Contents

	1.1	Revision History	1
2	Den	no Topology	2
3	Sett	ting up the OVA for Mobility Master	3
4	Mol	bility Master Basic Configuration	5
5	Con	ntroller Configuration	11
6	Mol	bility Master Configuration	13
	6.1	Dot1x Wireless Configuration	15
	6.2	ClearPass Basic Configuration	23
	6.3	Joining AD Domain	24
	6.4	ClearPass dot1x Service	
	6.5	ClearPass Access tracker	

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
02 Feb 2021	0.1	Ariya Parsamanesh	Initial creation
08 Feb 2021	0.2	Ariya Parsamanesh	Added section 5-6
15 Feb 2021	0.3	Ariya Parsamanesh	Minor modifications

2 Demo Topology

Here is the topology we'll be implementing. The aim here is to provide the starting point to put together a solution that include the Mobility conductor (formally known as mobility master), controllers, APs, ClearPass and Airwave.



This is the part 1 of the three parts series.

3 Setting up the OVA for Mobility Master

For the details please refer to the ArubaOS 8.7.1.0 virtual appliance installation guide. Here I just want to highlight the areas that some might forget to follow.



🚯 Edit settings - MM-1 (ESXi 5.0 virtual m	achine)		
Virtual Hardware VM Options			^
🔜 Add hard disk 🛛 🎫 Add network adap	ter 🔚 Add other device		
CPU	3 🔻 🚺		
Memory	6144 MB T		
Hard disk 1	4 GB •		\otimes
Hard disk 2	6 GB •		\otimes
SCSI Controller 0	LSI Logic Parallel	T	\otimes
Metwork Adapter 1	VM Network	▼ □ Connect	\otimes
Metwork Adapter 2	VM Network	Connect	\otimes
Metwork Adapter 3	VM Network	▼ □ Connect	\otimes
Floppy drive 1	Use existing floppy image	•	~

Just enable the correct VLAN/adapter to be assigned to network adapter 2 and power that one up. Next, connect to the console of the VM, as you need to setup the IP addressing, etc.

MM-1		🖬 🖬 🚍 🎇 Actions 🛞
Aruba Networks ArubaUS Version 8.7.1.1 (build 78245 ∕ label #78245) Built by pHoildepr-hpn-build05 on 2020-12-14 at 20:44 (c) Copyright 2020 Hewlett Packard Enterprise Developm	0:11 UTC (gcc version 4.9.4) ment LP.	
[09:18:08]:Starting device manager	C OK J	
Device Open FailedCreating New device <	HH-VA >>>>> [0K]	
[09:18:11]:Uncompressing core image files	E OK J	
[09:18:26]:Extracting corefs	сок ј	
[09:18:27]:Waiting for storage device Performing partition fast test	E DONE J	
Checking for file system	LOK J	
[09:18:29]:Scanning storage device filesystem	C OK J	
[09:18:34]:Mounting flash		
[09:18:34]:Mounting disk1		
109:18:35J:Hounting disk2		
[09:18:37] Turning suan ON on zRAMO		
[09:18:37] Installing factory image		

Success: Package default_airgroup_pkg installed successfully Success: Package default_ucm_pkg installed successfully Success: Package default_wms_pkg installed successfully Success: Package default_arm_cm_pkg installed successfully Success: Package default_web_cc_pkg installed successfully Success: Package default_nbapi_helper_pkg installed successfully Success: Package default_airmatch_pkg installed successfully Success: Package default_appRF_pkg installed successfully [OK] [09:46:06]:Verify the bootloader [09:46:07]:rcS Done(32 sec) [09:46:07]:Initializing CA bundle [OK] [09:46:07]:Starting OS services [OK] Starting ztp Starting ztp auto provision ***************** Welcome to the ArubaMM-VA setup dialog ****************** This dialog will help you to set the basic configuration for the switch. These settings, except for the Country Code, can later be changed from the Command Line Interface or Graphical User Interface. Commands: <Enter> Submit input or use [default value], <ctrl-I> Help <ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end <ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line <ctrl-P> Previous question <ctrl-X> Restart beginning <ctrl-R> Reload box Enter System name [ArubaMM-VA_04_D8_FA]: Aruba-MM1 Enter Controller VLAN ID [1]: Enter Controller VLAN port [GE 0/0/0]: Enter Controller VLAN port mode (access|trunk) [access]: Do you wish to configure IPV4 address on vlan (yes|no) [yes]: Enter VLAN interface IP address [172.16.0.254]: 192.168.1.55 Enter VLAN interface subnet mask [255.255.255.0]: Enter IP Default gateway [none]: 192.168.1.249 Enter DNS IP address [none]: 1.1.1.1 Do you wish to configure IPV6 address on vlan (yeslno) [yes]: no_ Enter Country code (ISD-3166), <ctrl-I> for supported list: AU You have chosen Country code AU for Australia (yesIno)?: yes Enter the controller's IAMA Time zone [America/Los_Angeles]: Australia/Melbourne Enter Time in UTC [09:47:23]: Enter Date (MM/DD/YYYY) [2/1/2021]: Enter Password for admin login (up to 32 chars): ******* Re-type Password for admin login: ******* Current choices are: System name: Aruba-MM1 Controller VLAN id: 1 Controller VLAN port: GE 0/0/0 Controller VLAN port mode: access Option to configure VLAN interface IPV4 address: yes VLAN interface IP address: 192.168.1.55 VLAN interface subnet mask: 255.255.255.0 IP Default gateway: 192.168.1.249 Domain Name Server to resolve FQDN: 1.1.1.1 Option to configure VLAN interface IPV6 address: no Country code: AU IANA Time Zone: Australia/Melbourne If you accept the changes the switch will restart! Type <ctrl-P> to go back and change answer for any question Do you wish to accept the changes (yesIno)

Once you have accepted the changes, MM will reboot and then you can browse to that IP address which you just configured. Once you login with the new credentials, you need to add the licenses. To be able to add the license, you need to get the license passphrase and send it to Aruba in which they can activate the evaluation licenses for it.

4 Mobility Master Basic Configuration

aruba	MOBILITY MAST Aruba-MM-1	ER	CON ©	ITROLLERS ACCES 0 ① 0 ⊘ 0	SS POINTS CLIENT	ALERTS		? admin	~
🔶 Mobility Master	>								Ŷ
€ <mark>,</mark>	۹	Configuration		License managem	ent: O Aruba Supp	ort Portal (ASP)	O External license server	Manual	
🔁 Mobility Master		Roles & Polic	les	License Usage	License Inventory				+
📼 Aruba-MM-1		Authenticati	on	LICENSE	DESCRIPTION	STATUS	EXPIRATION	INSTALLED	
Managed Network	< (0)	Services						to this Mobility Master	
		Interfaces		AP	Access Points	O Not Licensed	Not Licensed	0	^
		Controllers		PEFNG	Policy Enforcement Fire	O Not Licensed	Not Licensed	0	
		Suctem		RFP	RF Protect(WIP,Spectru	 Not Licensed 	Not Licensed	0	
		System		ACR	Advanced Cryptography	 Not Licensed 	Not Licensed	0	
		License		WebCC	Web Content Classificat	Not Licensed	Not Licensed	0	
		Redundancy		MM	Mobility Master Virtual	Not Licensed	Not Licensed	0	
				MC-VA-RW	Controller Virtual Appli	Not Licensed	Not Licensed	0	
				MC-VA-EG	Controller Virtual Appli	Not Licensed	Not Licensed	0	
	Aruba-MM-1		0	0 0 0 0	0 0 7 0	*0 △0		(g) admi	n ¥
	0		istali Licenses				0.5	<u></u>	
-κ	4	Configuration	To install new licer	nses you will need:			U External license serve	r 🥑 Manual	
Mobility Master		Roles & Pc	. The Serial Nu	mber of this Mobility M	Aaster: MM704D8E0				+
📼 Aruba-MM-1		Authentica	The License K	ev for each service you	wish to activate		EXPIRATION	INSTALLED	
🗎 Managed Network	(0)	Services	 License Passp 	hrase: MM704D8F0-0/	AncdT+w-f+tEVace-WSJ+PM	12G-wQH9hgXU		to this Mobility Master	
		Interfaces	Obtain License Ker	s from HDE Aruba My	Networking Portal		Not Licensed	0	^
		Centreller	Obtain License Re	ys nom nee Aruba wy	Networking Portai		Not Licensed	0	
		Controller	Enter the license k	eys in the text box belo	ow, one key per line.		Not Licensed	0	
		System	1				Not Licensed	0	
		License				ht.	Not Licensed	0	
		Redundan			and the second		Not Licensed	0	
					Cance	OK	Not Licensed	0	
				MC-VA-EG	Controller Virtual Appli		Not Licensed	0	

Here we'll cover the basic configuration starting with evaluation licensing.

Here is the passphrase which is highlighted. This needs to be sent to your Aruba contact or SE, they should be able to generate and send you the license key to be copy and pasted into the following dialog.

aruba	MOBILITY MASTE Aruba-MM1	R	CONTROLLERSACCESS POINTSCLIENTSALERTSImage: Control lengthImage: Control leng
🔶 Mobility Master	>		Install Licenses
Hobility Master Aruba-MM1 Managed Network	Q	Configuration Roles & Pc Authentica Services Interfaces Controller System License Redundan	To install new licenses you will need: The Serial Number of this Mobility Master: MM704D8F0 The License Key for each service you wish to activate License Passphrase: MM704D8F0-0AncdT+w-f+tEVace-WSJ+PM2G-wQH9hgXU Obtain License Keys from HPE Aruba My Networking Portal Enter the license keys in the text box below, one key per line. Image: Aruba Ar
			MC-VA-FG Controller Virtual Appli

And some of the licenses like PEFNG and RFP will prompt to enable them as shown below.

