Contents

	1.1	Revision History	1
2	De	mo Topology	2
3	Arı	uba Central Account	3
4	Arι	uba Central Configuration	6
	4.1	LAN Switch Configuration	6
	4.2	Gateway Configuration	7
	4.3	AP Configuration	12
	4.4	Assigning Static IP addresses for APs	14
	4.5	Firmware Upgrade	14
	4.6	Gateway Cluster	17
	4.7	Monitoring Gateway Cluster	17
5	Cle	arPass Initial Configuration	20
	5.1	Joining AD Domain	21
	5.2	ClearPass dot1x Service	22
	5.3	NAD Configuration	24
6	WL	AN Configuration	25
	6.1	Tunnelled Mode Wireless Configuration	25
	6.2	Tunnelled Mode Wireless dot1x Testing	27
	6.3	Bridge Mode Wireless Configuration	31
	6.4	ClearPass Service Modifications	34
	6.5	Bridge Mode Wireless dot1x Testing	36
	6.6	Mixed Mode Wireless Configuration	38
	6.7	ClearPass Service Modifications	43
	6.8	Mixed Mode Wireless dot1x Testing	44
7	RF	Monitoring	47
8	Gu	est Access Configuration	53
	8.1	Guest Wireless Configuration	53
	8.2	ClearPass Guest policy Configuration	57
	8.3	ClearPass Guest Portal Configuration	62
	8.4	Guest Testing	66

1.1 Revision History

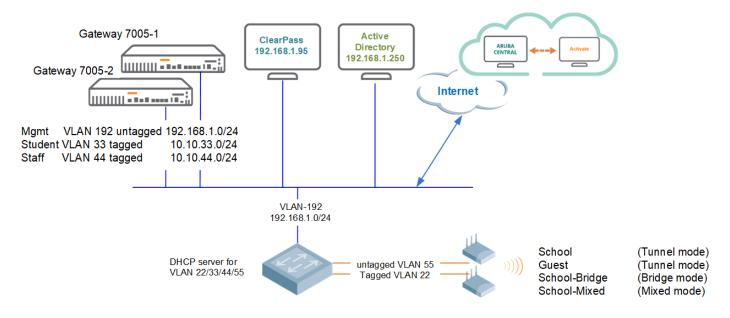
DATE	VERSION	EDITOR	CHANGES				
15 Mar 2021	0.1	Ariya Parsamanesh	Initial creation				
22 May 2021	0.2	Ariya Parsamanesh	Added the ClearPass guest operator login				
04 Jul 2021	0.3	Ariya Parsamanesh	Added the Monitoring section				
12 Jul 2021	0.4	Ariya Parsamanesh	Added the bridge and mixed mode WLANs				

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

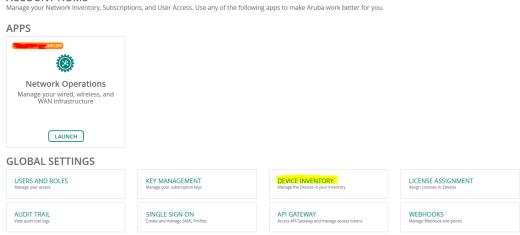
3 Aruba Central Account

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.

		Device Invento ted with your ac		automatically discovered and are not displayed in your inventory, you can add devices man	ually	by clicking the	ADD DEVICES
text.							
You can also a	add you	r devices using t	he Aruba Cer	tral mobile app and they will automatically appear in your inventory.			
All 15	A	ccess Points	Switche 5				
				ADD DEVICES			
DEVICES				SERIAL NUMBER MAC ADDRESS			\odot
Y Serial N	t≞ A	MAC Address	Y Part			Y Custo	▼ Assign
CNC0	- B4	4:5D:50:	IAP-324-	SERIAL NUMBER MAC ADDRESS		HPE Aruba	Foundation
CNC0	- B4	4:5D:50:	IAP-324-	SERIAL NUMBER MAC ADDRESS		HPE Aruba	Foundation
				SERIAL NUMBER MAC ADDRESS			
Add Devices	I	nport 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 ASSIGNME	NT						
Access Points	Unlicensed Licen 0 2	sed Switches	Gateways 8					
LICENSE SUMMAR		ICENSE ASSIGNMEN	MANAGE LICEN	ISE ASSIGNMENT (MANUAL	.)	×	Assigned License	SELECT ALL
Foundation	, 3		Overview of select	cted Access Points	2		Foundation Foundation	
Assigned 2 (1 available) Advanced			Choose License Type FOUNDATION			_		
Assigned 0 (0 available)	0			Cancel Unassign Update				
AUTO-ASSIGN	•							
Note: Licenses can be assig devices	gned manually on							2 ITEM(S) SELECTED

Access Points 2	Switches 5	Gateways Unlicen	sed Licensed 5				
ICENSE SUMMA		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)	0				_		
UTO-ASSIGN)D						
iote: Licenses cari be as levices	signed manually on						2 ITEM(5) SELECTED MANAGE ASSIGNMENT

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

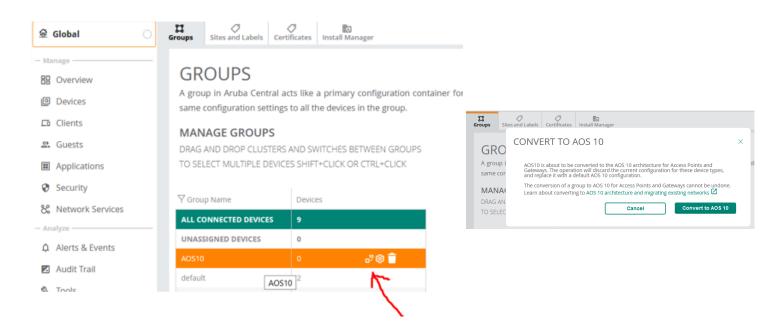
ACCOUNT HOME

APPS	ions, and user Access. Use any of the h	onowing apps to make Aruba work better for you.	
Network Operations Manage your wired, wireless, and WAN infrastructure			
LAUNCH			
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 1 abale Cartificate Install Mananar	
— Manage ———	CREATE NEW GROUP	×
Cverview	GROL	
Devices	A group in AOS10	devices with common con
🗖 Clients	configuration Use the group as Template group by selecting the device 1	
🕰 Guests	MANAGI DRAG AND AP AND GATEWAY SWITCH	
Applications	TO SELECT Group password settings	
Security	PASSWORD	
% Network Services	∀ Group Nar	
— 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		
ង្វៃ Organization		
	Image: Second	

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.

ය Groups	Sites and Labels	Certificates	Install Manager									
GROUPS A group in Aruba Central acts like a primary configuration container for devices. You can combine devices with common conficonfiguration settings to all the devices in the group. MANAGE GROUPS DRAG AND DROP CLUSTERS AND SWITCHES BETWEEN GROUPS TO SELECT MULTIPLE DEVICES SHIFT+CLICK OR CTRL+CLICK												
∀Grou	p Name	Dev	ices	∑ Name	√ Location							
ALL CO	DNNECTED DEVICE	S 12		7005_AOS10_gwy1	Melbourne,Australia							
UNAS	SIGNED 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

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 🕗											
	JWICH	Interface Security	System Routing IGMP	QoS Device Prof	file Configuration Audit						
erview			, ,								
ients	SWITCHES	SWITCHES (1)									
	Hostname										
Ν	Aruba-2930F-8G	-PoEP-2SFPP	10.224.254.2		10.224.254.1	b0:5a:da:98:9a:00	Melbou	rne			
evice											
Aruba-2930F-8G Switch Switch Switch Switch Stacks Interface Security Switch Stacks Switch Stacks Switch Spanning Tree											
Clients	Ports PoE Trur	nk Groups VLANs Sp.	anning Tree Loop Protect	ion							
Clients LAN	Ports PoE Trur		anning Tree Loop Protect	ion						6 VL	
Clients LAN Device		ettings	anning Tree Loop Protect	ion						6 VI	
Clients AN Device	\vee VLANs Se	ettings	anning Tree Loop Protect	ion						6 VI	
Clients LAN Device yze	 VLANs Se Primary V VLANs 	ettings /LAN: 1			Tagged Ports	Untagged Ports	DHCP Helper IP	Vaire	lumbo	6 11	
Clients LAN Device yze	✓ VLANs Se Primary V	ettings	IP Assignment DHCP	ion IP Address	Tagged Ports	Untagged Ports 6,9-10	DHCP Helper IP	Voice ×	Jumbo	6 VL	
Clients LAN Device Jyze Alerts & Events Audit Trail Tools	VLANS SC Primary V VLANS	attings /LAN: 1 Name	IP Assignment							6 VL	
	VLANS Se Primary V VLANS ID 1	Attings /LAN: 1 Name DEFAULT_VLAN	IP Assignment DHCP	IP Address		6,9-10	-	×	×	6 VL	

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.

