Contents

	1.1	Revision History	1
2	Dem	no Topology	2
3	Arul	ba Central Account	3
4	Arul	ba Central Configuration	6
	4.1	LAN Switch Configuration	6
	4.2	Gateway Configuration	7
	4.3	AP Configuration	
	4.4	Assigning Static IP addresses for APs	14
	4.5	Firmware Upgrade	14
	4.6	Gateway Cluster	
	4.7	Monitoring Gateway Cluster	
5	Clea	arPass Initial Configuration	20
	5.1	Joining AD Domain	21
	5.2	ClearPass dot1x Service	22
	5.3	NAD Configuration	24
6	WLA	AN Configuration	25
	6.1	Tunnelled Wireless Configuration	25
	6.2	Wireless dot1x Testing	27
7	RF N	Monitoring	
8	Gue	est Access Configuration	
	8.1	Guest Wireless Configuration	
	8.2	ClearPass Guest policy Configuration	41
	8.3	ClearPass Guest Portal Configuration	46
	8.4	Guest Testing	50

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
15 Mar 2021	0.1	Ariya Parsamanesh	Initial creation
22 May 2021	0.2	Ariya Parsamanesh	Added the ClearPass guest operator login
04 Jul 2021	0.3	Ariya Parsamanesh	Added the Monitoring section

2 Demo Topology

The aim here is to provide the starting point to put together a solution that include the AOS10 APs, two gateways, ClearPass and obviously Aruba Central.

Note that APs in AOS10 support bridged, tunnelled and mix mode wireless LANs (WLAN) however in this technote we'll be deploying tunnelled mode WLANs. We'll also demonstrate the gateway clustering with AOS10.

This is type of deployment is particularly useful when all the buildings in a school/college campus have L3 IP demarcation and are routed to various part of the campus.



With AOS10, the campus architecture consists of two layers:

- 1. The infrastructure layer consists of a WLAN setup which can be either a campus setup or a branch setup. The campus setup can consist only of access points (APs) or APs combined with gateway clusters. In case of a branch setup, the infrastructure layer includes an AP. Here we have combined the Instant APs and Campus APs into just APs, and you bridge, or tunnel user traffic based on the configuration on the APs.
- 2. **The cloud management layer** consists of Aruba Central which is a cloud management SaaS platform. The Network Operations app is one of the Aruba apps which is a part of Aruba Central and this app helps to create the SSID profiles for the different WLAN campus and branch setups.



As you can see in the above diagram, the classic components that would normally run on mobility master or instant APs are now run as services in Aruba Central. I am talking about Airmatch, Roaming, clientmatch, etc.

Here we'll not go to the details of the architecture for that please refer to this link

https://www.arubanetworks.com/techdocs/AOS10X_OLH/Content/overview/architecture-overview.htm

3 Aruba Central Account

You need an Aruba Central account with appropriate licenses for APs and gateways. You can sign up for a 90 days trial from this link

https://www.arubanetworks.com/products/network-management-operations/central/eval/

Once you login to your Central account you need to add your devices (APs and Gateways) to the device inventory

ACCOUNT HOME



Here I have already added my APs.

Account H If the devices a text. You can also a	ome > Device Invento associated with your act dd your devices using t	r y count are no he Aruba Cer	t automatically discovered and are not displayed in your inventory, you ntral mobile app and they will automatically appear in your inventory.	can add devices manua	ally by clicking the	ADD DEVICES
All 15	Access Points 2	Switche 5		×		
DEVICES			SERIAL NUMBER MAC ADDRESS			\odot
Y Serial N	↓= Y MAC Address	Y Part			▼ Custo	▼ Assign
CNC0	B4:5D:50:	IAP-324-	SERIAL NUMBER MAC ADDRESS		HPE Aruba	Foundation
CNC0	B4:5D:50:	IAP-324-	SERIAL NUMBER MAC ADDRESS		HPE Aruba	Foundation
			SERIAL NUMBER MAC ADDRESS			
Add Devices	Import via CSV	Download s	SERIAL NUMBER MAC ADDRESS			
			Add more devices	Done		

You do the same for the gateways as well. Then you need to assign the licenses to the devices, for this from Account home you need to go to "License Assignment"

GLOBAL SETTINGS			
USERS AND ROLES	KEY MANAGEMENT	DEVICE INVENTORY	LICENSE ASSIGNMENT
Manage user access	Manage your subscription keys	Manage the Devices in your Inventory	Assign Licenses to Devices
AUDIT TRAIL	SINGLE SIGN ON	API GATEWAY	WEBHOOKS
View audit-trail logs	Create and manage SAML Profiles	Access API Gateway and manage access tokens	Manage Webhook end points

CACCOUNT HOME	> LICENSE ASSIGNMEN	п						
Access Points	Unlicensed License 0 2	ed Switches	Gateways 8					
LICENSE SUMMAR	Y LI	CENSE ASSIGNMEN	MANAGE LICE	NSE ASSIGNMENT (M	ANUAL)	×	Assigned License	SELECT ALL
Foundation	, 2		Overview of sele	ected Access Points	5		Foundation Foundation	
Assigned 2 (1 available) Advanced			Choose License Type FOUNDATION		2			
Assigned 0 (0 available)	0			Cancel Unassign	Undate			
AUTO-ASSIGN	•							
Note: Licenses can be assi devices	gned manually on							2 ITEM(S) SELECTED

Access Points 2	Switches 5	Gateways Unlicen	sed Licensed 5				
ICENSE SUMMA	RY	LICENSE ASSIGNMEN	MANAGE LICENSE ASSIGNMENT (MANUA	L)	×	Assigned License	SELECT ALL (
kssigned 0 (0 available)	0		Overview of selected Gateways Foundation 7000/90XX	2		Foundation 703079000	
oundation 7000/9000	10		Choose License Type		~		
oundation 7210/ Issigned 0 (4 available)			Cancel Unassign				
oundation with Security Issigned 0 (0 available)	•				_		
UTO-ASSIGN)D						
iote: Licenses cari be as levices	signed manually on						2 ITEM(5) SELECTED

Now, we'll go the network operations App in Aruba Central.

ACCOUNT HOME Manage your Network Inventory, Subscript	ions, and User Access. Use any of the fo	bllowing apps to make Aruba work better for you.	
APPS			
Network Operations Manage your wired, wireless, and WAN Infrastructure			
GLOBAL SETTINGS			
USERS AND ROLES Manage user access	KEY MANAGEMENT Manage your subscription keys	DEVICE INVENTORY Manage the Devices in your inventory	LICENSE ASSIGNMENT Assign Licenses to Devices
AUDIT TRAIL View audit-trail logs	SINGLE SIGN ON Create and manage SAML Profiles	API GATEWAY Access API Gateway and manage access tokens	WEBHOOKS Manage Webhook end points

Here we'll create a group and move the devices into it. The groups are used for device configurations.

🗟 Global ା	Groups Sites and I shale Contificates Install Mananee	
– Manage –	CREATE NEW GROUP	(
B Overview	GROU	
Devices	A group in AOS10	devices with common con
🗖 Clients	Use the group as Template group by selecting the device i	
😩 Guests	MANAGI DRAG AND AP AND GATEWAY SWITCH	
Applications	TO SELECT Group password settings	
Security	PASSWORD	
🗞 Network Services	Y Group Nar	Y Location
— Analyze ————		Melbourne,Australia
🏚 Alerts & Events	UNASSIGNE Cancel Add Group	Melbourne,Australia
🛛 Audit Trail	default	Melbourne,Australia
🖏 Tools	test 2 TW00KM0052	Melbourne,Australia
🔝 Reports	TG test switch 2	
— Maintain ————		
Firmware		
ង្ខ Organization		
	New Group Broup Broup Broup	

Then you need to convert the group to AOS10.



Once the group is converted, you can then drag and drop the devices from the right hand side table.

Groups	Sites and Labels	<i>C</i> ertificates	हैं। Install Manager		
GR A grou config MAN DRAG TO SEL	OUPS up in Aruba Cen uration settings AGE GROUP AND DROP CLUS LECT MULTIPLE D	tral acts like to all the dev ' S T <mark>ERS AND SV IEVICES SHIFT</mark>	a primary configuration con ices in the group. ITCHES BETWEEN GROUPS +CLICK OR CTRL+CLICK	tainer for devices. You can combine devi	ces with common conf
∀Grou	p Name	Devi	ces	∑ Name	⊤Location
ALL CO	DNNECTED DEVICE	:S 12		7005_AOS10_gwy1	Melbourne,Australia
UNASS	GIGNED DEVICES	0		7005_AOS10_gwy2	Melbourne,Australia
AOS10		5	¥	Ariya-LTE_BGW1	Melbourne,Australia

For this demo, I have also added Aruba 2930F switch to Aruba Central's AOS10 group. We'll start with the configuration of the LAN switch to which we'll connect the APs and the gateways.

4.1 LAN Switch Configuration

Server-VLAN

mgmt-VLAN

Static

Static

192

4085

We won't go deep in this section as the focus here is AOS 10 demo. Take a note of the VLANs that are configured.

← 🖽 Aruba-2930F-8G ⊘	📼 Switch													Config
- Manage	Switches	Stacks In	nterface Security	System Ro	uting IGMP	QoS Devic	e Profile Configura	tion Audit						
B Overview														
🗔 Clients	SWITCHES (1)											\odot		
몷 LAN	Hostna	me			IP Address		Default Gatew	ay	MAC Address		Location		Contact	
	Aruba-29	930F-8G-Pol	EP-2SFPP		10.224.254.2		10.224.254.1		b0:5a:da:98:9a:00		Melbourne	-	-	
C Device														
← 📼 Aruba-2930F-8G ⊘	📼 Switch													c.
– Manage –	Switches	Stacks I	nterface Security	System F	Routing IGM	IP QoS De	vice Profile Config	uration Audit						
E Overview														
Cients	Ports PoE	Trunk G	iroups VLANs S	panning Tree	Loop Protect	tion								
TT LAN		ANIc Sotti	ings											6 VLANS
Device	V VLP	NVS JELLI	iigs											
- Analyze	Prin	nary VLA	N: 1											
Alerts & Events	VL	ANs												+
Audit Trail	ID		Name	IP Assig	nment	IP Addres	is Tag	ged Ports L	Intagged Ports	DHCP Helper	IP	Voice	lumbo	=
🖏 Tools	1		DEFAULT_VLAN	DHCP					6,9-10			×	×	
🛋 Reports	33		student-VLAN	Static		10,10,33	5.1 5.1	7	2			×	×	
— Maintain ————	44		Staff-VI AN	Static		10.10.44	L1 5.	7				×	×	
Firmware	55		AP-VI AN	Static		10 10 55	.1		3.4			×	×	

As the names suggests, APs are connected to AP-VLAN, gateways and ClearPass are connected to Server VLAN.

192,168,1,244

10.224.254.2

The gateways are connected to port 5 and 7 that are configured for VLAN trunking. DHCP for AP, staff, and student VLANs are configured on the switch.

5.7-8

← 🖽 Aruba-2930F-8G ⊘	E3 Switch	() Config
- Manage	Switches Stacks Interface Security System Routing IGMP QoS Device Pr	ofile Configuration Audit
E Overview	Access/DNS_Time_SNMP_CDP_DHCP	
Lo Clients		
윪 LAN		3 DHCP Pools
Device		
— Analyze ————		
Alerts & Events	DHCP Pools	+
🛛 Audit Trail	Name	rk Natrosk Edit Dalata =
🖏 Tools	AP-VI AN 10.1	155.0 255.255.255.0
🔝 Reports	Staff-VLAN 10.1	.44.0 255.255.255.0
— Maintain ———	Student-VLAN 10.1	33.0 255.255.255.0

```
dhcp-server pool "AP-VLAN"
    default-router "10.10.55.1"
    dns-server "10.224.254.1"
    lease 00:08:00
    network 10.10.55.0 255.255.255.0
    range 10.10.55.10 10.10.55.19
    exit
dhcp-server pool "Staff-VLAN"
```

```
default-router "10.10.44.1"
dns-server "1.1.1.1"
lease 00:04:00
network 10.10.44.0 255.255.255.0
range 10.10.44.50 10.10.44.59
exit
dhcp-server pool "Student-VLAN"
default-router "10.10.33.1"
dns-server "1.1.1.1"
lease 00:04:00
network 10.10.33.0 255.255.255.0
range 10.10.33.50 10.10.33.59
exit
dhcp-server enable
Aruba-2930F-8G-PoEP-2SFPP#
```

4.2 Gateway Configuration

Note that with AOS 10, Gateways are not mandatory. They are required if you want to tunnel user traffic to a central location particularly useful for scenarios that you need L2 roaming between APs in different subnets.

We'll start the configuration at group level before powering up the gateways. This is to minimise the reboots and some potential network issues especially when it comes to changing IP address and loosing connectivity.

We'll be using Aruba 7005 gateways which have 4x ports.

ជ AOS10	Access Points Switches Gatewa	ys					[List Summary Config
- Manage	Gateways • Online 0 0	• Offline 0	Clusters 0					
Devices	GATEWAYS							.↓. ⊖
🗂 Clients	V Device Name	Y Model	Y IP Address	∀ мас	▼ Serial	Firmware Version	Uptime	Inspection Engine
2. Guests								
Applications								

G Access Points	Suither Clouist	i ≡ List	II. Summary Config
	SET GROUP TYPE	Advanced Mode	Guidad Satup
System	Group needs to contain all devices which have a Gateway or VPNC persona. Group cannot have a mix of Gateway and VPNC devices. Once a Group is configured to be a Gateway or a VPNC group then it cannot be changed Branch Gateway VPNC 	Advanced Mode	Guided Setup
	Cancel Save Settings		

다 AOS10 이	Access Points Switches Gatewa	iys			SELECTED GROUP TYPE Gateway	Eist Summary Config
– Manage –	System Interface Routing					Advanced Mode
B Overview	General Admin Certificates	SNMP Logging Switching Ex	ternal Monitoring			
Devices	> Basic Info					
Clients	V Clock					
🔐 Guests	Time:	Get time from NTP server				
Applications						
Security		NTP servers			_	
Analyze		IP ADDRESS/FQDN	BURST MODE	AUTHENTICATION KEY	=	
Alerts & Events		216.239.35.4	Yes			
🛛 Audit Trail						
Tools						
Reports						
Maintain ————						
Firmware		+				
	Source interface:	-None- 💙				
	Use NTP authentication:					
	Time zone:	Australia: Australia/Melbourne (UTC+.				

다 AOS10 이	이 교 유 Access Points Switches Gateways			SELECTED GROUP TYPE Gateway	III II. Summary Config
- Manage	System Interface Routing				Advanced Mode
BB Overview	General Admin Certificates SNMP Logging	Switching External Monitoring			
Devices	> Basic Info				
Clients	> Clock				
a Guests	∨ Domain Name System				
Applications	Domain name:				
Security	Enable DNS name resolution: JPv4				
— Analyze —					
Alerts & Events	DNS servers 🕠				
🛛 Audit Trail	IP VERSION	IP ADDRESS	UPLINK VLAN		=
🖏 Tools	IPv4	1.1.1.1			
Reports	IPv4	192.168.1.1			

Disabling spanning tree

II AOS10	Access Points Switches Gateways	SELECTED GROUP TYPE Gateway	List Summary Config
- Manage	System Interface Routing		Advanced Mode
BB Overview	General Admin Certificates SNMP Logging Switching External Monitoring		
Devices	✓ Spanning Tree		
La Clients	Spanning tree:		
🔉 Guests			
Applications	> LACP		
	> Tunnel Loop Prevention		

Adding the relevant ports for Aruba 7005 gateway.

다 AOS10 이	Contemportation Contemport	SELECTED GROUP T	YPE	E II. ist Summary	Config
— Manage ———	System Inte			Advanced M	Лode
Overview	Ports VLAN Gateway models support up to a maximum of 4 ports, so you can create and configure upto 4 ports. Select the ports you wish to configure based on the				
Devices	device model.				
🗖 Clients	Ports				
😩 Guests	All 4 configurable ports	IING TREE DESCI	RIPTION		=
Applications	GE-0/0/0	GE0/0	0/0		
Security	GE-0/0/1	GE0/0)/1		
- Analyze	GE-0/0/2 GE-0/0/1	GE0/0)/2		
🏚 Alerts & Events	GE-0/0/3 GE-0/0/2	GE0/0)/3		
🛛 Audit Trail	GE-0/0/3				
🖏 Tools		-			
🔝 Reports	Cancel Cancel				

I am planning to sue interface 0/0/0 as my gateway uplink. This port needs to be in trunk mode and here we'll add the relevant VLANs.

II AOS10	Access Points Switches Gateways		SELECTED GROUP TYPE 🗮 II. Gateway List Summary Confe
- Manage	System Interface Routing		Advanced Mode
B Overview	Ports VLANs DHCP Pool Management GRE Tunnels Bulk of	onfiguration upload SLB	
Devices	Viane		
🗂 Clients	VIGIIS		
😩 Guests	NAME	ID(S)	=
Applications	Server-VLAN	192	
Applications	Staff-VLAN	44	
Security	Student-VI AN	33	
- Analyze	Staten () at		
Alerts & Events		1	

Adding the VLANs to appropriate ports.

ជ AOS10 이	Access Points Swit	ා ලූ tches Gateways								SELECTED G Gateway	ROUP TYPE	⊟ I ist Sum	IL 👸 Imary Conf
- Manage	System Interface	Routing										Advan	iced Mode
B Overview	Ports VLANs	DHCP Pool Mi	anagement GRE	Tunnels Bulk	configuration upload	SLB							
Devices	Dente												
La Clients	Veee	-			Vuen	~	V						_
😩 Guests		TYPE		Y POLICY	Y MODE		Y ACCESS VLAN	Y TRUNK VLANS	TRUSTED VLANS	SPANNING TREE	DESCRIPTION	÷	=
Applications	GE-0/0/0	-	Enabled	Not-defined		192	-	33,44,192	33,44,192	v ,	GE0/0/0		
Security	GE-0/0/2	-	Enabled	Not-defined	access		1	-	1_4094	·	GE0/0/2		
- Analyze	GE-0/0/3		Enabled	Not-defined	access		1		1.4094	· · ·	GE0/0/3		
Alerts & Events	GE-0/0/5		LINDICU	Notachinea	000033				1-40.54	v	020/0/5		
🗷 Audit Trail	1												
🖏 Tools													
	GE-0/0/0												
	Туре:		LAN 🗸										
	Admin stat	te:	~										
	Speed:		auto 🗸	Mbps									
	Duplex:		auto 🗸										
	Poe:												
	Trust:		•										
	Policy:		Not-defined	~									
	Mode:		Trunk 🗸										
	Native VLA	N:	192 🗸										
	Allowed VL	ANs:	33,44,192	~)								
	Description	1:	GE0/0/0										
	Jumbo MTU	J:											
	Port monito	oring:	-None- 🗸										

Adding the default route

다 AOS10 이	Image: Constraint of the second se	SELECTED GROUP TYPE Gateway	III II.							
- Manage	System Interface Routing WAN Security VPN High Availability Config Audit		Basic Mode							
B Overview	IP Routes Policy-Based Routing NextHop Configuration RIP OSPF BGP Overlay Routing									
Devices	> IP Routes									
La Clients	✓ Static Default Gateway									
🛎 Guests	Static default gateway									
Applications	Y DEFAULT GATEWAY COST		≡							
Security	192.168.1.1 1									

Adding the user roles by going to "security tab"

법 AOS10 이	Access Points Suitebox Catouraus		SELECTED GROUP TYPE 🗮 II. Gateway List Summary Contig
— Manage ————	System Inter		Basic Mode
88 Overview	Roles Polic Name: Student		ıll
Devices	Roles		
🗖 Clients		Cancel	Save Settings
😩 Guests	aprole	35 Dules	
Applications	authenticated	4 Dules	
Security	autienticated	4 Kules	
- Analyze	default-iap-user-role	2 Rules	
. Alerts & Events	default-via-role	3 Rules	
🛛 Audit Trail	default-vpn-role	4 Rules	
🖏 Tools	guest	11 Rules	
🗈 Reports	+		

ជ AOS10 이	Access Points				SELECTED GROUP TYPE Gateway	i List f	II. 👸 Summary Config
— Manage ———	System Inter						Basic Mode
B Overview	Roles Polic Add an existing policy:				Ш		
Devices							=
La Clients	Create a new policy: stateful-dot						
🛎 Guests	Student Policy type:	Session 🗸					
Applications	switch-logol Policy name:	allowall 🗸					
- Analyze	sys-ap-role						
ậ Alerts & Events	sys-switch-r Position:						
🛛 Audit Trail	voice			Gancel Save Settings			
🖏 Tools							
Reports	Student Policies Bandwidth M	ore					
Firmware	∀ NAME	RULES COUNT	∀түре	POLICY USAGE			=
	global-sacl	0	session	ap-role, authenticated, default-via-role	e, defa		
	apprf-student-sacl	0	session	Student			
	+						

Here we'll add the allow-all policy.

