Contents

1.1	Revision History	1
2 De	emo Topology	2
7 Gu	uest Access Configuration	3
7.1	MM Guest Wireless Configuration	3
7.2	ClearPass Guest policy Configuration	6
7.3	ClearPass Guest Portal Configuration	11
7.4	Guest Testing	15
7.5	Captive Portal Server Certificate for MD	20
7.6	General Operation	23
8 Gu	uest Access with Terms of use	24
9 Gu	Jest Operator	
9.1	ClearPass Guest Operator Configuration	
10	Managed Network Dashboard	37

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
02 Feb 2021	0.1	Ariya Parsamanesh	Initial creation
11 Feb 2021	0.2	Ariya Parsamanesh	Added section 9-10
15 Feb 2021	0.3	Ariya Parsamanesh	Minor modifications

2 Demo Topology

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



This is the part 2 of the three parts series.

7 Guest Access Configuration

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

7.1 MM Guest Wireless Configuration

We'll go through the Tasks wizard

lanaged Network > Lab >					
	Q Dashboard	New WLAN			
obility Master					
anaged Network (2)	WLANs	General	VLANs	Securit	ty
	Roles & Policies				
	Access Points	Name (SSID): Guest			
	AP Groups	Primary usage: Employee	Guest		
	Authentication	Broadcast on: All APs	 ✓ 		
		Forwarding mode: Tunnel			
		Torwarding mode.			
		New WLAN			
		General	VLANs	Security	Access
		VLAN: 1 🗸			
		Character and share the			
		New WLAN			
		New WLAN	VLANS	Security	Access
		New WLAN	VLANS	Security Captive Portal (Access
		New WLAN General	VLANS	Security	Access Dptions:
		ClearPass or other exter	VLANS	Security Captive Portal (Access Options: ClearPass
		New WLAN General	VLANS	Security	Access Dptions: ClearPass
		New WLAN General ClearPass or other exter Internal Captive Portal wit Internal Captive Portal wit	VLANS nal Captive Portal	Security Captive Portal of Auth servers:	Access Options: ClearPass
		New WLAN General ClearPass or other exter Internal Captive Portal wit Internal Captive Portal wit	VLANS nal Captive Portal h authentication h email registration	Security Captive Portal of Auth servers:	Access Options:
		New WLAN General ClearPass or other exter Internal Captive Portal wit Internal Captive Portal, no	VLANS nal Captive Portal h authentication h email registration auth or registration	Security Captive Portal of Auth servers:	Access Dptions: ClearPass
		New WLAN General ClearPass or other exter Internal Captive Portal wit Internal Captive Portal wit Internal Captive Portal, no No Captive Portal	VLANS	Security Captive Portal of Auth servers:	Access Deptions: ClearPass +
		New WLAN General ClearPass or other exter Internal Captive Portal wit Internal Captive Portal wit Internal Captive Portal, no No Captive Portal	VLANS nal Captive Portal h authentication h email registration auth or registration	Security Captive Portal of Auth servers: Host addressing:	Access Dptions: ClearPass + Interpretation Description
		New WLAN General ClearPass or other exter Internal Captive Portal wit Internal Captive Portal wit Internal Captive Portal, no No Captive Portal	VLANS nal Captive Portal h authentication h email registration auth or registration	Security Captive Portal of Auth servers: Host addressing: Host:	Access Dptions: ClearPass I Pv4 IPv6 Victory.clearpass.inft
		New WLAN General ClearPass or other exter Internal Captive Portal wit Internal Captive Portal wit Internal Captive Portal, no No Captive Portal	VLANS nal Captive Portal h authentication h email registration auth or registration	Security Captive Portal of Auth servers: Host addressing: Host: Page:	Access Dptions: ClearPass I Pv4 IPv6 Victory.clearpass.infc /guest/school phn
		New WLAN General ClearPass or other exter Internal Captive Portal with Internal Captive Portal with Internal Captive Portal	VLANS	Security Captive Portal of Auth servers: Host addressing: Host: Page:	Access Dptions: ClearPass I Pv4 IPv6 Victory.clearpass.infr /guest/school.php
		New WLAN General ClearPass or other exter Internal Captive Portal wit Internal Captive Portal wit No Captive Portal	VLANS	Security Captive Portal of Auth servers: Host addressing: Host: Page: Redirect URL:	Access Deptions: ClearPass ClearPass IPv4 IPv6 Victory.clearpass.infc /guest/school.php http://www.network;
		New WLAN General ClearPass or other exter Internal Captive Portal wit Internal Captive Portal, no No Captive Portal	VLANS	Security Captive Portal of Auth servers: Host addressing: Host: Page: Redirect URL: Use purple wi-fi:	Access Deptions: ClearPass Prove Pr
		New WLAN General ClearPass or other exter Internal Captive Portal wit Internal Captive Portal, no No Captive Portal	VLANS	Security Captive Portal of Auth servers: Host addressing: Host: Page: Redirect URL: Use purple wi-fi:	Access Deptions: ClearPass Prove Pr
		New WLAN General ClearPass or other exter Internal Captive Portal wit Internal Captive Portal wit Internal Captive Portal mit	VLANS	Security Captive Portal of Auth servers: Host addressing: Host: Page: Redirect URL: Use purple wi-fi:	Access
		New WLAN General ClearPass or other exter Internal Captive Portal wit Internal Captive Portal wit Internal Captive Portal nor No Captive Portal	VLANS	Security Captive Portal of Auth servers: Host addressing: Host: Page: Redirect URL: Use purple wi-fi: Security	Access

So, once you deploy the configurations, the wizard created a authentication server group.

Managed Network > Lab >						¢
Dashboard Configuration	Auth Servers AAA Profile:	5 L2 Authentication L	3 Authentication User Ru	ules Advanced		
WLANs	Server Groups 4					
Roles & Policies	NAME	SERVERS	FAIL THROUGH	LOAD BALANCE	SERVER RULES	=
Access Points	default	2			1	A
AP Groups	internal	1	-	-	1	
	school_dot1_svg	1			1	
Authentication	Guest_dot1_svg	1	-	-	0	<u> </u>
Services	+					
Interfaces						
Controllers	Server Group > Guest_dot1_s	svg Servers Options	Server Rules			i Drag rows to re-order
System	NAME	TYPE	IP ADDRESS	TRIM FQDN	MATCH RULES	
Tasks	ClearPass	RADIUS	<mark>192.168.1.95</mark>	-	0	

It also created an AAA profile with initial user role as "Guest-guest-logon". This user role will only provide access to DHCP, DNS and redirection to ClearPass

Managed Network > Lab >			
ashboard	Auth Servers AAA Profiles L2 Au	thentication L3 Authentication User Rules Advance	ced
onfiguration			
WLANs	AAA Profiles	AAA Profile: Guest_aaa_prof	
Roles & Policies		Initial role:	Guest-guest-logon
Access Points	⊖ 🕞 Guest_aaa_prof	MAC Authentication Default Role:	
AP Groups	802.1X Authentication		Bacar
Authentication	🕒 802.1X Authentication S	Server Group 802.1X Authentication Default Role:	guest 🗸
Services	MAC Authentication	Download Role from CPPM:	
Interfaces	MAC Authentication Ser	rver Group Set username from dhcp option 12:	
Controllers	🕞 RADIUS Accounting Ser	ver Group	
Svstem	RFC 3576 server	with the server Accounting.	
Tasks	TML API server	User lale timeout:	seconds
Redundancy	⊕	Max IPv4 for wireless user:	2
InT	🕀 🖻 default	RADIUS Roaming Accounting:	
	⊕ default-dot1x	RADIUS Interim Accounting:	
Intenance	⊕ default-dot1x-psk	RADIUS Acct-Session-Id In Access-Request	t:
	🕀 📑 default-iap-aaa-prof	User derivation rules:	-None- 💙

Now because we want to also enable MAC caching for the guest users, we need to add a MAC Authentication profile along with Auth server and accounting server groups for it. The aim of this workflow is that a new guest user gets redirected to captive portal on ClearPass and will use username/password or accepts term and conditions and gets in. Then for a specific period of time, if the same guest users disconnects and reconnects, will not get the captive portal again and will be MAC authenticated.