OLODO Aruba	i-MM1	CONTROLLE ⊘ 0 ④	O O O O	OINTS CLIEN ① 0 0	№ 0 △ 0		(?) a	
← Mobility Master >		Enable Features					Pending	g Changes
C Mobility Master	Configuration Roles & Pc	10 RFP licenses are availab	le in global license	e pool.		C External license serve	er 🖲 Mar	nual +
🗎 Managed Network (0)	Services					EXPIRATION	to this Mobility Master	
	Interfaces			Canc	CK OK	May 03 2021	10	
	Controllers	PEFNO	3	Policy Enforcement Fire.	🕑 Active	May 03 2021	10	
	controllers	RFP		RF Protect(WIP,Spectru	. ⊘ Active	May 03 2021	10	
	System	ACR		Advanced Cryptography		Not Licensed	0	
	License	WebC	c	Web Content Classificat.	🕞 Not Licensed	Not Licensed	0	
aruba MOBILIT Aruba	Y MASTER a-MM1	CONTROLLER ⊙ 0 ①	ACCESS PO	DINTS CLIENT	ALERTS № 0 △ 0		@ adm	in ¥
Mobility Master > Mobility Master > Mobility Master >	Y MASTER MM1 Q Configuration	CONTROLLEI O O O	ACCESS PO	CLIENT	S ALERTS	O External license server	 adm Pending Cl Manual 	in 🗸 hanges 🕻
Mobility Master > Mobility Master > Mobility Master > Mobility Master > Mobility Master >	Y MASTER MM1 Q Configuration Roles & Polic	CONTROLLEI 0 0 Licer Lice	ACCESS PO	CLIENT	S ALERTS 0 0 0	O External license server	 adm Pending Cl Manual 	in ~ hanges ¢ +
Mobility Master Mobility Master Aruba Aruba-MM1 Managed Network (0)	Configuration Roles & Pollu Authenticati Services	controller 0 0 0 Licer Licers	ACCESS PO	CLIENT CLIENT	S ALERTS	External license server EXPIRATION	 adm Pending Cl Manual INSTALLED to this Mobility Master 	in ~ hanges ¢ + ⊞
Mobility Master Mobility Master Aruba Aruba-MM1 Managed Network (0)	Configuration Roles & Politication Authenticati Services	CONTROLLEI 0 0 0 Licen Licens AP	ACCESS PO	CLIENT CLIENT	S ALERTS	External license server EXPIRATION May 03 2021	 adm Pending Cl Manual INSTALLED to this Mobility Master 10 	hanges ¢
Mobility Master Mobility Master Aruba Aruba-MM1 Managed Network (0)	Configuration Roles & Polic Authenticati Services Interfaces	CONTROLLEI 0 0 0 cles on Licen AP PEFNG	ACCESS PO	CLIENT CL	S ALERTS O Active O Active	Expiration May 03 2021 May 03 2021	adm adm compared by the second	in ~ hanges (+
Mobility Master Mobility Master Aruba Mobility Master Aruba-MM1 Managed Network (0)	Configuration Roles & Poli Authenticati Services Interfaces Controllers	CONTROLLEI O 0 0	ACCESS PO	CLIENT CL	STATUS ALERTS Contronation STATUS Control Active Control Active Control Con	External license server EXPIRATION May 03 2021 May 03 2021 May 03 2021	adm adm compared compared	in ∨ hanges ¢ + Ⅲ
Mobility Master Mobility Master Aruba Mobility Master Aruba-MM1 Managed Network (0)	Configuration Roles & Polin Authenticati Services Interfaces Controllers System	CONTROLLEI CONTROLLEI Cles Cles Cles AP PEFNG RFP ACR	ACCESS PO	CLIENT CL	STATUS ALERTS ALERTS O O O O O O O O O O O O O	External license server External license server Kay 03 2021 May 03 2021 May 03 2021 Not Licensed	adm adm control of the second s	in ∨ hanges ¢ + Ⅲ
Mobility Master > Mobility Master > Aruba Mobility Master Aruba-MM1 Managed Network (0)	Configuration Roles & Polit Authenticati Services Interfaces Controllers System License	CONTROLLEI 0 0 0 Cles cles on Licens AP PEFNG RFP ACR WebCC	ACCESS PO	CLIENT CL	STATUS C Active C Not Licensed D Not Licensed	External license server External license server Kay 03 2021 May 03 2021 May 03 2021 Not Licensed Not Licensed	adm adm control of the second s	in ~ hanges (+
Mobility Master Mobility Master Aruba Mobility Master Aruba-MM1 Managed Network (0)	AMASTER Configuration Roles & Poli Authenticati Services Interfaces Controllers System License Redundance	CONTROLLEI O 0 0 Licens AP PEFNG RFP ACR WebCC MM	ACCESS PO	CLIENT CL	S ALERTS 0 ALERTS 0 O 0 O 0 O 0 O 0 O 0 O 0 O 0 O	External license server EXPIRATION May 03 2021 May 03 2021 Not Licensed Not Licensed May 03 2021	adm Pending Cl • Manual Image: Cl • Manual Image: Cl	in ∨ hanges ¢ + Ⅲ
Mobility Master > Aruba Anobelity Master > Anobelity Master Aruba-MM1 Managed Network (0)	Configuration Roles & Polit Authenticati Services Interfaces Controllers System License Redundancy	CONTROLLEI 0 0 0 Licen Licen AP PEFNG RFP ACR WebCC MM MCVA-	RW CCESS PO	CLIENT CL	S ALERTS P 0 ALERTS OT POrtal (ASP) STATUS O Active O Active O Not Licensed O Active O Not Licensed O Active O Not Licensed	External license server EXPIRATION May 03 2021 May 03 2021 May 03 2021 Not Licensed Not Licensed May 03 2021 Not Licensed	adm adm compared compared	in ∨ hanges ¢ + Ⅲ
Mobility Master > Aruba-MM1 Managed Network (0)	Configuration Roles & Polit Authenticati Services Interfaces Controllers System License Redundancy	CONTROLLEI 0 0 0 Licen Licens AP PEFNG REP AC WebCCC MM MCVA-	RV CES PO	CLIENT CL	S ALERTS P 0 ALERTS O O O O O O O O O O O O O O O	External license server EXPIRATION Kay 03 2021 May 03 2021 May 03 2021 Not Licensed May 03 2021 Not Licensed Not Licensed Not Licensed Not Licensed Not Licensed Not Licensed	adm adm compared compared	in ∽ hanges ¢ + Ⅲ

Aruba-MM	ier I	CONTROLLERS A	CCESS POINTSCLIENTS00000000	ALERTS		? ad
← Mobility Master >	Pending Changes				1	Pending
Ek a					ense server	Manı
🗁 Mobility Master	Pending Changes for 1 G	roup				
📼 Aruba-MM1	🔽 🕣 Mobility Master (0 0	Controller)				INCTALLED
🗂 Managed Network (0)					I.	to this Mobility Master
			Close Discard cha	nges Deploy changes		10
	Controllors	I LING		Niay 05 202	61	10
	Controllers	RFP	RF Protect(WIP,Spectru 📀 A	ctive May 03 202	21	10

Once you have added your licenses, you should see all four license types (AP, PEF, RFP, WebCC) enabled.

🗲 Mobility Master >									
€ , Q	Configuration	License management: O Aruba	Support Porta	al (ASP)	🔿 Exte	rnal license s	server	🖲 Manua	al
🔁 Mobility Master	Roles & Policies	License Lisage License Inventory							
🗁 Managed Network (2)	Authentication		AP	PEF	RF Protect	ACR	WebCC	VIA	MM
🗁 Lab (2)	Services		Access Points	Policy Enforcement Firewall	Wireless Intrusion Protection	Advanced Cryptography	Web Content Classification	Virtual Intranet Access	Mobility Master
5 7008-1	Interfaces	⊖ Global License Pool	0/10	0/10	0/10	0/0	0/10	0/0	2/10000
5008-2	Controllers	😑 Lab	0	0	0	0	0	0	2
	System	□ 7008-1	0	0	0	0	0	0	1
	License	☎ 7008-2	0	0	0	0	0	0	1
	Redundancy	Usage for Global License Pool							
			AP	PEF	<mark>RF Protect</mark>	ACR	WebCC	VIA	MM
		Feature Enabled							
		Scope	Per-AP	Per-AP	Per-AP	Per-Session	Per-AP	Per-Session	Per-Device
		Pool Size	10	10	10	0	10	0	10000
		Expired Licenses	0	0	0	0	0	0	0

Now we'll add the controllers/ managed devices (MDs). This configuration is for Local controller IPSec keys that all the controllers use to connect to MM. Otherwise you need to specify them individually.

	TER CO 1 G	ONTROLLERS ACCE 0 0	SS POINTS C	LIENTS ALER	0	C	3) admin 🗸	
🗲 Mobility Master >								Ŷ
€ _k c	Configuration	Local Controller	IPsec Keys					
🗁 Mobility Master	Roles & Policies	IPV4 ADDRESS OF T	IPV6 ADDRESS OF T	KEY	MAC ADDRESS OF T	CERT TYPE		
📼 Aruba-MM1	Authentication	0.0.0.0		******		-		
🗁 Managed Network (0)	Services							
🗀 Lab (0)	Interfaces							
	Controllers	+						
	System							
	License							
	Redundancy							

Also note that we have created a folder under Managed Network called Lab. There is a feature called autopark which when enabled makes MD adoption much easier, especially if you have a task of bringing up multiple MDs into the MM. This feature automatically parks the MDs under any node below /md

So now when the controllers get adopted by the MM, it will be added under "/md/Lab"

🗧 Mobility Master 🤌			
		General Admin AirWave CPSec Certificates SNMP Logging	Profiles 💙
	Authentication	> Basic Info	
Managed Network (2) Eab (2)		> Domain Name System	
		Auto-parking Auto-parking for controllers:	
		Folder for auto-parking: Managed Network > Lab 💙	
	Redundancy	> Aruba Support Portal (ASP)	

Next, we'll configure NTP and DNS for the Lab folder

Managed Network > Lab >										
Dashboard	General Adm	in AirWave	CPSec	Certificates	SNMP	Logging	Profiles	More		
Configuration						00.0				
WLANs	 Basic Info 									
Roles & Policies	Clock									
Access Points	Set clock:	Set clock: Using NTP 🗸								
AP Groups	Time zone:	Australia:	Australia: Australia/Melbourne (UTC+1, *							
Authentication										
Services		NTP Serv	ers							-
Interfaces		1P ADDR	55	IBURST MC	DDÉ	AUTHEN	ITICATION K	YID		ш
Controllers		210.239.	13.4	165						
Isystem										
Managed Network > Lat	• >									
Dashboard	General	Admin	AirWave	CPSec	Certific	ates SN	IMP L	ogging	Profiles	More
Configuration		-								
WLANs	Basic I	nfo								
Roles & Policies	> Clock									
Access Points	> Doma	in Name Svs	tem							
AP Groups	ID	lomain lookun								
Authentication	IF V	iomanniookup.								
Services	D	NS Servers								
Interfaces	IF	VERSION			П	IP ADDRESS				
Controllors	IF	₩4			1	92.168.1.130				
Controllers										
System										

