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	Intr	oduction	.3
2	Hig	h Level Architecture	.3
3	Hig	h 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	5 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	5 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	Sun	nmary	23
7	Add	litional 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.

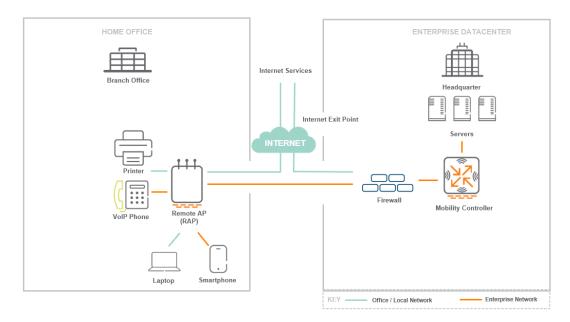


Figure 1: Aruba Remote Networking Solution - Home Office

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, <u>any Aruba AP</u> 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 <u>wireless networks & wired ports</u> 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 <u>zero</u> 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 <u>https://www.arubanetworks.com/assets/eo/EO_RemoteAccess.pdf</u>

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.

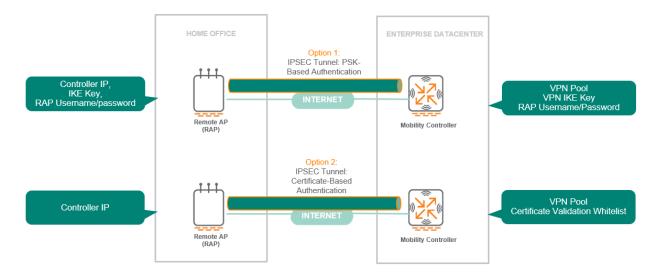
3.1 RAP needs to learn controller IP

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 certificatebased authentication which leverages the built-in signed certificates available in all Aruba APs. The Remote AP needs to reach the Mobility Controller on UDP Port 4500 (NAT-T). The mobility controller can have a public IP itself or port forwarding needs to be configured from 3rd party devices like firewalls to Mobility Controller on port 4500.



3.3 RAP needs to authenticate successfully

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

3.4 RAP needs to be assigned an IP address from controller

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

3.5 RAP needs to be configured in a group

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

4 AOS 6 – RAP Configuration (8 Steps)

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

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

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

Step 1: Connect the RAP to your network and let it join the controller like a regular CAP – Steps not shown here

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

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

ashboard Monitoring Configuration Diagnostics Mainten	nance Save Configuration				
ashboard Monitoring Configuration Diagnostics Mainten					
AP					
	rofiles			Profile Details	
Campus WLAN 📃 Wireless LAN		Virtual APs			
Remote AP 🕒 Virtual AP		Name AAA Profile REMOTE-dot1x Remote-dot1x-AAA		403 tunnel	ard mode Virtual AP er Enabled
WIP I REMOTE-dot1x AirWave I RF Management				405 Curiner	Enabled
ETWORK		Add a profile REMOTE ~	Add		
Controller QOS					
VLANs Mesh					
Ports					
Uplink IP					
ECURITY					
Authentication					
Access Control					
/IRELESS					
AP Configuration					
AP Installation					
e APs for wired connectivit	ty (Eth0 is used as	uplink so configu	ire other por	rts dependi	ng on AP
tep 4 (Optional): You can contend to the APs for wired connectivity to the total of the APs for wired control whe total of the total of total of the total of the total of total	ty (Eth0 is used as other wired traffic dged)	uplink so configu	ire other por	rts dependi	ng on AP
ne APs for wired connectivit nodel). You can control whe unneled, split-tunnel or bri	ty (Eth0 is used as other wired traffic dged)	uplink so configu	ire other por	rts dependi	ng on AP
ne APs for wired connectivit nodel). You can control whe unneled, split-tunnel or bri configuration > AP Group > Edit "REMOTE_	ty (Eth0 is used as other wired traffic dged)	uplink so configu is trusted or not	ire other por as well as the	rts dependi	ng on AP g mode
ne APs for wired connectivit nodel). You can control whe unneled, split-tunnel or brid configuration > AP Group > Edit "REMOTE_ Profiles	ty (Eth0 is used as other wired traffic dged)	uplink so configu	ire other por as well as the	rts dependi	ng on AP g mode
APs for wired connectivit odel). You can control whe unneled, split-tunnel or brid Configuration > AP Group > Edit "REMOTE_ Profiles	ty (Eth0 is used as other wired traffic dged)	uplink so configu is trusted or not	ire other por as well as the	rts dependi	ng on AP g mode
APs for wired connectivit odel). You can control whe unneled, split-tunnel or brid Configuration > AP Group > Edit "REMOTE_ Profiles Wireless LAN Wirtuel AP	ty (Eth0 is used as other wired traffic dged)	uplink so configu is trusted or not Wired AP profile > ENAE	ire other por as well as the	rts dependi	ng on AP g mode
e APs for wired connectivit odel). You can control whe unneled, split-tunnel or brid Configuration > AP Group > Edit "REMOTE_ Profiles Wireless LAN Virtual AP REMOTE-dot1x RF Management	ty (EthO is used as other wired traffic dged)	uplink so configu is trusted or not Wired AP profile > ENAE Basic Advanced	ire other por as well as the	rts dependi	ng on AP g mode
APs for wired connectivit addel). You can control whe unneled, split-tunnel or brid configuration > AP Group > Edit "REMOTE_ Profiles Urbual AP	ty (EthO is used as ether wired traffic dged) APS"	Wired AP profile > ENAE Basic Advanced General Wired AP enable Trusted	ire other por as well as the	rts dependi	ng on AP g mode
APs for wired connectivit addel). You can control whe unneled, split-tunnel or brid configuration > AP Group > Edit "REMOTE_ Profiles □ Virtual AP □ REMOTE-dot1x □ AP □ Ethernet interface 0 port configuration	ty (EthO is used as ether wired traffic dged) _APS"	Wired AP profile > ENABE Basic Advanced General Wired AP enable Trusted Forward mode	ire other por as well as the	rts dependi	Profile Details
APs for wired connectivit codel). You can control whe unneled, split-tunnel or brid configuration > AP Group > Edit "REMOTE_ Profiles	ty (EthO is used as ether wired traffic dged) _APS" default VLAN403	Wired AP profile > ENAE Basic Advanced General Wired AP enable Trusted	ire other por as well as the	rts dependi	ng on AP g mode
APs for wired connectivit addel). You can control whe unneled, split-tunnel or brid configuration > AP Group > Edit "REMOTE_ Profiles	default VLAN403 VLAN501	Wired AP profile > ENAE Basic Advanced General Wired AP enable Trusted Forward mode Switchport mode	ire other por as well as the	rts dependi	Profile Details
APS for wired connectivit codel). You can control whe unneled, split-tunnel or brid configuration > AP Group > Edit "REMOTE_ Profiles Wireless LAN Virtual AP REMOTE-dot1x RFM Anagement AP Ethemet interface 0 port configuration Ethemet interface 1 port configuration Ethemet interface 2 port configuration Ethemet interface 2 port configuration Wired AP	default vLAN403 vLAN501 ENABLED_501	Wired AP profile > ENAE Basic Advanced General Wired AP enable Trusted Forward mode Switchport mode	ire other por as well as the	rts dependi	Profile Details
APs for wired connectivit codel). You can control whe unneled, split-tunnel or brid configuration > AP Group > Edit "REMOTE_ Profiles	default VLAN403 VLAN501 ENABLED_501 default	Wired AP profile > ENAE Basic Advanced General Wired AP enable Trusted Forward mode Switchport mode	ire other por as well as the	rts dependi	Profile Details
e APs for wired connectivit odel). You can control whe unneled, split-tunnel or briv Configuration > AP Group > Edit "REMOTE_ Wireless LAN Virtual AP REMOTE-dot1x RF Management AP Ethemet interface 0 port configuration Ethemet interface 1 port configuration Ethemet interface 1 port configuration Wired AP Ethemet interface 1 port configuration	default VLAN403 VLAN501 ENABLED_501 default default default default default default	Wired AP profile > ENAE Basic Advanced General Wired AP enable Trusted Forward mode Switchport mode	ire other por as well as the	rts dependi	Profile Details

Step 4: Crea	ite a VPN Pool for RAPs – 1	This is the inner	IP that will be assigned	d for the RAPs.	It shouldn't
conflict with	n other IPs. It is not require	ed to be routabl	e.		
Dashboard Monitoring	Configuration Diagnostics Maintenance Save	Configuration 🦿			
WIZARDS	Ad ran ted Services > VEN Services > IPSEC				
AP	IPSEC PPTP Dialers Emulate VPN Servers	Site-To-Site VIA Advanced			
Controller	L2TP and XAUTH Parameters				
Campus WLAN Remote AP	Enable L2TP				
WIP	Enable XAuth				
AirWave	Authentication Protocols				
NETWORK	Primary DNS Server		0.0.0.0	·v2	
Controller	Secondary DNS Server		0.0.0.0		
VLANs Ports	Primary WINS Server		0.0.0.0		
Uplink	Secondary WINS Server		0.0.0.0		
IP	Address Pools				
SECURITY	Pool Name		Start Address		End Address
Authentication					
Access Control WIRELESS					
AP Configuration					
AP Installation					
MANAGEMENT		Name Define a pool – S	Start & End IP	RAP-POOL	
General	Source NAT Controller Start Campus WLAN	Address		10.4.5.1	
Administration Certificates	Enable Source NAT End A Remote AP	Address		10.4.5.100	
SNMP	NAT Pool WIP				
Logging	NAT-T AirWave				
Clock	Enable NAT-T NETWORK				
Guest Provisioning	Aggressive Mode				
Captive Portal SMTP	IKE Aggressive Group Name		(Only needed for XAUTH)		
Bandwidth Calculator	IP Compression		-		
Threshold	Enable IP Compression				
ADVANCED SERVICES	IKE Server Certificate IKE Server Certificate Assigned for VPN-Client		NONE ~		
Redundancy	CA Certificate Assigned for VPN-Clients		NONE V		
IP Mobility Stateful Firewall	CA Certificate Assigned for VPN-clients		CA Certificate		
External Services	None found				
> VPN Services	Add				
Wind Accord	IKE Shared Secrets				
Step 5: This	step is not required if the	AP was already	provisioned as CAP. H	owever, it is b	etter to
•		•	•		
whitelist the	e RAP by adding its MAC a	uuress and assig	gning it to the kemote	APS Group tha	it was
created in S	ten 1				
cicated in 5	ср 1.				