Managed Network > Lab >				
Dashboard A	Auth Servers AAA Profiles L2 Authentication	L3 Authentication User Rules Advanced		
Configuration				
WLANs	AAA Profiles	MAC Authentication Profile: default		
Roles & Policies				
Access Points	⊖ 📑 Guest_aaa_prof	MAC Authentication Profile:		
AP Groups	802.1X Authentication	Delimiter:	none 🗸	
Authentication	802.1X Authentication Server Group	Carrie	lauran bi	
Services	G MAC Authentication	Case.	lower 🗸	7
Interfaces	MAC Authentication Server Group	Max Authentication failures:	0	
Controllers	RADIUS Accounting Server Group	Reauthentication:		
System	RFC 3576 server	Reauthentication Interval:	86400	sec
Tasks	TML API server	Use Server provided Reauthentication Interval:		
	O NoAuthAAAProfile			

Dathband Auf. Srove AAA Porlies 2. Authonication Server Group: Gener, Gene	Managed Network > Lab >	
Configuration MA frontis: WLANs AA frontis: ALL Server Group: Guest dott seg A Groups Baile & Fallence A Groups Baile & Controllers Server Group Guest dott seg Controllers System Tasks	Dashboard	Auth Servers AAA Profiles 1.2 Authentication 1.3 Authentication User Rules Advanced
WLAIS AM Frofile: Roles & Policies Access Policies Access Policies Access Policies Ar Groups Ant Controllers System Controllers System Tatks	Configuration	
Roles & Policies Access Policies Active Configuration Banaged Network > Lab >	WLANs	AAA Profiles Server Group: Guest_dot1_svg
Access Points ACcess Points Arcess Points	Roles & Policies	
A P Groups A P Groups Services Controllers System Controllers Controllers System Controllers Con	Access Points	⊘ Guest_aaa_prof
Authentication Services Interfaces Controllers System Tasks	AP Groups	802.1X Authentication Fail Through:
Services McAuthentication McCathentication WCAthentication System Tasks Managed Network > Lab > Dashboard McAthentication WLANs Roles & Policies Access Polints Access Polints Access Polints Services Bothboard Authentication Services Bothboard Authentication WLANs Roles & Polints Access Polints Access Polints Authentication Services Bothboard Authentication Services Managed Network > Lab > Services System System Southentication Services Southentication Southentication Services Southentication Southentica	Authentication	802.1X Authentication Server Group Load Balance:
Interfaces Managed Network > Lab > Dashboard Auth Servers AAA Profile: Controuters: Managed Network > Lab > Dashboard Auth Servers AAA Profile: Controuters: Managed Network > Lab > Dashboard Auth Servers AAA Profile: Controuters: Managed Network > Lab > WLANS Configuration Configuration Controuters: Servers: Managed Network > Lab > 	Services	MAC Authentication
Controllers System Tasks Controllers Managed Network > Lab > Dashbaard Configuration WLANS Roles & Policies A AA Profiles Roles & Policies A AA Profiles Configuration Services Interfaces Controllers System Tasks Configuration Managed Network > Lab > Dashbaard Auth Servers MAA Profiles Configuration Services Interfaces Controllers System Tasks Configuration Managed Network > Lab > Dashbaard Auth Servers Configuration Managed Network > Lab > Dashbaard Managed Network > Lab > Dashbaard Auth Servers AAA Profiles Configuration Managed Network > Lab > Dashbaard Auth Servers Auth Servers Auth Servers Auth Servers Auth Servers Auth Servers Auth Servers Auth Servers Configuration Managed Network > Lab > Dashbaard Auth Servers Auth Servers Auth Servers Configuration Managed Network > Lab > Dashbaard Auth Servers Auth Servers Auth Servers Configuration Managed Network > Lab > Dashbaard Auth Servers Auth Servers Auth Servers Configuration Auth Servers Configuration Configuration Auth Servers Configuration Configuration Auth Servers Configuration Configu	Interfaces	G MAC Authentication Server Group
System Tasks Managed Network > Lab > Dashboard Mul API server Mul API ser	Controllers	RADIUS Accounting Server Group
Tasks Managed Network > Lab > Dashboard Configuration VLANs Access Points AP Groups Interfaces Controllers System Tasks Managed Network > Lab > Managed Network > Lab > Auth Servers AAA Profiles Interfaces Controllers System Tasks Managed Network > Lab > Managed Network > Lab > Managed Network > Lab > Controllers System Tasks Managed Network > Lab > Mathematication Services Auth Servers AAA Profiles Interfaces Controllers System Tasks Managed Network > Lab > Managed Network > Lab > MuthArritation Server Group Managed Network > Lab > Controllers System Tasks Managed Network > Lab > Deshboard Auth Servers AAA Profiles La Authentication Services Auth Servers AAA Profiles La Authentication Services Managed Network > Lab = MuthArritation	System	🕒 RFC 3576 server
Managed Network > Lab > Dashboard Configuration WLANS Roles & Policies Access Points Arth Servers Authentication Server Group: Controllers System Tasks Managed Network > Lab > Auth Servers Auth Servers Services Interfaces Controllers System Tasks Managed Network > Lab > Auth Servers AAA Profiles L2 Authentication Server Group: Managed Network > Lab > Auth Servers AAA Profiles L2 Authentication Managed Network > Lab > Auth Servers AAA Profiles L2 Authentication Managed Network > Lab > Auth Servers RC 3576 Server Services Managed Network > Lab > <td>Tasks</td> <td>C XML API server</td>	Tasks	C XML API server
Dashboard Configuration WLANS Roles & Policies Access Points AP Groups Services Interfaces Configuration Services Interfaces MAAP Pofilies L2 Authentication Server Group MAAP configuration	Managed Network > Lab >	
Auth Servers AAA Profiles L2 Authentication USer Rules WLANs Roles & Policies Access Points Access Points Ar Groups B02.1X Authentication Services Interfaces Controllers System Tasks Managed Network > Lab > Deshboard AAA Profiles AAA Profiles Configuration Managed Network > Lab > Managed Network > Lab > Deshboard MLANs Access Points AAA Profiles L2 Authentication System Tasks Auth Servers AAA Profiles L2 Authentication Services Managed Network > Lab > AAA Profiles Auth Servers AAA Profiles L2 Authentication Services Interfaces O Auth Servers AAA Profiles L2 Authentication Services Interfaces O Authentication Services Interfaces O Managed Network > Lab >	Dashboard	
WLAN WLAN Roles & Policies Access Points Access Points Access Points Botter & B	Configuration	Auth Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced
Roles & Policies Access Politis Access Politis Access Politis Access Politis Access Politis Access Politis Below Resource Bel	WIANC	AAA Profiles Server Group: Guest dot1 svg
Access Points Ac	Roles & Policies	
AP Groups AP Groups Authentication Services Interfaces Controllers System Tasks Managed Network > Lab > Dashboard Configuration WLANS Roles & Policies Access Points Access	Access Points	O ☐ Guest_daaa prof Server Group: Guest_dot1_svg ✓
Authentication Services Interfaces Controllers System Tasks	AP Groups	South Authentication South Authentication South Authentication
Services Interfaces	Authentication	802.1X Authentication Server Group
Jervites Interfaces Controllers System Tasks	Services	MAC Authentication
Interfaces Controllers System Tasks	Interfaces	AC Authentication Server Group
System Tasks Managed Network > Lab > Dashboard Configuration MLANs Roles & Policies Access Points Access Points Access Points AP Groups Authentication Services Interfaces MAC Authentication MAC Authentication MAC Authentication MAC Authentication MAC Authentication MAC Authentication Server Group MAC Authentication	Controllers	🕞 RADIUS Accounting Server Group
Tasks Managed Network > Lab > Dashboard Auth Servers AAA Profiles L2 Authentication User Rules Advanced AAA Profiles L2 Authentication WLANs AAA Profiles AAA Profiles L2 Authentication User Rules Advanced RFC 3576 Server: Image: Caster and Cas	System	🕞 RFC 3576 server
Managed Network > Lab > Dashboard Auth Servers AAA Profiles L2 Authentication ULANS AAA Profiles AAA Profiles Configuration WLANS AAA Configuration Configuration <td< td=""><td>Tasks</td><td>C XML API server</td></td<>	Tasks	C XML API server
Dashboard Auth Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced Configuration WLANs Roles & Policies Access Points Access Points Access Points B02.1X Authentication B02.1X Authentication B02.1X Authentication Services MAC Authentication MAC Authentication Server Group RFC 3576 server: +		
Auth Servers AAA Profiles L2 Authentication WLANs AAA Profiles Roles & Policies Access Points ACcess Points B02.1X Authentication B02.1X Authentication B02.1X Authentication B02.1X Authentication Services MAC Authentication Interfaces		
MLANS AAA Profiles RFC 3576 Server Roles & Policies Image: AAA Image: RFC 3576 Server Access Points Image: RFC 3576 Server Image: RFC 3576 Server A Groups Image: RFC 3576 Server Image: RFC 3576 Server Authentication Image: RFC 3576 Server Image: RFC 3576 Server Services Image: RFC 3576 Server Image: RFC 3576 Server Interfaces Image: RFC 3576 Server Image: RFC 3576 Server	Castiguration	Auth Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced
Roles AAA FFC 3576 SERVER Access Points Image: Bool 1X Authentication AP Groups Bool 1X Authentication Authentication Bool 1X Authentication Services Image: MAC Authentication Server Group Interfaces Image: MAC Authentication Server Group	WIANS	AAA Profiles RFC 3576 Server
Note of Folders O is MAX RFC 3576 SERVER Access Points 	Roles & Policies	
ALCESS Folints O C I Structure price AP Groups 802.1X Authentication 802.1X Authentication Server Group RFC 3576 server: Authentication Services Interfaces	Access Boints	C I STORE REC 3576 SERVER
Authentication Image: Boole Bo	AR Groups	Solution
Services MAC Authentication Interfaces	Authentication	RFC 3576 server:
Interfaces MAC Authentication Server Group +	Somisos	G MAC Authentication
Interfaces	Jetovfesos	MAC Authentication Server Group
Controllars	Controllers	RADIUS Accounting Server Group
Controllers Controllers	Controllers	🕒 RFC 3576 server
System Table	System	TML API server

