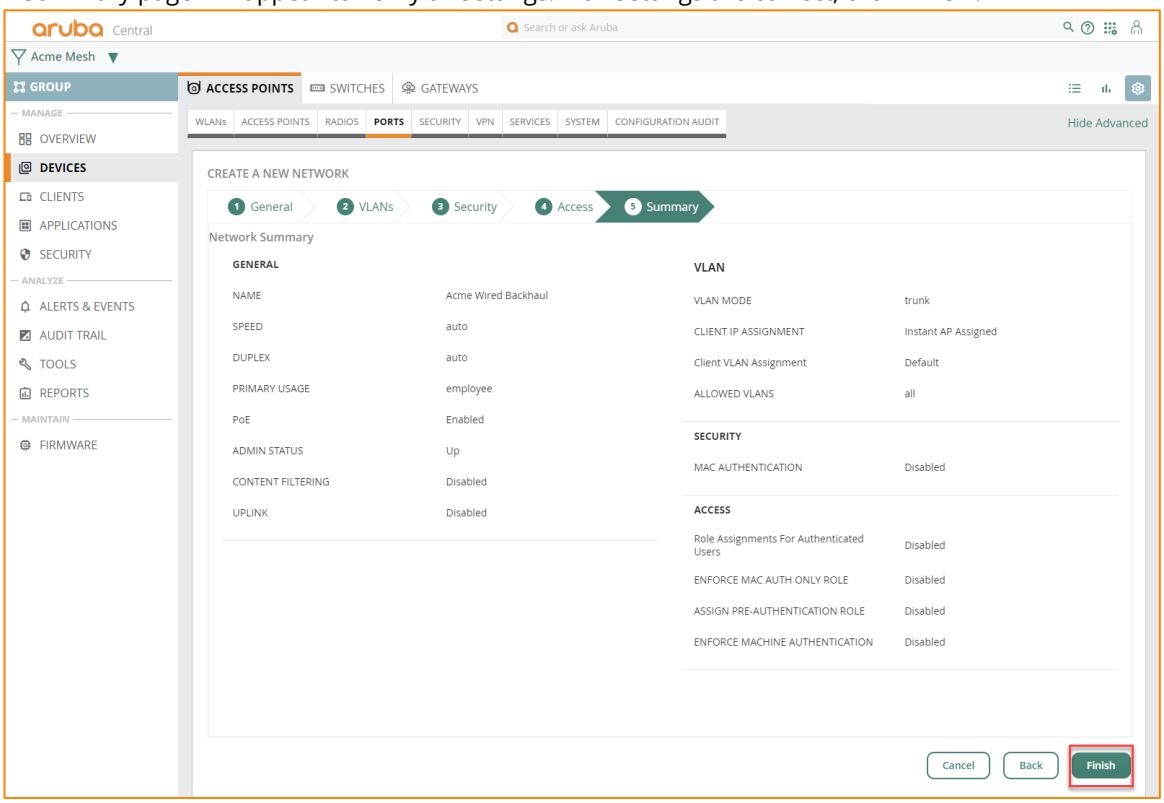
3. Configure the network settings for the AP's wired port. Note this will depend on the wired network uplink config on the portal's side as well as the mesh point side. Because Instant Mesh bridges, the network settings should match on each side for the AP's uplink and downlink interfaces. By default, the setting is 'Trunk' mode, native VLAN of '1', and 'all' VLANs are allowed to ensure maximum compatibility. Set as required for your site. Click 'Next'.



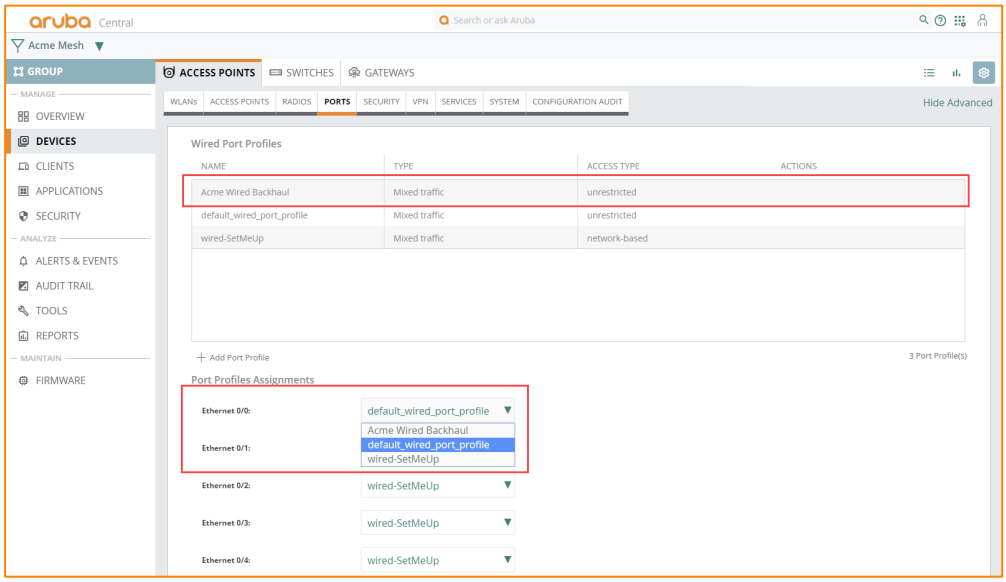
4. If necessary, created a wired security profile to apply to the wired port. Otherwise, set security to 'Open and mark as 'Trusted' to ensure all traffic is allowed over the mesh link. Click 'Next'.



5. A Summary page will appear to verify all settings. If all settings are correct, click 'Finish'.



6. Once the 'Wired Port Profile' is created, the new wired port profile needs to be applied to the APs on the appropriate Ethernet interface of the AP. For single port APs, this would be 'Ethernet 0/0'. If this is a multi-port AP, it should be applied to the port where the wired port profile should apply.



At this point, there should be a mesh portal with one or more mesh points up and active and connected to Central. Additionally, if wired backhaul was enabled, the mesh points should also be providing wired network services out of the mesh points' wired interface. This should all be tested in a lab or on a bench in a controlled environment before physically deploying the AP. This would include making sure all APs are up, that all settings are applied and correct, and that if wired backhaul services are offered, that clients, switches and devices have wired access over the mesh points to the main LAN.

CONCLUSION

Using the information in this document, a quick and capable Central managed Instant-based mesh network can be deployed in a rapid fashion to provide quick, reliable coverage in hard to reach areas, while also allowing for remote monitoring and management of the network. The logistics of a setup still have to be solved including: WAN or Internet traffic and how the clients and devices get out to the internet, power solutions for the hardware in use in a parking lot, or remote facility, and what infrastructure would be required to mount the APs to (tripods, light poles, stationary vehicles or trailers, etc. are all viable with creative solutions). Aruba's AP mounts are very simple, fast, and easy to use.

Please use the following links to find supporting documentation on Aruba's products, and if there are any questions, please reach out to your Aruba SE or Partner for more information.

Aruba Access Points

- https://www.arubanetworks.com/products/networking/access-points/

Outdoor AP Mounting Brackets

- https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/EntryId/28815/Default.aspx

aruba
a Hewlett Packard Enterprise company
www.arubanetworks.com
3333 Scott Blvd. | Santa Clara, CA 95054
1.844.472.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | info@arubanetworks.com