Aruba Remote Access Point Solution Guide for Teleworkers and Home Offices

aruba

a Hewlett Packard Enterprise company

Copyright Information

Open Source Code

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

Revision History

The following table lists the revisions of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

Chapter 2
Introduction

The following topics are discussed in this chapter:

- What is a RAP and how does it work?
- Overview of the RAP Configuration
- RAP Infrastructure Requirements
- Architecture of a RAP Deployment
- RAP Infrastructure Configuration
- RAP Termination to a Cluster with NAT Support

The Aruba Remote Access Point (RAP) solution caters to the needs of all fixed telecommuter, micro, and mobile access deployments. In these deployments, the Aruba RAP typically terminates on the Mobility Controllers in the network demilitarized zones (DMZ), that are managed by a pair of Mobility Masters in the data center.

Similar to the way that campus-based APs are terminated, the Mobility Controllers terminate the RAPs coming in over the Internet with IPsec-protected sessions. That way, the Mobility Controllers act as a headend to the RAPs IPsec tunnels (VPN Concentrator).

Redundancy and scalability can be achieved by leveraging the clustering feature in ArubaOS 8.x.

What is a RAP and how does it work?

Any Aruba access point can be provisioned to operate as a RAP. The purpose of deploying a RAP is to leverage the wireless and wired features of an Aruba access point from a remote location across the Internet.

The RAP is configured to use IPsec to connect to a Mobility Controller's public IP over UDP 4500 for NAT-T. Once the IPsec tunnel is established with the controller, the RAP receives an inner IP known to the controller from a pre-configured VPN IP pool.

From that point on, the RAP is treated like any other campus AP reachable using it's inner IP. All WLAN and wired port configurations used by campus APs are equally used by the RAP. In other words, the RAP extends the same SSIDs available in the office so that employees can work from home as if they were in the office without the need for additional VPN clients.

Overview of the RAP Configuration

Details about each of these steps are discussed in this document.

1. Refer to the RAP Infrastructure Requirements and the RAP Infrastructure Configuration before setting up the RAP deployment.
2. Decide on the RAP configuration type. The VPNC can either be a Managed Device or a Standalone Controller for less than 2000 RAPs and a cluster for larger deployments.
3. Configure a public IP address for the Managed Device. A VPNC deployment requires user VLANs configured and trunked to an upstream switch with external DHCP.
4. Configure the VPN server on the controller by adding the inner IP address pool and the IKE Shared Secrets for the RAP. In case the VPNC is a managed device under a Mobility Master or a standalone controller, create the RAP VPN pool on the VPNC. In case of a cluster of VPNCs, create the RAP pool on the Mobility Master. IKE shared secrets are not needed for certificate-based RAPs.
5. Create a RAP group. This is optional, but recommended.

6. To allow the connection from the RAP to the controller, add the RAP group to the Remote AP whitelist. You can do this either as a sync from Activate, imported as a CSV file or manually entered.
7. Set up the Internet Firewall with public IP address with UDP 4500 DST-NAT to the VPNC Controller-IP.
8. Create the required RAP users, firewall policies, and user roles.
9. Create the AAA, WLAN SSID, Virtual AP, AP system, RF, Regulatory domain and wired profiles.
10. Assign the Virtual AP, RF, Regulatory domain, and wired ports profiles to the RAP ap-group that was created earlier.
11. Provision the RAP.
12. Install the RAP at the remote location.

RAP Infrastructure Requirements

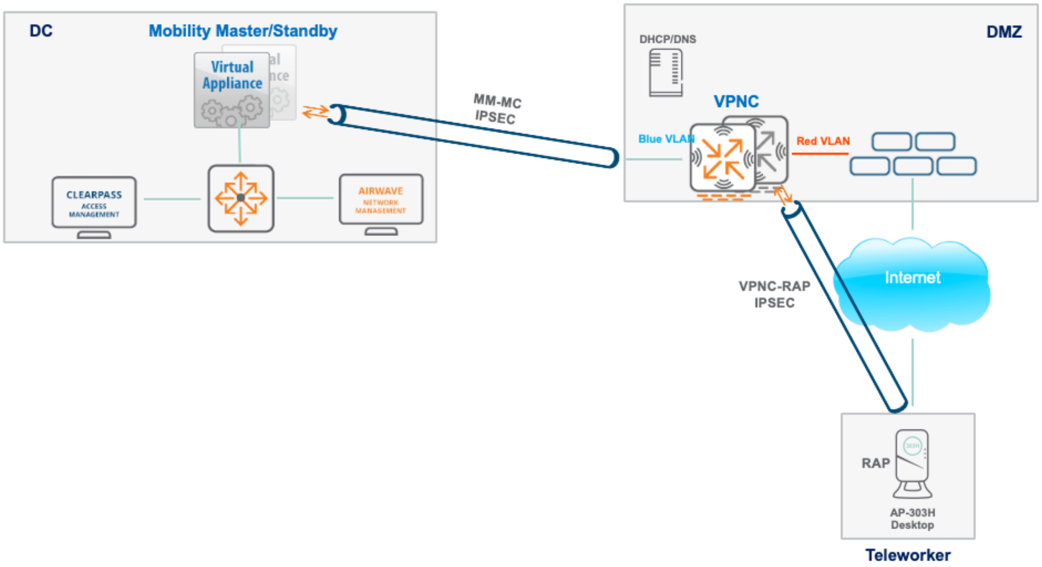
It is assumed in this document that an existing WLAN infrastructure is already in place to support wireless users at the corporate site. Nonetheless, listed below are the minimum infrastructure and network requirements:

- Mobility Controller as the VPN Concentrator (VPNC)
- One public IP per VPNC
- One or a pair of Mobility Masters (optional)
- Radius Server to authenticate the users (ClearPass)
- One/Two infrastructure VLANs and subnets (red and blue)
- User VLANs extended to the VPNC
- DHCP server to support user subnets that DHCP needs

Architecture of a RAP Deployment

The following illustration describes the functioning of a RAP.

Figure 1 *RAP Architecture*



Mobility Master

The Mobility Master deployment can be either a Mobility Master Virtual Appliance or Mobility Master Hardware Appliance.

A pair in L2-redundancy is recommend for high availability.

Listed below are the configuration tasks required to support the DMZ controllers acting as headend to terminate RAP IPsec tunnels:

- Mobility Master Virtual Appliance license (if the Mobility Master is virtual) and Mobility Controller Virtual Appliance license (if a VMC is used).
- AP and PEF licenses to support the number of AP/RAPs deployed.
- A group created in the configuration hierarchy to contain the DMZ controllers.
- VPNC device created in the hierarchy under the DMZ group.
- Mobility Controller IPsec configuration (PSK or cert-based).
- RAP local Pool:
  - Single Mobility Controller: The RAP pool is pushed down to the Mobility Controller.
  - Cluster of Mobility Controllers: The RAP pool configured on the Mobility Master, and not the Mobility Controller.
- RAP whitelisting: local-dB or external (ClearPass)

Mobility Controller

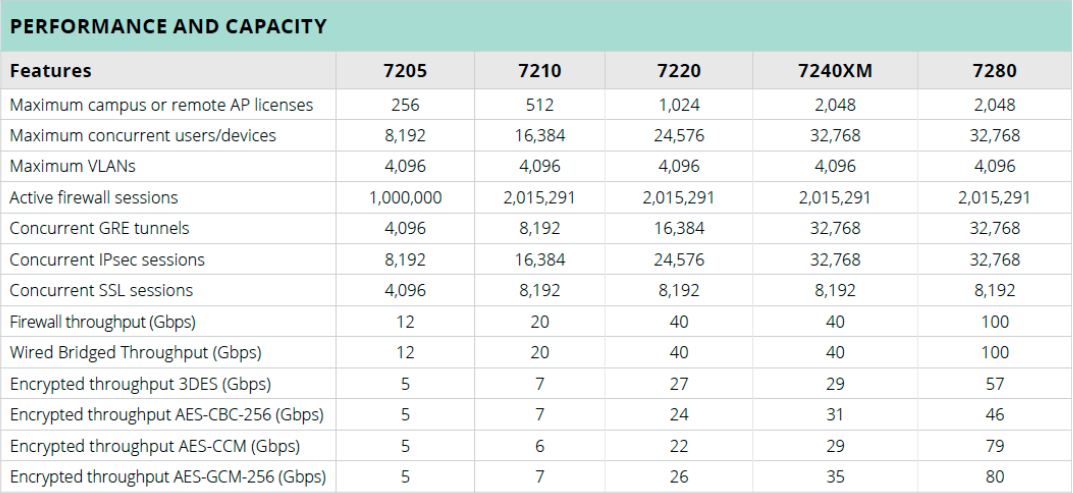
There are two Mobility Controller options, Hardware Mobility Controller (70xx, 72xx) or Virtual Mobility Controller.

In this document, only the deployment of the Hardware Mobility Controller is considered for RAP provisioning, with the following caveat.

> NOTE
>
> A certificate-based RAP does not come up on a Virtual Mobility Controller (VMC) because the VMC does not have a TPM certificate. In order to work around it, the RAP should be brought up on the Virtual Mobility Controller as a campus AP first, and then it is to be provisioned as a RAP with the Virtual Mobility Controller self-signed cert as a trust anchor.

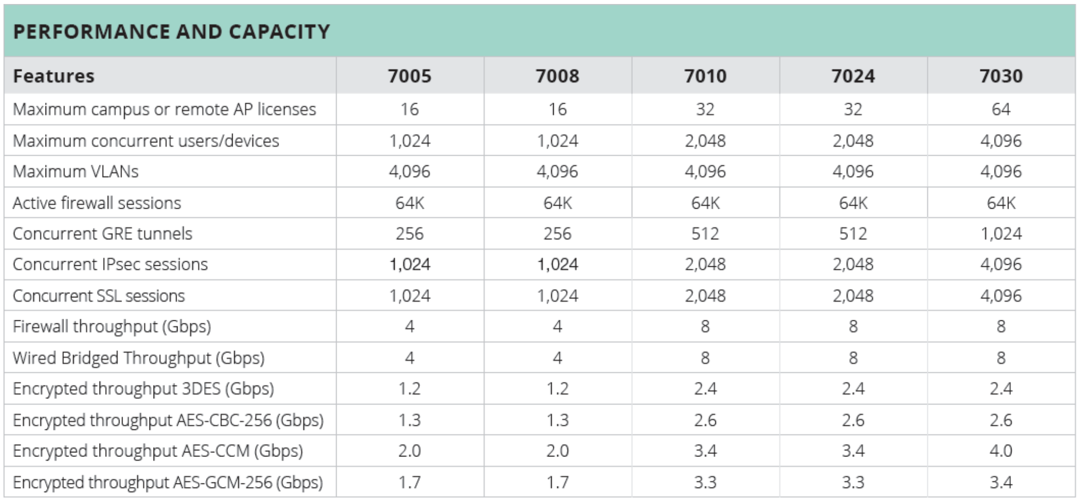
The full setup option is recommended in the initial setup of the Mobility Controller, if the Mobility Master is a Mobility Master Virtual Appliance.

Mobility Controller Sizing Guide



PERFORMANCE AND CAPACITY

Features	7205	7210	7220	7240XM	7280
Maximum campus or remote AP licenses	256	512	1,024	2,048	2,048
Maximum concurrent users/devices	8,192	16,384	24,576	32,768	32,768
Maximum VLANs	4,096	4,096	4,096	4,096	4,096
Active firewall sessions	1,000,000	2,015,291	2,015,291	2,015,291	2,015,291
Concurrent GRE tunnels	4,096	8,192	16,384	32,768	32,768
Concurrent IPsec sessions	8,192	16,384	24,576	32,768	32,768
Concurrent SSL sessions	4,096	8,192	8,192	8,192	8,192
Firewall throughput (Gbps)	12	20	40	40	100
Wired Bridged Throughput (Gbps)	12	20	40	40	100
Encrypted throughput 3DES (Gbps)	5	7	27	29	57
Encrypted throughput AES-CBC-256 (Gbps)	5	7	24	31	46
Encrypted throughput AES-CCM (Gbps)	5	6	22	29	79
Encrypted throughput AES-GCM-256 (Gbps)	5	7	26	35	80



PERFORMANCE AND CAPACITY					
Features	**7005**	**7008**	**7010**	**7024**	**7030**
Maximum campus or remote AP licenses	16	16	32	32	64
Maximum concurrent users/devices	1,024	1,024	2,048	2,048	4,096
Maximum VLANs	4,096	4,096	4,096	4,096	4,096
Active firewall sessions	64K	64K	64K	64K	64K
Concurrent GRE tunnels	256	256	512	512	1,024
Concurrent IPsec sessions	1,024	1,024	2,048	2,048	4,096
Concurrent SSL sessions	1,024	1,024	2,048	2,048	4,096
Firewall throughput (Gbps)	4	4	8	8	8
Wired Bridged Throughput (Gbps)	4	4	8	8	8
Encrypted throughput 3DES (Gbps)	1.2	1.2	2.4	2.4	2.4
Encrypted throughput AES-CBC-256 (Gbps)	1.3	1.3	2.6	2.6	2.6
Encrypted throughput AES-CCM (Gbps)	2.0	2.0	3.4	3.4	4.0
Encrypted throughput AES-GCM-256 (Gbps)	1.7	1.7	3.3	3.3	3.4

Design Considerations

- **One-arm Vs Two-arm**: The Mobility Controller in the DMZ can be deployed as either, a one-arm controller with one infrastructure VLAN and one IP address as the controller-ip that will be used to communicate with the Mobility Master or a two-arm controller using two infrastructure interfaces. In such case, it is important for future clustering considerations to use the controller-IP from the red subnet (refer to the above architecture diagram) that initiates the IPsec connection to the Mobility Master through the blue VLAN.
- **Public-IP**: The controller-ip could be the public IP that the RAPs terminate on, or a private IP mapped to a public IP (one-to-one NAT or Destination-NAT) on the Internet firewall. The Internet firewall requires a rule to allow UDP 4500 traffic to the controller-IP.
- **User VLANs**: It is best practice to dedicate one or more VLANs to remote teleworkers, and such VLANs are L2 extended to the uplink L3 switch that acts as the default gateway for those VLANs. Furthermore, it is equally important to control broadcast and multicast traffic by using VLAN and Virtual AP mitigation and optimization knobs.

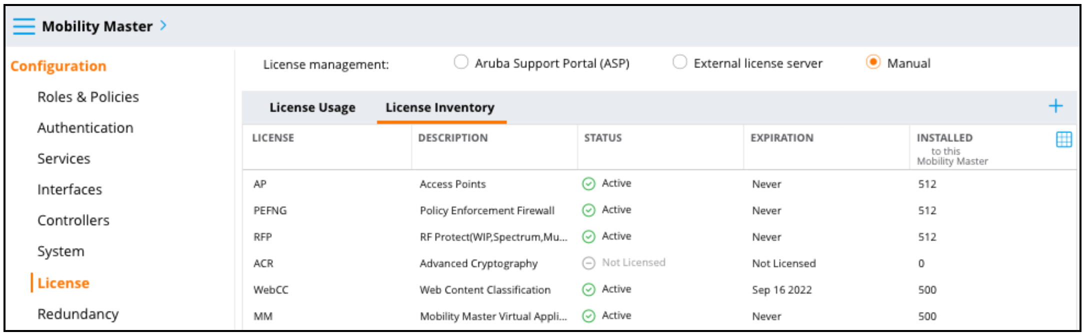
RAP Infrastructure Configuration

The following section describes the infrastructure configuration process.

Licensing

Licenses on the Mobility Master should be sufficient to support the VPNC and in RAP devices on one hand, as well as AP and PEF licenses on the other hand. By accessing the license inventory, additional licenses could be added either manually or downloaded from the Aruba Support Portal.

Figure 2 *Mobility Master License Inventory in ArubaOS 8.x*



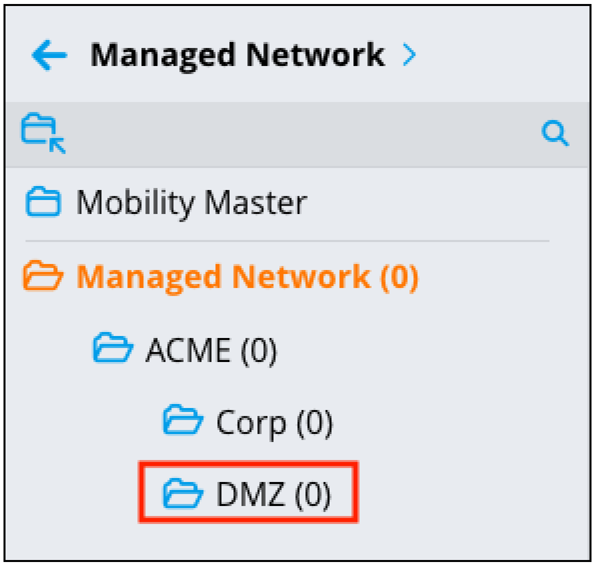
License management: ○ Aruba Support Portal (ASP) ○ External license server ● Manual

LICENSE	DESCRIPTION	STATUS	EXPIRATION	INSTALLED to this Mobility Master
AP	Access Points	✓ Active	Never	512
PEFNG	Policy Enforcement Firewall	✓ Active	Never	512
RFP	RF Protect(WIP,Spectrum,Mu...	✓ Active	Never	512
ACR	Advanced Cryptography	⊖ Not Licensed	Not Licensed	0
WebCC	Web Content Classification	✓ Active	Sep 16 2022	500
MM	Mobility Master Virtual Appli...	✓ Active	Never	500

Hierarchy

A DMZ group needs to be added to the Mobility Master's existing hierarchy under the **Managed Network**.

