

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	3
2	High Level Architecture.....	3
3	High Level Steps & Pre-requisites	4
3.1	RAP needs to learn controller IP	4
3.2	RAP needs to reach controller IP on UDP Port 4500	4
3.3	RAP needs to authenticate successfully	5
3.4	RAP needs to be assigned an IP address from controller	5
3.5	RAP needs to be configured in a group.....	5
4	AOS 6 – RAP Configuration (8 Steps)	5
4.1	Scenario 1 – Staging the RAP as CAP then provisioning it as RAP	5
4.2	Scenario 2 – Converting an IAP to RAP	9
4.3	Scenario 3 – Using Aruba Activate (ZTP).....	13
5	AOS 8 – RAP Configuration (8 Steps)	14
5.1	Scenario 1 – Staging the RAP as CAP then provisioning it as RAP	14
5.2	Scenario 2 – Converting an IAP to RAP	18
5.3	Scenario 3 – Using Aruba Activate (ZTP).....	21
6	Summary	23
7	Additional Resources	23

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.

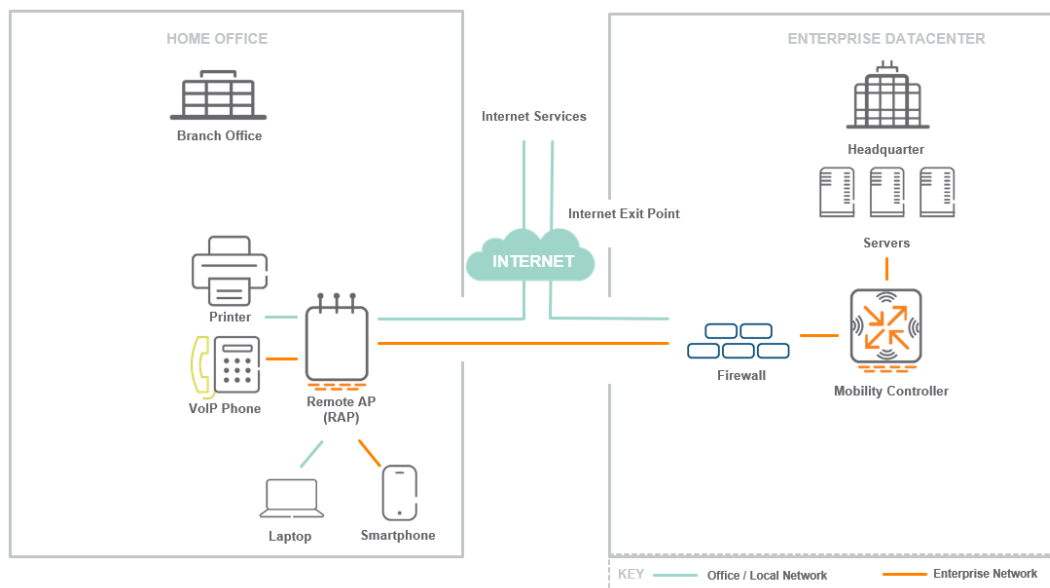


Figure 1: Aruba Remote Networking Solution - Home Office

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.