← 📼 Aruba-2930F-8G ⊘	Switch	c
Manage	Switches Stacks Interface Security System Routing IGMP QoS Device Profile Configuration Audit	
Overview	Access/DNS Time SNMP CDP DHCP	
🗖 Clients		
몲 LAN		3 DHCP Pools
Device	DHCP server	
Analyze	DHCP server	
✿ Alerts & Events	DHCP Pools	+
Audit Trail		=
🖏 Tools	Name Network Netmask Edit Delete	=
🛍 Reports	AP-VLAN 10.10.55.0 255.255.0	
Maintain	Staff-YLAN 10.10.44.0 255.255.25.0	
Firmware	Student-VLAN 10.10.33.0 255.255.0	

```
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.

🛱 AOS10	Access Points Switches	vays						ii ili Ust Summary Config
- Manage	Gateways • Online 0 0	• Offline 0	Clusters 0					
Devices	GATEWAYS							±
□ Clients	Y Device Name	▼ Model	Y IP Address	∀ мас	▼ Serial	Firmware Version	Uptime	Inspection Engine
😩 Guests								
Applications								

Access Points	Suitzbar Colouint	i List	LL 😥 Summary Config
	SET GROUP TYPE	Advanced Mode	Cuided Setue
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	iii II. 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+.				

법 AOS10 〇	Access Points Switches Gateways			SELECTED GROUP TYPE Gateway	III III List Summary Config
— Manage —	System Interface Routing				Advanced Mode
B 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: VIPv4				
— 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	Elist 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:		
a Guests			
Applications	> LACP		
	> Tunnel Loop Prevention		

Adding the relevant ports for Aruba 7005 gateway.

다 AOS10 이		SELECTED GROUP T		■ II. ist Summary	Config
— Manage ———	System Inte			Advanced M	Лode
B 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			=
Applications	GE-0/0/0 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				

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.

LI AOS10	Access Points Switches Gateways		SELECTED GROUP TYPE := 1h & Confe 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	Vians		
🗈 Clients			
a Guests	NAME	ID(S)	=
Applications	Server-VLAN	192	
	Staff-VLAN	44	
Security	Student-VLAN	33	
Analyze Alerts & Events		1	

Adding the VLANs to appropriate ports.

X AOS10	Access Points Switches	ے Gateways							SELECTED G Gateway	ROUP TYPE	= II. ist Summary Con
– Manage –	System Interface Ro	outing									Advanced Mode
B Overview	Ports VLANS DHO	P Pool Management	GRE Tunnels Bulk	configuration upload	SLB						
Devices											
Clients	Ports		-	-	~	-					
a Guests	∀PORT TYF GE-0/0/0	PE Y ADMIN ST	ATE POLICY	YMODE trunk	Y NATIVE VLAN	Y ACCESS VLAN	TRUNK VLANS	TRUSTED VLANS		DESCRIPTION GE0/0/0	=
Applications	GE-0/0/1	Enabled	Not-defined	access		1			✓ ✓	GE0/0/0	
Security	GE-0/0/2	Enabled	Not-defined	access		1		1-4094	v √	GE0/0/2	
- Analyze		Enabled	Not-defined	access		1		1-4094	√ √	GE0/0/3	
 Alerts & Events Audit Trail 											
Tools	+										
0 10015											
	GE-0/0/0										
	Туре:	LAN	•								
	Admin state:	~									
	Speed:	auto	Mbps								
	Duplex:	auto	/								
	Poe:										
	Trust:	✓ 🖊									
	Policy:	Not-defi	ned 🗸								
	Mode:	Trunk	~								
	Native VLAN:	192									
	Allowed VLANs:	33,44,192	~ ©)							
	Description:	GE0/0/0									
	Jumbo MTU:										
	Port monitoring:	-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		
Lo 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"

다 AOS10 이	O Access Points		<u>a</u>				SELECTED GROUP TYPE Gateway	I≣ List	III 👸 Summary Config
— Manage ———	System Inter	New role							Basic Mode
B Overview	Roles Polic	Name:	Student				ш		
Devices	Roles		Studing						
🗖 Clients					Cancel	Save Settings			=
😩 Guests				35 Rules	L				
Applications	ap-role								
Security	authenticat	ted		4 Rules					
- Analyze	default-iap-	-user-role		2 Rules					
Alerts & Events	default-via-	role		3 Rules					
🛛 Audit Trail	default-vpn	n-role		4 Rules					
🔍 Tools	guest			11 Rules					
🗊 Reports	+								

ជ AOS10 이	Access Points	© Catoway				SELECTED GROUP TYPE Gateway	i≣ List	II. Summary Config
- Manage	System Inter	icy						Basic Mode
Cverview	Deles Della	existing policy:				ш		
Devices								=
Lī Clients	Create a stateful-dot	a new policy:						
2. Guests	Student Policy ty	/pe:	Session 🗸					
Applications	switch-logor Policy n	ame:	allowall 🗸					
Security Analyze	sys-ap-role							
A Alerts & Events	sys-switch-r	1:						
Audit Trail	voice							
🖏 Tools	+				Cancel Save Settings			
🔝 Reports	Student Policies	Bandwidth Me	pre					
- Maintain			RULES COUNT	∀түре	POLICY USAGE			=
	global-sacl		0	session	ap-role, authenticated, default-via-role	, defa		
	apprf-student-sacl		0	session	Student			
	+							

Here we'll add the allow-all policy.

ជ AOS10	Access Points Switches Gateway	s			SELECTED GROUP TYPE Gateway	Elist Summary
— Manage ————	System Interface Routing WAN	Security VPN High Availability	Config Audit			Basic Mode
B Overview	Roles Policies Aliases Appl	ications Apply Policy Auth Ser	vers Role Assignment (AAA Profiles)	L2 Authentication L3 Authentication Adva	anced Firewall	
Devices			RULES			=
Clients	stateful-dot1x		0 Rules			
2. Guests	Student		2 Rules	Î		
Applications	switch-logon		1 Rules			
Security	sys-ap-role		23 Rules			
Analyze	sys-switch-role		24 Rules			
Alerts & Events	voice		41 Rules			
Audit Trail	+					
Tools						
Reports	Student Policies Bandwidth	More				
Firmware	∀ NAME	RULES COUNT	Ттуре	iggararrow POLICY USAGE		≡
NAME AND A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTIONO	global-sacl	0	session	ap-role, authenticated, d	efault-via-role, defa	
	apprf-student-sacl	0	session	Student		
	allowall	2	session	authenticated, default-ia	p-user-role, default	

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

ជ AOS10 이	Access Points Switches Gateways	SELECTED GROUP TYPE Gateway	⊞ II. List Summary Confi
— Manage —	System Interface Routing WAN Security VPN High Availability Config Audit		Basic Mode
B Overview	Roles Policies Allases 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 V		
Alerts & Events	Re-auth interval: 0 minutes 🗸		
🛛 Audit Trail			
🖏 Tools	Max sessions: 65535		
Reports	Deep packet inspection:		
Maintain Firmware			
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.

ជ AOS10	Image: Construction of the second s	SELECTED GROUP TYPE := II. Gateway List Summary
- 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 Authentica	tion Advanced Firewall
Devices	Roles	
Clients	A	
🔐 Guests	[™] NAME [™] NAME	=
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

디 AOS10 이	Access Points	Switches Gatewaye			SELECTED GROUP TYPE Gateway	iii List	II. B Summary Config
- Manage	System Interf	New server					Basic Mode
BB Overview	Roles Policie	Name:	ClearPass-GW				
Devices			ClearPass-Gw				
Clients		IP address / hostname:	192.168.1.95				
🚉 Guests		Туре:	Radius 🗸				
# Applications		.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	Radius				
Security				Cancel Save Settings			
- Analyze	+			Sancer Sectings			

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

ជ AOS10 이	Access Points Switches Gateways		SELECTED GROUP TYPE Gateway	III II. List Summary Conf
— Manage ————	System Interface Routing WAN Security V	PN High Availability Config Audit		Basic Mode
B Overview	Roles Policies Aliases Applications App	y Policy Auth Servers Role Assignment (AAA Profiles) L2 Authentication L3 Authentication Advanced	Firewall	
Devices	Server options			
🖻 Clients				
🚉 Guests	Name:	ClearPass-GW		
Applications				
Security	IP address / hostname:	192.168.1.95		
— Analyze ———	Secure radius:			
户 Alerts & Events				
🛛 Audit Trail	Auth port:	1812		
🖏 Tools	Acct port:			
🔝 Reports	Piece por a	1813		
— Maintain ————	Shared key:			
Firmware	Datasa kuu			
	Retype key:			
	Timeout:	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
	1001	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.

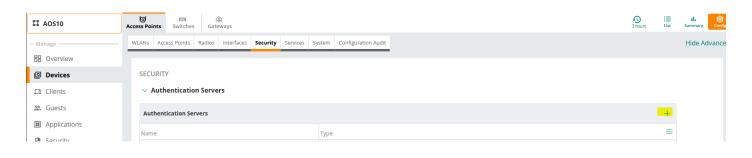
- Manage	System	WAN	Interface	Security V	PN Routing H	igh Availability Cor	nfig Audit				
88 Overview	Roles	Policies	Aliases	Applicatio	ns Apply Policy	Auth Servers	Role Assignment (AAA Profiles)	L2 Authentication	L3 Authentication	Advanced	Firewall
Devices		NAME			SERVERS		FAIL THROUGH	LOAD BALANCE		SERVER RULES	
🗈 Clients											
🚨 Guests											
Applications		19									
Security							No d	ata to display			
Analyze											
Alerts & Events		+									
Audit Trail											
🖏 Tools		All serv	vers								
Reports		NAME			TYPE		IP ADDRESS / HO	STNAME	SERVER GROU	JP	
Maintain ————		ClearPa	ass1		Radius		192.168.1.95			-	
Firmware					RFC 35		192.168.1.95		-		
					NIC 55		192.100.1195				

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	Timezone :	Melbourne UTC+10
Security		The selected country observes Daylight Savings 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:	5
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	SECURITY	
Devices	> Authentication Servers	
Clients		
a Guests	> MPSK Local	
Applications	> User For Internal Server	
Security	∨ Roles	
— Analyze —	Roles -+ Access Rules For Selected Roles	+
Alerts & Events	Role 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.

	Access Points Switches Gatewa	ays						iii th List Summa
age ———	Access Points • Online	• Offline Radios						
Overview	2 1	1 4						
evice	ACCESS POINTS (2)							
lients	▼ Device Name	Status	▼ IP Address	Y Model	Firmware Version	Y Group	Uptime	
ecurity	b4:5d:50:c6:82:3c	O Offline	10.10.55.10	AP-324	10.2.0.1_79907	AOS10	-	
ze	b4:5d:50:c6:82:4a	Online	10.10.55.11	AP-324	10.2.0.1_79907	AOS10	4 Hours 42 Minu	ites 18 Seconds
lerts & Events								
udit Trail								
ools								
tain ———								
ïrmware								
b4:5d:50:c6:82:3c 🛆 🗚	ccess Point							
ge	Access Points Configuration Audit							Hide /
verview								
evice	Access Points (1)							
ients			ddress	WLANs	Radio Profile	Ту		
curity	b4:5d:50:c6:82:3c	Down 10.10	0.55.10	All SSIDs selected	default	AP-:	324	
ze								
ze								
lerts & Events								
lerts & Events udit Trail								
lerts & Events udit Trail								
lerts & Events udit Trail pols	101							Ø
lerts & Events udit Trail pols	ලා ass Point							(ang
lerts & Events udit Trail ools b4:5d:50:c6:82:3c 🔺 Acc	Image: Solid Sector S							Come Hide Advanced
lerts & Events udit Trail b4:5d:50:c6:82:3c Acco pp								Ride Advanced
lerts & Events udit Trail b4:5d:50:c6:82:3c Acco perview		82-3C						Ride Advanced
lerts & Events udit Trail pols b4:5d:50:c6:82:3c 🔺 Acc	ccess Points Configuration Audit	82:3C						Ride Advanced
lerts & Events udit Trail b4:5d:50:c6:82:3c Acco perview evice	ccess Points Configuration Audit							Nide Advanced
lerts & Events udit Trail b4:5d:50:c6:82:3c A reverview evice lents iccurity	ACCESS POINTS / B4:5D:50:C6:8							Ride Advanced
lerts & Events udit Trail bd:5d:50:c6:82:3c perview evice lents scurity se	ACCESS POINTS / B4:5D:50:C6:8							Ride Advanced
erts & Events udit Trail bd:5d:50:c6:82:3c A Acc be-texted by the second sec	ACCESS POINTS / B4:5D:50:C6:8 SYSTEM WLANS RADIO EX Name:	ternal antenna Uplink b4:5d:50xc6:82:3c	DHCP server					Hide Advanced
erts & Events udit Trail b4:5d:50:c6:82:3c A verview everview everview everview everview everview udit Trail	ACCESS POINTS / B4:5D:50:C6:8 SYSTEM WLANS RADIO EX	CTERNAL ANTENNA UPLINK b4:5d:50xc6:82:3c Get IP Address from	DHCP server					Nide Advanced
erts & Events udit Trail b4:5d:50:c6:82:3c A verview everview everview everview everview everview udit Trail ools	ACCESS POINTS / B4:5D:50:C6:8 SYSTEM WLANS RADIO EX Name:	ternal antenna Uplink b4:5d:50xc6:82:3c	DHCP server					Nide Advanced
lerts & Events b4:5d:50:c6:82:3c b4:5d:50:c6:82:3c b everview evice ents security co erts & Events udit Trail sols ain	ACCESS POINTS / B4:5D:50:C6:8 SYSTEM WLANS RADIO EX Name:	CTERNAL ANTENNA UPLINK b4:5d:50xc6:82:3c Get IP Address from	DHCP server					Hide Advanced
erts & Events b4:5d:50:c6:82:3c b4:5d:50:50:50:50:50:50:50:50:50:50:50:50:50:	ACCESS POINTS / B4:5D:50:C6:8 SYSTEM WLANS RADIO EX Name: IP Address For Access Point:	CTERNAL ANTENNA UPLINK b4:5d:50x:6:82:3c Get IP Address from Static	Invalid IP Address					Hide Advanced
erts & Events b4:5d:50:c6:82:3c b4:5d:50:50:50:50:50:50:50:50:50:50:50:50:50:	ACCESS POINTS / B4:5D:50:C6:6 SYSTEM WLANS RADIO EX Name: IP Address For Access Point: IP Address: Netmask:	CTERNAL ANTENNA UPLINK b4:5d:50xc6:82:3c Get IP Address from Static xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx						Hide Advanced
erts & Events b4:5d:50:c6:82:3c b4:5d:50:50:50:50:50:50:50:50:50:50:50:50:50:	ACCESS POINTS / B4:5D:50:C6:3 SYSTEM WLANS RADIO EX Name: IP Address For Access Point: IP Address:	CTERNAL ANTENNA UPLINK b4:5d:50xc6:82:3c Get IP Address from Static xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Invalid IP Address					Hide Advanced
lerts & Events udit Trail b4:5d:50:c6:82:3c A reverview evice lents	ACCESS POINTS / B4:5D:50:C6:6 SYSTEM WLANS RADIO EX Name: IP Address For Access Point: IP Address: Netmask:	CTERNAL ANTENNA UPLINK b4:5d:50xc6:82:3c Get IP Address from Static xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Invalid IP Address Invalid Netmask Invalid IP Address					Hide Advanced
lerts & Events b4:5d:50:c6:82:3c b4:5d:50:c6:82:3c b everview evice ents security co erts & Events udit Trail sols ain	ACCESS POINTS / B4:5D:50:C6:8 SYSTEM WLANS RADIO EX Name: IP Address For Access Point: IP Address: Netmask: Default Gateway:	CTERNAL ANTENNA UPLINK b4:5d:50xc6:82:3c Get IP Address from • Static xxx.xxx.xxx xxx.xxxxxxxxx xxx.xxxxxxxx	Invalid IP Address Invalid Netmask Invalid IP Address					Hide Advanced

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.

ය AOS10	Access Points Switches Gatew				
— Manage ———					
B Overview	ACCESS POINTS (2)				
Devices	Name	1=.	Firmware Version	Recommended Version	٢
🗖 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			UPGRADE ACCESS F		
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 S	iwitches	∰ Gateways						
- Manage						() SET C	OMPLIANCE 👚 UPGRADE ALL		
B Overview	ACCESS POIN	ACCESS POINTS (2)							
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		
	e b4:5d:00000000000000000000000000000000000			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 ————									
Ø Firmware									

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

🛱 AOS10 🤇	Access Points Switches						:=
Manage	Access Points • Online	• Offline	Radios				
B Overview	2 2	0	4				
Devices	ACCESS POINTS (2)						
Clients	Y Device Name	Status	Y IP Address	Y Model	Firmware Version	Y Group	Uptime
Cuests	b4:5d:50:catalana	Online	10.224.254.161	AP-324	10.1.0.2_77953	AOS10	6 Hours 28 Minutes 55 Second
	b4:5d:50:	Online	10.224.254.198	AP-324	10.1.0.2_77953	AOS10	2 Hours 49 Minutes 33 Second
Applications							
AOS10	Access Points Switches Gatew	ays	Clusters				
Aosio	0	ays	Clusters 1				
AOS10	Access Points Switches Gatew Gateways • Online	ays • Offline					
Applications Aosto Anage Overview Devices Clients	Access Points Switches Gatew 2 2 2	ays • Offline	1	Ÿ MAC Firm	nware Version	Ÿ Group	Uptime
AOS10 (Manage	Gateways Online 2 CATEWAYS (2)	o Offline 0	1		wware Version .0.2_77953	Υ Group AOS10	

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

ជ AOS10	Access		ays								:= List	li. Summary	Config
Manage	-	Gateways Clusters 2 1											
Devices													
Clients	GA	ATEWAY CLUSTERS (1)										.↓	\odot
Cuests		Name	Group	AP Tunnel	Clients	Model	Site	Version	Hitless	Failover	Max Gateway Failover		
Applications	~	auto_gwcluster_178_0 (2…	AOS10	4	2	A7005		10.1.0.2_77953	POSSIBL	E	1		
Security		Gateway Name	AP Tunnel	Clients		Model	Site	Version		MAC Address	IP Address		
Analyze		• 7005_AOS10_gwy1	2	1	A	7005		10.1.0.2	77953	00:0b:86:b8:80:d0	192.168.1.24	3	
△ Alerts & Events		• 7005_AOS10_gwy2	2	1	A	7005		10.1.0.2	77953	20:4c:03:1a:2f:b4	192.168.1.242	2	

← auto_gwcluster_1 ⊘	Summary Gateways Tunnels				3 hours
— Manage ————	GATEWAY CLUSTER DETAILS				
BB Overview - Analyze ↓ Alerts & Events ☑ Audit Trail	CLUSTER INFO CLUSTER NAME auto.gwoluster_178_0 MAX GATEWAY FAILURE WITHSTAND COUNT 1	CLUSTER CLIENT CAPACITY 4095 SITE	VLAN MISMATCH Yes	CURRENT LEADER VERSION 10.1.0.2,77953	
	CLIENT CAPACITY	7005_A0510_GWY1	Mar 12, 2021, 16, G	■ + 80% ■ + 40% ■ trvalid	

← auto_gwcluster_1 ⊘ s	Image: Summary Image:							S hours
- Manage G	GATEWAY CLUSTER DETAILS							
器 Overview								
– Analyze –	GATEWAYS (2)							\odot
Alerts & Events	Gateway Name	IP Address	Status	Client Capacity (Active Standby)	Model	Role	Version	
Ļ Alerts & Events	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_AOS10_GWY1	~						
	GATEWAY PEER DETAIL (2)							\odot
	Туре	IP Address	Status	: F	Role	VLAN Mismatch		
	SELF 1	92.168.1.243		м	lember			
	PEER 1	92.168.1.242	Connec	ted Le	eader	1		

auto_gwcluster_1 ⊘	Summary Gateways	 Tunnels						
anage ———	GATEWAY CLUSTER D	ETAILS						
Overview	TUNNEL DOWN	STIMMARY						
alyze	AP Name	▼ IP Address	Last Connected	Last Key Recd By	AP Last Ke	y Recd By Gateway	Reason	Gateway Name
Alerts & Events								
Audit Trail								
					TB			
				No da	ata to display right now			
	GATEWAYS 7005	AOS10_GWY1 🗸						
	TUNNEL DETAILS	S						
	AP Name	▼ IP Address	SSID	Status	Uptime	Last Key Recd By Gateway	Las	it Key Recd By AP
	b4:5d:50:c6:82:3c	10.224.254.198	school	Up	15 Mins 41 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 peer 192.168.1.243 0 self 192.168.1.242 1 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.

Dashboard Monitoring Configuration Administration P ClearPass Portal Users and Privileges Server Manager P Server Configuration	Administration => Server Manager => Se Server Configuration Publisher Server: victory [192.168.				 * Change Clus * Cluster-Wid * Clear Machin * Make Subsc ☆ Make Subsc ☆ Manage Poli ☆ NetFvents 1 ※ NetFvents 1 ※ Set Date & * Virtual IP Se 	e Parameters ne Authentica riber cy Manager Z argets Time	tion Cacl
— Deg Configuration — Docal Shared Folders	# Server Name ▲	Management Port	Data Port	Zone	Cluster Sy	nc Last 9	Sync Tim
- Jucensing	1. victory	(IPv4) 192.168.1.95	-	default	Enabled	-	
Device Insight External Servers	Showing 1-1 of 1			Collect Logs Back Up	Restore Cleanup	Shutdown	Reboo
_	e for all nodes in the cluster: e on Publisher			e for all nodes in the clus	ster:		
Synchronize time with NT	P server	To cl	nange the time zon	e, select your area fro	m the list below:	:	
Primary Server:		Africa	a/Abidjan			^	
	216.239.35.4	Africa	a/Accra				
NTP Server			a/Addis Ababa				
Key ID							
		Africa	a/Algiers				
Key ID Key Value		Africa	a/Algiers a/Asmara				
Key ID		Africa Africa Africa	a/Algiers				
Key ID Key Value		Africa Africa Africa Africa	a/Algiers a/Asmara a/Asmera				
Key ID Key Value Algorithm		Africa Africa Africa Africa Africa Africa Africa	a/Algiers a/Asmara a/Asmera a/Asmera a/Bamako a/Bangui a/Bangui				
Key ID Key Value Algorithm Secondary Server (1):		Africa Africa Africa Africa Africa Africa Africa	a/Algiers a/Asmara a/Asmera a/Bamako a/Bamgui			~	
Key ID Key Value Algorithm Secondary Server (1): NTP Server		Africa Africa Africa Africa Africa Africa	/Algiers b/Asmara b/Asmera b/Bamako b/Bangui b/Banjul b/Bissau	Australia/Melhourne/G	:MT +11:00)	~	
Key ID Key Value Algorithm Secondary Server (1): NTP Server Key ID		Africa Africa Africa Africa Africa Africa	a/Algiers a/Asmara a/Asmera a/Asmera a/Bamako a/Bangui a/Bangui	Australia/Melbourne(G	:MT +11:00)	~	

Save Cancel

Save Cancel

≅Щ Mashboard O	Administration » Server Manage	er » Server Configu	ation - victory					
Monitoring O	Server Configuration	- victory (1	92.168.1.95)					
🖧 Configuration 🔹 📀								
🚰 Administration 📀								
	System Services Control	Service Parame		ng Network FI	IPS			
- De Server Configuration - De Log Configuration - De Local Shared Folders - De Licensing	FQDN: Policy Manager Zone: Enable Performance Monitoring	victory.cle default Display: 🗹 Enable	this server for performa	ance monitoring displa	ау	Manage Polic		
Device Insight	Insight Setting:	🗹 Enable	able Insight Enable as Insight Master Current Master:-					
🗉 📲 External Servers	Enable Ingress Events Processi	ng: Enable	\Box Enable Ingress Events processing on this server					
- Je External Accounts	Master Server in Zone:	Primary r	naster v					
Ecrtificates Jictionaries	Span Port:	None	~					
Agents and Software Updates			IP	v4	IPv6	Action		
- DrGuard Settings - DrGuard Updates - Software Updates	Management Port	IP Address Subnet Mask Default Gateway	25	2.168.1.95 5.255.255.0 2.168.1.249		Configure		
	Data/External Port	IP Address Subnet Mask				Configure		
		Default Gateway						
		Primary	19	2.168.1.250				
	DNS Settings	Secondary	19	2.168.1.130		Configure		
	bho betungs	Tertiary				conigure		
		DNS Caching	Dis	sabled				
	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	etwork FIPS	
Policy Mana	ger Zone:	default	•		Manage Policy Manager Zones
Enable Prof	Join AD Domain			•	
Enable Perf				ig display	
Insight Set	domain:	the controller and the sh	hort (NETBIOS) name for the	ht Master Current Master:-	
DHCP Span	Domain Controller	wlan-dc.wlan.net			
	NetBIOS Name	WLAN		IPv6	Action
	In case of a contro	ller name conflict		1640	Action
Manageme		fied Domain Controller iin Controller returned by nflict	γ DNS query		Configure
Data/Exte	🗹 Use default doma	ain admin user [Administ	trator]		Configure
Dutu/ LAtt	Username				comgato
	Password	••••••			
DNS Settii			Save Cancel		Configure
	10100	•)			
AD Domain	is:	Policy Manager is not	t part of any domain. Join to c	Jomain here.	Join AD Domain
•					

Join AD Domain 🔹	Join AD Domain	0
Adding host to AD domain $z_{m}^{M_{ex}}$	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: [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

Monitoring Authentication Sources - Ariya AD Summary General Authentication Sources - Ariya AD Summary Primary Attributes Name: Ariya AD Description:	
- C Service Templates & Wizards - C Services Name: Ariya AD	
- Services Name: Ariya AD	
Authentication	g attributes

		uration » Authentica	ition » Sou	rces » Add - Ariya AD				
Monitoring	• Auth	nentication So	urces -	Ariya AD				
Configuration	⊙ Sum	mary General	Primary	Attributes				
- 🛱 Service Templates & Wizards						Connectio	n Details	
— 🎲 Services]- 🖴 Authentication	Hostn	ame:	192.168.1	1.250]			
- 🖧 Methods	Conne	ction Security:	None	~]			
	Port:	,-		(For secure connecti	n use 636)			
Q Identity		Server Certificate:		•	tificate for secure connect			
- Single Sign-On (SSO)	Bind D			ator@wlan.net	1			
- 🛱 Local Users	Bind D	IN:		ministrator@example.	e.dc=com)			
- 🛱 Endpoints	Bind P	assword:			1		-,,	
- 🋱 Static Host Lists		OS Domain Name:	WLAN]			
- 🛱 Roles]		7	
- 🛱 Role Mappings	Base [dc=wlan,		1		Search Base Dn	
- TPosture	Searc	h Scope:	SubTree	Search ~				
Enforcement	LDAP	Referrals:		w referrals				
}- ‡ •Network –☆ Network Scan	Bind U	ser:	Allow	bind using user pass	vord			
	User 0	Certificate:	userCertif	ficate]			
Policy Simulation	Alway	s use NetBIOS name	: 🗌 Enabl	le to always use NetB	IOS name instead of the do	omain part in userr	ame for authentication	
		al Character Handling		led O Disabled				
	for LD	AP Query:						
Monitoring	Auther							
Configuration	• Summa	ntication Sourc		iya AD tributes				
- 🛱 Service Templates & Wizards	Summa Specify fil	ry General Printer queries used to fe	nary Att	ributes tication and authorizat				
Service Templates & Wizards	Summa Specify fill	ry General Prin	nary Att	tributes tication and authorizat Attribu	on attributes se Name	Alias		Enabled /
A Service Templates & Wizards C Services Authentication Athentication	Summa Specify fil	ry General Printer queries used to fe	nary Att	ributes tication and authorizat Attribu dn	e Name	UserDI	I	Enabled / -
Gervice Templates & Wizards Gervices Authentication Gervine Methods Gources	Summa Specify fill	ry General Printer queries used to fe	nary Att	tributes tication and authorizat Attribu dn departm	e Name	UserDI Depart	I	Enabled / - -
Service Templates & Wizards Services Authentication Authentication Authentices Q Identity	Summa Specify fill	ry General Printer queries used to fe	nary Att	tication and authorizat Attribu dn departm title	e Name ent	UserDI Depart Title	l ment	Enabled / - - -
Service Templates & Wizards Services Authentication Athends Sources Identity Gingle Sign-On (SSO)	O Summa Specify fill 1.	ry General Prin cer queries used to fe Iter Name	nary Att	iributes tication and authorizat Attribu dn departm title compan	ent	UserDI Depart Title compa	i ment ny	- - -
Service Templates & Wizards Services Authentication Methods Sources Identity Local Users	O Summa Specify fill 1.	ry General Printer queries used to fe	nary Att	ributes tication and authorizat Attribu dn departm title compan member	e Name ent / Df	UserDI Depart Title compa membr	i ment ny	
Service Templates & Wizards Services Authentication Authentication Authods Agroup Sources Identity Cost Single Sign-On (SSO) Local Users Cost Users Cost Discrete	O Summa Specify fill 1.	ry General Prin cer queries used to fe Iter Name	nary Att	ributes tication and authorizat Attribu dn departm title compan member telephoi	ent	UserDI Depart Title compa membi Phone	i ment ny	- - -
	O Summa Specify fill 1.	ry General Prin cer queries used to fe Iter Name	nary Att	ributes tication and authorizat Attribu dn departm title compan member telephoi mail	e Name ent / / Df eNumber	UserDI Depari Title compa membi Phone Email	i ment ny	- - - - - - - -
	O Summa Specify fill 1.	ry General Prin cer queries used to fe Iter Name	nary Att	ributes tication and authorizat Attribu dn departm title compan member telephoi mail displayA	e Name ent / Of eeNumber ame	UserDI Depari Title compa membr Phone Email Name	i ment ny rOf	
Service Templates & Wizards Services Authentication Authentication Official of the services Sources Identity Coll Users Official Operation Static Host Lists Official official Official Role Mappings Posture	Specify fill	y General Prin ter queries used to fe Iter Name	nary Att	ributes tication and authorizati Attribu dn departm title compan member telephor mail displayN account	e Name ent / Of eeNumber ame	UserDI Depari Title compa membr Phone Email Name Accou	i ment ny rof	- - - - - - - -
Service Templates & Wizards Services Authentication Authentication Gurces Identity Gingle Sign-On (SSO) Gingle Si	Specify fill	ry General Prin cer queries used to fe Iter Name	nary Att	ributes tication and authorizat Attribu dn departm title compan member telephon mail displayh account cn	e Name ent / Of eNumber ame Expires	UserDI Depart Title compa memby Phone Email Name Accou	ny rof nt Expires	- - - - - - - - - - - - - - - - - - -
Service Templates & Wizards Services Authentication O Methods Sources Identity O Local Users O Local Users O Roles O Role	Specify fill 1. 2. Gr 3.	y General Prin ter queries used to fe Iter Name	nary Att	ributes tication and authorizat Attribu dn departm title compan member telephon mail displayh account dNSHos	e Name ent	UserDI Depart Title compa membi Phone Email Name Accou Groups HostN	ny rof nt Expires	- - - - - - - -
Services Services Authentication Sources Coloral Users Authentity Authentication Authentication Coloral Users Authentication Coloral Users Authentication Coloral Users Authentication Authentication Authentication Authentication Coloral Users Authentication Coloral Users Authentication Coloral Users Authentication Coloral Users Authentication Authenticatin Authentication Authentication Authentication Au	Specify fill 1. 2. Gr 3.	y General Prin ter queries used to fe Iter Name	nary Att	ributes tication and authorizat Attribu dn departm title compan member telephon mail displayh account dNSHos operatir	e Name ent / / Df heNumber ame Expires Name gSystem	UserDI Depari Title compa membi Phone Email Name Accou Groupi HostN Opera	i ment	- - - - - - - - - - - - - - - - - - -
Services Authentication O Methods Sources Identity Call Users Call Users Call Constraints O Roles	Specify fill 1. 2. Gr 3. M	ry General Prin ter queries used to fe Iter Name	nary Att	ributes Attribu Attribu Attribu A Attribu Att	e Name ent	UserDI Depari Title compa membi Phone Email Name Accou Group; HostN Opera OSSer	ny nof nt Expires ime ingSystem vicePack	- - - - - - - - - - - - - - - - - - -
Services Services Authentication Sources Coloral Users Authentity Authentication Authentication Coloral Users Authentication Coloral Users Authentication Coloral Users Authentication Authentication Authentication Authentication Coloral Users Authentication Coloral Users Authentication Coloral Users Authentication Coloral Users Authentication Authenticatin Authentication Authentication Authentication Au	Specify fill 1. 2. Gr 3. M 4. Or	y General Prin ter queries used to fe Iter Name	mary Att	ributes tication and authorizat Attribu dn departm title compan member telephon mail displayh account dNSHos operatir	e Name ent	UserDI Depari Title compa membr Phone Email Name Accou Group HostN Opera OSSer Onboa	i ment	- - - - - - - - - - - - - - - - - - -

5.2 ClearPass dot1x Service

Here we create a dot1x service for wireless access.

aruba		ClearPass Poli	cy Manager		Menu
Dashboard	Configuration » Services	5			
] Monitoring	 Services 				👍 Add
Configuration	0				🐣 Impo 🌲 Expo
Service Templates & Wizards	This page shows the cu	rrent list and order of services that ClearPass follows	during authentication and authorizatio	ın.	