Dashboard Monitoring	Configuration Diagnostics	Maintenance Save Configura	ation 🕴 🕈				
WIZARDS AP Controller	Wireless > AP Installation > N Provisioning Provisioning P	2					
Campus WLAN	Whitelist Camp	us AP Remote AP	3				< <stat< th=""></stat<>
Remote AP WIP	Number of Entries: 3						Sea
AirWave	AP MAC Address	User Name	AP Group	AP Name	Description	Revoked	IP-Address
NETWORK Controller	00:0b:86		REMOTE_APS	155 ر			0.0.0.0
VLANs	00:05:80		REMOTE_APS				0.0.0.0
Ports	40:e3:d6i.		REMOTE_APS	AYMAN RAP 109			0.0.0.0
Uplink			Select 🗸				•
IP	Add Cancel						
SECURITY				1 1-3	of 3		
Authentication Access Control	4						
WIRELESS							
AP Configuration							
AP Installation 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

_		ssing Apply & Reboot. Option	, .	
	Configuration Diagnostics Maintenance Sav Wireless > AP Installation > Provision	z z		
	Provisioning Provisioning Profile Whitelist			
	AP Parameters	Colort Diabt Occur		
	AP Group	REMOTE_APS Select Right Group		
	AP Installation Mode			
	Default	O Indoor	00	utdoor
	Antenna Parameters			
	Antenna Selection Internal/Included Antenna	External Antenna		
	Authentication Method Remote AP 🕥	Yes O No Select Yes		
	Remote AP Authentication Method	O Pre-shared Key Certificate Select Ce	rtificate	
	PKCS12 Passphrase Representation Type	Text-based V		
	IKE PSK	Text-based V	Confirm IKE PSK	
	User credential assignment 💿			
	 Use Automatic Generation Global User Name/Password 	per AP User Name/Password		
	User Name	Generate		
	Password	Generate	Confirm Password	
	PPPoE Parameters			
	Service Name			
ng	User Name Password		Confirm Password	
	CHAP Secret		Confirm CHAP Secret	
lator	802.1x Parameters using PEAP			
	User Name Password		Confirm Password	
CES			Commin Password	
	O Use AP Discovery Protocol			
s	Use AP Discovery Protocol Master Controller IP Address/DNS name ③		TFTP Server (2)	
	Host Controller Name	aruba-master	Master Controller IP Address/DNS name ()	labvpn.
	Ŭ			
	IP Settings Uplink Vlan	0		
				 Specify Public IP or E(
ler p	public IP on UDP 4500	he network and connect to the the second s		
ler p s ne	connect the AP from t public IP on UDP 4500 etworks.	he network and connect to th		reach the
ler p s ne	connect the AP from t public IP on UDP 4500 etworks. Configuration Diagnostic Maintenance ?	he network and connect to th		reach the
ler p s ne	connect the AP from t public IP on UDP 4500 etworks.	he network and connect to th		reach the
ler p s ne	Connect the AP from t public IP on UDP 4500 etworks. Configuration Diagnostics Maintenance ? Controller > Access Points Search Results	he network and connect to th	AP and it will broadcast t	reach the
ler p s ne	Connect the AP from t public IP on UDP 4500 etworks. Configuration Diagnostics Maintenance ? Controller > Access Points Search Results	he network and connect to the . The AP will show up as RAP	AP and it will broadcast t	controller reach the the configure
ler p s ne	Configuration Diagnostics Maintenance ? Controller > Access Points Search Results Name AP Group AP IP Y	he network and connect to the . The AP will show up as RAP	AP and it will broadcast t	controller reach the the configure
ler p s ne	Configuration Diagnostics Maintenance * Configuration Diagnostics Maintenance * Configuration Configuration Diagnostics Maintenance * Controller > Access Points Search Results Name AP Group A AP IP * C AVMAN RAP 109 REMOTE_APS 1C 1 94	he network and connect to the . The AP will show up as RAP Outer AP II AP Type .bg Clients/Channel/ EIRP/HaxEIRP/Standard L2(36 RAP-109 1/1/920/n(20) 1 1-1 of 1 100	AP and it will broadcast t	controller reach the the configure
ler p s ne	Configuration Disgnatics Maintenance ? Configuration Disgnatics Maintenance ? Configuration Disgnatics Maintenance ? Configuration Disgnatics Maintenance ? Configuration Disgnatics Maintenance Configuration Search Results Configuration Disgnatics AP Group A AP ID Y Configuration Disgnatics Configuration Confi	he network and connect to the . The AP will show up as RAP Duter AP IP AP Type	AP and it will broadcast t a clients/Channel/EIRP/MaxEIRP/Standard 0/116+/18/23/n(40) Wired P ar D = Discom. Extra Calls On E = Wired AP enabled; F = AP fail the connected as standby: Y = Maintenance Mode; a = Reduce ARP P connected as standby: Y = Maintenance Mode; a = Reduce ARP	controller reach the the configure the configure the solution of the solution of the tot enable 3hi37m:225 d tot enable 3hi37m:225 d
ler p s ne	Configuration Disgnatics Maintenance ? Configuration Disgnatics Maintenance ? Configuration Disgnatics Maintenance ? Configuration Disgnatics Maintenance ? Configuration Disgnatics Maintenance Configuration Search Results Configuration Disgnatics AP Group A AP ID Y Configuration Disgnatics Configuration Confi	he network and connect to the . The AP will show up as RAP Outer AP IP AP Type .bg Clients/Channel/ EIRP/MaxEIRP/Standard L22 36 RAP-109 1/1/9/20/n(20) 1 1-1 of 1 10 erroin 2: A = Enet1 in active/standby mode: 8 = Battery Boot Oro; C = Callad Mathy N = Oro; C = Callad Mathy N = Oro; C = Callad	AP and it will broadcast t a clients/Channel/EIRP/MaxEIRP/Standard 0/116+/18/23/n(40) Wired P ar D = Discom. Extra Calls On E = Wired AP enabled; F = AP fail the connected as standby: Y = Maintenance Mode; a = Reduce ARP P connected as standby: Y = Maintenance Mode; a = Reduce ARP	controller reach the the configure the configure the solution of the solution of the tot enable 3hi37m:225 d tot enable 3hi37m:225 d
ler p s ne	Configuration Disgnatics Maintenance ? Configuration Disgnatics ? Configuration Disgnatics ? Con	he network and connect to the . The AP will show up as RAP Outer AP II AP Type .bg Clients/Channel/ EIRP/KlaxEIRP/Standard L2 36 RAP-109 J1/J9/20/n(20) 1 1-1 of 1 10 remion 2: A = Enet1 in active/standby mode; B = PBPDE; B = Remice AP. S = J -Cert RAP = Provisioned as Indoor; o = Provisioned as Outdoor; p = Ramit Channel followed by *** Indiates channel selected d	AP and it will broadcast t a cleats/channel/ EIRP/MaxEIRP/Standard Enet 1 0/116+/18/23/n(40) Wired P ar D = Discon. Extra Calls Cont E = Wired P bronnetted a standbyl X = Maintenance Modes a = AP fail to on unsported on POC-AFr = Boc111 E nabled (2 = DPB CAC timer ru us to onusported aconfigured channel.	controller reach the the configure the configure the configure fort enable 3hi37m:222 d tot enable 3hi
ler p s ne	Configuration Disgnatics Maintenance ? Configuration Disgnatics ? Configuration Disgnatics ? Con	he network and connect to the . The AP will show up as RAP Outer AP II AP Type .bg Clients/Channel/ EIRP/KlaxEIRP/Standard L2 36 RAP-109 J1/J9/20/n(20) 1 1-1 of 1 10 remion 2: A = Enet1 in active/standby mode; B = PBPDE; B = Remice AP. S = J -Cert RAP = Provisioned as Indoor; o = Provisioned as Outdoor; p = Ramit Channel followed by *** Indiates channel selected d	AP and it will broadcast t a cleats/channel/ EIRP/MaxEIRP/Standard Enet 1 0/116+/18/23/n(40) Wired P ar D = Discon. Extra Calls Cont E = Wired P bronnetted a standbyl X = Maintenance Modes a = AP fail to on unsported on POC-AFr = Boc111 E nabled (2 = DPB CAC timer ru us to onusported aconfigured channel.	controller reach the the configure the configure the configure fort enable 3hi37m:222 d tot enable 3hi
ler p s ne	Configuration Disgnatics Maintenance ? Configuration Disgnatics ? Configuration Disgnatics ? Con	he network and connect to the . The AP will show up as RAP Outer AP II AP Type .bg Clients/Channel/ EIRP/KlaxEIRP/Standard L2 36 RAP-109 J1/J9/20/n(20) 1 1-1 of 1 10 remion 2: A = Enet1 in active/standby mode; B = PBPDE; B = Remice AP. S = J -Cert RAP = Provisioned as Indoor; o = Provisioned as Outdoor; p = Ramit Channel followed by *** Indiates channel selected d	AP and it will broadcast t a cleats/channel/ EIRP/MaxEIRP/Standard Enet 1 0/116+/18/23/n(40) Wired P ar D = Discon. Extra Calls Cont E = Wired P bronnetted a standbyl X = Maintenance Modes a = AP fail to on unsported on POC-AFr = Boc111 E nabled (2 = DPB CAC timer ru us to onusported aconfigured channel.	controller reach the the configure the configure the configure fort enable 3hi37m:222 d tot enable 3hi
ler p s ne iitoring	Connect the AP from t public IP on UDP 4500 etworks. Configuration Diagnostics Maintenance ? Controller > Access Points Search Results Name AP Group AP IP C A YMAN RAP 109 REMOTE_APS IC 1 94 Flags 1 = 802.11X authenticated AP, 2 = Using INE v = 502.11X Enabled; L = Client Balancing Enabled; M Status Profile AP Activity	he network and connect to the . The AP will show up as RAP Outer AP II AP Type .bg Clients/Channel/ EIRP/KlaxEIRP/Standard L2 36 RAP-109 J1/J9/20/n(20) 1 1-1 of 1 10 remion 2: A = Enet1 in active/standby mode; B = PBPDE; B = Remice AP. S = J -Cert RAP = Provisioned as Indoor; o = Provisioned as Outdoor; p = Ramit Channel followed by *** Indiates channel selected d	AP and it will broadcast t a cleats/channel/ EIRP/MaxEIRP/Standard Enet 1 0/116+/18/23/n(40) Wired P ar D = Discon. Extra Calls Cont E = Wired P bronnetted a standbyl X = Maintenance Modes a = AP fail to on unsported on POC-AFr = Boc111 E nabled (2 = DPB CAC timer ru us to onusported aconfigured channel.	controller reach the the configure the configure the configure fort enable 3hi37m:222 d tot enable 3hi
ler p s ne	Connect the AP from t public IP on UDP 4500 etworks. Configuration Diagnostics Maintenance ? Controller > Access Points Search Results Name AP Group AP IP C A YMAN RAP 109 REMOTE_APS IC 1 94 Flags 1 = 802.11X authenticated AP, 2 = Using INE v = 502.11X Enabled; L = Client Balancing Enabled; M Status Profile AP Activity	he network and connect to the . The AP will show up as RAP Outer AP II AP Type .bg Clients/Channel/ EIRP/KlaxEIRP/Standard L2 36 RAP-109 J1/J9/20/n(20) 1 1-1 of 1 10 remion 2: A = Enet1 in active/standby mode; B = PBPDE; B = Remice AP. S = J -Cert RAP = Provisioned as Indoor; o = Provisioned as Outdoor; p = Ramit Channel followed by *** Indiates channel selected d	AP and it will broadcast t a cleats/channel/ EIRP/MaxEIRP/Standard Enet 1 0/116+/18/23/n(40) Wired P ar D = Discon. Extra Calls Cont E = Wired P bronnetted a standbyl X = Maintenance Modes a = AP fail to on unsported on POC-AFr = Boc111 E nabled (2 = DPB CAC timer ru us to onusported aconfigured channel.	controller reach the the configure the configure the configure fort enable 3hi37m:222 d tot enable 3hi
er p 5 ne itoring v v itoring	Connect the AP from t public IP on UDP 4500 etworks. Configuration Diagnostics Maintenance ? Controller > Access Points Search Results Name AP Group AP IP C A YMAN RAP 109 REMOTE_APS IC 1 94 Flags 1 = 802.11X authenticated AP, 2 = Using INE v = 502.11X Enabled; L = Client Balancing Enabled; M Status Profile AP Activity	he network and connect to the . The AP will show up as RAP Outer AP II AP Type .bg Clients/Channel/ EIRP/KlaxEIRP/Standard L2 36 RAP-109 J1/J9/20/n(20) 1 1-1 of 1 10 remion 2: A = Enet1 in active/standby mode; B = PBPDE; B = Remice AP. S = J -Cert RAP = Provisioned as Indoor; o = Provisioned as Outdoor; p = Ramit Channel followed by *** Indiates channel selected d	AP and it will broadcast t a cleats/channel/ EIRP/MaxEIRP/Standard Enet 1 0/116+/18/23/n(40) Wired P ar D = Discon. Extra Calls Cont E = Wired P bronnetted a standbyl X = Maintenance Modes a = AP fail to on unsported on POC-AFr = Boc111 E nabled (2 = DPB CAC timer ru us to onusported aconfigured channel.	controller reach the the configure the configure the configure fort enable 3hi37m:222 d tot enable 3hi
er p ne toring , ars	Connect the AP from t public IP on UDP 4500 etworks. Configuration Diagnostics Maintenance ? Controller > Access Points Search Results Name AP Group AP IP C A YMAN RAP 109 REMOTE_APS IC 1 94 Flags 1 = 802.11X authenticated AP, 2 = Using INE v = 502.11X Enabled; L = Client Balancing Enabled; M Status Profile AP Activity	he network and connect to the . The AP will show up as RAP Outer AP II AP Type .bg Clients/Channel/ EIRP/KlaxEIRP/Standard L2 36 RAP-109 J1/J9/20/n(20) 1 1-1 of 1 10 remion 2: A = Enet1 in active/standby mode; B = PBPDE; B = Remice AP. S = J -Cert RAP = Provisioned as Indoor; o = Provisioned as Outdoor; p = Ramit Channel followed by *** Indiates channel selected d	AP and it will broadcast t a cleats/channel/ EIRP/MaxEIRP/Standard Enet 1 0/116+/18/23/n(40) Wired P ar D = Discon. Extra Calls Cont E = Wired P bronnetted a standbyl X = Maintenance Modes a = AP fail to on unsported on POC-AFr = Boc111 E nabled (2 = DPB CAC timer ru us to onusported aconfigured channel.	controller reach the the configure the configure the configure fort enable 3hi37m:222 d tot enable 3hi