Next, we'll do some fine tuning on Captive portal profile that was created by the wizard. We'll reduce the redirect pause to 1 sec fand uncheck "logout popup window"

■ Managed Network > Lab >			
	Auth Servers AAA Profiles L2 Authentication	L3 Authentication User Rules Advanced	
	L3 Authentication	Captive Portal Authentication Profile: Guest_cppn	n_prof
Roles & Policies	⊖ 🕒 Captive Portal Authentication	Default Role:	guest 🗸
	⊖ 🗗 Guest_cppm_prof	Default Guest Pole:	guost V
	🕒 Server Group	Deladit Gdest Kole.	guesi
	🕀 🖻 default	Redirect Pause:	1 sec
	Stateful Kerberos Authentication	User Login:	
	⊕	Guest Login:	
	⊕	Logout popup window:	
	⊕	Ose HTTP for authentication:	_
	⊕	Logon wait minimum wait:	5 sec
	VPN Authentication	Logon wait maximum wait:	10 sec
loT	⊕	logon wait CPU utilization threshold:	60 %
		Max Authentication failures:	0

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 it is highly recommended to have a public cert for the controllers as well as ClearPass nodes.

7.2 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 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.
- Control of the sign-On (SSO)	Encrypted Wireless Access via 802.1X Public PEAP method 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 School State	Guest Access - Web Login To authenticate guest users logging in via guest portal.
Policies Profiles	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").
- - Event Sources Network Scan Policy Simulation	Onboard Service template for authorizing device credential provisioning and onboarding.
🖓 Administration 🛛 🛛 🖉	Onboard Services Only Service template for authorizing device credential and onboarding

Configuration » Service Templates & Wizards

Service Templates - Guest Authentication with MAC Caching

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

General	Wireless Net	work Settings	MAC Caching Settings	Posture Settings	Access Restrictions
Enable Pos	ture Checks	to perform hea	alth checks after authe	entication.	
Enable Post	ure Checks:	Configure G	uest Web Login page		

K Back to S	ervice Templates & Wizards	Delete Next → Add Service Car	cel				
General	Wireless Network Settings	MAC Caching Settings Posture Settings Access Restrictions					
• Enfor • Captiv • At lea	 Enforcement Type applies to the Captive Portal Access, Employee Access, Guest Access, and Contractor Access fields. Captive Portal Access is used for unauthenticated users and after the MAC caching duration has expired. At least one of Employee, Guest, and Contractor Access must be provided. 						
Enforcement	t Type <mark>*</mark> :	Aruba Role Enforcement					
Captive Port	al Access*:	Guest-guest-logon					
Days allowe	d for access <u>*</u> :	🗹 Monday 🗹 Tuesday 🗹 Wednesday 🖾 Thursday 🖾 Friday 🖾 Saturday 🖾 Sunday					
Maximum n	umber of devices allowed per u	er <u>*</u> : 5					
Maximum ba	andwidth allowed per user*:	0 MB (For unlimited bandwidth, set value to 0)					
Employee A	ccess:	Employee-Guest					
Guest Acces	s:	Guest					
Contractor A	Access:	Contractor					
K Back to S	ervice Templates & Wizards		icel				

Services



- Added 15 Enforcement Profile(s)
- Added 2 Enforcement 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)	
3.		3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	\bigcirc
4.		4	[Guest Operator Logins]	Application	Aruba Application Authentication	\bigcirc
5.		5	[Insight Operator Logins]	Application	Aruba Application Authentication	O
6.		6	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	\bigcirc
7.		7	AA Aruba 802.1X Wireless	RADIUS	Aruba 802.1X Wireless	\bigcirc
8.		8	GG MAC Authentication	RADIUS	MAC Authentication	\bigcirc
9.		9	GG User Authentication with MAC Caching	RADIUS	RADIUS Enforcement (Generic)	

We'll look at the MAC authentication service

Services - GG MAC Authentication

Note: This Service is created by Service Template

Summary	Service	Authentication	Authorization	Roles	5 Enforcement			
Name: GG MAC Authentication								
Description: MAC Authentication bypass for captive portal users								
Type: MAC Authentication								
Status:		Enabled						
Monitor Mode	:	Enable to m	onitor network a	ccess wit	ithout enforcement			
More Options:	More Options: 🛛 Authorization 🗋 Audit End-hosts 🗋 Profile Endpoints 🗋 Accounting Proxy							
Service Rule								
Matches O A	Matches 🔿 ANY or 🖲 ALL of the following conditions:							

	Туре	Name	Operator	Value	
1.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}	Ť
2.	Radius:Aruba	Aruba-Essid-Name	EQUALS	Guest	Ť
3.	Click to add				

Summary	Service	Authentication	Authorization	Roles	Enforcement	
Authentication	n Methods:	[Allow All MAC	AUTH]	^		Add New Authentication Method
					Move Up ↑	
					Move Down ↓	
					Remove	
					View Details	
					Modity	
		Select to Add		~		
Authenticatio	n Sources:	[Endpoints Ren	ository] [Local SOL]	Add New Authentication Source
		[Endpoints Rep		00]	Move Up ↑]
					Move Down ↓	
					Remove	
					View Details	
					Modify	
		Select to Add		\vee	~	
Summary	Service	Authentication	Authorization	Roles	Enforcement	
Authorization	Details:	Authorization s	sources from whic	h role ma	pping attributes ar	e fetched (for each Authentication Source)
		Authent	ication Source			Attributes Fetched From
		1. [Endpoin	ts Repository] [Lo	ocal SQL D	•B]	[Endpoints Repository] [Local SQL DB]
		Additional auth	orization sources	from which	ch to fetch role-ma	pping attributes -
		[Time Source] [Local SQL DB]	^	Remove	Add New Authentication Source
		[Guest User Rep	ository] [Local SQL	DB]	View Details	
				~	Modify	
		Select to Add-	-		~	
Summary	Service	Authentication	Authorization	Roles	Enforcement	
Role Mapping	Policy:	GG MAC Authent	ication Role Mapping	9	 ✓ Modif 	Add New Role Mapping Policy
		L		Ro	le Mapping Policy D	etails
Description:						
Default Role:		[Other]				
Rules Evaluati	on Algorithn	n: evaluate-all				
Conditio	ons					Role
AND (Authorizatio	n:[Time Source]:	Now DT LESS_TH	ount <i>EXIS</i> IAN %{Er	ndpoint:MAC-Auth	
1. Expiry})	Authorizatio	n:[Guest User Rei	pository1:Account	Expired <i>E</i>	OUALS false)	[MAC Caching]
AND (Authorizatio	n:[Guest User Re	pository]:Account	Enabled E	QUALS true)	
2. (Endpoir	t:Guest Role	E ID EQUALS 1)				[Contractor]
4. (Endpoir	t:Guest Role	e ID EQUALS 2)				[Guest] [Employee]
						[]
Summary	Service	Authentication	Authorization	Roles	nforcement	
Use Cached Re	esults:	Use cached R	oles and Posture a	attributes f	from previous sess	ions
Enforcement P	olicy:	GG MAC Authenti	cation Enforcement	Policy	~ M	odify Add New Enforcement Policy
D				Enf	forcement Policy De	tails
Description:			Profile]			
Rules Evaluati	on Algorithm	1: first-applicable	ronicj			
Conditio	ons					Enforcement Profiles
(Tips:R 1. [Guest]	ole MATCHE	S_ALL [MAC Cac	hing]			[Allow Access Profile], GG Guest Device Profile
[User Au (Tips:R 2 [Employ:	thenticated] ole MATCHE) <mark>S_ALL</mark> [MAC Cac	hing]			[Allow Acress Profile] GG Employee Davice Profile
[User Au	thenticated]		hinal			pairon Access Fromes, do Employee Device Prome
3. [Contrac [User Au	tor] thenticated])				[Allow Access Profile], GG Contractor Device Profile
(Tips:R 4. [Contrac [Employe	ole <i>MATCHE</i> tor] ee])	S_ANY [Guest]				[Allow Access Profile], GG Captive Portal Profile
Sack to Second Secon	ervices					Disable Copy Save Cancel

And here are the enforcement profiles that are used here.