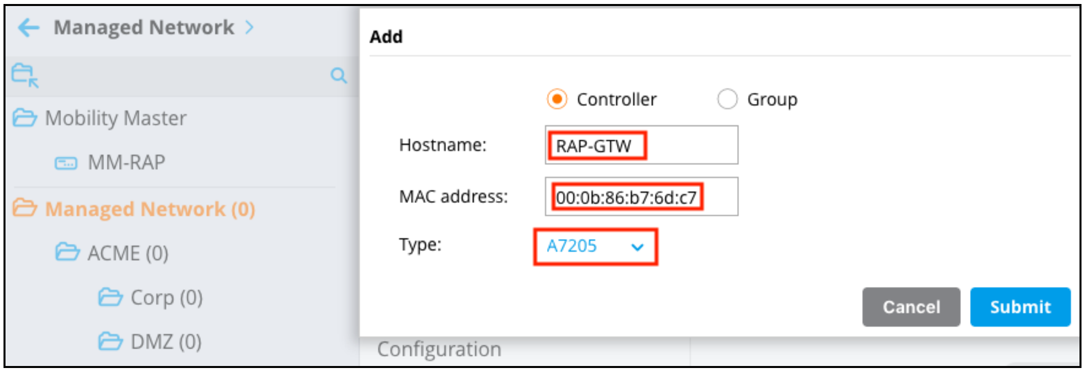
Figure 3 *DMZ Hierarchy in ArubaOS 8.x*



VPNC Device

With the device type and MAC address, the VPNC device can be created under the DMZ group as displayed below.

Figure 4 *Device Creation in ArubaOS 8.x*



Add

● Controller ○ Group

Hostname: RAP-GTW

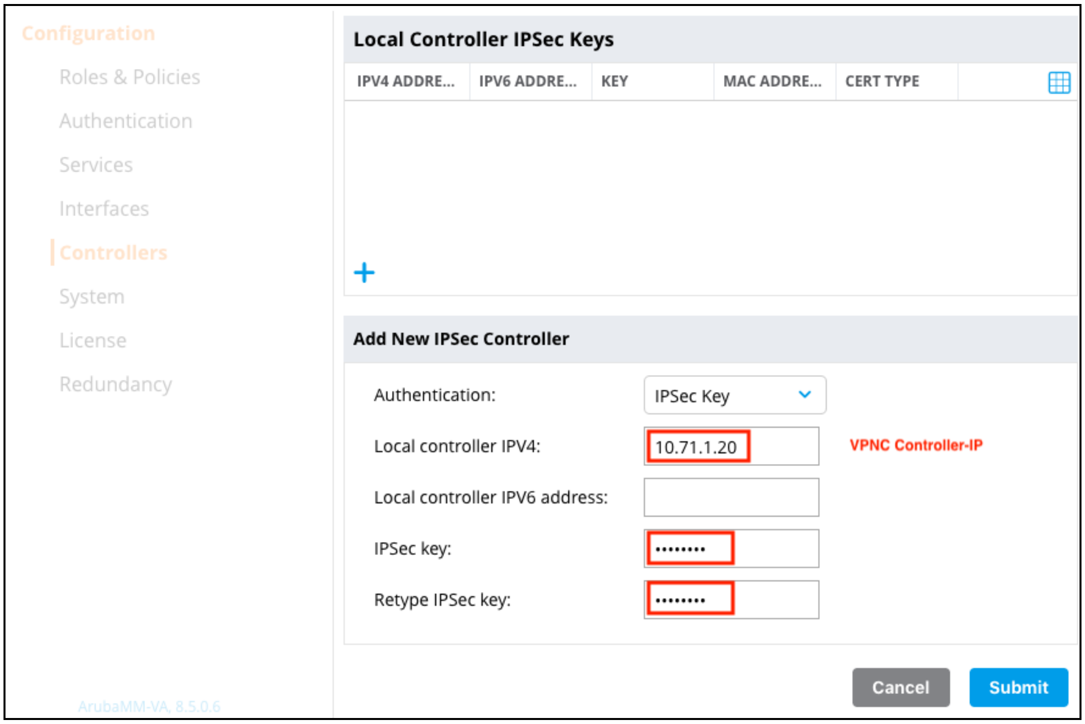
MAC address: 00:0b:86:b7:6d:c7

Type: A7205

IPsec Mobility Controller

PSK-based IPsec is used in the following example, although cert-based IPsec will also work. See, ArubaOS 8.5.0.0 user guide for further details.

Figure 5 *PSK-Based IPsec Key in ArubaOS 8.x*



Local Controller IPSec Keys

IPV4 ADDRE...	IPV6 ADDRE...	KEY	MAC ADDRE...	CERT TYPE

Add New IPSec Controller

Authentication:	IPSec Key
Local controller IPV4:	10.71.1.20
Local controller IPV6 address:	
IPSec key:	••••••••
Retype IPSec key:	••••••••

VPNC Controller-IP

RAP VPN Pool

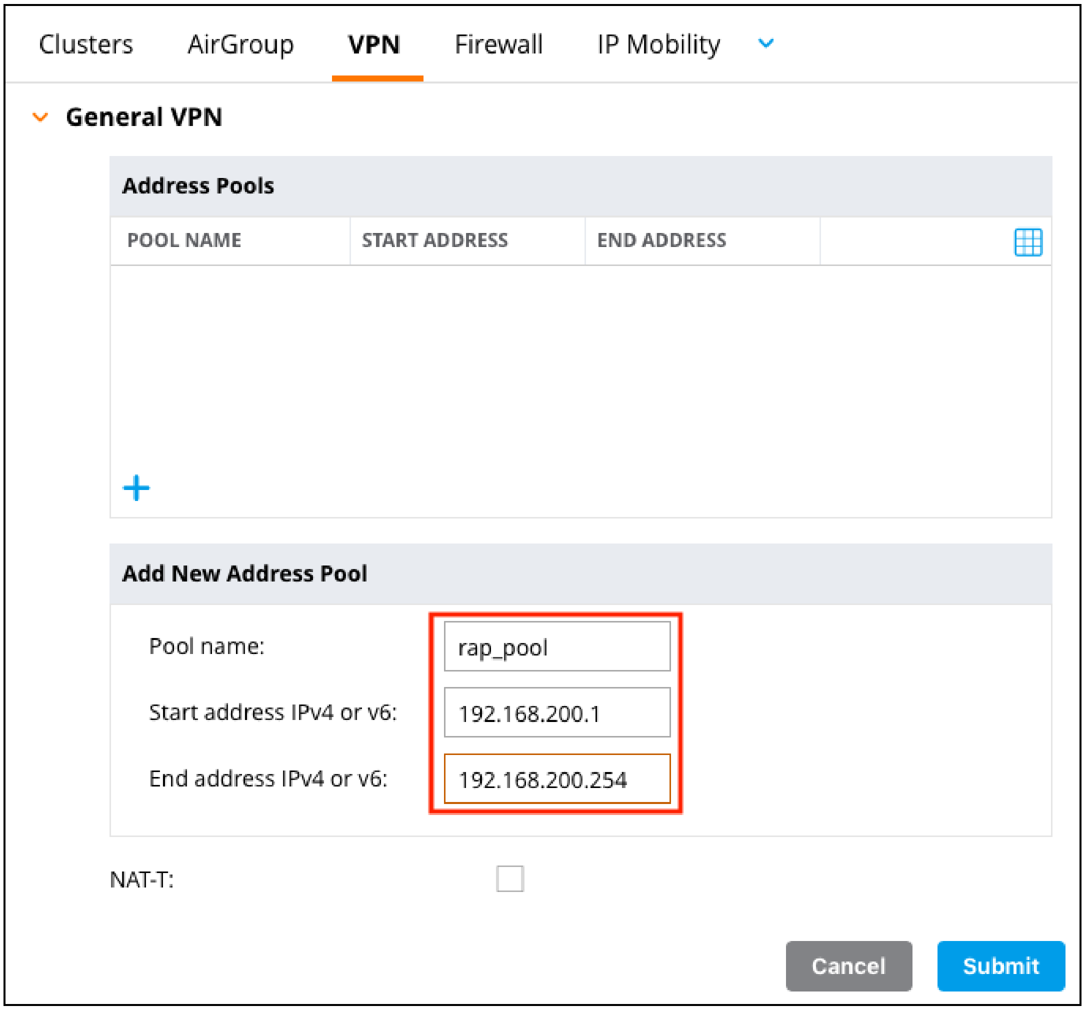
The VPN pool is configured to distribute inner IP addresses to the RAPs. All control communication and GRE tunnels take place inside the IPsec tunnel between the RAP's inner IP and the VPNC's controller-ip.

In the case of the VPNC being a managed device under a Mobility Master or a standalone controller, the RAP VPN pool resides on the VPNC. The RAP pool is created and resides on the Mobility Master in the case of a cluster of VPNCs.

Configuring VPNC as a Managed Device

From the VPNC device folder on the Mobility Master, navigate to **Configuration > Services > VPN > General VPN** to configure the RAP VPN pool.

Figure 6 *Configure RAP VPN Pool in ArubaOS 8.x*



Pool name: rap_pool

Start address IPv4 or v6: 192.168.200.1

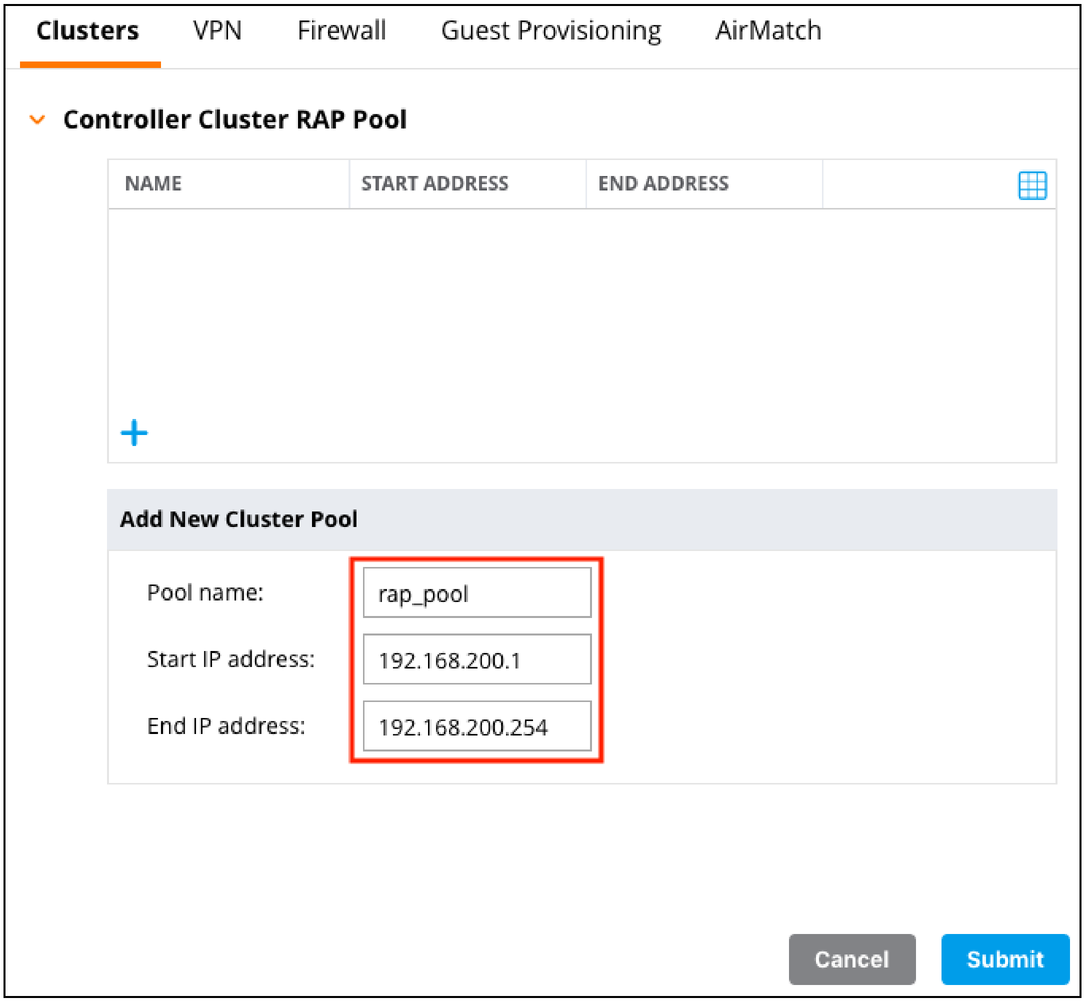
End address IPv4 or v6: 192.168.200.254

NAT-T: □

Configuring VPNC in a Cluster

From the Mobility Master in the Mobility Master hierarchy, navigate to **Configuration > Services > Clusters > Controller Cluster RAP Pool**.

Figure 7 *Configuring Cluster RAP Pool in ArubaOS 8.x*



Pool name: rap_pool

Start IP address: 192.168.200.1

End IP address: 192.168.200.254

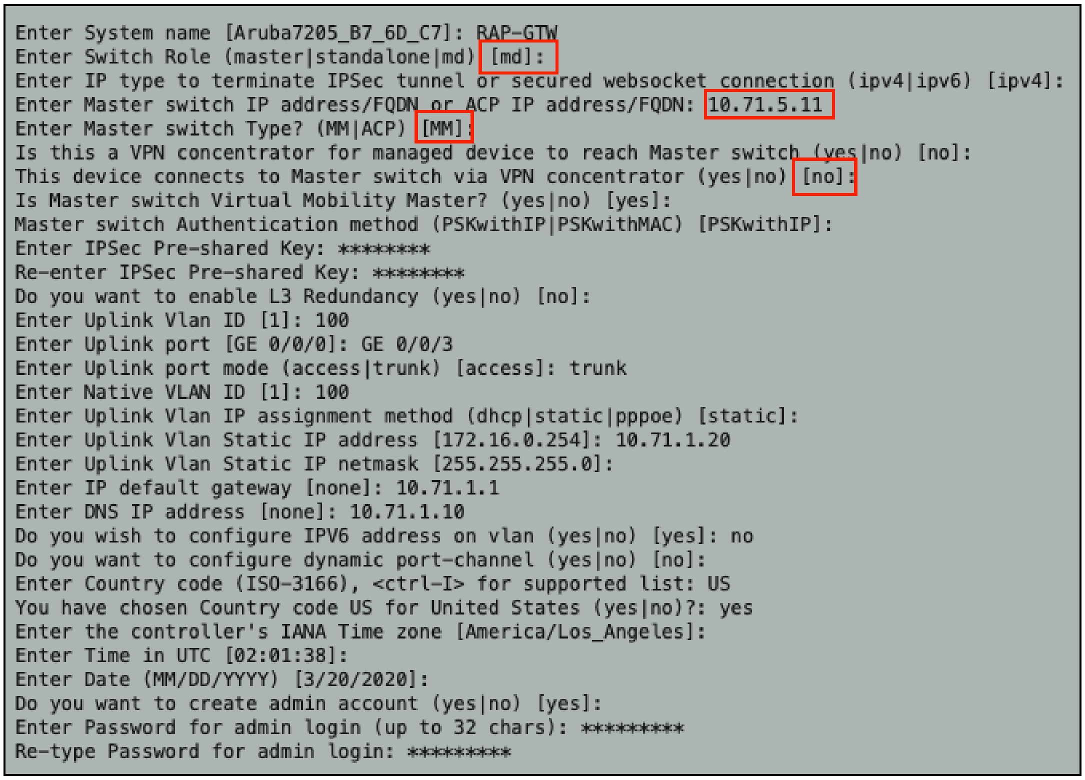
RAP Whitelisting

The RAP whitelisting is either done locally on the Mobility Master or the standalone VPNC. Refer to the Activate section if Activate syncing is desired, and the reference to CPPM for external database whitelisting.