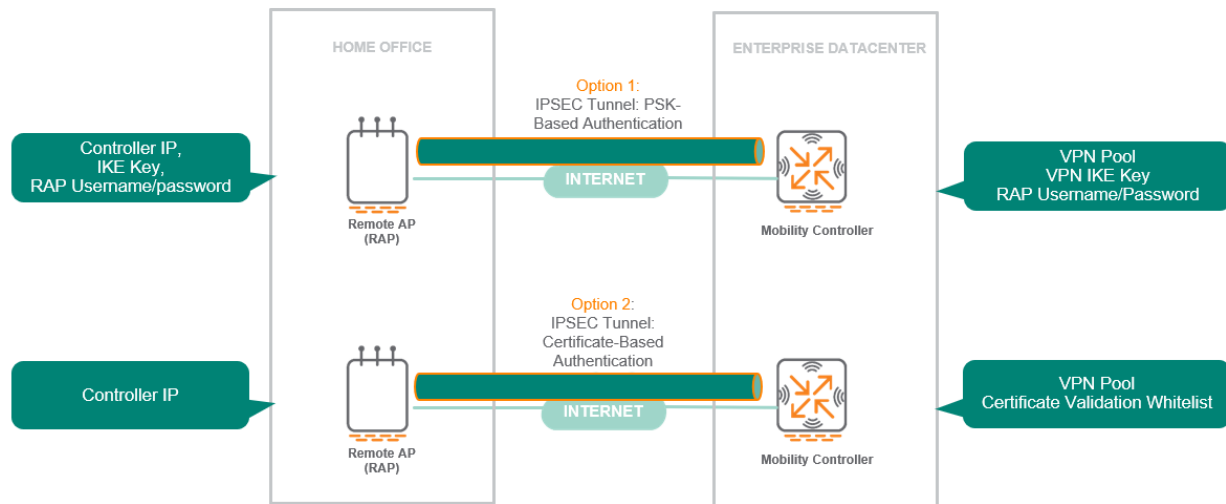
3.1 RAP needs to learn controller IP

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)

aruba NETWORKS MOBILITY CONTROLLER | WLC-VPN-1

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS
 AP
 Controller
 Campus WLAN
 Remote AP
 WIP
 AirWave
 NETWORK
 Controller
 VLANs
 Ports
 Uplink
 IP
 SECURITY
 Authentication
 Access Control
 WIRELESS
 > **AP Configuration**
 AP Installation
 MANAGEMENT

Configuration > AP Group

AP Group AP Specific

[default](#)
[LOCAL_APs](#)
[NoAuthApGroup](#)
[REMOTE_APS](#)

New

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.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS
 AP
 Controller
 Campus WLAN
 Remote AP
 WIP
 AirWave
 NETWORK
 Controller
 VLANs
 Ports
 Uplink
 IP
 SECURITY
 Authentication
 Access Control
 WIRELESS
 > **AP Configuration**
 AP Installation

Configuration > AP Group > Edit "REMOTE_APS"

Profiles		Profile Details					
Wireless LAN							
Virtual AP							
REMOTE-dot1x							
RF Management							
AP							
QOS							
IDS							
Mesh							

Virtual APs						
Name	AAA Profile	SSID Profile	VLAN	Forward mode	Virtual AP enable	
REMOTE-dot1x	Remote-dot1x-AAA	Remote-dot1x-SSID	403	tunnel	Enabled	

Add a profile REMOTE Add

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)

Configuration > AP Group > Edit "REMOTE_APS"

Profiles		Profile Details	
Wireless LAN			
Virtual AP			
REMOTE-dot1x			
RF Management			
AP			
Ethernet interface 0 port configuration	default		
Ethernet interface 1 port configuration	VLAN403		
Ethernet interface 2 port configuration	VLAN501		
Wired AP	ENABLED_501		
Ethernet interface link	default		
AP LLDP	default		
AAA	AAA_VLAN501		
Ethernet interface 3 port configuration	VLAN404		
Ethernet interface 4 port configuration	VLAN403		

Wired AP profile > ENABLED_501

Basic Advanced

General

Wired AP enable	<input checked="" type="checkbox"/>
Trusted	<input checked="" type="checkbox"/>
Forward mode	tunnel
Switchport mode	access
Access mode VLAN	501

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.

Dashboard | Monitoring | **Configuration** | Diagnostics | Maintenance | Save Configuration

WIZARDS
AP
Controller
Campus WLAN
Remote AP
WIP
AirWave
NETWORK
Controller
VLANs
Ports
Uplink
IP
SECURITY
Authentication
Access Control
WIRELESS
AP Configuration
➤ **AP Installation**
MANAGEMENT
General
Administration
Certificates
SNMP
Logging
Clock
Guest Provisioning
Captive Portal
SMTP
Bandwidth Calculator
Threshold
ADVANCED SERVICES
Redundancy
IP Mobility
Stateful Firewall
External Services
VPN Services
Wired Access
All Profiles
[E-mail Support](#)

Wireless > AP Installation > Provision

Provisioning | Provisioning Profile | Whitelist

AP Parameters
AP Group: REMOTE_APS Select Right Group

AP Installation Mode
☒ Default ☐ Indoor ☐ Outdoor

Antenna Parameters
Antenna Selection
☒ Internal/Included Antenna ☐ External Antenna

Authentication Method
Remote AP ☒ Yes ☐ No Select Yes
Remote AP Authentication Method
☐ Pre-shared Key ☒ Certificate Select Certificate

PKCS12 Passphrase
Representation Type: Text-based
IKE PSK
Confirm IKE PSK

User credential assignment
☒ Use Automatic Generation
☐ Global User Name/Password ☐ per AP User Name/Password

User Name
Password
Generate
Confirm Password

☐ PPPoE Parameters
Service Name
User Name
Password
Confirm Password
CHAP Secret
Confirm CHAP Secret

☐ 802.1x Parameters using PEAP
User Name
Password
Confirm Password

Master Discovery
☐ Use AP Discovery Protocol
☐ Master Controller IP Address/DNS name
TFTP Server
Master Controller IP Address/DNS name: labvpn.b.com

☒ Host Controller Name: aruba-master

IP Settings
Uplink VLAN: 0 Specify Public IP or FQDN of controller
☒ Obtain IP Address Using DHCP

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.