Authentication	Filter: Name	✓ contains ✓ +	Go Clear Filter		Show 20 v re
- 🛱 Methods - 🎝 Sources	# Order	▲ Name	Туре	Template	Status
Identity	1, 1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	0
- C Single Sign-On (SSO)	2. 2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	0
Local Users	3. 3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	õ
- 🛱 Endpoints	4. 4	[Guest Operator Logins]	Application	Aruba Application Authentication	ø
- 🛱 Static Host Lists	5. 5	[Insight Operator Logins]	Application	Aruba Application Authentication	0
🛱 Roles 🛱 Role Mappings	6. 6	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0
Posture	7. 7	AA Aruba 802.1X Wireless	RADIUS	Aruba 802.1X Wireless	0
me:	AA Aruba 802.1X Wireless				
escription:	To authenticate users to an wireless network via 802.12				
rpe:	Aruba 802.1X Wireless				
atus:	Enabled				
onitor Mode:	Enable to monitor network ad	ccess without enforcement			
ore Options:	Authorization Posture Co	ompliance 🗌 Audit End-hosts 🗌 Profile E	ndpoints 🗌 Accounting Proxy		
		Service	Rule		
atches 🔿 ANY or 🖲 A	LL of the following conditions:				
	Nan	ne	Operator	Value	
Туре					
	NAS	-Port-Type	EQUALS	Wireless-802.11 (19)	自由
		i-Port-Type vice-Type	EQUALS BELONGS_TO	Wireless-802.11 (19) Login-User (1), Framed-User (2), Authenticate-Only (8)	面

EQUALS

school

"school" is the name of the SSID

Aruba-Essid-Name

з.

4.

Radius:Aruba

Click to add.

0)

Ť

Summary	Service	Αι	uthentication	Roles	Enforcement		
Authentication	n Method	s:	[EAP PEAP]		4]	
			[EAP PEAP] [EAP TLS]		r		
						Move Up ↑	
						Move Down ↓	
						Remove	
						View Details	
						Modify	Ĩ
							5
			Select to Add		×	8	
Authentication	n Source	s:	Ariya AD [Active	Directory]	1	·	
						Move Up ↑	
						Move Down 1]
						Remove	
						View Details	
						Modify	
					~		
			Select to Add			~	
Strip Usernam	o Rulos:	1			omma constato	list of rules to stri	p username prefixes or suffixes
· ·		L			omma-separated		p username prenxes or surfixes
Service Certifi	icate:		Select to Add	•	×	/	
Summary Se	rvice Au	uthentica	ation Roles E	nforcement			
Role Mapping Polic		Select-		morecinem	✓ Modify		Add New Role Mapping Policy
	-,-	Select-	-		Role Mapping Poli	ry Dotaile	
Description:		-			Kole Mapping Poil	Ly Details	
Default Role:		-					
Rules Evaluation /	Algorithm:	-					
Conditions	5					Role	
conditions						KOIC	
Summary Service	a Authentic	ation I	Roles Enforcement				
Use Cached Results:	🗌 Use	cached Ro	oles and Posture attribu	tes from previ	ous sessions		
Enforcement Policy:	AA Aru	ba 802.1X V	Wireless Enforcement Policy		 ✓ Modify 		Add New Enforcement Policy
					Enforcement Policy	Details	
Description: Default Profile:		ha 802 1X	Wireless Default Profile				
Rules Evaluation Algori							
Conditions						Enforcement Profile	
1. (Authorization	:Ariya AD:mer	mberOf Co	ONTAINS Staff)			Location	eless Staff Profile, AA Aruba 802.1X Wireless Update Endpoint
2. (Authorization	:Ariya AD:mei	mberOf Co	ONTAINS Student)			AA-Aruba 802.1X Wire Location	eless Student Profile, AA Aruba 802.1X Wireless Update Endpoint
3. (Tips:Role EQ 3. AND (Autho	UALS [Machin	AD:membr	nticated]) erOf CONTAINS Staff)				eless Staff Profile, [Update Endpoint Known]
4 (Tips:Role EQ	UALS [Machir	ne Authen		1)		AA-Aruba 802.1X Wire	eless 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
٠	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	Profile	Attributes			
Profile:					
Name:		AA Aruba	802.1X Wireless Default Profile	802.1X Wireless Default Profile	802.1X Wireless Default Profile
Description:					
Type:		RADIUS			
Action:		Accept			
Device Group	List:	-			
Attributes:					
Туре			Name	Name	Name Value
1. Radius:	Aruba		Aruba-User-Role	Aruba-User-Role =	Aruba-User-Role = Employee

Enforcement Profiles - AA-Aruba 802.1X Wireless Staff Profile

Note: This Enforcement Profile is created by Service Template

Summary	Profile	Attributes		
Profile:				
Name:		AA-Aruba	802.1X Wireless Staff Profile	
Description:				
Type:		RADIUS		
Action:		Accept		
Device Group	List:	-		
Attributes:				
Туре			Name	Value
1. Radius:A	Aruba		Aruba-User-Role	= Staff

Enforcement Profiles - AA-Aruba 802.1X Wireless Student Profile

Note: This Enforcement Profile is created by Service Template

Summary Profil	Attributes
Profile:	
Name:	AA-Aruba 802.1X Wireless Student Profile
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-
Attributes:	
Туре	Name Value
1. Radius:Aruba	Aruba-User-Role = Student
Enforcement Profil	es - AA Aruba 802.1X Wireless Update Endpoint Location
	Note: This Enforcement Profile is created by Service Template
Summary Profile At	ributes
Profile:	
Name:	AA Aruba 802.1X Wireless Update Endpoint Location
Description:	
Туре:	Post_Authentication
Action:	

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}

=

	Configuration - Network - Devices	
Honitoring	Network Devices	🛶 Add
Configuration		& Impor
C Service Templates & Wizards		 Discov
() Services	A Network Access Device (NAD) must belong to the global list of devices in the ClearRuss database in order to connect to ClearRuss.	
Authentication		
- O Methods	File Edit Device Details	Show 2
O Sources		and the
Q Identity	Device SNMP Read Settings SNMP Write Settings CLI Settings OnConnect Enforcement Attributes	
- Q Single Sign-On (SSO)	Name: AOS10-AP	
Ö Local Users	2 IP or Subnet Address: 10.224.225.0/24	
O Endpoints	3 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20 or 2001:db8:a0b:12f0::1)	
Q Static Host Lists	4 Description:	
Q Roles		
O Role Mappings Posture	6	
Enforcement	RADIUS Shared Secret: Verify:	
O Policies	TACACS+ Shared Secret: Verify:	
O Profiles	Vendor Name: Aniba ·	
Network	Enable RADIUS Dynamic Authorization: 🗹 Port: 3799	
O DAVICES	Enable RadSec:	
Device Groups		
O Proxy Targets		
Q Event Sources		
Network Scan		
Policy Simulation	Configuation + Network + Devices	
Dietwork Scan S Policy Simulation Diskboard Honitoring Configuration		<mark>. ∉ Add</mark> & Impor & Expor
) Policy Simulation Dashboard Monitoring Configuration 2) Service Templates & Wizards	Configuration - Network - Divices Network Devices	🧟 Impo 🔔 Expor
Policy Simulation Deckhoord Configuration Service Templates & Wizards Service 1	Condiguation - Network - Devices	🧟 Impo 🚊 Expor
Policy Simulation Decideoard Menitoring Configuration Service Templates & Wizards Services Services	Configuration - Network - Devices Network Devices A Network Access Device (NAD) must being to the global lot of devices in the ClearRess database in order to connect to ClearRess.	🧟 Impo 🚊 Expor
Policy Sinulation Deckhoond Configuration Configuration Services resplates & Witards Services Authorised	Configuration - Network - Divices Network Devices	🏨 Impo 🧟 Expor 🗢 Disco
Pelicy Simulation Decideward Menahoring Configuration Configuration Service Templates & Witzerla Services Q Mittedis Q Sources	Configuration is Internet's Busices Network Devices Attraction Access Device (NKD) must belong to the global bit of devices in the OsarRess database in order to connect to CherRess. Add busice betals O	🏨 Impo 🧟 Expor 🗢 Disco
Policy Simulation Development Readboard Configuration Service Configuration Service Configuration Services Authentication Q Notices Q Notices Q Notices	Complyantium -> Network -> Devices Network Devices Access Device (M40) must being to the global lot of devices in the Charthess database in order to connect to Charthess. File to the Device Steller Device Stell Panel Setting StMP Web Settings CLI Settings OnConnect Enforcement Attributes	🏨 Impo 🧟 Expor 🗢 Disco
Pedicy Simulation Decidioard Healiboring Conformation Service Transfers & Witzerth Service Service Service Service Service Service Service Service Service Service Service Service Service Service Service Service Service Se	Condiguation - Nativerk - Devices Network Devices A factorial Access Device (NO) must belong to the global list of devices in the ClearRess database is order to connect to ClearRess. Factor Edit Device Details Factor ClearRess Access Device (NO) must belong to the global list of devices in the ClearRess database is order to connect to ClearRess. Factor Edit Device Details Factor ClearRess Access Device (NO) must belong to the global list of devices in the ClearRess database is order to connect to ClearRess. Factor Edit Device Details Factor ClearRess Access Device (NO) must belong to the global list of devices in the ClearRess database is order to connect to ClearRess. Factor Edit Device Details Factor ClearRess Access Device (NO) Factor ClearRess Access Device (NO) Factor ClearRess Access	🏨 Impo 🧟 Expor 🗢 Disco
Policy Simulation Deskiloward Configuration Service Templates & Wizards Services Authentication Services Generates G	Configuration - Nation's - Devices Network Devices Antervork Access Device (N40) must belong to the global lot of devices in the Clearthese database in order to connect to Clearthese. File: Device Stell Device Details Device Stelling Stelling Colonect faloroment Attributes None: None: Device Stelling Colonect faloroment Attributes Device Stelling Co	A Impo A Expo Disco
Pacicy Simulation Pacicy Simulation Confluences Sources Transplates & Witzerth Sources	Candiguation + Nativerk + Devices Network Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. A facture Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. A facture Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. A facture Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. A facture Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. Factor Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. Factor Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. Factor Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. Factor Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. Factor Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. Factor Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. Factor Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. Factor Access Device (MO) must belong to the global database in order to connect to ClearRead. Factor Access Device (MO) must belong to the global database in order to connect to ClearRead. Factor Access Device (MO) must belong to the global database in order to connect to ClearRead database in order to connect to clearRe	🏨 Impo 🧟 Expor 🗢 Disco
Pelicy Simulation Development Readbroard Configuration Service Configuration Services Authenticstion Of Mithols Of Mithol	Configuration - Nation's - Devices Network Devices Antervork Access Device (N40) must belong to the global lot of devices in the Clearthese database in order to connect to Clearthese. File: Device Stell Device Details Device Stelling Stelling Colonect faloroment Attributes None: None: Device Stelling Colonect faloroment Attributes Device Stelling Co	🏨 Impo 🧟 Expor 🗢 Disco
Pelicy Simulation Databased Configuration Configuration Service Templates & Witzels Services Authentication Mithods Services Services Services	Candiguation + Nativerk + Devices Network Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. A facture Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. A facture Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. A facture Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. A facture Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. Factor Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. Factor Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. Factor Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. Factor Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. Factor Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. Factor Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. Factor Access Device (MO) must belong to the global list of devices in the ClearRead database in order to connect to ClearRead. Factor Access Device (MO) must belong to the global database in order to connect to ClearRead. Factor Access Device (MO) must belong to the global database in order to connect to ClearRead. Factor Access Device (MO) must belong to the global database in order to connect to ClearRead database in order to connect to clearRe	🏨 Impo 🧟 Expor 🗢 Disco
Pelecy Simulation Deshtheard Configuration Service Templates & Witzerb Service Services Servi	Configuration - Network - Devices Network Device A Network Access Device (M40) must belong to the global dot of devices in the Charthese distates on order to connect to Chartness. For full Device Details For any other destings SMPP Write Settings CL1 Settings Concounced Enforcement Attributes For Subort Address: Descriptor: Descriptor: Descrip	🏨 Impo 🧟 Expor 🗢 Disco
Pedicy Simulation Pedicy Simulation Configuration Configuration	Comparation - Interventik - Dawiese Network Devices A textwork Access Service (WdD) must being to the global lat of devices in the ClearRess distables in order to connect to Cherriess. Reference External Setting State With Settings C1 Setting Outcoment Attributes Partial State Setting State Setting State Setting Outcoment Attributes Partial State Setting State Setting State Setting Outcoment Attributes Partial State Setting State Setting Outcoment Attributes Partial State Setting Outcoment Setting Outcoment Attributes Partial State Setting Outcoment Setting Outcoment Attributes Partial State Setting Outcoment Setting Outcoment Outcoment Outcoment Partial State Setting Outcoment Outcoment Outcoment Partial State Setting Partial Setting Outcoment Outcoment Partial Setting Outcoment Outcoment Partial Setting Outcoment Outcoment Partial Setting Par	🏨 Impo 🧟 Expor 🗢 Disco
Indery Simulation Databased Dat	Configuration: - Roteorik - Devices Network Device A Roteoric Access Device (W40) must belong to the global dist of devices in the Chartess database on order to connect on Chartess. For Efficiency States Secure (W40) must belong to the global dist of devices in the Chartess database on order to connect on Chartess. For Efficiency States Secure (W40) must belong to the global dist of devices in the Chartess database on order to connect to Chartess. For Efficiency States Secure (W40) For States Secure (W40) Fo	🏨 Impo 🧟 Expor 🗢 Disco
Indery Simulation Profession Source Transformed Source Transfor	Comparation - Interventi Devices Network Devices A textwork Access device (WdD) must being to the global for of devices in the ClearRess distates in order to connect to Cherriess. Network Devices A textwork Access device (WdD) must being to the global for of devices in the ClearRess distates in order to connect to Cherries. Network Devices A textwork Access device (WdD) must being to the global for of devices in the ClearRess distates in order to connect to Cherries. Network Devices A textwork Access device (WdD) must being to the global for of devices in the ClearRess distates in order to connect to Cherries. Network Devices Access device (WdD) must being to the global for of devices in the ClearRess distates in order to connect to Cherries. Network Devices Access device (WdD) must being to the global for of devices in the ClearRess distates in order to connect to Cherries. Network Devices Access device (WdD) must being to the global for of devices in the ClearRess distates in order to connect to Cherries. Network Devices Access device (WdD)	≗ Impo € Expo ♥ Disco show []
Pedicy Simulation Devikerson	Configuration - Insteads - Devices Network Device A testeoric Access Device (M40) must belong to the global list of devices in the Clearfless database in order to connect to Clearfless. Network Device A testeoric Access Device (M40) must belong to the global list of devices in the Clearfless database in order to connect to Clearfless. Network Device A testeoric Access Device (M40) must belong to the global list of devices in the Clearfless database in order to connect to Clearfless. Network Device A testeoric Access Device (M40) must belong to the global list of devices in the Clearfless database in order to connect to Clearfless. Network Device A testeoric Testeoric Clearfless Access Werly: Work Tame:	≗ Impo € Expo ♥ Disco show []
Pedicy Simulation	Comparation - Interventi Devices Network Devices A textwork Access device (WdD) must being to the global for of devices in the ClearRess distates in order to connect to Cherriess. Network Devices A textwork Access device (WdD) must being to the global for of devices in the ClearRess distates in order to connect to Cherries. Network Devices A textwork Access device (WdD) must being to the global for of devices in the ClearRess distates in order to connect to Cherries. Network Devices A textwork Access device (WdD) must being to the global for of devices in the ClearRess distates in order to connect to Cherries. Network Devices Access device (WdD) must being to the global for of devices in the ClearRess distates in order to connect to Cherries. Network Devices Access device (WdD) must being to the global for of devices in the ClearRess distates in order to connect to Cherries. Network Devices Access device (WdD) must being to the global for of devices in the ClearRess distates in order to connect to Cherries. Network Devices Access device (WdD)	≗ Impo € Expo ♥ Disco show []
Policy Simulation Devidence Configuration Confi	Configuration - Insteads - Devices Network Device A testeoric Access Device (M40) must belong to the global list of devices in the Clearfless database in order to connect to Clearfless. Network Device A testeoric Access Device (M40) must belong to the global list of devices in the Clearfless database in order to connect to Clearfless. Network Device A testeoric Access Device (M40) must belong to the global list of devices in the Clearfless database in order to connect to Clearfless. Network Device A testeoric Access Device (M40) must belong to the global list of devices in the Clearfless database in order to connect to Clearfless. Network Device A testeoric Testeoric Clearfless Access Werly: Work Tame:	≗ Impo € Expo ♥ Disco show []
Policy Simulation Devaluesraf Conflorente Service: Templates & Wiczeds Service: Templates & Wiczeds Service: Templates & Wiczeds Service: Templates & Wiczeds Service: Service Service: Service	Configuration - Insteads - Devices Network Device A testeoric Access Device (M40) must belong to the global list of devices in the Clearfless database in order to connect to Clearfless. Network Device A testeoric Access Device (M40) must belong to the global list of devices in the Clearfless database in order to connect to Clearfless. Network Device A testeoric Access Device (M40) must belong to the global list of devices in the Clearfless database in order to connect to Clearfless. Network Device A testeoric Access Device (M40) must belong to the global list of devices in the Clearfless database in order to connect to Clearfless. Network Device A testeoric Testeoric Clearfless Access Werly: Work Tame:	≗ Impo € Expo ♥ Disco show []
Policy Simulation Devidencing Configuration Con	Configuration - Insteads - Devices Network Device A testeoric Access Device (M40) must belong to the global list of devices in the Clearfless database in order to connect to Clearfless. Network Device A testeoric Access Device (M40) must belong to the global list of devices in the Clearfless database in order to connect to Clearfless. Network Device A testeoric Access Device (M40) must belong to the global list of devices in the Clearfless database in order to connect to Clearfless. Network Device A testeoric Access Device (M40) must belong to the global list of devices in the Clearfless database in order to connect to Clearfless. Network Device A testeoric Testeoric Clearfless Access Werly: Work Tame:	€ Expo € Expo ♥ Deco show [2
Policy Simulation	Configuration - Insteads - Devices Network Device A testeoric Access Device (M40) must belong to the global list of devices in the Clearfless database in order to connect to Clearfless. Network Device A testeoric Access Device (M40) must belong to the global list of devices in the Clearfless database in order to connect to Clearfless. Network Device A testeoric Access Device (M40) must belong to the global list of devices in the Clearfless database in order to connect to Clearfless. Network Device A testeoric Access Device (M40) must belong to the global list of devices in the Clearfless database in order to connect to Clearfless. Network Device A testeoric Testeoric Clearfless Access Werly: Work Tame:	S Impor

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 Mode Wireless Configuration

법 AOS10 이	Access Points Switches Gateways					Li Summary Config
- Manage	WLANS Access Points Radios Interfac	es Security Services System	Configuration Audit			Hide Advanced
BB Overview						
Devices	Wireless SSIDs					
🗂 Clients	DISPLAY NAME	OPMODE	ACCESS_TYPE	VLAN FORWARDING MODE	ACTIONS	
🔉 Guests						
# Applications						
Security				I F		
- Analyze			T.			
☆ Alerts & Events			No data	to display		
🛛 Audit Trail						
🖏 Tools						
	+ Add SSID					0 SSID(s)
🛱 AOS10 📀	Access Points Switches Gateways				i List	II. Summary Config
- Manage	WLANS Access Points Radios Interfac	es Security Services System	Configuration Audit			Hide Advanced
Overview						
Devices	CREATE A NEW NETWORK					
🗈 Clients	1 General 2 VLANs	3 Security 4 A	ccess (5) Summary			
🔉 Guests	Name (SSID):		school			
Applications	indirite (Sana).		actival.			
Security	> Advanced Settings					
- Analyze						
☆ Alerts & Events						
🛛 Audit Trail						
🖏 Tools					Cance	l 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			
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:	<mark>[192]</mark> ▼	
Reports	> Show Named VLANs		
Maintain			
g Filliwale			
업 AOS10 이	Image: Second	Configuration Audia	List Summary Con
B Overview	Accessions neuros interaces Security Services System	coniguiadon Addic	Hide Advanc
Devices	CREATE A NEW NETWORK		
Clients	1 General 2 VLANs 3 Security 4	Access Summary	
a. Guests			
Applications			
Security	Security Level:	Contraction Descention Destal Open	
Analyze		Enterprise Personal Captive Portal Open	
Alerts & Events			
🛛 Audit Trail	Key Management:	WPA2 Enterprise	
🖏 Tools			
Reports	Primary Server:	ClearPass-GW Y + X	
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	Image: Constraint of the second sec		Eist Summary
Manage	WLANs Access Points Radios Interfaces Security Services System Configuration Audit		Hide Advance
88 Overview	✓ Advanced Settings	-	
Devices			
🗖 Clients	Use Session Key for LEAP:		
 Applications 	Perform MAC authentication before 802.1X:		
 Applications Security 	MAC Authentication Fail-Through:		
- Analyze	Reauth Interval:	0 min V	
♪ Alerts & Events	Denylisting:		
Audit Trail	Max Authentication Failures:	0	
Tools	Enforce DHCP:		
Reports	Use IP for Calling Station ID:		
Firmware			
	Called Station ID Type:	MAC Address	
	Called Station ID Include SSID:		
	Caccounting		
	Accounting:	Use authentication servers	
	✓ 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	
		MAC AUDIESS	
	Called Station ID Include SSID:		
	 Accounting 		
	Accounting:	Use authentication servers	
	Accounting Interval:	1 min	
			i≡ II. 🎯 List Summary Cont
II AOS10	Access Points Switches Gateways		
- Manage	WLANs Access Points Radios Interfaces Security Services System Configuration Audit	-	Hide Advance
Devices	NETWORKS > CONFIGURATION - SCHOOL		
Clients			
🚊 Guests	General VLANs Security Access Summary		

😩 Guests	deneral rearra secondy		
Applications	Access rules		0
Security			Role Based Unrestricted
- Analyze	ROLE		ACCESS RULES FOR SELECTED ROLES
▲ Alerts & Events	NOLL	-	
Audit Trail	school	Î	Allow any to all destinations
🔩 Tools			
🔝 Reports			

And save the configuration.

aruba central 12				0 0 11 8
II AOS10				
- Marage	SUCCESS			Hide Advanced
BB Overview				
Devices	school is Configured Successfully			
Eb Clients	ок			
at. Guests		manine recommending the de		
Applications				
Security				
- 31-1910				

6.2 Tunnelled Mode 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	G Access Po	ints Switches	ے Gateways							SELECTED GROUP TYPE Gateway	List	II. Summary
- Manage	. System	Interface Routin	ng WAN Security	VPN High A	vailability Config Audit							Basic Mode
Overview	Roles	Policies Aliase	s Applications A	oply Policy	Auth Servers Role Assign	ment (AAA Profiles) L2 Authentio	cation L3 A	uthentication Ad	vanced Firewall			
Devices	✓ Au	thentication Serve	rs									
🗖 Clients		Server groups										
😩 Guests		NAME		SER	VERS	FAIL THROUGH	LOAD BALA	NCE	SERVER RULES			=
Applications		school_#1615532	2079504_41#acct_svg	1		**			0			
Security		s <mark>chool_#1615532</mark>	2079504_41#auth_svg	1			-		0			
- Analyze		s <mark>chool_#1615532</mark>	2079504_41#cp_svg	1					0			
Alerts & Events												
Audit Trail												
🖏 Tools 航 Reports		+										
Maintain												
Firmware		All servers										
		NAME		TYPE		IP ADDRESS / HOSTNAME		SERVER GROUP				=
		ClearPass-GW		Radius		192.168.1.95		s <mark>chool_#16155320</mark>	079504_41#acct_sv	vg sch		
				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								
E Dashboard	• Monitoring » Live Monitoring » A	onitoring » Live Monitoring » Access Tracker CCESS Tracker Mar 12, 2021 18:03:31 AEDT								
🗾 Monitoring	Access Tracker маг 12, 2									
Live Monitoring Access Tracker	The Access Tracker page provid									
	[All Requests]	victory (192.168.1.95)		Last 1 day before Too	ay	Edit				
Analysis & Trending				_						
Profiler and Network Scan	Filter: Request ID	✓ contains ✓	+ Go Clear Filte	r -		Show 20 \sim records				
	# Server	Source	Username	Service	Login Status	Request Timestamp 🔹				
	1. 192.168.1.95	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 Details								
Summary Input O	Accounting							
Login Status:	ACCEPT							
Session Identifier:	R0000006-01-604b111f							
Date and Time:	Mar 12, 2021 17:58:39 AEDT							
End-Host Identifier:	A0-88-B4-50-C0-84 (Computer / Windows / Windows)							
Username:	staff1							
Access Device IP/Port:	192.168.1.242							
Access Device Name:	10.224.254.161							
System Posture Status:	UNKNOWN (100)							
	Policies Used -							
Service:	AA Aruba 802.1X Wireless							
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2							
Authentication Source:	AD:192.168.1.250							
Authorization Source:	Ariya AD							
Roles:	[User Authenticated]							
Enforcement Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location. AA-Aruba 802.1X Wireless	~						
I ≤ Showing 1 of 1-7 reco	rds ► ►I Change Status Show Configuration Export Show Logs Clo	se						

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	\odot					
Endpoint:Last Known I	ocation 192.168.1.242:b4:5d:50:c6:82:4a					
Radius:Aruba:Aruba-U	ser-Role Staff					

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

Submit Cancel

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

Request Details							
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							
Utilization	(
Authentication Sessions Details	(

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	Agent O SNMP RADIUS COA O Server Action	
RADIUS CoA Type:	[ArubaOS Wireless - Terminat \vee	

Request Details

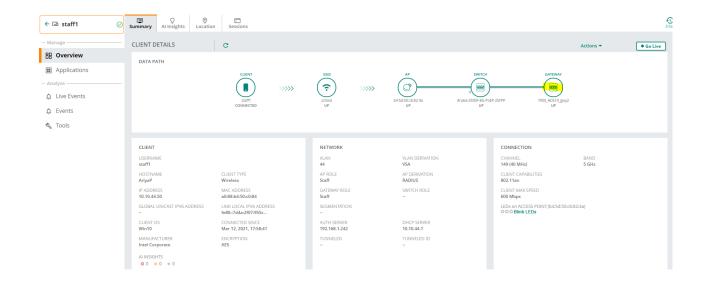
Radius [ArubaOS Wireless - Terminate Session] successful for client a088b450c084.

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.

법 AOS10 이	Clients				3	hours
- Manage	CLIENTS ALL C				244.08 MB (💮 8.04 h	IB ⊕ 236.05 MB)
Devices		onnected		Wired Remote		
🗈 Clients	1 0	1 0 0	0 1	0 0	_	
🚉 Guests						
# Applications	▼ Client Name Status	↓=_ ▼ IP Address V	LAN Connected To	▼ Gateway Role ▼ SSID	/Port Y Health Y	Usage
Security	🗢 staff1 O Connected	10.10.44.50 4	4 b4:5d:50:c6:82:4a	Staff school		244.08 MB



← 🗔 staff1	Visibility				3 hours
— 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	TCP	Network Service	19.9 MB (1.40%)	386 KB	19.5 MB
- 10013	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



← ♀ <mark>7005_AOS10_gwy2</mark> ⊘	Summary Routing Session	Ω AI Insights					3 hours
- Manage						Actions 👻	• Go Live
88 Overview							
Q WAN	DEVICE						
ය. 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 IP ADDRESS 203.63.103.176	
Device	FIRMWARE VERSION 10.1.0.2_77953	POE (DRAW/MAX)	REDUNDANCY PEER	GROUP NAME AOS10	SITE	LABELS	
E Clients	UPTIME	4G/LTE MODEM STATUS	4G/LTE MODEM TYPE	NTP SERVER	CONFIG SYNC STATUS	LAST REBOOT REASON	
Applications	9 hours 53 minutes	-		time2.google.com(Synchronized)	Update Successful 🛈	POE Power Cycle	
Security	CLUSTER NAME auto_gwcluster_178_0						
- Analyze							

← இ 7005_AOS10_gwy2 ⊘	Lū Clients								3 hou
- Manage	CLIENTS GATEWAY	c				244.	08 MB (🕀 8.	04 MB ⊕ 236.05 MB	3)
Q WAN	All O Connectin	ng O Connected O Fai	led Offline Ø Blocked 0 0	d Wireless Wire	d Remote				
윪 LAN									
Device									\odot
🗔 Clients		Status 🚛	Gateway Name	☆ Gateway Role	▼ IP Address	Port	VLAN	Usage	
Applications	🙃 staff1	O Connected	7005_AOS10_gwy2	Staff	10.10.44.50	Tunneled	44	244.08 MB	

Now we'll run a few CLI commands.

b4:5d:50:c6:82:4a# sh ap bss-table

D1100100100102110	on up boo cabie										
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.