er p one original original original original	Connect the AP from t public IP on UDP 4500 etworks. Configuration Diagnostics Maintenance ? Controller > Access Points Search Results Name AP Group AP IP C A YMAN RAP 109 REMOTE_APS IC 1 94 Flags 1 = 802.11X authenticated AP, 2 = Using INE v = 502.11X Enabled; L = Client Balancing Enabled; M Status Profile AP Activity	he network and connect to the . The AP will show up as RAP Outer AP II AP Type .bg Clients/Channel/ EIRP/KlaxEIRP/Standard L2 36 RAP-109 J1/J9/20/n(20) 1 1-1 of 1 10 remion 2: A = Enet1 in active/standby mode; B = PBPDE; B = Remice AP. S = J -Cert RAP = Provisioned as Indoor; o = Provisioned as Outdoor; p = Ramit Channel followed by *** Indiates channel selected d	AP and it will broadcast t a cleats/channel/ EIRP/MaxEIRP/Standard Enet 1 0/116+/18/23/n(40) Wired P ar D = Discon. Extra Calls Cont E = Wired P bronnetted a standbyl X = Maintenance Modes a = AP fail to on unsported on POC-AFr = Boc111 E nabled (2 = DPB CAC timer ru us to onusported aconfigured channel.	controller reach the the configure the configure the configure fort enable 3hi37m:222 d tot enable 3hi
Y Y P Hers S Interface	Connect the AP from t public IP on UDP 4500 etworks. Configuration Diagnostics Maintenance ? Controller > Access Points Search Results Name AP Group AP IP C A YMAN RAP 109 REMOTE_APS IC 1 94 Flags 1 = 802.11X authenticated AP, 2 = Using INE v = 502.11X Enabled; L = Client Balancing Enabled; M Status Profile AP Activity	he network and connect to the . The AP will show up as RAP Outer AP II AP Type .bg Clients/Channel/ EIRP/KlaxEIRP/Standard L2 36 RAP-109 J1/J9/20/n(20) 1 1-1 of 1 10 remion 2: A = Enet1 in active/standby mode; B = PBPDE; B = Remice AP. S = J -Cert RAP = Provisioned as Indoor; o = Provisioned as Outdoor; p = Ramit Channel followed by *** Indiates channel selected d	AP and it will broadcast t a cleats/channel/ EIRP/MaxEIRP/Standard Enet 1 0/116+/18/23/n(40) Wired P ar D = Discon. Extra Calls Cont E = Wired P bronnetted a standbyl X = Maintenance Modes a = AP fail to on unsported on POC-AFr = Boc111 E nabled (2 = DPB CAC timer ru us to onusported aconfigured channel.	controller reach the the configure the configure the configure the configure the configure the configure protect a shi27m:52s of the south and the sir d = Drop Mean ning
ler p s ne aitoring 7' Illers s Interface Bus	Configuration Disgnostic Maintenance Configuration Disgnostic Maintenance Configuration Disgnostic Maintenance Configuration Controller > Access Points Search Results AP Group A P IP C AP Group A P IP C Controller > Access Points Search Results Custom Districe Profile AP Activity	he network and connect to th . The AP will show up as RAP Duter AP IP AP Type Jg Clients/Channel/EIRP/HaxEIRP/Standard L2 35 RAP-109 J1/J9/20/n(20) 1 1 - 1 of 1 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/st	AP and it will broadcast t 	controller reach the the configure the configure the configure the configure the configure protect a uptime 4 PF tot enable 3h:37m:52z d tot enable 3h:37m:52z d tot enable 3h:37m:52z d
ler p s ne aitoring 7' Illers s Interface Bus	Configuration Disgnostic Maintenance Configuration Disgnostic Maintenance Configuration Disgnostic Maintenance Configuration Controller > Access Points Search Results AP Group A P IP C AP Group A P IP C Controller > Access Points Search Results Custom Districe Profile AP Activity	he network and connect to the . The AP will show up as RAP Outer AP II AP Type .bg Clients/Channel/ EIRP/KlaxEIRP/Standard L2 36 RAP-109 J1/J9/20/n(20) 1 1-1 of 1 10 remion 2: A = Enet1 in active/standby mode; B = PBPDE; B = Remice AP. S = J -Cert RAP = Provisioned as Indoor; o = Provisioned as Outdoor; p = Ramit Channel followed by *** Indiates channel selected d	AP and it will broadcast t 	controllor reach the the configure the configure tot enable 3hi37m:22 d tot enable 3hi37m:22 d tot enable 3hi37m:22 d
er p s nee toring y y rers	connect the AP from t public IP on UDP 4500 etworks. Configuration Diagnostic Maintenance Configuration Diagnostic Maintenance Configuration Provided AP 19 Configuration	he network and connect to th . The AP will show up as RAP Duter AP IP AP Type Jg Clients/Channel/EIRP/HaxEIRP/Standard L2 35 RAP-109 J1/J9/20/n(20) 1 1 - 1 of 1 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/st	AP and it will broadcast t 	controllor reach the the configure the configure tot enable 3hi37m:22 d tot enable 3hi37m:22 d tot enable 3hi37m:22 d
er p ne coring	Configuration Disgnostic Maintenance Configuration Disgnostic Maintenance Configuration Disgnostic Maintenance Configuration Controller > Access Points Search Results AP Group A P IP C AP Group A P IP C Controller > Access Points Search Results Custom Districe Profile AP Activity	he network and connect to th . The AP will show up as RAP Duter AP IP AP Type Jg Clients/Channel/EIRP/HaxEIRP/Standard L2 35 RAP-109 J1/J9/20/n(20) 1 1 - 1 of 1 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/st	AP and it will broadcast t 	controllor reach the the configure the configure tot enable 3hi37m:22 d tot enable 3hi37m:22 d tot enable 3hi37m:22 d
er p 5 ne toring 7 ers Interface torts	Connect the AP from t public IP on UDP 4500 etworks. Configuration Diagnostic Maintenance ? Controller > Access Points Search Results Mame AP Group AP IP V C A YMAN RAP 109 REMOTE_APS IC I 94 Flags: 1 = 802: 1X authenticated AP; 2 = Using IFC W Status Profile AP Activity status Profile AP Activity	he network and connect to th . The AP will show up as RAP Duter AP IP AP Type Jg Clients/Channel/EIRP/HaxEIRP/Standard L2 35 RAP-109 J1/J9/20/n(20) 1 1 - 1 of 1 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/st	AP and it will broadcast t 	controllor reach the the configure the configure tot enable 3hi37m:22 d tot enable 3hi37m:22 d tot enable 3hi37m:22 d
ler p s ne itaring v lers s i Interface Bus Bus Ver	Connect the AP from t public IP on UDP 4500 Etworks. Configuration Diagnostic Maintenance * Controller > Access Points Search Results Name AP Group A AP IP * C * 400.11K Enabled L = Client Balances Enabled (A Plages 1 = 800.15K Enabled AP) 2 = Using IKE v Cuttom Status Profile AP Activity * *	he network and connect to th . The AP will show up as RAP Duter AP IP AP Type Jg Clients/Channel/EIRP/HaxEIRP/Standard L2 35 RAP-109 J1/J9/20/n(20) 1 1 - 1 of 1 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Battery for Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/standard sevender = Color Color C = 0 - Cert RAP: 1P Overland a statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/statice/st	AP and it will broadcast t 	controllor reach the the configure the configure tot enable 3hi37m:22 d tot enable 3hi37m:22 d tot enable 3hi37m:22 d
ler p s ne itaring v lers s i Interface Bus Bus Ver	Connect the AP from t public IP on UDP 4500 Etworks. Configuration Diagnostic Maintenance * Controller > Access Points Search Results AP Group A AP IP V C AP ACOVER Status Profile AP ACOVER Status Profile AP ACOVER Status Profile AP ACOVER Controller > Clients Search Results Clients Controller > Clients Search Results AP ACOVER Status Profile AP ACOVER Controller > Clients Search Results AP ACOVER Status Profile AP ACOVER Status Profile AP ACOVER Controller > Clients Controller > Clients AP ACOVER Controller AP AC	he network and connect to tl . The AP will show up as RAP Outer AP IP P Type . g Clients/Channel/ EIRP/HaxEIRP/Standard L2 36 . 36 AP-109 . 1/1/9/20/n(20) 1 + 1 + 0 + 1 1 + 1 + 0 + 1 1 + 1 + 0 + 1 Channel followed by "*" Indicates channel selected d Packet Capture Launch AirMagnet	AP and it will broadcast t a. clents/Channel/ ERP/MaxERP/Standard a. clents/Channel/ ERP/MaxERP/Standard ari D = Discone. Extra Calls On: E = Wiend P enabled; F = AP fall wired P ari D = Discone. Extra Calls On: E = Wiend P enabled; F = AP fall brometeria arised on the Switching D = Discone. Extra Calls On: E = Wiend P enabled; F = AP fall brometeria arised on the Switching Ping Overview USE Ethernet Switching e and VLAN.	controller reach the the configure interaction of the configure interaction of the configure interaction of the configure led 802.11K Report 802.11K Report 802.11K Report
er p s ne itoring y ers : Interface sus Ver	Connect the AP from t public IP on UDP 4500 etworks. Configuration Diagnostic Maintenance ? Controller > Access Points Search Results AP Group A P IP V A YMAN RAP 109 REMOTE_APS IC I 94 Flags 1 = 902.11X authenticated AP, 2 = Using IC V Status Profile AP, 2 = Using IC V Status	he network and connect to tl . The AP will show up as RAP Outer AP IP P Type . g Clents/Channel/EIRP/HaxEIRP/Standard L3: 36 . 36 RAP:109 . 1/J/2/20/(20) 1 + 1 of 10 Channel followed by ** Indicates channel selected d Packet Capture Launch AirMagnet	AP and it will broadcast t to cleats/Channel/ EIRP/MaxEIRP/Standard I cne 1 0/116+/18/23/n(40) Wired P wired P enabled: F = AP [a] brometed as anothy: X = Maintenane Mode: a = AP (a) wired P enabled: a Coll to Die E-Wired AP enabled: F = AP (a) wired P enabled: a Coll to Die E-Wired AP enabled: F = AP (a) to on unoported configured channel. Phy Overview USB Ethernet Switching brownetwer USB Ethernet Switching brownetwer USB Ethernet Switching at the AP Hame Phy Type Age at XMAI RAP 109 ED2.11; FT 3b(c) 7m(c)	controller reach the the configure the configuret th
ler p s ne aitoring 7' Illers s Interface Bus	Connect the AP from t public IP on UDP 4500 Etworks. Configuration Diagnostic Maintenance * Controller > Access Points Search Results AP Group A AP IP V C AP ACOVER Status Profile AP ACOVER Status Profile AP ACOVER Status Profile AP ACOVER Controller > Clients Search Results Clients Controller > Clients Search Results AP ACOVER Status Profile AP ACOVER Controller > Clients Search Results AP ACOVER Status Profile AP ACOVER Status Profile AP ACOVER Controller > Clients Controller > Clients AP ACOVER Controller AP AC	he network and connect to the . . The AP will show up as RAP Outer AP II AP type	AP and it will broadcast t a cleats/Channel/EIRP/MaxEIRP/Standard Lent 1 0/116+/18/23/n(40) Wired P wired P	controller reach the the configure IPSEC Uptime 4 PF ort enable 3h:37m:52z d Bo2:11K Report B02:11K Report B02:11K Report
ler p s ne s ne ithering liers s Interface Bus Bus Ver	Connect the AP from t public IP on UDP 4500 Etworks. Configuration Diagnostic Maintenance * Controller > Access Points Search Results AP Group A AP IP V C AP ACOVER Status Profile AP ACOVER Status Profile AP ACOVER Status Profile AP ACOVER Controller > Clients Search Results Clients Controller > Clients Search Results AP ACOVER Status Profile AP ACOVER Controller > Clients Search Results AP ACOVER Status Profile AP ACOVER Status Profile AP ACOVER Controller > Clients Controller > Clients AP ACOVER Controller AP AC	he network and connect to the . . The AP will show up as RAP Outer AP II AP type	AP and it will broadcast t a cleats/Channel/EIRP/MaxEIRP/Standard Lent 1 0/116+/18/23/n(40) Wired P wired P	controller reach the the configure interaction of the configure interaction of the configure interaction of the configure led 802.11K Report B02.11K Report
ler p s ne s ne ithering liers s Interface Bus Bus Ver	Connect the AP from t public IP on UDP 4500 Etworks. Configuration Diagnostic Maintenance * Controller > Access Points Search Results AP Group A AP IP V C AP ACOVER Status Profile AP ACOVER Status Profile AP ACOVER Status Profile AP ACOVER Controller > Clients Search Results Clients Controller > Clients Search Results AP ACOVER Status Profile AP ACOVER Controller > Clients Search Results AP ACOVER Status Profile AP ACOVER Status Profile AP ACOVER Controller > Clients Controller > Clients AP ACOVER Controller AP AC	he network and connect to the . . The AP will show up as RAP Outer AP II AP type	AP and it will broadcast t a cleats/Channel/EIRP/MaxEIRP/Standard Lent 1 0/116+/18/23/n(40) Wired P wired P	controller reach the the configure IPSEC Uptime 4 PF ort enable 3h:37m:52z d Bo2:11K Report B02:11K Report B02:11K Report
er p s ne itoring y ers : Interface sus Ver	Connect the AP from t public IP on UDP 4500 Etworks. Configuration Diagnostic Maintenance * Controller > Access Points Search Results AP Group A AP IP V C AP ACOVER Status Profile AP ACOVER Status Profile AP ACOVER Status Profile AP ACOVER Controller > Clients Search Results Clients Controller > Clients Search Results AP ACOVER Status Profile AP ACOVER Controller > Clients Search Results AP ACOVER Status Profile AP ACOVER Status Profile AP ACOVER Controller > Clients Controller > Clients AP ACOVER Controller AP AC	he network and connect to the . . The AP will show up as RAP Outer AP II AP type	AP and it will broadcast t a cleats/Channel/EIRP/MaxEIRP/Standard Lent 1 0/116+/18/23/n(40) Wired P wired P	controller reach the the configure IPSEC Uptime 4 PF ort enable 3h:37m:52z d Bo2:11K Report B02:11K Report B02:11K 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.