VPNC Full Setup

Here is an illustration of a Mobility Controller full setup:

Figure 8 *Mobility Controller Full Setup in ArubaOS 8.x*



```
Enter System name [Aruba7205_B7_6D_C7]: RAP-GTW
Enter Switch Role (master|standalone|md) [md]:
Enter IP type to terminate IPSec tunnel or secured websocket connection (ipv4|ipv6) [ipv4]:
Enter Master switch IP address/FQDN or ACP IP address/FQDN: 10.71.5.11
Enter Master switch Type? (MM|ACP) [MM]:
Is this a VPN concentrator for managed device to reach Master switch (yes|no) [no]:
This device connects to Master switch via VPN concentrator (yes|no) [no]:
Is Master switch Virtual Mobility Master? (yes|no) [yes]:
Master switch Authentication method (PSKwithIP|PSKwithMAC) [PSKwithIP]:
Enter IPSec Pre-shared Key: ********
Re-enter IPSec Pre-shared Key: ********
Do you want to enable L3 Redundancy (yes|no) [no]:
Enter Uplink Vlan ID [1]: 100
Enter Uplink port [GE 0/0/0]: GE 0/0/3
Enter Uplink port mode (access|trunk) [access]: trunk
Enter Native VLAN ID [1]: 100
Enter Uplink Vlan IP assignment method (dhcp|static|pppoe) [static]:
Enter Uplink Vlan Static IP address [172.16.0.254]: 10.71.1.20
Enter Uplink Vlan Static IP netmask [255.255.255.0]:
Enter IP default gateway [none]: 10.71.1.1
Enter DNS IP address [none]: 10.71.1.10
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
Do you want to configure dynamic port-channel (yes|no) [no]:
Enter Country code (ISO-3166), <ctrl-I> for supported list: US
You have chosen Country code US for United States (yes|no)?: yes
Enter the controller's IANA Time zone [America/Los_Angeles]:
Enter Time in UTC [02:01:38]:
Enter Date (MM/DD/YYYY) [3/20/2020]:
Do you want to create admin account (yes|no) [yes]:
Enter Password for admin login (up to 32 chars): *********
Re-type Password for admin login: *********
```

Clustering

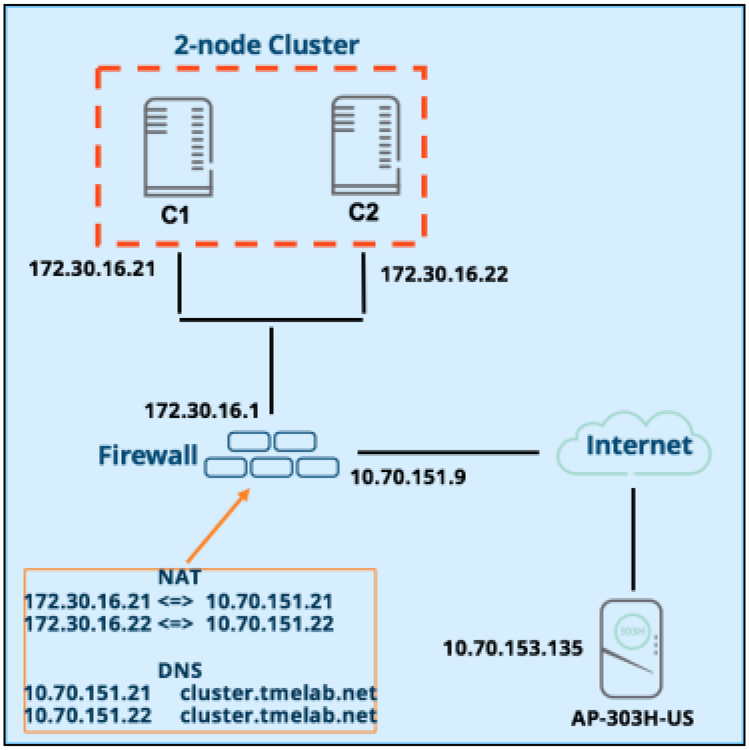
The RAP deployment can be scaled beyond the capacity of a single headend controller, using the clustering feature in ArubaOS 8.x. Placing multiple Mobility Controllers in an ArubaOS 8.x cluster (up to 12 for the 72xx) extends the RAP capacity while providing high availability for RAPs and clients. However, there are other considerations to be taken into account:

- A Mobility Master is mandatory with clustering.
- The inner RAP IP addresses are handed out by the Mobility Master, and the RAP pool is configured at the **/mm** level.
- Every Mobility Controller/node in the cluster requires its own public IP address. In other words, a cluster of 3 Mobility Controllers requires, 3 public IP addresses.
- External AP whitelist using ClearPass is supported for clustering from ArubaOS 8.6.
- The RAP master cannot be a VRRP address. It can only be one of the cluster members controller-IPs, or a round-robin DNS name that resolves to any of those same controller-IPs.

RAP Termination to a Cluster with NAT Support

The RAP termination to an ArubaOS 8.x cluster has been available since ArubaOS 8.0.0.0. However, public IP requirement on every cluster-node prevented deployments that did not meet such requirement. A new enhancement in ArubaOS 8.4.0.0 added support for NAT within the ArubaOS 8.x cluster, where it made it possible to NAT the private cluster nodes controller-IP to public IPs that the RAP could connect to. Since common RAP deployments leverage the Internet firewall to NAT a public IP to the Mobility Controller private IP (either 1-to-1 NAT mapping or via DST-NAT on UDP 4500), the ArubaOS 8.4.0.0 feature consists of adding the unique public IP (one per cluster node) to each controller configuration in the cluster group profile. Subsequently, the NAT mapping is communicated down to the RAP that maps each cluster node private controller-IP to its corresponding public IP.

Figure 9 *Topology Diagram*



Configuration

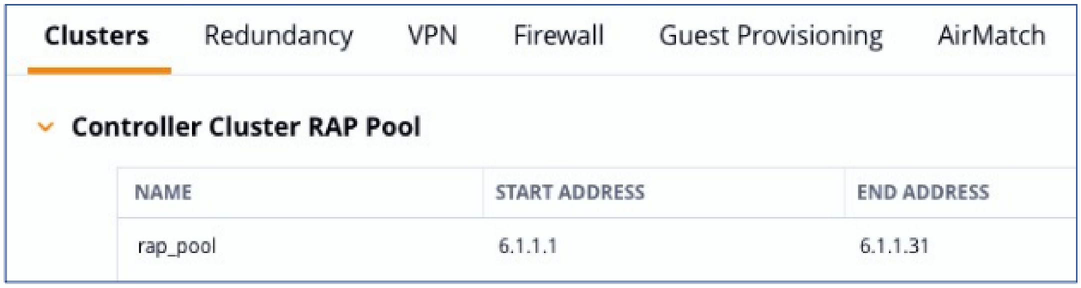
In order to tackle the pertinent configuration of this feature, it is assumed that the WLAN configuration that includes the RAP intended ap-group is already in place. Configuring the WLAN for your RAP is the same as for your typical campus AP.

Therefore, the cluster configuration comes down to the addition of the controllers into the cluster with their mapped public IP addresses. It is left to the reader to augment the cluster

configuration with any desired additional features. The configuration needed to terminate a SOHO RAP over the Internet to a cluster located in the DMZ involves the following steps:

1. In the Mobility Master hierarchy, go to **Configuration > Services > Clusters**, and add a RAP pool as per the following illustration:

Figure 10 *Creating a RAP Pool in ArubaOS 8.x*



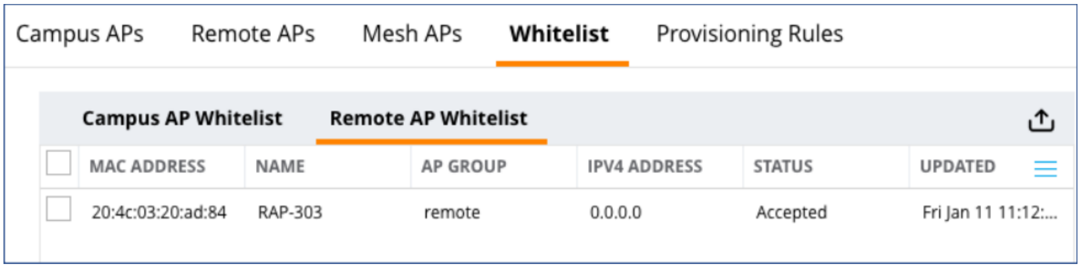
Controller Cluster RAP Pool

NAME	START ADDRESS	END ADDRESS
rap_pool	6.1.1.1	6.1.1.31

```
(AOS84-MM1) [mynode] (config) #lc-rap-pool rap_pool 6.1.1.1 6.1.1.31
```

2. In the **Managed Network** hierarchy, navigate to **Configuration > Access Points > Whitelist > Remote AP Whitelist**, and add the RAP MAC address along with the ap-group that the RAP will belong to.

Figure 11 *Adding a RAP MAC Address in ArubaOS 8.x*



□	MAC ADDRESS	NAME	AP GROUP	IPV4 ADDRESS	STATUS	UPDATED
□	20:4c:03:20:ad:84	RAP-303	remote	0.0.0.0	Accepted	Fri Jan 11 11:12:...

```
(AOS84-MM1) [mynode] #whitelist-db rap add mac-address 20:4c:03:20:ad:84 ap-group remote ap-name RAP-303
```

3. In order for the RAP to reach the cluster node's private controller-IP, a NAT mapping on the Internet firewall is setup to map each node controller-IP to a public IP reachable from the Internet. Such mapping could be a 1-to-1 mapping or a Destination NAT on UDP port 4500. Therefore, an N-nodes cluster requires N public IPs.

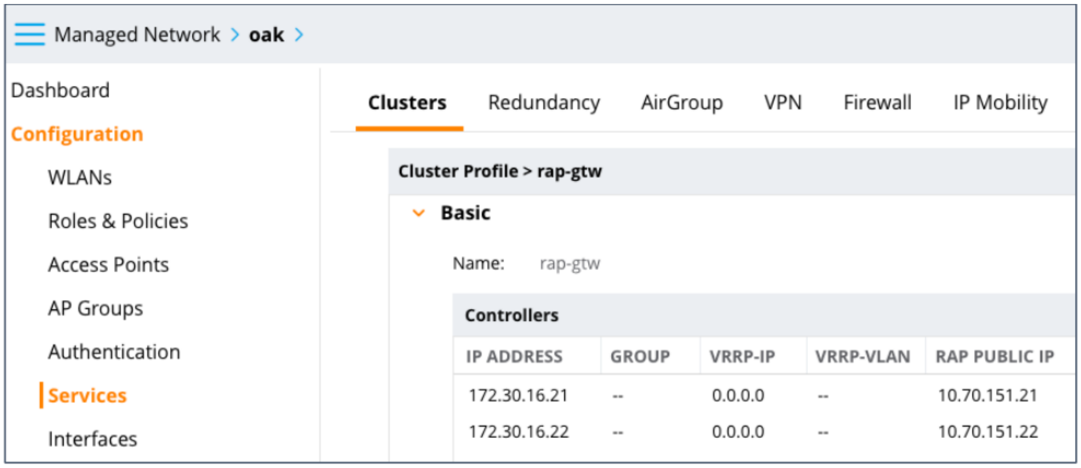
In the topology example provided in this paper, here is the 1-to-1 NAT mapping:

C1 controller-IP 172.30.16.21 <=> 10.70.151.21

C2 controller-IP 172.30.16.22 <=> 10.70.151.22

4. In the cluster group node hierarchy, navigate to **Configuration > Services > Clusters**, and add each node using its controller-IP and the RAP public IP that maps to it.

Figure 12 *Configuring the Cluster Group Profile in ArubaOS 8.x*



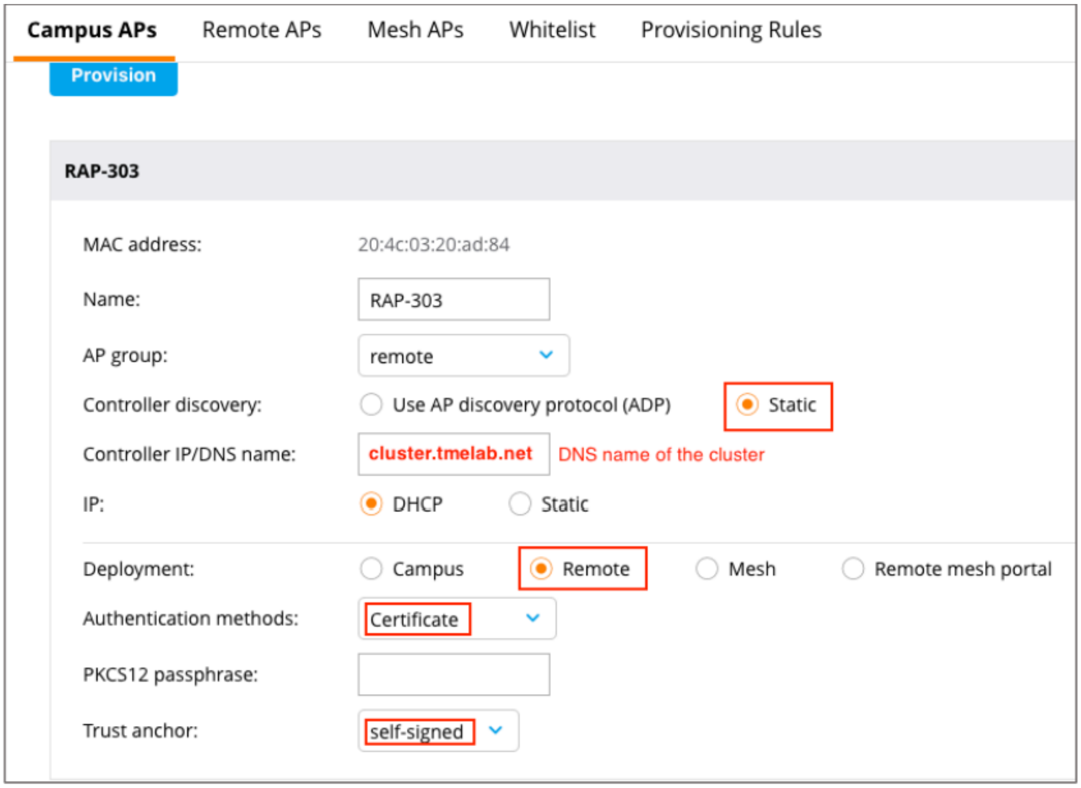
Name: rap-gtw

IP ADDRESS	GROUP	VRRP-IP	VRRP-VLAN	RAP PUBLIC IP
172.30.16.21	--	0.0.0.0	--	10.70.151.21
172.30.16.22	--	0.0.0.0	--	10.70.151.22

```
(AOS84-MM1) [oak] (config) #lc-cluster group-profile rap-gtw
(AOS84-MM1) ^[oak] (Classic Controller Cluster Profile "rap-gtw1")
#controller 172.30.16.21 rap-public-ip 10.70.151.21
(AOS84-MM1) ^[oak] (Classic Controller Cluster Profile "rap-gtw1")
#controller 172.30.16.22 rap-public-ip 10.70.151.22
(AOS84-MM1) ^[oak] (Classic Controller Cluster Profile "rap-gtw1") #end
```

There is more than one approach to provision an access point to be a RAP. The access point could be either a Campus AP, IAP, or an Unified AP that comes up as either as a Campus AP or IAP. Provisioning a Campus AP to a RAP requires the Campus AP to be terminated on a Mobility Controller, while the IAP provisioning to a RAP could either be done through an Activate provisioning profile or manually through the IAP WebUI. In this document, an AP-303H-US was used, and since a cluster of a pair of Mobility Controller Virtual Appliance was used, bringing the AP-303H as a Campus AP on the cluster was a requirement to acquire the controllers self-signed cert as an anchor. Therefore, the WebUI illustration will show a Campus AP being provisioned as a RAP.

Figure 13 *Provisioning Campus AP as RAP in ArubaOS 8.x*



RAP-303

MAC address: 20:4c:03:20:ad:84

Name: RAP-303

AP group: remote

Controller discovery: ○ Use AP discovery protocol (ADP) ● Static

Controller IP/DNS name: cluster.tmelab.net DNS name of the cluster

IP: ● DHCP ○ Static

Deployment: ○ Campus ● Remote ○ Mesh ○ Remote mesh portal

Authentication methods: Certificate

PKCS12 passphrase:

Trust anchor: self-signed

Chapter 3
Configuration Guidelines for RAPs

The following topics are discussed in this chapter:

- Modes of Operation for RAPs
- RAP Bootstrapping Process
- Configuration Profile for RAPs

Most telecommuters who work from home offices require the following services:

- Wired and wireless access to PCs and laptops to securely connect to the corporate resources.
- Wired and wireless access to VoIP phones to securely connect to the corporate voice server.
- Wired and wireless access for family members and guests so that they can connect to the Internet without the need for an additional Internet connection.
- Wired ports and wireless access for home printers and fax machines shared by the employees and the family members in a secure manner without compromising the corporate security policy.

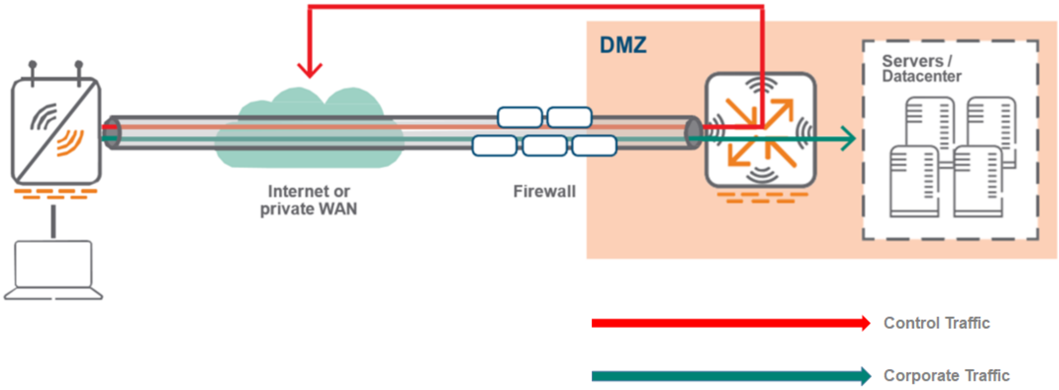
Modes of Operation for RAPs

Aruba RAPs can operate in a number of modes, depending on the requirements of the remote users and that of the corporate office. The forwarding mode parameter in the RAP profile controls how user traffic is handled, including where decryption occurs and where role-based firewall policies are applied. A RAP can operate in tunnel, split-tunnel, or bridge forwarding modes. Each of these modes are described in more detail in the next sections.