We'll also configure SNMP, so Airwave can manage/monitor it

Aruba-MM1	rer.	CONTROLLERS ACCESS POINTS CLIENTS ALERTS ○ 2 ○ 0 ○ 1 ○ 0 ○ 1 ○ 0 △ 0	admin ~
🗲 Mobility Master >			
C Mobility Master Imaged Network (2) Lab (2) Imaged Network (2) 7008-1 Imaged Network (2) 7008-2	Configuration Roles & Policies Authentication Services Interfaces Controllers System License Redundancy	General Admin AirWave CPSec Certificates SNMP Logging Profiles Whitelist More Community string for SNMPv1 and SNMPv2 thesagest	
← Mobility Master > ← Mobility Master ← Managed Network (2) ← Lab (2) ← Zene 1	Configuration Roles & Policies Authentication Services	General Admin AirWave CPSec Certificates SNMP Logging Profiles Whitelist More New community string Name:	
C 7008-1 C 7008-2	Interfaces Controllers System License Redundancy	Users for \$NMIPv3 AUTHENTICATION PROTOCOL PRIVACY PROTOCOL + Enable trap generation: Image: Comparison of the second of the	
		IP ADDRESS VERSION COMMUNITY/USERN PORT RETRY TIMEOUT INFORM 192.168.1.15 SNMP-2c thristogreat 162 - - -	

And then enabling the AirWave connectivity for MM and MDs

🗲 Mobility Master >										
€ k Q	Configuration	General Admin	AirWave	CPSec	Certificates	SNMP	Logging	Profiles	Whitelist	More
🗁 Mobility Master	Roles & Policies			_						
📼 Aruba-MM1	Authentication	Connect to AirWave:								
合 Managed Network (2)	Services	Airwave IP address:	192.168.1	.15						
🔁 Lab (2)	Interfaces	SNMP version:	v2	~						
5008-1	Controllers	Community string:	thisisgreat		~					
5008-2	System									
Managed Network > Lab >										
€ <mark>,</mark>	Q Dashboard	General A	dmin A	irWave	CPSec Ce	ertificates	SNMP	Logging	Profiles	More
🔁 Mobility Master	Configuration									
📼 Aruba-MM1	WLANs	Connect to Air	rWave:							
🔁 Managed Network (2)	Roles & Policies	Airwave IP ad	dress:	192.168.1.1	15					
🗁 Lab (2)	Access Points	SNMP version		v2 🗸						
5 7008-1	AP Groups	Community st	tring:	thisisgreat	~					
5008-2	Authentication	,								
	Services									
	Interfaces									
	Controllers									
	System									

And enabling a few services to send their data to Airwave.



Aruba APs will create a IPSEC tunnels as an overlay to the controller or cluster of controllers. So, you need to ensure all the needed VLANs are configured at the controller end. And the port that connects to the controllers are configured for VLAN trunking.

Configuring employee, staff, and students VLANs. The aim here is that after authentication, if the users don't match the user group of staff or students then they are put into employee VLAN

■ Managed Network > Lab >							
Dashboard	Ports	VLANs	IP Routes	GRE Tunnels	Pool Management	OSPF	Multicast
Configuration					5		
WLANs	VLA	Ns					
Roles & Policies	NAM	IE			ID(S)		
Access Points	staff	-VLAN			20		
AP Groups	Emp	loyee-VLAN			12		
Authoptication	Stud	ent-VLAN			30		
Adhenication					1		
Services	+						
Interfaces							

Make the port 0/0/0 as Trunk port with native VLAN as VLAN1

Managed Network > Lab >													
Dashboard	Ports	VLANs	IP Route	es GR	E Tunnels	Poo	l Managemen	t OSPF	Multicast				
Configuration													
WLANs	Port C	hannel											
Roles & Policies	NAME		MEMBERS	;	PROTOCOL		TRUSTED	POLICY	мо	DE	NATIVE VLA	N TI	RUNK VLANS
Access Points													
AP Groups													
Authentication													
Services	+												
Interfaces													
Controllers	Ports												
System	PORT	ADMI	N ST T	RUSTED	POLICY	MODE	NATIVE V	L ACCESS VL	TRUNK VL	SPANNIN	MONITOR	DESCRIPTI.	-
Tasks	GE-0/0	/0 Enabl	ed	~	Not-defin	trunk	1	1	1-4094	v	-	GE0/0/0	Ū
Redundancy	GE-0/0	/1 Enable	ed	~	Not-defined	access	1	1	1-4094	~		GE0/0/1	
Reduitdancy	GE-0/0	/2 Enable	ed	~	Not-defined	access	1	1	1-4094	~		GE0/0/2	
юТ	GE-0/0	/3 Enable	ed	~	Not-defined	access	1	1	1-4094	~		GE0/0/3	
Maintenance	GE-0/0	/4 Enable	ed	~	Not-defined	access	1	1	1-4094	~		GE0/0/4	

■ Managed Network > Lab >				
Dashboard	Ports VLANs IP Re	outes GRE Tunnels	Pool Management	OSPF Multicast
Configuration	GE-0/0/0			
WLANs	Admin state:			
Roles & Policies	Admini state.			
Access Points	Speed:	auto 🗸 Mbps		
AP Groups	Duplex:	auto 💙		
Authentication	PoE:			
Services	Trust:	\checkmark		
Interfaces	Policy:	Not-defined	~	
Controllers	Mode:	Trunk 🐱		
System	Native VLAN:	1 🗸		
Tasks	Allowed VLANs:	Allow all	~	
Redundancy		GE0/0/0		
IoT	Description:			
Maintenance				

Also note that you can configured LACP and aggregate the two or more interfaces together. This is not shown here. Lastly enable firewall visibility, deep packet inspection and Web content classification.

Managed Network > Lab >		
Dashboard	Clusters AirGroup VPN Firewall IP Mobility External Services DHCP WAN	
Configuration WLANS Roles & Policies Access Points AP Groups Authentication Services Interfaces Controllers System	Rate limit CP IKE traffic (pps):	
Managed Network > Lab >		Pending Changes
Dashboard Configuration WLANS Roles & Policies Access Points AP Groups Authentication Services Interfaces Controllers System Tasks	Clusters AirGroup VPN Firewall IP Mobility External Services DHCP WAN Rate limit CP IKE traffic (pps): Jumbo frames processing: Jumbo frames processing: Bark management frames: Enable frewall visibility: Enable deep packet inspection: Enable deep packet inspection: Connect to classification server using: IPV4 v Drop packets during web content cache miss: URL to redirect blocked sessions: Enable IP classification and reputation:	

For this we need to reload the MDs it they are already connected to the MM.

5 Controller Configuration

Once you power up the controllers that are in default state connect through the serial console and you'll see the following starting with "Auto-provisioning". There are many ways to auto provision them, here we'll do the basic configuration so it can join the mobility master and then all the configuration will be done from the MM.

Auto-provisioning is in progress. It requires DHCP and Activate servers Choose one of the following options to override or debug auto-provisioning... 'enable-debug' : Enable auto-provisioning debug logs 'disable-debug' : Disable auto-provisioning debug logs 'mini-setup' : Start mini setup dialog. Provides minimal customization and requires DHCP server 'full-setup' : Start full setup dialog. Provides full customization 'static-activate' : Provides customization for static or PPPOE ip assignment. Uses activate for master information

Enter Option (partial string is acceptable): full-setup

Current choices are:

Are you sure that you want to stop auto-provisioning and start full setup dialog? (yes/no): yes

Commands: <Enter> Submit input or use [default value], <ctrl-I> Help <ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end <ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line <ctrl-P> Previous question <ctrl-X> Restart beginning <ctrl-R> Reload box

Enter System name [Aruba7008]: 7008-2 Enter Switch Role (standalone|md) [md]: Enter IP type to terminate IPSec tunnel (ipv4|ipv6) [ipv4]: Enter Master switch IP address or FQDN: 192.168.1.55 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]: Enter Uplink port [GE 0/0/0]: Enter Uplink port mode (access|trunk) [access]: Enter Uplink Vlan IP assignment method (dhcp|static|pppoe) [static]: Enter Uplink Vlan Static IP address [172.16.0.254]: 10.10.10.5 Enter Uplink Vlan Static IP netmask [255.255.255.0]: Enter IP default gateway [none]: 10.10.10.1 Enter DNS IP address [none]: 192.168.1.1 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: AU You have chosen Country code AU for Australia (yes|no)?: yes Enter the controller's IANA Time zone [America/Los Angeles]: Australia/Melbourne Enter Time in UTC [12:53:36]: Enter Date (MM/DD/YYYY) [2/2/2021]: 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: *******

System name: 7008-2 Switch Role: md IP type to terminate IPSec tunnel: ipv4 Master switch IP address or FQDN: 192.168.1.55 Is this VPN concentrator: no Connect via VPN concentrator: no IPSec authentication method: PSKwithIP Vlan id for uplink interface: 1 Uplink port: GE 0/0/0 Uplink port mode: access Uplink Vlan IP assignment method: static Uplink Vlan static IP Address: 192.168.1.57 Uplink Vlan static IP net-mask: 255.255.255.0 Uplink Vlan IP default gateway: 192.168.1.249 Domain Name Server to resolve FQDN: 192.168.1.130 Option to configure VLAN interface IPV6 address: no Country code: AU IANA Time Zone: Australia/Melbourne Admin account created: yes Note: These settings require IP-Based-PSK configuration on Master switch If you accept the changes the switch will restart! Type <ctrl-P> to go back and change answer for any question Do you wish to accept the changes (yes|no)yes INFO: Backing up existing config dir. Creating configuration... Done. System will now restart! [12:55:07]:Starting rebootme [12:55:07]:Shutdown processing started

Now we see that both the controllers show up on MM

6 Mobility Master Configuration

Here we have done the previous process for two MDs and they have end up on the MM dashboard and have now got the basic configuration tat we did earlier for the "Lab" folder.

Aruba-MM1	ER	CONTROLLERS ⊙ 2 ① 0	ACCESS POINTS	CLIENTS	ALERTS			admin 🗸	
Managed Network >							🖏 Search		0,
ି Mobility Master	Dashboard Overview	← = 2	ê <mark>0</mark>	æ 2	•• 0				6
📼 Aruba-MM1	Infrastructure	Controllers 2	filtered by Status Up	• ×				∇	iii
🗁 Managed Network (2)	Traffic Analysis	NAME 🔺	STATUS	HEALTH	UPTIME	SOFTWARE	ACCESS	CLIENTS	
🗁 Lab (2)	Security	> 7008-1	⊘ Up	III Good	1h 36m	8.6.0.7	0	0	
= 7008-1	Services	> 7008-2	⊘ Up	III Good	1h 36m	8.6.0.7	0	0	
5008-2	Configuration								
	Maintenance								

Now from the MM's device view, we'll configure the IP addresses for VLAN1, 12, 20 and 30. The aim of hierarchical configuration through folder is that most of the configuration will be done at the folder level and device specific configuration to be done at the device level.