cenario 2– Converting an IAP to RAP
tep 1: Staging is not needed so this step is skipped
tep 2: Create a group for Remote APs (Recommended)
MOBILITY CONTROLLER WLC-VPN-1
Dashboard Monitoring Configuration Diagnostics Maintenance Save Configuration
WIZARDS Configuration > AP Group AP AP Group AP Specific Campus WLAN default Remote AP LOCAL_APs WIP NoAuthApGroup AirWave REMOTE_APS Controller NETWORK Controller New VLANs New Ports New Uplink IP SECURITY Authentication Access Control WIRELESS > AP Configuration AP Configuration MANAGEMENT NANAGEMENT
tep 3: Configure the Remote APs Group like a Campus Group (Add the necessary VAP, Wireless SIDs, AAA profilesetc.) You can use existing profiles or create new profiles as per your equirements.
ashboard Monitoring Configuration Diagnostics Maintenance Save Configuration ?
VIZARDS Configuration > AP Group > Edit "REMOTE_APS" AP Controller Profiles Profile Details
Campus WLAN def Virtual AP Remote AP def Virtual AP Remote AP def Virtual AP
NUP RENOTE-dottx Remote-dottx-AAA Remote-dottx-SSID 4.03 tunnel Enabled AIWave III PF Management Add a profile Remote-dottx-AAA Remote-dottx-SSID 4.03 tunnel Enabled ETWORK III PF Add a profile REMOTE Add Add Add Tunnel Enabled Controller III OS III OS IIII OS IIII OS IIIII OS IIIII OS IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
Access Control VIRELESS AP Configuration AP Installation
tep 4 (Optional): You can configure wired port profiles here in case you want to use other ports on
he APs for wired connectivity (EthO is used as uplink so configure other ports depending on AP
nodel). You can control whether wired traffic is trusted or not as well as the forwarding mode
cunneled, split-tunnel or bridged)