Tunnel Mode

When RAPs operate in Tunnel mode, all traffic is tunneled back to the corporate network. There is wireless encryption on the client and controller as well as wired encryption on the RAP and controller. In tunnel mode, there is no access to local traffic, for example a local printer or a home desktop. This type of deployment extends an L2 VLAN from the VPNC to the RAP.

Figure 14 *RAP Tunnel Mode Architecture*

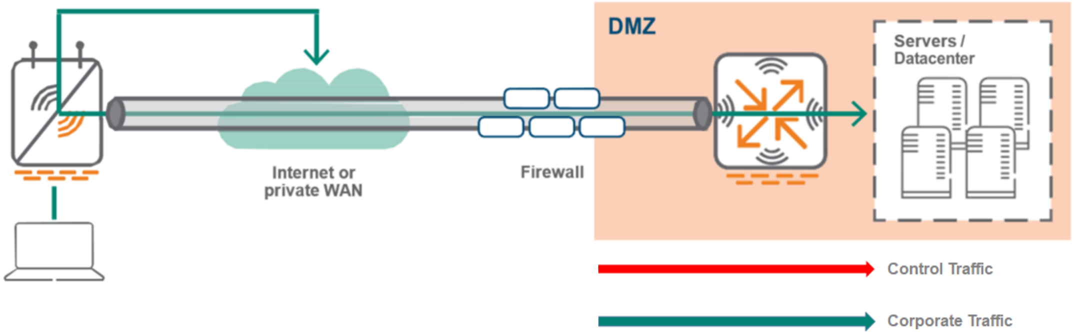


Split Tunnel Mode

Split Tunnel mode allows non-corporate traffic to be bridged out locally to the Internet which reduces the bandwidth in the tunnel between the RAP and the controller that is transporting the corporate traffic. In split-tunnel mode, there is wireless (L2) encryption and decryption on both the client and the RAP.

Corporate traffic is tunneled to the controller in the demilitarized zone (DMZ) and the rest of the corporate network. Traffic is encapsulated using GRE to preserve VLAN tags. The tunnel is trusted and shared by all Virtual Access Points (VAPs) and wired ports. Traffic between the RAP and the controller is encrypted by using IPsec. Local traffic is source NATed (to enet0 address) and forwarded on both the uplink and downlink wired interface ports according to the configured user role and session access control list (ACL).

Figure 15 *RAP Split Tunnel Mode Architecture*

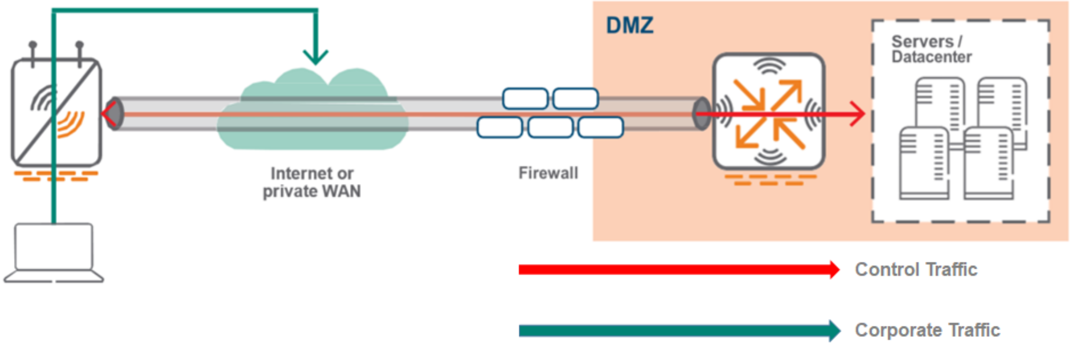


Bridge Mode

In Bridge mode, there is no access to corporate traffic. There is a user traffic bridge to the local network on the AP uplink. Traffic is not sent to the controller. User VLANs exist on the edge of the network and authenticated traffic is tunneled to the controller. Control Plane security (CPsec) is required. CPsec is a secure form (IPsec) of communication between the mobility controller and the RAP in order to protect the control plane communications. DHCP, Network Address Translation (NAT), and Port Address Translation (PAT) are provided either by the RAP or an external router.

Bridge mode is typically used so that non-corporate devices such as printers or family-owned devices can access the Internet directly by using the RAP uplink (similar to a home wireless router operation). This mode is not recommended for campus AP deployments as fewer features are supported in Bridge Mode.

Figure 16 *RAP Bridge Mode Architecture*



Secure Jack on Wired Ports

On any Aruba RAP that offers at least two Ethernet ports, the additional port can be configured for bridging or secure jack operation. This configuration provides maximum flexibility and allows for local wired access at remote sites. The additional Ethernet ports on a RAP can be configured for all the authentication types and forwarding modes available similar to a wireless service set identifier (SSID). A single SSID cannot be configured to provide 802.1X and MAC authentication simultaneously, however a wired port does not have the same limitation.

Just like the SSIDs, these ports are secured using the same authentication methods and servers while being configured to operate in various forwarding modes such as tunnel, split-tunnel, and bridge.

On any RAP, Eth 0 is always the uplink port. The remaining ports can be configured to provide the required functionality.

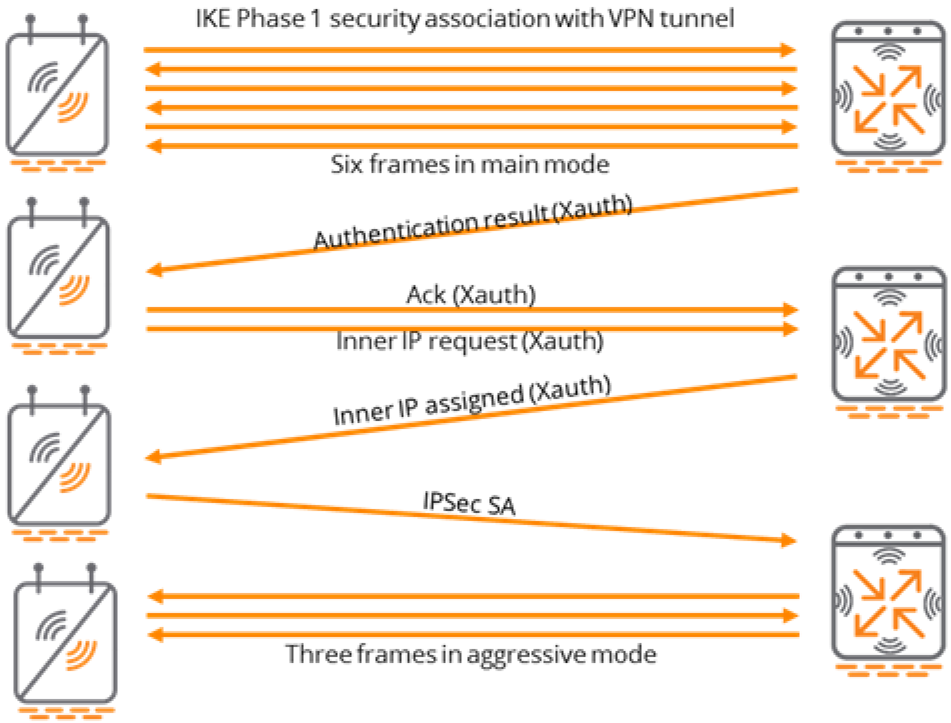
RAP Bootstrapping Process

RAP bootstrapping enables one or more IPsec encrypted GRE tunnels to be formed between the RAP and the designated controller depending on the configuration.

You must configure the VPN client settings on the RAP to instruct the RAP to use IPSec to connect to the controller. Provision the RAP and give it to users or enable remote users to provision the RAP. The method of provisioning is referred as Zero Touch Provisioning (ZTP).

You must provision the RAP before you install it at its remote location. To provision the RAP, the RAP must be physically connected to the local network or directly connected to the controller. When connected and powered on, the RAP must also be able to obtain an IP address from a DHCP server on the local network or from the controller.

Figure 17 *RAP Bootstrapping Process Call Flows*


IKE Phase 1 security association with VPN tunnel
Six frames in main mode
Authentication result (Xauth)
Ack (Xauth)
Inner IP request (Xauth)
Inner IP assigned (Xauth)
IPSec SA
Three frames in aggressive mode

The bootstrapping process is described in the following section:

1. The RAP first obtains an IP address on the wired interface (Eth 0) by using DHCP. In remote deployment scenarios, the IP address is typically provided by the Internet service provider (ISP) when it is directly connected to the Internet.
2. (optional) The RAP can also be provided a fully-qualified domain name (FQDN) or a static IP address of the Master Controller. If an FQDN is used, the RAP resolves the host name by using the DNS service provided by the ISP.
3. The RAP attempts to form an IPsec connection to the Master Controller through the Ethernet interface. Depending on the provisioning type, either the RAP's certificate or Internet Key Exchange (IKE) Pre-shared Key (PSK) is used to complete the phase 1 negotiation. XAuth (an extension to IKE phase 1) is used to authenticate the RAP.

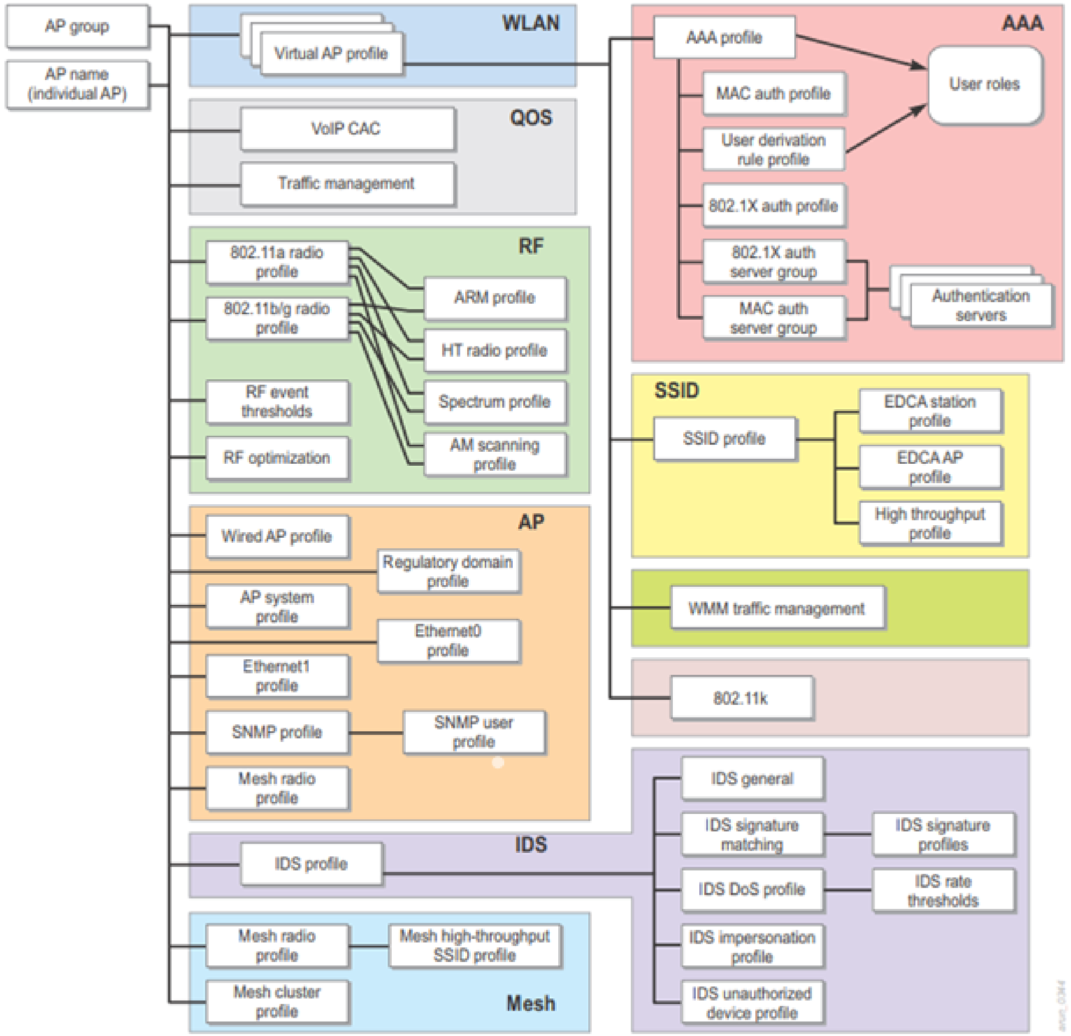
4. If IKE PSK is used, then XAuth authenticates the RAP with a username and password.
5. If a certificate is used, XAuth authenticates the MAC address in the certificate against the RAP whitelist.
6. An IPsec security association (SA) is then established between the RAP and the controller.
7. The Master Controller provides the RAP with the IP addresses of the controller (LMS and BLMS IP) where the RAP is terminated.
8. One or more IPsec encrypted GRE tunnels are formed between the RAP and the designated controller depending on the configuration.

Configuration Profile for RAPs

Configuration profiles allow different aspects of the Aruba WLAN deployment to be grouped into different configuration sets. Each profile is essentially a partial configuration. Some examples include SSID profiles, radio profiles, and AAA profiles. For more information about these configuration profiles, see the *Aruba 802.11ac Networks Validated Reference Design Guide* and *ArubaOS 8.6 User Guide*.

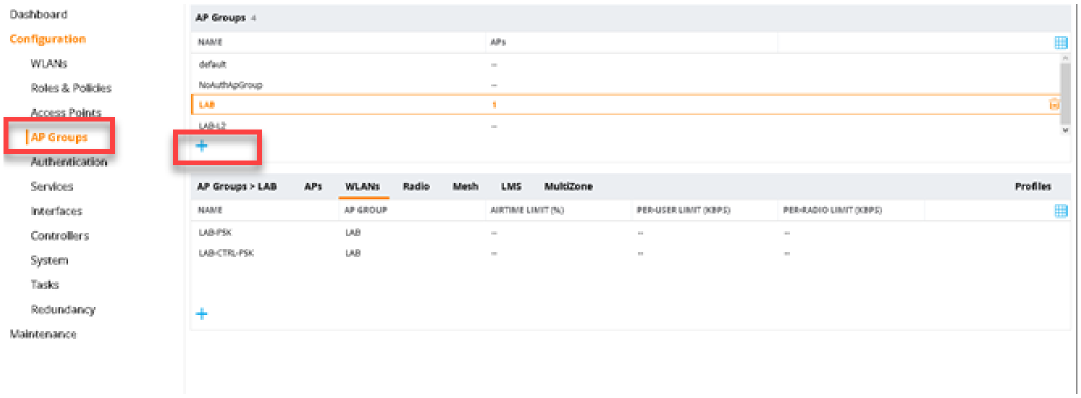
The following figure displays an overview of the profile structure and high-level overview of an AP group.

Figure 18 *High-Level Overview of an AP Group*



To create a dedicated RAP group, go to **Configuration** > **AP Groups** > and click the **+** sign.

Figure 19 *Creating a group of RAPs in ArubaOS 8.x*



AP Groups 4

NAME	APs
default	--
NoAuthApGroup	--
LAB	1
LAB-L2	--

NAME	AP GROUP	AIRTIME LIMIT (%)	PER-USER LIMIT (KBPS)	PER-RADIO LIMIT (KBPS)
LAB-PSK	LAB	--	--	--
LAB-CTRL-PSK	LAB	--	--	--

To create an AP group for RAPs, configure these roles and profiles.

- Firewall policies and user roles (required).
- SSID profiles (required)
- Server groups, AAA profiles (required)
- VAP profiles (required)
- Adaptive Radio Management (ARM) profile (optional, but recommended)
- 802.11a radio profile (required)
- 802.11g radio profile (required)
- AP system profile (required)
- Wired AP profile (required)
- Wired port profile (required)
- IDS profile (optional)

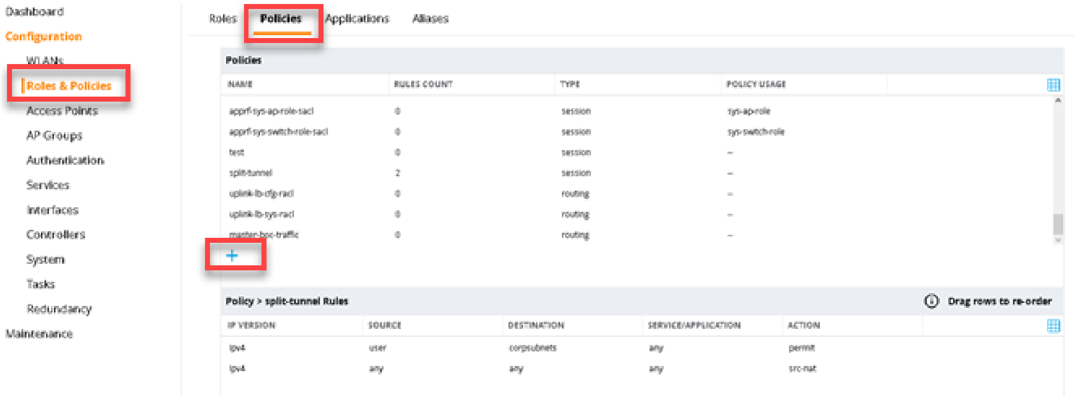
NOTE

The procedures for each of these steps are explained in the next section by using ArubaOS 8.x.