ជ AOS10 이	Access Points Switches Gateways			5	SELECTED GROUP TYPE	II. Summary Confi
— Manage ———	System Interface Routing WAN Security	VPN High Availability Config Audit				Basic Mode
88 Overview	Roles Policies Aliases Applications Ap	Apply Policy Auth Servers Role Assi	gnment (AAA Profiles) L2 Authentication	L3 Authentication Advanced Firew	all	
Devices		RULES				=
La Clients	etataful datta	0 Dulor				
😩 Guests	Student	2 Bules		a		_
Applications	suitsh laren	2 Rules				
Security	switch-logon	1 Rules				
— Analyze ————	sys-ap-role	23 Rules				-
↓ Alerts & Events	sys-switch-role	24 Rules				
🛛 Audit Trail	voice	41 Rules				
🔦 Tools	+					
Reports						
- Maintain	Student Policies Bandwidth More					
Firmware	VNAME RUL	LES COUNT	∀түре	\forall POLICY USAGE		=
	global-sacl 0		session	ap-role, authenticated, default-via-role,	defa	
	apprf-student-sacl 0		session	Student		
	allowall 2		session	authenticated, default-iap-user-role, def	fault	

Next, we'll assign a VLAN to this role.

ជ AOS10 이	Access Points Switches Gateways	SELECTED GROUP TYPE Gateway	E II.
– Manage –	System Interface Routing WAN Security VPN High Availability Config Audit		Basic Mode
B Overview	Roles Policies Aliases Applications Apply Policy Auth Servers Role Assignment (AAA Profiles) L2 Authentication L3 Authentication Advanced	Firewall	
Devices	voice 41 Rules		
Clients	+		
a Guests			
Applications	Student Policies Bandwidth More		
Security	✓ Network		
- Analyze	VLAN: 33		
Alerts & Events	Re-auth interval:		
Audit Trail			
🖏 Tools	Max sessions: 65535		
Reports	Deep packet inspection:		
- Maintain			
φ Filliware	Web content classification:		
	Youtube education:		
	Open flow:		
	> VPN		
	> Authentication		

We'll create a new user role staff and as before, we'll add a allow-all policy and assign VLAN 44 to it.

C AOS10	Access Points Switches Gateways		SELECTED GROUP TYPE 🗮 II. Gateway List Summary Co
- Manage	System Interface Routing WAN Security VPN High Availability	Config Audit	Basic Mode
B Overview	Roles Policies Aliases Applications Apply Policy Auth Serv	vers Role Assignment (AAA Profiles) L2 Authentication L3 Authentication Advanced	Firewall
Devices	Poles		
Clients		DUI 22	
a. Guests		ROLES	
Applications	guest-logon	27 Rules	
Security	logon	32 Rules	
— Analyze —	. school	1 Rules	
↓ Alerts & Events	Staff	2 Rules	
Audit Trail	stateful-dot1x	0 Rules	
🖏 Tools	Student	2 Rules	
💼 Reports	+		

We'll configure the authentication server and RFC3576 for RADIUS CoA

띠 AOS10 이	Access Points		SELECTED GROUP TYPE Gateway	III III List Summary Config
- Manage	System Interf			Basic Mode
B Overview	Roles Policie Name:			
Devices		ClearPass-GW		
🖬 Clients	IP address / hostname:	192.168.1.95		
🚉 Guests	Timer			
Applications	i)per	Radius 🗸		
Security				
- Analyze	+	Cancel Save Settings		

Then once saved, click on it to set the RADIUS secret key

법 AOS10 이	ල් Access Po	ints Swite	a ches G	ateways										SELECTED GROUP TYPE Gateway	List	IL Summary Cont
Manage	System	Interface	Routing	WAN	ecurity VP	N High	Availability Co	nfig Audit								Basic Mode
E Overview	Roles	Policies	Aliases	Applicat	ons Apply	Policy	Auth Servers	Role Assignm	nent (AAA Profiles)	L2 Authentication	L3 Authentication	Advanced	Firewa	11		
Devices		Server op	otions													
🗂 Clients																
🚉 Guests		Nam	e:			Clear	Pass-GW									
Applications																
Security		IP address / hostname:			192.1	68.1.95										
— Analyze ———		Secure radius:														
. Alerts & Events																
🛛 Audit Trail		Auth	n port:			1812										
🖏 Tools		Acct	port													
🔝 Reports		ALCI	porta			1813										
— Maintain ————		Shar	ed key:				••									
Firmware																
		Rety	pe key:			•••••	••									
		Time	out:			5										

And finally add a rfc3576 server for CoA.

G Access Poir	nts	Enterna				SELECTED GROUP TYPE Branch Gateway
System	WAN	New server				
Roles	Polic	IP address:	192.168.1.95			all
	1000	Key:	•••••			
		Retype key:	•••••			
		Туре:	RFC 3576			
	+				Cancel Save Settings	-
	All se	rvers				
	NAMI	E	TYPE	IP ADDRESS / HOSTNAME	SERVER GROUP	
	Clear	Pass1	Radius	192.168.1.95		
	-					

Note that they are not assigned to any authentication server groups.

- Manage	System	WAN	Interface	Security	VPN R	touting	High Availability	Config Audit					
89 Overview	Roles	Policies	Aliases	Applicat	ions a	Apply Polis	Cy Auth Server	s Role Assignn	nent (AAA Profiles)	L2 Authentication	L3 Authentication	Advanced	Firewall
Devices		NAME			SER	RVERS		FAIL THROU	IGH	LOAD BALANCE		SERVER RULES	
🗂 Clients													
🚨 Guests													
Applications		1°P											
Security		No data to display											
— Analyze —													
Alerts & Events		+											
🗷 Audit Trail													
🖏 Tools		All ser	vers										
Reports		NAME				TYPE			IP ADDRESS / HO	STNAME	SERVER GROU	IP	
— Maintain ————		ClearP	are1			Dadiu			102 168 1 05	///////	SERVER GROU		
Firmware		Cleare	d55 I			Radiu	15		192.108.1.95				
						RFC 3	1576		192.168.1.95				

4.3 AP Configuration

Here we'll go through the AP configuration. As always, we'll do the bulk of configuration at the group level.

II AOS10 〇	Access Points Switches Gateways	
- Manage	WLANs Access Points Radios Interfaces Security Services System C	Configuration Audit
B Overview		
Devices	SYSTEM	
🖽 Clients	∨ General	
🔐 Guests	Set Country code for group :	AU - Australia
Applications	Timesee	Melbourne LITC+10
Security	Timezone :	The selected country observes Davlight Swings Time
— Analyze	Preferred Band :	5 GHz
Alerts & Events		
Audit Trail	NTP Server :	216.239.35.4
🔦 Tools	DHCP Option 82 XML :	•
Reports		
- Maintain	Login Session Timeout:	3
Firmware	Console Access :	

Console Access :	
WebUI Access :	
Telnet Server :	
LED Display :	
Deny Inter User Bridging :	
Deny Local Routing :	
Mobility Access Switch Integration :	
URL Visibility:	
Restrict uplink port to specified VLANs:	
VOIP QOS Trust:	
> Administrator	
> Mesh	
> Time-Based Services	
> Enterprise Domains	
> Logging	
> SNMP	
> Proxy	
> IPM	



Server Type:					
	RADIUS				
Name:	ClearPass		Radsec:		
IP Address:	192.168.1.95		Auth Port:	1812	
Shared Key:	•••••		NAS IP Address:		
Retype Key:	•••••		NAS Identifier:		
Timeout :	s	sec	Retry Count:	3	
Service Type Framed User :	MAC/Captive Portal		Query Status of RADIUS Servers(RFC 5997) :	Authentication Accounting	
Dynamic Authorization:			Accounting Port:	1813	

As we did with gateways, we'll create various user roles here as well.

II AOS10 O	Access Points Switches Gateways	List Summary Config									
— Manage	WLANs Access Points Radios Interfaces Security Services System Configuration Audit	Hide Advanced									
B Overview	SECIENTY										
Devices	> Authonization Servere										
Clients											
a Guests	> MPSK Local										
Applications	> User For Internal Server										
Security	∨ Roles										
— Analyze —	Roles	+									
Alerts & Events	Allow any to all destinations	~ ~ 🖍 💼									
Audit Trail	staff										
🖏 Tools	Student										
Reports	default_wired_port, profile										
— Maintain —	school										
Firmware	wired-SetMeUp										

This is in case we want to change from tunnel mode to bridge mode for user traffic, otherwise we don't need these roles here.

4.4 Assigning Static IP addresses for APs

In most of the cases you'll go with DHCP based IP addresses, but in case you need to assign static IP addresses, it is done as shown below.

	0							ii (8
	Access Points Switches Gateways							Summary Con
- Manage	Access Points • Online •	Offline Radios						
		4	-					
Device	ACCESS POINTS (2)							. <u>↓</u> ⊖
🗖 Clients	Device Name	Status	Y IP Address	Y Model	Firmware Version	Y Group	Uptime	
Security	64:5d:50:c6:82:3c	O Ottline	10.10.55.10	AP-324	10.2.0.1_79907	AOS10	- 4 Hours 42 Minutes 18 Sec	onds
— Analyze ————	04:50:50:00:82:44	• Online	10.10.33.11	AI -324	10.2.0.1_75507	AUSTU	4 Hours 42 Windles To Sec	5105
Alerts & Events								
🛛 Audit Trail								
🖏 Tools								
— Maintain ————								
Firmware								
· · · · · · · · · · · · · · · · · · ·	н							
← ⓓ b4:5d:50:c6:82:3c 🛆	O Access Point							205 Config
- Manage	Access Points Configuration Audit							Hide Advanced
B Overview								
Device	Access Points (1)							\odot
Clients	Name Status	IP	Address	WLANs	Radio Profile	Туре		
	b4:5d:50:c6:82:3c Down	10.1	0.55.10	All SSIDs selected	default	AP-324		<u> </u>
- Analyze								EDIT
Alerts & Events								
🖏 Tools								
	0							®
 ♥ 0 b4:50:50:c6:82:3c 	Access Point							Config
- Manage	Access Points Configuration Audit						н	de Advanced
88 Overview								
Device	ACCESS POINTS / B4:5D:50:C6:82:3C							
Clients								
Security	SYSTEM WLANS RADIO EXTERNAL	ANTENNA UPLINK						
— Analyze ———								
Alerts & Events	Name:	b4:5d:50:c6:82:3c						
🗷 Audit Trail	IP Address For Access Point:	Get IP Address from	n DHCP server					
🖏 Tools		Static						
- Maintain								
Firmware	IP Address:		Invalid IP Address					
	Netmask:		Invalid Netmask					
	Default Gateway							
	Delauli Galeway.		Invalid IP Address					
	DNS Server:							
	Domain Name:							
	LACP Mode	Passive						
	LACP MODE	r daarve 🔻						

4.5 Firmware Upgrade

We'll now connect the APs that we previously added to Aruba Central inventory that are running Instant software to the network. The network must have Internet access. Ensure that the APs are in factory default mode to get rid of any previous configuration. When they are powered up, they will get DHCP IP address and with a valid DNS and will then contact Central and will end up in AOS10 group that we created before.

For the gateways ensure they are factory default and running the SD-branch image 8.6.0.4-2.2.x.x or better. Again, like the APs, once the gateways are powered up they can use DHCP to get their IP addresses and will then contact Aruba Central, but we'll go through the full setup without DHCP.

```
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 Are you sure that you want to stop auto-provisioning and start full setup dialog? (yes/no): yes 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 [Aruba7005]: 7005-1 Enter Switch Role (standalone|md) [md]: Enter IP type to terminate IPSec tunnel (ipv4|ipv6) [ipv4]: Enter Master switch IP address/FQDN or ACP IP address/FQDN: deviceapacsouth.central.arubanetworks.com Enter Master switch type(MM|ACP) ACP Enter Uplink Vlan ID [1]:192 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]: 192.168.1.243 Enter Uplink Vlan Static IP netmask [255.255.255.0]: Enter IP default gateway [none]: 192.168.1.1 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) [12/3/2021]: 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: ******* <omitted the other lines> System will now restart! [12:55:07]:Starting rebootme [12:55:07]:Shutdown processing started

Once the APs and gateways are online in Aruba Central, we'll upgrade them to AOS10 image. In the next release SDbranch and AOS10 firmware will merge. I have already upgraded my APs, but this is how you can do it.

ជ AOS10	Constantiation Constantiati Constantiation Constantiation Constantiation Constant	ays			
— Manage ———					
B Overview	ACCESS POINTS (2)				
Devices	Name	1=.	Firmware Version	Recommended Version	٢
⊑ ī Clients	b4:5d:5b4:5d:5		10.1.0.2_77953 10.1.0.2_77953	8.6.0.8_79369 8.6.0.8_79369	F
😫 Guests					
Applications			Firmware Version Custom Build	fw text build 10.1.0.2_77953	
Security			When		
— Analyze ————			Specify when to validate of devices for the first time.	compliance and upgrade the non-compliant	
Alerts & Events			Now O Later Da	ate	
🛛 Audit Trail					
🖏 Tools				Cancel Upgrade	
🗊 Reports					
— Maintain ————					
Firmware					

We'll use the same firmware version for the gateways as well.

II AOS10 〇	Access Points Switches	@ Gateways									
- Manage					() SET C	OMPLIANCE 🕈 UPGRADE ALL					
88 Overview	ACCESS POINTS (2)	CCESS POINTS (2) Q_ ⊢ (C									
Devices	Name	18.	Firmware Version	Recommended Version	∀ Upgrade Status	Compliance Status					
Clients	• b4:5d:3		10.1.0.2_77953	8.6.0.8_79369	Firmware up to date	Not Set					
Lu cherits	b4:5d:::::::::::::::::::::::::::::::::::		10.1.0.2_77953	8.6.0.8_79369	Firmware up to date	Not Set					
🔐 Guests											
Applications											
Security											
- Analyze											
Alerts & Events											
🛃 Audit Trail											
Tools											
Reports											
— Maintain ————											
Firmware											

Here we'll check to see if the APs and gateways are online with the correct firmware

H AOS10	Access Points Switches Ga	<u>ශ</u> teways					:= List
- Manage	Access Points • Onlin 2 2	ne Offline 0	Radios 4				
Devices	ACCESS POINTS (2)						
Clients	Y Device Name	Status	Y IP Addre	ss Y Mod	el Firmware Version	∀ Group	Uptime
🖳 Guests	b4:5d:50:c	Online	10.224.254	161 AP-324	10.1.0.2_77953	AOS10	6 Hours 28 Minutes 55 Seconds
	b4:5d:50:	Online	10.224.254	198 AP-324	10.1.0.2_77953	AOS10	2 Hours 49 Minutes 33 Seconds
Applications							
Applications	Access Points Switches Gat	ू न eways					iii. uu
Applications AOS10 Anage	Access Points Switches Gat	ू eways e o Offline	Clusters				ii ii
Applications Aopsto Aosto	Access Points Switches Gat	e o Offline 0	Ciusters 1				# G
Applications AOS10 Manage Overview Overview Devices	Gateways • Online 2 CATEWAYS (2)	eways • Offline 0	Clusters 1				H u
 Applications AOS10 (Manage (のverview) Overview Devices Clients 	Gateways • Onlin 2 2 CACTEWAYS (2) CATEWAYS (2) Content of the second se	eways e Offline 0	Clusters 1 Y IP Address	∀мас	Firmware Version	∑ Group	Lightime
副 Applications S AOS10 Manage Overview D Devices C Clients G Guests G Guests	Gateways • Online Cateways • Online V Device Name	eways e Offline 0 V Model A7005	Clusters 1 V IP Address 192.168.1.242	▼ MAC 20:4C: ▼	Firmware Version 10.1.0.2_77953	У Group АО510	I Uptime 7 Hours 42 Minutes 41 Seconds

Notice that there is one gateway cluster. The cluster will automatically be formed between gateways on the network using their system IP addresses.

4.6 Gateway Cluster

Cluster is a combination of multiple MDs working together to provide high availability to all the clients and ensure service continuity when a failover occurs. The gateways need not be identical and can be either L2- connected or L3- connected with a mixed configuration. In case of failover, the client SSO works for the L2- connected managed devices and the clients are de-authenticated for L3-connected managed devices in a cluster.

The aims of clustering are

- seamless Campus Roaming: When a client roams between APs of different managed devices within a large L2 domain, the client retains the same subnet and IP address to ensure seamless roaming. The clients remain anchored to a single managed device in a cluster throughout their roaming area which makes their roaming experience seamless because their L2 or L3 information and sessions remain on the same managed device.
- Hitless Client Failover: When a managed device fails, all the users fail over to their standby managed device seamlessly without any disruption to their wireless connectivity or existing high-value sessions.
- Client and AP Load Balancing: When there is excessive workload among the managed devices, the client and AP load is evenly balanced among the cluster members. Both clients and APs are load balanced seamlessly.

4.7 Monitoring Gateway Cluster

Here is how to check the gateway cluster

🛱 AOS10 💦	O Access Po	oints Switches Gatew	ays											i List	ll. Summary	© Config
- Manage	Ga	iteways Clusters														
B Overview		2 1														
Devices		•														
🖬 Clients	GAT	EWAY CLUSTERS (1)													.↓	\odot
& Guests	N	ame	Group	AP Tunnel	Clients		Model	Site	Version		Hitless Fa	ilover	Max Gates	way Failover		
	× .	auto_gwcluster_178_0 (2	AOS10	4	2		A7005		10.1.0.2_7	77953	POSSIBLE		1			
Applications																
Security		Gateway Name	AP Tunnel	Clients		Model		Site		Version		MAC Address		IP Address		
Analyze		7005_AOS10_gwy1	2	1		A7005				10.1.0.2_77953		00:0b:86:b8:80:d0	15	92.168.1.243		
Alorts & Evonts		7005_AOS10_gwy2	2	1		A7005				10.1.0.2_77953		20:4c:03:1a:2f:b4	19	92.168.1.242		

← auto_gwcluster_1 ⊘	Summary Gateways Tunnels				3 hours
- Manage	GATEWAY CLUSTER DETAILS				
BB Overview - Analyze	CLUSTER INFO CLUSTER NAME auto_gwcluster_178_0 MAX: GATEWAY FAILURE WITHSTAND COUNT 1	CLUSTER CLIENT CAPACITY 4096 SITE	VLAN MISMATCH Yes	CURRENT LEADER VERSION 10.1.0.2,77953	
	CLIENT CAPACITY	7005_AOS10_GWY1 7005_AOS10_GWY2 Mr 12,221,1513	Mar 12, 2021, 1643 Mar 12, 2027, 1813	50% 50% 50% 50% constd	

auto_gwcluster_1	Summary Gateways	 Tunnels					
iage	GATEWAY CLUSTER DET	AILS					
Overview							
lyze	GATEWAYS (2)						
Alexte 9 Duente	Gateway Name	IP Address	Status	Client Capacity (Active Standby)	Model	Role	Version
AIGHTS & EVENILS	7005_AOS10_gwy1	192.168.1.243	Up	1 (0 1)	A7005	Member	10.1.0.2_77953
Audit Trail	7005_AOS10_gwy2	192.168.1.242	Up	1 (1 0)	A7005	Leader	10.1.0.2_77953
	GATEWAYS 7005.AO	DS10_GWY1 ❤					
	GATEWAYS 7005,AO GATEWAY PEER DE	DS10_GWY1 ↓ TAIL (2)					
	GATEWAYS 7005_AO GATEWAY PEER DE Type	DS10_GWY1 ~ TAIL (2) IP Address	Stat	tus	Role	VLAN Mismatch	
	GATEWAYS 7005_AO GATEWAY PEER DET Type SELF	DS10_GWY1 ~ TAIL (2) IP Address 192.168.1.243	Stat	tus	Role Member	VLAN Mismatch	

← auto_gwcluster_1 ⊘	Summary Gateways	els						3 hou
- Manage	GATEWAY CLUSTER DETAILS							
	TUNNEL DOWN - SUMM	ARY						\odot
▲ Allerts & Events	AP Name Y II	P Address Last	Connected	Last Key Recd By	AP Last Key Reco	By Gateway Reas	son Ga	ateway Name
Audit Trail								
					B			
				No da	ta to display right now			
	GATEWAYS 7005_AOS10_G	WY1 🗸						
	TUNNEL DETAILS							\odot
	AP Name	▼ IP Address	SSID	Status	Uptime	Last Key Recd By Gateway	Last Key I	Recd By AP
	b4:5d:50:c6:82:3c	10.224.254.198	school	Up	15 Mins 41 Secs	15 Mins: 47 Secs ago		
	b4:5d:50:c6:82:4a	10.224.254.161	school	Up	15 Mins 42 Secs	15 Mins: 47 Secs ago		

Here is the CLI command to check the operation of the cluster.