Configuration >	> AP Group > Edit "REMOTE_APS"		
	Profiles		Profile Details
Ethernet inte Ethernet inte Wired AP Ethernet in AP LLDP AAA	lot1x ent erface 0 port configuration default erface 1 port configuration VLAN403 erface 2 port configuration VLAN501 ENABLED_ nterface link default default AAA_VLAI	Access mode VLAN	Profile Details
Ethernet Inte		is the inner IP that will be assigned fo	r the RAPs. It shouldn't
Dashboard Monitoring	h other IPs. It is not required to		
WIZARDS AP Controller	Ad Finted Sentices > VEN Services > IPSEC	ite VIA Advanced	
Compus WLAN Remote AP WIP AirWave NETWORK Controller VLANs Ports Uplink	L2TP and XAUTH Parameters Enable L2TP Enable XAuth Authentication Protocols Primary DNS Server Secondary DNS Server Primary WINS Server Secondary WINS Server	Image: Chap Chap MSCHAP MSCHAP MSCHAP MSCHAP 0.0.0.0 0	
IP SECURITY	Address Pools Pool Name	Start Address	End Address
Authentication Access Control	Foot Name	Junit Provides	Lin Address

WIRELESS					
AP Configuration					
AP Installation	Click Add				
MANAGEMENT	Add	Pool Name Define a pool -	Start & End IP	RAP-POOL	
General	Source NAT Controller	Start Address		10.4.5.1	
Administration	Enable Source NAT Campus WLAN	End Address		10.4.5.100	
Certificates	NAT Pool Remote AP				
SNMP	NAT-T NIN				
Logging	Airwave				
Clock	Enable NAT-T NETWORK				
Guest Provisioning	Aggressive Mode				
Captive Portal	IKE Aggressive Group Name		(Only needed for XAUTH)		
SMTP	IP Compression				
Bandwidth Calculator	Enable IP Compression				
Threshold	IKE Server Certificate				
ADVANCED SERVICES	IKE Server Certificate Assigned for VPN-Client		NONE ~		
Redundancy			- Tong		
IP Mobility	CA Certificate Assigned for VPN-Clients		CA Certificate		
Stateful Firewall	None found		CA Certificate		
External Services	Add				
> VPN Services					
Wind Accord	IKE Shared Secrets				

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

NETWORKS												
Dashboard	Monitoring	Configuration	Diagnostics	Maintenance	Save Configuration	2						
WIZARDS AP		Wireless > AP		Whitelist Profile White	list 2							
Controller					3							
Campus WL		Whitelist	Cam	PUS AP	Remote AP							< <stat< th=""></stat<>
Remote AP WIP		Number of Er	ntries: 3									Sea
AirWave		AP	MAC Address	U	ser Name	AP Group	AP Name		Description	Revoked	IF	P-Address
NETWORK		00:0b:86	5×1		REM	OTE_APS	٦,155				0.0.0.0	
VLANs		00:0b:8			REM	OTE_APS					0.0.0.0	
Ports		40:e3:d6	51.		REM	OTE_APS	AYMAN RAP 109				0.0.0.0	
Uplink					9	select 🗸						0
IP		Add Cancel	1									
SECURITY							1 1-3	3 of 3				
Authenticati		4										
Access Cont	trol											
AP Configure	ation	_										
AP Configur												

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

					System RF Security	Maintenance More + Help Lo
8:F3:2	4	Maintenance	Help			Search
+	1 Access	About Configuration Certificates Firmware Reboot Convert				
	Name 😓			ress	Network	Access Point
	ac:a3:1e:c8:f3:2	Convert one or more Access Points to: Remote APs managed by a Mobility Controller Hostname or IP Address of Mobility Controller: FQDN pr IP HERE × After conversion, all Access Points will be managed by the Controller specified abov Convert Now	re.	.99.10	instant Monitoring IDS AirG	ac:a3:1e:c8:f3:24
RF Dashbo	ard				Usage Trends	
				Errors	Clients	
All client	'S			-	5	