Firewall Polices and User Roles

To create a new policy, go to **Configuration** > **Roles & Policies** > **Policies** and click the **+** sign.

Figure 20 *Creating a New Policy in ArubaOS 8.x*



Policies

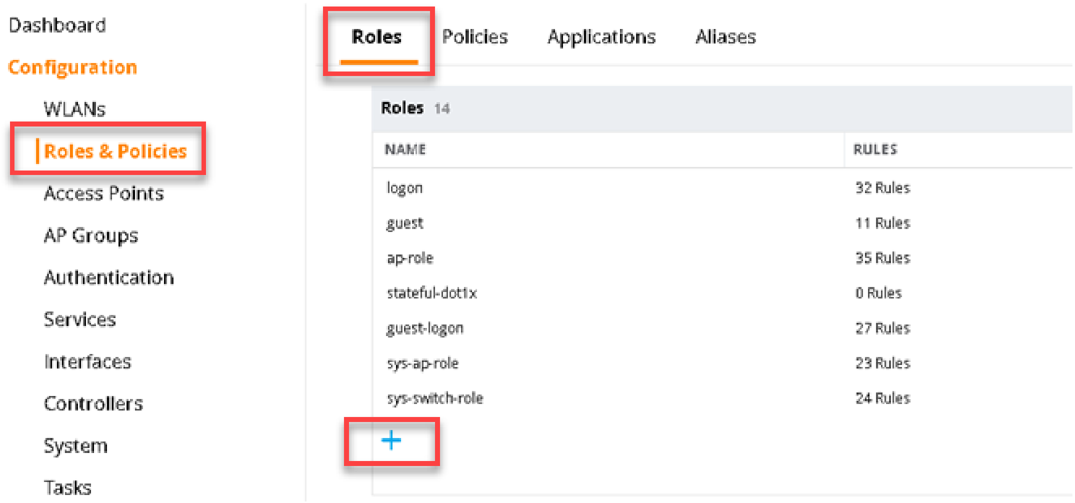
NAME	RULES COUNT	TYPE	POLICY USAGE
apprf-sys-ap-role-sacl	0	session	sys-ap-role
apprf-sys-switch-role-sacl	0	session	sys-switch-role
test	0	session	--
split-tunnel	2	session	--
uplink-lb-cfg-racl	0	routing	--
uplink-lb-sys-racl	0	routing	--
master-box-traffic	0	routing	--

Policy > split-tunnel Rules

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION
ipv4	user	corpsubnets	any	permit
ipv4	any	any	any	src-nat

To create a new user role, go to **Configuration** > **Roles & Policies** > **Roles** and click the **+** sign.

Figure 21 *Creating a New User Role in ArubaOS 8.x*

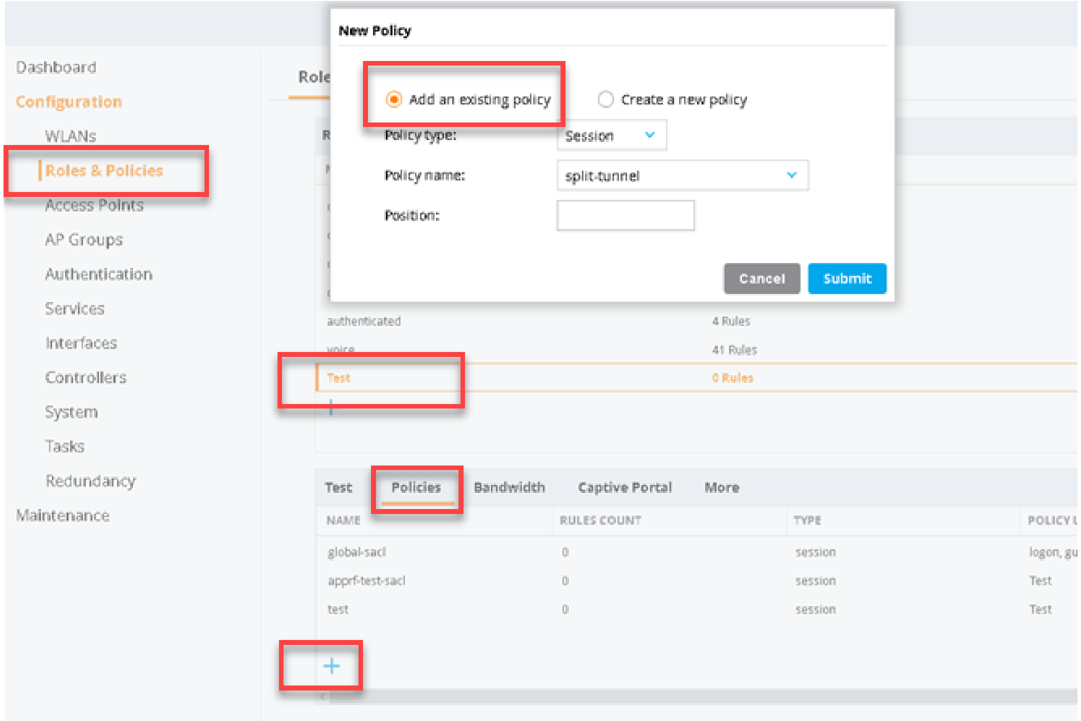


Roles 14

NAME	RULES
logon	32 Rules
guest	11 Rules
ap-role	35 Rules
stateful-dot1x	0 Rules
guest-logon	27 Rules
sys-ap-role	23 Rules
sys-switch-role	24 Rules

To assign the policy to the user role, go to **Configuration** > **Roles & Policies** > **Roles**. Select the role and click **Show Advanced View**. Click **Policies** and then click on the **+** sign.

Figure 22 *Applying a Policy to a User Role in ArubaOS 8.x*



New Policy

● Add an existing policy ○ Create a new policy

Policy type: Session

Policy name: split-tunnel

Position:

authenticated	4 Rules
voice	41 Rules
Test	0 Rules

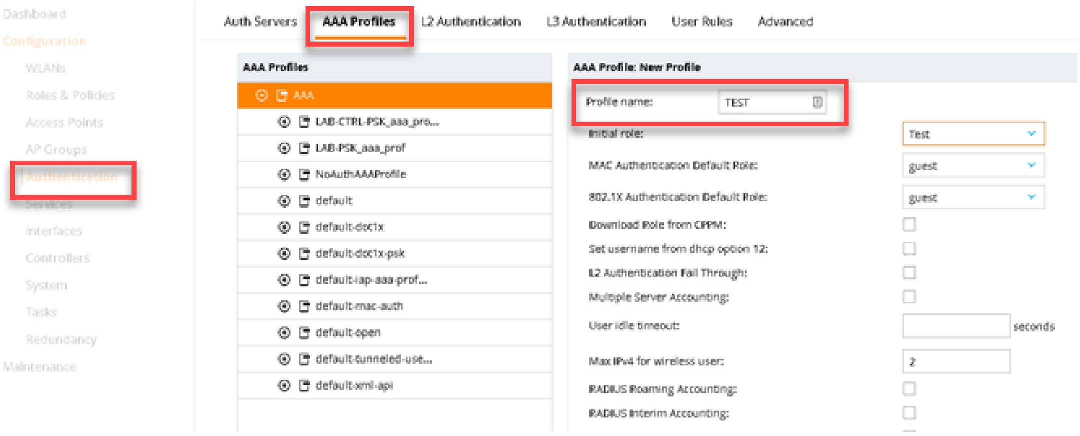
NAME	RULES COUNT	TYPE	POLICY U
global-sacl	0	session	logon, gu
apprf-test-sacl	0	session	Test
test	0	session	Test

For split tunneling, create a rule to send some traffic to your VPNC and keep the rest of the traffic local. Enter the subnets/IPs you want to send over the tunnel while configuring the firewall rule. The policy must then be applied to a user role.

AAA Profiles

To create an AAA profile, go to **Configuration** > **Authentication** > **AAA Profiles** and click on the **+** sign.

Figure 23 *Creating an AAA Profile in ArubaOS 8.x*



Profile name: TEST

Initial role: Test

MAC Authentication Default Role: guest

802.1X Authentication Default Role: guest

Download Role from CPPM: □

Set username from dhcp option 12: □

L2 Authentication Fail Through: □

Multiple Server Accounting: □

User idle timeout: seconds

Max IPv4 for wireless user: 2

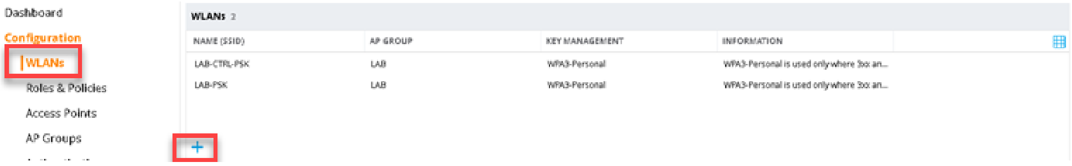
RADIUS Roaming Accounting: □

RADIUS Interim Accounting: □

WLAN SSID Profiles

To create an WLAN SSID profile, go to **Configuration** > **WLAN** and then click the **+** sign to follow the wizard. The mode of operation for RAPs is configured in the WLAN SSID profile.

Figure 24 *Create a WLAN Profile in ArubaOS 8.x*

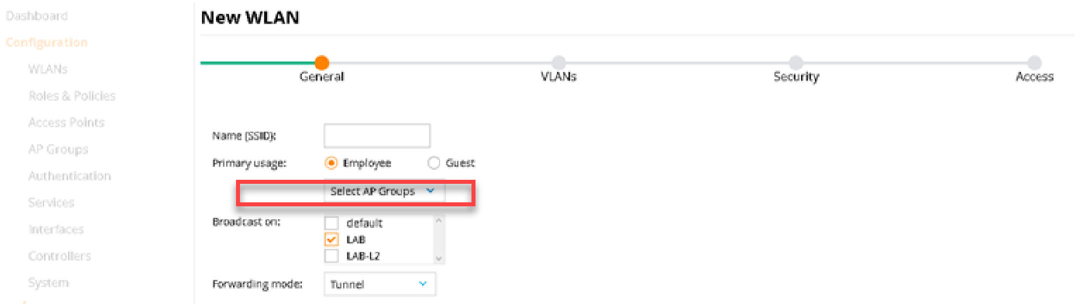


WLANs 2

NAME (SSID)	AP GROUP	KEY MANAGEMENT	INFORMATION
LAB-CTRL-PSK	LAB	WPA3-Personal	WPA3-Personal is used only where 3xx an...
LAB-PSK	LAB	WPA3-Personal	WPA3-Personal is used only where 3xx an...

You can either select an AP group or apply the WLAN profile to all AP groups.

Figure 25 *Apply the WLAN Profile to an AP Group in ArubaOS 8.x*



Name (SSID):

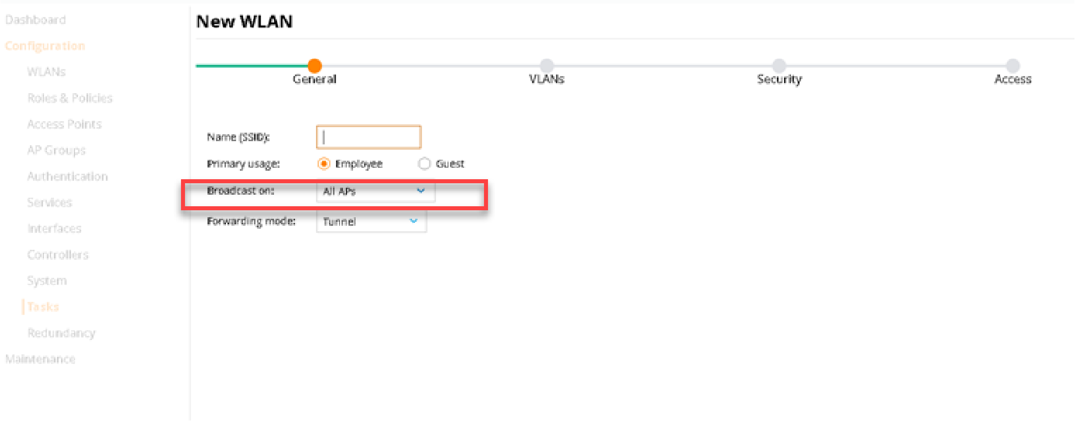
Primary usage: ● Employee ○ Guest

Select AP Groups

Broadcast on: □ default ☑ LAB □ LAB-L2

Forwarding mode: Tunnel

Figure 26 *Apply the WLAN Profile to All AP Groups in ArubaOS 8.x*



Name (SSID):

Primary usage: ● Employee ○ Guest

Broadcast on: All APs

Forwarding mode: Tunnel

Apply the new SSID profile to the RAP AP-group that you created.

See the *AOS 8 Fundamentals Guide* at https://community.arubanetworks.com/t5/Controller-Based-WLANs/ArubaOS-8-Fundamentals-Guide/ta-p/428914 to understand hierarchy and deployment best practices.

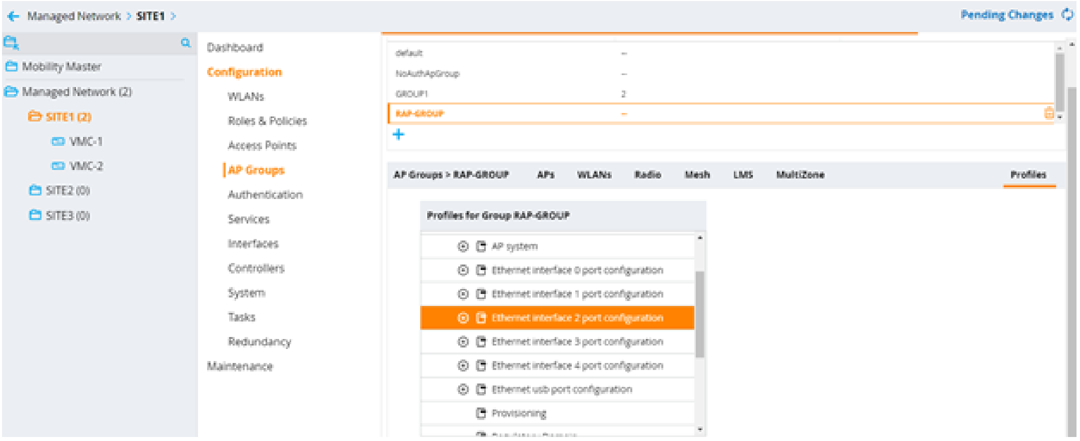
Configuration Profile for Wired Ports in a RAP

To configure a wired port on a RAP, create and apply an AP wired port profile to the required Ethernet port. The wired port profile is a container that holds other profiles, such as the wired AP profile and Ethernet interface link profile. The configuration of a wired port on a RAP requires these profiles:

- AP wired port profile—Enables or disables a port.
- Wired AP profile—Defines the switchport mode and the forwarding mode of a port.
- Ethernet interface link profile—Defines the speed and duplex values of a port.
- AAA profile—Defines the authentication types, authentication servers, and the default user role for authenticated user and unauthenticated users.

