Aruba Remote Access Point

Simplified Configuration Guide to Accelerate Deployment

Version 1 – March 18, 2020

Prepared by: Ayman Mukaddam

Email: ayman.mukaddam@hpe.com

Contents

1 Introduction

To help our customers maintain business continuity, we are sharing a brief technical configuration guide on how to setup Aruba Remote Access Points (RAPs) for both AOS 6 and AOS 8 deployments. If you need additional information, feel free to reach out to your local partner to help you implement a solution that meets your needs. Please note that this document doesn't cover all cases / requirements but is intended as a quick start guide to cater for the majority of our customer's immediate requirements.

2 High Level Architecture

At a high level, Aruba Remote AP will be deployed at the home office. It will establish an L2TP/IPSEC connection to the mobility controller located in the Headquarter. This AP can extend the same networks available at the office so employees can work from home as if they are in the office without needing additional VPN clients.

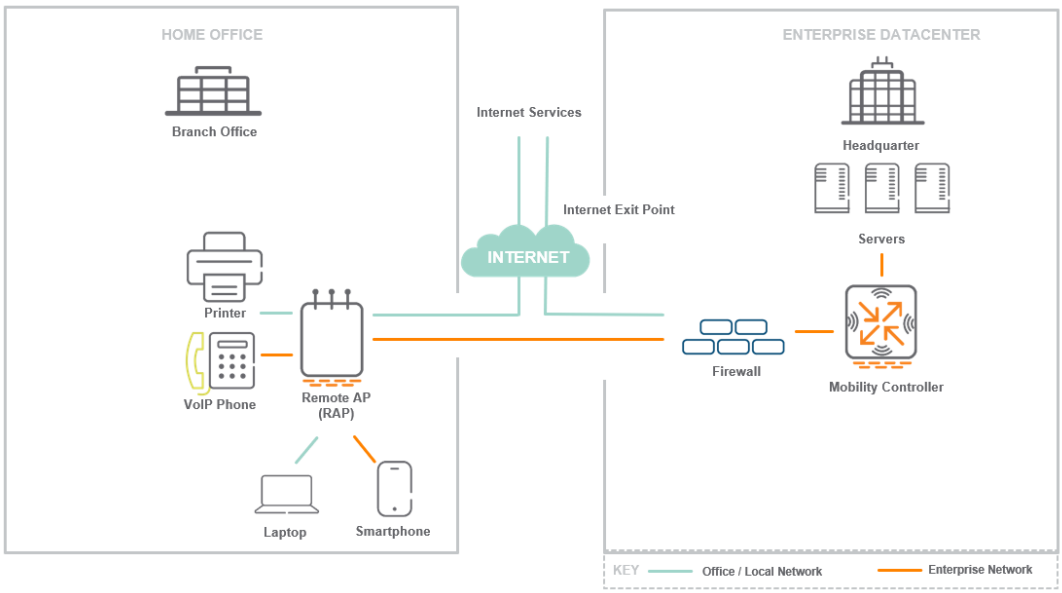


Figure 1: Aruba Remote Networking Solution - Home Office

Aruba offers specific AP models which are mainly intended to work as Remote APs since they offer additional wired ports, external power supply, desk-mount stands and optional PoE-out to power additional devices.

Figure 2: Remote Access Point with Desk-mount Stand

However, in reality, **any Aruba AP** can be configured to work as Remote AP making it easier for our customers to reuse their existing APs and deploy such solution faster without compromising on security.

From a centralized controller, the network admin can fully configure the **wireless networks & wired ports** of the RAPs in

- **Tunnel Mode** where all traffic is tunneled back to the corporate network
- **Bridge Mode** where traffic is bridged locally and not sent back to the corporate network
- **Split-Tunnel Mode** where the network admin decides which traffic is tunneled back and which traffic is bridged locally.

This offers the needed flexibility to extend the corporate network to the home office. If the chosen AP model has additional wired ports, the network admin can even configure them to connect additional devices like IP Phones, printers, PCs, switches ... etc. As such both the wired and wireless networks can be easily extended to the remote home office location. Needless to say, Aruba Remote APs also offer **zero touch provisioning capability** so the APs can be shipped to the site without initial configuration.

This document is intended to offer a brief quick guide on how to configure Aruba Remote APs. If you are interested to learn more about Aruba Remote Access Points and its unique capabilities, please check this link https://www.arubanetworks.com/assets/eo/EO_RemoteAccess.pdf

Sections 3 to 5 cover how to configure Aruba RAP if you are using AOS 6 or AOS 8. The document explains the setups based on a single Mobility controller but similar logic can be applied with redundant controllers.

3 High Level Steps & Pre-requisites

There are five main pre-requisites for a RAP to establish connectivity to a controller.

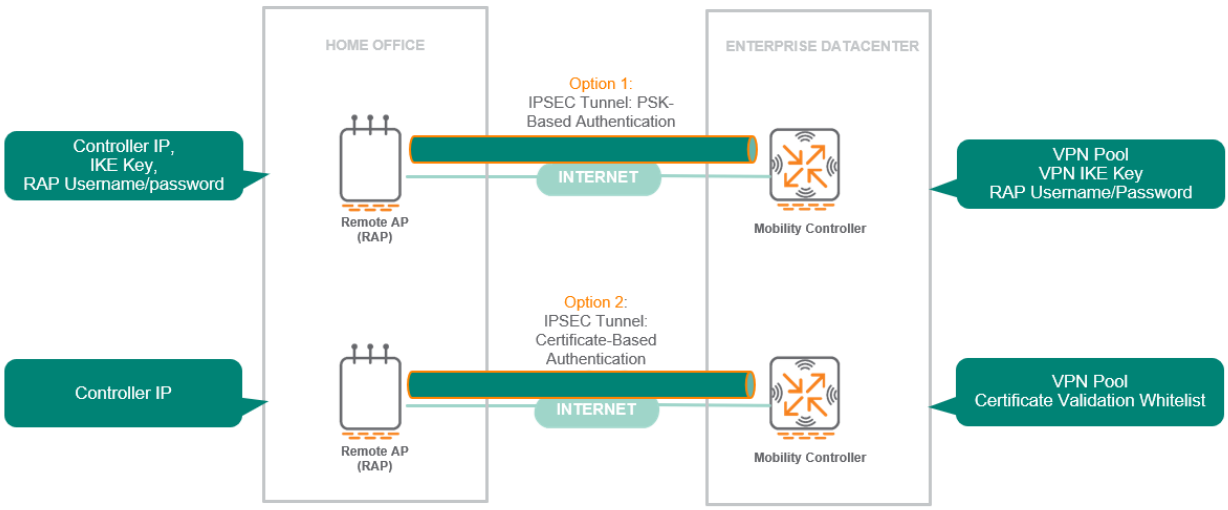
3.1 RAP needs to learn controller IP

The RAP needs to learn the controller IP (which is reachable from Internet). This can be done in several ways:

- By staging the RAP as a regular campus AP and then provisioning it as RAP
- By converting an Instant AP to RAP AP
- Using Aruba Activate: Aruba RAPs will automatically attempt to communicate with Aruba internet-based cloud service (Aruba Activate) to learn the controller IP. This can offer real ZTP capability

3.2 RAP needs to reach controller IP on UDP Port 4500

The RAP will build an IPSEC Tunnel to the Mobility Controller in HQ. The authentication can either be based on Pre-shared Key (PSK) or Certificates. To simplify the configuration, we will use the certificate-based authentication which leverages the built-in signed certificates available in all Aruba APs. The Remote AP needs to reach the Mobility Controller on UDP Port 4500 (NAT-T). The mobility controller can have a public IP itself or port forwarding needs to be configured from 3rd party devices like firewalls to Mobility Controller on port 4500.



3.3 RAP needs to authenticate successfully

The controller will not accept connections from any RAP. Depending on which authentication option is being used, the controller needs to be configured to allow the desired RAPs. The easiest option is to use certificate-based authentication for RAPs and whitelisting the RAPs on the controller or ClearPass.

3.4 RAP needs to be assigned an IP address from controller

The controller needs to provide an IP address for the RAP (inner IPs). A VPN pool needs to be configured on the controller.

3.5 RAP needs to be configured in a group

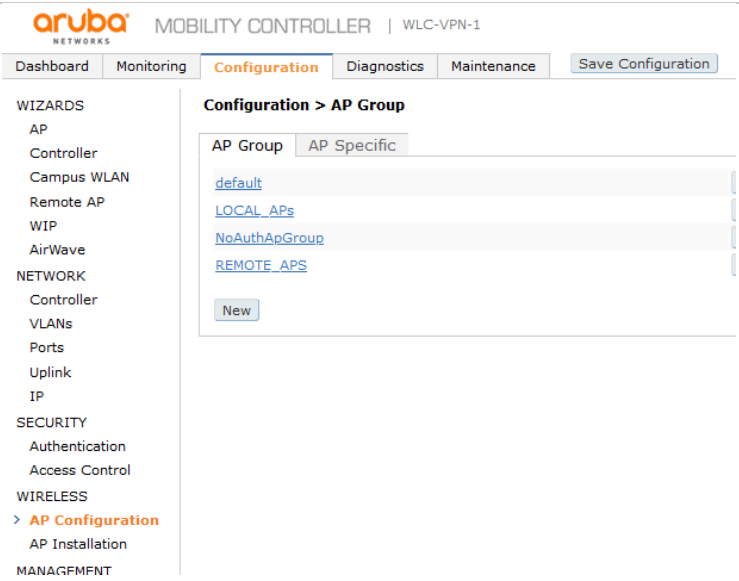
The RAP needs to be placed in a group to inherit the configuration of that group. If no group is defined, the RAP will be placed in default group. The RAP will take the configuration of that group including wireless and wired settings. This will cater for Virtual AP Profiles, WLAN Profiles, AAA Profiles, AP System Profiles configuration…etc.

4 AOS 6 – RAP Configuration (8 Steps)

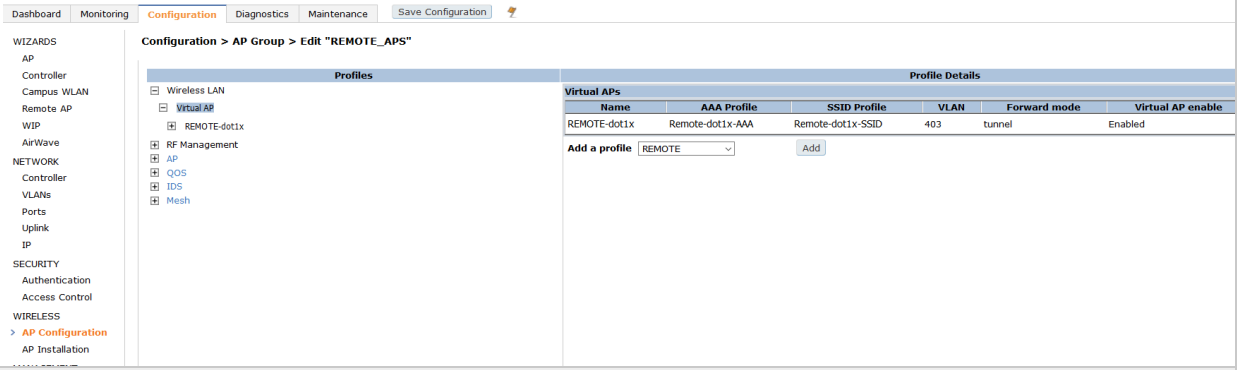
Section 4 includes the configurations based on AOS 6 setup. We have divided the configuration to 3 scenarios covering the majority of the deployment cases used by our customers.