Summary Profile	Attributes			
Profile:				
Name:	GG Guest I	Device Profile		
Description:	Role/VLAN	enforcement for Guest		
Type:	RADIUS			
Action:	Accept			
Device Group List:	-			
Attributes:				
Туре		Name	Value	
1. Radius:Aruba		Aruba-User-Role	= Guest	
2. Radius:IETF		User-Name	= %{Endpoint:U	sername}
Summary Profile	Attributes			
Profile:				
Name:	GG Employ	ee Device 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-Gu	iest
2. Radius:IETF		User-Name	= %{Endpoint:	Username}
	A			
Summary Profile	Attributes			
Profile:				
Name:	GG Contrac	tor Device Profile		
Description:	Role/VLAN	enforcement for Contractor		
Type:	RADIUS			
Action:	Ассерг			
Device Group List.				
Attributes:			× 1	
I ype		Name	Value	
2 Radius: IETE		Aruba-User-Role	= Contractor	sername}
2. Radius.iem		User Name		semaney
Summary Profile	Attributes			
Profile:				
Name:	GG Capt	ive Portal Profile		
Description:	Captive	Portal Role/VLAN enforcement		
Type:	RADIUS			
Action:	Accept			
Device Group List:	-			
Attributes				
Attributes:				
The second secon				
Type		Aruba User Dela		uppt long

Next, we'll look at the User Authentication with MAC caching service

Services - GG User Authentication with MAC Caching

	Note: This Service is created by Service Template								
Su	mmary Service	Authentication	Authorization	Roles	Enforcement				
Nam	Name: GG User Authentication with MAC Caching								
Desc	Description: Captive Portal authentication with MAC Caching								
Туре		RADIUS Enforce	ement (Generic)					
State	us:	Enabled							
Moni	itor Mode:	Enable to me	onitor network a	ccess wit	hout enforcement				
More	Options:	Authorizatio	n 🗆 Posture Co	mpliance	Audit End-host	Profile Endpo	oints 🗆 Accounting Proxy		
					Service Rule				
Matc	hes 🔿 ANY or 🖲 A	LL of the following	conditions:						
	Туре		Name	_	Оре	rator	Value		
1.	Radius:IETF		Calling-Station	-Id	EXI	STS		B	Ť
2.	Connection		Client-Mac-Ade	lress	NOT	_EQUALS	%{Radius:IETF:User-Name}		Ť
3.	Radius:Aruba		Aruba-Essid-Name EQUALS Guest		ß	Ť			
4.	Click to add								