GUI Samples of Configuring Wired Ports in RAP in ArubaOS 8.x

Figure 27 *Configuring the Wired Port Profile in ArubaOS 8.x*

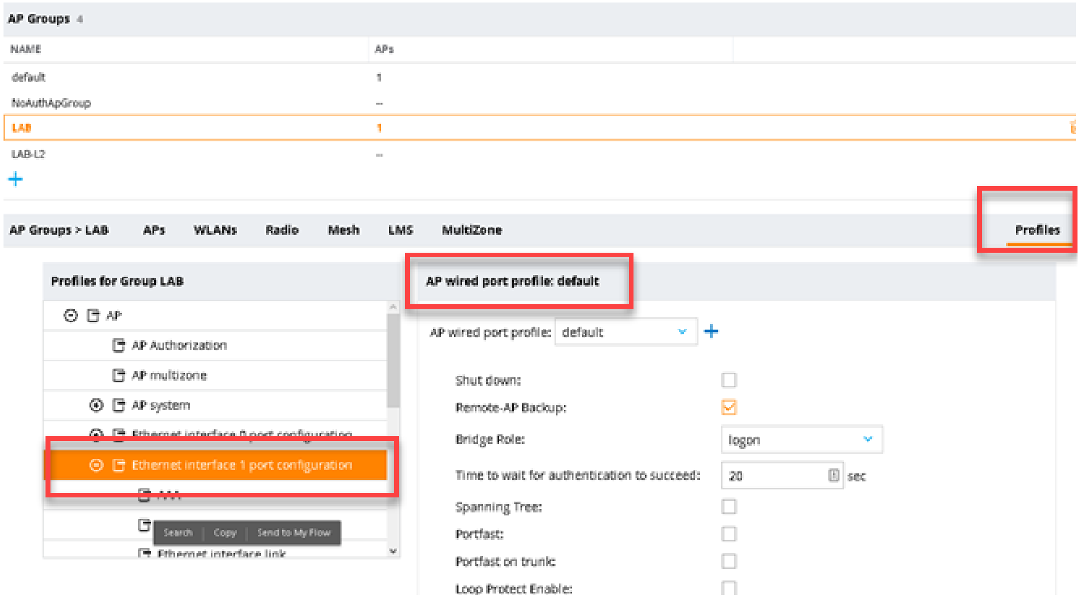


default	--
NoAuthApGroup	--
GROUP1	2
RAP-GROUP	--

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

Figure 28 *Configuring the Wired Port Profile Parameters in ArubaOS 8.x*



NAME	APs
default	1
NoAuthApGroup	--
LAB	1
LAB-L2	--

Profiles for Group LAB

- AP
  - AP Authorization
  - AP multizone
  - AP system
  - Ethernet interface 0 port configuration
  - Ethernet interface 1 port configuration
    - AAA
  - Ethernet interface link

AP wired port profile: default

AP wired port profile: default

Shut down: □

Remote-AP Backup: ☑

Bridge Role: logon

Time to wait for authentication to succeed: 20 sec

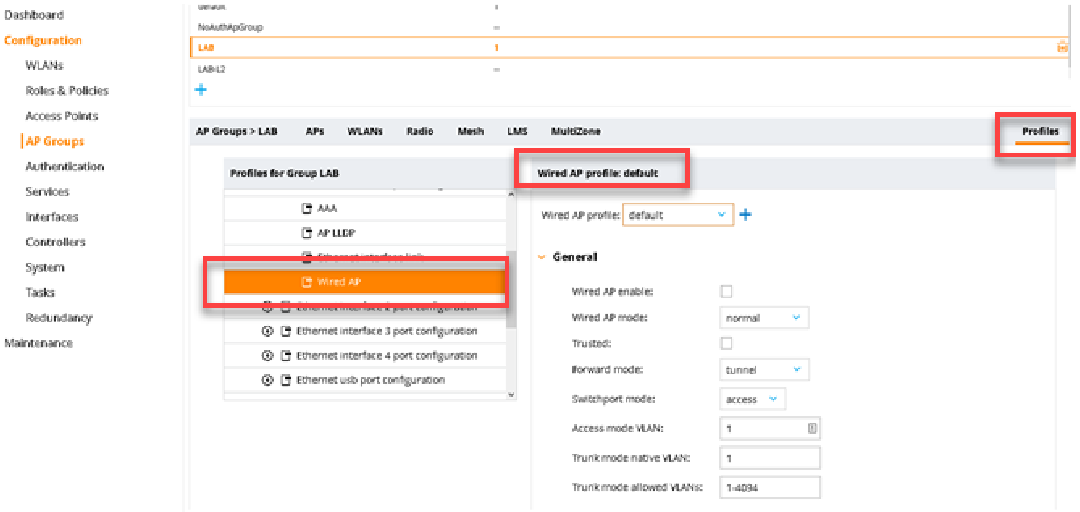
Spanning Tree: □

Portfast: □

Portfast on trunk: □

Loop Protect Enable: □

Figure 29 *Configuring the Wired AP Profile in ArubaOS 8.x*

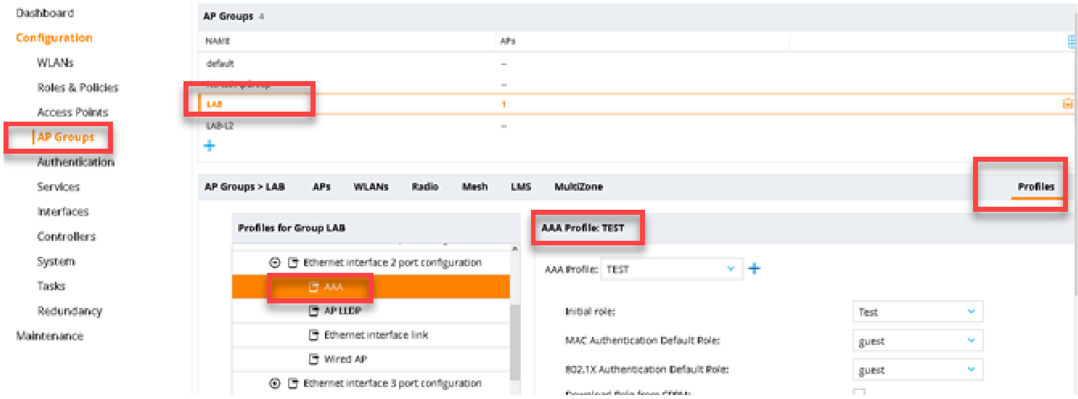


NoAuthApGroup	--
LAB	1
LAB-L2	--

Wired AP profile: default

Wired AP enable:	□
Wired AP mode:	normal
Trusted:	□
Forward mode:	tunnel
Switchport mode:	access
Access mode VLAN:	1
Trunk mode native VLAN:	1
Trunk mode allowed VLANs:	1-4094

Figure 30 *Configuring the AAA Profile in ArubaOS 8.x*



NAME	APs
default	--
	--
LAB	1
LAB-L2	--

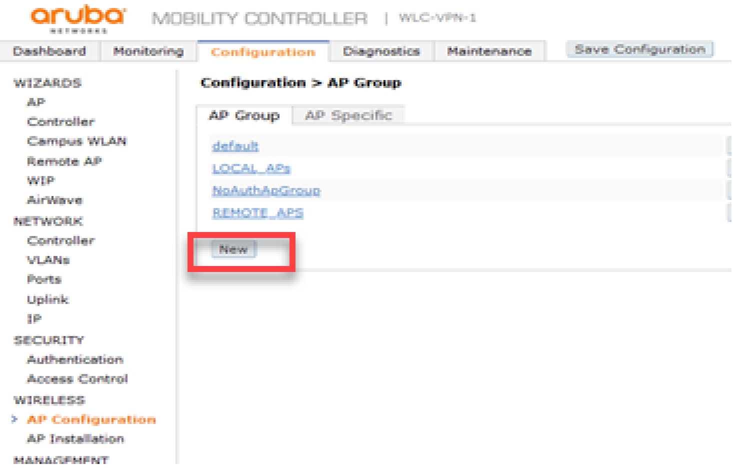
AAA Profile: TEST

Initial role:	Test
MAC Authentication Default Role:	guest
802.1X Authentication Default Role:	guest

GUI Samples of Configuring Wired Ports in RAP in ArubaOS 6.x

You must create a radio profile and a AAA profile for your Secure Jack configuration. You can refer to the ArubaOS 6.x deployment and user guides on what is required as well the best practices for creating these profiles. Some GUI samples are provided in this section.

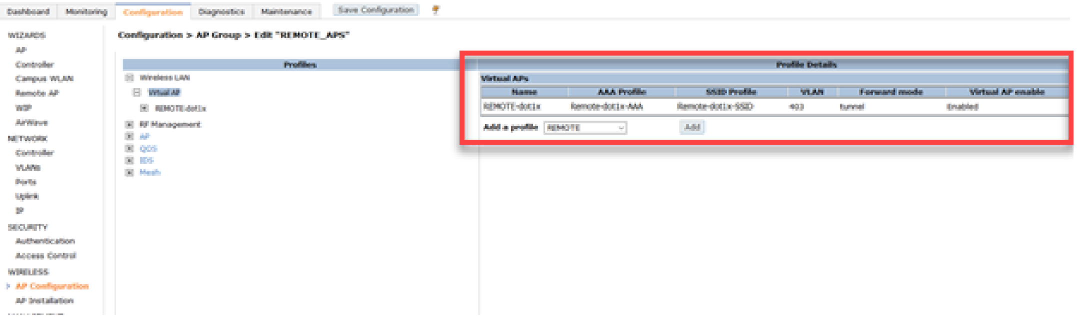
Figure 31 *Creating the RAP Group in ArubaOS 6.x*



Configuration > AP Group

- default
- LOCAL_APs
- NoAuthApGroup
- REMOTE_APS

Figure 32 *Adding the AAA Profile to a RAP Group in ArubaOS 6.x*



Configuration > AP Group > Edit "REMOTE_APS"

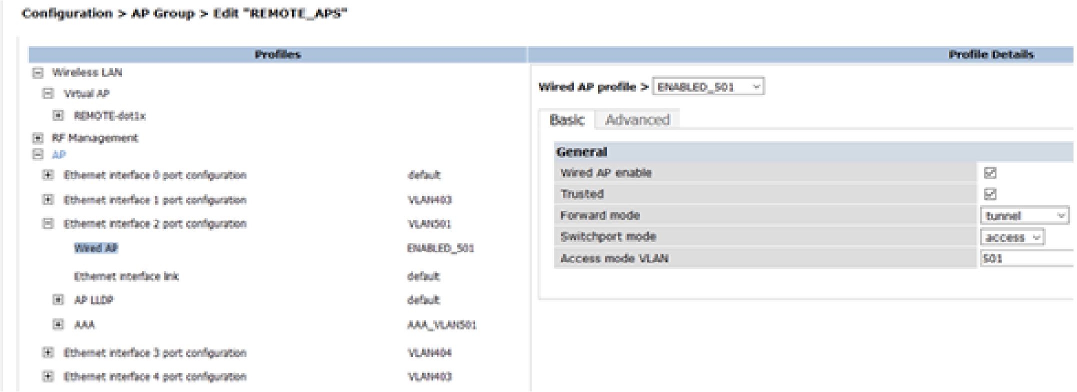
Profile Details

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

Figure 33 *Configuring the Wired AP Profile in ArubaOS 6.x*



Configuration > AP Group > Edit "REMOTE_APS"

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

General

Wired AP enable	☑
Trusted	☑
Forward mode	tunnel
Switchport mode	access
Access mode VLAN	501

Address Pool Considerations for RAPs

Every RAP and VIA client that authenticates successfully to the VPN server module of the controller is given a valid inner IP address and DNS server information. This inner IP address is issued from the address pool that is configured in the VPN server. More than one pool can be configured and you do not have to assign more addresses in the pool than the number of remote APs or VIA clients in the network. If only a single pool is configured, all the VPN clients (RAPs, VIA, and other third-party clients) are issued an inner IP address from the same pool. When multiple address pools are configured, the controller is configured to use distinct VPN pools for RAPs, VIA, and third-party VPN clients. This configuration can be achieved by appending a VPN pool to the role assigned to the RAPs, VIA and third-party VPN clients. When distinct VPN pools are not defined, the controller automatically uses the first pool in the VPN address pool. When this pool expires, the next pool in the list is used.

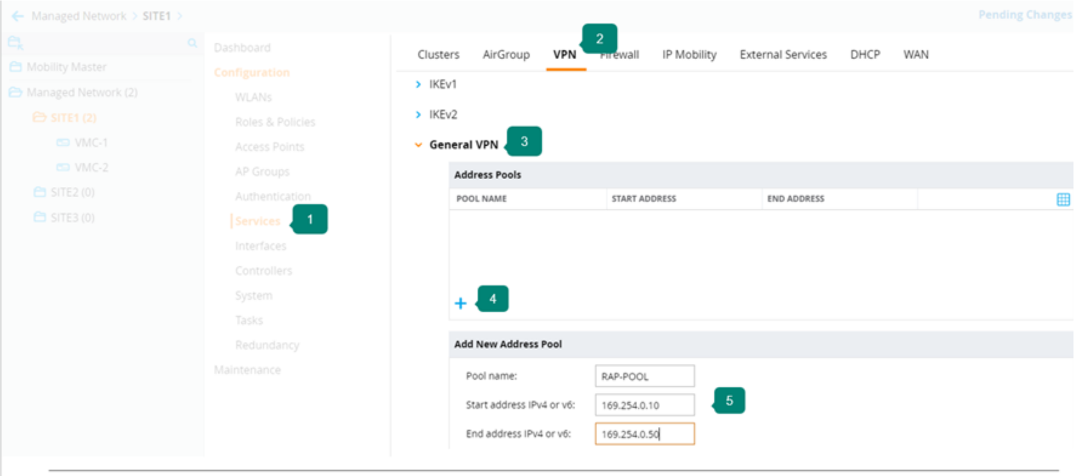
NOTE

If the VPN address pool is exhausted, new RAPs or VIA clients cannot establish the IPsec tunnel until the required number of IP addresses are added to the pool.

GUI Sample for VPN Address Pools in ArubaOS 8.x

In the Managed Network node hierarchy, navigate to **Configuration** > **Services** > **VPN**. Expand the **General VPN** accordion. Click + below the Address Pools table to create a new VPN address pool.

Figure 34 *Creating a VPN Address Pool in ArubaOS 8.x*



Pool name: RAP-POOL

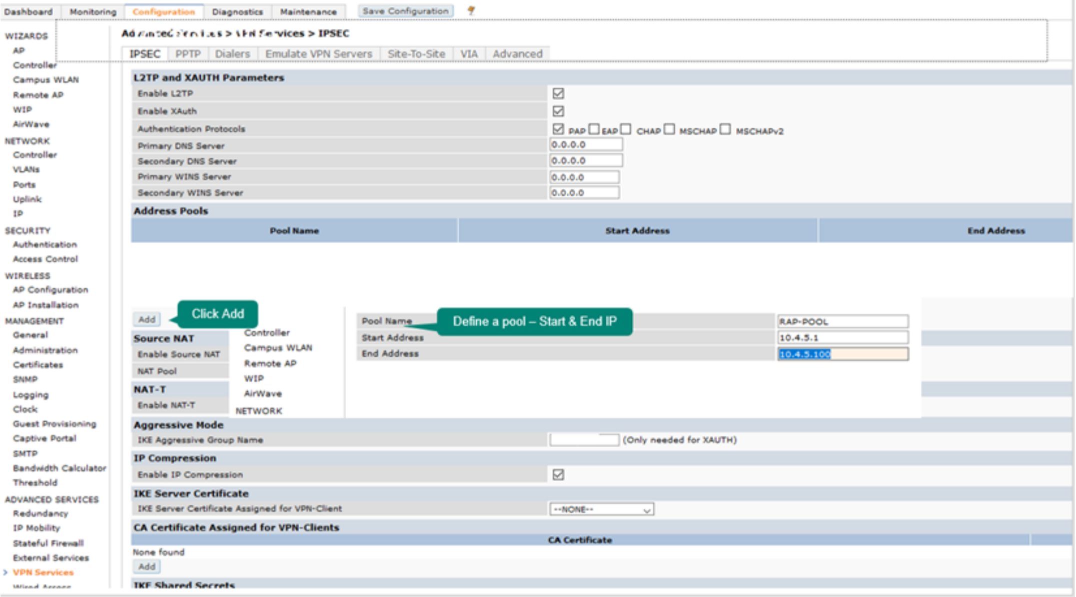
Start address IPv4 or v6: 169.254.0.10

End address IPv4 or v6: 169.254.0.50

GUI Sample for VPN Address Pools in ArubaOS 6.x

In the **Address Pools** section of the **IPSEC** tab, click **Add** to open the Add Address Pool page

Figure 35 *Creating a VPN Address Pool ArubaOS 6.x*



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

Pool Name	RAP-POOL
Start Address	10.4.5.1
End Address	10.4.5.100

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

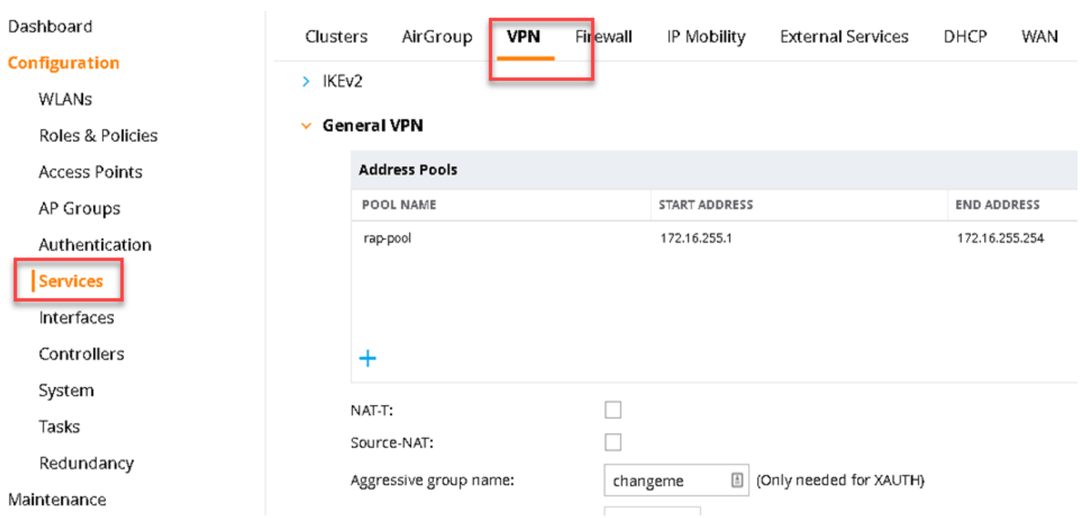
IKE Shared Secrets for RAPs

For VIA and RAPs that are pre-provisioned using PSK, a part of the IPsec process requires the VPN client to present a shared secret. Aruba enables you to configure keys that are specific to a subnet or you can specify a global key. To make the IKE key global, specify 0.0.0.0 for the subnet and subnet mask length fields. The previous image also displays the IKE shared secret key.