4.1 Scenario 1 – Staging the RAP as CAP then provisioning it as RAP

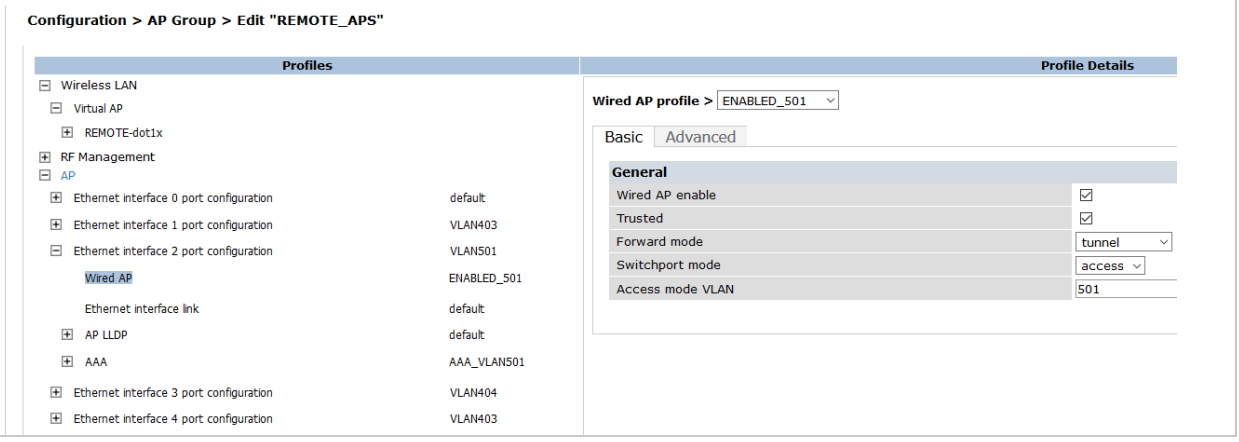
Scenario 1 – Staging the RAP as CAP then provisioning it as RAP
Step 1: Connect the RAP to your network and let it join the controller like a regular CAP – Steps not shown here
Step 2: Create a group for Remote APs (Recommended)



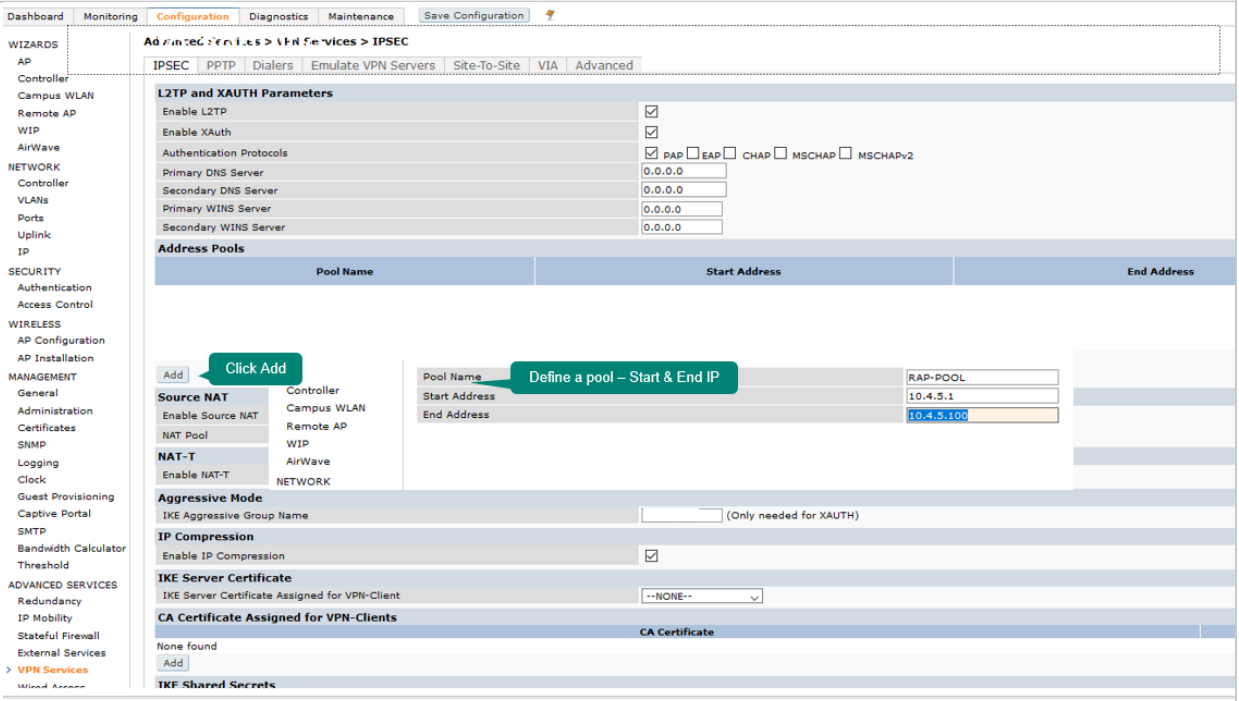
Step 3: Configure the Remote APs Group like a Campus Group (Add the necessary VAP, Wireless SSIDs, AAA profiles …etc.) You can use existing profiles or create new profiles as per your requirements.



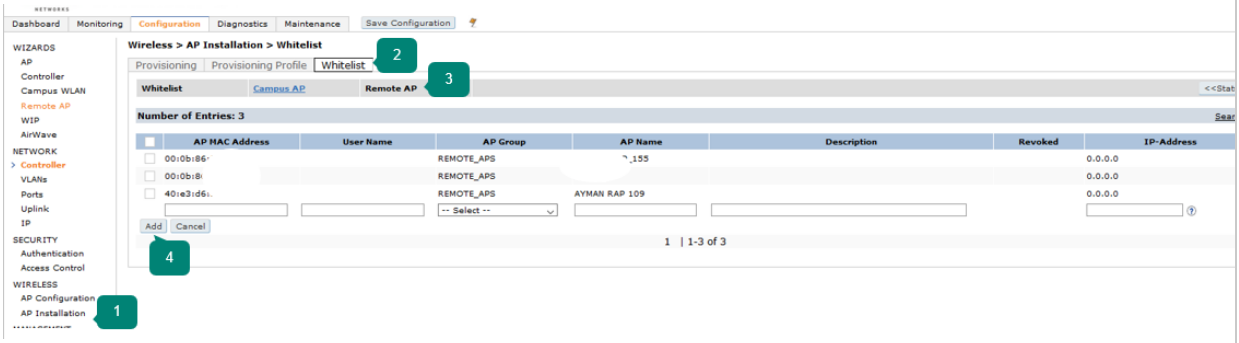
Step 4 (Optional): You can configure wired port profiles here in case you want to use other ports on the APs for wired connectivity (Eth0 is used as uplink so configure other ports depending on AP model). You can control whether wired traffic is trusted or not as well as the forwarding mode (tunneled, split-tunnel or bridged)



Step 4: Create a VPN Pool for RAPs – This is the inner IP that will be assigned for the RAPs. It shouldn't conflict with other IPs. It is not required to be routable.



Step 5: This step is not required if the AP was already provisioned as CAP. However, it is better to whitelist the RAP by adding its MAC address and assigning it to the Remote APs Group that was created in Step 1.

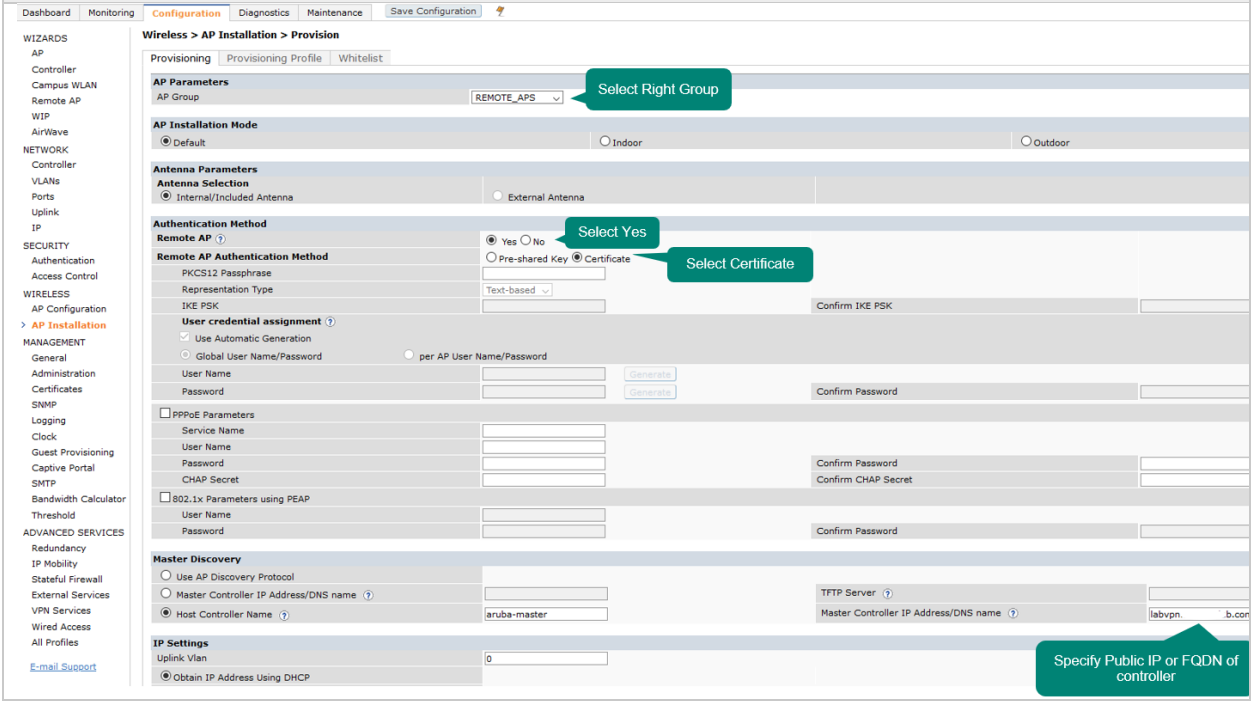


Note: If an IAP was converted to a RAP manually without staging, then the RAP whitelist command shown above (**whitelist rap add mac-address <MAC>)** is not enough. From the controller cli, the following command should be added as well if the RAP are authenticating locally on the controller.