Dashboard | **Monitoring** | Configuration | Diagnostics | Maintenance

NETWORK
Network Summary
All WLAN Controllers
All Access Points
All Mesh Nodes
All Air Monitors
All Routers
All WLAN Clients
CONTROLLER
➤ **Access Points**
Mesh Nodes
Air Monitors
IP Routing
IP Mobility
IP Multicast
Clients
Blacklist Clients
Firewall Hits
External Services Interface
Tunneled Node Ports
Ports
Uplink
Universal Serial Bus
WLAN
REMOTE-dot1x

Controller > Access Points

Search Results

Name	AP Group	AP IP	Outer AP IP	AP Type	.bg Clients/Channel/ EIRP/HaxEIRP/Standard	.a Clients/Channel/ EIRP/HaxEIRP/Standard	Enet 1	IPSEC	Uptime	PPPoE	Fl
AYMAN RAP 109	REMOTE_APS	10.1.94.20	36	RAP-109	1/1/9/20/n(20)	0/116+/18/23/n(40)	Wired Port	enable	3h:37m:52s	disable	RE

Flags: 1 = 802.1x authenticated AP; 2 = Using IKE version 2; A = Enet1 in active/standby mode; B = Battery Boost On; C = Cellular; D = Disconnect Extra Calls On; E = Wired AP enabled; F = AP failed 802.1x authentication; H = Hotspot Enabled; L = Client Balancing Enabled; M = Mesh; N = 802.11b protection disabled; P = PPPoE; R = Remote AP; S = AP connected as standby; X = Maintenance Mode; a = Reduce ARP packets in the air; d = Drop Mcast/Bcast On; i = Custom-Cert RAP; l = Provisioned as Indoor; o = Provisioned as Outdoor; p = Restriction mode in POE-AP; q = 802.11r Enabled; Q = DFS CAC timer running

Channel followed by "*" indicates channel selected due to unsupported configured channel.

Status | Profile | AP Activity | Packet Capture | Launch AirMagnet | Ping | Overview | USB | Ethernet Switching | 802.11K Report

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

Dashboard | Monitoring | Configuration | Diagnostics | Maintenance

NETWORK
Network Summary
All WLAN Controllers
All Access Points
All Mesh Nodes
All Air Monitors
All Routers
All WLAN Clients
CONTROLLER
Access Points
Mesh Nodes
Air Monitors
IP Routing
IP Mobility
IP Multicast
➤ **Clients**

Controller > Clients

Clients

Search Results

User Name	Device Type	HAC address	Client IP	User Role	Auth Type	ESSID	AP Name	Phy Type	Age	Roaming Status	Forward Mode
amukaddam	Android	60:21:c0:00:00:00	10.1.94.20	authenticated	802.1x	REMOTE-dot1x	AYMAN RAP 109	802.11g-HT	3h(s) 7min(s)	Wireless	tunnel

1 | 1-1 of 1 | 10

Status | Profile | Client Activity | Packet Capture | Debug | Disconnect | Blacklist | Ping | 802.11K Report

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)

The screenshot shows the Aruba Mobility Controller web interface. The top navigation bar includes 'Dashboard', 'Monitoring', 'Configuration' (selected), 'Diagnostics', and 'Maintenance'. A 'Save Configuration' button is on the right. The left sidebar lists various configuration categories: WIZARDS, AP, Controller, Campus WLAN, Remote AP, WIP, AirWave, NETWORK, Controller, VLANs, Ports, Uplink, IP, SECURITY, Authentication, Access Control, WIRELESS, > AP Configuration (selected), AP Installation, and MANAGEMENT. The main content area is titled 'Configuration > AP Group'. It shows a list of AP Groups: 'default', 'LOCAL_APs', 'NoAuthApGroup', and 'REMOTE_APS'. A 'New' button is at the bottom of the list.

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.