	rface
Dashboard	Convert
Overview	Convert one or more Access Points to Remote APs managed by a Mobility Controller 🗸
Networks	Hostname or IP Address of Mobility Controller abvpn.publicdomain.c
Access Points	After conversion, all Access Points will be managed by the Controller specified above.
Clients	Convert
Configuration	
🔎 Maintenance	
About	
Firmware	
Configuration	
Certificates	
Reboot	
Convert	
Regulatory	
Option 82 XML	
	AP will show up as RAP AP and it will broadcast the configured wireless networks.
NETWORK	Search Results Search Results
All WLAN Controllers	300101 ACSUIS
All Access Points	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 & FI
All Access Points All Mesh Nodes All Air Monitors All Routers	Name AP Group A AP IP Y Outer AP IP A AP Type .bg Clients/Channel/ EIRP/MaxEIRP/Standard .a Clients/Channel/ EIRP/MaxEIRP/Standard Enet 1 IPSEC A Uptime A PPPOE A FI
All Mesh Nodes All Air Monitors	AYMAN RAP 109 REMOTE ADS 10 1 94.2 36 RAP-109 1/1/9/20/n(20) 0/116+/18/23/n(40) Wired Port enable 3h;37m;52s disable R
All Mesh Nodes All Air Monitors All Routers All Nuth Clients CONTROLLER Access Points Mesh Nodes Air Monitors IP Routing	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 R 1 1-1 of 1 10 Flags: 1 = 802.11x suthenticated 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 802.11x suthentication; H = Hotspot Enable = 802.11K Enabled; L = Clent Balancing Enabled; M = Mesh N = 802.11b protection disabled; P = RPOTE; R = Remote AP is standby; X = Maintenance Mode; a = Reduce ARP packets in the air; d = Drop Meas/Ecast On: Custom-Cuto
All Mash Rodes All Air Montons All Routens All Routens Contro LLER Contro LLER Ara Monitons 19 Routing 19 Mobility 19 Mobility 19 Mobility Clients	AYMAN RAP 199 REMOTE_APS 10 1 94.2 36 RAP-109 1/1/9/20/r(20) 0/16+/18/23/r(40) Wired Port enable 3h:37m:52s disable R I 1 -1 of 1 1 v I 1 -1 of 1 1 v I 1 -1 of 1 1 v I I -1 of 1 1 v I I -1 of 1 1 v I I I -1 of 1 I v I I I -1 of I I v I I I I -1 of I I v I I I I -1 of I I v I I I I -1 of I I V I I I I I I I I I I I I I I I
All Mash Rodes All Air Montore All Routers All WAAC Cleants COTTPOLER All WAAC Cleants CottPOLER Mash Rodes All Monitors IP Routing IP Mobility IP Multicast Cleants Bicklinis Cleants Freevall Hits External Services Interface	AYMAN RAP 199 REMOTE_APS 10 1 94.2 36 RAP-109 1/1/9/20/r(20) 0/16+/18/23/r(40) Wired Port enable 3h:37m:52s disable R I 1 -1 of 1 1 v I 1 -1 of 1 1 v I 1 -1 of 1 1 v I I -1 of 1 1 v I I -1 of 1 1 v I I I -1 of 1 I v I I I -1 of I I v I I I I -1 of I I v I I I I -1 of I I v I I I I -1 of I I V I I I I I I I I I I I I I I I
All Meah Nodes All Air Montors All Routers Contro LLER Contro LLER Contro LLER Mash Nodes Air Monitors IP Routing IP Mobility IP Muhitast Clients Biakdist Clients Firewall Hits	AYMAN RAP 199 REMOTE_APS 10 1 94.2 36 RAP-109 1/1/9/20/r(20) 0/16+/18/23/r(40) Wired Port enable 3h:37m:52s disable R I 1 -1 of 1 1 v I 1 -1 of 1 1 v I 1 -1 of 1 1 v I I -1 of 1 1 v I I -1 of 1 1 v I I I -1 of 1 I v I I I -1 of I I v I I I I -1 of I I v I I I I -1 of I I v I I I I -1 of I I V I I I I I I I I I I I I I I I
All Mash Nodes All Air Montors All Youhars All Youhar Clents CONTOLLER CONTOLLER CONTOLLER Mash Nodes Air Monitors IP Routing IP Mobility IP Multicast Clents Blackins Clents Freenal Hits External Services Interface Tunnaled Rode Ports Uplink Universal Serial Bus WLAN	AYMAN RAP 199 REMOTE_APS 10 1 94.2 36 RAP-109 1/1/9/20/r(20) 0/16+/18/23/r(40) Wired Port enable 3h:37m:52s disable R I 1 -1 of 1 1 v I 1 -1 of 1 1 v I 1 -1 of 1 1 v I I -1 of 1 1 v I I -1 of 1 1 v I I I -1 of 1 I v I I I -1 of I I v I I I I -1 of I I v I I I I -1 of I I v I I I I -1 of I I V I I I I I I I I I I I I I I I
All Mash Rodes All Air Monitore All Routers All YCAN Clents CONTROLLER CONTROLLER Mash Nodes Air Monitors IP Routing IP Mobility IP Multicast Clents Biackillas Clents Firewall Mits External Services Interface Tunneled Hode Ports Ports Universal Service Interface Tunneled Hode Ports Ports Universal Service Interface WLAN REMOTE-dotts	AVMAN RAP 199 REMOTE APS 10 1 94.2 36 RAP-109 1/1/9/20/n(20) 0/16+18/23/n(40) Wired Port enable 3h:37m:52s disable R 1 1:1:01 10
All Mash Rodes All Air Monitors All Routers ContRoLLER ContRoLLER ContRoLLER Mash Nodes Air Monitors IP Routing IP Mobility IP Multicast Clients Biackins Clients Firewall Hits External Services Interface Tunneled Hode Ports Ports Uplink Universal Service Stateface Tunneled Hode Ports Ports Universal Service Stateface Tunneled Hode Ports Ports Universal Service Stateface Tunneled Hode Ports Dents Universal Service Bus WLAN REMOTE-dotts:	A VIMAN RAP 199 REMOTE AS 10 1 9.2 (3 RAP-10 1/1/2/2014(2) 0/16+/18/22/14(2) Wired Per mable 3h.37m:32 disable R 1 1:101
All Mash Nodes All Air Monitors All Routers All Routers COTTOLLE Controller Controller Controller Mash Nodes Air Monitors IP Routing IP Mobility IP Multicast Clents Bicklins Clents Freeall Hits External Services Interface Tunneled Node Ports Borts Universit Services Interface Tunneled Node Ports Borts Networks Interface Surgers Interface Surgers	AVMAN RAP 199 REMOTE APS 10 1 94.2 36 RAP-109 1/1/9/20/n(20) 0/16+18/23/n(40) Wired Port enable 3h:37m:52s disable R 1 1:1:01 10
All Mash Nodes All Air Monitors All YuAh Clents ControlLER ControlLER All Wohl Clents ControlLER Mash Nodes Air Monitors IP Routing IP Mobility IP Multicast Clents Blackist Clents Prevail Hits External Services Interface Tunnaled Node Ports Dats Uplink Universal Serial Bus WLAN REMOTE-dotix Steep 8: Verifit	• AVMAN RAP 19 RENOTE AS 10 1 9.2 3 RP-10 1/1/2/2/2/2 0 RP-10 1/1/2/2/2/2 0/2 1/1/2 0/2 0/2 0/2 0/2 0/2 0/2 0/2 0/2 0/2 0
All Mash Rodes All Air Monitors All Routers CottRoLER CottRoLER CottRoLER Mash Rodes Air Monitors IP Routing IP Mohilty IP Multicast Clients Bicklinds Clients Firewall Hits External Services Interface Tunneled Hode Ports Ports Universal Services Interface Tunneled Hode Ports Ports UNIVERS NETWORK NetWorks All Access Points	• AVMANE ARAP 109 REMOTE, ASS 10 1 9.2 3 RAP-10
All Mash Rodes All Air Monitors All Routers All WAC Ilents COTROLLER COTROLLER COTROLLER Controller Controller Controller Controller Development Devel	• AVMANE ARAP 109 REMOTE, ASS 10 1 9.2 3 RAP-10
All Mash Rodes All Air Monitors All Routers All Year Clearts COTTOLLER COTTOLLER COTTOLLER Mash Rodes Air Monitors IP Routing IP Mobility IP Multicast Clients Blacklist Clients Firewall Hits External Services Interface Tunneled Hode Ports Ports Uplink Universal Serial Bus WLAN REMOTE-dotts: Steep 8: Veriffe NETWORK NETWORK All Access Points All Access Points	• YMMAN RAP 199 REMOTE ASS 1 9.4.2 36 RAP-109 1/1/9/20/(20) 0/16+7/80/20/(40) Wind Port mable 3h:37m:32 disable R I = 1:01:10:0 I = 1:01:10:0 0/16+7/80/20/(40) Wind Port mable 3h:37m:32 disable R Plags 1: = 002.1:x authenticated AP, 2 = Using IKE version 2; A = Enter In active/standby mode IB = Babery, Boost 00; G = Callulary D = Versione AB actable 0; F = AP failed 802.1:x authentication, H = Hoteport Enable 3h: 2 = POPORE AB actable 0; F = AP failed 802.1:x authentication; H = Hoteport Enable 3h: 0 = POPORE AB actable 0; F = AP failed 802.1:x authentication; H = Hoteport Enable 0; C = POPORE AB actable 0; F = AP failed 802.1:x authentication; H = Hoteport Enable 0; C = POPORE AB actable 0; F = AP failed 802.1:x authentication; H = Hoteport Enable 0; C = POPORE AB actable 0; F = AP failed 802.1:x authentication; H = Hoteport Enable 0; C = POPORE AB actable 0; F = AP failed 802.1:x authentication; H = Hoteport Enable 0; C = POPORE AB actable 0; F = AP failed 802.1:x authentication; H = Hoteport Enable 0; C = POPORE AB actable 0; F = AP failed 802.1:x authentication; H = Hoteport Enable 0; C = POPORE AB actable 0; F = AP failed 802.1:x authentication; H = Hoteport Babery, Boost 0; F = AP failed 802.1:x authentication; H = Hoteport Babery, Boost 0; F = AP failed 802.1:x authentication; H = Hoteport Babery, Boost 0; F = AP failed 802.1:x authentication; H = Hoteport Babery, Boost 0; F = AP failed 802.1:x authentication; H = Hoteport Babery, Boost 0; F = AP failed 802.1:x authentication; H = Hoteport Babery, Boost 0; F = AP failed 802.1:x authentication; H = Hoteport Babery, B
All Mash Rodes All Air Monitore All Routers All Routers ContRolLER ContRolLER ContRolLER Mash Nodes Air Monitors IP Routing IP Mobility IP Multicast Clients Biackills Clients Firewall Mits External Services Interface Tunneled Hode Ports Ports Universit Service Stateface Tunneled Hode Ports Ports Universit Service State Universit Service State Universit Service State Universit Service State Universit Service State Universit Service State Universite State Universite State Universite State Universite State All Mesh Nodes All Routers All Work Service All Work Service Al	• AVMAN RAP 109 RMOTE AS 10 1 94.20 10 RAP 10 11 194.20 10 RAP 109 11/1920/200 11 194.200 100 114/1920/200 11 194.200 114
All Mesh Nodes All Air Monitors All You Ministry All You Ministry Corroller Corroller Mesh Nodes Air Monitors IP Routing IP Mobility IP Multicast Clents Blackiast Clants Freeall Vita Elsenai Services Interface Tunneled Node Ports Uplink Universal Serial Bus WLAN REMOTE-dottx: Steep S: Verify NETWORK NETWORK Ministry All Wuk Centrollers All Access Points All Access Points Mesh Nodes All Monitors	• AVMAN RAP 109 RMOTE AS 10 1 94.20 10 RAP 10 11 194.20 10 RAP 109 11/1920/200 11 194.200 100 114/1920/200 11 194.200 114

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

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.

Dashboard	Monitoring	Configuration	Diagnostics	Maintenance	Save Configuration	1 🦿		
WIZARDS		Network > Contr	oller > Sync	whitelist servic	e			
AP		System Setting	s Control F	Plane Security	Cluster Settings	Licenses	Centralized Licenses	Sync whitelist service
Controller		Sync Whitelist	with Activate					
Campus W Remote AP		Enable sync ser				Enable	Disable	
WIP		Activate user				user1		
AirWave		Activate passwo	rd			•••••		
NETWORK		Frequency				1 v (Day	s)	
> Controller								
VLANs								
Ports		Commands						
IP								
SECURITY								
Authenticat								
Access Cor	ntrol							
WIRELESS AP Configu	ration							
AP Coningu AP Installa								
MANAGEMEN	т							
Chain Ci (. اماریم مام		
•					-		acquire an IP via	
IAP/RAP	should	have interne	et reacha	bility (DHC	CP, DNS, HTTP	S, NTP,	NAT-T) so it can	communicate
with act	ivate an	d learn the o	controlle	IP and gro	oup.			