```
(7005 AOS10_gwy1) #show lc-cluster group-membership
Cluster Enabled, Profile Name = "auto gwcluster 178 0"
Heartbeat Threshold = 900 msec
Cluster Info Table
_____
Type IPv4 Address Priority Connection-Type STATUS

        self
        192.168.1.243
        128
        N/A CONNECTED (Member)

        peer
        192.168.1.242
        128
        L2-Connected CONNECTED (Leader)

                               N/A CONNECTED (Member)
(7005_AOS10_gwy1) #show lc-cluster load distribution client
Cluster Load Distribution for Clients
Type IPv4 Address Active Clients Standby Clients
---- ------
self 192.168.1.243
peer 192.168.1.242
                                0
                                                1
                               1
                                                0
Total: Active Clients 1 Standby Clients 1
(7005_AOS10_gwy1) #
(7005_AOS10_gwy1) #show lc-cluster load distribution ap
Cluster Load Distribution for APs
Type IPv4 Address Active APs Standby APs
_____ _____
self192.168.1.24311peer192.168.1.24211
Total: Active APs 2 Standby APs 2
```

(7005_AOS10_gwy1) #

Now checking the second gateway. Note we have 1x client and 2x APs that are connected.

Cluster Load Distribution for Clients -----Type IPv4 Address Active Clients Standby Clients 1 peer 192.168.1.243 0 self 192.168.1.242 1 0 Total: Active Clients 1 Standby Clients 1 (7005 AOS10 gwy2) # (7005_AOS10_gwy2) #show lc-cluster load distribution ap Cluster Load Distribution for APs -----Type IPv4 Address Active APs Standby APs 1 peer 192.168.1.243 1 self 192.168.1.242 1 1 Total: Active APs 2 Standby APs 2 (7005_AOS10_gwy2) #

5 ClearPass Initial Configuration

Here we'll do the basic ClearPass configuration and join it to the AD domain along with creation of dot1x service policy. We'll start with NTP and time zone.

Monitoring Configuration Administration	Administration > Server Manager > Set Server Configuration Publisher Server: victory [192.168.	rver Configuration			 Change Clus Cluster-Wid Clear Machin Make Subsc Manage Poli NetFyrents 1 O Set Date & Virtual IP Set 	ster Password e Parameters ne Authenticat riber cy Manager Zo argets Time titings	ion Cac ones
- Dog Configuration - Docal Shared Folders	# Server Name ▲	Management Port	Data Port	Zone	Cluster Sy	nc Last S	ync Tin
- Jucensing	1. victory	(IPv4) 192.168.1.95	-	default	Enabled	-	
- Device Insight	Showing 1-1 of 1			Collect Logs Back Up	Restore Cleanup	Shutdown	Rebo
This will change Date & Time Date & Time Time Zon	e for all nodes in the cluster: e on Publisher	This wi	l change Date & Time e & Time Time Zor	e for all nodes in the clus	ster:		
Synchronize time with NT	P server	To c	hange the time zon	e, select your area fro	m the list below:	:	
Primary Server:		Afric	a/Abidjan			^	
NTD Common	216.239.35.4	Afric	a/Accra				
NTP Server		Afric	a/Addis Ababa				
Key ID		And	-,				
Key ID Key Value		Afric	a/Algiers				
Key ID Key Value Algorithm		Afric Afric Afric Afric	a/Algiers a/Asmara a/Asmera				
Key ID Key Value Algorithm		Afric Afric Afric Afric Afric	a/Algiers a/Asmara a/Asmera a/Asmera a/Bamako				
Key ID Key Value Algorithm Secondary Server (1):		Afric Afric Afric Afric Afric Afric	a/Algiers a/Asmara a/Asmera a/Bamako a/Bamako a/Bangui				
Key ID Key Value Algorithm Secondary Server (1): NTP Server		Afric Afric Afric Afric Afric Afric Afric	a/Algiers a/Asmara a/Asmera a/Bamako a/Bangui a/Bangui				
Key ID Key Value Algorithm Secondary Server (1): NTP Server Key ID		Afric Afric Afric Afric Afric Afric Afric Afric	a/Algiers a/Asmara a/Asmera a/Bamako a/Bangui a/Banjul a/Bissau			~	
Key ID Key Value Algorithm Secondary Server (1): NTP Server Key ID Key Value		Afric Afric Afric Afric Afric Afric Afric Afric	a/Algiers a/Asmara a/Asmara a/Asmera a/Bamako a/Bangui a/Banjul a/Bissau	Australia/Melhourne//	:MT +11·00)	~	
Key ID Key Value Algorithm Secondary Server (1): NTP Server Key ID Key Value Algorithm		Afric Afric Afric Afric Afric Afric Afric Afric	a/Algiers a/Asmara a/Asmara a/Asmera a/Bamako a/Bangui a/Banjul a/Bissau ent time zone:	Australia/Melbourne(0	:MT +11:00)	~	

Save Cancel

Save Cancel

≅Щ Mashboard O	Administration » Server Manage	r » Server Config	ration - victory					
Monitoring O	Server Configuration	- victory (1	92.168.1.95)					
🖧 Configuration 🛛 🔹 🛛								
🚰 Administration 📀								
ClearPass Portal Gerrar and Privileges Server Manager Server Configuration	System Services Control Hostname:	Service Parame	ters System Monitorin	g Network FIP	s			
Berver configuration Berver configuration Berver configuration Berver configuration Berver configuration	Policy Manager Zone: Enable Performance Monitoring	Display: Carbon	this server for performa	nce monitoring display	<i>,</i>	Manage Polic		
Device Insight	Insight Setting:	🗹 Enab	Insight	Enable as Insight Mas	ter Current Master:-			
🗉 🖥 External Servers	Enable Ingress Events Processi	ng: 🗌 Enab	Enable Ingress Events processing on this server					
External Accounts	Master Server in Zone:	Primary	Primary master V					
	Span Port:	None	None V					
			IP	/4	IPv6	Action		
- Jb OnGuard Settings - Jb Software Updates	Management Port	IP Address Subnet Mask		192.168.1.95 255.255.255.0		Configure		
		Default Gateway	19	2.168.1.249				
		IP Address						
	Data/External Port	Subnet Mask				Configure		
		Default Gatewa						
		Primary	19	2.168.1.250				
	DNS Settings	Secondary	19	2.168.1.130		Configure		
		Tertiary						
		DNS Caching	Dis	abled				
	AD Domains:					Join AD Domain		

5.1 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 Ne	twork FIPS	
Policy Mana	ger Zone:	default	•		Manage Policy Manager Zones
Enable Prof	Join AD Domain			0	
Enable Perf				ig display	
Insight Set	Enter the FQDN of domain:	the controller and the sh	nort (NETBIOS) name for the	ht Master Current Master:-	
DHCP Span	Domain Controller	wlan-dc.wlan.net			
	NetBIOS Name	WLAN		TDv6	Action
	In case of a contro	ller name conflict		1640	Action
Manageme	● Use specif ◎ Use Doma ◎ Fail on cor	ied Domain Controller in Controller returned by nflict	γ DNS query		Configure
Data /Exte	🗹 Use default doma	ain admin user [Adminis!	trator]		Configure
Dutu/ LAtt	Username				comgato
	Password	••••••			
DNS Settii			Save Cancel		Configure
	10100	•)			
AD Domain	is:	Policy Manager is not	part of any domain. Join to c	Jomain here.	Join AD Domain
•					

Join AD Domain 📀	Join AD Domain	
Adding host to AD domain	Added host to the domain	
Adding host to AD domain INFO - Fetched REALM 'WLAN.NET' from domain FQDN 'wlan-dc.wlan.net' INFO - Fetched the NETBIOS name 'WLAN' INFO - Creating domain directories for 'WLAN' INFO - Using Administrator as the WLAN-DC's username Enter Administrator's password: Using short domain name WLAN Joined 'CP63LAB' to dns domain 'wlan.net' INFO - Creating service scripts for 'WLAN' Starting cpass-domain-server_WLAN: [OK]	INFO - Creating service scripts for 'WLAN' Starting cpass-domain-server_WLAN: [OK] INFO - updating domain configuration files Stopping cpass-domain-server_WLAN: [OK] [OK] Starting cpass-domain-server_WLAN: [OK] Stopping cpass-sysmon-server: [OK] Starting cpass-radius-server: [OK] Starting cpass-radius-server: [OK] Starting cpass-radius-server: [OK] INFO - CP63Lab joined the domain WLAN.NET	
Close		Close

Now we need to add the AD as authentication source

	onfiguration » Authentication » Sources » Add - Ariya AD									
Monitoring • A	uthentication Sou	urces - Ariya AD								
Configuration 📀	Summary General F	Primary Attributes								
Service Templates & Wizards Na Services Authentication Authentication De Sources Ty Identity Us Local Users Authentics Endpoints Static Host Lists Roles Roles Role Mappings See Posture Ca Network Ba Policy Simulation Simulation	ame: escription: ype: se for Authorization: uthorization Sources: erver Timeout: ackup Servers Priority:	Ariya AD Ariya AD Active Directory C Enable to use this Authentication Source to also fetch role mapping attributes Remove View Details Select ID seconds 36000 seconds Add Backup Remove Remove								

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	Po	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	Bind DN: administrator@wlan.net						
- 🛱 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	Always use NetBIOS name: Enable 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			
Gingle 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	-		

5.2 ClearPass dot1x Service

Here we create a dot1x service for wireless access.

aru	ba					ClearPass	Policy Manager		Menu 📕	
Mor	hboard litoring <mark>figuration</mark> rvice Templates & Wizards	0 0 0	Configuration » Services Services							
- 🋱 Se - 🏝 Au	thentication		Filter: N	lame		✓ [contains ∨]	+ Go Clear Filter		Show 20 v records	
	 Q Sources A Single Sign-On (SSO) Q Local Users D Local Users D Endpoints Q Static Host Lists Q Roles Q Role Mappings 		1. 2. 3. 4. 5. 6.		raer 🔺	[Anite] [Delicy Manager Admin Network Login Ser [AirGroup Authorization Service] [Aruba Device Access Service] [Guest Operator Logins] [Insight Operator Logins] [Insight Operator Logins] [Device Registration Disconnect]	rice] TACACS RADIUS TACACS Application Application WEBAUTH	TACACS+ Enforcement TACACS+ Enforcement RADIUS Enforcement (Generic) TACACS+ Enforcement Aruba Application Authentication Aruba Application Authentication Web-based Authentication		
e ♥ Po Sur	nmary Service	Authenticatio	on Ro	les Er	nforcem	ent	KAUIUS	Aluda 602.1A Wireless		
Name Desci	:: ription:	AA Aruba 803 To authens wireless	2.1X Wire ticate network	users to via 80	o an An 2.1X.	uba				
Туре	:	Aruba 802.1	1X Wirele	ess						
Statu	IS:	Enabled								
Monit	or Mode:	Enable t	o monito	or networ	rk acces	s without enforcement				
More	Options:	Authoriz	ation [Postur	e Compl	iance 🗌 Audit End-hosts 🗌 Pr	ofile Endpoints 🗌 Accounting P	Proxy		
						Se	rvice Rule			
Match	nes O ANY or 🖲 A	LL of the follo	owing co	onditions						
	Туре		Name Operator Value							
1.	Radius:IETF				NAS-Po	t-Type	EQUALS	Wireless-802.11 (19)	Ba ti	
2.	Radius:IETF				Service	Туре	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)		

EQUALS

school

Aruba-Essid-Name

з.

4.

Radius:Aruba

Click to add.

0)

Ť

Summary	Service	Authentication R	Roles Enforcement	
Authenticatio	n Methods:]
		[EAP TIS]		
				Move Up ↑
				Move Down ↓
				Remove
				View Details
				Modify
			~	
		Select to Add	~	
Authoraticatio	n Courcost			7
Authenticatio	n Sources:	Ariya AD [Active Dir	rectory]	
				Move Up ↑
				Move Down ↓
				Remove
				View Details
				Modify
			*	
		Select to Add		<u> </u>
Strip Usernam	ne Rules:	Enable to spec	cify a comma-separated	list of rules to strip username prefixes or suffixes
Service Certif	icate:	Select to Add	~	
Summary Se	ervice Auth	nentication Roles Enfo	orcement	
Role Mapping Poli	cy:	Select	✓ Modify	Add New Role Mapping Poli
			Role Mapping Policy	y Details
Description:	-			
Default Role:	-			
Rules Evaluation	Algorithm: -			
Conditions				Role
Summary Servic	e Authenticati	ion Roles Enforcement		
Use Cached Results:	Use ca	ched Roles and Posture attributes	from previous sessions	
Enforcement Policy:	AA Aruba	802.1X Wireless Enforcement Policy	✓ Modify	Add New Enforcement Polic
			Enforcement Policy I	Details
Description:				
Default Profile:	AA Aruba	802.1X Wireless Default Profile		
Condition	ionni: Insc-appli			Enforcement Droffler
1. (Authorization	n:Ariya AD:memb	erOf CONTAINS Staff)		AA-Aruba 802.1X Wireless Staff Profile, AA Aruba 802.1X Wireless Update Endpoint
2. (Authorization	1:Ariya AD:memb	erOf CONTAINS Student)		Location AA-Aruba 802.1X Wireless Student Profile, AA Aruba 802.1X Wireless Update Endpoint
(Tips:Role EC	QUALS [Machine	Authenticated])		Location AA-Aruba 802.1X Wireless Staff Profile, [Undate Endnoint Known]
AND (Author (Tips:Role EC	orization:Ariya AD QUALS [Machine	<pre>ememberOf CONTAINS Staff) Authenticated])</pre>		AA Aniba 802 IX Wireless Staff Profile, [opuate Engloint Known]
4. AND (Autho	orization: Ariya AD	memberOf CONTAINS 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
•	AA Aruba 802.1X Wireless Update Endpoint Location	Post_Authentication

Enforcement Profiles - AA Aruba 802.1X Wireless Default Profile

Note: This Enforcement Profile is created by Service Template

Summary Pro	file Attributes		
ofile:			
Name:	AA Aruba	802.1X Wireless Default Profile	
Description:			
Type:	RADIUS		
Action:	Accept		
Device Group List:	-		
Attributes:			
Туре		Name	١
1. Radius:Aruba	3	Aruba-User-Role	=

Enforcement Profiles - AA-Aruba 802.1X Wireless Staff Profile

Note: This Enforcement Profile is created by Service Template

S	Summary	Profile	Attributes				
Pro	ofile:						
Name: AA-Aruba 802.1X Wireless Staff Profile							
De	scription:						
Тур	be:		RADIUS				
Act	tion:		Accept				
De	vice Group	List:	-				
Att	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			
e:				
me:	AA-Aruba	802.1X Wireless Student Profile		
scription:				
pe:	RADIUS			
tion:	Accept			
evice Group List:	-			
tributes:				
Туре		Name		Valu
Radius:Aruba		Aruba-User-Role	=	Stud
forcement Profiles	- AA Aruba 8	02.1X Wireless Update Endpoint Location		
	No	ote: This Enforcement Profile is created by Service Template		
Summary Profile Attrib	No	te: This Enforcement Profile is created by Service Template		
ummary Profile Attribu	No	te: This Enforcement Profile is created by Service Template		
ummary Profile Attribution offile: me: AA	utes Aruba 802.1X Wire	te: This Enforcement Profile is created by Service Template		
Summary Profile Attribution rofile: ame: AA escription:	No utes Aruba 802.1X Wire	te: This Enforcement Profile is created by Service Template		

5.3 NAD Configuration

Last Known Location

Device Group List: Attributes:

1. Endpoint

Here we are adding Network Access Devices (NAD). This will be the AOS10 APs and gateways. Note that you need to either add the AP IP addresses individually or just add their subnet as I have done here.

Value %{Radius:IETF:NAS Location-Id}

=

	Non-standard and the second standards of the second standard standard standards and standards of the second standard standard st Standard standard st Standard standard st Standard standard stand Standard standard stand Standard standard stan Standard standard stand Standard standard stand Standar	
Monitoring	Network Devices	🛶 Add
Configuration		& Impor
2 Service Templates & Wizards		Export Discov
() Services	A fletwork Access Device (IMD) must belong to the global list of devices in the ClearRess database in order to connect to ClearRess.	
Authentication		
- Q Methods	Edit Device Details	Show 2
O Sources		and In
2 Identity	Davice SNMP Read Settings SNMP Write Settings CLI Settings OnConnect Enforcement Attributes	
-Q Single Sign-On (SSO)	ADS10-APs	
Q Local Users	2 IP or Subnet Address: 10.224.225.0/24	
- C Enapoints	(e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20 or 2001:db8:a0b:12f0::1)	
C Roles	Description:	
O Role Manager		
Posture		
Enforcement	KADIUS Shared Secret: Vermy:	
© Policies	TACACS+ shared secret: Verify:	
O Profiles	Vendor Name : Aruba *	
-Network	Enable RADIUS Dynamic Authorization: 🗹 Port: 5799	
O Devices	Enable RadSec:	
Device Groups		
- O Proxy Targets		
C Event Sources		
Network Scan		
	Capy Save Canad	
Pashboard Monitoring	Copy Saw Conce Contguation - National - Education Network Devices	Add
Dashboard Monitoring Configuration	Corpy Saw Concer	Add & Impor
Dashboard Meniltaring Configuration) Service Templates & Wizards	Copy Son Conce Configuration - Notices Network Devices	<mark>⊯ Add</mark> ▲ Impo ● Expo Ø Disco
Doshboord Monitoring Configuration) Service Templates & Wizardh 3 Service Services	Configuration - Network - Devices Configuration - Network - Devices Network Devices A Network Access Device (Md) must belong to the global lot of devices in the ClearRess detabase in order to connect to ClearRess.	<mark>∳ Add</mark> & Impo & Expo ♦ Disco
Deskloard Monitoring Configuration :Service Templates & Wizarda Services Jathenication	Correct Access Device (M40) must belong to the global lot of devices in the Charltess database in order to connect to Charltess.	<mark>. ● Add</mark> ▲ Impo ▲ Expo ● Disco
Deskilvard Mohibridg Configuration Service Templates & Wizards Services Services Services	Conjugation - Nation's - Devices Conjugation - Nation's - Devices Network Devices A Retwork Access Service (Md) must belong to the global lat of devices in the ClearRess database in order to connect to ClearRess. Rese I did borks betain	and Anno € Espo ⊕ Disco Show
Desklaard Nesklaard Configuration Service Touglates & Wizerla Services Services Services Services Services	Copy Inst Configuration - Network - Devices Network Devices A heterork Access Device (M40) must belong to the global lot of devices in the Charltess database in order to connect to Charltess. Rec full Device belon	<mark>. ∳ Add</mark> & Impo & Espo ♥ Disco Show