The screenshot shows the 'Configuration > AP Group > Edit "REMOTE_APS"' page. The left sidebar is the same as in the previous screenshot. The main content area is divided into two sections: 'Profiles' and 'Profile Details'. The 'Profiles' section shows a tree view with 'Wireless LAN' expanded, containing 'Virtual AP' and 'Remote-dot1x'. The 'Profile Details' section shows a table with columns: 'Name', 'AAA Profile', 'SSID Profile', 'VLAN', 'Forward mode', and 'Virtual AP enable'. The table contains one row for 'REMOTE-dot1x' with values: 'Remote-dot1x-AAA', 'Remote-dot1x-SSID', '403', 'tunnel', and 'Enabled'. Below the table is an 'Add a profile' section with a dropdown menu set to 'REMOTE' and an 'Add' button.

Name	AAA Profile	SSID Profile	VLAN	Forward mode	Virtual AP enable
REMOTE-dot1x	Remote-dot1x-AAA	Remote-dot1x-SSID	403	tunnel	Enabled

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)

Configuration > AP Group > Edit "REMOTE_APS"

Profiles	Profile Details										
<ul style="list-style-type: none"> Wireless LAN <ul style="list-style-type: none"> Virtual AP <ul style="list-style-type: none"> REMOTE-dot1x RF Management AP <ul style="list-style-type: none"> Ethernet interface 0 port configuration: default Ethernet interface 1 port configuration: VLAN403 Ethernet interface 2 port configuration: VLAN501 Wired AP: ENABLED_501 <ul style="list-style-type: none"> Ethernet interface link: default AP LLDP: default AAA: AAA_VLAN501 Ethernet interface 3 port configuration: VLAN404 Ethernet interface 4 port configuration: VLAN403 	<p>Wired AP profile > ENABLED_501</p> <p>Basic Advanced</p> <p>General</p> <table> <tr> <td>Wired AP enable</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Trusted</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Forward mode</td> <td>tunnel</td> </tr> <tr> <td>Switchport mode</td> <td>access</td> </tr> <tr> <td>Access mode VLAN</td> <td>501</td> </tr> </table>	Wired AP enable	<input checked="" type="checkbox"/>	Trusted	<input checked="" type="checkbox"/>	Forward mode	tunnel	Switchport mode	access	Access mode VLAN	501
Wired AP enable	<input checked="" type="checkbox"/>										
Trusted	<input checked="" type="checkbox"/>										
Forward mode	tunnel										
Switchport mode	access										
Access mode VLAN	501										

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.

Dashboard Monitoring Configuration Diagnostics Maintenance Save Configuration

WIZARDS AP Controller Campus WLAN Remote AP WIP AirWave

NETWORK Controller VLANs Ports Uplink IP

SECURITY Authentication Access Control

WIRELESS AP Configuration AP Installation

MANAGEMENT General Administration Certificates SNMP Logging Clock Guest Provisioning Captive Portal SMTP Bandwidth Calculator Threshold

ADVANCED SERVICES Redundancy IP Mobility Stateful Firewall External Services

> VPN Services

Advanced Services > VPN Services > IPSEC

IPSEC PPTP Dialers Emulate VPN Servers Site-To-Site VIA Advanced

L2TP and XAUTH Parameters

Enable L2TP ☒

Enable XAuth ☒

Authentication Protocols ☒ PAP ☐ EAP ☐ CHAP ☐ MSCHAP ☐ MSCHAPv2

Primary DNS Server 0.0.0.0

Secondary DNS Server 0.0.0.0

Primary WINS Server 0.0.0.0

Secondary WINS Server 0.0.0.0

Address Pools

Pool Name	Start Address	End Address
RAP-POOL	10.4.5.1	10.4.5.100

Click Add

Define a pool – Start & End IP

Source NAT

Enable Source NAT ☒

NAT Pool Remote AP

NAT-T

Enable NAT-T ☒

Aggressive Mode

IKE Aggressive Group Name (Only needed for XAUTH)

IP Compression

Enable IP Compression ☒

IKE Server Certificate

IKE Server Certificate Assigned for VPN-Client --NONE--

CA Certificate Assigned for VPN-Clients

CA Certificate

None found

Add

IKF Shared Secrets

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

Dashboard Monitoring Configuration Diagnostics Maintenance Save Configuration

WIZARDS AP Controller Campus WLAN Remote AP WIP AirWave

NETWORK Controller VLANs Ports Uplink IP

SECURITY Authentication Access Control

WIRELESS AP Configuration AP Installation

Wireless > AP Installation > Whitelist

Provisioning Provisioning Profile Whitelist

Whitelist Campus AP Remote AP

Number of Entries: 3

AP MAC Address	User Name	AP Group	AP Name	Description	Revoked	IP-Address
00:0b:b6:		REMOTE_APS	^_155			0.0.0.0
00:0b:b8:		REMOTE_APS				0.0.0.0
40:e3:d6:		REMOTE_APS	AYMAN RAP 109			0.0.0.0