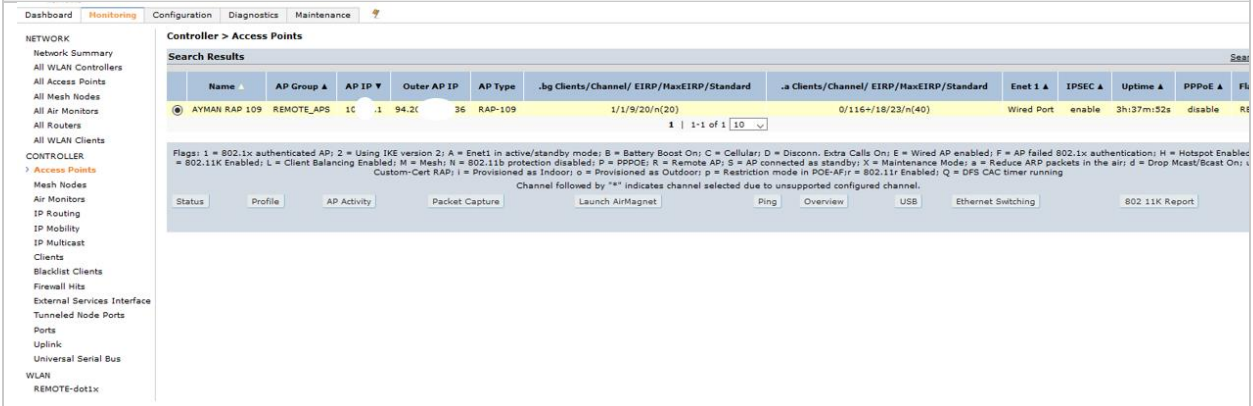
iap trusted-branch-db add mac-address <MAC> where <MAC> should be replaced with the MAC address of the remote access point.

The below commands can be used to verify that the MAC is whitelisted.
show whitelist-db rap
show iap trusted-branch-db

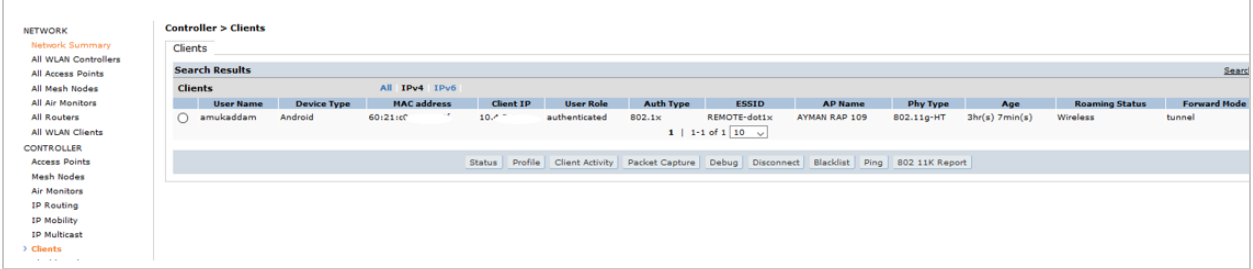
Step 6: Convert the CAP to RAP by selecting right group, making it RAP with certificate, specifying Controller Public IP and then pressing Apply & Reboot. Optionally give the AP a name.



Step 7: Disconnect the AP from the network and connect to the Internet where it can reach the controller public IP on UDP 4500. The AP will show up as RAP AP and it will broadcast the configured wireless networks.



Step 8: Verify Clients are able to connect and get the right role and VLAN.



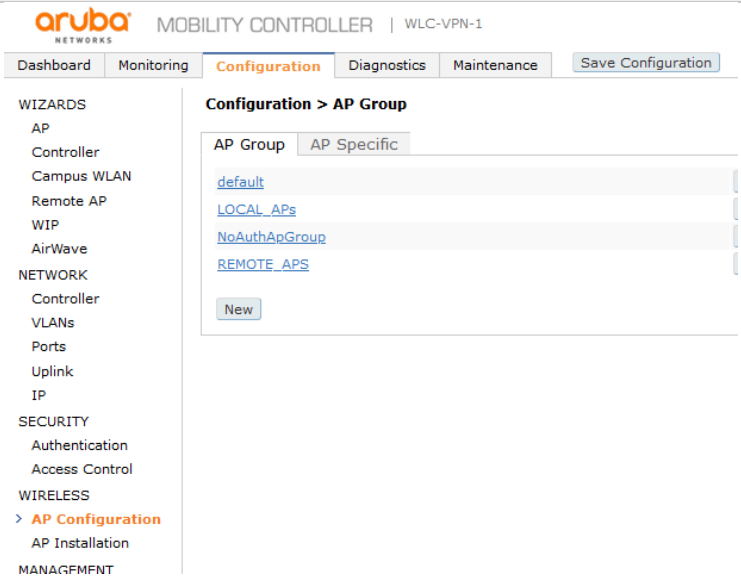
4.2 Scenario 2 – Converting an IAP to RAP

This scenario is similar to the first scenario with differences in steps 1, 5 and 6.

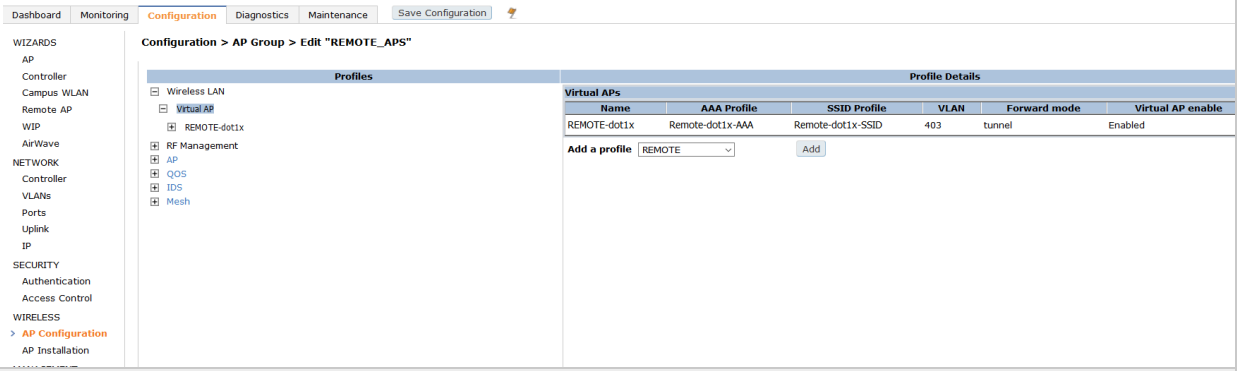
Scenario 2– Converting an IAP to RAP

Step 1: Staging is not needed so this step is skipped

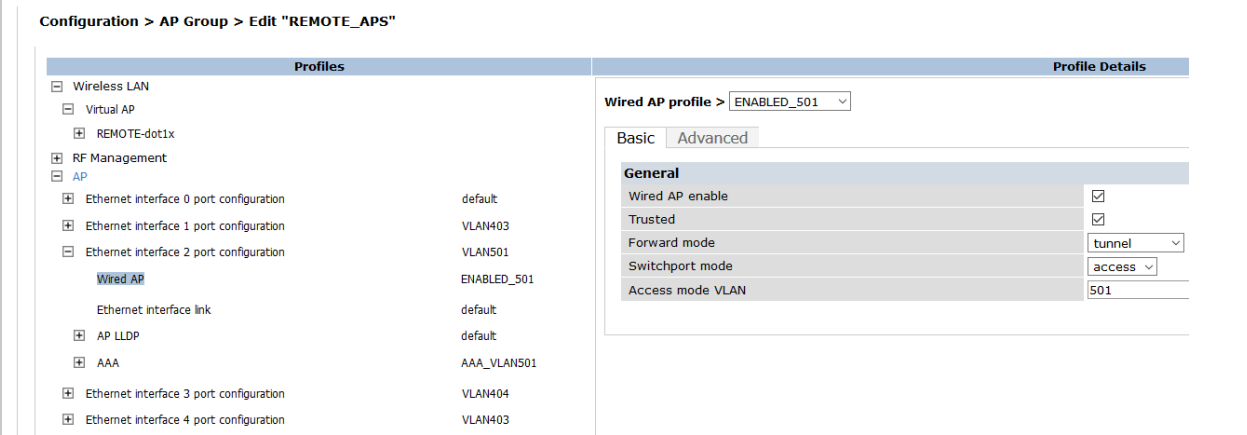
Step 2: Create a group for Remote APs (Recommended)



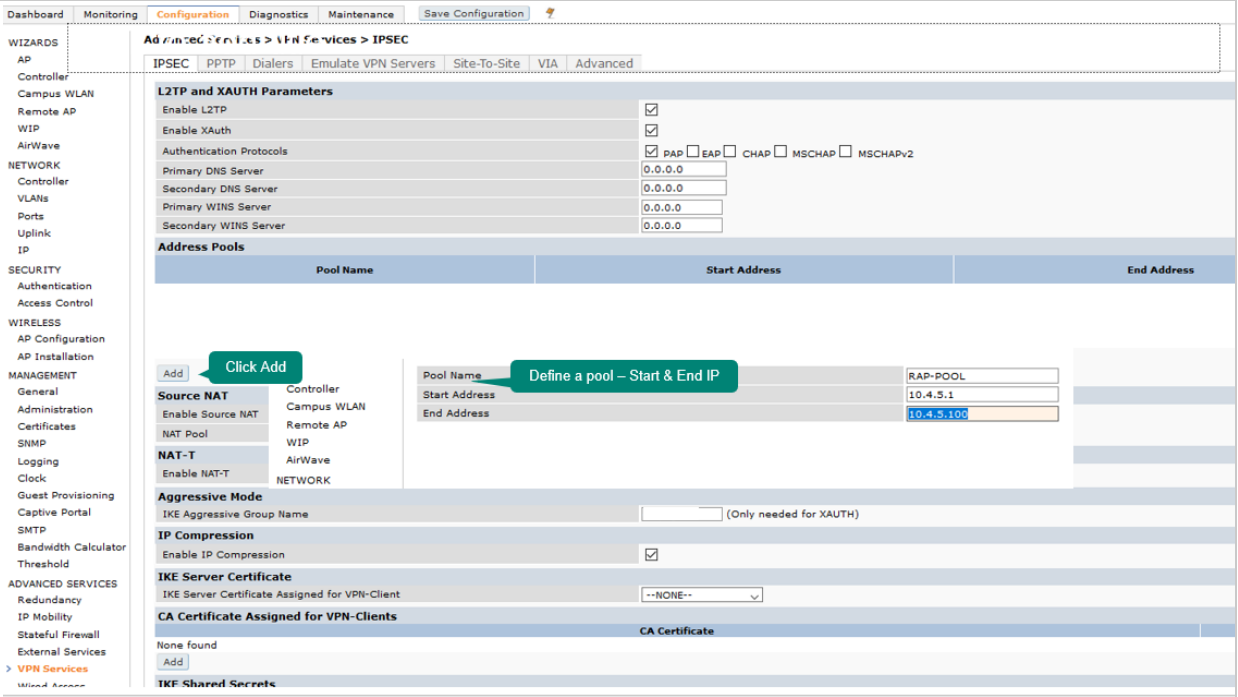
Step 3: Configure the Remote APs Group like a Campus Group (Add the necessary VAP, Wireless SSIDs, AAA profiles …etc.) You can use existing profiles or create new profiles as per your requirements.