Summary Service	Authentication Authorization Roles En		
Authentication Methods:	[PAP]		Add New Authentication Method
	[MSCHAP]	Move Up ↑	
	[CHAP]	Nove Down	
		Remove	
		View Details	
		Modify	
	Select to Add ~		
Authentication Sources:			Add New Authentication Source
	[duest oser Repository] [Local SQL DD]	Maria IIa A	
		View Details	
		Modify	
		mouny	
	Soloct to Add		
	Select to Ada		
Summary Service	Authentication Authorization Roles Enf	orcement	
uthorization Details:	Authorization sources from which role mappin	g attributes are fetched (for each Authenticatio	n Source)
	Authentication Source	Attributes Fetched F	rom
	1. [Guest User Repository] [Local SQL DB]	[Guest User Repository	/] [Local SQL DB]
	Additional authorization sources from which to	o fetch role-mapping attributes -	Add New Authentication Source
	[Endpoints Repository] [Local SQL DB]	move	Add New Addiendcation Source
	Vie	w Details	
	Dia Contractione de la contractica de la con		
	V MO	dify	
	Select to Add	dify	
	Select to Add	dify	
Summary Service	-Select to Add- Authorization Roles Enformation	orcement	
Summary Service	Authentication Authorization Roles Enfo GG User Authentication with MAC Caching Role Map	orcement pping ~ Modify	Add New Role Mapping Policy
Summary Service kole Mapping Policy:	Authentication Authorization Roles Enfo GG User Authentication with MAC Caching Role Map Role Map	orcement ping Modify Apping Policy Details	Add New Role Mapping Policy
Summary Service tole Mapping Policy: Description:	Authentication Authorization Roles Enfo GG User Authentication with MAC Caching Role Map Role M	orcement pping ~ Modify Mapping Policy Details	Add New Role Mapping Policy
Summary Service tole Mapping Policy: Description: Default Role:	Authentication Authorization Roles Enfr GG User Authentication with MAC Caching Role Map Role M [Other]	orcement pping ~ Modify Mapping Policy Details	Add New Role Mapping Policy
Summary Service ole Mapping Policy: Description: Default Role: ules Evaluation Algorithm	Authentication Authorization Roles Enfr GG User Authentication with MAC Caching Role Map Role Map (Other) n: evaluate-all	orcement pping ~ Modify Mapping Policy Details	Add New Role Mapping Policy
Summary Service ole Mapping Policy: Description: Default Role: ules Evaluation Algorithm Conditions	Authentication Authorization Roles Enf GG User Authentication with MAC Caching Role Map Role Map (Other) n: evaluate-all	orcement pping Modify Mapping Policy Details Role	Add New Role Mapping Policy
Summary Service ole Mapping Policy: Pescription: Pefault Role: Lules Evaluation Algorithm Conditions (GuestUser:Role ID	Authentication Authorization Roles Enfr GG User Authentication with MAC Caching Role Map Role M [Other] m: evaluate-all EQUALS 1)	orcement opping Modify Apping Policy Details Role [Contractor]	Add New Role Mapping Policy
Summary Service ole Mapping Policy: Pescription: Pefault Role: Lules Evaluation Algorithm Conditions (GuestUser:Role ID (GuestUser:Role ID	Authentication Authorization Roles Enfo GG User Authentication with MAC Caching Role Map Role	orcement pping Modify Apping Policy Details Role [Contractor] [Guest]	Add New Role Mapping Policy
Summary Service iole Mapping Policy: Description: Default Role: tules Evaluation Algorithm Conditions (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID)	Authentication Authorization Roles Enfo GG User Authentication with MAC Caching Role Mag Role	orcement pping Modify Apping Policy Details Role [Contractor] [Guest] [Employee]	Add New Role Mapping Policy
Summary Service tole Mapping Policy: Description: Default Role: Lules Evaluation Algorithm Conditions (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID	Authentication Authorization Roles Enfr GG User Authentication with MAC Caching Role Map Role M [Other] m: evaluate-all EQUALS 1) EQUALS 2) EQUALS 3)	orcement pping Modify Apping Policy Details Role [Contractor] [Guest] [Employee]	Add New Role Mapping Policy
Summary Service iole Mapping Policy: Description: Default Role: Utues Evaluation Algorithm Conditions (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID)	Authentication Authorization Roles Enf GG User Authentication with MAC Caching Role Map Role M	orcement pping Modify Mapping Policy Details Role [Contractor] [Guest] [Employee] orcement	Add New Role Mapping Policy
Summary Service befault Role: Conditions (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID (Summary Service) Jse Cached Results: Efformance Role Role	Authentication Authorization Roles Enf GG User Authentication with MAC Caching Role Map Role N [Other] n: evaluate-all EQUALS 1) EQUALS 2) EQUALS 3) Authentication Authorization Roles Enf Use cached Roles and Posture attributes from	orcement pping Modify Mapping Policy Details Role [Contractor] [Guest] [Employee] orcement m previous sessions	Add New Role Mapping Policy
Summary Service ole Mapping Policy: befault Role: tules Evaluation Algorithm (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID Summary Service Jse Cached Results: inforcement Policy:	Authentication Authorization Roles Enf GG User Authentication with MAC Caching Role Map Role Map Role Map [Other]	orcement pping Modify Mapping Policy Details Role [Contractor] [Guest] [Employee] orcement m previous sessions ment Policy Modify	Add New Role Mapping Policy
Summary Service Lole Mapping Policy: Description: Default Role: tutes Evaluation Algorithm (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID Summary Service Jse Cached Results: Enforcement Policy:	Authentication Authorization Roles Enf GG User Authentication with MAC Caching Role Map Role N (Other] n: evaluate-all EQUALS 1) EQUALS 2) EQUALS 3) Authentication Authorization Roles Enf Use cached Roles and Posture attributes from GG User Authentication with MAC Caching Enforcem Enfor	orcement pping Modify Apping Policy Details Role [Contractor] [Guest] [Employee] orcement m previous sessions net Policy Details	Add New Role Mapping Policy
Summary Service tole Mapping Policy: Description: Default Role: tules Evaluation Algorithm Conditions (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID) Summary Service Jse Cached Results: Enforcement Policy: Description:	Authentication Authorization Roles Enf GG User Authentication with MAC Caching Role Map Role N [Other] n: evaluate-all EQUALS 1) EQUALS 2) EQUALS 2) EQUALS 3) Authentication Authorization Roles Enf Use cached Roles and Posture attributes from GG User Authentication with MAC Caching Enforcem Enfor	orcement pping Modify Apping Policy Details Role [Contractor] [Guest] [Employee] orcement m previous sessions ment Policy Vetails	Add New Role Mapping Policy
Summary Service iole Mapping Policy: bescription: vescription: vescription: vescription: Conditions (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID Summary Service Ise Cached Results: inforcement Policy: Description: Description:	Authentication Authorization Roles Enf GG User Authentication with MAC Caching Role Map Role N Role N [Other]	orcement pping Modify Apping Policy Details Role [Contractor] [Guest] [Employee] orcement m previous sessions ment Policy V Modify cement Policy Details	Add New Role Mapping Policy
Summary Service tole Mapping Policy: bescription: >efault Role: tules Evaluation Algorithm Conditions (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID Summary Service Jse Cached Results: inforcement Policy: Description: Description: Default Profile: Rules Evaluation Algorithm	Authentication Authorization Roles Enf GG User Authentication with MAC Caching Role Map Role N (Other] m: evaluate-all EQUALS 1) EQUALS 2) EQUALS 2) EQUALS 3) Authentication Authorization Roles Enf Use cached Roles and Posture attributes from GG User Authentication with MAC Caching Enforcem Enform [Allow Access Profile] m: first-applicable	orcement ping Modify Apping Policy Details Role [Contractor] [Guest] [Employee] orcement m previous sessions nent Policy Vetails cement Policy Details	Add New Role Mapping Policy
Summary Service ole Mapping Policy: Description: Default Role: Utels Evaluation Algorithm Conditions (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID Summary Service Dise Cached Results: Enforcement Policy: Description: Default Profile: Rules Evaluation Algorithm Conditions	Authentication Authorization Roles Enf GG User Authentication with MAC Caching Role Map Role N (Other] m: evaluate-all EQUALS 1) EQUALS 2) EQUALS 2) EQUALS 3) Authentication Authorization Roles Enf Use cached Roles and Posture attributes from GG User Authentication with MAC Caching Enforcem Enform (Allow Access Profile) m: first-applicable	orcement ping Modify Apping Policy Details Role [Contractor] [Guest] [Employee] orcement m previous sessions ment Policy Details Enforcement Policy Details	Add New Role Mapping Policy
Summary Service Role Mapping Policy: Description: Default Role: Rules Evaluation Algorithm Conditions (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID Summary Service Jse Cached Results: Enforcement Policy: Description: Default Profile: Rules Evaluation Algorithm Conditions 1.	Authentication Authorization Roles Enf GG User Authentication with MAC Caching Role Map Role N [Other] m: evaluate-all EQUALS 1) EQUALS 2) EQUALS 2) EQUALS 3) Authentication Authorization Roles Enf Use cached Roles and Posture attributes fro GG User Authentication with MAC Caching Enforcem Enfor [Allow Access Profile] m: first-applicable	orcement pping ~ Modify Aapping Policy Details Role [Contractor] [Guest] [Employee] orcement m previous sessions nent Policy ~ Modify cement Policy Details	Add New Role Mapping Policy
Summary Service tole Mapping Policy: Description: Default Role: Utules Evaluation Algorithm Conditions (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID Summary Service Jse Cached Results: Enforcement Policy: Description: Default Profile: Rules Evaluation Algorithm Conditions 1. (Authorization:[Er (Tips:Role E0UMI	Authentication Authorization Roles Enf GG User Authentication with MAC Caching Role Map Role N (Other] m: evaluate-all EQUALS 1) EQUALS 2) EQUALS 2) EQUALS 3) Authentication Authorization Roles Enf Use cached Roles and Posture attributes fro GG User Authentication with MAC Caching Enforcem Enfor [Allow Access Profile] m: first-applicable Authorization GREA S [Employee])	orcement ping Modify Apping Policy Details	Add New Role Mapping Policy Add New Enforcement Policy Add New Enforcement Policy Contemporation of the second sec
Summary Service Lole Mapping Policy: Description: Default Role: Conditions (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID) (GuestUser:Role ID) Summary Service Description: Default Profile: Rules Evaluation Algorith Conditions 1. (Authorization:[Er 2. ANO (Date:Day)	Authentication Authorization Roles Enf GG User Authentication with MAC Caching Role Mag Role 1 [Other] m: evaluate-all EQUALS 1) EQUALS 2) EQUALS 2) EQUALS 3) Authentication Authorization Roles Enf GG User Authentication with MAC Caching Enforcem Enfor [Allow Access Profile] m: first-applicable dpoints Repository]:Unique-Device-Count GREA S [Employee]) of-Week BELONGS_TO	orcement pping ✓ Modify 4apping Policy Details	Add New Role Mapping Policy Add New Role Mapping Policy Add New Enforcement Policy Add New Enforcement Policy meout, GG MAC Caching Bandwidth Limit, mit, GG Employee MAC Caching, [Update Taching Do Fynire, GG MAC Caching, Evpire
Summary Service lole Mapping Policy: Description: Default Role: tules Evaluation Algorithi Conditions (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID Summary Service Use Cached Results: Enforcement Policy: Description: Default Profile: Rules Evaluation Algorith Conditions 1. (Authorization:[Er 2. ANO (Date:Day Monday,Tuesday,We	Authentication Authorization Roles Enf GG User Authentication with MAC Caching Role Mag Role N (Other] m: evaluate-all EQUALS 1) EQUALS 2) EQUALS 2) EQUALS 3) Authentication Authorization Roles Enf GG User Authentication with MAC Caching Enforcen Enfor (Allow Access Profile] m: first-applicable Authorita Repository]:Unique-Device-Count GREA S [Employee]) of-Week BELONGS_TO denesday,Thursday,Friday,Saturday,Sunday)	orcement pping ✓ Modify 4apping Policy Details	Add New Role Mapping Policy Add New Role Mapping Policy Add New Enforcement Policy Add New Enforcement Policy neout, GG MAC Caching Bandwidth Limit, mit, GG Employee MAC Caching, [Update Caching Do Expire, GG MAC Caching Expire Ofile
Summary Service ole Mapping Policy:	Authentication Authorization Roles Enf GG User Authentication with MAC Caching Role Mag. Role N (Other] m: evaluate-all EQUALS 1) EQUALS 2) EQUALS 2) EQUALS 3) Authentication Authorization Roles Enf Use cached Roles and Posture attributes fro GG User Authentication with MAC Caching Enforcen Enfor [Allow Access Profile] m: first-applicable dipoints Repository]:Unique-Device-Count GREA S [Employee]] of-Week BELONGS_TO denesday,Thursday,Friday,Saturday,Sunday) S [Contractor]]	orcement pping ▼ Modify Apping Policy Details	Add New Role Mapping Policy Add New Role Mapping Policy Add New Enforcement Policy Add New Enforcement Policy Reout, GG MAC Caching Bandwidth Limit, Mit, GG Employee MAC Caching, [Update Caching Do Expire, GG MAC Caching Expire ofile Reout, GG MAC Caching Bandwidth Limit,
Summary Service bole Mapping Policy:	Authentication Authorization Roles Enf GG User Authentication with MAC Caching Role Mag Role N (GG User Authentication with MAC Caching Role Mag Role N (Other] : evaluate-all EQUALS 1) EQUALS 2) EQUALS 2) EQUALS 3) Authentication Authorization Roles Enf Use cached Roles and Posture attributes fro GG User Authentication with MAC Caching Enforcem Enfort [Allow Access Profile] m: first-applicable : Authonis Repository]:Unique-Device-Count GREA S [Employee]) -of-Week BELONGS_TO divesday,Friday,Saturday,Sunday) S [Contractor]) -of-Week BELONGS_TO	orcement pping ▼ Modify Apping Policy Details	Add New Role Mapping Policy Add New Role Mapping Policy Add New Enforcement Policy Add New Enforcement Policy Comparison of the second state of th
Summary Service lole Mapping Pollcy: befault Role: befault Role: tules Evaluation Algorithi Conditions (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID Summary Service Jse Cached Results: Enforcement Pollcy: Description: Default Profile: Rules Evaluation Algorithi 1. (Authorization:[Er 2. AND Monday, Tuesday, We 3. AND	Authentication Authorization Roles Enf GG User Authentication with MAC Caching Role Mag Role N Role N [GG User Authentication with MAC Caching Role Mag Role N Role N [Other]	orcement pping ▼ Modify Aapping Policy Details	Add New Role Mapping Policy Add New Role Mapping Policy Add New Enforcement Policy Add New Enforcement Policy Comparison of the second
Summary Service Role Mapping Policy: Description: Default Role: Utes Evaluation Algoritht Conditions (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID Summary Service Jse Cached Results: Enforcement Policy: Description: Default Profile: Rules Evaluation Algorith Conditions 1. (Authorization:[Er 1. (Authorization;[Er 2. ANO Monday,Tuesday,We (Tips:Role EQUAL 3. ANO Conditions	Authentication Authorization Roles Enf GG User Authentication with MAC Caching Role Map Role N Role N [GG User Authentication with MAC Caching Role Map Role N Role N [Other]	orcement ping ♥ Modify Aapping Policy Details	Add New Role Mapping Policy Add New Role Mapping Policy Add New Enforcement Policy Add New Enforcement Policy Add New Enforcement Policy Caching Do Expire, GG MAC Caching Expire Ofile neout, GG MAC Caching Bandwidth Limit, nit, GG Contractor MAC Caching Expire ofile neout, GG MAC Caching Bandwidth Limit, nit, GG Contractor MAC Caching Expire ofile neout, GG MAC Caching Bandwidth Limit,
Summary Service Lole Mapping Policy: Description: Default Role: Utles Evaluation Algorithin Conditions (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID (GuestUser:Role ID Summary Service Jse Cached Results: Enforcement Policy: Description: Description: Default Profile: Rules Evaluation Algorithin Conditions 1. (Authorization:[Er 1. (Authorization:[Er 2. AND (Date:Day Monday,Tuesday,We 3. AND (Tips:Role EQUAL 3. AND (Date:Day Monday,Tuesday,We 4. ANO	Authentication Authorization Roles Enf GG User Authentication with MAC Caching Role Map Role N Role N [GG User Authentication with MAC Caching Role Map Role N Role N [Other] n: evaluate-all Role N [QUALS 1) EQUALS 2) EQUALS 3) Roles Enf Authentication Authorization Roles Enf Use cached Roles and Posture attributes fro GG User Authentication with MAC Caching Enforcem [Authentication Authorization Roles Enfor [Allow Access Profile] m: first-applicable Enfor [Allow Access Profile] m: first-applicable S S [Contractor]) of-Week BELONCS_TO Meesday,Thursday,Friday,Saturday,Sunday) S S [Contractor]) of-Week BELONCS_TO Meesday,Thursday,Friday,Saturday,Sunday) S S [Guest]) of-Week BELONCS_TO Meesday,Thursday,Friday,Saturday,Sunday) S	orcement	Add New Role Mapping Policy Add New Role Mapping Policy Add New Enforcement Policy Add New Enforcement Policy Add New Enforcement Policy Caching Do Expire, GG MAC Caching Expire ofile neout, GG MAC Caching Bandwidth Limit, mit, GG Contractor MAC Caching, [Update Caching Do Expire, GG MAC Caching Expire ofile neout, GG MAC Caching Bandwidth Limit, mit, GG Contractor MAC Caching, [Update Caching Do Expire, GG MAC Caching Expire ofile neout, GG MAC Caching Bandwidth Limit, mit, GG Guest MAC Caching Bandwidth Limit, mit, GG Guest MAC Caching Expire ofile