Add Cancel

1 | 1-3 of 3

1

2

3

4

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

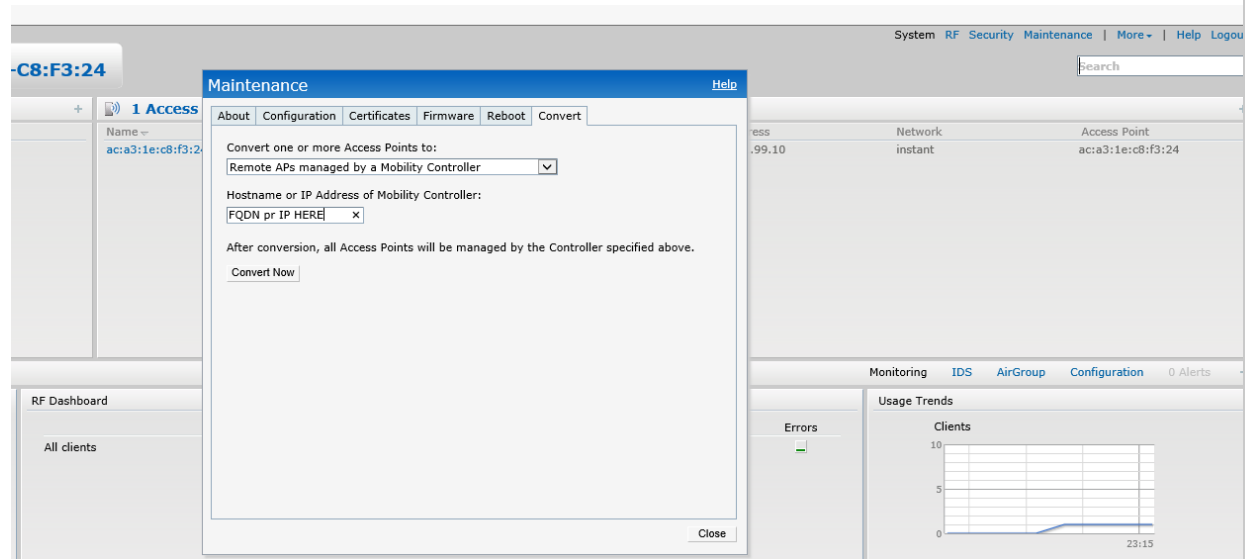
Step 6: Connect to the IAP web Interface, choose Maintenance and Convert to Remote AP. Specify the Public IP or FQDN of the controller and press convert. If the operation is successful, you will be prompted with a success message and the access point will reboot and join the controller.

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

- Dashboard
 - Overview
 - Networks
 - Access Points
 - Clients
- Configuration
- Maintenance
 - About
 - Firmware
 - Configuration
 - Certificates
 - Reboot
 - Convert
 - Regulatory
 - Option 82 XML

Convert

Convert one or more Access Points to

Remote APs managed by a Mobility Controller

Hostname or IP Address of Mobility Controller

labvpn.publicdomain.c

After conversion, all Access Points will be managed by the Controller specified above.

Convert

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

Dashboard Monitoring Configuration Diagnostics Maintenance

NETWORK

- Network Summary
- All WLAN Controllers
- All Access Points
- All Mesh Nodes
- All Air Monitors
- All Air Routers
- All Routers
- All WLAN Clients

CONTROLLER

- Access Points
- Mesh Nodes
- Air Monitors
- IP Routing
- IP Mobility
- IP Multicast
- Clients
- Blacklist Clients
- Firewall Hits
- External Services Interface
- Tunneled Node Ports
- Ports
- Uplink
- Universal Serial Bus
- WLAN
- REMOTE-dot1x

Controller > Access Points

Search Results

Name	AP Group	AP IP	Outer AP IP	AP Type	.bg Clients/Channel/ EIRP/MaxEIRP/Standard	.a Clients/Channel/ EIRP/MaxEIRP/Standard	Enet 1	IPSEC	Uptime	PPPoE	Fl
AYMAN RAP 109	REMOTE_APS	10.1.1.94	20.1.1.36	RAP-109	1/1/9/20/n(20)	0/116+/18/23/n(40)	Wired Port	enable	3h:37m:52s	disable	RE