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

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 gro	un for Remote AP	s (Recommended)	
Managed Network > SITE1 >			Pending Changes
C Mobility Master	Dashboard Configuration	AP Groups 4 NAME APs	
Managed Network (2) SITE1 (2) SVMC-1	WLANs Roles & Policies Access Points	default NoAuthApGroup GROUP1 2	
 VMC-2 SITE2 (0) 	ACCESS POINTS AP Groups Authentication	RAP-GROUP +	
SITE3 (0)	Services Interfaces	AP Groups > RAP-GROUP APs WLANs Radio Mesh LMS MultiZone NAME IPV4 ADDRESS IPV6 ADDRESS MAC ADDRESS TYPE	SERIAL #
	Controllers System		
	Tasks Redundancy Maintenance		

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 🗘
€ <u>k</u>	Q Dashboard	
🗀 Mobility Master	Configuration	default NoAuthApGroup
🔁 Managed Network (2)	WLANs	GROUP1 2
🗁 SITE1 (2)	Roles & Policies	RAP-GROUP - 🔟
S VMC-1	Access Points	+
📼 VMC-2	AP Groups	
🗂 SITE2 (0)	Authentication	AP Groups > RAP-GROUP APs WLANs Radio Mesh LMS MultiZone Profiles
C SITE3 (0)	Services	Profiles for Group RAP-GROUP Virtual AP profile: AOS8-PSK
	Interfaces	
	Controllers	Regulatory Domain
		⊕
	System	
	Tasks	⊙
	Redundancy	⊕
	Maintenance	⊙ G Wireless LAN > RF
		⊙ 🕒 Virtual AP
		Advanced
		> Broadcast/Multicast
(tunneled, split-tu	unnel or bridged)	Pending Changes
C,	0	
C Mobility Master	Dashboard	default
Managed Network (2)	Configuration	NoAuthApGroup GROUP1 2
	WLANs	RAP-GROUP - 🔟
SHEY(2) SHEY(2)	Roles & Policies	+
S VMC-2	Access Points	
C SITE2 (0)	AP Groups	AP Groups > RAP-GROUP APs WLANs Radio Mesh LMS MultiZone Profiles
SITE3 (0)	Authentication	Profiles for Group RAP-GROUP
	Interfaces	
	Controllers	Ethernet interface 0 port configuration
	System	Ethernet interface 1 port configuration
	Tasks	Thernet interface 2 port configuration
	Redundancy	Ethernet interface 3 port configuration
	Maintenance	⊕ Ethernet interface 4 port configuration
		Ethernet usb port configuration
		Provisioning
		Providence Provide
		s – This is the inner IP that will be assigned for the RAPs. It shouldn't
conflict with othe	er IPs. It is not req	uired to be routable.

Managed Network > SITE1 >		Pending Chang
E. 0		2
C Mobility Master		Clusters AirGroup VPN Firewall IP Mobility External Services DHCP WAN
Managed Network (2)		> IKEv1
➡ SITE1 (2)		> IKEv2
📼 VMC-1		General VPN
📼 VMC-2		
📇 SITE2 (0)		Address Pools
C SITE3 (0)	Services 1	POOL NAME START ADDRESS END ADDRESS
		+ 4
		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
created in Step 1. Managed Network > Mobility Master Managed Network (2) SITE1 (2) VMC-1 VMC-2 SITE2 (0)	Configuration WLANs Roles & Policies AP Groups	Campus APs Remote APs Mesh APs Whitelist Provisioning Rules Campus AP Whitelist Remote AP Whitelist Provision ing Rules Campus AP Whitelist Campus
SITE3 (0)	Authentication	
	Interfaces	T
	Controllers System	Delete Revoke 50 V < 1 >
	Tasks	Remote AP Whitelist > ac:a3:1e:c8:f3:24
	Redundancy	AP name: RAP-214
	Maintenance	
		AP group: RAP-GROUP V
		Description:
shown above (whit following command iap trusted-branch	elist rap add mac- d should be added -db add mac-addr	AP manually without staging, then the RAP whitelist command -address <mac>) is not enough. From the controller cli, the as well if the RAP are authenticating locally on the controller. ress <mac> where <mac> should be replaced with the MAC</mac></mac></mac>
address of the rem	ote 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.

MAC address:	ac:a3:1e:c8:f3:24
Name:	RAP214 2
AP group:	RAP-GROUP 👻 🛃
Controller discovery:	Use AP discovery protocol (ADP)
Controller IP/DNS name:	rou e.com
IP:	DHCP Static
5 GHz antenna gain:	3.0
2.4 GHz antenna gain:	3.0
Deployment:	Campus 💿 Remote Mesh Campus remote Mesh
Authentication method:	Certificate 🗸 🗸
PKCS12 passphrase:	
Trust anchor:	self-signed 🗸 🛛
Wi-Fi uplink:	

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.

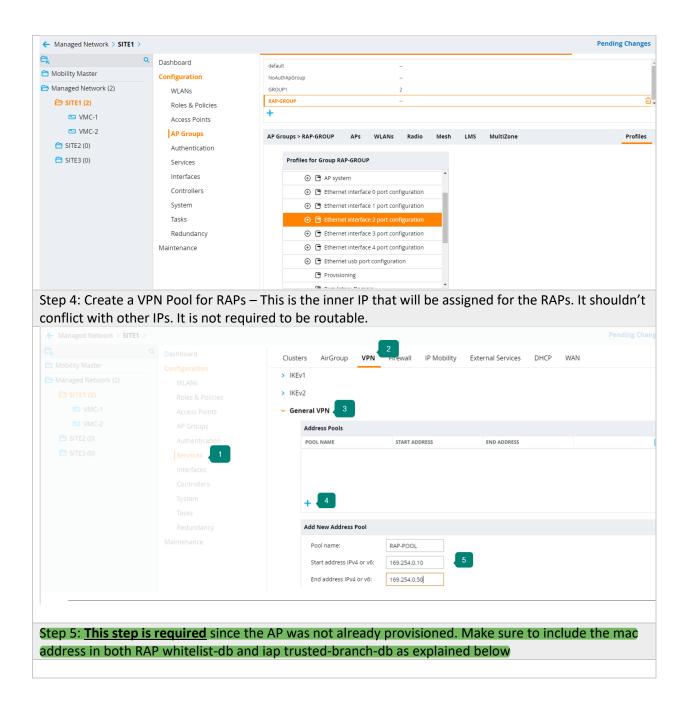
aruba	MOBILITY MASTER MM-1			coi ⊘	2 ① 0	ACCESS POINTS	CLIENTS	ALERTS			admin
Managed Networ	k >									🖏 Search	'n
ashboard Overview	<	- 🗔 2 _{Cont}	rollers	🗐 2 Access De	evices of	🛠 🚺 Uplinks		Clusters			
Infrastructure	Ad	cess Points 2	filtered by Status U	P ×							∇
Traffic Analysis		NAME	STATUS	CLI	ENTS	UPTIME	MANAGE	D BY G	ROUP	MODEL	
,	>	RAP214	🕗 Up	3		12m 33s	VMC-1	R	AP-GROUP	214	
Security Services	>	AP-225-1	🕗 Up	0		9w 2d	VMC-1	G	ROUP1	225	
ten 8. Verit	fv Client	s are ah	le to con	nect and	d get th	e right role	and VI	AN			
aruba	MOBILITY MASTER MM-1		le to con	CON	-	e right role ACCESS POINTS ⊙ 2 ○ 0 ?		ALERTS		<i>.</i>	admin 🗸
Aruba	MOBILITY MASTER MM-1	2		CON ©	2 0 0	ACCESS POINTS	CLIENTS 3 № 0	ALERTS		🔅 Search	admin 🗸
Aruba Managed Networ	MOBILITY MASTER MM-1			CON	2 0 0	ACCESS POINTS	CLIENTS	ALERTS		🖄 Search	admin 🗸
Aruba		2	its -	CON ©	NTROLLERS 2 0 0	ACCESS POINTS	CLIENTS 3 № 0	ALERTS		🕸 Search	admin 🗸
Anaged Networ ashboard		- A 3 clier	nts	CON © 1 WLAN 5 Point MAC address a	NTROLLERS 2 0 0 ctal:1ec8:f3:24 >	Access Points	cLIENTS * 3 ≠ 0	ALERTS 1 adios	WIAN		
Managed Networ ashboard Overview Infrastructure		- <u>A</u> 3 clier	its -	con ⊙ え 1 wlan	NTROLLERS 2 0 0	ACCESS POINTS	CLIENTS 3 № 0	ALERTS	WLAN A058-P5K	Search	
Managed Networ ashboard Overview Infrastructure Traffic Analysis	MOBILITY MASTEI MM-1 rk >	reless Clients	ats filtered by Access	COM © 1 WLAN S Point MAC address & HEALTH	NTROLLERS 2 ① 0 Acca3:1e:c8:f3:24 > BAND	Access points © 2 ○ 0 ⇒ 14.0 MB < ROLE	CLIENTS 3 0 ((p)) 4 R SNR	ALERTS 1 adios		CONNECTE	
Anaged Networ ashboard Overview Infrastructure Traffic Analysis Security	MOBILITY MASTEI MM-1 rk >	Clier NAME A 172.16.99.15	IF ADDRESS 172.16.99.15	CON © 1 WLAN POINT MAC address a HEALTH BIG GOOD	NTROLLERS 2 ① 0 Acca3:1ex8:f3:24 > BAND 5 GHz	ACCESS POINTS © 2 0 0 P 14.0 MB K ROLE DemoUserRole	CLIENTS 3 0 ((p)) 4 R SNR 37 dB	ALERTS 1 adios USAGE -	AOS8-PSK	CONNECTE 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 – Stagir	ng the RAP as CAP	• then provisioning it as R	AP	
Step 1: Staging is n	ot needed so this	step is skipped		
Step 2: Create a gr	oup for Remote A	Ps (Recommended)		
Managed Network > SITE1 >				Pending Changes
C, Q				0 0
C Mobility Master	Dashboard	AP Groups 4		
Anaged Network (2)	Configuration	NAME AF	Ps	
➡ SITE1 (2)	WLANs Roles & Policies	default		
VMC-1		GROUP1 2		
VMC-2	Access Points	RAP-GROUP		
SITE2 (0)	AP Groups	+		
SITE3 (0)	Services	AP Groups > RAP-GROUP APs WLANs	Radio Mesh LMS MultiZone	
	Interfaces	· · ·	V6 ADDRESS MAC ADDRESS TYPE	SERIAL #
	Controllers	IT IT IT IT IT IT		JERIAL #
	System			
	Tasks			
	Redundancy			
	Maintenance			
	Wantenance			
			(Add the necessary VAP, Wi	reless
SSIDs, AAA profiles	etc.) You can us	se existing profiles or crea	te new profiles as per your	
requirements.				
Managed Network > SITE1 >				Pending Changes 🤇
C _k q	Darkhaurd			
C Mobility Master	Dashboard	default		Â
Managed Network (2)	Configuration WLANs	NoAuthApGroup GROUP1 2		
➡ SITE1 (2)	Roles & Policies	RAP-GROUP -		
📼 VMC-1	Access Points	+		
S VMC-2	AP Groups			
🗀 SITE2 (0)	Authentication	AP Groups > RAP-GROUP APs WLANS R	tadio Mesh LMS MultiZone	Profiles
🗂 SITE3 (0)	Services	Profiles for Group RAP-GROUP	Virtual AP profile: AOS8-PSK	
	Interfaces	Provisioning	the General	
	Controllers	🕒 Regulatory Domain	✓ General	
	System		Virtual AP enable:	
	Tasks	⊕ 🖻 Mesh	• VLAN: 99	
	Redundancy	⊕ 🖻 qos	Forward mode: tunnel	~
	Maintenance	RF Management	Openflow Enable: 🔽	
		G Wireless LAN	> RF	
			> Advanced	
		⊖ 🕒 AOS8-PSK	Broadcast/Multicast	
Stop 4 (Optional)	/ou con configuro	wired port profiles here it	n case you want to use othe	norts on
	•	• •	•	•
			gure other ports depending o	
1 13 57	ntrol whether wir	red traffic is trusted or not	t as well as the forwarding m	ode