Managed Network > Lab > 7008	-1 i) Version 8.6.0.7										Ś
€ <mark>,</mark> Q	Dashboard		B Routos		abore	CDE Tur	nolc	Real Ma	aaromon	+ ~	
🗁 Mobility Master	Configuration		S IF ROULES	IF VO INEIGI	10015	GRE TUI	IIICIS	FUUI IVIAI	lagement		
📼 Aruba-MM1	WLANs	VLANs									
🗁 Managed Network (2)	Roles & Policies	NAME		ID(S)							
🗁 Lab (2)	Access Points	staff-VLAN		20							
5008-1	AP Groups	Student-VLAN		30							A -
5 7008-2	Authentication	-		1							Ø Ш
	Services	+									
	Interfaces										
	Controller	VLANs \	LAN IDs Optio	ns							
	System	ID IP	/4 ADDRESS	IPV6 A	ENAB	PORT	ADMI	OPERA	PD CLI	DHCP	
	Tasks	1 19	2.168.1.57/255.255.255	.0		0/0/0,	Enabled	N/A	Disabl	None	
Managed Network > Lab > 7008	-1 (i) Version 8.6.0.7										Ğ
ମ୍ <mark>ଟି</mark> ପ	Dashboard		ID Boutos		bborg	CDE TU	ppole	Pool Ma	nagomor	at v	
🔁 Mobility Master	Configuration	POILS VLAN	s if Roules	IFV0 Neig	10012	GRE TU	TITIEIS	FUULING	inagemen	n •	
📼 Aruba-MM1	WLANs	VLANs									
🔁 Managed Network (2)	Roles & Policies	NAME		ID(S)							
🗁 Lab (2)	Access Points	staff-VLAN		20							
5008-1	AP Groups	Student-VLAN		30				()			Ø
5008-2	Authentication			1							
	Services	+									
	Interfaces										
	Controller	VLANs > Stud	lent-VLAN VL	AN IDs O	Options						
	System	ID IP	V4 ADDRESS	IPV6 A	ENABL	PORT	ADMI	OPERA	PD CLI	DHCP	
	Tasks	30 10	0.10.30.2/255.255.255.0			0/0/0	Enabled	N/A	Disabled	None	

Managed Network > Lab > 7008	-1 (i) Version 8.6.0.7												¢
€ <mark>k</mark> Q	Dashboard	Dort		ID Doutos		aighborg		nnola	Deel Ma		+ v		
🔁 Mobility Master	Configuration	Porte	VLAINS	IP ROULES	IPVOIN	eignoors	GRE TU	meis	POOLINIA	nagemen	ι 🔹		
📼 Aruba-MM1	WLANs	v	LANs										
🗁 Managed Network (2)	Roles & Policies	N	AME		ID(5)						ſ	⊞
🔁 Lab (2)	Access Points	s	taff-VLAN		20				()			Ø	
5008-1	AP Groups	S	tudent-VLAN		30								
5 7008-2	Authentication	-			1								
	Services	-	-										
	Interfaces												
	Controller	v	LANs > staff-	VLAN VLAN	Ds C	options							
	System	П	D IPV	4 ADDRESS	IPV6 A	ENABL	PORT	ADMI	OPERA	PD CLI	DHCP		
	Tasks	2	0 10.1	0.20.2/255.255.255.0			0/0/0	Enabled	N/A	Disabled	None		
Managed Network > Lab > 7008-	-1 i Version 8.6.0.7												(Y
<u>ମ୍</u> ଟ୍ୟୁ ସ୍	Dashboard	Porte		IR Poutos		loighborg	CDE T	unnols	Pool M	nagomor	at v		
🗀 Mobility Master	Configuration	POILS	VLANS	IF ROULES	IPVOI	ieigi iboi s	GRE II	IIIIEIS	POULINI	anagemei			
🔁 Managed Network (2)	WLANs	v	LANs										
🔁 Lab (2)	Roles & Policies	N	AME		ID(5)							
5008-1	Access Points	s	taff-VLAN		20								^
5 7008-2	AP Groups	s	tudent-VLAN		30								-11
	Authentication	E	mployee-VLAN		12				U			Ø	-
	Services	-	_		1								~
	Interfaces												
	Controller	v	LANs > Emplo	oyee-VLAN V	LAN IDs	Options	5						
	System	10	D IPV	ADDRESS	IPV6 A	ENABL	PORT	ADMI	OPERA	PD CLI	DHCP		
	Tasks	1	2 10.1	0.12.2/255.255.255.0			0/0/0	Enabled	N/A	Disabled	None		

We are going to create couple of AP-groups, you can then put various APs in each group, and they would have their own specific WLAN settings.

Managed Network > Lal	b >		
Dashboard	AP Groups 4		
Configuration	NAME	APs	
WLANs	default	-	
Roles & Policies	NoAuthApGroup		
Access Points	Building1	-	
AP Groups	Building2	-	
Authentication	· · · · · · · · · · · · · · · · · · ·		

Also enable auto certificate provisioning of the APs.

aruba	MOBILITY MA Aruba-MI	ASTER M1		co ⊘	NTROLLERS	ACCESS POI	INTS	CLIENTS ♡ 0 ∞ 0	ALERTS	
Managed Netwo	rk > Lab >									
Dashboard		General	Admin	AirWave	CPSec	Certificates	SNMP	Logging	Profiles	More
Configuration WLANS Roles & Policies Access Points AP Groups Authentication Services Interfaces Controllers		 Control Enab Enab Only 	Plane Sect le CPSec: le auto cert accept APs f	urity provisioning: rom specified r	ranges: C					

You need to enable the following as well to be able to see the classification and WebCC info in the MD dashboard as well as in Airwave.

🗲 Mobility Master 👌		
 Mobility Master > Mobility Master Mobility Master Aruba-MM1 Managed Network (2) Lab (2) 	Configuration Roles & Policies Authentication Services Interfaces Controllers System	Clusters VPN Firewall Guest Provisioning AirMatch IoT Rate limit CP trusted mcast traffic (pps): 1953 1953 Rate limit CP route traffic (pps): 976 Rate limit CP session mirror traffic (pps): 976 Rate limit CP VRRP traffic (pps): 512 Rate limit CP ARP traffic (pps): 976
	License Redundancy	Rate limit CP I2 protocol/other traffic (pps):976Rate limit CP auth process traffic (pps):976Rate limit CP IKE traffic (pps):1953Jumbo frames processing:1953Jumbo frames processing:Mark management frames:Enable deep packet inspection:Enable web content classification:Connect to classification server using:IPv4 Drop packets during web content cache miss:URL to redirect blocked sessions:Enable IP classification and reputation:

6.1 Dot1x Wireless Configuration

We'll go through the Task wizard to set this up. We are going to create a dot1x WLAN that uses ClearPass as the Authentication server.

Managed Network > Lab >		
€ ,	Dashboard	Tasks
🔁 Mobility Master	Configuration	
🔁 Managed Network (2)	WLANs	Deploy New Access Points
🗁 Lab (2)	Roles & Policies	Create a new WLAN
5008-1	Access Points	 Define Wireless Intrusion Protection (WIP) policy
5008-2	AP Groups	→ Bulk configuration upload
	Authentication	→ Install new software
	Services	→ Reboot controllers
	Interfaces	Show upgrade status
	Controllers	
	System	
	Tasks	
	Redundancy	
	IoT	
	Maintenance	
Dashboard	New WLAN	

WLANS	General		VLANs	Security	Access
Roles & Policies				2	
Access Points	Name (SSID):	school			
AP Groups	Primer (3310).		Cuert		
Authentication	Primary usage:	Employee	Guest		
Services		Select AP Groups	~		
Interfaces	Broadcast on:	default	^		
Controllers		Building2	~		
System	Forwarding mode:	Tunnel	~		

Dashboard

Configuration

WLANs Roles & Policies Access Points AP Groups

Authentication

New WLAN





New WLAN



Cancel

Reauth interval:

Submit

1440

min. 🗸

Dashboard

Shared key:

Retype key:

Timeout:

•••••

•••••

Open

5

Less

abriboura				
	General	VLANs	Security	Access
WLANS				
Roles & Policies				
Access Points	More Secure	Key management:	WPA2-Enterprise 💙	
AP Groups	Steart		ClearPass	
Authentication	Enterprise			
Services				
Interfaces	Personal	Auth servers:		
Controllers	i ci sonai		+	
System	Open			
	, i	Reauth interval:	1440 min. 🗸	
Redundancy	Less			
IoT	Secure	Machine authentication:	Disabled 💙	
laintenance		Blacklisting:	0	

New WLAN

		_		_
WLANS	General	VLANs	Security	Access
Roles & Policies				
Access Points	Default relay	quest		
AP Groups	Deraut role.			
Authentication	Server-derived roles:	Lice value returned from	clearDace or other auth conver	
Services	Derivation method:	Use rules defined in table	below	
Interfaces	Show roles			
Controllers				
Managed Network > Lab >				Pending Changes 🗘
Dashboard	New WLAN			

Dashboard New WLAN Configuration The new WLAN can be viewed in the WLAN List WLANs The new WLAN can be viewed in the WLAN List Roles & Policies NOTE: The new WLAN has been added to the pending changes list. To deploy all pending changes, click Pending Changes at top right.

Managed Network > Lab >		Configuration De	ployment Status		
Dashboard	Tasks	Update for 2	Managed Controller(s)		
Configuration		opulle for 2	managea controner(s)		
	Deploy New /	TARGET	NODEPATH	STATUS	MESSAGE
WLANS	Croate a pow	7008-2	Managed Network	\odot	
Roles & Policies		7008-1	Managed Network	\odot	
Access Points	→ Define Wirel€		0	Ŭ	
AP Groups	→ Bulk configur				
Authentication	→ Install new sc				
Services	→ Reboot contr				
Interfaces	🔺 Show upgrad				Close

Make sure to submit and apply changes.