> NOTE
>
> For VIA using IKE version 1 with PSK and RAPs provisioned using PSK, the IKE shared secret must be configured for the IPsec tunnel to be established.

GUI Sample for VPN Server Configuration in ArubaOS 8.x

Figure 36 *Configuring Address Pools for VPN in ArubaOS 8.x*



Address Pools

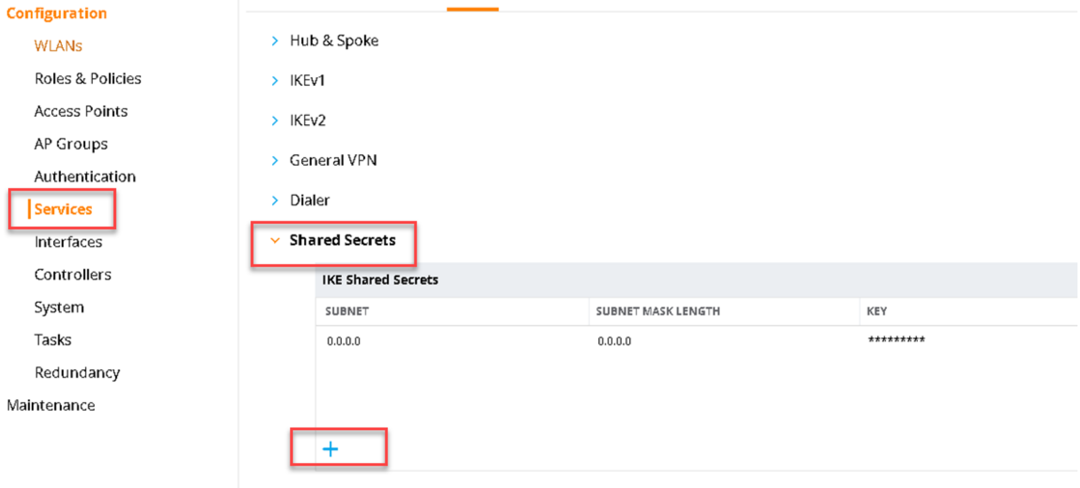
POOL NAME	START ADDRESS	END ADDRESS
rap-pool	172.16.255.1	172.16.255.254

NAT-T: □

Source-NAT: □

Aggressive group name: changeme (Only needed for XAUTH)

Figure 37 *Configuring IKE Shared Secrets in ArubaOS 8.x*



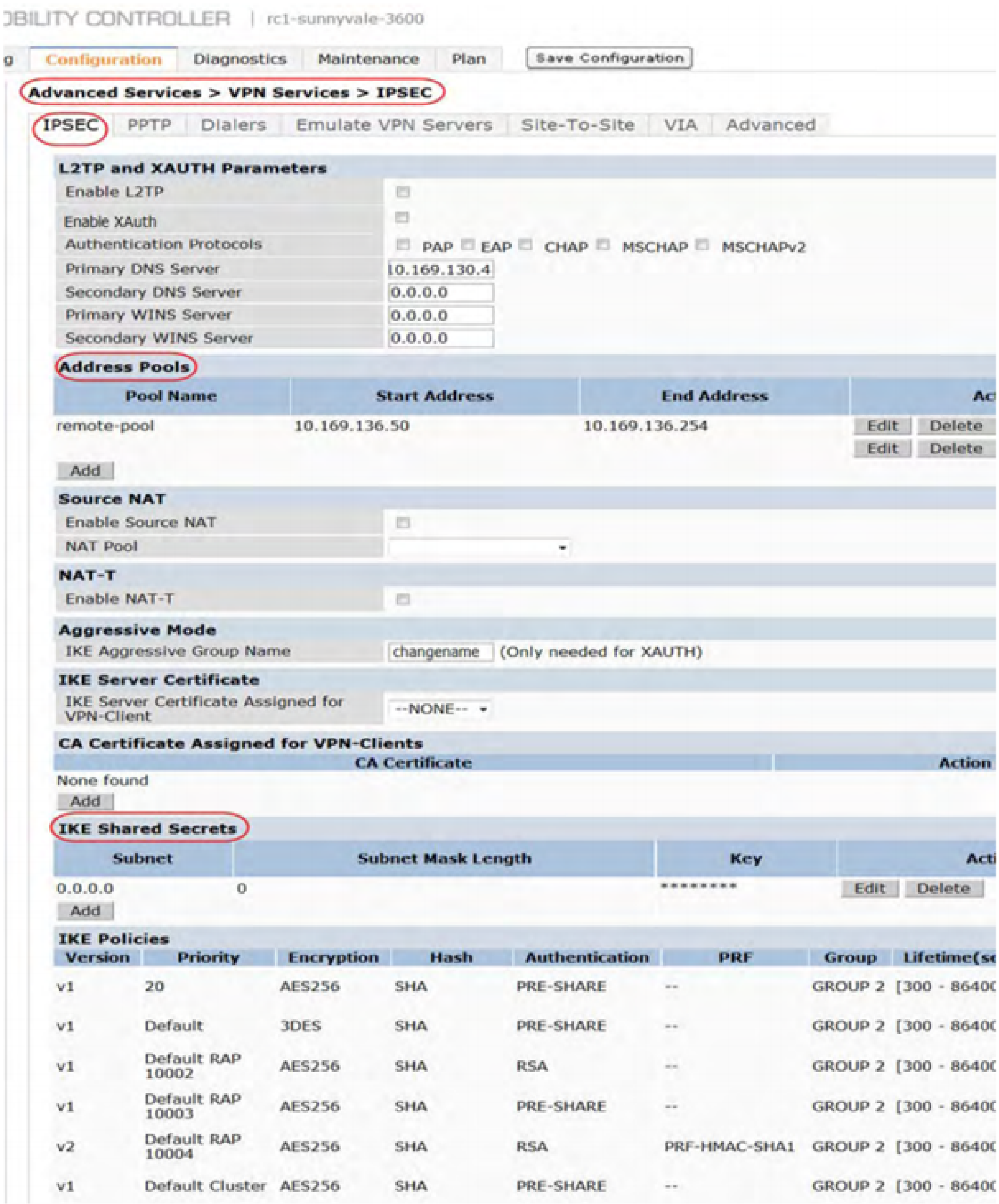
IKE Shared Secrets

SUBNET	SUBNET MASK LENGTH	KEY
0.0.0.0	0.0.0.0	*********

GUI Sample for VPN Server Configuration in ArubaOS 6.x

In the example network shown in the following figure, the remote-pool is used for the inner IP address of the RAPs. Also, the example network uses a global key. In the **IKE Shared Secrets** section of the **IPsec** tab, click **Add** to open the Add IKE Secret page.

Figure 38 *Sample VPN Server Configuration in ArubaOS 6.x*



Advanced Services > VPN Services > IPSEC

L2TP and XAUTH Parameters

Enable L2TP	☐
Enable XAuth	☐
Authentication Protocols	☐ PAP ☐ EAP ☐ CHAP ☐ MSCHAP ☐ MSCHAPv2
Primary DNS Server	10.169.130.4
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	Ac
remote-pool	10.169.136.50	10.169.136.254	Edit Delete
			Edit Delete

Add

Source NAT

Enable Source NAT	☐
NAT Pool	

NAT-T

Enable NAT-T	☐

Aggressive Mode

IKE Aggressive Group Name	changename (Only needed for XAUTH)

IKE Server Certificate

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

CA Certificate Assigned for VPN-Clients

CA Certificate	Action
None found	

Add

IKE Shared Secrets

Subnet	Subnet Mask Length	Key	Acti
0.0.0.0	0	********	Edit Delete

Add

IKE Policies

Version	Priority	Encryption	Hash	Authentication	PRF	Group	Lifetime(se
v1	20	AES256	SHA	PRE-SHARE	--	GROUP 2	[300 - 8640(
v1	Default	3DES	SHA	PRE-SHARE	--	GROUP 2	[300 - 8640(
v1	Default RAP 10002	AES256	SHA	RSA	--	GROUP 2	[300 - 8640(
v1	Default RAP 10003	AES256	SHA	PRE-SHARE	--	GROUP 2	[300 - 8640(
v2	Default RAP 10004	AES256	SHA	RSA	PRF-HMAC-SHA1	GROUP 2	[300 - 8640(
v1	Default Cluster	AES256	SHA	PRE-SHARE	--	GROUP 2	[300 - 8640(

Related Topics

[Understanding Remote AP Modes of Operation]

[Roles and Policies]

[Configuring WLANs]

[Remote Access Points]

Chapter 4
Converting AP to RAP

The following topics are discussed in this chapter:

- Component Required
- How to Convert Access Point to RAP
- Activate Rules for Instant AP or Unified AP

This chapter describes how to convert an Access Point (AP) to a Remote AP Access Point (RAP) and basic controller configuration to support a RAP-VPN solution. This chapter does not cover all deployment types or advanced design scenarios but provides an outline of the best solutions for scale and ease of deployment.

Aruba recommends to review the following documents to understand all deployment scenarios and options and how to setup teleworker solutions:

- ArubaOS 8 Fundamentals Guide
- Remote AP Validated Reference Design Guide
- Aruba VIA Validated Reference Design Guide

Component Required

This section lists the components require to convert AP to RAP.

Controller

A controller is mandatory to convert an AP to RAP.

Recommended Solution

Hardware controller models of 7000 Series or greater. For additional information, see Gateways and Controllers.

Optional Solution

Virtual controllers are not recommended without design consultation from a Certified Aruba integrator or sales team. Virtual controllers do not have a TPM and require resource reservations on the Hypervisor for reliable operation. Hardware controllers have greater scale and have TPM modules for RAP authentication. For additional information, see VMC Deployment Guide.

Licensing

This section lists the licenses required to convert an AP to a RAP.

- An AP license is mandatory for each RAP that is connected to a controller.
- A PEFNG (firewall license) is recommended.
- An RFProtect (WIPS/WIDS license) is optional.

License all devices equally. For example, 500 RAPs require 500 AP licenses, 500 RFProtect licenses, and 500 PEFNG licenses.

AP or RAP

A RAP can refer to either hardware or a deployment mode.

The RAP hardware is a desktop or a portable form factor that runs the same software as other access points. RAP mode can be used in all AP models and is a mode where the AP contacts a controller over an IPSec tunnel for a hardware VPN-style deployment.

Both RAP hardware and RAP mode support the teleworker solution from Aruba.

All AP models can be installed in RAP mode. Instant AP or unified AP models are easier to deploy because they support Zero Touch Provisioning (ZTP). A campus AP requires an extra provisioning step before it is sent to an end user.

Aruba Indoor Access Points

If an AP has a regulatory domain (IL, US, RW, JP) or has Instant AP (IAP) in the description, it can support ZTP. For example, Aruba IAP-305 (US) Instant 2x/3x 11ac AP is an Instant AP (IAP).

If an AP does not have a regulatory domain, it is a campus AP and must be staged before being deployed. For example, Aruba AP-305 Dual 2x2/3x3 802.11ac AP is a campus AP.

Activate Account

Aruba recommends the use of an Activate account and complete ZTP of the devices. There is no charge for Activate but it should be configured before ordering hardware. If the Activate account is configured after placing an order, the devices should be manually populated before ZTP. For additional information, see Activate.

How to Convert Access Point to RAP

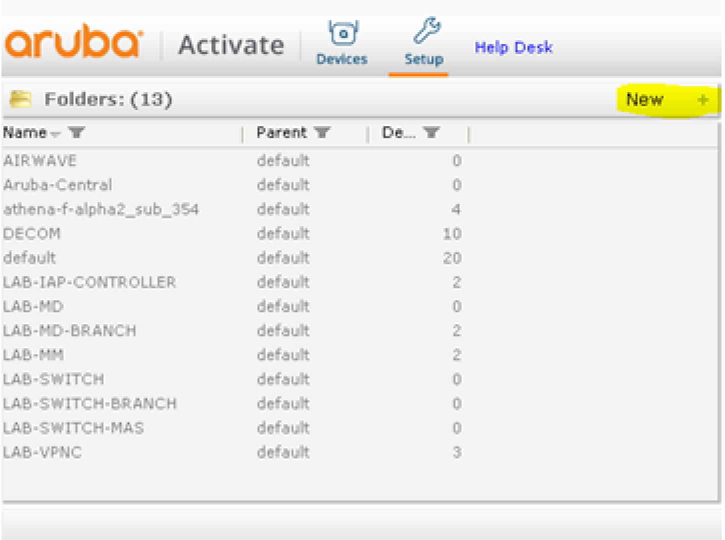
This section describes how to convert an AP to a RAP.

Activate Rules for Instant AP or Unified AP

Aruba Activate is ZTP enabled and is the recommended solution to quickly deploy several access points. Two rules are required for a simple deployment. A rule to move an AP into a group and a provisioning rule to direct the AP to a controller where the AP will terminate. Both Instant AP and unified AP models support Activate provisioning and Activate ZTP.

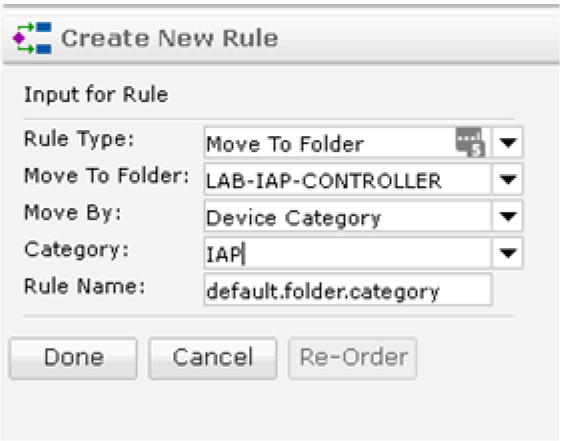
Campus access points do not support this method. See Campus AP Conversion.

1. To create Activate rules for Instant AP or unified AP:
2. Log in the WebUI of Activate.
3. Create a new folder in Aruba Activate.



Name	Parent	De...
AIRWAVE	default	0
Aruba-Central	default	0
athena-f-alpha2_sub_354	default	4
DECOM	default	10
default	default	20
LAB-IAP-CONTROLLER	default	2
LAB-MD	default	0
LAB-MD-BRANCH	default	2
LAB-MM	default	2
LAB-SWITCH	default	0
LAB-SWITCH-BRANCH	default	0
LAB-SWITCH-MAS	default	0
LAB-VPNC	default	3

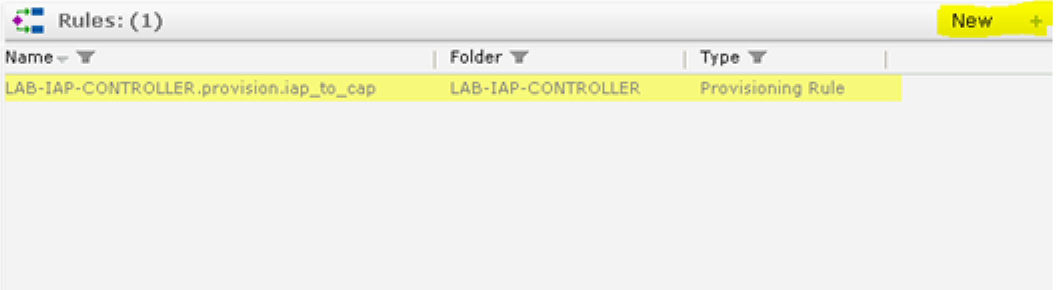
4. Create a rule to move the devices to the folder created in the previous step.