```
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#
```

Now, checking the IPSEC tunnels from the AP

b4:5d:50:c6:82:4a# sh ata endpoint							
ATA Endpoint Status							
UUID GRE VLANS HBT(Jiff/Missed/Ser	IP ADDR t/Rcv) INNER I	STATE IP UP TIME(s)	TUN DEV	TUN SPI(OUT/IN)	PORT (SRC/DST)	VALID TIME(s)	TUNNEL TYPE
522d59ab-05d0-43b6-ab49-177e49fb7bb0 1,33,44,192,4094 3999/0/3808/3808		SM_STATE_CONNECTED .254.161 2021-03-13	<mark>tun0</mark> 08:28:59	lad1b900/c6d09100	<mark>4500/4500</mark>	125781	GRE
5bb2c1da-f402-4afa-af39-c09d4aafa946 1,33,44,192,4094 3999/0/3807/3807 Total Endpoints Count: 2 b4:5d:50:c6:82:4a#		SM_STATE_CONNECTED 254.161 2021-03-13	<mark>tun1</mark> 08:29:01	92607100/969£6100	<u>4500/4500</u>	125783	GRE

6.3 Bridge Mode Wireless Configuration

For this mode we have VLAN 22 which will be set aside for Student that will be connecting to this SSID. The LAN switch that the APs are connected to will have VLAN 22 as tagged as well as providing DHCP service for it.