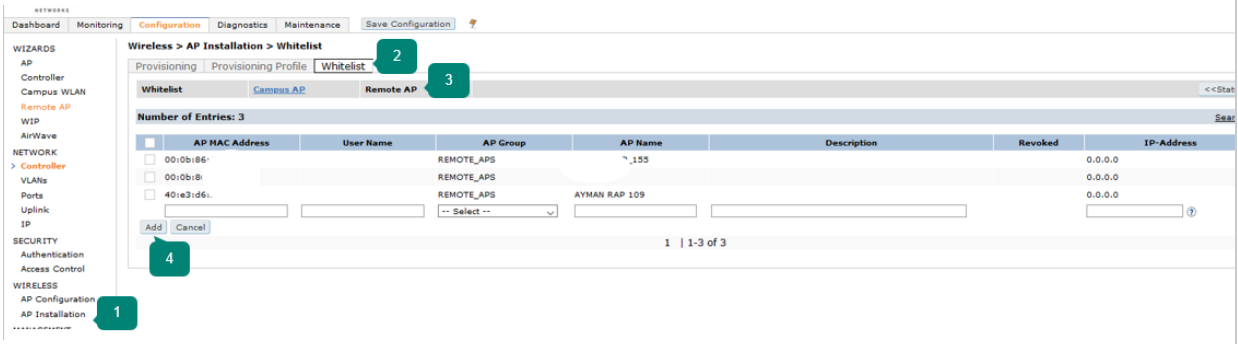
Step 4 (Optional): You can configure wired port profiles here in case you want to use other ports on the APs for wired connectivity (Eth0 is used as uplink so configure other ports depending on AP model). You can control whether wired traffic is trusted or not as well as the forwarding mode (tunneled, split-tunnel or bridged)



Step 4: Create a VPN Pool for RAPs – This is the inner IP that will be assigned for the RAPs. It shouldn't conflict with other IPs. It is not required to be routable.



Step 5: **<u>This step is required</u>** since the AP was not already provisioned. Make sure to include the mac address in both RAP whitelist-db and iap trusted-branch-db as explained below



Note: If an IAP was converted to a RAP manually without staging, then the RAP whitelist command shown above (**whitelist rap add mac-address <MAC>)** is not enough. From the controller cli, the following command should be added as well if the RAP are authenticating locally on the controller.

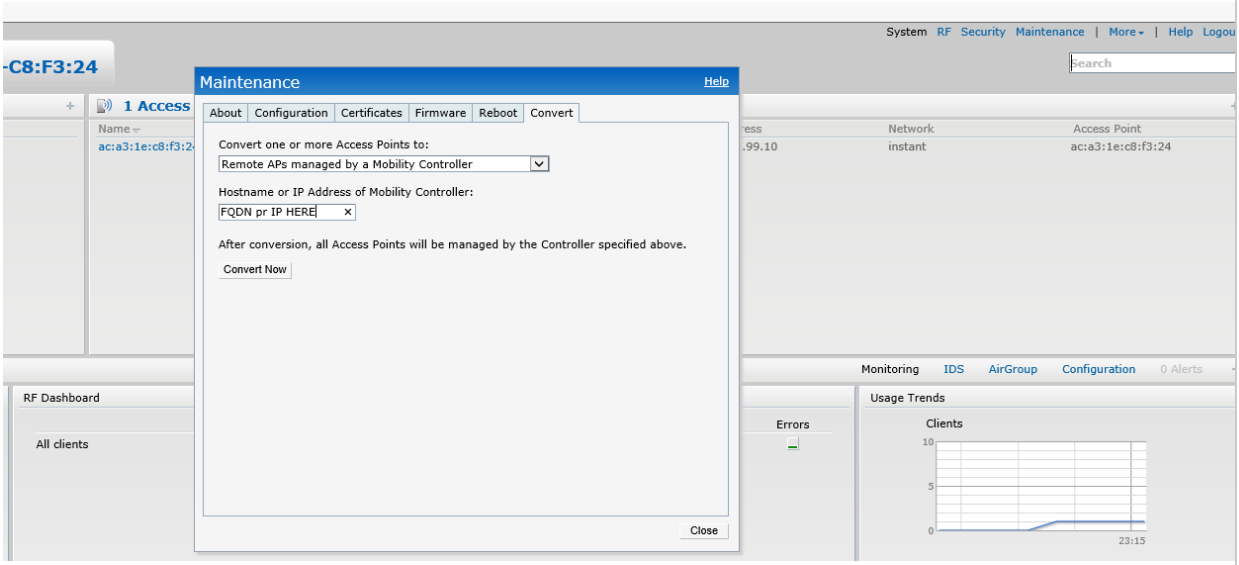
iap trusted-branch-db add mac-address <MAC> where <MAC> should be replaced with the MAC address of the remote access point.

The below commands can be used to verify that the MAC is whitelisted.
show whitelist-db rap
show iap trusted-branch-db

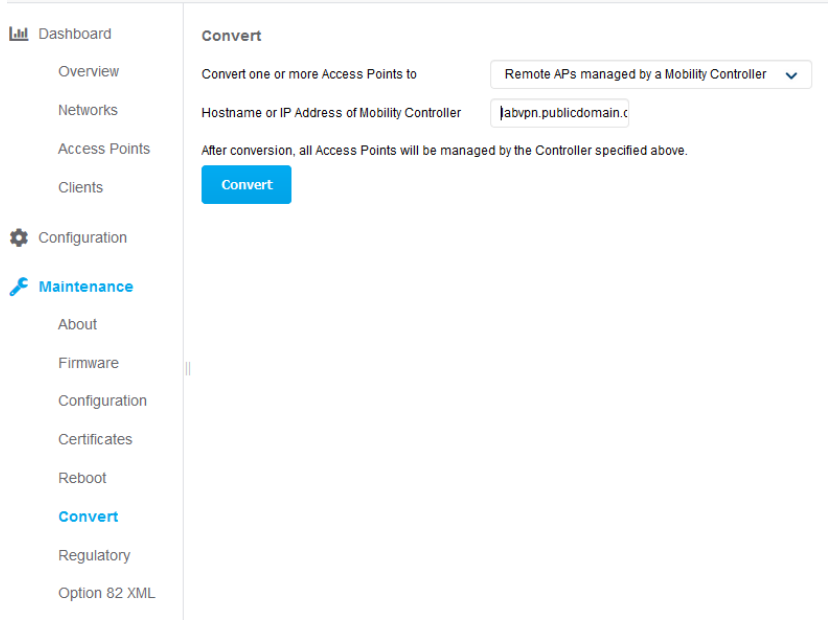
Step 6: Connect to the IAP web Interface, choose Maintenance and Convert to Remote AP. Specify the Public IP or FQDN of the controller and press convert. If the operation is successful, you will be prompted with a success message and the access point will reboot and join the controller.

Depending on your IAP Web Interface, select Maintenance → Convert
Choose Convert to Remote AP Managed by a Mobility Controller
Provide the IP Address or FQDN of the controller

OLD IAP Interface

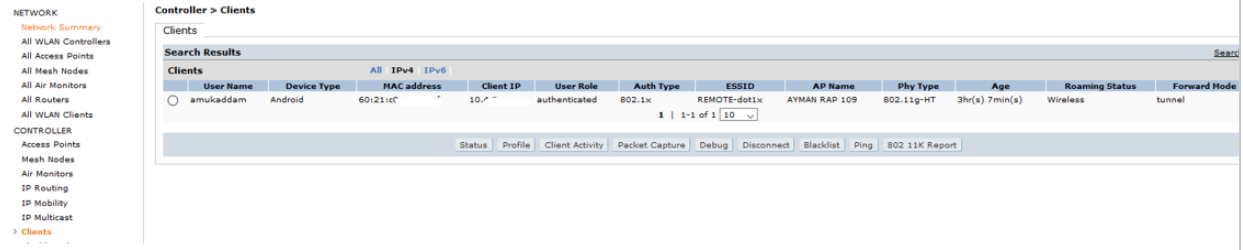


New IAP Interface



Step 7: The AP will show up as RAP AP and it will broadcast the configured wireless networks.

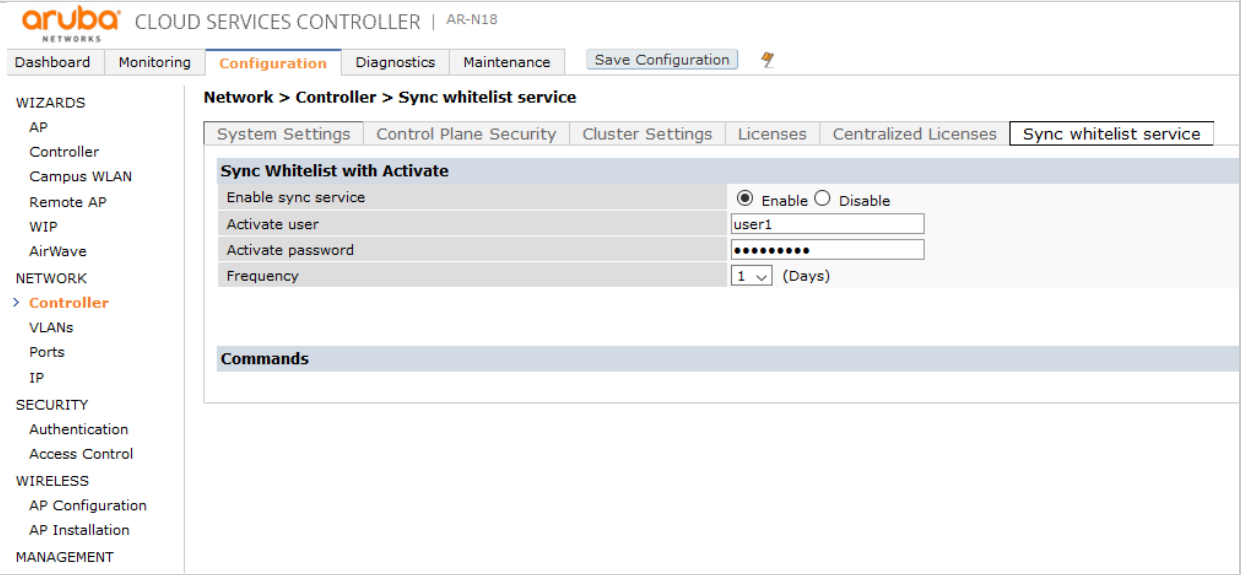
Step 8: Verify Clients are able to connect and get the right role and VLAN.



Note: If you need a demo video for a similar configuration, check this excellent video from Herman Robers on Airheads Community - https://community.arubanetworks.com/t5/Video/Setting-up-Aruba-Remote-Access-Point-RAP/ta-p/550413

4.3 Scenario 3 – Using Aruba Activate (ZTP)

This scenario is similar to the first scenario with differences in steps 1, 5 and 6.