The enforcement profiles

Summ	ary Profile	Attributes			
Profile:					
Name:		GG Empl	oyee Profile		
Description: Role/VLAN enforcement for Employee					
Type:		RADIUS			
Action:		Accept			
Device 0	Group List:	-			
Attribut	es:				
Ту	ре		Name		Value
1. Ra	dius:Aruba		Aruba-User-Role	=	Employee-Guest

Summary	Profile	Attributes		
Profile:				
Name:		GG Gues	Profile	
Description:		Role/VLA	N enforcement for Guest	
Type:		RADIUS		
Action:		Accept		
Device Group) List:	-		
Attributes:				
Туре			Name	Value
1. Radius:	Aruba		Aruba-User-Role	= Guest
Summary Profile:	Profile	Attributes		
Name:		GG Contra	ctor Profile	
Description:		Role/VLAN	enforcement for Contractor	
Type:		RADIUS		
Action: Accept				
Device Group	List:	-		
Attributes:				
Туре			Name	Value
1. Radius:	Aruba		Aruba-User-Role	= Contracto

7.3 ClearPass Guest Portal Configuration

Here we'll configure the captive portal pages.

aruba			ClearPass	Policy Manager			Menu 📕
Dashboard	-						Default 🗸
Alerts Latest Alerts	Clust	er Status s Host Name	Management IPv4	Management IPv6	Server Role	Last Replication	© Status
All Requests Trend all Policy Manager requests	© Sucto	victory	192.168.1.95	-	Publisher	-	ок
Applications Launch other ClearPass Applications	Syste	100					
Authentication Status Trend Successful and Failed authentications		and the second s			u mece	\wedge	
Cluster Status		50 Solution			은 100 년 북 문		
Device Category		0 14:35 14:40	0 14:45 14:50 14:55 Time (mins)	15:00	E 0 14:35 14:40	14:45 14:50 14:55 Time (mins)	15:00
Device Family		- Syst	em 🔶 User 🖶 IO Wait 🛨 Idle		- RA	DIUS 🔶 AppAuth	
Endpoint Profiler Summary							
Failed Authentications Track the latest failed authentications	Quick	Links		^ ٥	II Requests		0
Health Status Trend Healthy and Unhealthy requests	∯ Sta Ø Ma	art Configuring Policies			30		
Latest Authentications	Ja Ac	cess Tracker			10		
License Usage	All 🗘 Ne	twork Devices			andrage 10		
MDM Discovery Summary	Se St Cle	rver Manager earPass Guest					
OnGuard Clients Summary	- Cle	earPass Onboard earPass Insight			12:00 3. Feb 12:00 4.	Feb 12:00 5. Feb 12:00 6. Feb Time	12:0
Monitoring	/ 🔅 Cle	earPass Extensions				[All Requests]	
Configuration							

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

aruba	ClearPass Guest	Menu
🖳 Guest 💿	Home » Guest	
- 📲 Active Sessions	Guest Manager	
- 🚑 Create Account		
-ger Create Multiple	Guest Account Management	
Export Accounts	Use the accompands below to monor your activestic quest was accounts	
Manage Accounts	use the commanus below to manage your network's guest user accounts.	
- S Manage Multiple Accounts	Create New Guest Account Set up a new account for guest access to your network.	
	Create Multiple Guest Accounts Create multiple guest accounts, each with a randomly- assigned username and password.	
	Manage Guest Accounts View a lat of all curvers guest accounts. You can modify and remove individual user accounts here.	
	Edit Multiple Guest Accounts View a lad of all courters guest accounts for Cu can modify and remove bio or more used accounts here.	
	Active Sessions View active accounting sessions and disconnect or channes authorization for sessions.	
	Import Guest Accounts import a list of quests from a text file and create a guest account for each error yor he list.	
	Export Guest Accounts Export a list of all current quest accounts to a file. You can estel the format you used to export to here.	

aruba		ClearPass Guest					
🕄 Guest 📀	Home » Guest » Create Account						
- Active Sessions	Create Guest	Account					
- freate Multiple	New guest account being created by admin.						
Export Accounts		Create New Guest Account					
Import Accounts 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 Select an option for changing the expiration time of this account.					
	* Account Role:	[[Guest] v 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					
	* required field						

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

aruba				ClearPass	Guest					
Guest	Home » Guest » Manag	je Accounts								
Active Sessions	Manage Guest	Manage Guest Accounts								
- 🥵 Create Account	The following table sho	The following table shows the quest accounts that have been created. Click an account to modify it								
- P Export Accounts										
- 🃅 Import Accounts	1 Quick Help	1 Quick Help 🔒 Create 📴 More Option								
B Manage Accounts	Filter:									
– 📲 Manage Multiple Accounts	△ Username	Role	State	Activation	Expiration					
	S cpguser	[Guest]	Active	23 hours ago	No expiry					
	🛞 Reset password	🕑 Change expirati	ion 🔀 Remove	Edit (1) Sessions	Print Show Details	1 -6 1				
	C Refresh		1	L	20 rows per pa	−1or1 ge ∨				
	📲 Back to guests									
	& Back to main									
* 1 ⁰										
Guest	O Quick Help	4	💄 Create		More Options					
- 🧟 Create Account	Filter:									
💣 Create Multiple	△ Username	Role	State	Activation	Expiration					
- 📝 Export Accounts	🤶 cpguser	[Guest]	Active	23 hours ago	No expiry					
- 🋐 Import Accounts	Reset password	Change expirati	on 👩 Remove	Pressions	💫 Print 🧕 Show Details					
Manage Accounts	To undate the properties	of this quest accourt	at use the form he	low:						
– 🛃 Manage Multiple Accounts	To update the properties	To update the properties of this guest account, use the form below:								
			Edit Account							
	* Guest's Name:	cpguser Name of the guest.								
	* Username:	cpguser Name of the account	t.							
	Account Activation:	(No changes: Accou Select an option for	unt is active) \sim changing the activa	tion time of this account.						
	Account Expiration:	(No changes: Accou Select an option for	unt will not expire) changing the expira	vition time of this account.						
	Account Lifetime:	N/A ~ The amount of time	after the first login	before the account will ex	pire and be deleted.					
	Total Allowed Usage:	(No changes) Select an option for	changing the allowe	d usage time of this acco	unt.					
	Account Role:	(No changes: [Gues Role to assign to this	s account.							
	* Password:	Type in a new password Select an option for editing the guest account's password.								
	New password:	Type in a new password to assign to the guest account.								
	Confirm Password:	Repeat the new password for the guest account.								
	Session Limit:	0 The number of simu	Itaneous sessions a	llowed for this account. Ty	pe 0 for unlimited use.					
j″ Devices	0									
0 Onboard	• Notes:									
Onboard Configuration	o Notes:									

Next we'll create a weblogin page, note that the page name will be in the redirection URL, also if you are using public certificate on the controllers, you need to change securelogin.arubanetworks.com. We'll cover this later.