(tunneled, split-tunnel or bridged)



← Managed Network >			
C Mobility Master		mpus APs Remote APs Mesh APs Whitelist Provisioning Ru	ules
Managed Network (2) SITE1 (2) SITE1 (2) VMC-1 VMC-2	Configuration WLANs Roles & Policies Access Points AP Groups	Campus AP Whitelist Remote AP Whitelist MAC ADDRESS NAME AP GROUP DESCRIPTION IPV4 ADDRESS IP aca3:tec8:f RAP-214 RAP-GROUP - 0.00.0 -	ter prof Address status Revoke text Updated Accepted – Tue Mar 1
 SITE2 (0) SITE3 (0) 	Authentication Services Interfaces Controllers System	Delete Revoke	50 🗸 🚺 >
	Tasks Redundancy Maintenance	Remote AP Whitelits > ac:a3:1e:c8:f3:24 AP name: RAP-214 AP group: RAP-GROUP Description:	

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 \rightarrow Convert Choose Convert to Remote AP Managed by a Mobility Controller Provide the IP Address or FQDN of the controller

OLD IAP Interface

-C8:F3:24	Maintenance Helic	2	System RF Security Ma	intenance More∓ Help Logo Search
+	About conniguration certificates minimare Reboot convert	ess .99.10	Network instant	Access Point ac:a3:1e:c8:f3:24
RF Dashboard			Monitoring IDS AirGrou Usage Trends	p Configuration 0 Alerts
All clients	Close	Errors	Clients	23:15

New IAP Interf	face	
Lul Dashboard	Convert	
Overview	Convert one or more Access Points to	Remote APs managed by a Mobility Controller 🗸 🗸
Networks	Hostname or IP Address of Mobility Controller	abvpn.publicdomain.c
Access Points	After conversion, all Access Points will be manage	d by the Controller specified above.
Clients	Convert	
Configuration		
🔎 Maintenance		
About		
Firmware		
Configuration		
Certificates		
Reboot		
Convert		
Regulatory		
Option 82 XML		

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.

	M-1		\odot	2 ① 0 (⊙2 ①0 ₹	3 🕫 0					
Managed Network >									Ŷ	Search	
ashboard Overview	← 🗔 2 _{Contro}	llers	a 2 Access Dev	vices	0 Uplinks	📰 <mark>(</mark>) cl	usters				
Infrastructure	Access Points 2	filtered by Status U	$P \times$								∇
Traffic Analysis	NAME	STATUS	CLIE	ENTS	UPTIME	MANAGED	BY GF	ROUP	MODEL		
	> RAP214	🕗 Up	3		12m 33s	VMC-1	RA	P-GROUP	214		
Security	> AP-225-1	🕗 Up	0		9w 2d	VMC-1	GF	ROUP1	225		
aintenance tep 8: Verify C		e to con		-							
aintenance	lients are abl Y MASTER M-1	e to con	CON	TROLLERS AG	CCESS POINTS	clients	AN. Alerts 1		چې چې	earch	admin ~
aintenance tep 8: Verify C orubo ^{MOBILIT} Managed Network >	Y MASTER M-1		CON ② 2	TROLLERS AC	CCESS POINTS	CLIENTS 3 № 0	ALERTS		¢) S	earch	admin 🗸
Laintenance Step 8: Verify C Orubo Monaged Network >	Y MASTER	<u>.</u>	CON	TROLLERS AC 2 ○ 0 ○	CCESS POINTS	CLIENTS	ALERTS		¢) S	earch	admin ~
Annaged Network >	Y MASTER M-1	filtered by Access	CON ② 2 ③ 1 WLAN s Point MAC address ac	ITROLLERS AG 2 ○ 0 ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	CCESS POINTS ⇒ 2 ○ 0 ₹ 14.0 MB	CLIENTS [•] 3 ≠ 0 (°) ³ 4 _{Rad}	ALERTS 1 ios				
Annaged Network >	MASTER M-1	filtered by Access	con ⊙ 2 ② 1 wlan	TROLLERS AC 2 ○ 0 ○	CCESS POINTS	CLIENTS 3 № 0	ALERTS	WLAN ACS8-PSK	© S	CTE	
Managed Network > Managed Netwo	MASTER M-1	filtered by Access	CON 2 2 2 1 WLAN POINT MAC address ac HEALTH	TROLLERS ACC 2 0 0 6 Callers Callers Acc Callers F3:24 × BAND	CCESS POINTS 2 0 7 14.0 MB ROLE	CLIENTS 3 P 0	ALERTS 1 ios		CONNE	CTE	
Managed Network > Managed Network > Cashboard Overview Infrastructure Traffic Analysis Security	Y MASTER M-1 Wireless Clients 3 NAME A > 172.16.99.15	filtered by Access IP ADDRESS 172.16.99.15	CON © 2 T WLAN POINT MAC address ac HEALTH IIII GOOD	TROLLERS Ad 2 0 0 0 0 Call C <thc< th=""> C <th< td=""><td>CCESS POINTS 2 0 0 14.0 MB ROLE DemoUserRole</td><td>CLIENTS 3 0 ((ϕ) 4 Rad SNR 37 dB</td><td>ALERTS 1 ios USAGE -</td><td>AOS8-PSK</td><td>CONNE RAP214</td><td>CTE</td><td></td></th<></thc<>	CCESS POINTS 2 0 0 14.0 MB ROLE DemoUserRole	CLIENTS 3 0 ((ϕ) 4 Rad SNR 37 dB	ALERTS 1 ios USAGE -	AOS8-PSK	CONNE RAP214	CTE	

5.3 Scenario 3 – Using Aruba Activate (ZTP)

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

Scenario 3 – Using Aruba Activate

Step 1: Create an account on activate and follow this guide to create a provisioning rule for IAPs to RAPs. Optionally, you can add a notification rule once an AP gets provisioned from activate, an email will be sent.

https://community.arubanetworks.com/t5/Wireless-Access/Tutorial-Provisioning-RAPs-with-Aruba-Activate-Dec13-Tutorial/td-p/128707

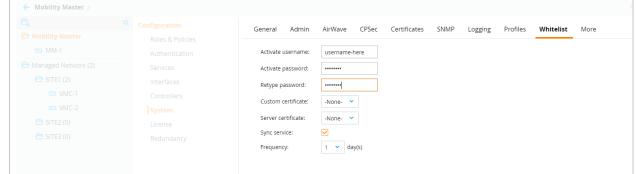
Step 2: Create a group for Remote APs (Recommended)

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

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

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

Step 5: Controller needs to be configured to whitelist the RAPs. This can happen manually as described in the previous scenarios or via the below configuration of enabling activate sync-service.



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

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

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

6 Summary

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

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

7 Additional Resources

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