Scenario 3 – Using Aruba Activate
Step 1: Create an account on activate and follow this guide to create a provisioning rule for IAPs to RAPs. Optionally, you can add a notification rule once an AP gets provisioned from activate, an email will be sent. **https://community.arubanetworks.com/t5/Wireless-Access/Tutorial-Provisioning-RAPs-with-Aruba-Activate-Dec13-Tutorial/td-p/128707**
Step 2: Create a group for Remote APs (Recommended)
Step 3: Configure the Remote APs Group like a Campus Group (Add the necessary VAP, Wireless SSIDs, AAA profiles …etc.) You can use existing profiles or create new profiles as per your requirements.
Step 4 (Optional): You can configure wired port profiles here in case you want to use other ports on the APs for wired connectivity (Eth0 is used as uplink so configure other ports depending on AP model). You can control whether wired traffic is trusted or not as well as the forwarding mode (tunneled, split-tunnel or bridged)
Step 4: Create a VPN Pool for RAPs – This is the inner IP that will be assigned for the RAPs. It shouldn't conflict with other IPs. It is not required to be routable.
Step 5: Controller needs to be configured to whitelist the RAPs. This can happen manually as described in the previous scenarios or via the below configuration of enabling activate sync-service.

Step 6: Connect the RAP or IAP to the internet. The IAP/RAP should acquire an IP via DHCP. The IAP/RAP should have internet reachability (DHCP, DNS, HTTPS, NTP, NAT-T) so it can communicate with activate and learn the controller IP and group.
Step 7: The AP will show up as RAP AP and it will broadcast the configured wireless networks.

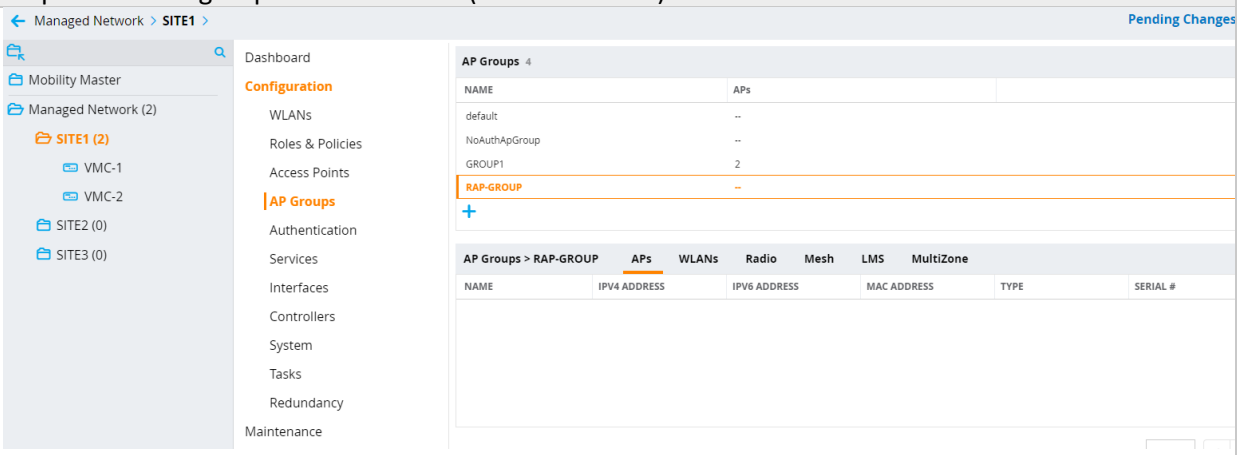
Step 8: Verify Clients are able to connect and get the right role and VLAN.

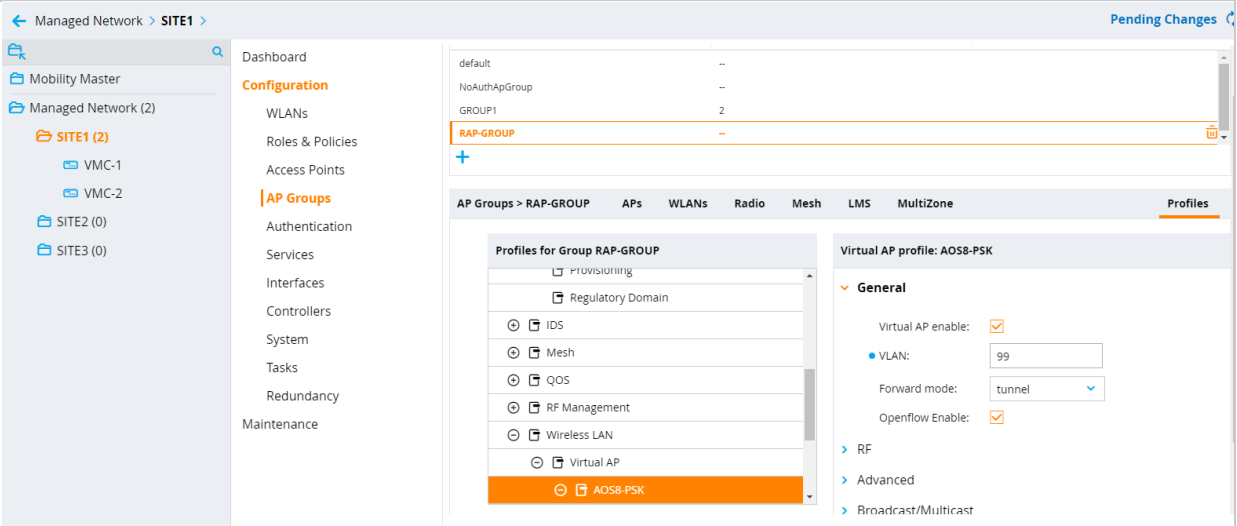
5 AOS 8 – RAP Configuration (8 Steps)

Section 5 includes the configurations based on AOS 8 setup. We have divided the configuration to 3 scenarios covering the majority of the deployment cases used by our customers. These scenarios are similar to the AOS 6 scenarios discussed in section 4.

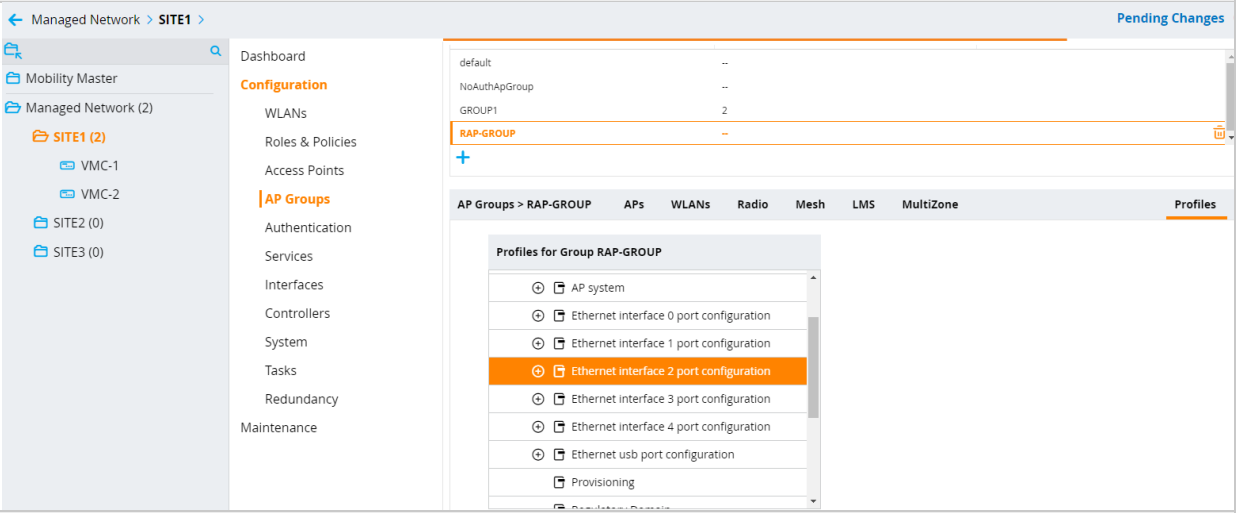
As a reminder, the below configurations are based on a single controller (without clustering). Terminating RAPs on a cluster is supported but few minor modifications are required like creating VPN Pool at MM level, mapping unique public IPs to each cluster member as part of cluster group-profile, upgrading to AOS 8.4 or later for RAP in a Cluster with NAT to work…etc. which are not documented here. If you need additional information, please contact your Aruba SE to support you.

5.1 Scenario 1 – Staging the RAP as CAP then provisioning it as RAP

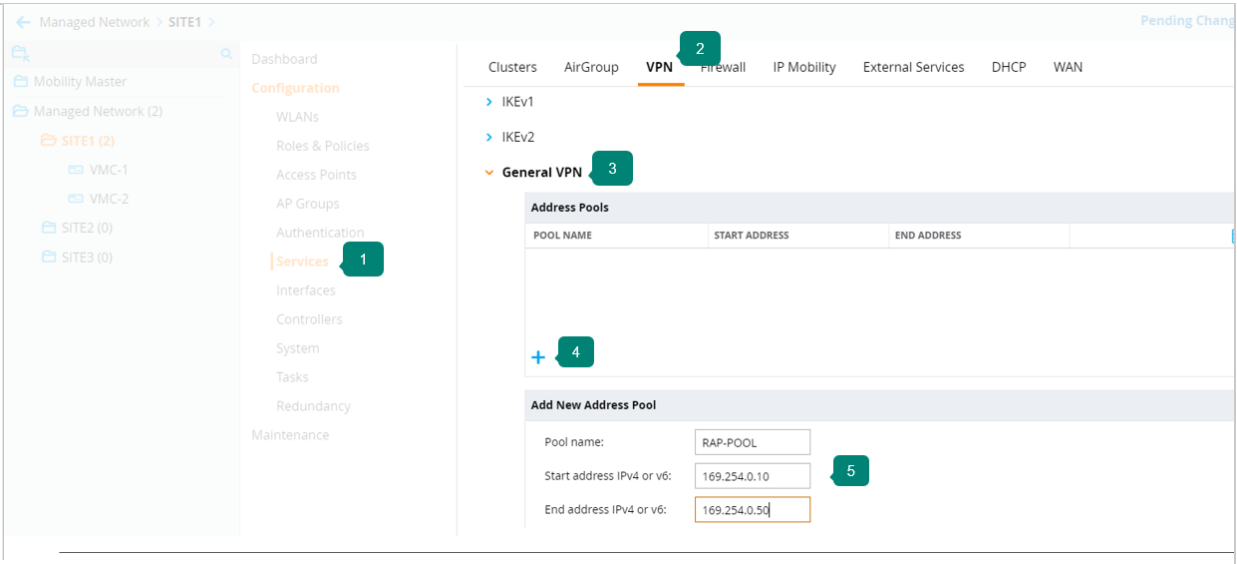
Scenario 1 – Staging the RAP as CAP then provisioning it as RAP
Step 1: Connect the RAP to your network and let it join the controller like a regular CAP – Steps not shown here
Step 2: Create a group for Remote APs (Recommended)

Step 3: Configure the Remote APs Group like a Campus Group (Add the necessary VAP, Wireless SSIDs, AAA profiles …etc.) You can use existing profiles or create new profiles as per your requirements.