Decklosard Molitoring Conference Templates & Wizarda Services Templates & Wizarda Services Services O Mothoda O Mothoda O Mothoda O Mothoda	Corp. Son Condignation - Honorch - Devices Condignation - Honorch - Devices A Horburch Access Gevice (MG) must belong to the global list of devices in the Charless database in order to connect to Charless. File full Device Databa Device Stells Pland Settlings SHIP Webs Settlings CL1 Settlings Out-connect Attributes	iæ Add ▲ Impo ● Disco Show
Durskhaard Realizering Service Translates & Wizards Services Services Services Services Services Services Services Services Services Services	Copy Tax Constant Configuration - Instruct Daylers Configuration - Instruct Daylers A Instruct Access Device (MdI) must belong to the global lot of devices in the Charltees database in order to connect to Charltees. Rec If Device Shalls Content Information Atcludes Content Information Atcludes Content Information Atcludes Content Information Co	<mark>∳Add</mark> & Impo ♦ Disco show[
Destabused Modificing Configuration Service Templates & Wizzels Services Se	Corp. Exe Conduction - Instance: - Devices Conduction - Instance: - Devices Conduction - Instance: - Devices Conduction - Devices Condu	₽ Add ▲ Impo ▲ Expo ● Disco Show [
Dauhaard Moduloring Cardigustion Services Servic	Corp. In the second sec	<mark>● Add</mark> ▲ Impo ● Disco show
Destabused Modification Configuration Service Templates & Wizzels Services Servic	Condiguration := Instance: = Devices Network Devices A Redwork Access Device (N40) must being to the global list of devices in the Charltess database in order to connect to Charltess. File Idd Device Databas Overoit Devices Network Access Device (N40) must being to the global list of devices in the Charltess database in order to connect to Charltess. File Idd Device Databas Point Point Adress: 103:14:142-21 Cig., 102:156.1.1/2 or 102:166.1.1/2 or 102:166.1.	₽ Add A Impo & Expo ♥ Disco Show [
Dauhaand Maalaand Cardigaata Sarves S	Configuration - Instruct - Devices Configuration - Instruct - Devices A Retwork Access Device (MAD) must belong to the piblial lot of devices in the ClearRess database in order to connect to ClearRess. For full Device Intel The State Read Setting SMPP Write Settings Cli Settings Outcoment Information Attributes P or Subast Advess: D or 10 212461.120-240 D occiptor: D occiptor: D occipto	<mark>● Add</mark> ▲ Impo ● Disco Show
Destabused Destabused Configuration Service Templates & Wizzels Services	Configuration + Network + Davies Configuration + Network + Davies Network Devices A Network Access Device (MKI) must belong to the global bit of devices in the Charltese database in order to connect to Charltese. Provide State Access Device (MKI) must belong to the global bit of devices in the Charltese database in order to connect to Charltese. Provide State Access Device (MKI) must belong to the global bit of devices in the Charltese database in order to connect to Charltese. Provide State Access Device (MKI) must belong to the global bit of devices in the Charltese database in order to connect to Charltese. Provide State Access Device (MKI) must belong to the global bit of devices in the Charltese database in order to connect to Charltese. Provide State Access Device (MKI) must belong to the global bit of devices in the Charltese database in order to connect to Charltese. Provide State Access Device (MKI) must belong to the global bit of devices in the Charltese database in order to connect to Charltese. Provide State Access Device (MKI) must belong to the global bit of devices in the Charltese database in order to connect to Charltese. Provide State Access Device (MKI) must belong to the global bit of the Unit of the U	₽ Add La Impo Se Dated Shore [
Santa e analastan Santa e anala	Configuration - Instruct - Devices Configuration - Instruct - Devices Retwork Access Device (MoD) must belong to the piblial lot of devices in the ClearRess database in order to connect to ClearRess. Profile Table Road Setting: Device Table Road Setting:	● Add Lampe © Disc Show
Destabused Destabused Configuration Services Templates & Wizzels Service	Configuration + Network + Davies: Configuration + Network + Davies: Network Devices A Network Access device (MO) must belong to the global lat of devices in the Charltese database in order to connect to Charltese. Provide State Access Device (MO) must belong to the global lat of devices in the Charltese database in order to connect to Charltese. Provide State Access Device (MO) must belong to the global lat of devices in the Charltese database in order to connect to Charltese. Provide State Access Device (MO) must belong to the global lat of devices in the Charltese database in order to connect to Charltese. Provide State Access Device (MO) must belong to the global lat of devices in the Charltese database in order to connect to Charltese. Provide State Access Device (MO) must belong to the global lat of devices in the Charltese database in order to connect to Charltese. Provide State Access Device (MO) must belong to the global lat of devices in the Charltese database in order to connect to Charltese. Provide State Access Device (MO) must belong to the global lat of devices in the Charltese database in order to connect to Charltese. Provide State Access Device (MO) must belong to the global lat of devices in the Charltese (MO) must belong to the global database (MO) must beload to the global d	₽ Add La Impo S Dated Shore
Next Annual Control Co	Configuration - Indexed: - Environ Configuration - Indexed: - Environ Configuration - Indexed: - Environ Performed: Configuration - Environ A Retwork Access: Busine (Molt) must balance to the plobal lost of devices in the ClearMean database in order to connect to ClearMean. Point State Rand Setting: Device State Setting: Device State Section: Weight: Device Section: Weight:	€ Add Mappo € Expo Show Show
Deskhoard Koshorda Configuration Services	Configuration + Noticesk + Davies: Configuration + Noticesk Chronic Devices A Indexert Access device (MSI) must belong to the global late of devices in the Charltese database in order to connect to Charltese A Indexert Access device (MSI) must belong to the global late of devices in the Charltese database in order to connect to Charltese A Indexert Access device (MSI) must belong to the global late of devices in the Charltese database in order to connect to Charltese A Indexert Access device (MSI) must belong to the global late of devices in the Charltese in order to connect to Charltese Field Device Database Field Device Datab	€ Add & Impo & Dieco Source Source
Destinante Configuration Configura	Configuration - Induced - Devices Configuration - Induced - Devices Percent Access device (MoD) must belong to the piblical loci of devices in the ClearMess database in order to connect to ClearMess. Point for the Read Setting: Point for the Read Read Read Setting: Point for the Read Read Read Setting: Point for the Read Read Read Read Read Read Read Rea	€ Add ≧ Enpo ● Disco Snov Corr Est
Deshaver Des	Configuration - Network - Devices Central Configuration - Network - Devices Activation Secure (MKD) music belongs to the global lact of devices in the Chartese statistics in order to connect to Charteses Part Configuration - Devices Activation - Devices Configuration - Secure (MKD) music belongs to the global lact of devices in the Charteses in order to connect to Charteses Part Configuration - Devices Configuration - Devices <td>€ add E Impo Show [Show]</td>	€ add E Impo Show [Show]
Deside-and Nonitation Configuration Configuration Service Templates & Watards Services Ser	Conjugation - Reduced - Environ Performance Reduced Reduce (Mod2) mund: Subley fait the piblical fact of devices in the ClearRese distations in order to connect to ClearRese. Point State Reduce (Mod2) mund: Subley fait the piblical fact of devices in the ClearRese distations in order to connect to ClearRese. Point State Reduce State(scale St	€ Add ▲ Impo ● Disco Show
Configuration Config	Conjunction - National A-Division Conjunction - Section	€ Add ▲ Impo ● Deco Show [[Doy] Exr
Desidenard Roalinear Configuration Service Trapholets & Waards Services		€ Add ▲ Impo ● Disco Snow

6 WLAN Configuration

Here we'll configure the AOS10 APs to broadcast a tunnelled SSID. This is done at the group level.

6.1 **Tunnelled Wireless Configuration**

\$3 AOS10	Access Points Switches					III III List Summary Config
— Manage —	WLANS Access Points Radios Inter	aces Security Services System C	onfiguration Audit			Hide Advanced
BB Overview						
Devices	Wireless SSIDs					
🗈 Clients	DISPLAY NAME	OPMODE	ACCESS_TYPE	VLAN FORWARDING MODE	ACTIONS	
🔉 Guests						
# Applications				. –		
Security			14	III E		
— Analyze —						
Alerts & Events			No data	to display		
🛛 Audit Trail						
🖏 Tools						0.55(D(s)
업 AOS10	Access Points Switches Gateways					List Summary Config
— Manage —	WLANS Access Points Radios Inter	aces Security Services System C	onfiguration Audit			Hide Advanced
BB Overview						
Devices	CREATE A NEW NETWORK					
Clients	1 General 2 VLA	Is ③ Security ④ Act	cess (5) Summary			
😩 Guests	Name (SSID):		school			
Applications	conce (asse).					
Security	> Advanced Settings					
- Analyze						
∴ Alerts & Events						
Audit Trail						
S Tools					Ca	Next

You can choose the cluster from the menu. Also note that the VLAN IDs are being displayed from the gateways.

법 AOS10 〇	Access Points Switches Gateways		i≣ II. List Summary Co
– Manage –	WLANs Access Points Radios Interfaces Security Services System	Configuration Audit	Hide Advan
B Overview			
Devices	CREATE A NEW NETWORK		
Clients	1 General 2 VLANs 3 Security 4	Access 3 Summary	
🚉 Guests	Traffic forwarding mode:	Bridge Tunnel Mixed	
Applications	name to har any model		
Security	Primary Gateway Cluster:	AOS10 auto_gwcluster_178_0	
- Analyze	Secondary Gateway Cluster:	None	
Alerts & Events		Static Dynamic	
Audit Trail	Client VLAN Assignment:		
🖏 Tools	VLAN ID:		
Reports	> Show Named VLANs		
- Maintain			
g Filliwale			
업 AOS10 〇	Content of the second of the s	Configuration Audia	List Summary
Manage	Accessions neuros interaces Security Services System	coniguiadon Addic	Hide Advanc
Devices	CREATE A NEW NETWORK		
Clients	1 General 2 VI ANS 3 Security (4) A	Arcess Summary	
a. Guests			
Applications			
Security	Security Level:	Contraction Descention Destal One-	
Analyze		cinterprise Personal Captive Portal Open	
Alerts & Events			
🛛 Audit Trail	Key Management:	WPA2 Enterprise	
🖏 Tools			
Reports	Primary Server:	ClearPass-GW + /	
Maintain	Secondary Server:	- Select - 🔻 +	
Firmware			
	Advanced Settings		

Select the authentication server that we had configured on the gateways. It gets automatically populated using the drop down menu. Note that this is not the RADIUS server that we configured in the AP group but rather from the gateway group. Next select Accounting from the advance Setting section

ជ AOS10 이	Contraction Contra		Eist Summary
— Manage —	WLANs Access Points Radios Interfaces Security Services System Configuration Aud	iit.	Hide Advan
8 Overview	V Advanced Settings		
Devices			
Clients	Use Session Key for LEAP:		
Guests	Perform MAC authentication before 802.1X:		
Security	MAC Authentication Fail-Through:		
- Analyze	Reauth Interval:	0 min V	
û Alerts & Events	Denylisting:		
🛛 Audit Trail	Max Authentication Failures:	0	
🖏 Tools	Enforce DHCP:		
Reports Maintain	Lise IP for Calling Station ID:		
Firmware	ose in for caning station by		
	Called Station ID Type:	MAC Address	
	Called Station ID Include SSID:		
	Accounting		
	Accounting:	Use authentication servers V	
	✓ Advanced Settings		
	Use Session Key for LEAP:		
	Perform MAC authentication before 802.1X:		
	MAC Authentication Fail-Through:		
	Reauth Interval:	0 min V	
	Denylisting:		
	Max Authentication Failures:	0	
	Enforce DHCP:		
	Use IP for Calling Station ID:		
	Called Station ID Type:	MAC Address	
	Called Station ID Include SSID:		
	 Accounting 		
	Accounting:	Use authentication servers	
	Accounting Interval:	1 min	
ជ AOS10 〇	Access Points Switches Gateways		:Ξ IIi List Summary C
— Manage ———	WLANS Access Points Radios Interfaces Security Services System Configuration Aut	dit	Hide Advar
B Overview			
Devices	NELWORNS > CONFIGURATION - SCHUUL		
Eu Clients	Consult MIANIN Consulty Assess Community		

🙁 Guests	General VLANs Security Access Summary	
Applications	Access rules	0
Security		Role Based Unrestricted
- Analyze	ROLE	ACCESS RULES FOR SELECTED ROLES
Alerts & Events	school	Allow any to all destinations
Audit Trail		
🖏 Tools		
n Reports		

And save the configuration.

aruba central Im				0 0 11 8
II AOS10				the O
+ Maragal	SUCCESS			Hide Advanced
BB Overview				
Devices	school is Configured Successfully			
25 Clients	ок			
🕮 Guests		manne na marung fitode		
Applications				
@ Security				
- Analyte				

6.2 Wireless dot1x Testing

First, we'll check the gateway authentication server configuration, the highlighted lines were pushed form the AP's tunnel configuration.

II AOS10 O	ල Access Po	ints Switches Gateways				selected gro Gateway	UP TYPE	ili Summary Cont	
Manage	System	Interface Routing WAN Security VI	PN High Availability Config Audit					Basic Mode	
B Overview	Roles	Policies Aliases Applications App	y Policy Auth Servers Role Assign	nment (AAA Profiles) L2 Authenti	ication L3 Authentication Ad	vanced Firewall			
Devices	✓ Authentication Servers								
🗖 Clients		Server groups							
🔉 Guests		NAME	SERVERS	FAIL THROUGH	LOAD BALANCE	SERVER RULES		=	
Applications		school_#1615532079504_41#acct_svg	1			0			
Security		s <mark>chool_#1615532079504_41#auth_svg</mark>	1		-	0			
— Analyze ———		s <mark>chool_#1615532079504_41#cp_svg</mark>	1	-		0			
☆ Alerts & Events									
Audit Trail									
🖏 Tools		+							
🗊 Reports									
— Maintain ————		All servers							
Firmware		NAME	ТҮРЕ	IP ADDRESS / HOSTNAME	SERVER GROUP			=	
		ClearPass-GW	Radius	192.168.1.95	school #16155320	079504 41# acct svg scl			
			RFC 3576	192.168.1.95	-				

Now we'll get a laptop to connect to "school" SSID with staff1 user credentials and check ClearPass access tracker

aruba		ClearPass Policy Manager										
Dashboard O	Monitoring » Live	tonitoring » Live Monitoring » Access Tracker										
🗾 Monitoring 📀	Access Trac	Access Tracker Mar 12, 2021 18:03:31 AEDT										
Live Monitoring Access Tracker	The Access Trac	ker page provides a real-time display of per-sessio	n access activity on the selec	ted server or domain.								
- Accounting	Tall Request	s] victory (192.168	8.1.95)	Last 1 day before Tod	Edit							
- Analysis & Trending												
	Filter: Request ID	✓ contains ✓	Go Clear Filter	r		Show 20 \checkmark records						
	# Server	Source	Username	Service	Login Status	Request Timestamp 🕶						
	1. 192.168	3.1.95 RADIUS	staff1	AA Aruba 802.1X Wireless	ACCEPT	2021/03/12 17:58:39						

Note that 192.168.1.242 is the IP address of the gateway-1 and 10.224.254.161 is the IP address of the AP.

Request Detai	s								
Summary	Input	Output	t Accounting						
Login Status:		AC	ССЕРТ	^					
Session Ident	ifier:	RO	0000006-01-604b111f						
Date and Tim	e:	Ma	ar 12, 2021 17:58:39 AEDT						
End-Host Ide	ntifier:	AO	-88-B4-50-C0-84 (Computer / Windows / Windows)						
Username:			aff1						
Access Device IP/Port:			92.168.1.242						
Access Devic	e Name:	10.	10.224.254.161						
System Postu	ire Status	: UN	UNKNOWN (100)						
			Policies Used -						
Service:		AA	Aruba 802.1X Wireless						
Authenticatio	n Method	: EA	P-PEAP,EAP-MSCHAPv2						
Authenticatio	n Source:	AD	:192.168.1.250						
Authorization	Source:	Ari	iya AD						
Roles:		[Us	ser Authenticated]						
Enforcement	Profiles: 1 of 1-7 i	AA records	Aruba 802.1X Wireless Update Endpoint Location. AA-Aruba 802.1X Wireless	✓ Close					

Request Details	
Summary Input	Output Accounting
Enforcement Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless Staff Profile
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)
RADIUS Response	Θ
Endpoint:Last Known I	ocation 192.168.1.242:b4:5d:50:c6:82:4a
Radius:Aruba:Aruba-U	ser-Role Staff

Showing 1 of 1-7 records K Change Status Show Configuration Export Show Logs Close

And we also have the accounting tab, which indicates RADIUS accounting is working

Request betails	
Summary Input Output	Accounting
Account Session ID:	B45D50E824B0-A088B450C084-604B111F-EA565
Start Timestamp:	Mar 12, 2021 17:58:39 AEDT
End Timestamp:	Still Active
Status:	Active
Termination Cause:	-
Service Type:	-
Number of Authentication Sessions:	1
Network Details	0
Utilization	0
Authentication Sessions Details	•

I Show Configuration Export Show Logs Close

Lastly, we need to test if CoA is working, click on the "change status" to terminate the session