Managed Network > Lab >											¢)
Dashboard	AP Groups 4										
Configuration	NAME			4	\Ps						
WLANs	default			1	I						^
Roles & Policies	NoAuthApGroup			-	-						_
Access Points	Building1				-						Ō
AP Groups Authentication	Building2				-						~
Services	AP Groups > Building1	APs	WLANs	Radio	Mesh	LMS	М	ultiZone	ΙοΤ		
Interfaces	NAME	AP GROU	Р	A	IRTIME LIMIT	(%)		PER-USER L	LIMIT (KBPS)	PER-RADIO LIMIT (KBPS)	=
Controllers	school	Building1	1	-				-		•	Ū

Now you can connect the APs, we'll not be covering the discovery process that APs use, but since the APs are not sharing L2 adjacencies with the controllers, we'll use the DNS method. Here you'll notice that the new AP has ended up in default ap-group.

aruba	MOBILITY MAS Aruba-MM	TER 1	co ©	NTROLLERS ACC 2 ○ 0 ⊘	ESS POINTS 0	CLIENTS ALE	RTS O		admin 🗸	
Managed Netwo	ork >							🔄 Search		٥,
)ashboard Overview			rs Etred by Status Up X	1 Access Device	2 Uplinks		0 Clusters		∇	iii
Traffic Analysis Security		NAME > 20:4c:03:5c:05:6e	STATUS	CLIENTS 0	UPTIME 1h 9m	MANAGED BY	GROUP default	MODEL 303H		
Services										

Notice that the AP has landed on 7008-1 because "aruba-master" resolves to that IP address. If we had enabled clustering, then after AP's initial contact to 7008-1 it would also learn the IP address of the 7008-2 controller. More

about that later. Note that the best practice is to point the "aruba-master" DNS resolution to VRRP VIP address that covers two or more controllers.

Anyway, we'll select this AP and move to builling1 AP-group

Jashboard	Campus APs Remote APs Mesh APs Whitelist Provisioning Rules	
onfiguration		
WLANs	Campus APs 1	Q
Roles & Policies	AP NAME AP GROUP IPV4 ADDRESS IPV6 ADDRESS SWITCH IP MAC ADDRESS SERIAL # TYPE	FLAGS
Access Points	✓ 20:4c:03:5c:05:6e default 10.10.10.20 - 192.168.1.57 20:4c:03:5c:05:6e CNHVK2R42H 303H	2
AP Groups		
Authentication		
Services		
Interfaces		
Controller	Provision 50 ×	< 1 →
System	Flags:	
Tasks	U = Unprovisioned, N = Duplicate name, G = No such group, L = Unlicensed, I = inactive, D = Dirty or no config. E = Regulatory Domain Mismatch, X = Maintenance Mode in AP, s = LACP striping, R = Remote AP, R = Remote AP requires Auth, C = Cellular RAP, c = CRET-Based RAP, I = 802, I x use E forder sector 2. Under Version 2. Under Sector D R = Estending works and the Sector Sector RET Resource Londong e - Durder V = Auch and	, P = PPPOE AP, B = Bu ST, 1 - = 802.1x use
Dedundance	Datazone AP, \mathbf{e} = Custom EST cert, \mathbf{p} = In deep-sleep status, \mathbf{A} = Using WiFi uplink, \mathbf{r} = Power Restricted, \mathbf{T} = Thermal ShutDown, \mathbf{F} = AP failed 802.1x authentication	, r – Mesii Recovery, z
Managed Network > Lab >	2008-1 🕕 Version 8.6.0.7	
ashboard		
	Campus APs Remote APs Mesh APs Whitelist Provisioning Rules	
	Provision 50	✓ < 1
MLANS		
Roles & Policies	20:4c:03:5c:05:6e	
AP Groups	MAC address: 20:4c:03:5c:05:6e	
Authentication	Name: 20:4c:03:5c:05:6e	
	AP group: Building1 V	
Interfaces	Controller discoven	
	Controller discovery preference:	
	IP: (•) DHCP () Static	
Tasks	IP: • DHCP Static	
Tasks Redundancy	IP: Deployment: Campus Remote Mesh Remote Remote Deployment:	
Tasks Redundancy aintenance	IP: • DHCP Static Deployment: • Campus Remote WI-Fl uplink:	
Tasks Redundancy Intenance Managed Network > Lab > 7	IP: • DHCP • Static Deployment: • Campus • Remote WI-FI uplink: 7008-1 • Access Points will be Pabooted	
Tasks Redundancy Jintenance Managed Network > Lab > 7 Shboard	IP: • DHCP • Static Deployment: • Campus • Remote Wi-Fi uplink: • Access Points will be Rebooted	
Tasks Redundancy aintenance Managed Network > Lab > 7 shboard nfiguration	IP: • DHCP • Static Deployment: • Campus • Remote Wi-Fl uplink: • Campus 7008-1 Version 8.6.0.7 Campus APs Remot CAUTION: Applying this configuration change will	
Tasks Redundancy Intenance Managed Network > Lab > 7 Shboard nfiguration WLANS	IP: • DHCP • Static Deployment: • Campus • Remote Wi-Fi uplink: • Campus 7008-1 Version 8.6.0.7 Campus APs Remot CAUTION: Applying this configuration change will interrupt service while the affected Access Points are	
Tasks Redundancy Intenance Managed Network > Lab > 7 Shboard Infiguration WLANS Roles & Policies	IP: • DHCP • Static Deployment: • Campus • Remote Wi-Fi uplink: • Campus 7008-1 Version 8.6.0.7 Campus APs Remot CAUTION: Applying this configuration change will interrupt service while the affected Access Points are rebooted.	< 1 >
Tasks Redundancy Intenance Managed Network > Lab > 7 Shboard Infiguration WLANs Roles & Policies	IP: • DHCP • Static Deployment: • Campus • Remote Wi-Fi uplink: • Campus 7008-1 Version 8.6.0.7 Campus APs Remot CAUTION: Applying this configuration change will interrupt service while the affected Access Points are rebooted. Do you want to continue ? Do you want to continue ?	
Tasks Redundancy Intenance Managed Network > Lab > 7 Shboard Infiguration WLANs Roles & Policies Access Points	IP: • DHCP • Static Deployment: • Campus • Remote Wi-Fi uplink: • Campus 7008-1 Version 8.6.0.7 • Campus APs remot • 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 ?	
Tasks Redundancy Redundancy Intenance Managed Network > Lab > 7 shboard Infiguration WLANs Roles & Policies Access Points AP Groups Utables	IP: Deployment: W-Fi uplink: Campus APs Remot Provision CAUTION: Applying this configuration change will interrupt service while the affected Access Points are rebooted. Do you want to continue ? MAC address: Cancel Continue & Reboot	
Tasks Redundancy Intenance Managed Network > Lab > 7 shboard figuration WLANs Roles & Policies Access Points AP Groups Authentication	IP: Deployment: W-Fi uplink: Campus APs Remot Provision 20:4c:03:5c:05:6e MAC address: Name: 20:4c:03:5c:05:6e Marcel Cancel Continue & Reboot Cancel Continue & Reboot Continue & Reboot Continue & Reboot	
Tasks Redundancy Intenance Managed Network > Lab > 7 shboard figuration WLANS Roles & Policies Access Points AP Groups Authentication Services	IP: Deployment: W-Fi uplink:	
Tasks Redundancy Redundancy Intenance Managed Network > Lab > 7 Shboard figuration WLANs Roles & Policies ACCess Points AP Groups Authentication Services Interfaces	IP: Deployment: W-Fi uplink:	
Tasks Redundancy Intenance Managed Network > Lab > 7 Shboard figuration WLANS Roles & Policies Access Points AP Groups Authentication Services Interfaces Controller	IP: Deployment: W-Fi uplink:	
Tasks Redundancy Redundancy Intenance Managed Network > Lab > 7 Shboard figuration WLANs Roles & Policies AP Groups Authentication Services Interfaces Controller System	IP: Deployment: W-Fi uplink: 7008-1 ○ Version 8.6.0.7 Campus APs Remot CAUTION: Applying this configuration change will interrupt service while the affected Access Points are rebooted. Do you want to continue ? MAC address: Name: 20:4c:03:5c:05:6e MAC address: Name: 20:4c:03:5c:05:6e AP group: Building1 ♥ Controller discovery: © Use AP discovery protocol (ADP) Static Controller discovery preference: Provision Provision Do you want to continue 8 Reboot	
Tasks Redundancy Redundancy Intenance Managed Network > Lab > 7 Hanaged Network > Lab > 1 Hanage	IP: Deployment: Wi-Fi uplink:	
Tasks Redundancy Redundancy intenance Managed Network > Lab > 7 shboard figuration WLANs Roles & Policies Access Points AIP Groups Authentication Services Interfaces Controller System Tasks Redundancy	IP: Deployment: Wi-Fi uplink:	

Now when the AP reboots, it will be in building1 ap-group and will broadcast "school" SSID.

Here we'll create the user roles that ClearPass will pass to MDs based on the policies that will be configured

Managed Network > Lab	>	
Dashboard	Roles Policies Applications Alias	es
Configuration		
WLANs	Roles 14	
Roles & Policies	NAME	RULES
Access Points	logon	32 Rules
AP Groups	guest	11 Rules
Authentication	ap-role	35 Rules
Services	stateful-dot1x	0 Rules
Interfaces	sys-ap-role	24 Rules
Controllers	sys-switch-role	24 Rules
System	+	
Managed Network > Lab >	New Role	
Dashboard	Roles Polic Name: Staff	
Configuration		
WLANS	Roles 16	Cancel
Roles & Policies	NAME	
Access Points	denyall 1 R	tules

Managed Network > Lab >								
Dashboard	Roles Policies A	Applications Aliases						
Configuration								
WLANs	Roles 16							
Roles & Policies	NAME		RULES					
Access Points	denyall		1 Rules					
AP Groups	default-via-role		3 Rules					
Authentication	default-vpn-role		4 Rules					
Services	authenticated		4 Rules					
Interfaces	voice		43 Rules					
	<mark>Staff</mark>		0 Rules					
Controllers	<mark>Studen</mark> t		0 Rules					
System	+							

We'll just add a "allow-all" policy to both user roles.