🖳 Guest 🛛 🔹	Home » Configuration »	» Pages » Web Logins					
Devices	Web Login (school)						
Onboard O	Web Login (Sei						
Configuration	Use this form to make	changes to the Web Login school.					
• Authentication		Web Login Editor					
- Content Manager		school					
- Wi Private Files	* Name:	Enter a name for this web login page.					
- 🥶 Public Files		school					
- 🕵 Guest Manager	Page Name:	Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".					
Hotspot Manager							
- () Pages	Description:						
Fields		Comments or descriptive text about the web login.					
- III List Views	* Vendor Settings:	Aruba ~					
Self-Registrations	Vendor Settingsr	Select a predefined group of settings suitable for standard network configurations.					
- Keb Logins	Login Method:	Controller-initiated — Guest browser performs HTTP form submit V Select how the user's network login will be handled.					
- 🛃 Web Pages	-	Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.					
±- 🚵 Receipts	* Address:	securelogin.arubanetworks.com					
BI SMS Services		Enter the IP address of hostname or the vehoor's product here.					
Translations	Secure Login:	Select a security option to apply to the web login process.					
		The controller will send the IP to submit credentials					
	Dynamic Address:	In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection.					
		The aduress above will be used whenever the parameter is not available of rails the requirements below.					
	Page Redirect						
	Options for specifying pa	rameters passed in the initial redirect.					
	Security Hash:	Do not check - login will always be permitted 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	e behaviour and content of the login form.					
	Authentication:	Credentials – Require a username and password Select the authentication requirement. 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.					
	Prevent CNA:	Access Code and Anonymous require the account to have the osename Addiencedon new set. Imable bypassing the Apple Captive Network Assistant 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:	Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.					
	CAPTCHA:	None Select a CAPTCHA mode.					
	Default Destination Options for controlling th	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.					

# chiev	Galleria Skin 3 V					
··· 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).					
Header HTML:	<pre>{nwa_cookiecheck) {if %errmsg}(nwa_icontext type=error)(%errmsg]escape){/nwa_icontext}{/if} {nwa_text id=7980} Flease login to the network using your username and password. //nwa_text)</pre>					
	Insert V					
Footer HTML:	<pre>(nwa_text id=7979) Contact a staff member if you are experiencing difficulty logging in. {/nwa_text}</pre>					
	Insert V					
Login Message:	<pre>{mma_text id=7978}Logging in, please wait {/mwa_text}</pre>					
	Insert V					
*						
· Login Delay:	The time in seconds to delay while displaying the login message.					
dvertising Service: nable advertising cont Advertising	s tent on the login page.					
Advertising Service nable advertising cont Advertising Cloud Identity ptionally present gue Enabled	s tent on the login page.					
dvertising Service: inable advertising coni Advertising Cloud Identity pptionally present gue Enabled Multi-Factor Authen	s tent on the login page. :: □ Enable Advertising Services content sts with various cloud identity / social login options. :: □ Enable logins with cloud identity / social network credentials tication					
dvertising Service inable advertising cont Advertising Cloud Identity pitionally present gue Enabled Multi-Factor Authen lequire a secondary for	s tent on the login page. I: Enable Advertising Services content sts with various cloud identity / social login options. I: Enable logins with cloud identity / social network credentials tication stor when authenticating.					
Advertising Service inable advertising con Advertising Cloud Identity Optionally present gue Enabled Aulti-Factor Authen tequire a secondary fa Provider	s tent on the login page. : Enable Advertising Services content sts with various cloud identity / social login options. :: Enable logins with cloud identity / social network credentials tication actor when authenticating. : No multi-factor authentication					
dvertising Service inable advertising con Advertising Cloud Identity optionally present gue: Enabled Aulti-Factor Authen Require a secondary fa Provider Verwork Login Acce Controls access to the	s tent on the login page. : Enable Advertising Services content sts with various cloud identity / social login options. Enable logins with cloud identity / social network credentials tication authenticating. : No multi-factor authentication > Sts login page. 					
Advertising Service inable advertising con Advertising Cloud Identity pptionally present gue: Enabled Aulti-Factor Authen Require a secondary fe Provider Hetwork Login Acces Controls access to the Allowed Access	s tent on the login page. : Enable Advertising Services content sts with various cloud identity / social login options. i: Enable logins with cloud identity / social network credentials tication actor when authenticating. :: No multi-factor authentication :: In the image. :: Lingth = authentication ::: Lingth = authentication Lingth = aut					
Advertising Service inable advertising con Advertising Cloud Identity pptionally present gue: Enabled Aulti-Factor Authen Require a secondary fa Provider Verwork Login Access Controls access to the Allowed Access	s tent on the login page. : Enable Advertising Services content sts with various cloud identity / social login options. :: Enable logins with cloud identity / social network credentials tication actor when authenticating. :: No multi-factor authentication >:ss login page. :: Enter the IP addresses and networks from which logins are permitted. ::					
Advertising Service: inable advertising cont Advertising Cloud Identity Enabled Aulti-Factor Authen Lequire a secondary fa Provider Hetwork Login Access Controls access to the Allowed Access Denied Access	s tent on the login page. : Enable Advertising Services content sts with various cloud identity / social login options. : Enable logins with cloud identity / social network credentials tication actor when authenticating. : No multi-factor authentication >sts login page. ::					
Advertising Service: nable advertising cont Advertising Cloud Identity ptionally present gue Enabled Aulti-Factor Authen tequire a secondary fa Provider Network Login Access Allowed Access Denied Access * Deny Behavior * Deny Behavior	s tent on the login page. : : :					
Advertising Service inable advertising con Advertising Cloud Identity pptionally present gue Enabled Aulti-Factor Authen lequire a secondary fa Provider Autorok Login Access Controls access to the Allowed Access Denied Access * Deny Behavior Post-Authentication Autors to perform afte Health Check	s tent on the login page. : Enable Advertising Services content sts with various cloud identity / social login options. : Enable logins with cloud identity / social network credentials tication Enable logins with cloud identity / social network credentials tication Enable logins with cloud identity / social network credentials tication Social stor when authenticating. Social : No multi-factor authentication : No multi-factor authentication : No multi-factor authentication : Inter the IP addresses and networks from which logins are permitted. : Inter the IP addresses and networks from which login access. : Send HTTP 404 Not Found status : Senduth the propunine to a re					



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.

aruba			Clear	Pass Gues	t				
🐫 Guest 🛛	Home » Configuration »	Content Manager » Public Fil	les						
្តាំ ¹ Devices	Public Files	Public Files							
🗐 Onboard	D								
Configuration	Use this list view to mai	Use this list view to manage the content items stored on this ClearPass Guest.							
Authentication	These files are public ar	nd will be accessible via HTTI	P/HTTPS under /gu	est/public.					
🥪 Content Manager	Currently showing direc	tory: Poot Directory							
- 🥨 Private Files	currencity showing unce	cory. Noor Directory.							
- Willic Files	 Quick Help 	👚 Upload New Content	🦊 Download N	lew Content 🛛 👰 🤉	Create New Directory				
Suest Manager	△ Name	Owner	Туре	Date Mo	dified Size				
- 靲 Hotspot Manager	advertising-campai	gns-blue.png	image/png	2021-02-06 1	1:14 24.0 KB				
- 🏵 Pages 🌆 Fields	advertising-campai orange.png	gns-	image/png	2021-02-06 1	1:14 25.1 KB				
- 🋅 Forms	🙀 advertising-campai	gns-steel.jpg	image/jpeg	2021-02-06 1	1:14 26.7 KB				
– 🛄 List Views – 🌻 Self-Registrations	advertising-service	5-	image/png	2021-02-06 1	1:14 25.3 KB				
Web Logins	advertising-service 728x90.png	s-orange-	image/png	2021-02-06 1	1:14 25.3 KB				
SMS Services	advertising-service 728x90.jpg	is-steel-	image/jpeg	2021-02-06 1	1:14 24.2 KB				
M Iranslations	A terms.html	admin	text/html	2021-02-06 1	1:14 2.9 KB				
	📑 Properties 🔞 De	elete 🛄 Rename 📓 Down	load 🔍 View Con	tent 🕨 Quick View	A Edit				
	This Policy is a guide Any individual conner other network(s), m other network(s) or l School MAKES NO RE THE GUEST WIRELES WIRELESS NETWORK OR DAMAGES THAT M	Sc Guest Wireless Acces to the acceptable use of the s eted to the Guest Wireless Nel ist comply with this policy, the host(s) used, and all applicable PRESENTATIONS OR WARRANT S NETWORK, AND ALL USE IS F S NETWORK, AND ALL USE IS F YOU AGREE TO DEFEND, INDE AY RESULT FROM YOUR USE OF	chool is Acceptable School Guest Wirele twork in order to us stated purposes an e laws, rules, and ro IES CONCERNING TI FROVIDED ON AN AS EMNIFY, AND HOLD H THE GUEST WIREL	Use Policy ss network facilities te it directly or to cor nd Acceptable Use p egulations. HE AVAILABILITY OR -15 BASIS. BY USING IARMLESS School FO ESS NETWORK.	and services. nnect to any olicies of any SECURITY OF 5 THE GUEST IR ANY LOSSES				
K Administration	School takes no resp downloaded by you o or compromised while	oonsibility and assumes no liab or any third party, or for anyth e connected to the Guest Wire	vility for any content ing you may encour eless Network.	uploaded, shared, nter or any data tha	transmitted, or t may be lost				