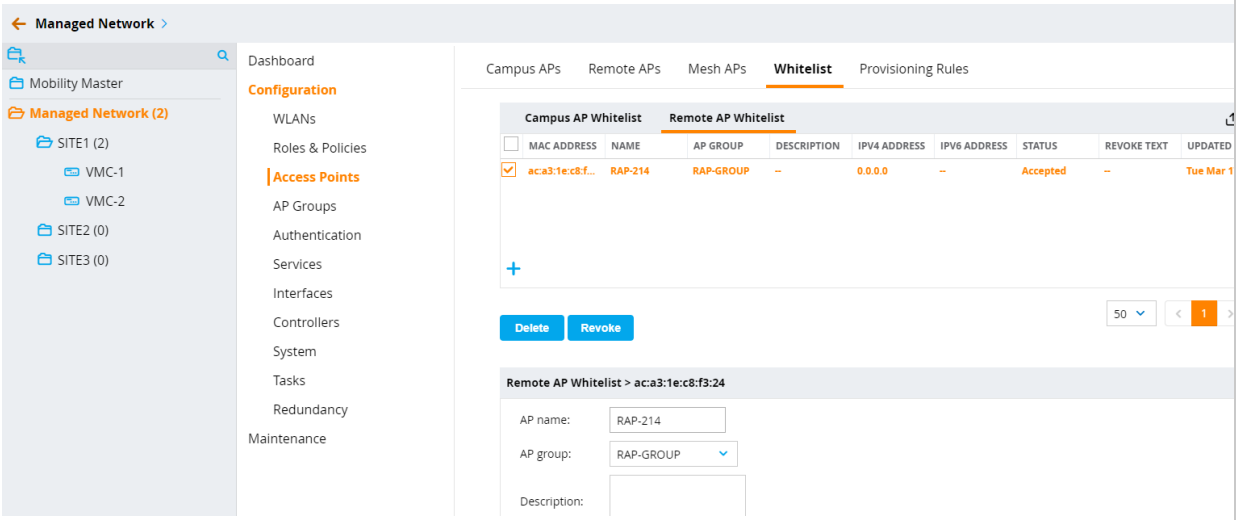
Step 4 (Optional): You can configure wired port profiles here in case you want to use other ports on the APs for wired connectivity (Eth0 is used as uplink so configure other ports depending on AP model). You can control whether wired traffic is trusted or not as well as the forwarding mode (tunneled, split-tunnel or bridged)



Step 4: Create a VPN Pool for RAPs – This is the inner IP that will be assigned for the RAPs. It shouldn't conflict with other IPs. It is not required to be routable.



Step 5: This step is not required if the AP was already provisioned as CAP. However, it is better to whitelist the RAP by adding its MAC address and assigning it to the Remote APs Group that was created in Step 1.

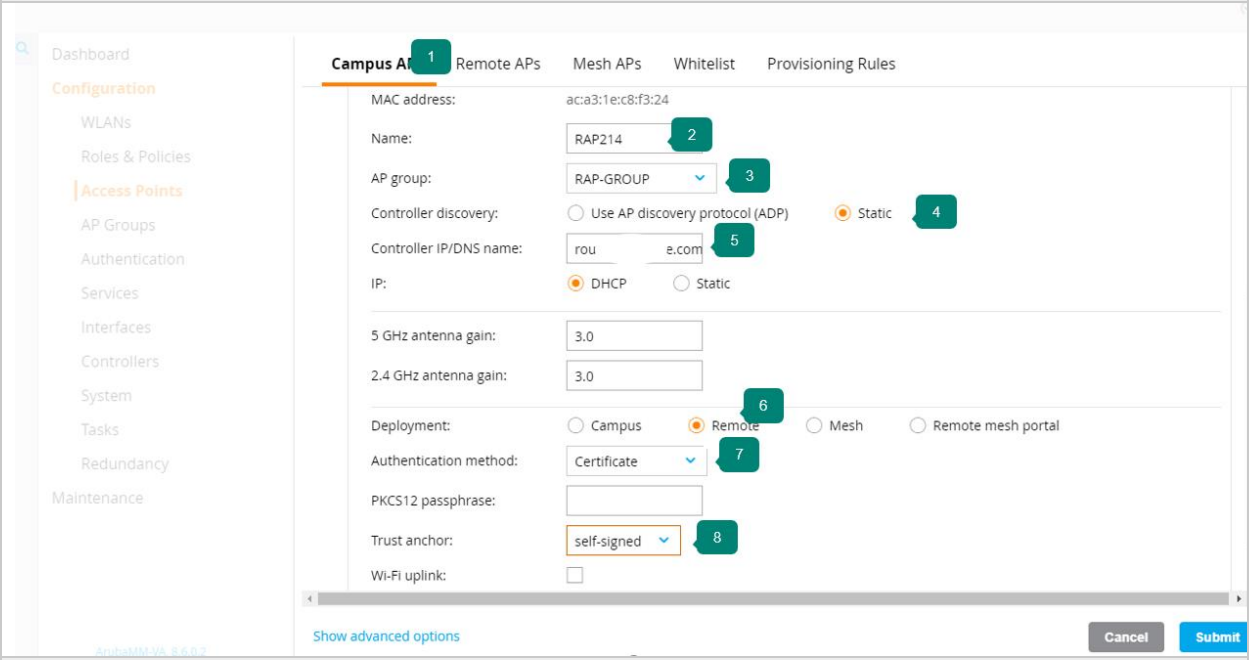


Note: If an IAP was converted to a RAP manually without staging, then the RAP whitelist command shown above (**whitelist rap add mac-address <MAC>)** is not enough. From the controller cli, the following command should be added as well if the RAP are authenticating locally on the controller.

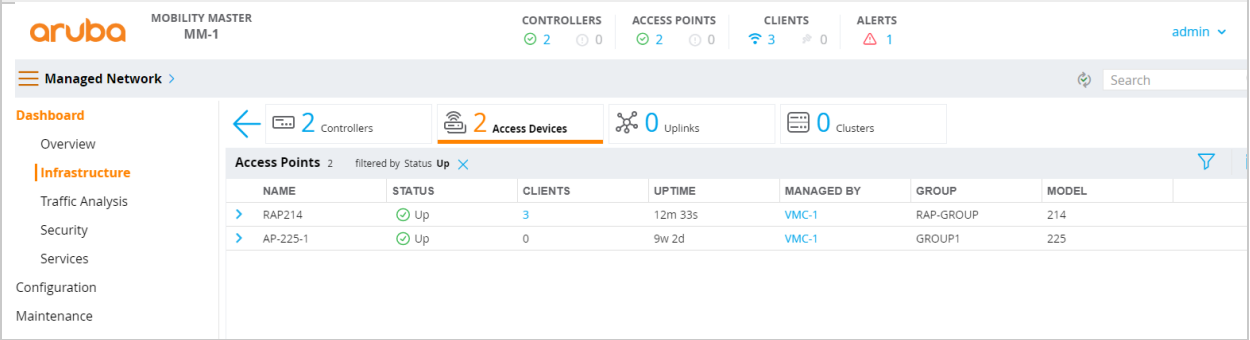
iap trusted-branch-db add mac-address <MAC> where <MAC> should be replaced with the MAC address of the remote access point.

The below commands can be used to verify that the MAC is whitelisted.
show whitelist-db rap
show iap trusted-branch-db

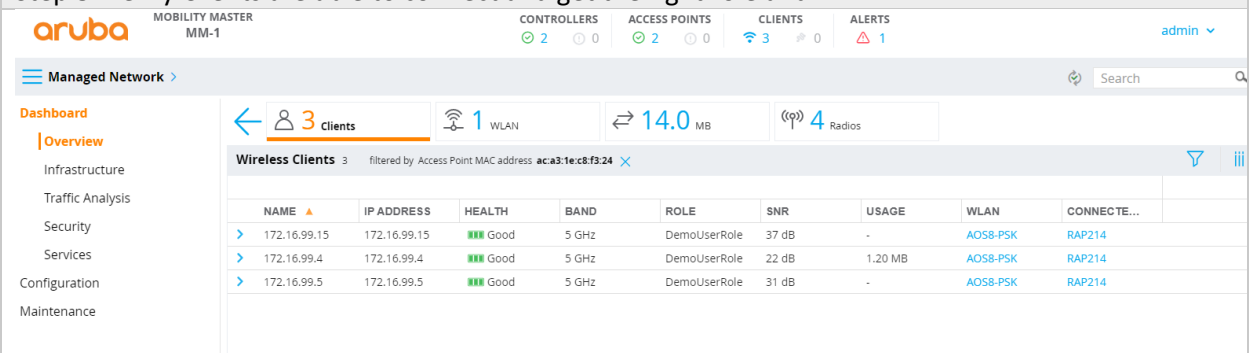
Step 6: Convert the CAP to RAP by selecting right group, giving it a name, making it a RAP with certificate and self-signed trust anchor (if connecting to a virtual controller), specifying Controller Public IP/FQDN and then pressing submit.



Step 7: Disconnect the AP from the network and connect to the Internet where it can reach the controller public IP on UDP 4500. The AP will show up as RAP AP and it will broadcast the configured wireless networks.

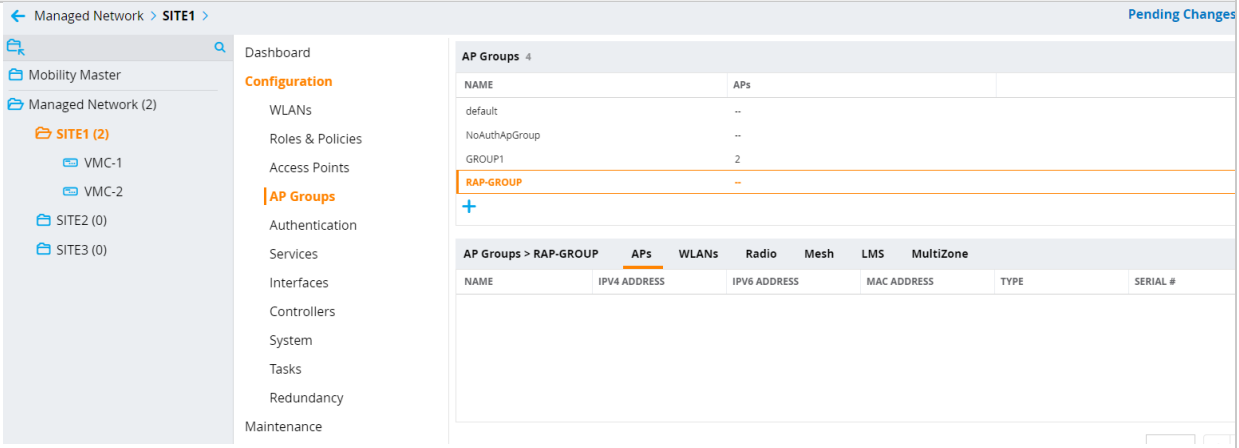
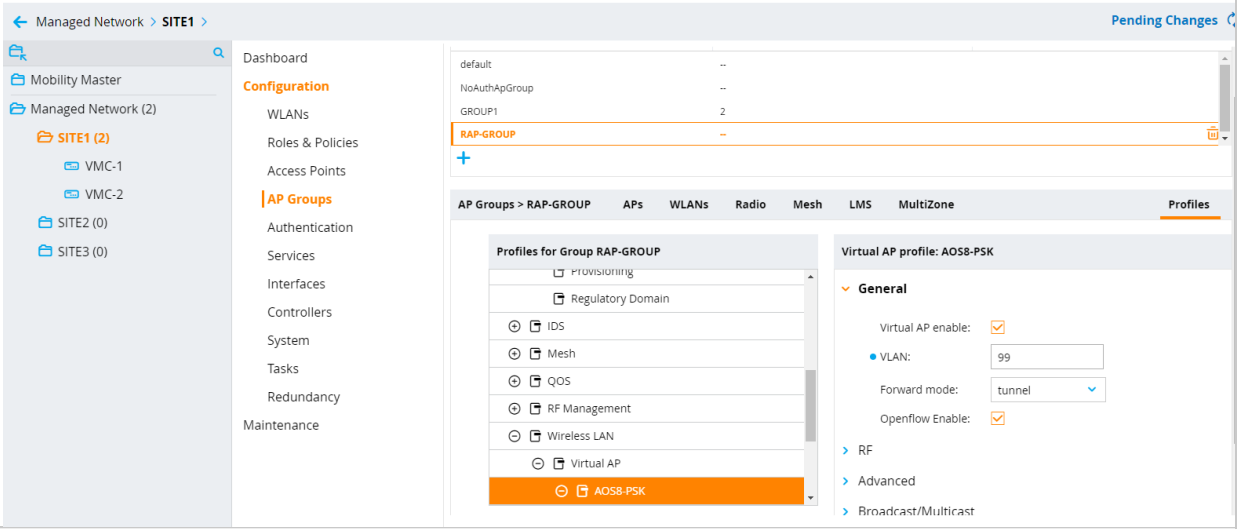