```
1
vlan 22
  name "Student-Bridge-VLAN"
  untagged 2
   tagged 3-4
  ip address 10.10.22.1 255.255.255.0
   dhcp-server
   exit
1
dhcp-server pool "Student-Bridge-VLAN"
  default-router "10.10.22.1"
   dns-server "1.1.1.1"
  lease 00:04:00
  network 10.10.22.0 255.255.255.0
  range 10.10.22.50 10.10.22.59
   exit
!
```

Now, we'll start the configuration of the Bridge mode WLAN.

ជ AOS10	Access Points Switches Gateway	s				List Summary Con
— Manage —	WLANS Access Points Radios In	terfaces Security Services Syste	em Configuration Audit			Hide Advand
B Overview						
Devices	Wireless SSIDs					
🗂 Clients	NAME	SECURITY	ACCESS TYPE	TRAFFIC FORWARDING M	NETWORK ENABLED	
😩 Guests	school	wpa2-aes	Unrestricted	Tunnel	Yes	
Applications	Schoo-Guest	Captive Portal(external)	Role Based	Tunnel	Yes	
Security						
- Analyze						
🏚 Alerts & Events						
Audit Trail						
🖏 Tools	+ Add SSID					2 SSID(s)

P1 40540	6 = 4		i II. 👸 List Summary Config
ជ AOS10 〇	Access Points Switches Gateways		
- Manage	WLANS Access Points Radios Interfaces Security Services System Configurat	ion Audit	Hide Advance
Overview Devices	CREATE A NEW NETWORK		
La Clients	1 General ② VLANs ③ Security ④ Access	3 Summary	
😩 Guests	Name (SSID):	school-Bridge	
Applications	(שובכ).	Schon-Shage	
Security	> Advanced Settings		
— Analyze ————			
Alerts & Events			
Audit Trail			Cancel Next
ជ AOS10	Access Points Switches Gateways		Elst Summary Config
- Manage	WLANS Access Points Radios Interfaces Security Services System Configurat	ion Audit	Hide Advance
B Overview			
Devices	CREATE A NEW NETWORK		
🗖 Clients	1 General 2 VLANs 3 Security 4 Access	(5) Summary	
😩 Guests	Traffic forwarding mode:	Bridge Tunnel Mixed	
Applications	Client VLAN Assignment:	Static Dynamic Native VLAN	
Security			
─ Analyze Alerts & Events			
Audit Trail			
🖏 Tools			Cancel Back Next
다 AOS10	Access Points Switches Gateways		Eist Summary
- Manage	WLANS Access Points Radios Interfaces Security Services System Configuration	tion Audit	Hide Advance
B Overview			
Devices	CREATE A NEW NETWORK		
□ Clients	1 General 2 VLANs 3 Security 4 Access	5 Summary	
😩 Guests			
Applications	Security Level:	0	
Security Analyze		Enterprise Personal Captive Portal Open	
▲ Alerts & Events			
🗷 Audit Trail	Key Management:	WPA2 Enterprise	
🖏 Tools			
🛍 Reports	Primary Server:	ClearPass 🔻 + 🖍 🛢	
- Maintain	- Secondary Server:	Select V +	
Firmware			
	✓ 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:		
	Passpoint Service Profile:	None Manage Passpoint Services	

	Fast Roaming Opportunistic Key Caching (OKC): 802.11r: MDID:	
	802.11k: O	
II AOS10 O	Coss Points Switches Gateways	Cancel Back Next III Summary Can List Summary Can
- Manage	WLANs Access Points Radios Interfaces Security Services System Configuration Audit	Hide Advance
E Overview		
Devices	CREATE A NEW NETWORK	
Clients	1 General 2 VLANs 3 Security 4 Access 3 Summary	
😩 Guests	Access rules	
Applications	Role Based Network Based Unrestricted	
Security	ROLE ACCESS RULES FOR SELECTED ROLES	
- Analyze	school-Bridge	
Alerts & Events	CP-Guest	
Audit Trail	Schoo-Guest	
Tools	default_wired_port_profile	
Reports Maintain	school	
Firmware	wired-SetMeUp	
	+ Add Role 6 Role(5) + Add Rule	1 Rule(s)
	+ Add Role 6 Role(s) + Add Rule	
	+ Add Role 6 Role(s) + Add Rule	1 Rule(s)
	ROLE ASSIGNMENT RULES	
	Default role: school-Bridge	
	+ ADD ROLE ASSIGNMENT	1 Role(s)
	ENFORCE MACHINE AUTHENTICATION:	
		Cancel Back Next

다 AOS10	Access Points Switches Gateways			i≡ II. List Summary Config
— Manage ————	WLANs Access Points Radios Interfaces	Security Services System Configuration Audit		Hide Advance
B Overview				
Devices	CREATE A NEW NETWORK			
Clients	1 General 2 VLANs	3 Security 4 Access 5 Summar	ry	
😩 Guests	Network Summary			
Applications	General		Security	
Security	ESSID	school-Bridge	Security Level	Enterprise
— Analyze ———	Multicast Optimization	Disabled	Auth Server 1	ClearPass
Alerts & Events	Band	all	Key Management	WPA2 Enterprise
🛛 Audit Trail	DTIM Interval	1 beacons	MAC Authentication	Disabled
🖏 Tools	Primary Usage	employee	VLANs	
🔝 Reports	Inactivity Timeout	1000 secs	Traffic forwarding mode	Bridge
- Maintain	Dynamic Multicast OPT	Disabled	Client VLAN Assignment	Native VLAN
ty rinnvare	Content Filtering	Disabled	VLAN	
	Airtime	unlimited	Access	
	Hide SSID	Disabled	Role Assignments For Authenticated Users	Disabled
	Broadcast filtering	arp	ENFORCE MAC AUTH ONLY ROLE	Disabled
	Transmit Rates (legacy Only)	2.4 GHz Min: 1Mbps Max: 54Mbps	ASSIGN PRE-AUTHENTICATION ROLE	Disabled
			ENFORCE MACHINE AUTHENTICATION	Disabled
		5 GHz Min: 6Mbps Max: 54Mbps		
				Cancel Back Finish

Now since we are planning to send back user-role "Student-Bridge" from ClearPass, we'll create a local user at the group level for the AOS10 APs.

ជ AOS10	Access Points		i≣ li. List Summary Config
— Manage —	WLANS Access Points Radios Interfaces	Security Services System Configuration Audit	Hide Advanced
Overview	,		
Devices	> User For Internal Server		
🗖 Clients	∨ Roles		
😩 Guests	Roles	+ Access Rules For Selected Roles	+
Applications	Roles	▲ Assign to VLAN: 22	
Security	Role	 Deny Adult and Pornography 	~ ~ 🖉 🖥
– Analyze	CP-Guest	Deny Gambling	~ ~ 🖉 👕
Alerts & Events	Schoo-Guest	 Allow any to all destinations 	n 🗸 🖉 💼
Audit Trail	Student-Bridge		
🖏 Tools	default_wired_port_profile		
Reports	school		
– Maintain	school-Bridge		
	wired-SetMeUp		
Firmware			

6.4 ClearPass Service Modifications

I am planning to use the same ClearPass dot1x service that was used for tunnelled mode WLAN. So, I'll just need a specific enforcement profile for the bridge mode to send back the user-role and then I'll modify the service.

aruba

ClearPass Policy Manager

Dashboard	Configuration » Enforcem	nent » Profiles » Edit Enforcement Profile - AA-Aruba 8	02.1X Wireless Student-Bridge Profile				
Monitoring O	Enforcement Pro	Enforcement Profiles - AA-Aruba 802.1X Wireless Student-Bridge Profile					
🝰 Configuration 📀	Summary Profile	Attributes					
 — Service Templates & Wizards — Services 	Profile:						
- Authentication	Name:	AA-Aruba 802.1X Wireless Student-Bridge Profile					
⊒- Identity	Description:						
–🛱 Single Sign-On (SSO)	Туре:	RADIUS					
- C Local Users	Action:	Accept					
– 🛱 Endpoints	Device Group List:	-					
– 🗘 Static Host Lists – 🙀 Roles	Attributes:						
- 🗘 Role Mappings	Туре	Name	Value				
🖅 🖶 Posture	1. Radius:Aruba	Aruba-User-Role	= Student-Bridge				
Enforcement Olicies Olicies Olicies Olicies							

Now, I'll just change the service rule for matching the ESSID name.

aruba			Clea	arPas	s Policy Mar	nager			Menu	Ξ
Dashboard O	Configu	uration » Services	» Edit - AA Aruba	802.1X \	Wireless					
Monitoring O	Serv	rices - AA Ar	uba 802.1X	Wirele	SS					
🝰 Configuration 📀	Sumn	mary Service	Authentication	Roles	Enforcement					
 Service Templates & Wizards Services 	Name:		AA Aruba 802.1	(Wireless]				
→ Authentication → Q Identity	Descrip	otion:	To authentic wireless net							
- Single Sign-On (SSO)	Type:		Aruba 802.1X	Wireless	///.]				
 Local Users Endpoints 	Status:	:	Enabled							
- Static Host Lists	Monitor	r Mode:	Enable to m	onitor ne	twork access without	enforceme	nt			
- O Roles	More O)ptions:	Authorization	n 🗆 Pos	sture Compliance 🛛	Audit End-	hosts 🗌 Profile End	points 🗌 Accounting Proxy		
- 🛱 Role Mappings						Service R	ıle			
±- 🖶 Posture	Matche	s 🔿 ANY or 🔘 /	ALL of the followin	g conditio	ons:					
∃- 🛎 Enforcement	т	уре		Name		C	perator	Value		
- 🗘 Policies	1. R	adius:IETF		NAS-Po	rt-Type	E	QUALS	Wireless-802.11 (19)	E	à î
- 🛱 Profiles 🖅 🖶 Network	2. R	adius:IETF		Service	-Туре	В	ELONGS_TO	Login-User (1), Framed-Us (2), Authenticate-Only (8)	er 👔	b t
– 🗘 Network Scan	3. R	adius:Aruba		Aruba-E	ssid-Name	C	ONTAINS	school	E	à t
- 🛱 Policy Simulation	4 . C	lick to add								

And add a logic in the enforcement policy.

aruba	ClearPass Policy Manager	Menu
Dashboard 0	Configuration » Services » Edit - AA Aruba 802.1X Wireless	
Monitoring O	Services - AA Aruba 802.1X Wireless	
Configuration 📀	Summary Service Authentication Roles Enforcement	
 Service Templates & Wizards Services Authentication 	Use Cached Results: Use cached Roles and Posture attributes from previo Enforcement Policy: AA Aruba 802.1X Wireless Enforcement Policy	us sessions v Modify Add New Enforcement Police
2 Identity	Enforcement Pol	icy Details
Gingle Sign-On (SSO) Good Local Users Good Local Users Good Local Lists Good Lists	Description: Default Profile: AA Aruba 802.1X Wireless Default Profile Rules Evaluation Algorithm: first-applicable	·
– C Roles	Conditions	Enforcement Profiles
A Role Mappings Posture Enforcement A Policies Profiles	1. (Authorization:Ariya AD:Nested Groups EQUALS test-users) 2. (Authorization:Ariya AD:memberOf CONTAINS Staff) 3. (Authorization:Ariya AD:memberOf CONTAINS Student) AND (Connection:SSID CONTAINS Bridge)	AA-Aruba 802.1X Wireless Student Profile AA-Aruba 802.1X Wireless Staff Profile, AA Aruba 802.1X Wireless Update Endpoint Location AA-Aruba 802.1X Wireless Student-Bridge Profile, AA Aruba 802.1X Wireless Update Endpoint Location AA-Aruba 802.1X Wireless Student Profile, AA Aruba 802.1X Wireles
 → Network → Network Scan → Policy Simulation 	4. (Authorization:Ariya AD:memberOf CONTAINS Student) 5. (Tips:Role EQUALS [Machine Authenticated]) AND (Authorization:Ariya AD:memberOf CONTAINS Staff) 6. (Tips:Role EQUALS [Machine Authenticated]) AND (Authorization:Ariya AD:memberOf CONTAINS Studen)	Update Endpoint Location AA-Aruba 802.1X Wireless Staff Profile, [Update Endpoint Known] AA-Aruba 802.1X Wireless Student Profile, [Update Endpoint Knowr
~	Back to Services	Disable Copy Save Cancel

6.5 Bridge Mode Wireless dot1x Testing

Here are the access tracker screenshots.

Summary Input O	Accounting			
Login Status:	ACCEPT	^		
Session Identifier:	R000000c-01-60e299cb			
Date and Time:	Jul 05, 2021 15:34:04 AEST			
End-Host Identifier:	F0-D5-BF-4B-67-11			
Username:	student1			
Access Device IP/Port:	10.10.55.11			
Access Device Name:	10.10.55.11			
System Posture Status:	UNKNOWN (100)			
	Policies Used -			
Service:	AA Aruba 802.1X Wireless			
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2			
Authentication Source:	AD:192.168.1.250			
Authorization Source:	Ariya AD			
Roles:	Student, [User Authenticated]			
Enforcement Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless	\checkmark		
I < Showing 1 of 1-13 red	cords ► ► Change Status Show Configuration Export Show Logs Close	se		

Note that the RADIUS authentication is coming directly for the AP's IP addresses.

	Summary	Input	Output	Accounting		
1	Username:		student1			^
I	End-Host Ide	ntifier:	F0-D5-BF-4	4B-67-11		
,	Access Device	e IP/Port:	10.10.55.1	1		
	RADIUS Req	uest			⊘	
	Radius:Arul	ba:Aruba-	AP-Group	AOS10		
	Radius:Arul	ba:Aruba-	Essid-Name	school-Bridge		
	Radius:Arul	ba:Aruba-	Location-Id	b4:5d:50:c6:82:3c		
	Radius:IETF	:Called-S	itation-Id	b45d50c6823c		
	Radius:IETF	-:Calling-	Station-Id	f0d5bf4b6711		
	Radius:IETF	F:Framed-	MTU	768		
	Radius:IETF	:NAS-Ide	ntifier	10.10.55.11		
	Radius:IETF	-:NAS-IP-	Address	10.10.55.11		
	Radius:IETF	:NAS-Por	t	0		
	Radius:IETF	:NAS-Por	t-Type	19		
L	D 11 TETE		÷			\sim
I	 Showing 	1 of 1-13	records > >	Change Status Show Configuration Export Show Logs	Clo	ose

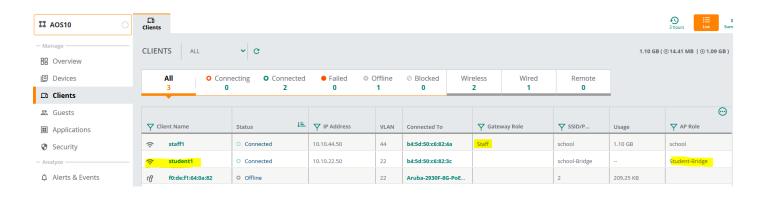
Request Details

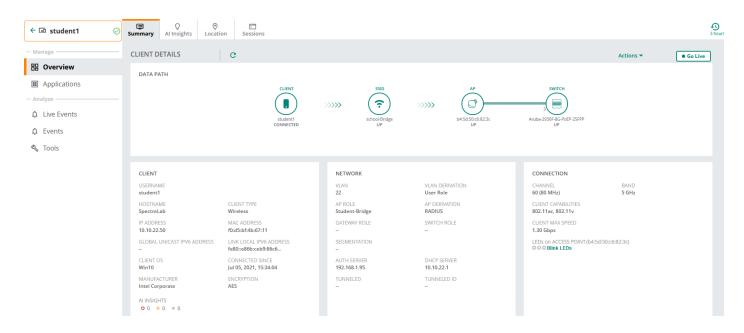
Summary	Input	Output	Accounting	
Enforcement Profiles: AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless Update 80.1X Wireless Update 80.1X Wireless Update 80.1X Wireless Update 80.1X Wireless 100.1X				
System Posture Status: UNKNOWN (100)				
Audit Posture Status: UNKNO			/N (100)	
RADIUS Resp	onse		G	
Endpoint:La	st Known I	Location	10.10.55.11:b4:5d:50:c6:82:3c	
Radius:Arub	a:Aruba-U	Jser-Role	Student-Bridge	

I ◄ Showing 1 of 1-13 records ► ►	Change Status Show Configuration Export Show Logs Close
Summary Input Output	accounting
Account Session ID:	B45D50E823D2-F0D5BF4B6711-60E299CC-23AA
Start Timestamp:	Jul 05, 2021 15:34:04 AEST
End Timestamp:	Still Active
Status:	Active
Termination Cause:	-
Service Type:	-
Number of Authentication Sessions:	1
Network Details	•
Utilization	۲
Authentication Sessions Details	۲

 Image: Showing 1 of 1-13 records >>>
 Change Status
 Show Configuration
 Export
 Show Logs
 Close

Checking Aruba Central side.





← 🗔 student1	⊘ Â Events	s		4 31
Manage		EVENTS 40	CED FILTERING	
∴ Live Events		EVENTS (40)		
ti Events		Y Occurred On ↓	Event Type	Description
🔦 Tools		Jul 5, 2021, 15:34:45	Client Association Success	Associated successfully to SSID school-Bridge on channel 60E of AP hostname b4:5d:50:c6:
	>	Jul 5, 2021, 15:34:04	Client DHCP Acknowledged	DHCP acknowledgement received from DHCP server 10.10.22.1 on BSSID b4:5d:50:e8:23:d
	>	Jul 5, 2021, 15:28:04	Client 802.11 De-authentication from Client	De-authentication sent to BSSID b4:5d:50:e8:23:d2 on channel 60E of AP hostname b4:5d:5
	>	Jul 5, 2021, 15:28:00	Client 802.1x Radius Timeout	802.1x Radius Timeout occurred for client f0:d5:bf:4b:67:11 on BSSID b4:5d:50:e8:23:d2 on
		Jul 5, 2021, 15:28:00	Client EAP Timeout from Client	EAP response to BSSID b4:5d:50:e8:23:d2 on channel 60E of AP hostname b4:5d:50:c6:82:3
		Jul 5, 2021, 15:22:45	Client Association Success	Associated successfully to SSID school-Bridge on channel 60E of AP hostname b4:50:c6:
		Jul 5, 2021, 15:22:14	Client Match Steer	Client match attempted a BAND STEER using 11v MODE from radio BSSID b4:5d:50:e8:23:c

6.6 Mixed Mode Wireless Configuration

In this mode for the same SSID allows both bridging of the user traffic as well as tunnelling it to a cluster of gateways based on the attributes it receives by the RADIUS server. It should be noted that currently mixed Mode SSID is only supported for 802.1X authentication.

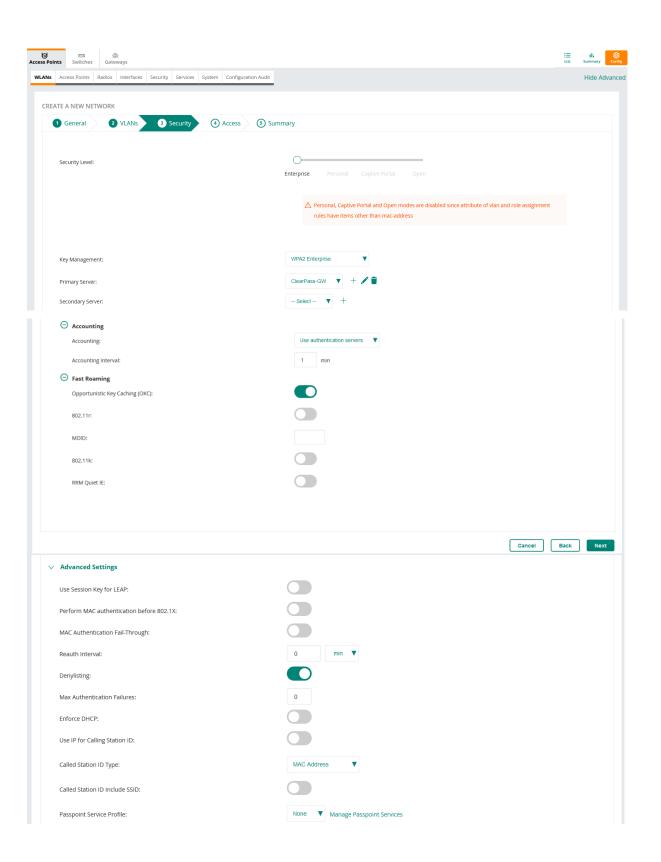
We'll be making use of Server Derivation Rule (SDR) to decide which user role that ClearPass sends will be bridged.

In mixed mode the default VLAN is a tunnel VLAN. So, a bridged mode Rule must be defined.

Now we'll start the configuration of the mixed mode WLAN.

Central		Q				۹	ሳ 🛛 👪 🖁
다 AOS10	Access Points Switches Gateways					List	II. Summary Config
- Manage	WLANS Access Points Radios Inte	erfaces Security Services System	Configuration Audit				Hide Advanced
Overview							
Devices	Wireless SSIDs						
🗖 Clients	NAME	SECURITY	ACCESS TYPE	TRAFFIC FORWARDING MODE	NETWORK ENABLED		
a. Guests	school 🖬	wpa2-aes	Unrestricted	Tunnel	Yes		
Applications	Schoo-Guest	Captive Portal(external)	Role Based	Tunnel	Yes		
Security	school-Bridge	wpa2-aes	Unrestricted	Bridge	Yes		
- Analyze							
Alerts & Events							
Audit Trail							
🖏 Tools							
	+ Add SSID						3 SSID(s)
Access Points Switches	இ Gateways					List	ii. Summary Config
WLANs Access Points I	Radios Interfaces Security Service	s System Configuration Audit					Hide Advanced
CREATE A NEW NET	WORK						
1 General	2 VLANs 3 Security	4 Access 5 Sur	nmary				
Name (SSID):			school-Mixed				
> Advanced Set	ttings						
						Cancel	Next

Coss Points Switches Gateways		i List	II. Summary Config
WLANS Access Points Radios Interfaces Security Services System Configuration Audit			Hide Advanced
Traffic forwarding mode:	Bridge Tunnel Mixed		
Primary Gateway Cluster:	AOS10 auto_gwcluster_176_0		
Secondary Gateway Cluster:	None		
Client VLAN Assignment:	• Dynamic		
VLAN Assignment Rules Default VLAN: 1			
Default VLAN. 1			
- Add Rule	1 Rule(s)		
O Catagoria		List	ili 🐯 Summary Config
Access Points Switches Gateways WLANS Access EDIT VI AN ASSIGNMENT RUILE			Hide Advanced
	×		nice novanced
Attribute: Operator: String: VLAN At Aruba-User-Role V equals V Executive-Bridge	VLAN Type: VLAN: Bridge V 22		
Defau			
II If			
III II			
Cancel	ок		
	3 Rule(s)		
+ Add Rule	(בקוואר כ		
Access Points Switches Gateways		List	II. Summary Config
WLANS Access EDIT VLAN ASSIGNMENT RULE	×		Hide Advanced
Attribute: Operator: String:	VLAN Type: VLAN:		
VLAN A: Aruba-User-Role V equals V Contractor	Tunnel ▼ 44(44) × ▼		
Defau III If			
II If			
Cancel	ок		
+ Add Rule	3 Rule(s)		
			_
Image: Constant Sector Points Image: Sector Points		List	t Summary Config
WLANS Access Points Radios Interfaces Security Services System Configuration Audit			Hide Advance
1 General 2 VLANs 3 Security 4 Access 5 St	ummary		
Traffic forwarding mode:	Bridge Tunnel Mixed		
Primary Gateway Cluster:	AOS10:auto_gwcluster_178_0		
Secondary Gateway Cluster:	None		
Client VLAN Assignment:			
	Dynamic		
VLAN Assignment Rules	Dynamic		
	Dynamic		
VLAN Assignment Rules	Dynamic		



Cess Points Switches Gateways		List	Li 🚱 Summary Config
MLANs Access Points Radios Interfaces Security Services	System Configuration Audit		Hide Advanced
CREATE A NEW NETWORK			
1 General 2 VLANs 3 Security	Access Summary		
Access rules	0		
	Role Based Network Based Unrestricted		
ROLE	ACCESS RULES FOR SELECTED ROLES		
School-Mixed	Allow any to all destinations		
CP-Guest			
Employee			
Schoo-Guest			
school			
+ Add Role	5 Role(s) + Add Rule		1 Rule(s)
		List	IL E
ccess Points Switches Gateways		Ust	
WLANS Access ADD ROLE	×		Hide Advanc
CREATE A N Role:	Contractor		
1 Gen	Cancel		
Access ru			
	Role Based Network Based Unrestricted		
Image: Switches Gateways		List	LL 👸 Summary Config
Access ADD ROLE	×		Hide Advanced
	Unrestricted		
Role:	xecutive-Bridge		
Contrac			
School-I	Cancel		
CP-Guest			
Employee			
Schoo-Guest			
school			
+ Add Role	6 Role(s) + Add Rule		1 Rule(s)

ල් Access Points	E Swit	ා ඉඩ cches Gateways				th mmary	Config
WLANS A	ccess	NEW ROLE ASSIGNMENT RULE			>	< A	dvanced
+	Add Re	Attribute:	Operator:			∋(s)
	DLE AS efault	Augeoscience		Cancel	ave		
+	ADD ROL	E ASSIGNMENT			1	Role(s)
ENFO	ORCE MA	ACHINE AUTHENTICATION:					

Points Switches Gateways		List	llı Summary
Is Access Points Radios Interfaces Security Security	ervices System Configuration Audit		Hide Adv
REATE A NEW NETWORK			
1 General 2 VLANs 3 Secu	urity Access ③ Summary		
Access rules	0		
	Role Based Network Based Unrestricted		
ROLE	ACCESS RULES FOR SELECTED ROLES		
Executive-Bridge	Allow any to all destinations		
Contractor			
School-Mixed			
CP-Guest			
Employee			
Schoo-Guest			
school			
+ Add Role	7 Role(s) + Add Rule		1 Rule(s)
ROLE ASSIGNMENT RULES			
Default role: School-Mixed			
			1 Role(s)
ENFORCE MACHINE AUTHENTICATION:			
Points Switches Gateways		List	II. Summary
Is Access Points Radios Interfaces Security Se	rvices System Configuration Audit		Hide Adva
EATE A NEW NETWORK			
EATE A NEW NETWORK General VLANs Secu	arity Access (3) Summary		
	arity Access 3 Summary		
1 General 2 VLANs 3 Secu	rifty Access ③ Summary Role Based Network Based Unrestricted		
1 General 2 VLANs 3 Secu	0		
General Z VLANS Secu	Role Based Network Based Unrestricted		
General Q VLANs 3 Secu Access rules ROLE	Role Based Network Based Unrestricted ACCESS RULES FOR SELECTED ROLES		
General 2 VLANs 3 Secu Access rules ROLE Contractor	Role Based Network Based Unrestricted ACCESS RULES FOR SELECTED ROLES		
General 2 VLANs 3 Secu Access rules ROLE Contractor School-Mixed	Role Based Network Based Unrestricted ACCESS RULES FOR SELECTED ROLES		
General 2 VLANs 3 Secu Access rules ROLE Contractor School-Mixed CP-Guest	Role Based Network Based Unrestricted ACCESS RULES FOR SELECTED ROLES		
General 2 VLANs 3 Secu Access rules ROLE Contractor School-Mixed CP-Guest Employee	Role Based Network Based Unrestricted ACCESS RULES FOR SELECTED ROLES		
General 2 VLANs 3 Secu Access rules Image: Security of the secur	Role Based Network Based Unrestricted ACCESS RULES FOR SELECTED ROLES		
General 2 VLANs 3 Secu Access rules Image: Security of the secur	Role Based Network Based Unrestricted ACCESS RULES FOR SELECTED ROLES		1 Rule(s)
Access rules ROLE Contractor School-Mixed CP-Guest Employee School-Guest school	Role Based Network Based Unrestricted ACCESS RULES FOR SELECTED ROLES IIII • Allow any to all destinations		1 Rule(s)
General 2 VLANs 3 Secu Access rules Image: Contractor Image: Contractor School-Mixed Image: Contractor Image: Contractor School-Guest Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor School-Mixed Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contrator C	Role Based Network Based Unrestricted ACCESS RULES FOR SELECTED ROLES Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Compa		1 Rule(s)
General 2 VLANs 3 Secu Access rules Image: Contractor Image: Contractor School-Mixed Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor School-Mixed Image: Contractor Image: Contractor School-Mixed Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor Image: Contractor	Role Based Network Based Unrestricted ACCESS RULES FOR SELECTED ROLES Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Compa		1 Rule(s)
General VLANS Secu Access rules ROLE Contractor School-Mixed CP-Guest Employee Schoo-Guest school + Add Role ROLE ASSIGNMENT RULES	Role Based Network Based Unrestricted ACCESS RULES FOR SELECTED ROLES Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Compa		1 Rule(s)