Managed Network > Lab >	Nev	v Policy			
Dashboard	Roles Polic				
Configuration	derault-via-role	Add an existing policy	Create a new policy		
WLANs	default-vpn-rol	Policy type:	Session 🗸		
Roles & Policies	authenticated	Policy name:	allowall	~	
Access Points	Staff	Position:			
AP Groups	Student				
Authentication	+		Cance	al Submit	
Services	_				
Interfaces	Staff Policie	es Bandwidth Capti	ve Portal More		Show Basic View
Controllers	NAME	RULES COUNT	TYPE	POLICY USAGE	III
System	global-sacl	0	session	logon, guest, ap-role, stateful-dot.	
Tasks	apprf-staff-sacl	0	session	Staff	
Redundancy	Staff	0	session	Staff	

Managed Network > Lab >						Pending Changes
Dashboard	Roles Policies Ap	plications A	liases			
Configuration	detault-via-role		3 Rules			
WLANs	default-vpn-role		4 Rules			
Roles & Policies	authenticated		4 Rules			
Access Points	voice		43 Rules			
AP Groups	Staff		2 Rules			
Authoptication	Student		2 Rules			Ш _У
Authentication	+					
Services						
Interfaces	Student Policies	Bandwidth	Captive Portal	More		Show Basic View
Controllers	NAME	RULES COU	JNT	ТҮРЕ	POLICY USAGE	Ħ
System	global-sacl	0		session	logon, guest, ap-role, stateful-dot	^
Tasks	apprf-student-sacl	0		session	Student	
Redundancy	Student	0		session	Student	
IoT	allowall	2		session	default-iap-user-role, default-via	~

Lastly, we'll also assign a VLAN to each role

	Dashboard	Roles Policies Applications Aliases	
🗎 Mobility Master			
🔁 Managed Network (2)	WLANS	Staff 2 Rules	
		Student 2 Rules	~
5008-1	Access Points		
5 7008-2	AP Groups		
	Authentication	Staff Policies Bandwidth Captive Portal More	Show Basic View
		 Network 	
	Interfaces	VI AN:	
	Controllers		
		Re-auth interval: 0 minutes V	
	Tasks	Max sessions: 65535	
	Redundancy	Deep packet inspection:	
	IoT	Web content classification:	
	Maintenance	Youtube education:	

We'll do the same thing for the student user role.

Here we'll configure dynamic authorisation that will use CoA. It is pointing to the same ClearPass

■ Managed Network > Lab >		New Server				
Dashboard Configuration WLANs Roles & Policies Access Points AP Groups Authentication Services	Auth Servers	Type: IP address vers IP address:	Dynamic A sion: IPv4 192.168.1.5 	Authorization IPv6 IPv6	Cancel Subm	Advanced server 1 1 1
Interfaces Controllers System Tasks Redundancy	All Servers 2 NAME ClearPass Internal		TYPE RADIUS	IP ADDRESS / 1 192.168.1.95	HOSTNAME	SERVER GROUP school_dot1_svg default internal

Managed Network > Lab >					Pending Changes 🗘
Dashboard	Auth Servers A	AA Profiles L2 Authentication	L3 Authentication User R	ules Advanced	
	All Servers 3				^
WLANs	NAME	ТҮРЕ	IP ADDRESS / HOSTNAME	SERVER GROUP	
Roles & Policies	ClearPass	RADIUS	192.168.1.95	school_dot1_svg	
Access Points	Internal		-	default internal	
AP Groups	-	RFC 3576	192.168.1.95	-	Ū
	+				
Services					
Interfaces	Server Options				
	Key:	•••••			
Tasks	Retype I	ey:			
Redundancy					
loT					
Maintenance	٢				>
					Cancel

And we'll add rfc3576 sever to the AAA profile for the School WLAN

ashboard	Au	th Servers	AAA Profiles	L2 Authentication	L3	Authentication Use	r Rules Advanced	
onfiguration				•				
WLANs		AAA Profiles				RFC 3576 Server		
Roles & Policies		÷ =	default-dot1x-psk		^		RFC 3576 SERVER	
Access Points		⊕ ⊡	default-iap-aaa-pr	of			192.168.1.95	
AP Groups		⊕ ⊡	default-mac-auth			REC 3576 server		
Authentication		÷	default-open		1			
Services		⊕ Ξ	default-tunneled-u	use			+	
Interfaces		÷	default-xml-api					
Controllers		ΘΒ	school_aaa_prof					
System			📑 802.1X Authe	ntication				
Tasks			📑 802.1X Authe	ntication Server Group				
Redundancy			📑 MAC Authent	ication				
ют			🖻 MAC Authent	ication Server Group				
aintenance	<							

And enable RADIUS accounting, note that we can create a new accounting server group but here we'll sue the same.

Managed Network > Lab >	
Dashboard	Auth Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced
Configuration	
WLANs	AAA Profiles Server Group: school_dot1_svg
Roles & Policies	default-dot1x-psk
Access Points	Gefault-iap-aaa-prof
AP Groups	G default-mac-auth Fail Through:
Authentication	C default-open
Services	
Interfaces	
Controllers	⊙ 🕒 school_aaa_prof
System	B02.1X Authentication
Tasks	802.1X Authentication Server Group
Redundancy	MAC Authentication
IoT	MAC Authentication Server Group
Maintenance	RADIUS Accounting Server Group
	RFC 3576 server
	C XML API server

Now because CoA will need to have a specific IP address of MD (controller), we need to specify that at the device level and as seen here we are assigning 192.168.1.57 as NAS ID.

Managed Network > Lab > 700	8-1 🕕 Version 8.6.0.7						
€ <mark>,</mark> c	Dashboard	Auth Servers AAA Pr	ofiles 12 Authenti	cation 13 Author	atication User Rules	Advanced	
🔁 Mobility Master	Configuration	Addi Scivers 70000			incutori osci itales	Advanced	
🗁 Managed Network (2)	WLANs	Server Groups 3					
🔁 Lab (2)	Roles & Policies	NAME	SERVERS	FAIL THROUGH	LOAD BALANCE	SERVER RULES	(
📼 7008-1	Access Points	default	1	-	-	1	
5008-2	AP Groups	internal	1	-		1	•
	Authentication	school_dot1_svg	1	-	-	1	0
	Services	+					
	Interfaces						
	Controller	Server Group > school_	dot1_svg Servers	Options Serve	er Rules		 Drag rows to re-order
	System	NAME	ТҮРЕ	IP ADDRESS	TRIM FQDN	MATCH RULES	
	Tasks	ClearPass	RADIUS	192.168.1.95	-	0	Ū
	Redundancy						
	Maintenance						
		Server Group > school	dot1_svg > ClearPass	Server Options	Server Group Trim FQDN	Server Group Match Rules	
		Name:		ClearPass			
		IP address / ho	istname:	192.168.1.95			
		Auth port:		1812			
		Acct port:		1813			
		Shared key:		•••••			
		Retype key:		•••••			
		Timeout:		5			
		Retransmits:		3			
		NAS ID:					
		NAS IP:		192.168.1.57			
		Enable IPv6:					
		NAS IPv6:					

Here is the table outlining the user roles and their corresponding VLAN IDs and subnets.

User role	VLAN ID	IP subnet
Staff	20	10.10.20.0/24
Student	30	10.10.30.0/24
Employee	12	10.10.12.0/24

6.2 ClearPass Basic Configuration

In this section we'll do the basic ClearPass configuration and join it to the AD domain. We'll start with NTP and time zone.

Dashboard 0	Administr	ration » Server Manage	r » Server Configuration					
C Monitoring • C Configuration • C Administration •	Serve	r Configuration				♥ Change Clus ♥ Cluster-Wid ♥ Clear Machir ♦ Make Subsc	ster Password e Parameters ne Authentica riber	tion Cache
—						Manage Poli NetEvents T Set Date &	cy Manager Z argets Time	lones
Server Manager						* Virtual IP Se	ttings	
- P Log Configuration	Publishe	er Server: victory [192	.168.1.95]					
- Jucal Shared Folders	#	Server Name 🔺	Management Port	Data Port	Zone	Cluster Sy	nc Last	Sync Time
- Jucensing	1.	victory	(IPv4) 192.168.1.95	-	default	Enabled	-	
- Jevice Insight	Showing	1-1 of 1			Collect Logs Back Up	Restore Cleanup	Shutdown	Reboot
🖘 🖓 External Servers								

Change Date and Tin	ne	8	Change Date and Time		- 6
This will change Date	& Time for all nodes in the cluster:		This will change Date & Tim	ne for all nodes in the cluster:	
Date & Time T	ime Zone on Publisher		Date & Time Time Zo	one on Publisher	
Synchronize time	with NTP server	^	To change the time zon	ne, select your area from the list below:	
Primary Server:			Africa/Abidjan		~
NTP Server	216.239.35.4		Africa/Accra		
Key ID			Africa/Addis_Ababa		
Key Value			Africa/Algiers		
Algorithm			Africa/Asmara		
Algorithm	· · · · ·		Africa/Bamako		
Secondary Server ((1):		Africa/Bangui		
NTP Server			Africa/Banjul		
Key ID			Africa/Bissau		~
Key Value			Current time zone:	Australia/Melbourne(CMT +11:00)	
Algorithm	\sim	~	current time zone.	Australia/Melbourne(GMT +11.00)	
<		>			
WARNING: After con restarted. This may t	nmand execution, Policy Manager service take a few minutes.	es will be	WARNING: After command restarted. This may take a	execution, Policy Manager services will be few minutes.	
	Save	Cancel		Save	

Then enabling Insight which is the reporting module of ClearPass

Dashboard O Monitoring O Monitoring O Configuration O Configuration O Configuration O Configuration O Configuration O Server Manager	Administration » Server Manage Server Configuration System Services Control Hostname:	r » Server C - victory Service Pa	configuration y (192.1 arameters tory	- victory 68.1.95) System Monit	oring Network	FIPS			
- De Server Configuration - De Log Configuration	FQDN: Policy Manager Zone:	vict	tory.clearpass.i efault	nfo ~					Manage Polic
- Jb Local Shared Folders - Jb Licensing	Enable Performance Monitoring	Display: 🗹	Enable this s	erver for perfo	rmance monitoring	display			
- Jevice Insight	Insight Setting:		Enable Insigl	nt	Enable as Insig	nt Master	Current Master:-		
🖅 🚰 External Servers	Enable Ingress Events Processin	ng:	Enable Ingress Events processing on this server						
- Destination	Master Server in Zone:	Pri	Primary master V						
	Span Port:		None v						
🖃 🗞 Agents and Software Updates					IPv4		IPv6		Action
- DrGuard Settings		IP Address			192.168.1.95				
Software Updates	Management Port	Subnet Ma	isk		255.255.255.0			Configure	
H- Support		Default Gateway			192.168.1.249				
		IP Address							
	Data/External Port	Subnet Ma	isk						Configure
		Default Gat	teway						
		Primary			192.168.1.250				
	DNS Settings	Secondary			192.168.1.130				Configure
	-	Tertiary							
		DNS Cachir	ng		Disabled				
	AD Domains:								Join AD Domain

6.3 Joining AD Domain

Configure the IP addresses and the rest as per your Lab setup but ensure you have the IP address of your domain controller as the primary DNS. CPPM needs to join the AD domain, in order to authenticate against it. Make sure the clock time for AD and CPPM are almost in sync. It is best to use NTP. If they are not in sync then CPPM will not be able to join the domain. When you click on the "join domain" button, you need to provide the FQDN of the DC and that's why you need the DNS entry to resolve the name of your domain controller.