Flags: 1 = 802.1x authenticated AP; 2 = Using IKE version 2; A = Enet1 in active/standby mode; B = Battery Boost On; C = Cellular; D = Disconn. Extra Calls On; E = Wired AP enabled; F = AP failed 802.1x authentication; H = Hotspot Enabled; L = Client Balancing Enabled; M = Mesh; N = 802.11b protection disabled; P = PPPOE; R = Remote AP; S = AP connected as standby; X = Maintenance Mode; a = Reduce ARP packets in the air; d = Drop Mcast/Bcast On; i = Custom-Cert RAP; I = Provisioned as Indoor; o = Provisioned as Outdoor; p = Restriction mode in POE-AF; r = 802.11r Enabled; Q = DFS CAC timer running

Channel followed by "*" indicates channel selected due to unsupported configured channel.

Status Profile AP Activity Packet Capture Launch AirMagnet Ping Overview USB Ethernet Switching 802.11K Report

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

Dashboard Monitoring Configuration Diagnostics Maintenance

NETWORK

- Network Summary
- All WLAN Controllers
- All Access Points
- All Mesh Nodes
- All Air Monitors
- All Air Routers
- All Routers
- All WLAN Clients

CONTROLLER

- Access Points
- Mesh Nodes
- Air Monitors
- IP Routing
- IP Mobility
- IP Multicast
- Clients
- Blacklist Clients
- Firewall Hits
- External Services Interface
- Tunneled Node Ports
- Ports
- Uplink
- Universal Serial Bus
- WLAN
- REMOTE-dot1x

Controller > Clients

Clients

Search Results

User Name	Device Type	HAC address	Client IP	User Role	Auth Type	ESSID	AP Name	Phy Type	Age	Roaming Status	Forward Mode
amukaddam	Android	60:21:c6:00:00:00	10.1.1.10	authenticated	802.1x	REMOTE-dot1x	AYMAN RAP 109	802.11g-HT	3h(s) 7min(s)	Wireless	tunnel

Status Profile Client Activity Packet Capture Debug Disconnect Blacklist Ping 802.11K Report

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.

The screenshot shows the Aruba Cloud Services Controller (AR-N18) configuration page. The top navigation bar includes 'Dashboard', 'Monitoring', 'Configuration' (selected), 'Diagnostics', and 'Maintenance'. A 'Save Configuration' button is visible. The left sidebar lists various configuration categories: WIZARDS, AP, Controller, Campus WLAN, Remote AP, WIP, AirWave, NETWORK (expanded), > Controller (selected), VLANs, Ports, IP, SECURITY, Authentication, Access Control, WIRELESS, AP Configuration, AP Installation, and MANAGEMENT. The main content area is titled 'Network > Controller > Sync whitelist service'. It features several tabs: 'System Settings', 'Control Plane Security', 'Cluster Settings', 'Licenses', 'Centralized Licenses', and 'Sync whitelist service' (selected). Under the 'Sync Whitelist with Activate' section, there are four configuration items: 'Enable sync service' with radio buttons for 'Enable' (selected) and 'Disable'; 'Activate user' with a text field containing 'user1'; 'Activate password' with a masked password field; and 'Frequency' with a dropdown set to '1' and '(Days)'. Below this is a 'Commands' section.

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)

The screenshot displays the Aruba AOS 8 web interface. On the left, a sidebar shows the navigation menu with 'Managed Network > SITE1' selected. The main content area is titled 'Configuration' and lists various settings like WLANs, Roles & Policies, Access Points, and AP Groups. The 'AP Groups' section is highlighted, showing a table with columns 'NAME' and 'APs'. The table lists 'default' (2), 'NoAuthApGroup' (2), 'GROUP1' (2), and 'RAP-GROUP' (2). Below this, a sub-table for 'RAP-GROUP' is shown with columns: NAME, IPV4 ADDRESS, IPV6 ADDRESS, MAC ADDRESS, TYPE, and SERIAL #. The interface also includes a 'Pending Changes' indicator in the top right corner.

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.