General VLANS Secu	Role Based Network Based Unrestricted ACCESS RULES FOR SELECTED ROLES Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Compa		
General 2 VLANS 3 Secu Access rules 3 Secu ROLE	Role Based Network Based Unrestricted ACCESS RULES FOR SELECTED ROLES Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Compa	:= UM	
General 2 VLANS 3 Secu Access rules 3 Secu ROLE Contractor 5 School-Mixed 7 6 CP-Guest Employee 5 School-Guest 5 5 School 1 1 + Add Role 1 1 ROLE ASSIGNMENT RULES 1 Assign role returned as value of Aruba-User-Rol Default role: School-Mixed 1 1 Points Switches Gateways	Role Based Network Based Unrestricted ACCESS RULES FOR SELECTED ROLES Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Compa	:= LM	il. Summary
General 2 VLANs 3 Secu Access rules 3 Secu ROLE Contractor 5 School-Mixed CP-Guest 6 CP-Guest Employee 5 School-Guest 5 5 School 1 1 + Add Role 1 1 ROLE ASSIGNMENT RULES 1 1 Basign role returned as value of Aruba-User-Roli 1 Default role: School-Mixed 1 Points Switches Gateways	Role Based Network Based Unrestricted ACCESS RULES FOR SELECTED ROLES Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Comparison of the structure Image: Compa	in the second seco	II. Summary
Contractor	Role Based Network Based Unrestricted ACCESS RULES FOR SELECTED ROLES Image: Im	:== LM	II. Summary
Contractor	Role Based Unrestricted ACCESS RULES FOR SELECTED ROLES Image: Imag	:== List	II, Summary
Contractor Contractor Contractor Contractor Contractor Contractor CP-Guest CP-Guest Employee School-Mixed CP-Guest School + Add Role ROLE ASSIGNMENT RULES ROLE ASSIGNMENT RULE Add Role ROLE ASSIGNMENT RULE ROLE ASSIGNMENT RULE ROLE ASS	Role Based Network Based ACCESS RULES FOR SELECTED ROLES Image: Comparison of the comparison		ıl. Summary X Adva
Contractor Contractor Contractor School-Mixed CP-Guest Employee School-Mixed CP-Guest School + Add Role ROLE ASSIGNMENT RULES Access NEW ROLE ASSIGNMENT RULE Attribute: Attr	Role Based Unrestricted ACCESS RULES FOR SELECTED ROLES Image: Imag	i Lus Save	ıl. Summary X Adva
General VLANS Secu Access rules ROLE Contractor School-Mixed CP-Guest Employee School-Mixed CP-Guest School + Add Role ROLE ASSIGNMENT RULES Access NEW ROLE ASSIGNMENT RULE Attribute: At	Role Based Network Based ACCESS RULES FOR SELECTED ROLES Image: Comparison of the comparison		il. Summary X Adva
General VLANS Secu Access rules ROLE Contractor School-Mixed CP-Guest Employee School-Mixed CP-Guest School + Add Role ROLE ASSIGNMENT RULES Access NEW ROLE ASSIGNMENT RULE Attribute: At	Role Based Network Based ACCESS RULES FOR SELECTED ROLES Image: Comparison of the comparison		il. Summary X Adva
Contractor Contractor Contractor School-Mixed CP-Guest Employee School-Mixed CP-Guest School + Add Role ROLE ASSIGNMENT RULES Access NEW ROLE ASSIGNMENT RULE Attribute: Attr	Role Based Network Based ACCESS RULES FOR SELECTED ROLES Image: Comparison of the comparison		ıl. Summary X Adva
Contractor Contractor Contractor Contractor Contractor Contractor Contractor CP-Guest Employee School-Mixed CP-Guest School C	Role Based Network Based ACCESS RULES FOR SELECTED ROLES Image: Comparison of the comparison		ıl. Sunmary X Adv
Contractor Contractor Contractor Contractor Contractor Contractor Contractor CP-Guest Employee School-Mixed CP-Guest School C	Role Based Network Based ACCESS RULES FOR SELECTED ROLES Image: Comparison of the comparison		il. Summary X Adva

ල් Access Po	ints Switches	ුමූ Gateways							i List	II. Summary Config
WLANS	Access Points F	Radios Interfa	es Security	Services	System	Configuration Audit				Hide Advanced
	DTIM Interval			1 bea	icons		MAC Authentication	Disabled		
	Primary Usage			emplo	yee		VLANs			
	Inactivity Timeout			1000	secs		Traffic forwarding mode	Mixed		
	Dynamic Multicast	t OPT		Disab	ed		Primary Gateway Cluster	AOS10:auto_gwcluster_178_0		
	Content Filtering			Disabl	ed		Client VLAN Assignment	Dynamic		
	Airtime			unlim	ted		VLAN	1		
	Hide SSID			Disab	ed		Access			
	Broadcast filtering	ł		arp			Role Assignments For Authenticated Users	Enabled		
	Transmit Rates (le	gacy Only)		2.4 GI		n: 1Mbps x: 54Mbps	ENFORCE MAC AUTH ONLY ROLE	Disabled		
							ASSIGN PRE-AUTHENTICATION ROLE	Disabled		
				5 GHz		n: 6Mbps x: 54Mbps	ENFORCE MACHINE AUTHENTICATION	Disabled		
								Cancel	Back	Finish

6.7 ClearPass Service Modifications

We'll use the same ClearPass dot1x service that was used for tunnelled and bridge mode WLAN. So, I'll just need a specific enforcement profile for the mixed mode to send back the user-role and then I'll modify the service.

aruba		ClearPass Policy Mana	iger						
Dashboard	Configuration » Enforcement » Profiles » Edit Enforcement Profile - AA-Aruba 802.1X Wireless Contractor Profile								
Monitoring	Enforcement F	Enforcement Profiles - AA-Aruba 802.1X Wireless Contractor Profile							
😤 Configuration	Summary Profile	Attributes							
- 🗘 Service Templates & Wizards	Profile:								
- Services	Name:	AA-Aruba 802.1X Wireless Contractor Profile							
- Authentication		AA-Aruba 802.1X Wireless Contractor Prome							
Methods	Description:	DADTIC							
- ☆ Sources - ♀ Identity	Туре:	RADIUS							
Single Sign-On (SSO)	Action:	Accept							
Local Users	Device Group List:	Device Group List: -							
- C Endpoints	Attributes:								
- Static Host Lists	Туре	Name	Value						
- 🛱 Roles	1. Radius:Aruba	Aruba-User-Role	= Contractor						
Role Mappings									
±- 🖶 Posture									
🖃 💐 Enforcement									
- 🛱 Policies									
Profiles									
*									
aruba		ClearPass Policy Manager	•						
Dashboard	Configuration » Enforcer	nent » Profiles » Edit Enforcement Profile - AA-Aruba 802.1X V	Vireless Executive-Bridge Profile						
Monitoring C	Enforcement Pro	files - AA-Aruba 802.1X Wireless Executiv	ve-Bridge Profile						
🖧 Configuration 🖸		Attributes	5						
—🎲 Service Templates & Wizards	Profile:								
- 🗘 Services									
- 🖴 Authentication	Name:	AA-Aruba 802.1X Wireless Executive-Bridge Profile							
—🔅 Methods	Description:								
- Sources	Туре:	RADIUS							
- Q Identity	Action:	Accept							
Single Sign-On (SSO)	Device Group List:	-							
– 🛱 Local Users – 🛱 Endpoints	Attributes:								
Static Host Lists	Туре	Name	Value						
- C Roles	1. Radius:Aruba	Aruba-User-Role	= Executive-Bridge						
Role Mappings	1. Radius.Araba	Alubu ösel köle	Executive bridge						
→ + + + + + + + + + + + + + + + + + + +									
⇒ ∰ Enforcement									
- Policies									
Profiles									
The Provinces	1								

And now we'll add a logic in the enforcement policy.

aruba		ClearPass Policy Manag	ger	Menu 🔜
Dashboard O	Configuration » Services » E	dit - AA Aruba 802.1X Wireless		
🐼 Monitoring 🔹 🔍	Services - AA Arub	a 802.1X Wireless		
🝰 Configuration 📀	Summary Service A	uthentication Roles Enforcement		
- Carl Service Templates & Wizards	Use Cached Results:	Use cached Roles and Posture attributes from previ	ous sessions	
- 🎲 Services	Enforcement Policy:	AA Aruba 802.1X Wireless Enforcement Policy	✓ Modify	Add New Enforcement Policy
- Q Methods		Enforcem	ent Policy Details	
- O Sources	Description:			
- Q Identity	Default Profile:	AA Aruba 802.1X Wireless Default Profile		
- 🎝 Single Sign-On (SSO) - 🖧 Local Users	Rules Evaluation Algorithm:	first-applicable		
- C Endpoints	Conditions		Enforcement Profiles	
- 🛱 Static Host Lists	1. (Authorization:Ariya	AD:Nested Groups EQUALS test-users)	AA-Aruba 802.1X Wireless Student Prof	ile
– 🛱 Roles – 🛱 Role Mappings	2. (Authorization:Ariya	AD:memberOf CONTAINS Staff)	AA-Aruba 802.1X Wireless Staff Profile, Endpoint Location	AA Aruba 802.1X Wireless Update
⊕ 🖶 Posture		AD:memberOf CONTAINS Student) SSID CONTAINS Bridge)	AA-Aruba 802.1X Wireless Student-Brid Wireless Update Endpoint Location	ge Profile, AA Aruba 802.1X
Enforcement	(Authorization:Ariya	AD:memberOf CONTAINS Contractor) SSID CONTAINS Mixed)	AA-Aruba 802.1X Wireless <mark>Contractor P</mark> Update Endpoint Location	rofile, AA Aruba 802.1X Wireless
- Profiles	(Authorization:Ariya	AD:memberOf CONTAINS Executive) SSID CONTAINS Mixed)	AA-Aruba 802.1X Wireless <mark>Executive-Br</mark> Wireless Update Endpoint Location	<mark>idge Profile,</mark> AA Aruba 802.1X
Network Scan		AD:memberOf CONTAINS Student)	AA-Aruba 802.1X Wireless Student Prof Update Endpoint Location	ile, AA Aruba 802.1X Wireless
-‡ Policy Simulation		[Machine Authenticated]) n:Ariya AD:memberOf CONTAINS Staff)	AA-Aruba 802.1X Wireless Staff Profile,	[Update Endpoint Known]
	8 (Tips:Role EQUALS	[Machine Authenticated]) n:Ariya AD:memberOf CONTAINS Studen)	AA-Aruba 802.1X Wireless Student Prof	ile, [Update Endpoint Known]

Now we are ready to test it out.

6.8 Mixed Mode Wireless dot1x Testing

The contractor credentials should get tunnelled to the gateway clusters and should get VLAN 44 while the Executive credentials should get bridged to VLAN 22.

Here are the access tracker screenshots.

equest Details Summary		Output Accounting
Login Status.	Input	ACCEP
Session Identi	fier:	R0000006-01-60e8f20f
Date and Time	:	Jul 10, 2021 11:04:15 AEST
End-Host Iden	tifier:	F0-D5-BF-4B-67-11
Jsername:		contractor1
Access Device	IP/Port:	192.168.1.242
Access Device	Name:	10.10.55.11
System Postur	e Status:	UNKNOWN (100)
		Policies Used -
Service:		AA Aruba 802.1X Wireless
Authentication	Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication	Source:	AD:192.168.1.250
Authorization S	Source:	Ariya AD
Roles:		Contractors, [User Authenticated]
Enforcement P	rofiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless Contractor Profile
🛾 🖣 Showing 1	of 1-15 re	ecords ► ► Change Status Show Configuration Export Show Logs Close
Request Details	5	
Summary	Input	Output Accounting
Enforcement I	Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless Contractor Profile
System Postu	re Status:	UNKNOWN (100)
Audit Posture	Status:	UNKNOWN (100)
RADIUS Resp	00000	(

Looking at the Clients from Aruba Central we see that both clients are in the respective VLANs.

Endpoint:Last Known Location 192.168.1.242:b4:5d:50:c6:82:3c

Radius:Aruba:Aruba-User-Role Contractor

orubo Central			Q Se							۹ ¢ ()	
I AOS10 ි	Lū Clients									S hours ∷≣	Sur
Manage	CLIENTS ALL	~ c							1.55 MB (⊕901.	19 KB ④689.81 KB)	
Devices	All O Conne 2 0	cting O Connected	 Failed O 	Offline 0	Ø Blocked Wire 0	eless Wir		te			
ī Clients		2	v	U			, 0				
Guests	Client Name	Status J=	▼ IP Address	VLAN	Connected To	SSID/Port		Y AP Role		Authentication	···
Applications					b4:5d:50:c6:82:4a	School-Mixed	Usage		Key Management		
Security	 exec1 contractor1 	Connected Connected	10.10.22.50	22	b4:5d:50:c6:82:3c	School-Mixed		Executive-Bridge Contractor	WPA2_ENTERPRISE	DOT1X DOT1X	
nalyze	contractori	Connected	10.10.44.50	44	D4:50:50:00:82:50	School-Mixed		Contractor	WFA2_EINTERFRISE	DOTIX	
Central			Q Se							۹ ¢ Ø) #
👵 contractor1 🛛 🕗	Summary Al Insights Location	n Sessions									
inage —	CLIENT DETAILS									_	
Overview		C							Actions 🔻	• Go	Live
Applications	DATA PATH	CLIENT		SSID		AP	SWITCH	GATEWA			
nalyze			>>>>>	(?)	>>>> (~)		
Live Events		contractor1	////	School-Mixed		:50:c6:82:3c	Aruba-2930F-8G-PoEP-2SFI	PP 7005_AOS10	_gwy2		
Events		CONNECTED		UP		UP	UP	UP			
Tools											
	CLIENT			NETWORK				CONNECTION			
						LAN DERIVATION		CHANNEL 6 (20 MHz)	BAND 2.4 GHz		
	USERNAME contractor1			VLAN 44		VSA		o (eo mine)	2.4 GHz		
		CLIENT TYPE Wireless			ł	VSA AP DERIVATION RADIUS		CLIENT CAPABILITIES 802.11gn, 802.11v	2.4 GHZ		
	contractor1 HOSTNAME			44 AP ROLE	1	AP DERIVATION		CLIENT CAPABILITIES	2.4 002		
	contractor1 HOSTNAME SpectreLab IP ADDRESS	Wireless MAC ADDRESS	s	44 AP ROLE Contractor GATEWAY ROLI		AP DERIVATION RADIUS SWITCH ROLE		CLIENT CAPABILITIES 802.11gn, 802.11v CLIENT MAX SPEED	2.4 UT2		
	contractor1 HOSTNAME SpectreLab IP ADDRESS 10.10.44.50 GLOBAL UNICAST IPV6 ADDRESS	Wireless MAC ADDRESS f0:d5:bf:4b:67:11 LINK LOCAL IPV6 ADDRES	s	44 AP ROLE Contractor GATEWAY ROLI Contractor SEGMENTATIO	E	AP DERIVATION RADIUS SWITCH ROLE		CLIENT CAPABILITIES 802.11gn, 802.11v CLIENT MAX SPEED 288 Mbps LEDs on ACCESS POINT	24 012		

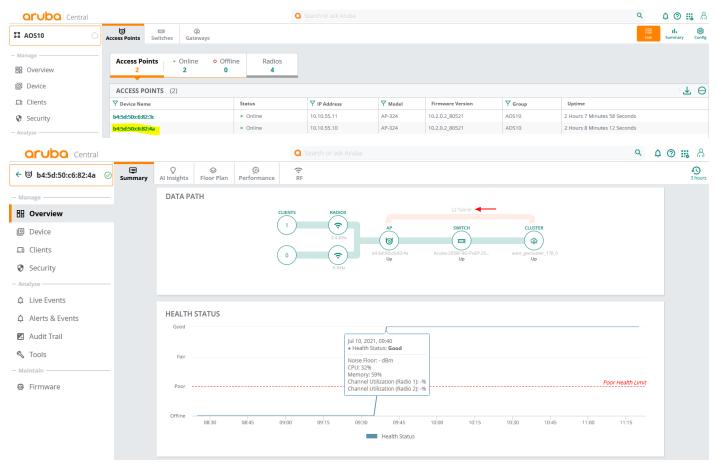
Note that Auth server shown above is the IP address of one of the gateways. Now we'll use another client and login with exec1 credentials. First checking ClearPass Access tracker

Summary Input	Output Accounting							
Login Status:	ACCEPT							
Session Identifier:	R0000004-01-60e8f063							
Date and Time:	Jul 10, 2021 10:57:07 AEST							
End-Host Identifier:	A0-88-B4-50-C0-84							
Jsername:	exec1							
Access Device IP/Port:	192.168.1.242							
Access Device Name:	10.10.55.10							
System Posture Status:	UNKNOWN (100)							
	Policies Used -							
Service:	AA Aruba 802.1X Wireless							
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2							
Authentication Source:	AD:192.168.1.250							
Authorization Source:	Ariya AD							
Roles:	Executives, [User Authenticated]							
Enforcement Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless							
l	Executive-Bridge Profile records >> Change Status Show Configuration Export Show Logs Clos Output Accounting							
Enforcement Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless Executive-Bridge Profile							
System Posture Status:	UNKNOWN (100)							
Audit Posture Status:	UNKNOWN (100)							
RADIUS Response	C							
Endpoint:Last Known	Location 192.168.1.242:b4:5d:50:c6:82:4a							

Checking the client dashboard on Aruba Central

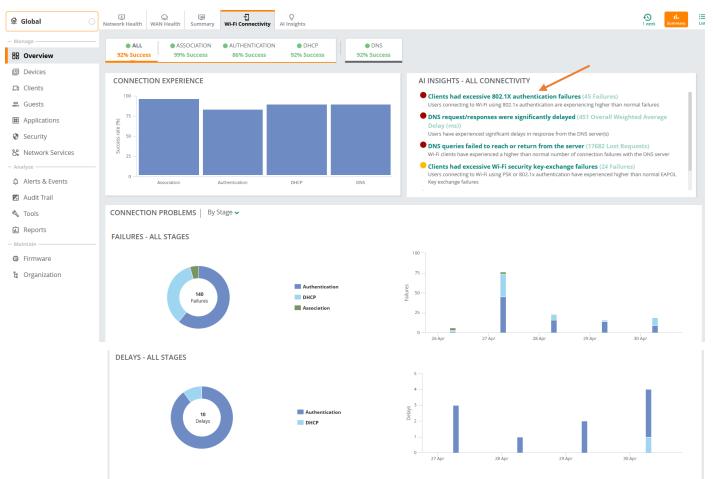
다 AOS10 이	Lū Clients									3 hours
- Manage	CLIENTS ALL	~ C							1.59 MB (💮	916.75 KB ④712.28 KB)
Device	All O Conr			• Offline	Ø Blocked	Wireless	Wired	Remote		
🗅 Clients	2 0	2	0	0	0	2	0	0		
Security										\odot
- Analyze	V Client Name	Status 🚛	Y IP Address	VLAN	Connected To	∀ ssid	/P Usage	Y AP F	cole Key Management	Authentication
↓ Live Events	œ <mark>exec1</mark>	O Connected	10.10.22.50	22	b4:5d:50:c6:82:4a	School-M	fixed 1.59 M	B Executiv	e-Bridge WPA2_ENTERPRISE	DOT1X
🏚 Alerts & Events		O Connected	10.10.44.50	44	b4:5d:50:c6:82:3c	School-N	fixed	Contract	or WPA2_ENTERPRISE	DOT1X

Checking the AP view to see the graphical tunnel for



7 RF Monitoring

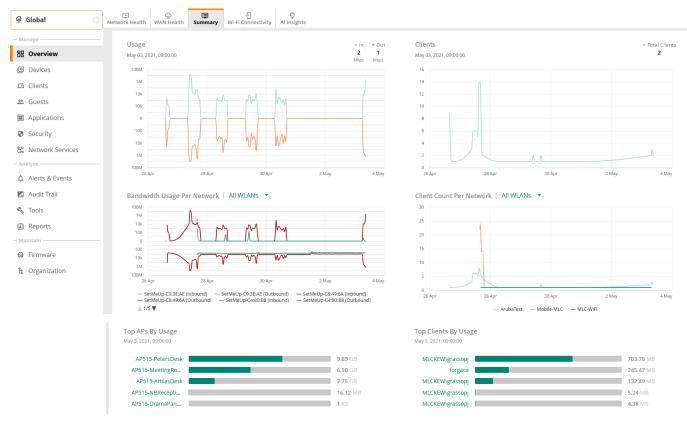
Here we'll just touch on some of the RF mgmt. info that are available in Central. To start with at the global level, you can check the WiFi connectivity and then drill down on any specifics, like AI insights, associations, authentication, etc.



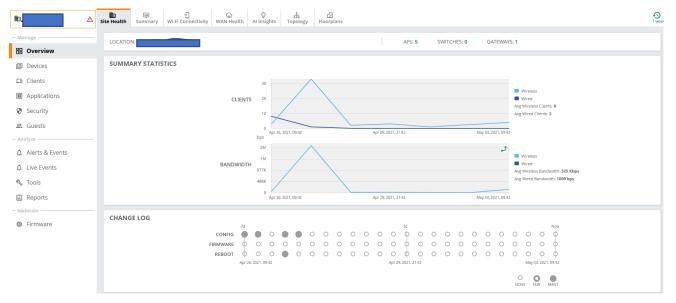
Clicking on "clients had excessive 802.1.x failures"

Severity Description Impact • Clients had excessive 802.1X authentication failures Connectivity - Wi-Fi 10 Impacted Clients (62.42% of 16), 45 Failures (28.85% of 156) Reason Recommendation Check user's provisioned status and validate the password 22 Server Rejected Authentication Check user's provisioned status and validate the password 22 Timeout - Authentication Server Check authentication server's log to verify the authentication request reached the server 18 Timeout - Client Check the client and it's environment for adequate connection quality 9 Failures - Last 1 Week Impact Impact apr 25 Apr 26 Apr 27 Apr 28 Apr 29 Apr 30 May 1	Clients had excessive 802.1X authentication failures Connectivity - Wi-Fi 10 Impacted Clients (62.42% of 16), 45 Failures (28.85% of 156) Reason Recommendation Recommendation Failures Server Rejected Authentication Check user's provisioned status and validate the password 22 22 Timeout - Authentication Server Check authentication server's log to verify the authentication request reached the server Image: Check the client and it's environment for adequate connection quality 9 Failures - Last 1 Week Image: Check the client and it's environment for adequate connection quality Image: Check the client and it's environment for adequate connection quality Image: Check the client and it's environment for adequate connection quality Image: Check the client and it's environment for adequate connection quality Image: Check the client and it's environment for adequate connection quality Image: Check the client and it's environment for adequate connection quality Image: Check the client and it's environment for adequate connection quality Image: Check the client and it's environment for adequate connection quality Image: Check the client and it's environment for adequate connection quality Image: Check the client for adequate connection quality Image: Check	ISIGHTS													
Reason Recommendation Failures Server Rejected Authentication Check user's provisioned status and validate the password 22 Timeout - Authentication Server Check authentication server's log to verify the authentication request reached the server 18 Timeout - Client Check the client and it's environment for adequate connection quality 3	Reason Recommendation Failures Server Rejected Authentication Check user's provisioned status and validate the password 22 Timeout - Authentication Server Check authentication server's log to verify the authentication request reached the server 18 Timeout - Client Check the client and it's environment for adequate connection quality 3	Severit						~	Impact		_				
Server Rejected Authentication Check user's provisioned status and validate the password 22 Timeout - Authentication Server Check authentication server's log to verify the authentication request reached the server 18 Timeout - Client Check the client and it's environment for adequate connection quality 3 Failures - Last 1 Week ag High Medium Low	Server Rejected Authentication Check user's provisioned status and validate the password Timeout - Authentication Server Timeout - Client Failures - Last 1 Week Apr 25 Check user's provisioned status and validate the password Check authentication request reached the server Check the client and it's environment for adequate connection quality Failures - Last 1 Week Failures - Marrin Last 1 Week Failures - Last 		Clients had exce	ssive 802.1X authenticati	ion failures		Connectivity - Wi-	-Fi	10 Impacted 0	Clients (62.4)	2% of 16), 45 F	ailures (28.859	% of 156)		
Timeout - Authentication Server Check authentication server's log to verify the authentication request reached the server Image: Check authentication server's log to verify the authentication request reached the server Image: Check authentication server's log to verify the authentication request reached the server Image: Check authentication server's log to verify the authentication request reached the server Image: Check authentication server's log to verify the authentication request reached the server Image: Check authentication server's log to verify the authentication request reached the server Image: Check authentication server's log to verify the authentication request reached the server Image: Check authentication server's log to verify the authentication request reached the server Image: Check authentication server's log to verify the authentication request reached the server Image: Check authentication server's log to verify the authentication request reached the server Image: Check authentication server's log to verify the authentication request reached the server Image: Check authentication server's log to verify the authentication request reached the server Image: Check authentication server's log to verify the authentication request reached the server Image: Check authentication server's log to verify the au	Timeout - Authentication Server Timeout - Client Check authentication server's log to verify the authentication request reached the server Check authentication server's log to verify the authentication request reached the server Check authentication server's log to verify the authentication request reached the server Check authentication server's log to verify the authentication request reached the server Check the client and it's environment for adequate connection quality Failures - Last 1 Week apr 25 Apr 25 Apr 25 Apr 26 Apr 27 Apr 28 Apr 30 May 1 Site Server Access Point Access Point Access Point Apr 20 Apr 30 May 1	Reaso	son											Failures	
Timeout - Client Check the client and it's environment for adequate connection quality Failures - Last 1 Week	Timeout - Client Check the client and it's environment for adequate connection quality Failures - Last 1 Week apr 25 Apr 25 Apr 26 Apr 27 Apr 28 Apr 29 Apr 30 May 1 Site Server Access Point Acc													22	4
Failures - Last 1 Week	Failures - Last 1 Week g_{g} Apr 25 Apr 26 Apr 27 Apr 28 Apr 29 Apr 30 May 1	Timeo	out - Authentication S	erver			Check authentication	ı server's log to	o verify the auth	entication re	equest reache	I the server		18	4
High Medium Low	High Apr 25 Apr 26 Apr 27 Apr 28 Apr 29 Apr 30 May 1 Site Main Server Main Access Point Main Client Main Access Point Apr 30 Apr 30 May 1														
Apr 25 Apr 26 Apr 27 Apr 28 Apr 29 Apr 30 May 1	Site Server Access Point Client Access Point	Failu					Check the client and i	it's environmer	nt for adequate	connection	quality			High Mediu	
		Failu	ures - Last 1 Wee	K		1								High Mediu	Im