Request Details	8
Access Control Capabilities -	
Select Access Control Type : \bigcirc Agent \bigcirc SNMP \textcircled{O} RADIUS COA \bigcirc Server Action	
RADIUS CoA Type: [ArubaOS Wireless - Terminat >	

Request Details								
Radius [ArubaOS Wireless - Terminate Session] <mark>successful fo</mark> r client a088b450c084.								
Summary Input Output	Accounting							
Account Session ID:	B45D50E824B0-A088B450C084-604B111F-EA565							
Start Timestamp:	Mar 12, 2021 17:58:39 AEDT							
End Timestamp:	Still Active							
Status:	Active							
Termination Cause:	-							
Service Type:	-							
Number of Authentication Sessions:	1							
Network Details	0							
Utilization	0							
Authentication Sessions Details	0							

I< < Showing 1 of 1-7 records ►►I Change Status Show Configuration Export Show Logs Close

Now looking at Aruba Central pages.

및 AOS10 이	Lū Clients								O ∷ 3 hours List Summa
- Manage	CLIENTS ALL	~ c						244.08 MB (🟵 8.04	4 MB ⊕ 236.05 MB)
Devices	All O Conn	ecting O Connected	Falled Offlin O	ne ⊘B	ilocked Wireless	Wired	Remote		
🗈 Clients									
🚉 Guests									\odot
Applications	Y Client Name	Status 🚛	Y IP Address	VLAN	Connected To	Y Gateway Role	▼ SSID/Port	Y Health ✓	Usage
Security		O Connected	10.10.44.50	44	b4:5d:50:c6:82:4a	Staff	school		244.08 MB



← 🗔 staff1 🛛 ⊘	III Visibility				S hours 3 hours List Summa
- Manage	Applications Websites				
Overview					
Applications	APPLICATIONS Passive Monitoring				
- Analyze	Total Transferred: 1.4 GB				
☆ Live Events	APPLICATION	CATEGORY	USAGE	SENT	RECEIVED
☆ Events	YouTube	Streaming	1.3 GB (93.21%)	28.0 MB	1.3 GB
Tools	тср	Network Service	19.9 MB (1.40%)	386 KB	19.5 MB
1 0005	Microsoft	Office365 SAAS	2.2 MB (0.16%)	309 KB	1.9 MB
	HTTPS	Web	959 KB (0.07%)	101 KB	858 KB
	🕒 Google Ads	Google SAAS	355 KB (0.02%)	72 KB	284 KB
	Mozilla	Web	319 KB (0.02%)	57 KB	262 KB
	Google Generic	Google SAAS	212 KB (0.01%)	110 KB	102 KB
	Microsoft OneDrive	sharepoint_onedrive_saas	163 KB (0.01%)	12 KB	151 KB
	Netbios Name Service	Network Service	76 KB (0.01%)	76 KB	0 B
	🕒 Bing.com	Web	51 KB (0.00%)	7 KB	44 KB
	 Microsoft Azure 	Office365 SAAS	47 KB (0.00%)	3 KB	43 KB
	G SOAP	Network Service	42 KB (0.00%)	42 KB	0 B
	 Microsoft Office 365 	Office365 SAAS	35 KB (0.00%)	4 KB	31 KB
	Server Message Block	Network Service	13 KB (0.00%)	13 KB	0 B
	Unclassified	Unclassified	72.3 MB (5.08%)	798 KB	71.5 MB

Clicking on the gateway symbol takes us to the gateway that is terminating the user traffic

← เ๗ staff1 ⊘	Summary AJ Insights Location	Sessions								310
— Manage ———	CLIENT DETAILS	с							Actions 🔻	• Go Live
88 Overview	DATA PATH									
Applications		CLIENT		SSID		A.P	SWITCH	GATEWAY		
— Analyze ————			22222	(?)	>>>>>					
Live Events		staff1		school		b4.5d:50:c6:82:4a	Aruba-2930F-8G-PoEP-25FPP	7005_AO510_gwy2		
☆ Events		CONNECTED		UP		UP	UP	UP		
🔩 Tools										

← இ 7005_AOS10_gwy2 ⊘	Summary Routing	Sessions	Q Al Insights						3 hours
Manage								Actions 💌	• Go Live
器 Overview									
😞 WAN	DEVICE								
움 LAN	NAME 7005_AOS10_gwy2		SERIAL NUMBER CP0031855	MODEL A7005	MAC ADDRESS 20:4c:03:1a:2f:b4	SYSTEM IP ADDRESS 192.168.1.242	PUBLIC 203.6	IP ADDRESS 3.103.176	
Device	FIRMWARE VERSION 10.1.0.2_77953		POE (DRAW/MAX)	REDUNDANCY PEER	GROUP NAME AOS10	SITE	LABELS		
La Clients	UPTIME		4G/LTE MODEM STATUS	4G/LTE MODEM TYPE	NTP SERVER	CONFIG SYNC STATUS	LAST RI	EBOOT REASON	
Applications	9 hours 53 minutes		-		time2.google.com(Synchronized)	Update Successful 🛈	POE P	ower Cycle	
Security	CLUSTER NAME auto_gwcluster_178_0								

← ♀ 7005_AOS10_gwy2 ⊘	Lū Clients								€ 3 hou
- Manage	CLIENTS GATEWAY	с				244.0	08 MB (⊕8.0	4 MB)
Q WAN	All O Connecting	g O Connected O Faile 1 0	ed Offline ⊘ Blocked 0 0	Wireless Wire 1 0	ed Remote				
💑 LAN								(Ð
□ Clients		Status 🚛	Gateway Name	☆ Gateway Role	▼ IP Address	Port	VLAN	Usage	
# Applications	र्रे staff1	O Connected	7005_AOS10_gwy2	Staff	10.10.44.50	Tunneled	44	244.08 MB	

Now we'll run a few CLI commands.

Aruba AP BSS Table

bss flags	ess	port	ip	phy	type	ch/EIRP/max-EIRP	cur-cl	ap name	in-t(s)	tot-t	
b4:5d:50:e8:24:b0	school	?/?	10.224.254.161	a-VHT	ap	36E/15.0/21.5	1	b4:5d:50:c6:82:4a	0	1h:2m:16s	
b4:5d:50:e8:24:b1	Guest	?/?	10.224.254.161	a-VHT	ap	36E/15.0/21.5	1	b4:5d:50:c6:82:4a	0	4m:29s	0
b4:5d:50:e8:24:b2	owetm Guest2874425900	?/?	10.224.254.161	a-VHT	ap	36E/15.0/21.5	0	b4:5d:50:c6:82:4a	0	4m:28s	WO
b4:5d:50:e8:24:a0	school	?/?	10.224.254.161	g-HT	ap	3/7.5/21.5	0	b4:5d:50:c6:82:4a	0	1h:2m:15s	
b4:5d:50:e8:24:a1	Guest	?/?	10.224.254.161	g-HT	ap	3/7.5/21.5	0	b4:5d:50:c6:82:4a	0	4m:29s	0
b4:5d:50:e8:24:a2	_owetm_Guest2874425900	?/?	10.224.254.161	g-HT	ap	3/7.5/21.5	0	b4:5d:50:c6:82:4a	0	4m:28s	WO

Channel followed by "*" indicates channel selected due to unsupported configured channel. "Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:6

Flags: K = 802.11K Enabled; W = 802.11W Enabled; 3 = WPA3 BSS; O = Enhanced-open BSS with transition mode; o = Enhanced-open transition mode open BSS; M = WPA3-SAE mixed mode BSS; E = Enhanced-open BSS without transition mode; m = Agile Multiband (MBO) BSS; c = MBO Cellular Data Capable BSS; I = Imminent VAP Down; T = Individual TWT Enabled; t = Broadcast TWT Enabled b4:5d:50:c6:82:4a#

checking the IPSEC tunnels from the AP

b4:5d:50:c6:82:4a# sh ata endpoint

ATA Endpoint Stat	us								
UUID		IP ADDR	STATE		TUN DEV	TUN SPI(OUT/IN)	PORT (SRC/DST)	VALID TIME(s)	TUNNEL TYPE
GRE VLANs	HBT(Jiff/Missed/Sen	t/Rcv) INNER I	P	UP TIME(s)					
522d59ab-05d0-43b	6-ab49-177e49fb7bb0	192.168.1.242	SM_STAT	E_CONNECTED	<mark>tun0</mark>	1ad1b900/c6d09100	<mark>4500/4500</mark>	125781	GRE
1,33,44,192,4094	3999/0/3808/3808	10.224.	254.161	2021-03-13	08:28:59				
5bb2c1da-f402-4af	a-af39-c09d4aafa946	<mark>192.168.1.243</mark>	SM_STAT	E_CONNECTED	<mark>tun1</mark>	92607100/969£6100	<mark>4500/4500</mark>	125783	<mark>GRE</mark>
1,33,44,192,4094	3999/0/3807/3807	10.224.	254.161	2021-03-13	08:29:01				
Total Endpoints C	ount: 2								
b4:5d:50:c6:82:4a	#								

7 RF Monitoring

Here we'll just touch on some of the RF mgmt. info that are available in Central. To start with at the global level, you can check the WiFi connectivity and then drill down on any specifics, like AI insights, associations, authentication, etc.



Clicking on "clients had excessive 802.1.x failures"

Netwo	t rk Health	Q WAN Health Sur	폐 원 mmary Wi-Fi Connectivity	Q Al Insights									J week
IN	SIGHTS	(7)											\odot
	Severity	Description				▼ Category	~	Impact					
~	-	Clients had excessive	e 802.1X authentication failures			Connectivity - Wi	-Fi	10 impacte	d Clients (62.42% of	16), 45 Failures	(28.85% of 156)		
	Reason				F	Recommendation					Failures		
	Server Re	ejected Authentication			Cł	neck user's provisio	oned status and	l validate the	password			22	49%
	Timeout ·	- Authentication Serve	r		Ch	neck authentication	n server's log to	verify the au	uthentication reques	reached the se	rver	18	40%
	Timeout ·	- Client			Cł	neck the client and	it's environmer	nt for adequa	ate connection qualit	y		5	11%
I	Failures	Apr 25	Apr 26	Apr 27		Apr 28	Apr	29	Apr 30		May 1	High Medius Low	n
	Site) A Impacted	Server > 2 Impacted	Access Point > 4 Impacted	Client	10 mpacted							

Next, we can check the usage summary



We can then go to the Site level and see some of the stats



	Image: Book of the second			
- Manage	Access Points • Online • Offline 5 4 1	Radios 10		
Devices	ACCESS POINTS (5)			
Clients		Status	▼ IP Address	▼ Model
Applications	AP515-DramaPanelRoom	O Offline	10.16.136.201	AP-515
Cocurity	AP515-NBReception	Online	10.2.136.12	AP-515
Security	AP515-PetersDesk	Online	10.2.136.10	AP-515
😩 Guests	AP515-AttilasDesk	Online	10.2.136.13	AP-515
— Analyze ————	AP515-MeetingRoom	• Online	10.2.136.11	AP-515

Ð



Looking at 5GHz band



Access Points Switches						د	×
	CHANNEL CHAN	NGES (10)					
Ac	Event Time	Reason	From Channel	To Channel	Band	Access Point	
	Apr 28, 2021, 05:00	Algorithm Assigned	149E	157E	5 GHz	AP515-NBReception	
	Apr 28, 2021, 05:00	Algorithm Assigned	112E	108E	5 GHz	AP515-MeetingRoom	
RAI	Apr 28, 2021, 05:00	Algorithm Assigned	40E	48E	5 GHz	AP515-AttilasDesk	
	Apr 28, 2021, 05:00	Algorithm Assigned	60E	52E	5 GHz	AP515-PetersDesk	
	Apr 26, 2021, 18:30	Algorithm Assigned	108E	112E	5 GHz	AP515-MeetingRoom	
	Apr 26, 2021, 18:30	Algorithm Assigned	153E	149E	5 GHz	AP515-NBReception	
	Apr 26, 2021, 18:30	Algorithm Assigned	36E	40E	5 GHz	AP515-AttilasDesk	1
N	Apr 26, 2021, 18:30	Algorithm Assigned	64E	60E	5 GHz	AP515-PetersDesk	
GH	Apr 26, 2021, 18:15	Algorithm Assigned	100E	108E	5 GHz	AP515-MeetingRoom	
20	Apr 26, 2021, 18:15	Algorithm Assigned	36E	153E	5 GHz	AP515-NBReception	

Next, we can have a look at the Live view, for that we'll choose a specific AP.

LABELS

— Maintain

Firmware

🗟 Global 🛛 🔅	Access Points Switches Gateway:	5				
Manage	Access Points • Online	• Offline Radios				
B Overview	5 4	1 10				
Devices	ACCESS POINTS (5)					
🗖 Clients	V Device Name	Status	Y IP Add	ress	Y Model	
🙁 Guests	AP515-DramaPanelRoom	O Offline	10.16.136	.201	AP-515	
Applications	AP515-NBReception	Online	10.2.136.	12	AP-515	
	AP515-MeetingRoom	Online	10.2.136.	11	AP-515	
Security	AP515-PetersDesk	Online	10.2.136.	10	AP-515	
Network Services	AP515-AttilasDesk	• Online	10.2.136.	13	AP-515	
- 🗑 AP515-AttilasDesk 🔗 summ	Al Insights Floor Plan Performance F	₽ RF			Actions ▼	• Go Liv
侣 Overview	DEVICE		NETWORK			
Device	AP MODEL	COUNTRY CODE	ETHO	SPEED (Mbps) / DUPLEX	VLAN Trupk (all)	
ā Clients	AE-212	AU	• 00	10007 Pull		
	MAC	SERIAL NUMBER				LLDP Detail
Security	MAC d0:15:a	SERIAL NUMBER	eth1 O Down	SPEED (Mbps) / DUPLEX	VLAN	LLDP Detai
Security	MAC d0:15:a UPTIME 5 Days 22 Hours 30 Minutes	SERIAL NUMBER LAST REBOOT REASON AP reload	ETH1 O Down CURRENT UPLINK Ethernet (br0)	SPEED (Mbps) / DUPLEX - UPLINK CON	VLAN - NECTED TO	LLDP Detai
Security Analyze Live Events	MAC d0:15:a UPTIME 5 Days 22 Hours 30 Minutes FIRMWARE VERSION	LAST REBOOT REASON AP reload CONFIGURATION STATUS	ETH1 O Down CURRENT UPLINK Ethernet (br0) IP ADDRESS	SPEED (Mbps) / DUPLEX - UPLINK CON - PUBLIC IP AT	VLAN - NECTED TO	LLDP Detai
 Security Analyze Live Events Alerts & Events 	MAC d0:15:a UPTIME 5 Days 22 Hours 30 Minutes FIRMWARE VERSION 10.2:0.1_79907	SERIAL NUMBER LAST REBOOT REASON AP reload CONFIGURATION STATUS Synchronized Last Config Changed on Apr 28, 2021, 03:51	ETH1 Down CURRENT UPLINK Ethernet (br0) IP ADDRESS 10.2.136.13 (DHCP)	SPEED (Mbps) / DUPLEX - UPLINK CON - PUBLIC IP AC 203.1.203.1	VLAN - NECTED TO	LLDP Detail:
 Security Analyze Live Events Alerts & Events Audit Trail 	MAC do:15:a UPTIME 5 Days 22 Hours 30 Minutes FIRMMARE VERSION 10.2.0.1_79907 BAND SELECTION Dual Band	SERIAL NUMBER LAST REBOOT REASON AP reload CONFIGURATION STATUS Synchronized Last Config Changed on Apr 28, 2021, 03:51 POWER DRAW 13.16 W	ETH1 O Down CURRENT UPLINK Ethernet (br0) IP ADDRESS 10.2.136.13 (DHCP) DNS NAME SERVERS 10.99.64.202	SPEED (Mbos) / DUPLEX - - PUBLIC IP AL 203.1.203.1 DEFAULT GA 10.2.136.1	VLAN - NECTED TO DDRESS 51 TEWAY (DHCP)	LLDP Detai
 Security Analyze Live Events Alerts & Events Audit Trail Tools 	MAC d0:15:a UPTIME 5 Days 22 Hours 30 Minutes FIRMWARE VERSION 10.2.0.1_79907 BAND SELECTION Dual Band POWER NEGOTIATION	SERIAL NUMBER LAST REBOOT REASON AP reload CONFIGURATION STATUS Synchronized Last Config Changed on Apr 28, 2021, 03:51 POWER DRAW 13.16 W GROUP	ETH1 Down CURRENT UPLINK Ethernet (br0) IP ADDRESS 10.2.136.13 (DHCP) DNS NAME SERVERS 10.99.64.202 NTP SERVER 10.99.64.202	SPEED (Mbps) / DUPLEX - UPLINK CON - PUBLIC IP AC 203.1.203.1 DEFAULT GA 10.2.136.1	VLAN - NECTED TO DDRESS 51 TEWAY (DHCP)	LLDP Detai

LEDs on ACCESS POINT







40 20

0 10:00

12:00

14:00

16:00

18:00

20:00

22:00

3 May

02:00

04:00

06:00

08:00



Now you can click on go live to get real-time view of the RF counter for 15min.



8 Guest Access Configuration

Here we'll start with AP configuration followed by ClearPass.

8.1 Guest Wireless Configuration

The Guest WLAN will be tunnelled to the gateways, for this scenario all the configuration will take place on the AP group.

다 AOS10 이	Access Points Switches Gateways		i⊟ II. List Summary Config
- Manage	WLANs Access Points Radios Interfaces Security Services System Configuration	on Audit	Hide Advanced
B Overview			
Devices	CREATE A NEW NETWORK		
☐ Clients	1 General ② VLANs ③ Security ④ Access	5 Summary	
a Guests	Name (SSID):	Schoo-Guest	
Applications			
Security	✓ Advanced Settings		
Analyze Alerts & Events	Broadcast/Multicast		
Audit Trail	Transmit Rates (Legacy Unity) Andwidth Control		
🖏 Tools	WiFi Multimedia		
🛍 Reports	Miscellaneous		
— Maintain ————	Time Range Profiles		
Firmware			
			Cancel
P	(a)		:= ıh 🧕
LI AOS10	Access Points Switches Gateways		List Summary Config
- Manage	WLANs Access Points Radios Interfaces Security Services System Configuration	on Audit	Hide Advanced
B Devices			
Devices			
Guests	General 2 VLANS 3 Security 4 Access	Summary	
	Traffic forwarding mode:	Bridge Tunnel Mixed	
Security	Primary Gateway Cluster:	AOS10:auto_gwcluster_178_0	
- Analyze	Secondary Gateway Cluster	None	
🗘 Alerts & Events	Secondary Calency Caser.		
Audit Trail	Client VLAN Assignment:	Static Dynamic	
🖏 Tools	VLAN ID:	▼	
🔝 Reports	> Show Named VLANs		
— Maintain ———			
Firmware			
			Cancel Back Next
법 AOS10 이	Image: Construction Image: Construction		i≣ II. 🥸 List Summary Config
- Manage	WLANS Access Points Radios Interfaces Security Services System Configurati	ion Audit	Hide Advance
E Overview			
Devices	CREATE A NEW NETWORK		
🗖 Clients	1 General 2 VLANs 3 Security 4 Access	5 Summary	
😩 Guests			
Applications		\bigcirc	
Security	Security Level:	Enterorise Personal Cantive Portal Open	
- Analyze		and procession captive ronal open	
Alerts & Events			
🛛 Audit Trail	Splash Page		
🖏 Tools	Captive Portal Type:	External 🔻	
🛍 Reports			
- Maintain	Captive Portal Profile:	Select 🔻 🕇	
τµr FilliliWdi€		This field is mandatory.	

ជ AOS10 이	ි Access Points	📼 🙊 Switches Gateways		
— Manage ———	WLANS Acce	EXTERNAL CAPTIVE PORTAL-NEW		×
Overview				
Devices		Name:	CP-Guest	
□ Clients		Authentication Type:	RADIUS Authentication	▼
😩 Guests	Splash F	IP or Hostname:	victory.clearpass.info	
Applications	Cap			
Security		URL:	/guest/school.php	
— Analyze ———	Cap	Port:	443	
♠ Alerts & Events		Use HTTPS:		
Audit Trail	Prin			
🖏 Tools		Captive Portal Failure:	Deny Internet	
🛍 Reports	Enci	Server offload:		
— Maintain ————	Key			
Firmware		Cancel		ок
	> Adv			



Captive Portal Proxy Server IP:	
Captive Portal Proxy Server Port:	
MAC Authentication:	
Use IP for Calling Station ID:	
Delimiter Character:	
Called Station ID Type:	MAC Address
Reauth Interval:	0 min V
Denylisting:	
Max Authentication Failures:	0

Use authentication servers			
1 min			
	Use authentication servers V	Use authentication servers	Use authentication servers 1 min Cancel

In the above we have also enabled MAC auth and RADIUS accounting. MAC auth is enabled because we want to also enable MAC caching for the guest users.

🛱 AOS10 📀	Access Points Switches Gateways			List Summary Cor
- Manage	- WLANS Access Points Radios Interfaces Securit	y Services System Configuration Audit		Hide Advan
🗄 Overview				
Devices	CREATE A NEW NETWORK			
⊑ ī Clients	1 General 2 VLANs 3	Security 4 Access 5 Summary		
😩 Guests				
Applications	Accessitules	0		
Security		Role Based Network Based	Unrestricted	
- Analyze	ROLE	ACCESS RULES FOR SELECTED ROLES		
Alerts & Events	Schoo-Guest	Allow any to all destinations		
🛛 Audit Trail	school			
🖏 Tools	CP-Guest			
品 Reports				
- Maintain	_			
Firmware				
	ROLE ASSIGNMENT RULES			
	Default role: Schoo-Guest			
	+ ADD ROLE ASSIGNMENT			T Kole(s)
	ASSIGN PRE-AUTHENTICATION ROLE:	CP-Guest V		
	ENFORCE MAC AUTH ONLY ROLE:			
				Cancel Back Next
		Search or ask Aruba		م
AOS10				III III
Manage WI	LANs Access Points Radios Interfaces Security	SUCCESS		Hide Advanced
88 Overview		SUCCESS		
Devices	DTIM Interval	Schoo-Guest is Configured Successfully		
🗈 Clients	Primary Usage			
A Guests	Inactivity Timeout			
Applications				

Now we have our Guest SSID configured.

II AOS10	Access P	oints	Switches	۾ Gate	a ways							List	II. Summary	Config
- Manage	WLAN	s Acc	cess Points	Radios	Interfaces	Security	Services	System	Configuration Audit				Hide A	dvanced
B Overview														
Devices		Wirele	ess SSIDs											
🗖 Clients		NAM	1E		S	ECURITY			ACCESS TYPE	TRAFFIC FORWARDING MODE	NETWORK ENABLED			
Suests		Ⅲ s	school		W	/pa2-aes			Unrestricted	Tunnel	Yes			
Applications		•	Schoo-Guest	t	C	aptive Port	al (external)	Role Based	Tunnel	Yes			
Security														

We don't need to do any configuration on the gateways as all the relevant configuration will be pushed to them, which are:

- Authentication Servers and groups.
- L3 Captive Portal Authentication