System	Services Control	Service Parameters	System Monitoring	Network FIPS	
Policy Mana	ger Zone:	default	•		Manage Policy Manager Zones
Enable Prof	Join AD Domain			•	
Enable Perf				ig display	
Insight Set	Enter the FQDN of domain:	the controller and the sh	ort (NETBIOS) name fo	r the Iht Master Current Master:-	
DHCP Span	Domain Controller	wlan-dc.wlan.net			
	NetBIOS Name	WLAN		TDuc	Action
	In case of a contro	ller name conflict		IPV6	Action
Manageme	 ● Use specifi ○ Use Doma ○ Fail on cor 	ied Domain Controller in Controller returned by nflict	DNS query		Configure
Data/Exte	✓ Use default doma	ain admin user [Administ	rator]		Configure
	Username				
	Password	•••••			
DNS Settin			Save Ca	ncel	Configure
	101010	• 1			
AD Domain	ns:	Policy Manager is not	part of any domain. Joi	in to domain here.	Join AD Domain
•					
Join AD Do	omain		•	Join AD Domain	8
	Adding	host to AD domain	3 ¹¹ /2	Added host t	o the domain
Adding hos INFO - Fett INFO - Cre INFO - Usi Enter Adm Using short Joined 'CP6 INFO - Cre Starting cp	st to AD domain ched REALM 'WLAN. ched the NETBIOS r ating domain direct ng Administrator as inistrator's passwor t domain name W 53LAB' to dns doma ating service scripts pass-domain-server_	.NET' from domain FQD name 'WLAN' ories for 'WLAN' the WLAN-DC's userna d: VLAN in 'Wlan.net' s for 'WLAN' _WLAN: [OK]	N 'wlan-dc.wlan.net' me	Starting cpass-domain-server_WLAM INFO - updating domain configuratic Stopping cpass-domain-server_WLAM [OK] Starting cpass-domain-server: [OK Stopping cpass-sysmon-server: [OK Stopping cpass-radius-server: [OK Starting cpass-radius-server: [OK Starting cpass-radius-server: [OK] INFO - CP63Lab joined the domain M	VLAN. X X X X X X X X X X X X X X X X X X X

Now we need to add the AD as authentication source.

Monitoring Authentication Sources - Ariya AD Service Templates & Wizards Services Authentication Methods Sources Authentication Sources Authentication Sources Identity Single Sign-On (SSO) Cacle Users Cache Timeout: Static Host Lists Remove Remove Remove View Details Static Host Lists Role Mappings Enforcement Network Network Network Scan Policy Simulation	Dashboard O	Configuration » Authentication » Sources » Add - Ariya AD					
Summary General Primary Attributes Service Templates & Wizards Services Authentication Methods Sources Identity Single Sign-On (SSO) Cale Identity Static Host Lists Cales Roles Roles Role Mappings Server Timeout: Server Single Sign-Con (SSO) Static Host Lists Roles Roles Roles Roles Network Network Network Policy Simulation Server Simulation Methods Authorization: Methods Package Sign-On (SSO) Static Host Lists Roles Roles Remove View Details Server Timeout: Seconds Backup Servers Priority: <th>Monitoring O</th> <th colspan="5">Authentication Sources - Ariya AD</th>	Monitoring O	Authentication Sources - Ariya AD					
Service Templates & Wizards Services Authentication Methods Sources Sources Single Singh-On (SSO) Static Host Lists Static Host Lists Soles Renove Renove Server Timeout: Server Timeout: Server Timeout: Server Single	🖧 Configuration 💿	Summary General	Primary Attributes				
	 Service Templates & Wizards Services Authentication Methods Sources Identity Single Sign-On (SSO) Local Users Local Users Endpoints Static Host Lists Roles Roles Role Mappings Posture Enforcement Network Scan Policy Simulation 	Name: Description: Type: Use for Authorization: Authorization Sources: Server Timeout: Cache Timeout: Backup Servers Priority:	Ariya AD Active Directory Active Directory P Enable to use this Authentication Source to also fetch role mapping attributes Prove View Details Select View Details 36000 seconds Move Up 1 Move Down J Add Backup Remove				
			. Addition of				

•

Close

Close

Dashboard	O Co	nfiguration » Authenticat	ion » Sources » Add	- Ariya AD		
Monitoring	• A	uthentication Sou	urces - Ariva A	D		
Configuration	•	Summary General	Primary Attributes			
—🛱 Service Templates & Wizards					Compation Dataila	
- 🏠 Services	_				Connection Details	
🖃 🖴 Authentication	Ho	stname:	192.168.1.250			
- 🛱 Methods	Co	nnection Security:	None	~		
- 🛱 Sources		rt:	389 (For secure	connection, use 636)		
E- Q Identity	Ve	rify Server Certificate:	Enable to verify	Server Certificate for secure connec	tion	
-🌣 Single Sign-On (SSO)	Bir	d DN:	administrator@wlan.ne	t		
- 🛱 Local Users			(e.g. administrator@	example.com OR cn=administrator,c	n=users,dc=example,dc=com)	
- 🛱 Endpoints	Bir	d Password:	•••••			
Static Host Lists Roles	Ne	tBIOS Domain Name:	WLAN			
Role Mappings	Ba	se DN:	dc=wlan,dc=net		Search Base Dn	
🖅 🖶 Posture	Se	arch Scope:	SubTree Search	~		
	LD	AP Referrals:	Follow referrals			
Network Scap	Bir	nd User:	Allow bind using	user password		
- C Policy Simulation	Us	er Certificate:	userCertificate			
	Ah	ways use NetBIOS name:	Enable to always	able to always use NetBIOS name instead of the domain part in username for authentication		
	Sp	ecial Character Handling	Enabled Disal	bled		
	foi	LDAP Query:				
Dashboard	O Config	juration » Authentication »	Sources » Add - Ariya	a AD		
Monitoring	Aut	nentication Source	es - Ariva AD			
Configuration	Sun	mary General Prim	ary Attributes			
- 🛱 Service Templates & Wizards	Specif	filter queries used to fet	ch authentication and	authorization attributes		
— 🛱 Services	opeen	Filter Name		Attribute Name	Alias Name	Enabled A
- Authentication	1			dp	UserDN	-
— 🗘 Methods	1.			department	Department	-
				title	Title	
Ginalo Sign-Op (SSO)				comp30/	company	-
Local Users		Authenting		mambar06	company	-
- 🖧 Endpoints		Autientication		telester attender	Phase	-
- 🖧 Static Host Lists				telephoneNumber	Phone	-
- 🛱 Roles				mail	Email	-
- 🛱 Role Mappings				displayName	Name	-
🖭 🖶 Posture				accountExpires	Account Expires	-
	2.	Group		cn	Groups	-
Network	3.			dNSHostName	HostName	-
- 🛱 Network Scan		Machine		operatingSystem	OperatingSystem	-
- 🛱 Policy Simulation				operatingSystemServicePack	OSServicePack	-
	4.	Onboard Device Owner		memberOf	Onboard memberOf	-
	5.	Onboard Device Owner G	roup	cn	Onboard Groups	-

6.4 ClearPass dot1x Service

Here we'll create a dot1x service for wireless access.

aruba		ClearPass Policy Manager					≡	
Dashboard	O Conf	Configuration > Services						
Monitoring	• Se	rvices				🚽 Add		
Configuration	o					Limpo Limpo Limpo	ort ort All	
— 🋱 Service Templates & Wizards — 🛱 Services	This	page shows the curr	ent list and order of services that ClearPass follows	during authentication and authorization				
🖃 🗣 Authentication	Filte	r: Name	v contains v	Go Clear Filter		Show 20 V rr	ecords	
- 🛱 Methods	#	Order A	Name	Type	Template	Status		
- I doptity	1	. 1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	0		
Single Sign-On (SSO)	2	2. 2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)			
Local Users	3	a. 🗌 3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	0		
- 🛱 Endpoints	4	H. 4	[Guest Operator Logins]	Application	Aruba Application Authentication	0		
- 🛱 Static Host Lists	5	5. 5	[Insight Operator Logins]	Application	Aruba Application Authentication	0		
Roles	6	i. 🗌 6	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0		
Posture	7	7. 7	AA Aruba 802.1X Wireless	RADIUS	Aruba 802.1X Wireless	I		
Summary Service Auth Name: AA	Aruba 802.1X W	Roles Enforce	nent					
Description: To	authenticat ireless netwo	e users to an ork via 802.1X.	Aruba !					
Type: An	uba 802.1X Wi	1X Wireless						
Status: En	abled							
Monitor Mode:	Enable to mor	ble to monitor network access without enforcement						
More Options:	Authorization	Posture Com	pliance 🗌 Audit End-hosts 🗌 Profile E	indpoints 🗌 Accounting Proxy				
			Service	Rule				
Matches O ANY or O ALL o	of the following	conditions:						
Туре		Name		Operator	Value			
1. Radius:IETF		NAS-P	ort-Type	EQUALS	Wireless-802.11 (19)	B	Ť	
2. Radius:IETF		Servic	е-Туре	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)		Ť	
3. Radius:Aruba		Aruba	Essid-Name	EQUALS	school		Ť	
4. Click to add								

"school" is the name of the SSID

Summary Servic	e Authentication Roles Enforcement						
Authentication Metho	ds: [EAP PEAP] [EAP TLS] Move Up ↑ Move Down ↓ Remove View Details Modify						
Authentication Source	Ariya AD [Active Directory] Move Up ↑ Move Down ↓ Remove View Details Modify Select to Add ~						
Strip Username Rules:	Enable to specify a comma-separated list of rules to strip username prefixes or suffixes						
Service Certificate:	Select to Add V						
Summary Service Authentication Roles Enforcement							