Input for Rule

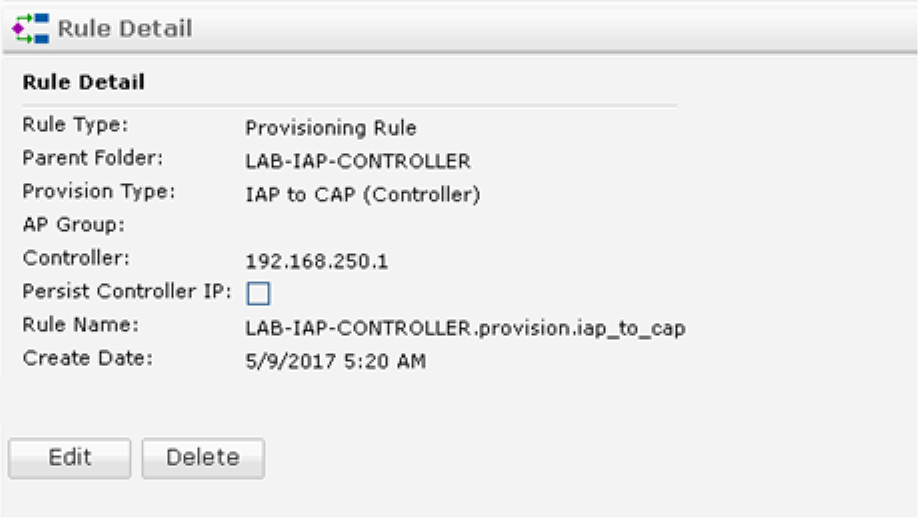
Rule Type: Move To Folder
Move To Folder: LAB-IAP-CONTROLLER
Move By: Device Category
Category: IAP
Rule Name: default.folder.category

5. Create a provisioning rule.



Name	Folder	Type
LAB-IAP-CONTROLLER.provision.iap_to_cap	LAB-IAP-CONTROLLER	Provisioning Rule

6. View the details of the provisioning rule.



Rule Detail

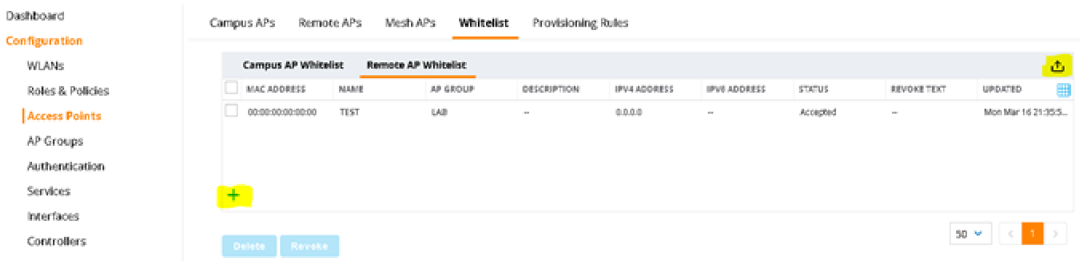
Rule Type: Provisioning Rule
Parent Folder: LAB-IAP-CONTROLLER
Provision Type: IAP to CAP (Controller)
AP Group:
Controller: 192.168.250.1
Persist Controller IP: □
Rule Name: LAB-IAP-CONTROLLER.provision.iap_to_cap
Create Date: 5/9/2017 5:20 AM

RAP Authentication

A RAP should be authenticated when connecting to a controller. Aruba recommends to use ClearPass Policy Manager to authorize a RAP. For additional information, see RAP Whitelist ASE Solution.

If you are using a Controller or Mobility master for whitelisting, then you must add entries manually, import as a CSV, or sync with Activate.

Figure 39 *RAP Whitelist*



□	MAC ADDRESS	NAME	AP GROUP	DESCRIPTION	IPV4 ADDRESS	IPV6 ADDRESS	STATUS	REVOKE TEXT	UPDATED
□	00:00:00:00:00:00	TEST	LAB	--	0.0.0.0	--	Accepted	--	Mon Mar 16 21:35:5...

Adding Entries Manually

To add entries manually:

1. Log in to the WebUI of the controller or Mobility Master.
2. Navigate to **Configuration > Access Points > Whitelist**.
3. Click **Remote AP Whitelist**.
4. Click **+**.
5. Add the entries.

Uploading CSV File

To upload a CSV file:

1. Log in to the WebUI of the controller or Mobility Master.
2. Navigate to **Configuration > Access Points > Whitelist**.
3. Click Remote AP Whitelist.
4. Click **Upload** at the top right of the **Remote AP Whitelist** table.
5. Navigate and select the CSV file.
6. Click **Upload**.

Synchronizing with Aruba Activate

To synchronize with Aruba Activate:

1. Log in to the CLI of the controller or Mobility Master.
2. Issue the following commands:

```
activate
whitelist-enable
username <activate username>
password <activate password>
device-interval 8
```

Campus AP Conversion

This section describes how to convert a campus AP to a RAP.

Recommended Method

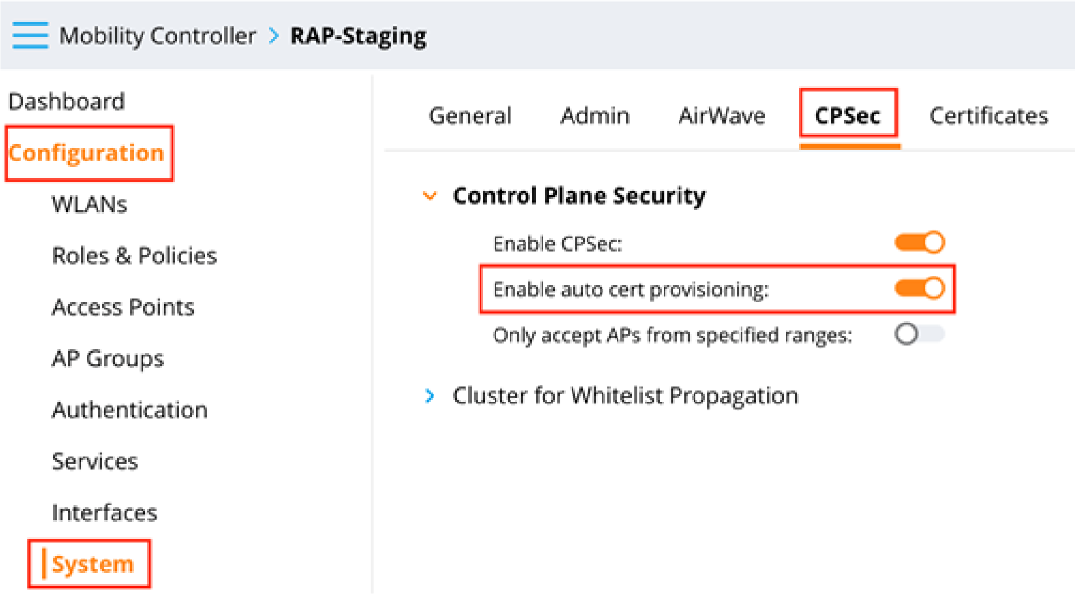
The preferred method to convert a campus AP to a RAP is to use a staging controller. This method targets campus access points with the following SKUs:

- AP-304 and AP-305
- AP-314 and AP-315
- AP-324 and AP-325
- AP-334 and AP-335

This method requires a VPN concentrator, that is a RAP head-end controller infrastructure like a managed device under a Mobility Master or a stand-alone Mobility Controller with the required AP licenses to simultaneously support the access points.

To convert a campus AP to a RAP through a staging controller:

1. Log in to the WebUI of the managed device or stand-alone Mobility Controller.
2. Navigate to **Configuration > System**.
3. Click **CPSec**.
4. Move the **Enable auto cert provisioning** slider to the right.



Enable CPSec: ●
Enable auto cert provisioning: ●
Only accept APs from specified ranges: ○

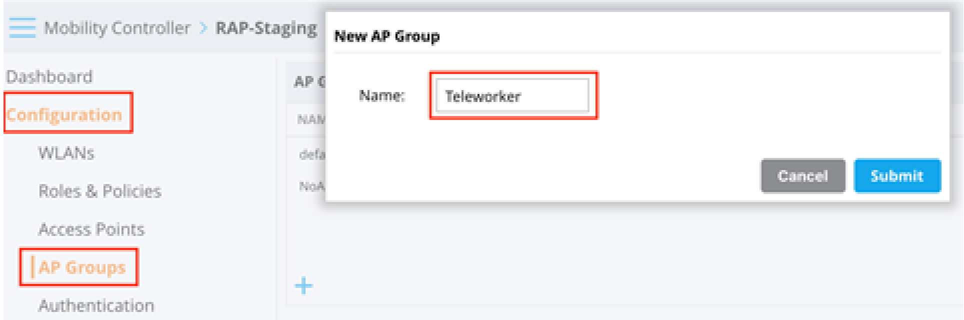
When a campus AP is connected to the network, it automatically initiates a master discovery using either one of the following methods:

- Aruba Discovery Protocol (ADP)
- DHCP options 43 and 60
- DNS

After a campus AP successfully discovers and connects to a Mobility Controller, it falls into the default group and is listed in the AP database list of either the Mobility Master or the stand-alone controller.

To create a RAP AP-group:

1. Log in to the WebUI of the managed device or stand-alone Mobility Controller.
2. Navigate to **Configuration > AP Groups**.
3. Click **+**.
4. Type a name for the RAP AP-group.

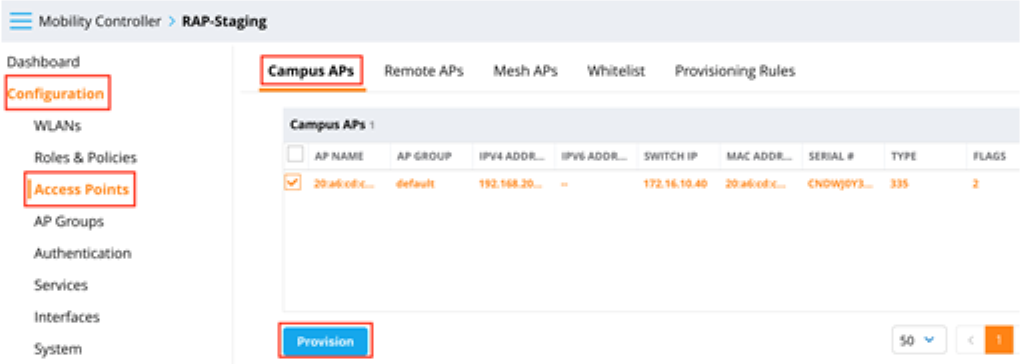


Name: Teleworker

5. Click **Submit**.

To provision an AP:

1. Log in to the WebUI of the managed device or stand-alone controller.
2. Navigate to **Configuration > Access Points**.
3. Click **Campus APs**.
4. Select the required access points.
5. Click **Provision**.

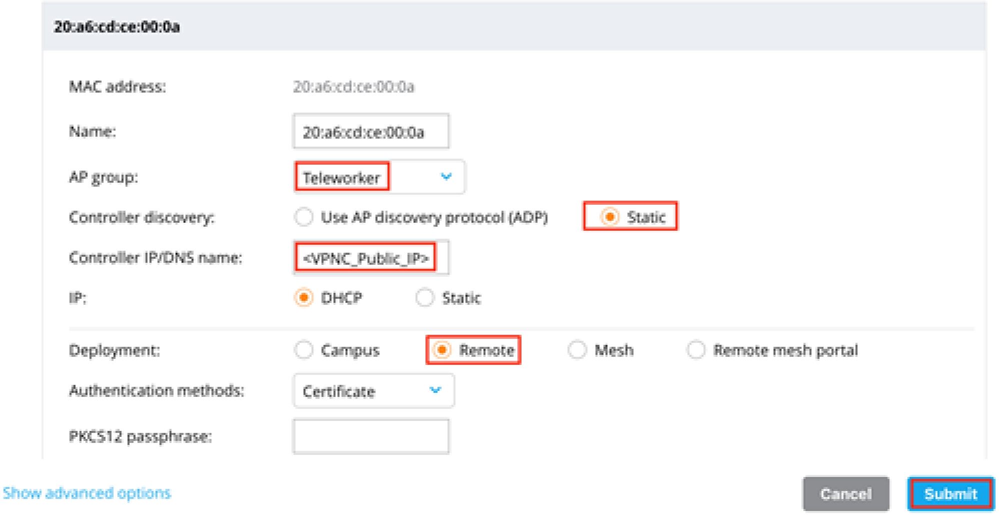


Campus APs 1

☐	AP NAME	AP GROUP	IPV4 ADDR...	IPV6 ADDR...	SWITCH IP	MAC ADDR...	SERIAL #	TYPE	FLAGS
☑	20:a6:cd:c...	default	192.168.20...	--	172.16.10.40	20:a6:cd:c...	CNDWJ0Y3...	335	2

To assign a controller to the RAP:

1. Log in to the WebUI of the managed device or stand-alone controller.
2. Navigate to **Configuration > Access Points**.
3. Click **Campus APs**.
4. Select the required access point.
5. Set **AP group** to name of the AP group.
6. Set **Controller discovery** to **Static**.
7. Set **Controller IP/DNS name** to the public IP address of the VPN concentrator.
8. Set **Deployment** to **Remote**.
9. Click **Submit**.



20:a6:cd:ce:00:0a

MAC address: 20:a6:cd:ce:00:0a

Name: 20:a6:cd:ce:00:0a

AP group: Teleworker

Controller discovery: ○ Use AP discovery protocol (ADP) ● Static

Controller IP/DNS name: <VPNC_Public_IP>

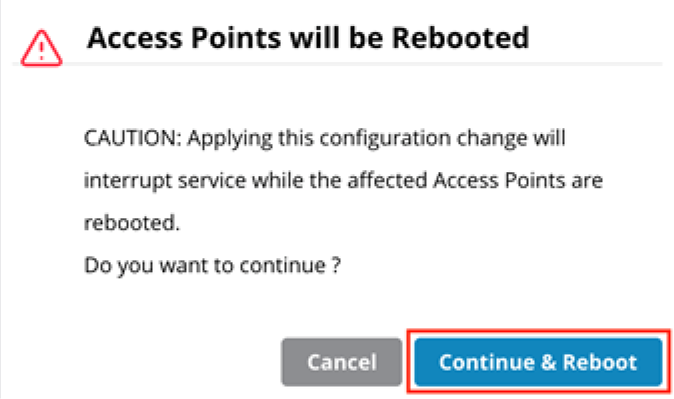
IP: ● DHCP ○ Static

Deployment: ○ Campus ● Remote ○ Mesh ○ Remote mesh portal

Authentication methods: Certificate

PKCS12 passphrase:

10. In the pop-up, click **Continue & Reboot**.



Access Points will be Rebooted

CAUTION: Applying this configuration change will interrupt service while the affected Access Points are rebooted.

Do you want to continue ?

Manual Method

Use the manual method to convert a campus AP to a RAP when a staging controller is not available. This method may also be used with smaller number of campus access points.

Prerequisites

- An appropriate console cable of an AP with adapter.
- A PoE switch to supply power to the AP or the power adapter of the AP.
- A terminal application like Putty.

To manually convert a campus AP to a RAP:

Boot the AP and monitor the console messages.

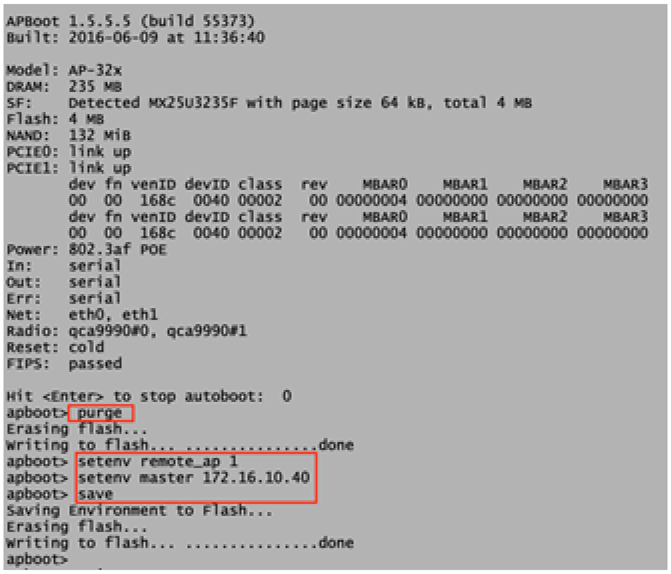
When the console displays Hit <Enter> to stop autoboot, press the Enter key, interrupt the AP boot, and allow the AP to remain at the apboot prompt.

Issue the following commands:

```
purge
setenv remote_ap 1
setenv master <VPNC_public_ip>
save
reboot
```

Following is sample AP console configuration.

Figure 40 *Sample AP Configuration*



```
APBoot 1.5.5.5 (build 55373)
Built: 2016-06-09 at 11:36:40

Model: AP-32x
DRAM:  235 MB
SF:    Detected MX25U3235F with page size 64 kB, total 4 MB
Flash: 4 MB
NAND:  132 MiB
PCIE0: link up
PCIE1: link up
       dev fn venID devID class  rev    MBAR0    MBAR1    MBAR2    MBAR3
       00  00  168c  0040 00002   00 00000004 00000000 00000000 00000000
       dev fn venID devID class  rev    MBAR0    MBAR1    MBAR2    MBAR3
       00  00  168c  0040 00002   00 00000004 00000000 00000000 00000000
Power: 802.3af POE
In:    serial
Out:   serial
Err:   serial
Net:   eth0, eth1
Radio: qca9990#0, qca9990#1
Reset: cold
FIPS:  passed

Hit <Enter> to stop autoboot:  0
apboot> purge
Erasing flash...
Writing to flash... ...............done
apboot> setenv remote_ap 1
apboot> setenv master 172.16.10.40
apboot> save
Saving Environment to Flash...
Erasing flash...
Writing to flash... ...............done
apboot>
```

NOTE

The RAP whitelist provides the AP-group and AP-name to the RAP.

Chapter 5
Related Documents

The following guides are part of the complete documentation for the Aruba user-centric network:

- ArubaOS 8 Fundamentals Guide
- Remote AP Validated Reference Design Guide
- ArubaOS 8.5.0.0 User Guide