- Pre-authentication user role

다 AOS10	Access Points Sv	itches Gate) ways								SELECTED GROU Gateway	P TYPE	i≣ I List Sum	ili nmary Cor
— Manage ————	System Interfac	e Routing W	AN Security	VPN High	Availability Co	nfig Audit							Ba	asic Mode
Overview	Roles Policies	Aliases A	Applications A	pply Policy	Auth Servers	Role Assignm	ent (AAA Profiles) I	.2 Authentica	tion L3 Authentication	Advanced	Firewall			
Devices	✓ Authenticat	on Servers												
Clients	Server	groups												
😫 Guests	NAME				SERVERS		FAIL THROUGH		LOAD BALANCE	SERV	ER RULES			=
Applications	Schoo-	Guest_#1615938	135060_41#acc	:t_svg	1		-		-	0		î		
Security	Schoo-G	Guest_#1615938	135060_41#au	th_svg	1					0				
- Analyze	Schoo-	ouest_#1615938	135060_41#cp_	svg	1					0				
Alerts & Events	school_	#1615532079504	4_41#acct_svg		1		-		-	0				
Audit Trail	school	#1615532079504	4_41#auth_svg		1				-	0				
K Tools	school_	#1615532079504	4_41#cp_svg		1					0				
II. Reports	+													
Firmware														
	Server	Group > Schoo-	Guest_#1615938	135060_41#	_acct_svg	vers Option	s Server Rules					() (Drag rows to	re-order
	NAME		TYPI			IP ADDRESS		TRIM FQD	N	MATCH RULE	ES			=
	ClearPa	ss-GW	Radi	us		192.168.1.95				0				

법 AOS10 〇	Access Points Switches Gateways		SELECTED GROUP TYPE Gateway	List Summary Config
- Manage	System Interface Routing WAN Security VPN High A	vailability Config Audit		Basic Mode
B Overview	Roles Policies Aliases Applications Apply Policy	Auth Servers Role Assignment (AAA Profiles) L2 Authentication L3 Authentication Advanced	Firewall	
Devices	L3 Authentication	Captive Portal Authentication Profile: New Profile		
🗖 Clients	O 🕞 Captive Portal Authentication			
🚨 Guests	🕀 📑 default	Captive Portal Authentication Profile: +		
Applications				
Security				
— Analyze ———				
Alerts & Events				
🛛 Audit Trail				
Tools	VPN Authentication			
10013				

口 AOS10 〇	Access Points Switches Gateways				SELI Gat	ECTED GROUP TYPE	II. Summary Conf
— Manage —	System Interface Routing WAN	Security VPN High Availability	Config Audit				Basic Mode
B Overview	Roles Policies Aliases Applica	tions Apply Policy Auth Sen	vers Role Assignment (AAA Profiles)	L2 Authentication L3 Authentica	ation Advanced Firewall		
Devices	Balas						
Clients	Roles						
🔐 Guests	YNAME		RULES				
# Applications	ap-role		35 Rules				
Security	authenticated		4 Rules		-		_
– Analyze —	CP-Guest		5 Rules				_
	default-iap-user-role		2 Rules				
Audit Trail	default-via-role		3 Rules				
🖏 Tools	default-vpn-role		4 Rules				
Reports	+						
- Maintain							
Firmware	CP-Guest Policies Bandwidth	More					
	∀ NAME	RULES COUNT	Ттуре		SAGE		≡
	global-sacl	0	session	ap-role, aut	henticated, CP-Guest, default-vi		
	apprf-cp-guest-sacl	0	session	CP-Guest			
	cp-guest	5	session	CP-Guest			

Lastly note that we have not use a publicly signed HTTPS server certificate for the controllers and hence the redirection of a web page will issue a warning on the client's web browser. In all deployment you need to have a public cert for the controllers as well as ClearPass nodes.

8.2 ClearPass Guest policy Configuration

We'll go through the guest confirmation needed on ClearPass. There are two part to it, one is the web pages that the client redirects to and the other is the policy service we need to create. We'll start with the policy service. Here we are using the following template. This creates 2x services one is MAC authentication and the second one is Guest redirection to captive portal page.

aruba	ClearPass Policy Manager
Dashboard	To authenticate users logging in via captive portal with their cloud identity or social media accounts. Guests must re-authenticate after their session ends.
Monitoring O	To authenticate guest devices based on their MAC address.
→☆ Services → Authentication	EDUROAM service Service template for roaming users to connect to campus networks that are part of the eduroam federation.
Gontely G	Service Template for providing encrypted wireless access to (guest) users via fixed 802.1X PEAP credentials.
- C Static Host Lists	Guest Access To authenticate guest users logging in via captive portal. Guests must re-authenticate after their session ends.
- ✿ Role Mappings ♥ Posture ♥ Enforcement	Guest Access - Web Login To authenticate guest users logging in via guest portal.
	Guest Authentication with MAC Caching To authenticate users once using captive portal and later to allow logins using cached MAC Address of the device.
- 🗘 Devices - 🗘 Device Groups - 🗘 Proxy Targets	Service template for API clients authenticating with username and password (OAuth2 grant type "password").
- C Event Sources - C Network Scan - Policy Simulation	Onboard Service template for authorizing device credential provisioning and onboarding.
Administration O	Onboard Services Only Service template for authorizing device credential and onboarding

Configuration » Service Templates & Wizards

Service Templates - Guest Authentication with MAC Caching

General	Wireless Network	Settings	MAC Caching Settings	Posture Settings	Access Restrictions						
Name Prefi	x*: GG										
				Description	n						
Users fir access c vary acc enabled,	Users first login via captive portal and their MAC addresses are cached. Subsequent logins will use MAC authentication and bypass the captive portal. Network access can be restricted based on day of the week, bandwidth limit or number of unique devices used by the User. The cache lifetime of the MAC address can vary according to the user's role (Guest, Employee or Contractor) and after that the user will have to re-authenticate via captive portal. Posture checks can be enabled, optionally, to validate the client device for antivirus, anti-spyware, firewall status. These results will determine the enforcement for the device.										
< Back to S	Service Templates	& Wizard	5			Delete	$\textbf{Next} \rightarrow$	Add Service	Cancel		
General	Wireless Network	Settings	MAC Caching Settings	Posture Settings	Access Restrictions						
Select NAD	Client: MD-1		~								
Wireless SS	SID <u>*</u> : Guest										
< Back to	Service Templates	& Wizard	s			Delete	Next \rightarrow	Add Service	Cancel		
General	Wireless Network	Settings	MAC Caching Settings	Posture Settings	Access Restrictions						
Enter MAC	Caching duration	for the us	ers. After this time ex	pires, users will ha	ave to re-authenticat	e via captive	portal				
Cache dura	tion for Employee:	One Month	~								
Cache dura	tion for Guest:	One Day	~								
Cache dura	tion for Contractor:	One Week	~								
< Back to	Service Templates	& Wizard	s			Delete	$\textbf{Next} \rightarrow$	Add Service	Cancel		

General	Wireless Network Setting	s MAC	Caching Settings	Posture Set	tings Access Restriction	ons		
Enable Pos	sture Checks to perform	health ch	ecks after auth	entication.				
Enable Post	ure Checks: 🗌 Configure	e Guest W	eb Login page					
< Back to :	Service Templates & Wiz	ards				Delete	Next \rightarrow Add Service	e Cancel
General	Wireless Network Setting	IS MAC	Caching Settings	Posture Set	tings Access Restriction	ons		
. Enfo	reement Type applies to	the Canti	vo Portal Accor	c. Employee A	anna Guart Arran	and Contractor Acces	e fielde	
• Enro • Capt	ive Portal Access is used	for unau	thenticated use	s, Employee A ers and after t	he MAC caching durati	on has expired.	s fields.	
• At le	ast one of Employee, Gu	est, and (Contractor Acce	ss must be pr	ovided.	•		
Enforceme	nt Type*:		Aruba Role Enfor	cement ~				
Captive Po	rtal Access*:		GuestCptivePortal					
Days allow	ed for access*:		Mon Guest-	guest-logon	Vednesday 🗹 Thursday	y 🗹 Friday 🗹 Satu	rday 🗹 Sunday	
Maximum I	number of devices allowed p	oer user <u>*</u> :	5					
Maximum I	bandwidth allowed per user	*:	0	MB (For	unlimited bandwidth, set	value to 0)		
Employee /	Access:		Employee-Guest					
Guest Acce	ess:		Guest					
Contractor	Access:		Contractor					
< Back to	Service Templates & Wiz	ards				Delete	Next → Add Service	e Cancel
Convior								🛶 Add
Service	15							🛓 Import
								🛓 Export All
				 Added 15 E Added 2 Fn 	nforcement Profile(s) forcement Policies			

- Added 2 Role Mapping Policies Added 2 service(s)

This page shows the current list and order of services that ClearPass follows during authentication and authorization.

Filter:	Name		contains	🛨 Go Clear Filter		Show 20 \checkmark records
#		Order 🔺	Name	Туре	Template	Status
1.		1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	0
2.		2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	S
3.		3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	O
4.		4	[Guest Operator Logins]	Application	Aruba Application Authentication	O
5.		5	[Insight Operator Logins]	Application	Aruba Application Authentication	O
6.		6	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	O
7.		7	AA Aruba 802.1X Wireless	RADIUS	Aruba 802.1X Wireless	\bigcirc
8.		8	GG MAC Authentication	RADIUS	MAC Authentication	0
9.		9	GG User Authentication with MAC Caching	RADIUS	RADIUS Enforcement (Generic)	O

We'll look at the MAC authentication service

Services - GG MAC Authentication

3. Click to add..

Note: This Service is created by Service Template

Su	mmary Service	Authentication Authorization Roles Enforcement									
Nam	e:	GG MAC Authentication									
Desc	cription:	MAC Authentication bypass for captive portal users !	C Authentication hypass for captive rtal users								
туре	9:	MAC Authentication									
Stat	us:	Enabled									
Moni	itor Mode:	Enable to monitor network access without enforcement	:								
More	e Options:	Authorization Audit End-hosts Profile Endpoint	s 🗌 Accounting Proxy								
			Service Rule								
Mato	ches 🔿 ANY or 🔍	ALL of the following conditions:									
	Туре	Name	Operator	Value							
1.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}	Pe t						
2.	Radius:Aruba	Aruba-Essid-Name	BEGINS_WITH	Guest	Pe ti						

Summary	Service	Authentication Authoriz	ation Roles	Enforcement		
Authentication	n Methods:	[Allow All MAC AUTH]	^]		Add New Authentication Method
				Move Up ↑		
				Move Down ↓		
				Remove		
				View Details		
				Modify		
		Colort to Add	×	1		
Authontication	n Sourcos:	Select to Add	· · · · · · · · · · · · · · · · · · ·	1		
Macheneloucio	n bources.	[Endpoints Repository] [Lo	cal SQL DBJ	Marcalla		Add New Addientication Source
				Move Down		
				Remove		
				View Details		
				Modify		
			~			
		Select to Add		~		
Summary	Service	Authentication Authoriz	ation Roles	Enforcement		
Authorization	Details:	Authorization sources fr	om which role m	apping attributes are	e fetched (for each Authentication Sou	
		Authentication S	ource	apping attributes an	Attributes Fetched From	
		1. [Endpoints Reposit	ory] [Local SQL	DB]	[Endpoints Repository] [Loca	I SQL DB]
		Additional authorization	sources from wh	ich to fetch role-ma	pping attributes -	Add New Authentication Source
		[Guest User Repository] [L	ocal SQL DB]	Remove View Detaile		Add New Addientication Source
				Modify		
		Select to Add	~	×		
]		
Summary	Service	Authentication Authoriza	ation Roles	Enforcement		
Role Mapping	Policy:	GG MAC Authentication Rol	e Mapping	 ✓ Modif 		Add New Role Mapping Policy
			R	Role Mapping Policy D	etails	
Description:						
Default Role:		[Other]				
Rules Evaluat	ion Algorithr	n: evaluate-all				
Conditio	ons zation:[End	ointe Ropository]:Uniquo-F	Dovico-Count EX	ISTS)	Role	
AND (Authorizatio	n:[Time Source]:Now DT	ESS_THAN %{E	Endpoint: MAC-Auth		
1. Expiry}) AND (Authorizatio	n:[Guest User Repository]:	AccountExpired	EOUALS false)	[MAC Caching]	
AND (Authorizatio	n:[Guest User Repository]:	AccountEnabled	EQUALS true)		
2. (Endpoir	nt:Guest Rol	e ID EQUALS 1)			[Contractor]	
4 (Endpoir	nt:Guest Rol	e ID EQUALS 2)			[Guest]	
4. (Endpoir	it. Guest Noi	eib Equility			[Employee]	
Summary	Service	Authentication Authoriza	tion Roles	Enforcement		
Use Cached Re	esults:	Use cached Roles and I	Posture attributes	s from previous sess	ions	
Enforcement F	Policy:	GG MAC Authentication Enfo	prcement Policy	~ M	odify	Add New Enforcement Policy
			E	nforcement Policy De	tails	
Description:						
Default Profile	:	[Deny Access Profile]				
Rules Evaluati	ion Algorithn	n: first-applicable				
Conditio	ons				Enforcement Profiles	
(Tips:R 1. [Guest]	thore to the start	ES_ALL [MAC Caching]			[Allow Access Profile], GG Guest Dev	vice Profile
(Tips:R	tole MATCH	I) ES_ALL [MAC Caching]				
2. [Employ [User Au	ee] ithenticated)			[Allow Access Profile], GG Employee	Device Profile
(Tips:R	tole MATCHI	ES_ALL [MAC Caching]				
 [Contrac [User Au 	tor] thenticated])			[Allow Access Profile], GG Contracto	r Device Profile
(Tips:R	ole MATCH	ES_ANY [Guest]				
4. [Contrac [Employ	tor] ee])				[Allow Access Profile], GG Captive P	ortal Profile
K Back to S	ervices				Disable	Copy Save Cancel

And here are the enforcement profiles that are used here

Profile:	TTOTAL	Attributes	
Name:		GG Guest Device Profile	
Description		Role/VLAN enforcement for Gue	est
Type:		RADIUS	
Action:		Accept	
Device Grou	ıp List:	-	
Attributes			
Туре		Name	Value
1. Radiu	:Aruba	Aruba-Use	r-Role = Guest
2. Radiu	:IETF	User-Name	e = %{Endpoint:Username}
Summary	Profile	Attributes	
Profile:			
Name:		GG Employee Device Profile	
Description		Role/VLAN enforcement for Em	ployee
Туре:		RADIUS	
Action:		Accept	
Device Grou	p List:	-	
Attributes:			
Туре		Name	Value
1. Radius	:Aruba	Aruba-Use	r-Role = Employee-Guest
2. Radius	:IETF	User-Nam	e = %{Endpoint:Username}
Summary	Profile	Attributes	
Summary Profile:	Profile	Attributes	
Summary Profile: Name:	Profile	Attributes GG Contractor Device Profile	
Summary Profile: Name: Description	Profile	Attributes GG Contractor Device Profile Role/VLAN enforcement for Cor	tractor
Summary Profile: Name: Description Type:	Profile	Attributes GG Contractor Device Profile Role/VLAN enforcement for Cor RADIUS	tractor
Summary Profile: Name: Description Type: Action:	Profile	Attributes GG Contractor Device Profile Role/VLAN enforcement for Contractor RADIUS Accept	tractor
Summary Profile: Name: Description Type: Action: Device Grou	Profile	Attributes GG Contractor Device Profile Role/VLAN enforcement for Contractor RADIUS Accept -	tractor
Summary Profile: Name: Description Type: Action: Device Grou Attributes:	Profile	Attributes GG Contractor Device Profile Role/VLAN enforcement for Corr RADIUS Accept -	tractor
Summary Profile: Name: Description Type: Action: Device Grou Attributes: Type	Profile	Attributes GG Contractor Device Profile Role/VLAN enforcement for Corr RADIUS Accept -	tractor Value
Summary Profile: Name: Description Type: Action: Device Grou Attributes: Type 1. Radius	Profile p List: ::Aruba	Attributes GG Contractor Device Profile Role/VLAN enforcement for Corr RADIUS Accept - Name Aruba-User	tractor Value Role = Contractor
Summary Profile: Name: Description Type: Action: Device Grou Attributes: Type 1. Radius 2. Radius	Profile p List: ::Aruba ::IETF	Attributes GG Contractor Device Profile Role/VLAN enforcement for Con RADIUS Accept - Name Aruba-Usee User-Name	tractor -Role = Contractor -Role = %{Endpoint:Username}
Summary Profile: Name: Description Type: Action: Device Grou Attributes: Type 1. Radius 2. Radius	Profile Profile Profile Profile Profile Profile Profile	Attributes GG Contractor Device Profile Role/VLAN enforcement for Cor RADIUS Accept - Name Aruba-User User-Name Attributes	tractor -Role = Contractor = %{Endpoint:Username}
Summary Profile: Name: Description Type: Action: Device Grou Attributes: Type 1. Radius 2. Radius 2. Radius Summar	Profile Profile Profile Profile	Attributes GG Contractor Device Profile Role/VLAN enforcement for Corr RADIUS Accept - Name Aruba-User User-Name	tractor -Role = Contractor = %{Endpoint:Username}
Summary Profile: Name: Description Type: Action: Device Grou Attributes: Type 1. Radius 2. Radius Summar Profile: Name:	Profile Profile Profile Profile	Attributes GG Contractor Device Profile Role/VLAN enforcement for Con RADIUS Accept Name Aruba-User User-Name GG Captive Portal Profile	tractor -Role = Contractor = %{Endpoint:Username}
Summary Profile: Name: Description Type: Action: Device Grou Attributes: Type 1. Radiu: 2. Radiu: Summary Profile: Name: Description	Profile Profile Profile Profile Profile	Attributes GG Contractor Device Profile Role/VLAN enforcement for Corr RADIUS Accept - Name Aruba-User User-Name Attributes GG Captive Portal Profile Captive Portal Role/VLAN enforcement	tractor Role = Contractor = %{Endpoint:Username} iforcement
Summary Profile: Name: Description Type: Action: Device Grou Attributes: Type 1. Radiu: 2. Radiu: Summary Profile: Name: Description Type:	Profile Profile Profile Profile Profile	Attributes GG Contractor Device Profile Role/VLAN enforcement for Corr RADIUS Accept Accept Accept Accept GG Captive Portal Profile GG Captive Portal Role/VLAN en RADIUS	tractor Role = Contractor Role = %{Endpoint:Username} forcement