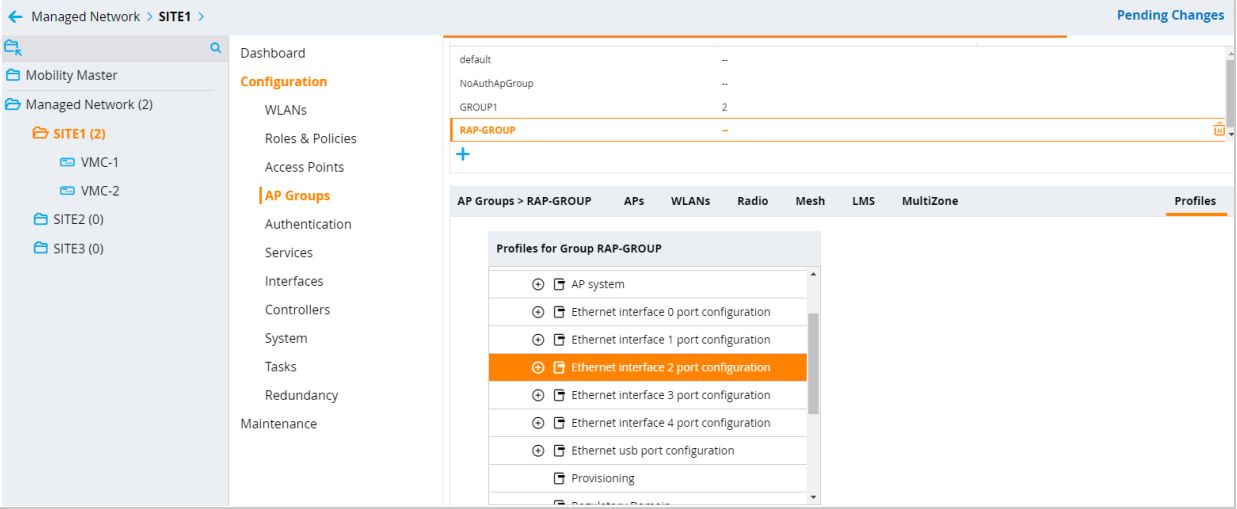
Step 8: Verify Clients are able to connect and get the right role and VLAN.



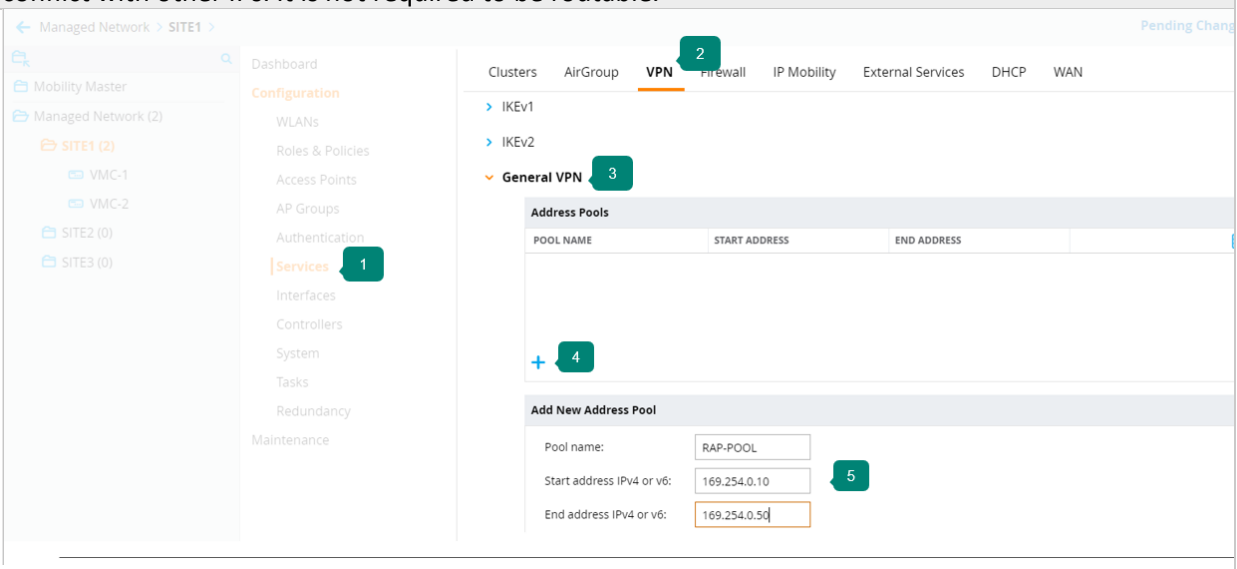
5.2 Scenario 2 – Converting an IAP to RAP

This scenario is similar to the first scenario with differences in steps 1, 5 and 6.

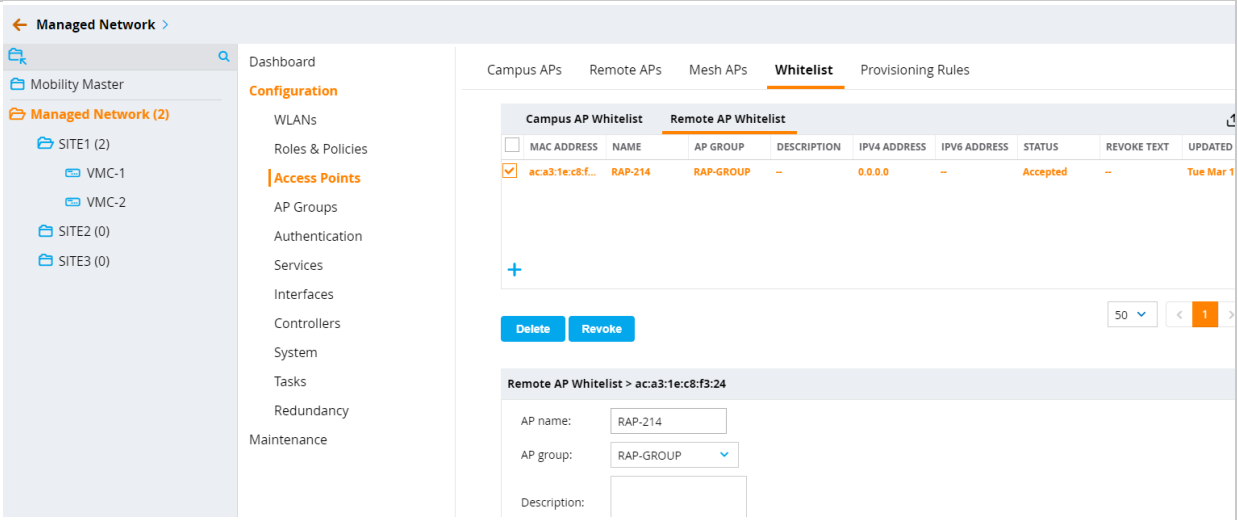
Scenario 1 – Staging the RAP as CAP then provisioning it as RAP
Step 1: Staging is not needed so this step is skipped
Step 2: Create a group for Remote APs (Recommended)

Step 3: Configure the Remote APs Group like a Campus Group (Add the necessary VAP, Wireless SSIDs, AAA profiles …etc.) You can use existing profiles or create new profiles as per your requirements.

Step 4 (Optional): You can configure wired port profiles here in case you want to use other ports on the APs for wired connectivity (Eth0 is used as uplink so configure other ports depending on AP model). You can control whether wired traffic is trusted or not as well as the forwarding mode (tunneled, split-tunnel or bridged)



Step 4: Create a VPN Pool for RAPs – This is the inner IP that will be assigned for the RAPs. It shouldn't conflict with other IPs. It is not required to be routable.



Step 5: **This step is required** since the AP was not already provisioned. Make sure to include the mac address in both RAP whitelist-db and iap trusted-branch-db as explained below



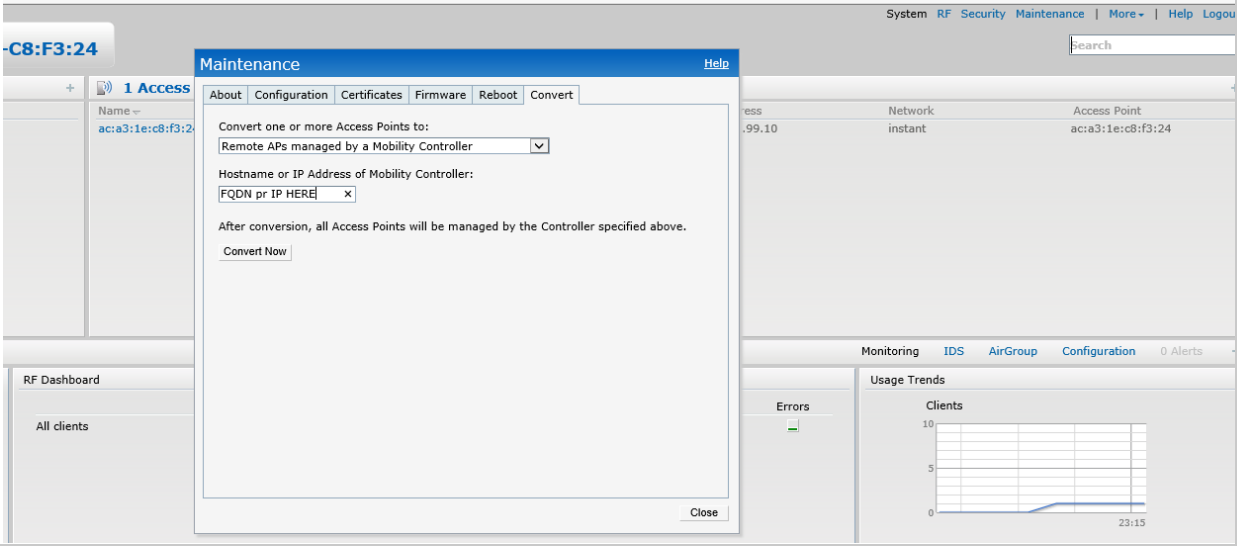
Note: If an IAP was converted to a RAP manually without staging, then the RAP whitelist command shown above (**whitelist rap add mac-address <MAC>)** is not enough. From the controller cli, the following command should be added as well if the RAP are authenticating locally on the controller.

iap trusted-branch-db add mac-address <MAC> where <MAC> should be replaced with the MAC address of the remote access point.