Next, we can check the usage summary

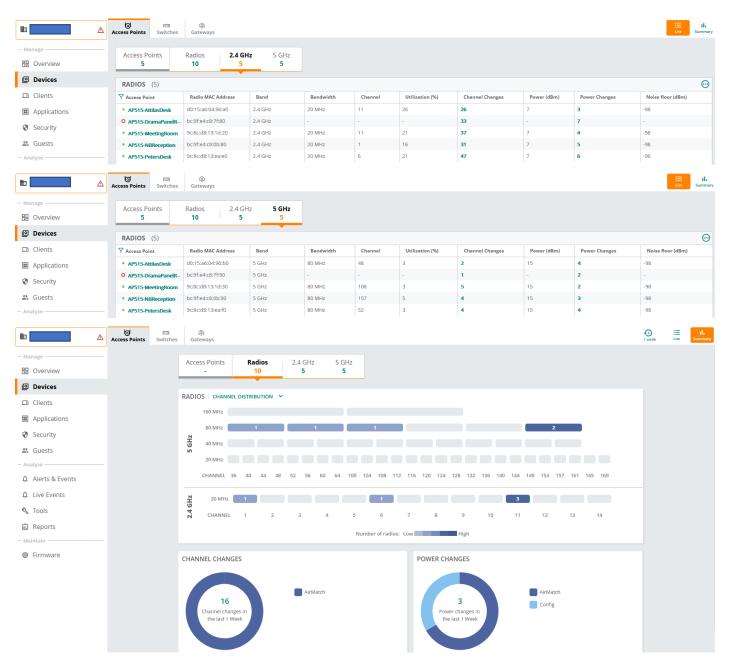


We can then go to the Site level and see some of the stats

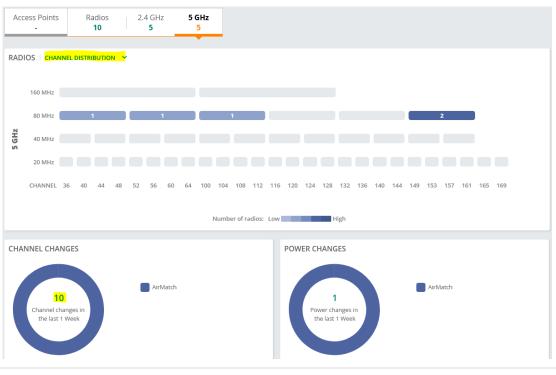


	Access Points Switches Gateways			
- Manage	Access Points • Online • Offline 5 4 1	Radios 10		
Devices	ACCESS POINTS (5)			
Clients		Status	▼ IP Address	Y Model
Applications	AP515-DramaPanelRoom	O Offline	10.16.136.201	AP-515
Consulta	AP515-NBReception	Online	10.2.136.12	AP-515
Security	AP515-PetersDesk	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



Switches						×	
	CHANNEL CHA	NGES (10)					
A	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 2	
N	Apr 26, 2021, 18:30	Algorithm Assigned	64E	60E	5 GHz	AP515-PetersDesk	
GHz	Apr 26, 2021, 18:15	Algorithm Assigned	100E	108E	5 GHz	AP515-MeetingRoom	
LO LO	Apr 26, 2021, 18:15	Algorithm Assigned	36E	153E	5 GHz	AP515-NBReception	

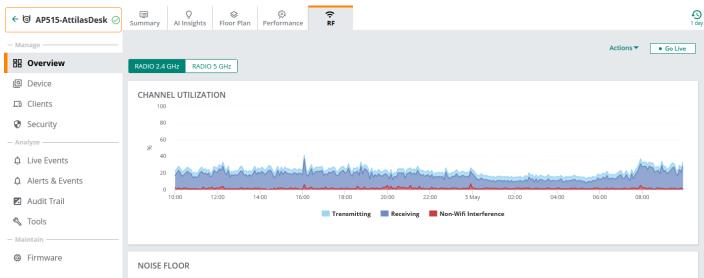
Next, we can have a look at the Live view, for that we'll choose a specific AP.

LABELS

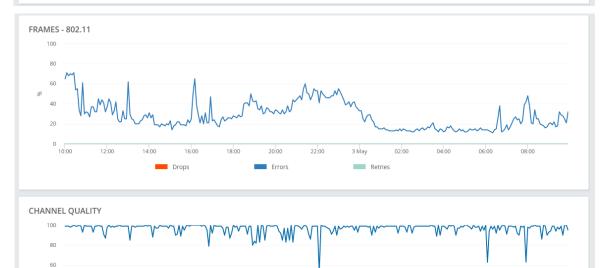
Firmware

🖗 Global	Access Points Switches Gateway	ays			
Manage	Access Points • Online 5 4	Offline Radios 1 10			
Devices	ACCESS POINTS (5)				
🗖 Clients		Status	Y IP Add	ress	Y Model
😩 Guests	AP515-DramaPanelRoom	O Offline	10.16.136	5.201	AP-515
	AP515-NBReception	Online	10.2.136.	12	AP-515
Applications	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
영 AP515-AttilasDesk ⊘ sun	AP515-AttiliasDesk	• Online	10.2.136.	13	·
・ 「 AP515-AttilasDesk () Sun	⊟ (2) ⊗ (2)	÷	10.2.136.	13	AP-515 Actions▼ ● Go Li
· ⓒ AP515-AttilasDesk ⊘ sun Manage 문 Overview 의 Device	⊟ (2) ⊗ (2)	÷	10.2.136. NETWORK ЕТН0 • Up	SPEED (Mbos) / DUPLEX 1000 / Full	
Image Image Image Image		RF COUNTRY CODE	NETWORK ETHO	SPEED (Mbps) / DUPLEX	Actions - Go Li
O AP515-AttilasDesk Sur	Al Insights Floor Plan Performance DEVICE AP MODEL AP-515 MAC	RF COUNTRY CODE AU SERIAL NUMBER LAST REBOOT REASON	NETWORK ETH0 • Up ETH1 • Down CURRENT UPLINK	SPEED (Mbps) / DUPLEX 1000 / Full SPEED (Mbps) / DUPLEX - UPLINK COP	Actions • Go Li VLAN Trunk (all) LLDP Deta
C AP515-AttilasDesk Sum Manage C Overview D Device C Clients Security Analyze	Al Insights Floor Plan Performance DEVICE AP MODEL AP-515 MAC d0:15:a UPTIME 5 Days 22 Hours 30 Minutes FIRMWARE VERSION	RF COUNTRY CODE AU SERIAL NUMBER LAST REBOOT REASON AP reload CONFIGURATION STATUS	NETWORK ETH0 • Up ETH1 • Down CURRENT UPLINK Ethernet (br0)	SPEED (Mbos) / DUPLEX 1000 / Full SPEED (Mbos) / DUPLEX - UPLINK CON -	Actions Go Li VLAN Trunk (all) LLDP Deta VLAN - NRECTED TO
Image Sum Manage Image Image Image Ima	Al Insights Floor Plan Performance Al Insights Floor Plan Performance DEVICE AP MODEL AP-515 MAC d0:15:a UPTIME 5 Days 22 Hours 30 Minutes	RF COUNTRY CODE AU SERIAL NUMBER LAST REBOOT REASON AP reload	NETWORK ETH0 • Up ETH1 • Down CURRENT UPLINK Ethernet (br0) IP ADDRESS 10.2.136.13 (DHCP)	SPEED (Mbps) / DUPLEX 1000 / Full SPEED (Mbps) / DUPLEX - UPLINK COP	Actions Go Li VLAN VLAN VLAN VLAN - VLAN - NNECTED TO DDDRESS
	Al Insights Floor Plan Performance DEVICE AP MODEL AP-515 MAC d0:15:a UPTIME 5 Days 22 Hours 30 Minutes FIRMWARE VERSION	RF	NETWORK ETH0 • Up ETH1 • Down CURRENT UPLINK Ethernet (br0) IP ADDRESS	SPEED (Mbos) / DUPLEX 1000 / Full SPEED (Mbos) / DUPLEX - UPLINK CON - PUBLIC IP A	Actions Go Li VLAN Trunk (all) LLDP Deta VLAN - VLAN - NRECTED TO DORESS 51 NEEWAY

LEDs on ACCESS POINT







40 20

0 10:00

12:00

14:00

16:00

18:00

20:00

22:00

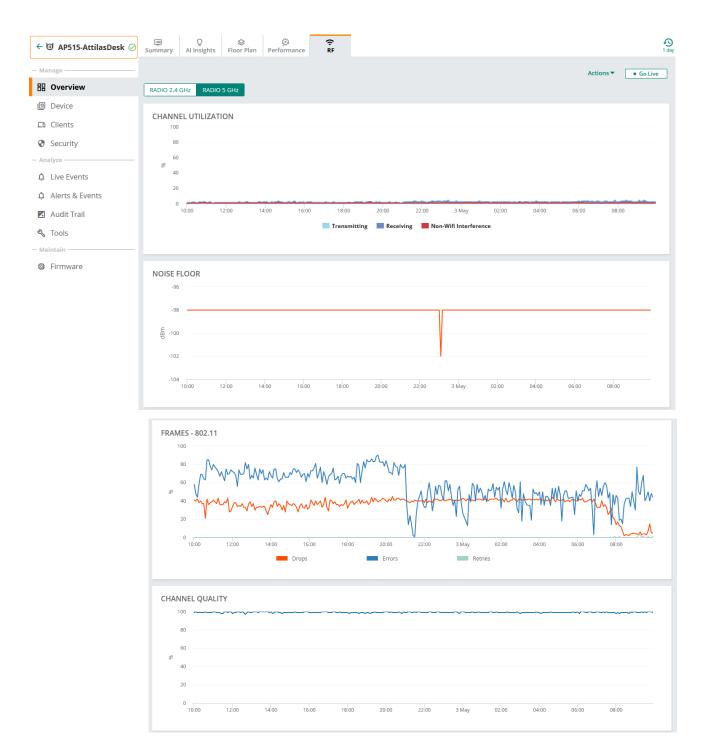
3 May

02:00

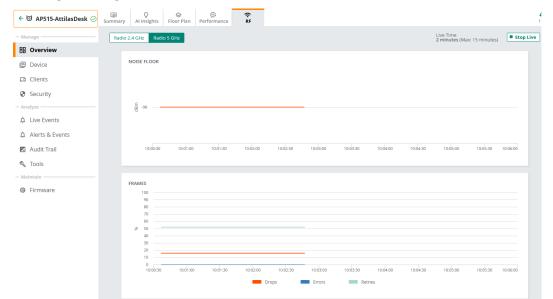
04:00

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

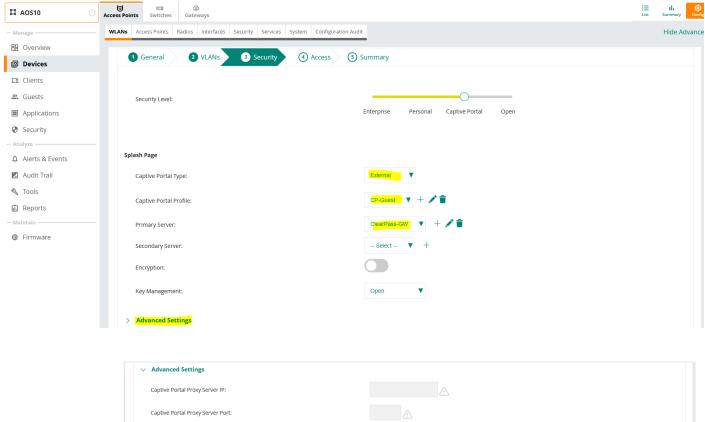
Here we'll start with AP configuration followed by ClearPass.

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.

디 AOS10 〇	Access Points Switches Gateways		i≣ li, List Summary Config
— Manage —	WLANs Access Points Radios Interfaces Security Services System Control	nfiguration Audit	Hide Advanced
B Overview			
Devices	CREATE A NEW NETWORK		
🗖 Clients	1 General ② VLANs ③ Security ④ Acce	(5) Summary	
Suests	Name (SSID):	Schoo-Guest	
ApplicationsSecurity	✓ Advanced Settings		
- Analyze	Broadcast/Multicast		
♪ Alerts & Events	Transmit Rates (Legacy Only)		
🛛 Audit Trail	🕂 Bandwidth Control		
🖏 Tools	🕀 WiFi Multimedia		
🛍 Reports	Miscellaneous		
— Maintain	Time Range Profiles		
Firmware			
			Cancel Next
ଘ AOS10 이	Access Points Switches Gateways		는 나 왕 List Summary Config
— Manage —	WLANS Access Points Radios Interfaces Security Services System Co	nfiguration Audit	Hide Advanced
B Overview			
Devices	CREATE A NEW NETWORK		
🗖 Clients	1 General 2 VLANs 3 Security 4 Acco	ess 3 Summary	
😩 Guests	Traffic forwarding mode:	Bridge Tunnel Mixed	
Applications	Primary Gateway Cluster:	AOS10:auto_gwcluster_178_0	
 Security Analyze 			
▲ Alerts & Events	Secondary Gateway Cluster:	None	
Audit Trail	Client VLAN Assignment:	Static Dynamic	
🖏 Tools	VLAN ID:		
🛍 Reports	> Show Named VLANs		
— Maintain —			
Firmware			
			Cancel Back Next
법 AOS10 이	Access Points Switches Gateways		i⊟ II. List Summary Config
- Manage	- WLANs Access Points Radios Interfaces Security Services System Co	nfiguration Audit	Hide Advance
B Overview			
Devices	CREATE A NEW NETWORK		
□ Clients	1 General 2 VLANs 3 Security 4 Acc	ess 3 Summary	
a Guests			
Applications	Security Level:		
Security		Enterprise Personal Captive Portal Open	
Analyze	-		
Audit Trail			
Tools	Splash Page		
Reports	Captive Portal Type:	External V	
— Maintain	Captive Portal Profile:	Select 🔻 🕂	
Firmware		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 V	
🛍 Reports	Enci	Server offload:		
— Maintain ————	Key			
Firmware		Cancel		ок
	> Adı			



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:	o min 🔻
Denylisting:	
Max Authentication Failures:	0

Use authentication servers		
1 min		

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.

법 AOS10 이	Access Points Switches Gateways			는 II. List Summary Con
- Manage	- WLANS Access Points Radios Interfaces Security	y Services System Configuration Audit		Hide Advan
B Overview				
Devices	CREATE A NEW NETWORK			
🗖 Clients	1 General 2 VLANs 3	Security 4 Access 5 Summary		
😩 Guests				
Applications	Access rules	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			
Reports				
- Maintain				
Firmware				
	ROLE ASSIGNMENT RULES			
	Default role: Schoo-Guest			
	+ ADD ROLE ASSIGNMENT			1 Role(s)
	ASSIGN PRE-AUTHENTICATION ROLE:	CP-Guest		
	ENFORCE MAC AUTH ONLY ROLE:			
				Cancel Back Next
	0	Search or ank Aruba		a 4 @ ## &
AOS10				ille Summary Config
	ANs Access Points Radios Interfaces Security	SUCCESS		Hide Advanced
B Overview		SUCCESS		
Devices	DTIM Interval	Schoo-Guest is Configured Successfully		
🗈 Clients	Primary Usage	ок		
🔐 Guests	Inactivity Timeout			
Applications				

Now we have our Guest SSID configured.

II AOS10	Access Pe	oints	Switches	Gate										List	th Summary Config
- Manage	WLANs	WLANs Access Points Radios Interfac				Security	Security Services System Configuration Audit								Hide Advance
B Overview															
Devices	V	Wireless SSIDs													
🗗 Clients		NAME			SECURITY		ACCESS TYPE	TRAFFIC FORM	TRAFFIC FORWARDING MODE NETWORK EN/						
😩 Guests		■ school			wpa2-aes		Unrestricted	Tunnel	Tunnel Yes						
Applications		Schoo-Guest			Captive Portal (external)		Role Based	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

AOS10	Access Poi	nts Switche	s Gate								SELECTE	D GROUP TYPE	List	II. Summary
– Manage –	System	Interface R	touting W	AN Security	VPN High	n Availability Cor	nfig Audit							Basic Mod
Overview	Roles	Policies A	Jiases A	Applications	Apply Policy	Auth Servers	Role Assignme	nt (AAA Profiles)	L2 Authentic	ation L3 Authentication	n Advanced Firewall			
Devices	✓ Aut	hentication S	ervers											
⊑ a Clients		Server grou	os											
😩 Guests		NAME				SERVERS		FAIL THROUGH		LOAD BALANCE	SERVER RULES			=
Applications		Schoo-Guest	_#1615938	135060_41#ac	ct_svg	1		-		-	o	î		
Security		Schoo-Guest	_#1615938	135060_41#aı	ith_svg	1					0			
– Analyze –		Schoo-Guest	_#1615938	135060_41#cp	_svg	1				-	0			
Alerts & Events		school_#161	553207950	4_41#acct_svg		1		-			0			
Audit Trail		school_#161	553207950	4_41#auth_svį	3	1					0			
🖏 Tools		school_#161	553207950	4_41#cp_svg		1					0			
🗈 Reports		+												
Maintain —														
Firmware		Server Grou	p > Schoo-	Guest_#161593	8135060_41#	_acct_svg Ser	vers Options	s Server Rules				()	Drag rows	s to re-orde
		NAME		TYP	E		IP ADDRESS		TRIM FQI	DN	MATCH RULES			=
		ClearPass-G	N	Rad	lius		192.168.1.95				0			

법 AOS10 〇	Access Points Switches Gateways			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	CPN Authentication			
10013				

ជ AOS10 이	Access Points Switches	s				SELECTED GROUP TYPE Gateway	List	II. Summary Cor
Manage	System Interface Routing WAN	Security VPN High Availability	Config Audit					Basic Mode
B Overview	Roles Policies Aliases Appl	ications Apply Policy Auth Sen	ers Role Assignment (AAA Profiles)	L2 Authentication L3 Auther	tication Advanced Fire	wall		
Devices	Roles							
🗖 Clients	^							
🔐 Guests	∀NAME		RULES					=
Applications	ap-role		35 Rules					
Security	authenticated		4 Rules					
Analyze	CP-Guest		5 Rules		Î			
Alerts & Events	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 Bandwidt	h More						
	∀ NAME	RULES COUNT	TYPE	POLIC	USAGE			=
	global-sacl	0	session	ap-role,	authenticated, CP-Guest, defa	ult-vić		
	apprf-cp-guest-sacl	0	session	CP-Gues	CP-Guest			
	cp-guest 5		session	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 Monitoring Configuration Service Templates & Wizards	To authenticate guest devices based on their MAC address.
-☆ Services ⊒- Authentication ⇒ Q Identity	EDUROAM service Service template for roaming users to connect to campus networks that are part of the eduroam federation.
Single Sign-On (SSO) CLCal Users CLCal Users	Service Template for providing encrypted wireless access to (guest) users via fixed 802.1X PEAP credentials.
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 ⊒- ॾ 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						
access c vary acc	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 → Add Service	e Cancel
General	Wireless Network Setting	IS MAC	Caching Settings	Posture Set	tings Access Restriction	ons		
. Enfo	rcement Type applies to	the Canti	vo Portal Accor	c. Employee A	anna Guart Arran	and Contractor Acces	e fielde	
	ive Portal Access is used	-					s fields.	
-	ast one of Employee, Gu				-	•		
Enforceme	nt Type*:		Aruba Role Enfor	cement ~				
	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
					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 v 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)	\bigcirc
3.		3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	O
4.		4	[Guest Operator Logins]	Application	Aruba Application Authentication	Ø
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	
8.		8	GG MAC Authentication	RADIUS	MAC Authentication	S
9.		9	GG User Authentication with MAC Caching	RADIUS	RADIUS Enforcement (Generic)	\bigcirc

We'll look at the MAC authentication service

Services - GG MAC Authentication

Click to add..

з.

Note: This Service is created by Service Template

Sum	nary Service	Authentication	Authorization	Roles	Enforcement						
Name:		GG MAC Authent	tication								
Descrip	otion:	MAC Authenti portal users	C Authentication bypass for captive rtal users								
Type:		MAC Authentic	Authentication								
Status	:	Enabled	bled								
Monito	r Mode:	Enable to n	\Box Enable to monitor network access without enforcement								
More C	ptions:	Authorizati	on 🗌 Audit End	hosts [Profile Endpoints 🗌 Acc	ounting Proxy					
						Service Rule					
Matche	s O ANY or O	ALL of the followi	ing conditions:								
	Туре	Name Operator Value									
1.	Connection		Cli	ent-Mac-	Address	EQUALS	%{Radius:IETF:User-Name}		Ŧ		
2.	Radius:Aruba		Aruba-Essid-Name BEGINS_WITH Guest 🗎 🕆								

Summary	Service	Authentication Authoriza	tion Roles	Enforcement		
Authentication	n Methods:	[Allow All MAC AUTH]	^			Add New Authentication Method
				Move Up ↑		
				Move Down ↓		
				Remove		
				View Details		
				Modify		
		Select to Add	×			
Authentication	n Sourcos:		×	1		
Macheneleacion	n bources.	[Endpoints Repository] [Loca	al SQL DB]	Marcalla		Add New Authentication Source
				Move Up ↑ Move Down ⊥		
				Remove		
				View Details		
				Modify		
			~			
		Select to Add		~		
Summary	Service	Authentication Authorizat	ion Roles	Enforcement		
Authorization					e fetched (for each Authentication Sourc	0)
		Authonization Sources Iron		apping attributes ar	Attributes Fetched From	
		1. [Endpoints Repositor		DB]	[Endpoints Repository] [Local	SQL DB]
		Additional authorization so			pping attributes -	Add New Authentication Source
		[Time Source] [Local SQL DB [Guest User Repository] [Loc		Remove		Add New Addiendcation Source
				View Details Modify		
		Select to Add	~	~		
		Select to Add				
Summary	Service	Authentication Authorizat	ion Roles	Enforcement		
Role Mapping	Policy:	GG MAC Authentication Role	Mapping	 ✓ Modif 	y	Add New Role Mapping Policy
			R	Role Mapping Policy [etails	
Description:						
Default Role:		[Other]				
	_	n: evaluate-all				
Conditio		points Repository]:Unique-De	ules Count EX		Role	
		n:[Time Source]:Now DT LE				
 Expiry}) AND (Authorizatio	n:[Guest User Repository]:A	countExpired	FOUALS false)	[MAC Caching]	
		n:[Guest User Repository]:A				
		e ID EQUALS 1)			[Contractor]	
		e ID EQUALS 2)			[Guest]	
4. (Endpoir	nt:Guest Koi	e ID <i>EQUALS</i> 3)			[Employee]	
Summary	Service	Authentication Authorizati	on Roles	Enforcement		
Use Cached Re	esults:	Use cached Roles and Po	sture attributes	s from previous sess	ions	
Enforcement F	Policy:	GG MAC Authentication Enforce	ement Policy	~ N	lodify	Add New Enforcement Policy
		-	E	nforcement Policy De	etails	
Description:						
Default Profile	:	[Deny Access Profile]				
Rules Evaluati	ion Algorithn	n: first-applicable				
Conditio	ons				Enforcement Profiles	
(Tips:R 1. [Guest]	ole MATCHI	ES_ALL [MAC Caching]			[Allow Access Profile], GG Guest Devi	ce Profile
	thenticated]) ES_ALL [MAC Caching]				
2. [Employ					[Allow Access Profile], GG Employee [Device Profile
(Tips:R	ole MATCHI	ES_ALL [MAC Caching]				
 [Contrac [User Au 	tor] ithenticated])			[Allow Access Profile], GG Contractor	Device Profile
(Tips:R	ole MATCHI	ES_ANY [Guest]				
4. [Contrac [Employe					[Allow Access Profile], GG Captive Por	tal Profile
K Back to S	ervices				Disable	Copy Save Cancel

And here are the enforcement profiles that are used here

	:Aruba	Arub	a-User-Role		= Guest-guest-logo
Туре	_	Nam	e	_	Value
Attributes:					
Device Grou	p List:	-			
Action:		Accept			
Туре:		RADIUS			
Description:		Captive Portal Role/VLAN	enforcement		
Profile: Name:		GG Captive Portal Profile			
Summary	Profile	Attributes			
2. Radius:		User-Na		=	%{Endpoint:Username}
L. Radius:	Aruba	Aruba-U	ser-Role	=	Contractor
ttributes: Type		Name			Value
Device Group	LISL.	-			
Action:	List:	Accept			
Гуре:		RADIUS			
Description:		Role/VLAN enforcement for C	Contractor		
Name:		GG Contractor Device Profile			
rofile:					
Summary	Profile	Attributes			
2. Radius:I	ETF	User-Na	ime	=	%{Endpoint:Username
1. Radius:			Jser-Role	=	Employee-Guest
Туре		Name			Value
ttributes:					
evice Group	List:	-			
action:		Accept			
ype:		RADIUS			
escription:		Role/VLAN enforcement for	Employee		
lame:		GG Employee Device Profile			
rofile:					
Summary	Profile	Attributes			
2. Radius:	IETF	User-Na	me	=	%{Endpoint:Username}
1. Radius:	Aruba	Aruba-U	ser-Role	=	Guest
Туре		Name			Value
Attributes:					
Device Group	List:	-			
Action:		Accept			
Type:		RADIUS	Juest		
Name: Description:		GG Guest Device Profile Role/VLAN enforcement for 0	Suget		

We'll look at the User Authentication with MAC caching service

Services - GG User Authentication with MAC Caching

Sumr	nary Service	Authentication	Authorization Re	oles Enforcement							
Name:	Name: GG User Authentication with MAC Caching										
Descrip	tion:	Captive Porta MAC Caching	l authentication	with							
Type:		RADIUS Enforcement (Generic)									
Status	:	Enabled									
Monito	r Mode:	Enable to monitor network access without enforcement									
More O	ptions:	Authorization	n 🗌 Posture Compl	liance 🗌 Audit End-hosts 🗌	Profile Endpoints Accounting Proxy						
					Service Rule						
Matche	s O ANY or 🖲	ALL of the following	g conditions:								
	Туре		Name		Operator	Value					
1.	Radius:IETF		Calling	-Station-Id	EXISTS		₿ <u>a</u>	Ŵ			
2.	Connection		Client-	Mac-Address	NOT_EQUALS	%{Radius:IETF:User-Name}	Ba	Ť			
з.	Radius:Aruba		Aruba-	-Essid-Name	BEGINS_WITH	Guest	Ba	Ť			
4.	Click to add										

Summary	Service	Authentication Authorization R	oles Enforcement	
Authenticatio	on Methods:	[PAP]	^	Add New Authentication Method
		[MSCHAP]	Move Up ↑	
		[CHAP]	Move Down ↓	
			Remove	
			View Details	
			Modify	
			~	
	_	Select to Add	~	
Authenticatio	on Sources:	[Guest User Repository] [Local SQL DB	·] ^	Add New Authentication Source
			Move Up ↑	
			Move Down ↓ Remove	
			View Details	
			Modify	
			~	~
		Select to Add	~	
Summary	Service	Authentication Authorization Rol	es Enforcement	
Authorization	Details:		le mapping attributes are	e fetched (for each Authentication Source)
		Authentication Source 1. [Guest User Repository] [Local	SOL DB1	Attributes Fetched From [Guest User Repository] [Local SQL DB]
			502.001	
		Additional authorization sources from	n which to fetch role-map	··· =
		[Endpoints Repository] [Local SQL DB] [Time Source] [Local SQL DB]	Remove	Add New Authentication Source
			View Details	
		Calact to Add	Modify	
		Select to Add		
Summary	Service	Authentication Authorization Role	es Enforcement	
Role Mapping	Policy:	GG User Authentication with MAC Caching	g Role Mapping 🖂 Modify	Add New Role Mapping Policy
			Role Mapping Policy D	etails
Description:				
Default Role:		[Other]		
	_	m: evaluate-all		
Condition				Role
		EQUALS 1) EQUALS 2)		[Guest]
		EQUALS 3)		[Employee]
Summary	Service	Authentication Authorization Role	es Enforcement	
Use Cached R		Use cached Roles and Posture attr	butes from previous ses	
Enforcement	Policy:	GG User Authentication with MAC Cachine	g Enforcement Policy 🕥 🚺	Add New Enforcement Policy
			Enforcement Policy D	etails
Description:				
Default Profile		[Allow Access Profile] m: first-applicable		
	-	пт. птяс-аррпсавле		
Conditi 1. (Autho		ndpoints Repository]:Unique-Device-Cou	nt GREATER THAN 5)	Enforcement Profiles [Deny Access Profile]
	_	<i>S</i> [Employee])		GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit,
2. AND	(Date:Day	-of-Week BELONGS_TO		GG MAC Caching Session Limit, GG Employee MAC Caching, [Update Endpoint Known], GG MAC Caching Do Expire, GG MAC Caching Expire
Monday	,Tuesday,We	ednesday,Thursday,Friday,Saturday,Sund	ay)	Post Login, GG Employee Profile
		S [Contractor])		GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit, GG MAC Caching Session Limit, GG Contractor MAC Caching, [Update
		-of-Week BELONGS_TO ednesday,Thursday,Friday,Saturday,Sund	lay)	Endpoint Known], GG MAC Caching Do Expire, GG MAC Caching Expire
	Role <i>EQUAI</i>			Post Login, GG Contractor Profile GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit,
4. <i>AND</i>	(Date:Day	-of-Week BELONGS_TO		GG MAC Caching Session Limit, GG Guest MAC Caching, [Update Endpoint Known], GG MAC Caching Do Expire, GG MAC Caching Expire
Monday	,Tuesday,We	ednesday,Thursday,Friday,Saturday,Sund	ay)	Post Login, GG Guest Profile

The enforcement profiles

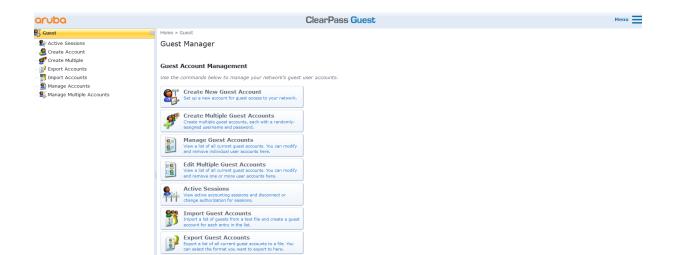
Summary	Profile	Attributes		
Profile:				
Name:		GG Employ	ee Profile	
Description:		Role/VLAN	enforcement for Employee	
Туре:		RADIUS		
Action:		Accept		
Device Group	List:	-		
Attributes:				
Туре			Name	Value
1. Radius:	Aruba		Aruba-User-Role	= Employee-Guest
	D (1			
Summary	Profile	Attributes		
Profile:				
Name:		GG Gue	st Profile	
Description:		Role/VL	AN enforcement for Guest	
Туре:		RADIUS	;	
Action:		Accept		
Device Grou	p List:	-		
Attributes:				
Туре			Name	Value
1. Radius	:Aruba		Aruba-User-Role	= Guest
Summary	Profile	Attributes		
Profile:				
Name:		GG Cont	actor Profile	
Description:		Role/VLA	N enforcement for Contractor	
Type:		RADIUS		
Action:		Accept		
Device Grou	p List:	-		
Attributes:				
Туре	_		Name	Value
1. Radius	:Aruba		Aruba-User-Role	= Contractor

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	10 etra				() 200 E E 100	\wedge	
Cluster Status Control the status of the entire cluster Control to the status of the entity of the entire clus	Perce	0 0 14:35 14:4		****		14:45 14:50 14:55	15:00
Device Categories Device Family Device Family Device Family		- Syst	Time (mins) tem → User 🖶 IO Wait ⊯ Idle		- RAD	Time (mins)	
Endpoint Profiler Summary Endpoint profiling details					ll Requests		0
Failed Authentications 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				10		
MDM Discovery Summary Mobile Device Management discovery details	ClearPa	<mark>ss Guest</mark> ss Onboard			0 12:00 3, Feb 12:00 4, I	Feb 12:00 5, Feb 12:00 6, Fe	2 12:0