Managed Network > SITE1 > Pending Changes

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

Controllers

System

Tasks

Redundancy

Maintenance

default

NoAuthApGroup

GROUP1

RAP-GROUP

AP Groups > RAP-GROUP

Profiles for Group RAP-GROUP

Virtual AP profile: AOS8-PSK

General

Virtual AP enable: ☒

VLAN: 99

Forward mode: tunnel

Openflow Enable: ☒

RF

Advanced

Broadcast/Multicast

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)

Managed Network > SITE1 > Pending Changes

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

Controllers

System

Tasks

Redundancy

Maintenance

default

NoAuthApGroup

GROUP1

RAP-GROUP

AP Groups > RAP-GROUP

Profiles for Group RAP-GROUP

Virtual AP profile: AOS8-PSK

General

Virtual AP enable: ☒

VLAN: 99

Forward mode: tunnel

Openflow Enable: ☒

RF

Advanced

Broadcast/Multicast

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.

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

Controllers

System

Tasks

Redundancy

Maintenance

Campus AP 1 Remote APs Mesh APs Whitelist Provisioning Rules

MAC address: aca3:1e:c8:f3:24

Name: RAP214 2

AP group: RAP-GROUP 3

Controller discovery: ☐ Use AP discovery protocol (ADP) ☒ Static 4

Controller IP/DNS name: rou.e.com 5

IP: ☒ DHCP ☐ Static

5 GHz antenna gain: 3.0

2.4 GHz antenna gain: 3.0

Deployment: ☐ Campus ☒ Remote 6 ☐ Mesh ☐ Remote mesh portal

Authentication method: Certificate 7

PKCS12 passphrase:

Trust anchor: self-signed 8

Wi-Fi uplink: ☐

Show advanced options

Cancel 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.

aruba MOBILITY MASTER MM-1

CONTROLLERS 2 ACCESS POINTS 2 CLIENTS 3 ALERTS 1

Managed Network

Dashboard

Overview

Infrastructure

Traffic Analysis

Security

Services

Configuration

Maintenance

2 Controllers 2 Access Devices 0 Uplinks 0 Clusters

Access Points 2 filtered by Status Up

NAME	STATUS	CLIENTS	UPTIME	MANAGED BY	GROUP	MODEL
RAP214	Up	3	12m 33s	VMC-1	RAP-GROUP	214
AP-225-1	Up	0	9w 2d	VMC-1	GROUP1	225

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

aruba MOBILITY MASTER MM-1

CONTROLLERS 2 ACCESS POINTS 2 CLIENTS 3 ALERTS 1

Managed Network

Dashboard

Overview

Infrastructure

Traffic Analysis

Security

Services

Configuration

Maintenance

3 Clients 1 WLAN 14.0 MB 4 Radios

Wireless Clients 3 filtered by Access Point MAC address aca3:1e:c8:f3:24

NAME	IP ADDRESS	HEALTH	BAND	ROLE	SNR	USAGE	WLAN	CONNECTE...
172.16.99.15	172.16.99.15	Good	5 GHz	DemoUserRole	37 dB	-	AOS8-PSK	RAP214
172.16.99.4	172.16.99.4	Good	5 GHz	DemoUserRole	22 dB	1.20 MB	AOS8-PSK	RAP214
172.16.99.5	172.16.99.5	Good	5 GHz	DemoUserRole	31 dB	-	AOS8-PSK	RAP214

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)

The screenshot shows the Aruba Mobility Master configuration page for 'Managed Network > SITE1'. The left sidebar shows the navigation menu with 'Managed Network (2)' expanded, showing 'SITE1 (2)', 'SITE2 (0)', and 'SITE3 (0)'. The main content area is divided into a left sidebar with 'Configuration' selected, and a main panel showing 'AP Groups'. The 'AP Groups' table lists 'default', 'NoAuthApGroup', 'GROUP1', and a new 'RAP-GROUP' which is highlighted in orange. Below the table, the 'AP Groups > RAP-GROUP' configuration page is shown, with tabs for 'APs', 'WLANs', 'Radio', 'Mesh', 'LMS', and 'MultiZone'. The 'APs' tab is active, showing a table with columns: NAME, IPV4 ADDRESS, IPV6 ADDRESS, MAC ADDRESS, TYPE, and SERIAL #.

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.