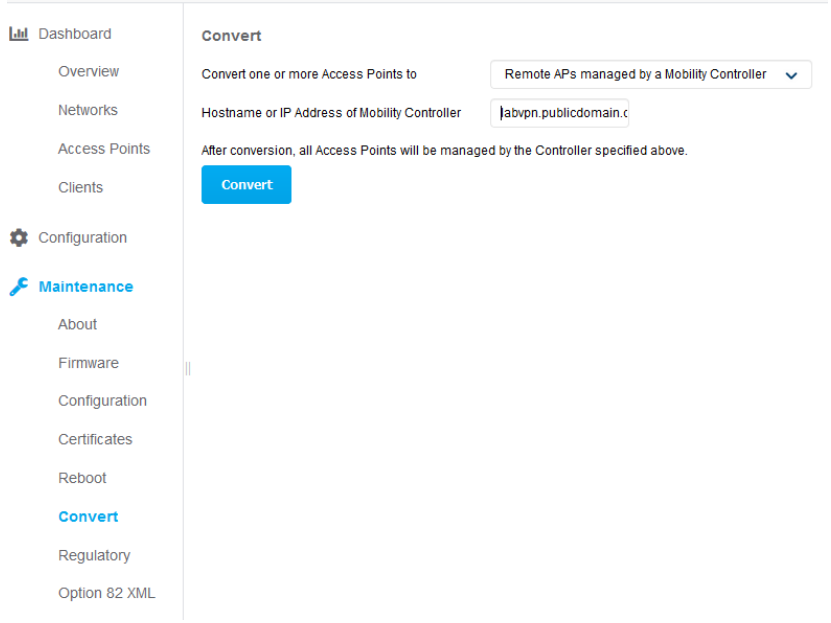
The below commands can be used to verify that the MAC is whitelisted.
show whitelist-db rap
show iap trusted-branch-db

Step 6: Convert the CAP to RAP by selecting right group, giving it a name, making it a RAP with certificate and self-signed trust anchor (if connecting to a virtual controller), specifying Controller Public IP/FQDN and then pressing submit.

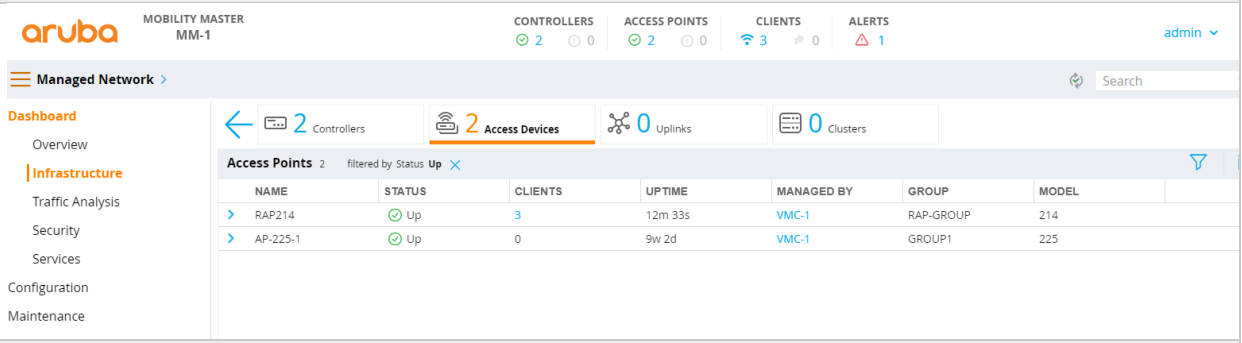
Depending on your IAP Web Interface, select Maintenance → Convert
Choose Convert to Remote AP Managed by a Mobility Controller
Provide the IP Address or FQDN of the controller
OLD IAP Interface



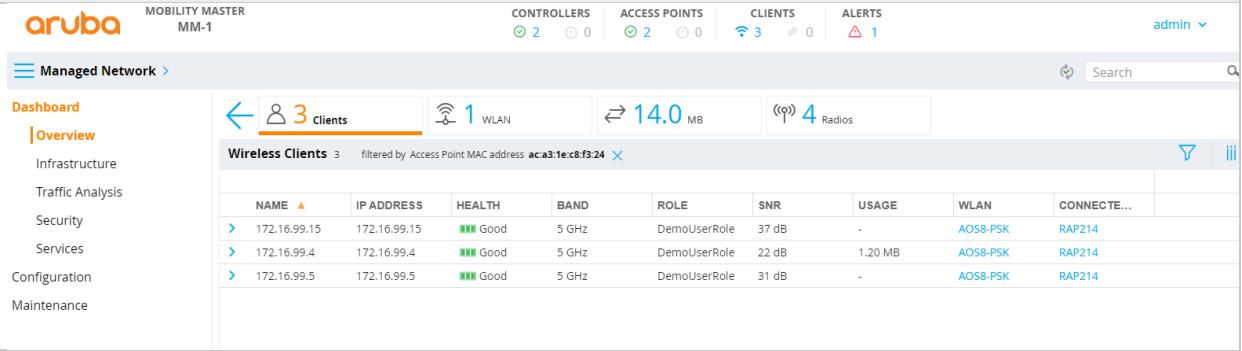
New IAP Interface



Step 7: Disconnect the AP from the network and connect to the Internet where it can reach the controller public IP on UDP 4500. The AP will show up as RAP AP and it will broadcast the configured wireless networks.

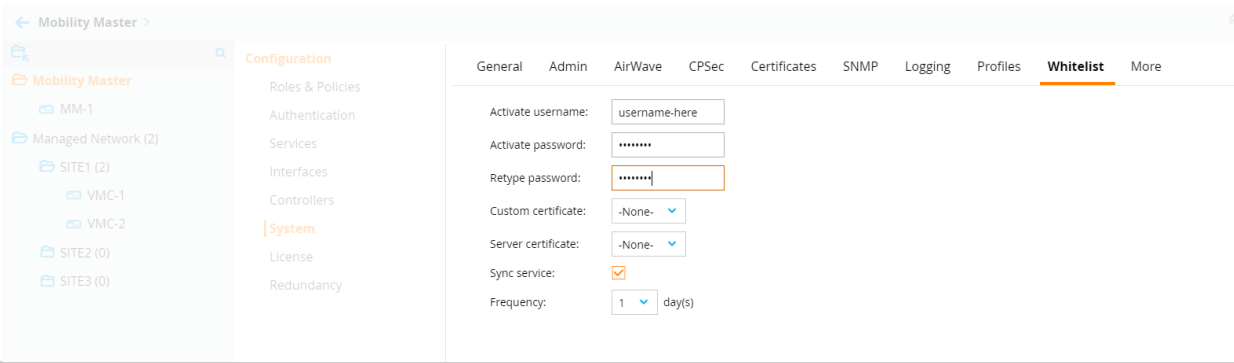


Step 8: Verify Clients are able to connect and get the right role and VLAN.



5.3 Scenario 3 – Using Aruba Activate (ZTP)

This scenario is similar to the first scenario with differences in steps 1, 5 and 6. Check other scenarios for the detailed screenshots.

Scenario 3 – Using Aruba Activate
Step 1: Create an account on activate and follow this guide to create a provisioning rule for IAPs to RAPs. Optionally, you can add a notification rule once an AP gets provisioned from activate, an email will be sent. **https://community.arubanetworks.com/t5/Wireless-Access/Tutorial-Provisioning-RAPs-with-Aruba-Activate-Dec13-Tutorial/td-p/128707**
Step 2: Create a group for Remote APs (Recommended)
Step 3: Configure the Remote APs Group like a Campus Group (Add the necessary VAP, Wireless SSIDs, AAA profiles …etc.) You can use existing profiles or create new profiles as per your requirements.
Step 4 (Optional): You can configure wired port profiles here in case you want to use other ports on the APs for wired connectivity (Eth0 is used as uplink so configure other ports depending on AP model). You can control whether wired traffic is trusted or not as well as the forwarding mode (tunneled, split-tunnel or bridged)
Step 4: Create a VPN Pool for RAPs – This is the inner IP that will be assigned for the RAPs. It shouldn't conflict with other IPs. It is not required to be routable.
Step 5: Controller needs to be configured to whitelist the RAPs. This can happen manually as described in the previous scenarios or via the below configuration of enabling activate sync-service.

Step 6: Connect the RAP or IAP to the internet. The IAP/RAP should acquire an IP via DHCP. The IAP/RAP should have internet reachability (DHCP, DNS, HTTPS, NTP, NAT-T) so it can communicate with activate and learn the controller IP and group.
Step 7: The AP will show up as RAP AP and it will broadcast the configured wireless networks.
Step 8: Verify Clients are able to connect and get the right role and VLAN.

6 Summary

This document provided a brief overview on how to configure Aruba RAPs with both AOS6 and AOS 8 setups. This document is not a comprehensive document and it doesn't cover all cases or more advanced options like integrating with ClearPass or deploying redundant or clustered controllers. It is just intended as a quick start simplified configuration guide to support our customers in their urgent business continuity strategy. If additional information is required, feel free to contact your Aruba representative. Below are some additional documents related to Aruba RAP. Finally, in case you need VPN client solution for your workers on the road, make sure to check our Aruba VIA solution.

I hope this document will be beneficial to our customers. Feel free to share your comments & feedback at ayman.mukaddam@hpe.com

7 Additional Resources

1. Setting Up an Aruba Remote AP - https://community.arubanetworks.com/t5/Video/Setting-up-Aruba-Remote-Access-Point-RAP/ta-p/550413
2. Aruba Remote Access Points - https://www.arubanetworks.com/assets/eo/EO_RemoteAccess.pdf
3. Aruba VPN Services- https://www.arubanetworks.com/products/security/vpn-services/
4. Aruba VIA Client for Mobile Workers - https://www.arubanetworks.com/assets/ds/DS_VIA.pdf
5. IAP Trusted Branch - https://community.arubanetworks.com/t5/Controller-Based-WLANs/Instant-Trusted-Branch-DB/ta-p/234095
6. Aruba Activate (IAP to RAP) - https://community.arubanetworks.com/t5/Wireless-Access/Tutorial-Provisioning-RAPs-with-Aruba-Activate-Dec13-Tutorial/td-p/128707