OnGuard Clients Summary OnGuard Clients details	Je ClearPa				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 G	Home » Guest » Cre	ate Account				
- Sur Active Sessions - Create Account	Create Guest Account					
- 🌮 Create Multiple - 🔐 Export Accounts	New guest account	being created by admin.				
mport Accounts		Create New Guest Account				
- 🗐 Manage Accounts	* Guest's Name:	cpguser Name of the guest.				
- 🕵 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 V 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 /	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.						
- IV Export Accounts - Import Accounts - Manage Accounts	Quick Help Filter:	🔔 c	reate	E	More Options		
— 📲 Manage Multiple Accounts	△ Username	Role	State	Activation	Expiration		
	g cpguser (A) Reset password (C) Refresh (D) Back to guests (A) Back to main	[Guest] Change expiration	Active Remove	23 hours ago	No expiry Print Show Details Showing 1 – 1 of 1 20 rows per page ~		

Guest 📀					
-Straine Sessions	 Quick Help 	4	Create	<u></u>	More Options
— 🥵 Create Account	Filter:				
—💕 Create Multiple	△ Username	Role	State	Activation	Expiration
- 🔐 Export Accounts	🧕 cpguser	[Guest]	Active	23 hours ago	No expiry
- j Import Accounts	🛞 Reset password	🕑 Change expiratio	on 🔀 Remove	📴 Edit 🤎 Sessions 🍦	🎍 Print 🍳 Show Details
- S Manage Accounts	To update the properties	of this quest account	t use the form h	low	~ •
— 😂 Manage Multiple Accounts	To apaste the properties	o or this gatet account			
			Edit Account		
	* Guest's Name:	cpguser Name of the guest.			
	* Username:	cpguser Name of the account			
	Account Activation:	(No changes: Accou Select an option for o		tion time of this account.	
	Account Expiration:	(No changes: Accou Select an option for o		✓ ation time of this account.	
	Account Lifetime:	N/A ~ The amount of time a	after the first login	before the account will expir	e and be deleted.
	Total Allowed Usage:	(No changes) Select an option for o	changing the allowed the al	ed usage time of this accoun	t.
	Account Role:	(No changes: [Gues Role to assign to this			
	* Password:	Type in a new pass Select an option for e		ccount's password.	
	New password:	••••••• Type in a new passw	ord to assign to the	e guest account.	
	Confirm Password:	Repeat the new pass	word for the guest	account.	
/41	Session Limit:	0 The number of simul	taneous sessions a	llowed for this account. Type	o for unlimited use.
t) Devices ۲۰۰۰ ۲۰۰۰ ۲۰۰۰ ۲۰۰۰ ۲۰۰۰ ۲۰۰۰ ۲۰۰۰ ۲۰	Notes:				
 Configuration 					
Administration					
			🌱 Update Accoi	unt	

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 🔹 🔍	Home » Configuration » Pages » Web Logins					
💕 Devices 🔹 🛛 🔿	Web Login (sch	nool)				
📋 Onboard 🔹 📀	Use this form to make	changes to the Web Login school .				
- 🍫 Authentication		Web Login Editor				
Content Manager - @ Private Files	* Name:	schoo Enter a name for this web login page.				
- 🍄 Public Files - 🛱 Guest Manager	Page Name:	school Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".				
Hotspot Manager Konges Konge Kong	Description:	for AOS-10				
List Views	* Vendor Settings:	Aruba V 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 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.				

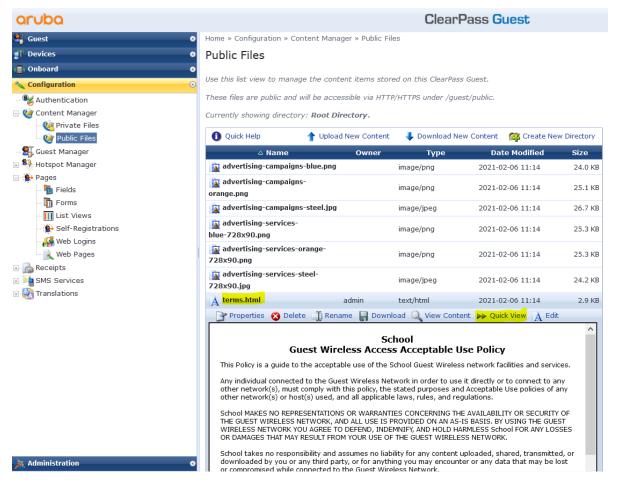
Page Redirect Options for specifying pa	rameters passed in the initial redirect.
	Do not check – login will always be permitted
Security Hash:	Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the 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 V Select the authentication requirement.
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.
Prevent 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 username and password should be checked before proceeding to the NAS authentication.
Terms:	Select now the username and password should be checked before proceeding to the NAS authentication.
	If checked, the user will be forced to accept a Terms and Conditions checkbox. None
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 default destination for all clients If selected, the client's default destination will be overridden regardless of its value.
Login Page	
	e look and feel of the login page.
* 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) (nwa text id=7980)</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 difficulty logging in.</pre>
Footer HTML:	
	Insert v
	{nwa_text id=7978} LoggIng in, please wait
Login Message:	
	Insert V HTML template code displayed while the login attempt is in progress.
* Login Delay:	0
	The time in seconds to delay while displaying the login message.
Advertising Services	
Advertising	Enable Advertising Services content
Cloud Identity Optionally present gues	sts with various cloud identity / social login options.
	Enable logins with cloud identity / social network credentials
Multi-Factor Authent	tication ctor when authenticating.
	No multi-factor authentication
Network Login Acce Controls access to the	
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 🗸
Post-Authentication	Select the response of the system to a request that is not permitted.
	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		ClearPass	Guest			Menu
Ӌ Guest	• Home » Configuration » Pages » Web Logins					
💕 Devices	 Web Logins 				👬 Ci	reate a new web login pa
📳 Onboard	0					
🔦 Configuration	 Many NAS devices support Web-based auther 	tication for visitors.				
- 🌯 Authentication	By defining a web login page on the ClearPas	s Guest you are able to provide a	customized graphi	cal login page fo	r visitors accessing the network through these NAS devices.	
🥶 Content Manager	Use this list view to define new web login page	ges, and to make changes to exis	ting web login page	5.		
- 🥸 Private Files - 🎯 Public Files	ightarrow Onboard device provisioning pages are n	ow managed from the Web Login	tab within provision	ng settings		
Suest Manager	△ Name	Page Title	Page Name	Page Skin		
📲 Hotspot Manager	🚜 school	scho	ool Gi	illeria Skin 3		
Pages - 🌇 Fields	📑 Edit 🕞 Duplicate 😵 Delete 🍇 Tran	slations 🛶 Launch				
- 🛅 Forms	1 web login 🏠 Reload		Show al	rows \sim		
- III List Views Self-Registrations 	 Back to pages Back to configuration 					
- Neb 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

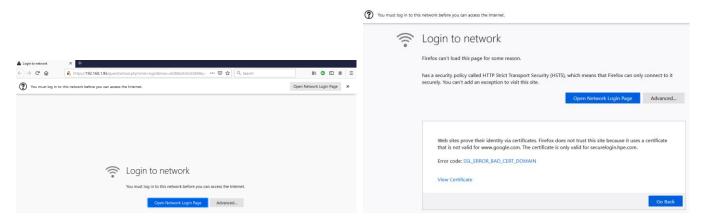
The "guest/school.php" is used in the URL redirection which we configured in MM

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		
DNS Name	securelogin.hpe.com	

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:> 🚥 🗵 🏠	III\ 💿 🗊 🛎 =
	Calleria WiFi Dease login to the network using your username and password. Username: cpguser Password: Password: Crems: Crems: Crems: Cog In Cog II Cog In Cog II	
	Contact a staff member if you are experiencing difficulty logging in.	
	aruba NETWORKS	

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.

Manage	CLIENTS ALL	~ C							7.84	4 MB (🕀 1.6	51 MB ⊕6.23 MB
Devices	All O Conne				Ø Blocked	Wireless		Remote			
Clients	3 0	1	0	2	0	1	2	0			
🙁 Guests											(
Applications	♥ Client Name	Status 🚛	P Address	VLAN	Connected	То	T Gateway Role	▼ SSID/Port	Y Health	~	Usage
Security	AriyaP	 Connected 	192.168.1.132	192	b4:5d:50:c6	:82:4a	C <mark>P-Guest</mark>	Schoo-Guest			7.84 MB
anage	Summary Q Q Summary Al Insights Locat										
Overview	CLIENT DETAILS	С							Ad	ctions 🔻	• Go
Applications	DATA PATH	CLIENT	SSIC			AP	SWI	гсн	GATEWAY		
Live Events	DATA PATH	CLIENT Rrya ^p CONNECTED	SSUC SSUC		>>>>>	AP b4:5d:50:c6:82:4a UP	4 Aruba-2930F-8		GATEWAY		
nalyze 1 Live Events 1 Events		AriyaP	Schoo-G	uest		b4:5d:50:c6:82:4a	4 Aruba-2930F-8	IG-POEP-25FPP	7005_AOS10_gwy2		
nalyze 1 Live Events 1 Events	CLIENT	AriyaP	School G	work		64:50:50:c6.82:4a UP	4 Arube 2936F-6 U	CONNECTION	0005_A0510_gwy2	PAND	
nalyze 1 Live Events 1 Events	CLIENT USERNAME #088b450c084	Ariyafi CONVIECTED	>>>>> Sono-G UP NET VLA 192	work V		b45050:c6824a uP VLAN DERIV/ VSA	Aruba 29307-6 U	Соллестоо Судер-25779 Соллестоо Смаллец 6 (20 Мнг2)	UP UP	BAND 2.4 GHz	
nalyze 1 Live Events 1 Events	CLIENT USERNAME	AriyaP	>>>>> School UP NET VLA2 AP F	work V		b45d50:c682:4a up	Aruba 29307-6 U	CONNECTION CHANNEL	UP UP		
Live Events	CLIENT USERNAME #088b450c084 HOSTNAME	Arya ^p CONNECTED	۱ ۱ ۱ ۱ ۱ ۱ 1	WORK N OLE		VLAN DERIV/ VSA	Aruba 233054	Greep-25PPP	2005,AC510,gwy2 up		
Live Events	CLIENT USERNAME #088b450x084 HIOSTNAME AriyaP IP ADDRESS	CLIENT TYPE Wireless MAC ADDRESS	>>>>> Sono-C UP VLA AP F CP-C GAT GAT	WORK N IOLE iuest EWAY ROLE		VLAN DERIV VSA AP DERIVATIV SWITCH ROL	Aruba 233054	Grade 25899 CONNECTION CHANNEL 6 (20 MHz) CLIENT CARABILITIE: 8002.11gn CLIENT MAX SPEED 288 Mbps	2005,AC510,gwy2 up	2.4 GHz	
. Live Events	CLIENT USERNAME a0884-550-084 HIOSTNAME ArfyaP IP ADDRESS 192.168.1.132 GLOBAL UNICAST IPV6 ADDRESS	CLIENT TYPE Wireles MAC ADDRESS a0:88:b4:50:c0:84 LINK LOCAL IPV6 ADDRESS	>>>>> Sono-Co UP NET VLA AP F CP-4 GP-4 SS SS SS SS SS SS SS SS SS S	WORK N IOLE iuest EWAY ROLE iuest		VLAN DERIV VSA AP DERIVATIV SWITCH ROL	Aruba 2304-4 Ju Aruba 2304-4 U Aruba 2304-4 U U Aruba 2304-4 U U U U U U U U U U U U U U U U U U	CONNECTION CHANNEL 6 (20 MHz) CLIENT CAPABILITIE 802.11gn CLIENT MAX SPEED 288 Mbps LEDS on ACCESS PO	2003 A0510, gwy2 up	2.4 GHz	
Applications Analyze Analyze Curve Events Events Tools	CLIENT USERNAME #088b-50c084 HOSTNAME ArtyaP IP ADDRESS 192.168.1.132 GLIDBAL UNICAST IPV6 ADDRESS CLIENT OS	CULENT TYPE Wireless MAC ADDRESS a0:88:b4:50:c0:84 LINK LOCAL IPV6 ADDRESS fe80:7244:207:955c CONNECTED SINCE	>>>>> Schoold UP Schoold UP NET VLA 192 AP CP-4 GT CP-4 SEG - - AU 192 SEG - - - - - - - - -	WORK V OLE Suest EWAY ROLE Suest MENTATION H SERVER		VLAN DERIVI UP VLAN DERIVI VSA AP DERIVITI SWITCH ROL 		CONNECTION CHANNEL 6 (20 MHz) CLIENT CAPABILITIE 802.11gn CLIENT MAX SPEED 288 Mbps LEDS on ACCESS PO	2003 A0510, gwy2 up	2.4 GHz	

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

aruba			Clear	Pass Policy Manager			Menu
- Dashboard	• Monitoring »	Live Monitoring » Acc	ess Tracker				
Monitoring	Access T	racker Mar 17, 202	Auto Refres				
Live Monitoring	The Access	Tracker page provides	a real-time display of per-se	ession access activity on the selected	server or domain.		
- Accounting 	T [All Rec	quests]	victory (192	2.168.1.95)	Last 1 day before Too	lay	Edit
- Analysis & Trending							
- 🔜 System Monitor 🛃 Profiler and Network Scan	Filter: Reques	st ID ,	contains ~	+ Go Clear Filter			Show 20 v reco
🖉 Audit Viewer	# Se	rver	Source	Username	Service	Login Status	Request Timestamp 🔹
Event Viewer Data Filters	1. 192	2.168.1.95	RADIUS	cpguser	GG User Authentication with MAC Caching	ACCEPT	2021/03/17 11:26:22
				a088b450c084	GG MAC Authentication		

Request Details		Reques	t Details							8
Summary Input Ou	Alerts	Sum	mary	Input	output	Alerts				
Login Status:	REJECT	Enforc	ement Pr	ofiles:	Deny Ac	cess Profile]				
Session Identifier:	R0000009-01-60514c96	System	n Posture	Status:						
Date and Time:	Mar 17, 2021 11:25:58 AEDT	Audit F	Posture S	tatus:	JNKNOWN	V (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	ords > > Show Configuration Export Show Logs Close	I4 ≤ Sh	howing 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 _____ Name Server Port Url Auth Text Redirect 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	Clients													hours	t Summ
- Manage	CLIENTS ALL	~ 0	;									8.	31 MB (🕀 1.	75 MB ⊕6.5	6 MB)
Devices		• Connecting	• Connected	• Failed	• Offli	ne 🤅	Blocked	Wireles		ired	Remote				
🗅 Clients	3	0	1	0	2		0	1		2	0				
😩 Guests															\odot
Applications		Status	1±	\mathbf{Y} IP Address		VLAN	Connected T	o	Y Gateway R	ple	▼ SSID/Port	∀ Health	~	Usage	
Security	cpguser	O Con	nected	192.168.1.132	1	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		ClearPass Policy Manager							
Dashboard O	Monitorin	ng » Live Monitoring	» Access Tracker						
Monitoring O	Acces	CCESS Tracker Mar 17, 2021 11:27:56 AEDT							
Live Monitoring Access Tracker	9 The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.								
- Jaccounting - Jaccounting OnGuard Activity	Accounting [All Requests] [1 victory (192.168.1.95) [10] Last 1 day bef						Edit		
Analysis & Trending									
	Filter: Re	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 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:		ACC	EPT	^			
Session Iden	tifier:	R000	0000a-01-60514cae				
Date and Tim	e:	Mar	17, 2021 11:26:22 AEDT				
End-Host Ide	ntifier:	A0-8	8-B4-50-C0-84				
Username:	Username:		iser				
Access Device IP/Port:		192.	192.168.1.242				
Access Devic	e Name:	AOS	AOS10-gateways				
System Postu	ure Status	: UNKI	NOWN (100)				
			Policies Used -				
Service:		<mark>GG L</mark>	Iser Authentication with MAC Caching				
Authenticatio	n Method	PAP					
Authenticatio	n Source:	Loca	l:localhost				
Authorization	Source:	[Gue	st User Repository], [Endpoints Repository], [Time Source]				
Roles:		[<mark>Gue</mark>	st], [User Authenticated]				
Enforcement			IAC Caching Bandwidth Limit. GG MAC Caching Session Limit. GG Guest MAC Change Status Show Configuration Export Show Logs	Close			

Summary	Input	Output	Accounting		
udit Posture	Status:	UNKNOW	N (100)		1
RADIUS Res	ponse			⊘	
Bandwidth-	Check:Allo	owed-Limit	0		1
Bandwidth-	Check:Ch	eck-Type	Today		
Bandwidth-	Check:Lim	nit-Units	MB		
Endpoint:G	uest Role 1	ID	2		
Endpoint:M	AC-Auth E	Expiry	2021-03-18 11:00:00		
Endpoint:U	sername		cpguser		
Expire-Time	-Update:(GuestUser	0		
Expiry-Che	ck:Expiry-	Action	0		
Post-Auth-	Check:Act	tion	Disconnect		
Post-Auth-	Check:Act	tion	Disconnect and Block Access		
Radius:Arul	ba:Aruba-l	User-Role	Guest		
Radius:IETI	Session-	Timeout	0		

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	•	Configuratio	on » Identity » Endpoints					
Monitoring	•	Endpoin	nts					👍 Add
A Configuration	o							🐣 Import 🏩 Export All
 —					ndpoints. An endpoint is a device that co rkstations, Internet-of-things (IoT) devic		h a network to which it is	
- 🖞 Authentication								
—🖧 Methods		Filter: MAC /	Address v conta	ains 🗸	+ Go Clear Filter			Show 20 ${\sim}$ records
- 🛱 Sources		#	MAC Address 🔺	Hostname	Device Category	Device OS Family	Status	Profiled
E Minuty			00-0C-29-F3-EF-AF	victory			Unknown	
- 🛱 Single Sign-On (SSO)		1.	00-0C-29-F3-EF-AF	VICTORY	Server	ClearPass	Unknown	Yes
-‡ Single Sign-On (SSO) -‡ Local Users		2.	A0-88-B4-50-C0-84	VICTORY	Computer	Windows	Known	Yes

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.

Login Status:	ACCEPT	^				0		
Session Identifier:	R0000000a-01-60514cae	_	Select Access Control T	ype: 🔾 Agent	SNMP RADIUS C	COA 🔾 Server Action	1	
Date and Time:	Mar 17, 2021 11:26:22 AEDT		RADIUS CoA Type:	[ArubaOS Wire	less - Terminat ∨			
End-Host Identifier:								
Username:	A0-88-84-50-C0-84							
	cpguser							
Access Device IP/Port:	192.168.1.242							
Access Device Name:	AOS10-gateways							
System Posture Status:	UNKNOWN (100)	- 1						
	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: I I I Showing 1 of 1-11 re equest Details Radius [Ar	ubaOS Wireless - Terminate Session] successful for client a088b450c084.	Close					Submit	Cance
Enforcement Profiles: I I I Showing 1 of 1-11 re lequest Details Radius [Ar Summary Input C	Change Status Show Configuration Export Show Logs ubaOS Wireless ~ Terminate Session] successful for Client a088b450c084. output Accounting	Close					Submit	Cance
Enforcement Profiles: I	Accept Change Status Show Configuration Export Show Logs	_					Submit	Cance
Enforcement Profiles: I	Accept Accept R0000000-01-60514cae Know Configuration	Close					Submit	Cance
Enforcement Profiles: I	Accept Roomonous - 01-60514cae Mar 17, 2021 11:26:22 AEDT	Close					Submit	Cance
Enforcement Profiles: A dequest Details Radius [Ar Summary Input C Login Status: Session Identifier: Date and Time: End-Host Identifier:	Acccept Romonogou-on-60514cae Mar 17, 2021 11:26:22 AEDT Ao-88-84-50-0C-84	Close					Submit	Cancel
Enforcement Profiles: A 4 Showing 1 of 1-11 re Request Details Radius [Ar Summary Input C Login Status: Session Identifier: Date and Time: End-Host Identifier: Username:	Accept Accounting R00000000-01-60514cae Mar 17, 2021 11:26:22 AEDT A0-88-84-50-C0-84 cpguser	Close					Submit	Cancel
Enforcement Profiles:	Accounting Accounting Accounting Mar 17, 2021 11:26:22 AEDT Ao-88-84-50-C0-84 Cpguser 192.168.1.242 Show Logs	Close					Submit	Cancel
Enforcement Profiles: A Showing 1 of 1-11 re Radius [Ar Summary Input C Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: Access Device Name:	Change Status Show Configuration Export Show Logs Marceunting Accept Accept R0000000-01-60514cae Ar-88-84-50-C0-84 Ap.98-84-50-C0-84 Cpguser 192.168.1.242 AOS10-gateways	Close					Submit	Cancel
Enforcement Profiles: A Showing 1 of 1-11 re Radius [Ar Summary Input C Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: Access Device Name:	Accept Knowless Accept Kooologa Mar 17, 2021 11:26:22 AEDT Ao-88-84-50-C0-84 Apsile 38-450-C0-84 Copuser 192.168.1.242 AoS10-gateways UNKNOWN (100) Vince 2000	Close					Submit	Cance
Enforcement Profiles: A Showing 1 of 1-11 re Radius [Ar Summary Input C Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: Access Device Name: System Posture Status:	Acccept Room of the second s	Close					Submit	Cance
Enforcement Profiles: A Showing 1 of 1-11 re equest Details Radius [Ar Summary Input C Login Status: Session Identifier: Date and Time: End-Host Identifier: JJsername: Access Device IP/Port: Access Device Name: System Posture Status: Service:	Acccept Romonopoint Export Show Logs Acccept Accept Accept Ansite Accept Accept Ansite Accept Accept Ansite Accept Accept Accept Accept Accept Accept Accept Accept Ansite Beat Accept Accept Accept Accept <td>Close</td> <td></td> <td></td> <td></td> <td></td> <td>Submit</td> <td>Cance</td>	Close					Submit	Cance
Enforcement Profiles: equest Details Radius [Ar Summary Input C Login Status: Session Identifier: Date and Time: End-Host Identifier: Jsername: Access Device IP/Port: Access Device Name: System Posture Status: Service: Authentication Method:	Accept Konstant Accept Accept R0000000a-01-60514cae Accept Mar 17, 2021 11:26:22 AEDT Accept A0-88-84-50-C0-84 Coguser 192.168.1.242 Aologa attraction MINKNOWN (100) VINKNOWN (100)	Close					Submit	Cance
Enforcement Profiles: equest Details Radius [Ar Summary Input C Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: Access Device Name: System Posture Status: Service: Authentication Method: Authentication Source:	Accept Show Configuration Export Show Logs Accept Accept R0000000a-01-60514cae Image: Status Image: Status Mar 17, 2021 11:26:22 AEDT A0-88-84-50-C0-84 Image: Status Image: Status 192,168.1.242 AO-30-gateways Image: Status Image: Status VNKNOWN (100) Image: Status Image: Status Image: Status GG User Authentication with MAC Caching Image: Status Image: Status Image: Status PAP Local-localhost Image: Status Image: Status Image: Status	Close					Submit	Cance
Enforcement Profiles: equest Details Radius [Ar Summary Input C Login Status: Session Identifier: Date and Time: End-Host Identifier: Username: Access Device IP/Port: Access Device Name: System Posture Status: Service: Authentication Method:	Accept Konstant Accept Accept R0000000a-01-60514cae Accept Mar 17, 2021 11:26:22 AEDT Accept A0-88-84-50-C0-84 Coguser 192.168.1.242 Aologa attraction MINKNOWN (100) VINKNOWN (100)	Close					Submit	Cance

aruba			Clear	Pass Policy Manager			Menu 📥
Dashboard	• Mon	itoring » Live Monitoring »	Access Tracker				
Monitoring	Ac	cess Tracker Mar 17	🔗 Auto Refresh				
	The	Access Tracker page pro	ides a real-time display of per-se	ssion access activity on the selected ser	ver or domain.		
		[All Requests]	victory (192	.168.1.95)	Last 1 day before Tod	Last 1 day before Today	
M Analysis & Trending System Monitor	Filte	r: Request ID	 ✓ contains ✓ 	⊕ Go Clear Filter			Show 20 v record
		Server	Source	Username	Service	Login Status	Request Timestamp 🔻
——————————————————————————————————————	1						
	1	100 100 1 05	RADIUS	cpguser	GG MAC Authentication	ACCEPT	2021/03/17 11:33:04
		192.168.1.95		cpguser cpguser	GG MAC Authentication GG User Authentication with MAC Caching	ACCEPT ACCEPT	2021/03/17 11:33:04 2021/03/17 11:26:22

Looking at the details of that session

Request Details			Request Details
Summary Input Ou	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 📀
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:	I Allow Access Profile1. GG Guest Device Profile ords ► ► Change Status Show Configuration Export Show Logs Clocenter	✓ose	

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

(7005_AOS10_gwy2) #sho This operation can tak		n number of us	ers. Please	be patient	
Users					
IP MA	.C Name	Role	Age(d:h:m)	Auth VPN	link
Connected To Roami mode Type Host Nam		Profile		Foi	rward
192.168.1.132 a0:88:b					
b4:5d:50:c6:82:4a Wi Win 10 WIR	reless Schoo-Guest ELESS	Schoo-Gues	t_#161593813	5060_41#_	<mark>dtunnel</mark>
User Entries: 1/1 Curr/Cum Alloc:1/6 Fr (7005_AOS10_gwy2) #	ee:0/5 Dyn:1 AllocErr	:0 FreeErr:0			