Role Mapping Policy:	Select	~ Modify	Add New Role Mapping Policy
		Role Mapping Policy	Details
Description:	-		
Default Role:	-		
Rules Evaluation Algo	rithm: -		
Conditions			Role
Summary Service	Authentication Roles Enforcement		
Use Cached Results:	Use cached Roles and Posture attributes from	previous sessions	
Enforcement Policy:	AA Aruba 802.1X Wireless Enforcement Policy	✓ Modify	Add New Enforcement Policy
		Enforcement Policy D	etails
Description:			
Default Profile:	AA Aruba 802.1X Wireless Default Profile		
Rules Evaluation Algorithm:	first-applicable		
Conditions			Enforcement Profiles
1. (Authorization:Ariy	a AD:memberOf CONTAINS Staff)		AA-Aruba 802.1X Wireless Staff Profile, AA Aruba 802.1X Wireless Update Endpoint Location
2. (Authorization:Ariy	(Authorization:Ariya AD:memberOf CONTAINS Student)		AA-Aruba 802.1X Wireless Student Profile, AA Aruba 802.1X Wireless Update Endpoint Location
3. (Tips:Role EQUALS AND (Authorizati	[Machine Authenticated]) on:Ariya AD:memberOf CONTAINS Staff)		AA-Aruba 802.1X Wireless Staff Profile, [Update Endpoint Known]
4. (Tips:Role EQUALS AND (Authorizati	[Machine Authenticated]) on:Ariya AD:memberOf <i>CONTAINS</i> Studen)		AA-Aruba 802.1X Wireless Student Profile, [Update Endpoint Known]

And here are the enforcement profiles that are being used in the enforcement policy

•	AA Aruba 802.1X Wireless Default Profile	RADIUS
•	AA-Aruba 802.1X Wireless Staff Profile	RADIUS

- AA-Aruba 802.1X Wireless Student Profile
- RADIUS n Post_Authentication
- AA Aruba 802.1X Wireless Update Endpoint Location

Enforcement Profiles - AA Aruba 802.1X Wireless Default Profile

Note: This Enforcement Profile is created by Service Template

Su	mmary	Profile	Attributes			
Prof	ile:					
Nam	ne:		AA Aruba	802.1X Wireless Default Profile		
Desc	cription:					
Туре	e:		RADIUS			
Actio	on:		Accept			
Devi	ice Group	List:	-			
Attributes:						
	Туре			Name		Value
1.	Radius:/	Aruba		Aruba-User-Role	=	Employee

Enforcement Profiles - AA-Aruba 802.1X Wireless Staff Profile

Note: This Enforcement Profile is created by Service Template

Su	mmary	Profile	Attributes			
Profile:						
Nam	ne:		AA-Aruba	802.1X Wireless Staff Profile		
Des	cription:					
Туре	e:		RADIUS			
Actio	on:		Accept			
Dev	ice Group	List:	-			
Attributes:						
	Туре			Name		Value
1.	Radius:	Aruba		Aruba-User-Role	=	Staff

Enforcement Profiles - AA-Aruba 802.1X Wireless Student Profile

Note: This Enforcement Profile is created by Service Template

Summary	Profile	Attributes					
Profile:							
Name:		AA-Aruba	802.1X Wireless Student Profile				
Description:							
Туре:		RADIUS					
Action:		Accept					
Device Group	List:	-					

Attributes:

	Туре	Name		Value	
1.	Radius:Aruba	Aruba-User-Role	=	Student	

Enforcement Profiles - AA Aruba 802.1X Wireless Update Endpoint Location

				Note. This Enforcement Prome i	is created by	Service remplate	
Sı	immary	Profile	Attributes				
Pro	file:						
Nan	ne:		AA Aruba	802.1X Wireless Update Endpoint Location			
Des	cription:						
Тур	e:		Post_Aut	hentication			
Acti	on:						
Dev	ice Group	List:	-				
Attr	Attributes:						
	Туре			Name		Value	
1.	Endpoint	t		Last Known Location	=	%{Radius:IETF:NAS-IP-Address}:%{Radius:Aruba:Aruba- Location-Id}	

6.5 ClearPass Access tracker

Now we'll test by connecting to the school SSID.

	Manihari		Assess Tracker				
Dashboard •	Moniton	ng » Live Monitoning »	Access Tracker				
Monitoring O	Acces		Auto Refresh				
🖧 Configuration 🔹 💿	ation • The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.						
🔐 Administration 💿				-			
- // ClearPass Portal	💎 [A	ll Requests]	ictory (192.168.1.95)	15 Last 1 day before Tod	ау	Edit
🗉 🚔 Users and Privileges							
🖃 🖉 Server Manager							
- Jerver Configuration	Filter: R	equest ID	✓ contains ✓	+ Go Clear Filter			Show 20 $$
- 🌽 Log Configuration	#	Server	Source	Username	Service	Login Status	Request Timestamp +
- Jocal Shared Folders	1.	192,168,1,95	BADIUS	staff1	AA Aruba 802.1X Wireless	ACCEPT	2021/02/06 11:54:09
- 🌽 Licensing	1.	172.100.1.75	1000105	500111	AA Arubu 002.1X Wireless	Accel	2021/02/00 11:01:00

Summary Input Ou	tput Accounting					
Login Status:	ACCEPT					
Session Identifier:	R0000000-01-601de8a8					
Date and Time:	Feb 06, 2021 11:54:09 AEDT					
End-Host Identifier:	A0-88-B4-50-C0-84 (Computer / Windows / Windows)					
Username:	staff1					
Access Device IP/Port:	192.168.1.57 (MD-1 / Aruba)					
Access Device Name:	7008-1					
System Posture Status:	UNKNOWN (100)					
	Policies Used -					
Service:	AA Aruba 802.1X Wireless					
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2					
Authentication Source:	AD:192.168.1.250					
Authorization Source:	Ariya AD					
Roles:	[User Authenticated]					
Enforcement Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless	~				
I ≤ Showing 1 of 1-20 reco	ords ► ► Change Status Show Configuration Export Show Logs C	lose				

Request Details

Summary Input	Output Accour	ting	
Username:	staff1		
End-Host Identifier:	A0-88-B4-50-C0-	84 (Computer / Windows / Windows)	
Access Device IP/Port:	192.168.1.57	(MD-1 / Aruba)	
RADIUS Request			۲
Authorization Attribute	5		T
Authorization: Ariya AD: Account Expires		9223372036854775807 [30828-09-14 12:48:05 AEST]	
Authorization:Ariya AD:memberOf		CN=Administrators,CN=Builtin,DC=wlan,DC=net, CN=Staff,CN=Users,DC=wlan,DC=net	
Authorization:Ariya AD:Name		staff1	
Authorization:Ariya Al	D:UserDN	CN=staff1,CN=Users,DC=wlan,DC=net	
Computed Attributes			۲
Endpoint Attributes			٩

Summary	Input	Output	Accounting			
Enforcement	Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless Staff Profile				
System Postu	ire Status:	UNKNOV	IKNOWN (100)			
Audit Posture	Status:	UNKNOV	UNKNOWN (100)			
RADIUS Res	ponse		\odot			
Endpoint:La	ast Known	Location	192.168.1.57:20:4c:03:5c:05:6e			
Radius:Arub	a:Aruba-U	ser-Role	Staff			

Summary	Input	Output	Accounting			
Account Session ID:			staff1A088	450C084-601DE8B3-C2FE1		
Start Timesta	imp:		Feb 06, 202	Feb 06, 2021 11:54:11 AEDT		
End Timestan	ıp:		Still Active	Still Active		
Status:			Active			
Termination Cause:		-				
Service Type:		-				
Number of Authentication Sessions:		5: 1				
Network Details			\odot			
Utilization				\odot		
Authentication Sessions Details			•			

We'll use another device to connect and login as student1

-

Access Tracker Feb 06, 2021 11:59:19 AEDT

📀 Auto Refresh

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

Table [1] [] victory (192.168.1.95)	Y Edit
---	--------

Filter: R	equest ID \sim cont	ains ∨	+ Go Clear Filter			Show $20 \sim$ records
#	Server	Source	Username	Service	Login Status	Request Timestamp 🔹
1.	192.168.1.95	RADIUS	student1	AA Aruba 802.1X Wireless	ACCEPT	2021/02/06 11:59:18
2.	192.168.1.95	RADIUS	staff1	AA Aruba 802.1X Wireless	ACCEPT	2021/02/06 11:59:08

Summary Input	Output	Accounting	
Login Status:	ACC	СЕРТ	^
Session Identifier:	R00	000004-01-601de9e6	
Date and Time:	Feb	06, 2021 11:59:18 AEDT	
End-Host Identifier:	12-	65-72-CA-22-BE	
Username:	stud	dent1	
Access Device IP/Port	: 192	.168.1.57 (MD-1 / Aruba)	
Access Device Name:	700	8-1	
System Posture Status	s: UNK	(NOWN (100)	
		Policies Used -	
Service:	AA J	Aruba 802.1X Wireless	
Authentication Method	I: EAP	P-PEAP	
Authentication Source	: AD:	192.168.1.250	
Authorization Source:	Ariy	ra AD	
Roles:	[Use	er Authenticated]	
Enforcement Profiles:	AA	Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless	~
I ≤ Showing 2 of 1-20) records)	Change Status Show Configuration Export Show Logs	Close

Summary	Input	Output	Accounting	
Username:		student1		
End-Host Ider	ntifier:	12-65-72	-CA-22-BE	
Access Devic	e IP/Port:	192.168.1	L.57	(MD-1 / Aruba)
RADIUS Req	uest			0
Authorization	Attribute	5		\odot
Authorizatio	n:Ariya Al	D:Account	Expires 922	372036854775807 [30828-09-14 12:48:05 AEST]
Authorizatio	n:Ariya Al	D:Email	ariya	ap@hpe.com
Authorizatio	n:Ariya Al	D:memberC	Of CN=	Student,CN=Users,DC=wlan,DC=net
Authorizatio	n:Ariya Al	D:Name	stud	ent1
Authorizatio	n:Ariya Al	D:UserDN	CN=	student1,CN=Users,DC=wlan,DC=net

Computed Attributes

Summary Inpu	Output	Accounting		
Enforcement Profiles: AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless Student Profile				
System Posture Sta	us: UNKNO	UNKNOWN (100)		
Audit Posture Statu	3: UNKNOWN (100)			
RADIUS Response				
Endpoint:Last Kno	wn Location	192.168.1.57:20:4c:03:5c:05:6e		
Radius:Aruba:Arub	a-User-Role	Student		

And here is what we see on the MM dashboard.



Next, check part 2 of this document.