Summary Profile: Name: Description Type: Action: Device Grou Attributes: Type 1. Radiu: 2. Radiu: 2. Radiu: Summary Profile: Name: Description Type: Action:	Profile Profile Profile Profile Profile	Attributes GG Contractor Device Profile Role/VLAN enforcement for Corr RADIUS Accept - Name Aruba-User User-Name Attributes GG Captive Portal Profile Captive Portal Role/VLAN en RADIUS Accept	tractor Value -Role = Contractor = %{Endpoint:Username} forcement - -
Summary Profile: Name: Description Type: Action: Device Grou Attributes: Type 1. Radius 2. Radius 2. Radius Profile: Name: Description Type: Action: Device Grou	Profile Profile Profile Profile Profile Profile	Attributes GG Contractor Device Profile Role/VLAN enforcement for Corr RADIUS Accept Accept Aruba-User User-Name Attributes GG Captive Portal Profile GG Captive Portal Role/VLAN en RADIUS Accept J Attributes	tractor Value Role = Contractor = %{Endpoint:Username} iforcement - -
Summary Profile: Name: Description Type: Action: Device Grou Attributes: 2. Radius 2. Radius 2. Radius Profile: Name: Description Type: Action: Device Grou Attributes	Profile Profile Profile Profile Profile Profile Profile Profile	Attributes GG Contractor Device Profile Role/VLAN enforcement for Contractor ADUS Accept Accept Accept Aruba-User User-Name Attributes GG Captive Portal Profile Captive Portal Role/VLAN entractor RADIUS Accept -	tractor Value -Role = Contractor = %{Endpoint:Username} iforcement = %
Summary Profile: Name: Description Type: Action: Device Grou Attributes: Summary Profile: Name: Description Type: Action: Device Grou Attributes: Devi	Profile Profile Profile Profile Profile	Attributes GG Contractor Device Profile Role/VLAN enforcement for Con Accept Accept Aruba-User User-Name GG Captive Portal Profile GG Captive Portal Role/VLAN en Accept A	tractor Value -Role = Contractor = %(Endpoint:Username) forcement

Services - GG User Authentication with MAC Caching

Sun	mary Service	Authentication	Authorization	Roles	Enforcement	t							
Name	:	GG User Authentic	GG User Authentication with MAC Caching										
Descr	iption:	Captive Porta MAC Caching	Captive Portal authentication with MAC Caching										
Type:		RADIUS Enforce	ment (Generic)										
Statu	s:	Enabled											
Monit	or Mode:	Enable to mo	onitor network a	ccess wit	nout enforcem	ent							
More	Options:	Authorization	n 🗌 Posture Co	ompliance	Audit End	d-hosts 🗌 Profile Endpoints 🗌 Accounting Proxy							
						Service Rule							
Match	ies 🔿 ANY or 🖲	ALL of the followin	g conditions:										
	Туре		Na	ime		Operator	Value						
1.	Radius:IETF		Ca	lling-Stat	on-Id	EXISTS		Ba	Ŵ				
2.	Connection		Cli	ent-Mac-	Address	NOT_EQUALS	%{Radius:IETF:User-Name}	印刷	Ť				
з.	Radius:Aruba		An	uba-Essid	Name	BEGINS_WITH	Guest	Æ	Ť				
4	Click to add												

Summary	Service	Authentication Authorization Ro	les Enforcement	
Authentication	Methods:	[PAP]	^	Add New Authentication Method
		[MSCHAP]	Move Up ↑	
		[CHAP]	Move Down ↓	
			Remove	
			View Details	
			Modify	
			\sim	
	_	Select to Add	~	
Authentication	1 Sources:	[Guest User Repository] [Local SQL DB]	^	Add New Authentication Source
			Move Up ↑	
			Move Down J	
			View Details	
			Modify	
			~	
		Select to Add	~	
	1			
Summary	Service	Authentication Authorization Role	s Enforcement	
Authorization [Details:	Authorization sources from which role	e mapping attributes are	fetched (for each Authentication Source)
		Authentication Source		
			JQE 00]	
		Additional authorization sources from	which to fetch role-map	ping attributes -
		[Endpoints Repository] [Local SQL DB]	Remove	Add New Authentication Source
			View Details	
			Modify	
		Select to Add		
Summary	Service	Authentication Authorization Roles	Enforcement	
Role Mapping F	Policy:	GG User Authentication with MAC Caching	Role Mapping \vee 🛛 Modify	Add New Role Mapping Policy
			Role Mapping Policy De	tails
Description:				
Default Role:		[Other]		
Rules Evaluatio	on Algorithr	n: evaluate-all		
Conditio	ns aruBala ID	50UALS 1)		Role
 (GuestUs (GuestUs) 	er:Role ID	EQUALS 1)		[Guest]
3. (GuestUs	er:Role ID	EQUALS 3)		[Employee]
Summary	Service	Authentication Authorization Roles	Enforcement	
Use Cached Re	esults:	Use cached Roles and Posture attrib	utes from previous sess	ions
Enforcement P	Policy:	GG User Authentication with MAC Caching	Enforcement Policy 🗸 🚺	odify Add New Enforcement Policy
			Enforcement Policy De	tails
Description:				
Default Profile	:	[Allow Access Profile]		
Rules Evaluation	on Algorith	m: first-applicable		
Conditio	ons	desinte Repository]: Unique-Device-Cour	CREATER THAN 5)	Enforcement Profiles
1. (Author			CORLATER_THAN 5)	GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit,
2. AND	Ole EQUAL (Date:Day	of-Week <i>BELONGS_TO</i>		GG MAC Caching Session Limit, GG Employee MAC Caching, [Update
Monday,	Tuesday,We	dnesday,Thursday,Friday,Saturday,Sunda	у)	Post Login, GG Employee Profile
(Tips:R	ole EQUAL	S [Contractor])		GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit, GG MAC Caching Session Limit, GG Contractor MAC Caching, Ellipdate
3. AND Monday.	(Date:Day Tuesday.We	of-Week BELONGS_TO dnesday,Thursday,Friday,Saturdav.Sunda	y)	Endpoint Known], GG MAC Caching Do Expire, GG MAC Caching Expire
(7)		C [Cuest])		Post Login, GG Contractor Profile GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit,
4 AND	OIE EQUAL (Date:Day	of-Week BELONGS_TO		GG MAC Caching Session Limit, GG Guest MAC Caching, [Update
	· ·			Endbolint Knowin Lists MALL aching the Expire List Multi Sching Expire

The enforcement profiles

Summary	Profile	Attributes							
Profile:									
Name:		GG Employe	e Profile						
Description:		Role/VLAN e	enforcement for Employee						
Type:		RADIUS							
Action:		Accept							
Device Group) List:	-							
Attributes:									
Туре			Name	Value					
1. Radius:	Aruba		Aruba-User-Role	= Employee-Gue					
Summary	Profile	Attributes							
Profile:	110110	, nethodecos							
Name:		GG Gue	st Profile						
Description:		Role/VL/	Role/VLAN enforcement for Guest						
Type:		RADIUS	RADIUS						
Action:		Accent	Accept						
Device Grou	in List:	-							
Attributor									
Attributes.			Nie waa	V-L					
1 Rodius	Aruba		Aruba Usor Bolo						
I. Kaulus	S.Aluba		Aluba-Osel-Kole	- Gue					
Summary	Profile	Attributes							
Profile:									
Name:		GG Contr	GG Contractor Profile						
Description:		Role/VLA	Role/VLAN enforcement for Contractor						
Type:		RADIUS	RADIUS						
Action:		Accept							
Device Grou	p List:	-							
Attributes:									
Туре			Name	Value					
1. Radius	:Aruba		Aruba-User-Role	= Contract					

8.3 ClearPass Guest Portal Configuration

Here we'll configure the portal pages.

aruba			ClearPass	Policy Manager			Menu
Dashboard	-						Default 🗸
Alerts Latest Alerts	Cluster Sta Status	itus Host Name	Management IPv4	Management IPv6	Server Role	Last Replication	⊗ Status
All Requests Trend all Policy Manager requests Sep Applications	System CP	victory U Utilization	192.168.1.95	-	Publisher equest Processing Time	-	ок
Launch other ClearPass Applications Authentication Status Trend Successful and Failed authentications	e transference e construction de la construcción de la constru	0			(5 200	\wedge	
Cluster Status Control the status of the entire cluster Control the status of	Perce	0 0 14:35 14:4		****		14:45 14:50 14:55	15:00
Device Categories		- Syst	Time (mins) tem → User 🖶 IO Wait ⊯ Idle		- RAD	Time (mins)	
Endpoint Profiler Summary Endpoint profiling details					II Requests		0
Track the latest failed authentications	Quick Links	5		©	n noquusts		
Health Status Trend Healthy and Unhealthy requests	🛱 Start Co	onfiguring Policies Services			30		
Latest Authentications Latest Authentications	Access Analysis	Tracker and Trending			20		-
License Usage	🔅 Networ	k Devices Manager			10		
MDM Discovery Summary Mobile Device Management discovery details	ClearPa	<mark>ss Guest</mark> ss Onboard					120
OnGuard Clients Summary OnGuard Clients details	ClearPa	ss Insight ss Extensions			12.00 5. PED 12:00 4. 1	Time	, 12.0
Monitoring						All Requests]	

Now we'll create a guest user called cpguser with no expiration on the account.



aruba		ClearPass Guest						
Guest 📀	Home » Guest » Cre	ate Account						
- Su Active Sessions - S Create Account - Streate Multiple	Create Guest Account New guest account being created by admin.							
Export Accounts Import Accounts	Create New Guest Account							
Manage Accounts	* Guest's Name:	cpguser Name of the quest.						
– 🚉 Manage Multiple Accounts	* Company Name:	Company name of the guest.						
	* Email Address:	cpuser@aa.com The guest's email address. This will become their username to log into the network.						
	Account Activation:	Now Select an option for changing the activation time of this account.						
	Account Expiration:	Account will not expire Select an option for changing the expiration time of this account.						
	* Account Role:	[[Guest] ~ Role to assign to this account.						
	Password:	234726						
	Notes:							
	* Terms of Use:	☑ I am the sponsor of this account and accept the terms of use						
		Create						

Once created we'll modify it to change the username and password

aruba				ClearPass	Guest		
🗒 Guest 📀	Home » Guest » Manage A	Accounts					
- 💱 Active Sessions - 🚑 Create Account - 💇 Create Multiple	Manage Guest Accounts The following table shows the guest accounts that have been created. Click an account to modify it:						
-	Quick Help Filter:	🔔 c	🚑 Create		More Options		
- 🖳 Manage Multiple Accounts	△ Username	Role	State	Activation	Expiration		
	 cpguser Reset password Refresh Back to guests Back to main 	[Guest] Change expiration	Active Remove	23 hours ago Edit (예) Sessions	No expiry Print Show Details Showing 1 – 1 of 1 20 rows per page V		

🛃 Guest 💿		8		-				
-Strain Active Sessions	1 Quick Help		Create	B	More Options			
- 🥵 Create Account	Filter:							
- 💕 Create Multiple	△ Username	Role	State	Activation	Expiration			
- Export Accounts	🤵 cpguser	[Guest]	Active	23 hours ago	No expiry			
- mort Accounts	Reset password	🕑 Change expiratio	n 🔀 Remove	📴 Edit 🤎 Sessions	실 Print 🧕 Show Details			
— 😫 Manage Accounts	To undate the properties	of this quast account	uco the form h		~			
- 🚽 Manage Multiple Accounts	To update the properties	or this guest account	, use the form L	1970W.				
			Edit Accoun	t				
	* Guest's Name:	cpguser Name of the guest.						
	* Username:	cpguser Name of the account.						
	Account Activation:	(No changes: Accour Select an option for c	it is active) $$	ation time of this account.				
	Account Expiration:	(No changes: Accour Select an option for c	nt will not expire) hanging the expir	→ ration time of this account.				
	Account Lifetime:	N/A ∽ The amount of time a	fter the first logir	before the account will exp	ire and be deleted.			
	Total Allowed Usage: (No changes)							
	Account Role:	(No changes: [Guest Role to assign to this]) ∨ account.					
	* Password:	Type in a new passw Select an option for e	vord vord	ccount's password.				
	New password:	••••••• Type in a new passwo	ord to assign to th	e guest account.				
	Confirm Password:	Repeat the new passv	vord for the gues	t account.				
(0) - •	Session Limit:	0 The number of simult	aneous sessions	allowed for this account. Typ	e 0 for unlimited use.			
Devices •								
Onboard O	Notes:							
🔨 Configuration 🔹 💿								
🔭 Administration 🛛 🔹 💿			峇 Update Acco	ount				

Next we'll create a weblogin page, note that the page name will be in the redirection URL, also securelogin.hpe.com will need to change to CN in the server certificate on Aruba controller.

Guest O Home » Configuration » Pages » Web Logins							
ਗੈ ¹ Devices 0	Web Login (school)						
📳 Onboard 🔹 💿	Use this form to make changes to the Web Login school .						
- 🎭 Authentication	Web Login Editor						
🖃 🥑 Content Manager — 🙀 Private Files	* Name:	School Enter a name for this web login page.					
- 🍲 Public Files - 🕵 Guest Manager	Page Name: Description: * Vendor Settings:	School Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".					
Hotspot Manager Pages Fields Comparison		for AOS-10					
List Views		Aruba Select a predefined group of settings suitable for standard network configurations.					
- 😒 Self-Registrations - 🥵 Web Logins - ≷ Web Pages	Login Method:	Controller-initiated — Guest browser performs HTTP form submit V Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.					
	* Address:	securelogin.hpe.com Enter the IP address or hostname of the vendor's product here.					
Translations	Secure Login:	Use vendor default Select a security option to apply to the web login process.					
	Dynamic Address:	☐ The controller will send the IP to submit credentials In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.					

Page Redirect Options for specifying pa	rameters passed in the initial redirect.					
Convibuliants	Do not check – login will always be permitted					
Security Hash:	Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.					
Login Form Options for specifying the	behaviour and content of the login form.					
	Credentials - Require a username and password					
Authentication:	Access Code requires a single code (username) to be entered. Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required.					
	Auto is similar to anonymous but the page is automatically submitted. Access Code and Anonymous require the account to have the Username Authentication field set.					
Broyopt CNA:	Enable bypassing the Apple Captive Network Assistant					
Prevent CIVA.	The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.					
Custom Form:	Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.					
Custom Labels:	Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.					
* Pre-Auth Check:	None – no extra checks will be made Select how the upgrame and parameter should be checked before properties to the NAC suthestication					
Terms:	Select now the username and password should be checked before proceeding to the NAS authentication.					
Terma.	If checked, the user will be forced to accept a Terms and Conditions checkbox.					
CAPTCHA:	Select a CAPTCHA mode.					
Default Destination Options for controlling the	e destination clients will redirect to after login.					
* Default URL:	Enter the default URL to redirect clients.					
	Please ensure you prepend "http://" for any external domain.					
Override Destination:	Force gerauit destination for all clients If selected, the client's default destination will be overridden regardless of its value.					
Login Page						
Options for controlling th	calleria Skin 3					
* Skin:	Choose the skin to use when this web login page is displayed.					
Title:	The title to display on the web login page.					
	Leave blank to use the default (Login). [mwa_cookiecheck)					
	<pre>{if \$errmsg}{nwa_icontext type=error}{\$errmsg escape}{/nwa_icontext}{/if} </pre>					
Header HTML:	Flease login to the network using your username and password.					
	HTML template code displayed before the login form.					
	<pre>{nwa_text id=7979} Contact a staff member if you are experiencing different location in</pre>					
Footer HTML:						
	Insert v					
	{nwa_text_id=7978;					
Login Message:	Logging in, please wait //nwa_text}					
	Insert					
* Login Delay:						
	The time in seconds to delay while displaying the login message.					
Advertising Services	5 ent on the login page.					
Advertising	Enable Advertising Services content					
Cloud Identity Optionally present gues	sts with various cloud identity / social login options.					
Enabled	Enable logins with cloud identity / social network credentials					
Multi-Factor Authent	tication ctor when authenticating.					
Provider	No multi-factor authentication					
Network Login Acce	ss Jogin page.					
Allowed Access						
	Enter the IP addresses and networks from which logins are permitted.					
Denied Access						
	Enter the IP addresses and networks that are denied login access.					
* Deny Behavior	Send HTTP 404 Not Found status \checkmark					
Post-Authentication	Select die response of the system to a request that is Not permitted.					
Actions to perform afte	r a successful pre-authentication.					
Health Check	If selected, the guest will be required to pass a health check prior to accessing the network.					
Update Endpoint	If selected, the endpoint's attributes will also be updated with other details from the user account.					
	Save Changes 🛛 🕵 Save and Reload					

aruba	Clear	ClearPass Guest								
📲 Guest 🔹 🛛 🛛	Home » Configuration » Pages » Web Logins									
👔 Devices 🔹 📀	Web Logins		🚜 Create a new web login page							
📮 Onboard 🔹 🧿	-									
🔨 Configuration 📀	Many NAS devices support Web-based authentication for visitors.									