The screenshot shows the Aruba Mobility Master configuration page for 'Managed Network > SITE1'. The left sidebar shows the navigation menu with 'Managed Network (2)' expanded, showing 'SITE1 (2)', 'SITE2 (0)', and 'SITE3 (0)'. The main content area is divided into a left sidebar with 'Configuration' selected, and a main panel showing 'AP Groups'. The 'AP Groups' table lists 'default', 'NoAuthApGroup', 'GROUP1', and a new 'RAP-GROUP' which is highlighted in orange. Below the table, the 'AP Groups > RAP-GROUP' configuration page is shown, with tabs for 'APs', 'WLANs', 'Radio', 'Mesh', 'LMS', and 'MultiZone'. The 'Profiles' tab is active, showing a list of profiles for the group 'RAP-GROUP'. The 'Virtual AP profile: AOS8-PSK' is selected. The 'General' section is expanded, showing 'Virtual AP enable' checked, 'VLAN' set to 99, 'Forward mode' set to 'tunnel', and 'Openflow Enable' checked. Other sections like 'RF', 'Advanced', and 'Broadcast/Multicast' are collapsed.

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)

Managed Network > SITE1 > Pending Changes

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

Controllers

System

Tasks

Redundancy

Maintenance

default --

NoAuthApGroup --

GROUP1 2

RAP-GROUP --

AP Groups > RAP-GROUP

Profiles for Group RAP-GROUP

- AP system
- Ethernet interface 0 port configuration
- Ethernet interface 1 port configuration
- Ethernet interface 2 port configuration**
- Ethernet interface 3 port configuration
- Ethernet interface 4 port configuration
- Ethernet usb port configuration
- Provisioning
- Rest API

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.

Managed Network > SITE1 > Pending Changes

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

Controllers

System

Tasks

Redundancy

Maintenance

Clusters

AirGroup

VPN

Firewall

IP Mobility

External Services

DHCP

WAN

IKEv1

IKEv2

General VPN

Address Pools

POOL NAME	START ADDRESS	END ADDRESS

Add New Address Pool

Pool name: RAP-POOL

Start address IPv4 or v6: 169.254.0.10

End address IPv4 or v6: 169.254.0.50

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

Dashboard

Overview
Networks
Access Points
Clients

Configuration

Maintenance

About
Firmware
Configuration
Certificates
Reboot
Convert
Regulatory
Option 82 XML

Convert

Convert one or more Access Points to

Remote APs managed by a Mobility Controller

Hostname or IP Address of Mobility Controller

labvpn.publicdomain.c

After conversion, all Access Points will be managed by the Controller specified above.

Convert

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.

aruba MOBILITY MASTER MM-1 CONTROLLERS 2 ACCESS POINTS 2 CLIENTS 3 ALERTS 1 admin

Managed Network

Dashboard

Overview

Infrastructure

Traffic Analysis

Security

Services

Configuration

Maintenance

Access Points 2 filtered by Status Up

NAME	STATUS	CLIENTS	UPTIME	MANAGED BY	GROUP	MODEL
RAP214	Up	3	12m 33s	VMC-1	RAP-GROUP	214
AP-225-1	Up	0	9w 2d	VMC-1	GROUP1	225

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

aruba MOBILITY MASTER MM-1 CONTROLLERS 2 ACCESS POINTS 2 CLIENTS 3 ALERTS 1 admin

Managed Network

Dashboard

Overview

Infrastructure

Traffic Analysis

Security

Services

Configuration

Maintenance

Wireless Clients 3 filtered by Access Point MAC address ac:a3:1e:c8:f3:24

NAME	IP ADDRESS	HEALTH	BAND	ROLE	SNR	USAGE	WLAN	CONNECTE...
172.16.99.15	172.16.99.15	Good	5 GHz	DemoUserRole	37 dB	-	AOS8-PSK	RAP214
172.16.99.4	172.16.99.4	Good	5 GHz	DemoUserRole	22 dB	1.20 MB	AOS8-PSK	RAP214
172.16.99.5	172.16.99.5	Good	5 GHz	DemoUserRole	31 dB	-	AOS8-PSK	RAP214

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.

The screenshot shows the Aruba Mobility Master configuration interface. On the left is a navigation tree with 'Mobility Master' and 'Managed Network (2)' containing 'SITE1 (2)' and 'SITE3 (0)'. The main area is titled 'Configuration' and has tabs for 'General', 'Admin', 'AirWave', 'CPSec', 'Certificates', 'SNMP', 'Logging', 'Profiles', 'Whitelist', and 'More'. The 'Whitelist' tab is selected. It contains fields for 'Activate username' (set to 'username-here'), 'Activate password' (masked with dots), and 'Retype password' (also masked). Below these are dropdown menus for 'Custom certificate' and 'Server certificate', both set to '-None-'. There is a checked checkbox for 'Sync service' and a 'Frequency' field set to '1' day(s).

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>