- 🎭 Authentication	By defining a web login page on the ClearPass Guest you are able to pr	vide a customized graphical login page fo	r visitors accessing the network through these NAS devices.							
⊒-🮯 Content Manager	Use this list view to define new web login pages, and to make changes	to existing web login pages.								
- 🥸 Private Files - 🍲 Public Files	Onboard device provisioning pages are now managed from the Web	Login tab within provisioning settings								
🕵 Guest Manager	△ Name Page Title	Page Name Page Skin								
🖅 靲 Hotspot Manager	🚜 school	school Galleria Skin 3								
⊒- 💭 Pages	🚰 Edit 🕞 Duplicate 😵 Delete 🍇 Translations 🛶 Launch									
- Torms	1 web login 🏠 Reload	Show all rows								
- III List Views -) Self-Registrations	🛞 Back to pages									
- 🥵 Web Logins	🔦 Back to configuration									
web Pages	🗠 Back to main									

You can test the page as well, when you'll click on the launch a tab will open and you'll see the captive portal note the URL which in this case is https://victory.clearpass.info/guest/school.php? browser=1

The "guest/school.php" is used in the URL redirection which we configured in MM

Now go to content manager and upload your terms and condition page.



8.4 Guest Testing

Now we'll get a test device to connect to Guest SSID, it gets automatically redirected to guest page in ClearPass but the browser will issue a warning



We'll have a look at the certificate, and we'll see it is the default captive portal certificate which is on the controller.

securelogin.hpe.com	DigiCert Global CA G2	DigiCert Global Root G2
Subject Name		
Country	US	
State/Province/County	California	
Locality	Palo Alto	
Organisation	Hewlett Packard Enterprise Company	
Organisational Unit	Aruba Networks	
Common Name	securelogin.hpe.com	
Issuer Name		
Country	US	
Organisation	DigiCert Inc	
Common Name	DigiCert Global CA G2	
Validity		
Not Before	Fri, 04 Dec 2020 00:00:00 GMT	
Not After	Sat, 04 Dec 2021 23:59:59 GMT	
Subject Alt Names		
DNCN		

We'll accept this and carry on, but for all deployments you need to have a public server certificate for your controllers. Once we accept the certificate, we'll get redirected to the captive portal page on ClearPass

🔾 Galleria WiFi Login	× +	
$\left(\leftarrow \right) \rightarrow$ C $rac{1}{2}$	📵 🖴 🗝 https://victory.dearpass.info/guest/school.php?cmd=login&mac=a0:88:> 🚥 😾 📿 Search	II\ I I I I I I
	Galleria WiFi Dease login to the network using your username and password. Username: cpguser Password: Terms: I accept the terms of use Log In	
	Contact a staff member if you are experiencing difficulty logging in.	
	Aruba: NETWORKS	-
		Manager and Manager and Andrews

Before we login with our guest credentials, we'll look at the MM dashboard and see the user is in guest-login role with minimum access.

다 AOS10 이	Lū Clients								31	iours List Summary
- Manage	CLIENTS ALL	~ C							7.84 MB (① 1.6	1 MB ⊙6.23 MB)
Devices	All O Connec	ting • Connected	• Failed •	Offline	Ø Blocked	Wireless	Wired	Remote		
🗅 Clients			U	2	U		2	0		
😩 Guests										\odot
Applications		Status 🚛	Y IP Address	VLAN	Connected	То	Y Gateway Role	▼ SSID/Port	Y Health ✓	Usage
Security	AriyaP	O Connected	192.168.1.132	192	b4:5d:50:c6	:82:4a	C <mark>P-Guest</mark>	Schoo-Guest		7.84 MB
← 🗔 a088b450c084 🛛 ⊘	B Q ⊘ Summary Al Insights Location	on Sessions								4 31
— Manage ————	CLIENT DETAILS	C							Actions 🔻	• Go Live
器 Overview	DATA PATH									
Applications		CLIENT	SSID			AP	SWITCH		GATEWAY	
— Analyze —			»»» (?		>>>>>					
Live Events		AriyaP	Schoo-G	Jest		b4:5d:50:c6:82:4a	Aruba-2930F-8G-PoE	P-2SEPP	7005_AOS10_gwy2	
♪ Events		CONTECTED				5	01		01	
🖏 Tools										
	CLIENT		NET	NORK				CONNECTION		
	USERNAME		VLAN	1		VLAN DERIVA	TION	CHANNEL	BAND	
	a088b450c084 HOSTNAME	CLIENT TYPE	192 AP R	OLE		AP DERIVATIO	N	6 (20 MHz) CLIENT CAPABILIT	2.4 GHz	
	AriyaP IP ADDRESS	Wireless	CP-G GATE	WAY ROLE		 SWITCH ROLE	E	CLIENT MAX SPEE	D	
	GLOBAL UNICAST IPV6 ADDRESS	au:88:D4:DU:CU:84	SEGI	uest IENTATION		-		LEDs on ACCESS P	OINT (b4:5d:50:c6:82:4a)	
	CLIENT OS	CONNECTED SINCE	AUTI 192	+ SERVER		DHCP SERVER 192 168 1 1	R			
	MANUFACTURER Intel Corporate	ENCRYPTION	TUN	NELED		TUNNELED IC	þ			
	ALINSIGHTS ● 0 ● 0 ● 0									

Then we'll check the access tracker and see that we have a failed MAC authentication.

aruba			Menu 🗮							
Dashboard O	Monitoring	g » Live Monitoring								
🗾 Monitoring 📀	Access	ess Tracker Mar 17, 2021 11:26:30 AEDT								
Live Monitoring The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.										
- P Accounting	TAII	Requests]	victory (192.168	.1.95)	15 Last 1 day before Tod	Edit				
- Analysis & Trending										
- 🔜 System Monitor D 🛃 Profiler and Network Scan	Filter: Red	quest ID	✓ contains ✓	+ Go Clear Filter			Show 20 v records			
	#	Server	Source	Username	Service	Login Status	Request Timestamp 🔻			
	1.	192.168.1.95	RADIUS	cpguser	GG User Authentication with MAC Caching	ACCEPT	2021/03/17 11:26:22			
	2.	192.168.1.95	RADIUS	a088b450c084	GG MAC Authentication	REJECT	2021/03/17 11:25:58			

Request Details		Requ	Request Details							8
Summary Input O	utput Alerts	S	Summary	Input	Dutput	Alerts				
Login Status:	Login Status: REJECT					cess Profile]				
Session Identifier:	R0000009-01-60514c96	Sys	/stem Posture	Status:		v (100)				
Date and Time:	Mar 17, 2021 11:25:58 AEDT	Auc	udit Posture S	tatus:	UNKNOWN	N (100)				
End-Host Identifier:	A0-88-B4-50-C0-84									
Username:	a088b450c084									
Access Device IP/Port:	192.168.1.242									
Access Device Name:	AOS10-gateways									
System Posture Status:	UNKNOWN (100)									
	Policies Used -									
Service:	GG MAC Authentication									
Authentication Method:	MAC-AUTH									
Authentication Source:	None									
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]									
Roles:	[Other], [User Authenticated]									
Enforcement Profiles:	[Denv Access Profile]									
I Showing 2 of 1-11 rec	cords >>> Show Configuration Export Show Logs Close	I .	 Showing 1 	of 1-14 re	cords 🕨	4	Show Configuration	Export	Show Logs	Close

This is normal as this MAC address has not been seen before.

It should be noted that the redirection happens from the AP not the gateways

b4:5d:50:c6:82:4a# sh client

Client List Name IP Address MAC Address OS ESSID Access Point Channel Type Role IPv6 Address Signal Speed (mbps) ---- ------ ------_____ _____ __ _____ ____ Number of Clients :0 Info timestamp :8460 b4:5d:50:c6:82:4a# b4:5d:50:c6:82:4a# b4:5d:50:c6:82:4a# sh client Client List _____ Name IP Address MAC Address OS ESSID Access Point Channel Type Role IPv6 Address Signal Speed (mbps) _____ _____ -----____ -----____ ___ ----a088b450c084 192.168.1.132 a0:88:b4:50:c0:84 Win 10 Schoo-Guest b4:5d:50:c6:82:4a 6 GN CP-Guest fe80::7d4a:2f07:955c:cd4f 54(good) 72(ok) Number of Clients :1 Info timestamp :9155 b4:5d:50:c6:82:4a# b4:5d:50:c6:82:4a# sh external-captive-portal External Captive Portal _____ Auth Text Redirect Url Name Server Port Url Server Fail Through Disable Auto Whitelist Use HTTPs Server Offload Prevent Frame Overlay In Use Redirect Mode Switch IP _____ ____ ---- ----_____ _____ _____ _____ _____ default localhost / 80 Authenticated Yes Disable Enable No Disable No Yes No CP-Guest victory.clearpass.info 443 /guest/school.php http://www.arubanetworks.com Disable Enable Yes No Disable Yes Yes No b4:5d:50:c6:82:4a# sh external-captive-portal CP-Guest Name :CP-Guest Server :victory.clearpass.info Port :443 Url :/guest/school.php Auth Text : Redirect Url :http://www.arubanetworks.com Server Fail Throuth :Disable Disable Auto Whitelist : Enable Use HTTPs :Yes Server Offload :No Prevent Frame Overlay :Disable In Used :Yes Redirect Mode :Yes Switch IP :No b4:5d:50:c6:82:4a#

Now when the user performs a successful the login (we are using username cpguser) process, they will be redirected to the "redirect URL" that we specified.



Now let's look at the Client dashboard and access tracker, note that the user role is now "guest".

법 AOS10 이	Lū Clients							3h	ours
- Manage	CLIENTS ALL ~	С					8.31 N	ИВ (🕀 1.75	5 MB ⊕6.56 MB)
Devices	All O Connecting	• Connected • Fai	iled Offline @	Blocked Wireless	s Wired	Remote			
🗔 Clients	3 0	1 0	2	0 1	2	0			
😩 Guests									\odot
Applications	▼ Client Name Status	us ↓= Y IP A	Address VLAN	Connected To	Y Gateway Role	▼ SSID/Port	Y Health	~	Usage
Security	cpguser ○ Con Con	onnected 192.168	3.1.132 192	b4:5d:50:c6:82:4a	guest	Schoo-Guest	Good		8.31 MB

And the access tracker shows a successful authentication that matches with "GG User Authentication with MAC Caching" policy.

aruba			Menu 🗮							
Dashboard O	Monitorin	ng » Live Monitoring								
Monitoring 📀	Acces	SS Tracker Mar 17, 2021 11:27:56 AEDT 🔗 AUTO								
Access Tracker	The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.									
- Accounting 		Edit								
Analysis & Trending										
- System Monitor	Filter: Re	equest ID	✓ contains ✓				Show 20 $$			
– Januar - J	#	Server	Source	Username	Service	Login Status	Request Timestamp 🔻			
	1.	192.168.1.95	RADIUS	cpguser	GG User Authentication with MAC Caching	ACCEPT	2021/03/17 11:26:22			
	2.	192.168.1.95	RADIUS	a088b450c084	GG MAC Authentication	REJECT	2021/03/17 11:25:58			

Request Detai	ls							
Summary	Input	Output	Accounting					
Login Status:	:	ACCE	PT	^				
Session Iden	tifier:	R000	1000000a-01-60514cae					
Date and Time:		Mar 1	Mar 17, 2021 11:26:22 AEDT					
End-Host Identifier:		<mark>A0-8</mark>	8-B4-50-C0-84					
Username:		cpgu	guser					
Access Device IP/Port:		192.1	192.168.1.242					
Access Devic	Access Device Name:		AOS10-gateways					
System Post	ure Status:		IOWN (100)					
			Policies Used -					
Service:		<mark>GG U</mark>	ser Authentication with MAC Caching					
Authenticatio	on Method:	PAP						
Authenticatio	on Source:	Local	:localhost					
Authorization	Source:	[Gue	[Guest User Repository], [Endpoints Repository], [Time Source]					
Roles:		[<mark>Gue</mark>	st], [User Authenticated]					
Enforcement	Profiles:	GG M	AC Caching Bandwidth Limit, GG MAC Caching Session Limit, GG Guest MAC	~				
I I Showing	1 of 1-11	records 🕨	Change Status Show Configuration Export Show Logs	Close				

Request Details						
Summary Input Output Acc	counting					
Audit Posture Status: UNKNOWN (1	00)		^			
RADIUS Response		۲				
Bandwidth-Check:Allowed-Limit	0					
Bandwidth-Check:Check-Type	Today					
Bandwidth-Check:Limit-Units	мв					
Endpoint:Guest Role ID	2					
Endpoint:MAC-Auth Expiry	2021-03-18 11:00:00					
Endpoint:Username	cpguser .					
Expire-Time-Update:GuestUser	0					
Expiry-Check:Expiry-Action	0					
Post-Auth-Check:Action	Disconnect					
Post-Auth-Check:Action	Disconnect and Block Access					
Radius:Aruba:Aruba-User-Role	Guest					
Radius:IETF:Session-Timeout	0					
I ≤ Showing 1 of 1-11 records ► ►	Change Status Show Configuration Export Show Logs	Clo	ose			

Request Details

Also note that one of the post authentication actions were to update the endpoint repository status for that MAC address to be known.

Dashboard O	Configura	ation » Id	lentity » Endpoints			iguration » Identity » Endpoints									
Monitoring O	Endpo	dpoints													
🝰 Configuration 📀															
- 🛱 Service Templates & Wizards	This pag	ige automatically lists all discovered, ingested or authenticated endpoints. An endpoint is a device that communicates back and forth with a network to which it is													
— 🛱 Services	connecte	ed (e.g. [Desktops, Laptops, Sma	rtphones, Tablets, Servers	, Workstations, Internet-of-things (IoT) devi	ces).									
🖃 🖴 Authentication															
🛱 Methods	Filter: M	IAC Addres	s v cont	ains 🗸	+ Go Clear Filter			Show 20 v records							
- 🛱 Sources			MAC Address .	llostnamo	Douise Category	Device OF Family	Ctatue	Drefiled							
🖃 🚨 Identity			MAC Address *	Hostilallie	Device Category	Device OS Faililiy	Status	Profiled							
- 🛱 Single Sign-On (SSO)	1.		00-0C-29-F3-EF-AF	victory	Server	ClearPass	Unknown	Yes							
- 🛱 Local Users	2.		A0-88-B4-50-C0-84		Computer	Windows	Known	Yes							
-🔅 Endpoints	Showing	1-2 of 2			Authentication Records Bulk Updat	e Bulk Delete Trigger S	erver Action Update Fin	ngerprint Export Delete							
- 🛱 Static Host Lists															

Now because the status of this endpoint is known the next time, this client connects it will not be redirected to the captive portal until its allotted time has expired. So now if we disconnect the client, we should see it will successfully MAC auths. This uses RADIUS CoA. We can do that directly from the access tracker.

Summary Input C	Output Accounting	_	Access Control Capabilities -
Login Status:	ACCEPT	Select Access Control Type :	: O Agent O SNMP RADIUS COA O Server Action
Session Identifier:	R000000a-01-60514cae		
Date and Time:	Mar 17, 2021 11:26:22 AEDT	RADIUS COA Type:	[ArubaOS Wireless - Terminat >
End-Host Identifier:	A0-88-B4-50-C0-84		
Username:	cpguser		
Access Device IP/Port:	192.168.1.242		
Access Device Name:	AOS10-gateways		
System Posture Status:	UNKNOWN (100)		
	Policies Used -		
Service:	GG User Authentication with MAC Caching		
Authentication Method:	ΡΑΡ		
Authentication Source:	Local:localhost		
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]		
Roles:	[Guest], [User Authenticated]		
Enforcement Profiles:	GG MAC Cachina Bandwidth Limit, GG MAC Cachina Session Limit, GG Guest MAC	·	
Radius [Aru Summary Input O	ubaOS Wireless - Terminate Session] successful for client a088b450c084.		
Login Status:	ACCEPT		
Session Identifier:	R000000a-01-60514cae		
Date and Time:	Mar 17, 2021 11:26:22 AEDT		
End-Host Identifier:	A0-88-B4-50-C0-84		
Username:	cpguser		
Access Device IP/Port:	192.168.1.242		
Access Device Name:	AOS10-gateways		
System Posture Status:	UNKNOWN (100)		
	Policies Used -		
Service:	GG User Authentication with MAC Caching		
Authentication Method:	PAP		
Authentication Source:	Local:localhost		
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]		
Roles:	[Guest], [User Authenticated]		
Enforcement Profiles:	GG MAC Cachino Bandwidth Limit. GG MAC Cachino Session Limit. GG Guest MAC cords ► ⊨ Change Status Show Configuration Export Show Logs Close		

aruba			Menu 🗮								
Dashboard O	Monitorir	unitoring » Live Monitoring » Access Tracker									
🛃 Monitoring 📀	Acces	cess Tracker Mar 17, 2021 11:33:25 AEDT									
Live Monitoring Access Tracker	The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.										
- Jaccounting - Jaccount Activity	T [AI	II Requests]	Edit								
Analysis & Trending											
- Joseph Monitor	Filter: R	equest ID	✓ contains ✓	+ Go Clear Filter			Show 20 v records				
	#	Server	Source	Username	Service	Login Status	Request Timestamp 🔻				
	1.	192.168.1.95	RADIUS	cpguser	GG MAC Authentication	ACCEPT	2021/03/17 11:33:04				
	2.	192.168.1.95	RADIUS	cpguser	GG User Authentication with MAC Caching	ACCEPT	2021/03/17 11:26:22				
	з.	192.168.1.95	RADIUS	a088b450c084	GG MAC Authentication	REJECT	2021/03/17 11:25:58				

Looking at the details of that session

Request Details		Request Details						
Summary Input O	utput Accounting	Summary Input Output Accounting						
Login Status:	ACCEPT	^	Enforcement Profiles: [Allow Access Profile], GG Guest Device Profile					
Session Identifier:	R000000b-01-60514e40		System Posture Status: UNKNOWN (100)					
Date and Time:	Mar 17, 2021 11:33:04 AEDT		Audit Posture Status: UNKNOWN (100)					
End-Host Identifier:	A0-88-B4-50-C0-84		RADIUS Response	۲				
Username:	cpguser							
Access Device IP/Port:	192.168.1.242		Radius:Aruba:Aruba-User-Role Guest					
Access Device Name:	AOS10-gateways		Radius:IETF:User-Name cpguser					
System Posture Status:	UNKNOWN (100)							
	Policies Used -							
Service:	GG MAC Authentication							
Authentication Method:	MAC-AUTH							
Authentication Source:	Local:localhost							
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]							
Roles:	[Guest], [MAC Caching], [User Authenticated]							
Enforcement Profiles:	[Allow Access Profile]. GG Guest Device Profile	~	the Chaming Lof L12 records and Change Status Show Configuration Export Show Logs	Class				
a showing 1 of 1 12 fee	Close		A showing for 1-12 records P Change status Show Conliguration Export Show Logs	ciose				

Here we can see the user in the gateway's user table using tunnel forwarding mode and in guest user role.

(7005_AOS10_gwy This operation	2) #show user can take a while	depending of	n number of u	sers. Please	be patient	
Users						
IP	MAC	Name	Role	Age(d:h:m)	Auth VPN	link
Connected To mode Type H	Roaming Ession ost Name User Ty	d/Bssid/Phy ype	Profile		Fo	rward
192.168.1.132	a0:88:b4:50:c0:84	a088b450c)84 guest	00:00:03	MAC	1
Win 10	4a Wireless So WIRELESS	cnoo-Guest	Schoo-Gue	st_#161593813	5060_41#_	atunnel
User Entries: 1 Curr/Cum Alloc (7005_AOS10_gwy	/1 :1/6 Free:0/5 Dyr 2) #	n:1 AllocErr	:0 FreeErr:0			