7.4 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

	•))	Login to network
		You must log in to this network before you can access the Internet.
		Open Network Login Page Advanced
▲ Legate network × + ← → C ▲ Mtpc:/192.168.1951guest/whost.php?lond=logat@mac-u0583b450xd3848ip= •••• ♥ ↓ Q. Search Mt ● ● ≡		Web sites prove their identity via certificates, which are issued by certificate authorities.
You must log in to this network before you can access the Internet. Open Network Login Page X		Firefox is backed by the non-profit Mozilla, which administers a completely open certificate authority (CA) store. The CA store helps ensure that certificate authorities are following best practices for user security.
		Firefox uses the Mozilla CA store to verify that a connection is secure, rather than certificates supplied by the user's operating system. So, if an antivinus program or a network is intercepting a connection with a security certificate issued by a CA that is not in the Mozilla CA store, the connection is considered unsafe.
		Error code: MOZILLA_PKIX_ERROR_MITM_DETECTED
🔶 Login to network		View Certificate
You must log in to this network before you can access the Internet.		
Open Network Login Page Advanced		Go Back (Recommended) Accept the Risk and Continue

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

Certificate							
securelogin.arubanetworks.com							
Subject Common Organi Co	Name Name sation puntry	securelogin.arubanetworks.com Aruba Networks US					
Issuer Common Organi Co	Name Name sation puntry	Aruba7008-CNDRJSP06J Aruba Networks US					
Va Not E Not	alidity Before t After	1/1/2016, 11:00:00 AM (Australian Eastern Daylight Time) 1/26/2051, 11:08:30 PM (Australian Eastern Daylight Time)					

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	× +				
$\left(\leftarrow ight) ightarrow m{C}$ $\left(\bigtriangleup ight)$	🔘 🖴 🗝 https://victory.dearpass.info/guest/school.php?cmd=login&mac=a0:88::= 🚥 😨 🏠 🔍 Search	lii1	•	۲	≡
↔ → ♂ ŵ				•	
The second			-		
			e		

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.

aruba	MOBILITY MASTER Aruba-MM1	CONTROLLER ⊘ 2 ः	ACCESS POINTS CI 0 ⊙ 1 0 ? 1	LIENTS ALERTS № 0 ▲ 0			admin 🗸
🗮 Managed Netwo	ork >					🖏 Search	٩,
Dashboard		2 WLANS	≓ 19.4 мв	((q)) 2 Radios			
Infrastructure	Wireless Clients 1						∑ iii
Traffic Analysis	NAME 🔺 IP ADD	RESS HEALTH BAND	D ROLE	SNR USAGE	WLAN	CONNECTE	
Security	> 192.168.1.123 192.16	8.1.123 🗰 Good 5 GHz	z Guest-guest-logon	44 dB -	Guest	20:4c:03:5c:05:6e	

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

Dashboard O	Monitori	toritoring » Live Monitoring » Access Tracker							
😥 Monitoring 📀	Acces	Access Tracker Feb 06, 2021 14:46:43 AEDT							
Live Monitoring Access Tracker	The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.								
Accounting	💎 [A	ll Requests]	victory (192.168.1.95)		15 Last 1 day before Toda	iy	Edit		
- System Monitor	Filter: R	equest ID V cont	ains V	+ Go Clear Filter			Show 20 v records		
	#	Server	Source	Username	Service	Login Status	Request Timestamp 🔹		
	1.	192.168.1.95	RADIUS	a088b450c084	GG MAC Authentication	REJECT	2021/02/06 14:43:48		

Request Details		8	Request Details						
Summary Input Ou	Alerts	Summary Input Output Alerts							
Login Status:	REJECT	^	Enforcement Profiles: [Deny Access Profile]						
Session Identifier:	R00000012-01-601e1074		System Posture Status: UNKNOWN (100)						
Date and Time:	Feb 06, 2021 14:43:48 AEDT		Audit Posture Status: UNKNOWN (100)						
End-Host Identifier:	A0-88-B4-50-C0-84 (Computer / Windows / Windows)								
Username:	a088b450c084								
Access Device IP/Port:	192.168.1.57 (MD-1 / Aruba)								
Access Device Name:	7008-1								
System Posture Status:	UNKNOWN (100)								
	Policies Used -								
Service:	GG MAC Authentication								
Authentication Method:	MAC-AUTH								
Authentication Source:	None								
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]								
Roles:	[Other], [User Authenticated]								
Enforcement Profiles:	[Denv Access Profile]	~							
I ≤ Showing 1 of 1-20 rec	ords >>> Show Configuration Export Show Logs Close		I ◄ Showing 1 of 1-20 records ► ► Show Configuration Export Show Logs Close						

This is normal as this MAC address has not been seen before and hence the failed MAC authentication.

Now when the user performs the login process with cpguser credentials, the following will be seen.

\leftrightarrow × \diamond	🛛 🔒 https://securelogin.arubanetworks.com/cgi-bin/login	🗵 🔂 🔍 Search	III\ 🚺 🗉 🔹
--------------------------------	---	--------------	------------

Authentication successful

In 1 seconds you will be automatically redirected to http://www.arubanetworks.com.

Click here to go there directly.

Click here to bookmark this page.

logout

And then redirected to the page that was configured on the AAA profile on the MM



The MM dashboard and access tracker show that the user role is now "guest".

aruba	MOBILITY MASTER Aruba-MM1	IASTER CONTROLLERS ACCESS POINTS CLIENTS ALERTS IM1 ∅ 2 0 ∅ 1 0 ↑ 1 ๗ 0								admin 🗸
Managed Netwo	rk >								🖏 Search	٩,
Dashboard Overview	< ≜ 1 ₀	Client	2 WLANS	\rightleftharpoons	19.6 мв	((p)) 2 Radios				
Infrastructure	Wireless Clien	ts 1								V iii
Traffic Analysis										
frame / fragsis	NAME 🔺	IP ADDRESS	HEALTH	BAND	ROLE	SNR	USAGE	WLAN	CONNECTE	
Security	> cpguser	192.168.1.123	💷 Good	5 GHz	guest	44 dB	32.6 kB	Guest	20:4c:03:5c:05:6e	
Constants										

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

Monitor	ring » Live Monitoring	» Access Tr	racker				•••••
Acce	ss Tracker Feb cess Tracker page pl	06, 2021 14: rovides a rea	:52:26 AEDT al-time display of per-se	ession access activity on the selecte	d server or domain.		🛛 Auto Refresh
? [/	All Requests]		victory (192.1	.68.1.95)	15 Last 1 d	lay before Today	Edit
- 1	Downed Th			Go Clear Filter	1		Show 20 x records
Filter:	Request ID	↓ COI			Comico	Login Status	Bequest Timestamp -
	102 102 1 05		Source	Username	GG User Authent	ication with	
1.	192.168.1.95		RADIUS	cpguser	MAC Caching	ACCEPT	2021/02/06 14:51:23
2.	192.168.1.95		RADIUS	a088b450c084	GG MAC Authent	ication REJECT	2021/02/06 14:43:48
tequest	Details						
Sumr	mary Input Ou	utput Acc	counting				
Login S	Status:	ACCEPT			^		
Sessior	n Identifier:	R0000013	3-01-601e123b				
Date a	nd Time:	Feb 06, 20	021 14:51:23 AEDT				
End-Ho	ost Identifier:	A0-88-B4-	50-C0-84 (Computer	/ Windows / Windows)			
Userna	me:	cpguser					
Access	Device IP/Port:	192.168.1	.57 (MD-1 / Aruba)				
Access	Device Name:	7008-1	(
System	n Posture Status:	UNKNOWN	(100)				
			Policies Use	d -			
Service	3:	GG User A	uthentication with MAC	Caching			
Authen	itication Method:	PAP	llesse				
Authori	ization Source:	Ecuest Us	ar Repository] [Endpoi	ate Repository] [Time Source]			
Roles:	ization Source.	[Guest] [User Authenticated]	its Repository], [Time Source]			
Enforce	ement Profiles:	GG MAC C	aching Bandwidth Limit	, GG MAC Caching Session Limit, GG	Guest MAC 🗸		
ا م	iowing 1 of 1-20 rec	ords 🕨 🕨	Change Status St	now Configuration Export S	ihow Logs Close		
Sumn	nary Input Ou	itput Acc	counting				
	PO	ost Login, Gi	G MAC Caching Session	1 Imeout, GG Guest Profile	^		
System	Posture Status: U	NKNOWN (10	00)				
Audit P	osture Status: U	NKNOWN (10	00)				
RADIU	S Response				•		
Bandy	width-Check:Allowed	d-Limit	0				
Bandy	width-Check:Check-	Туре	Today				
Bandy	width-Check:Limit-U	nits	MB				
Endpo	oint:Guest Role ID		2				
Endpo	pint:MAC-Auth Expir	У	2021-02-07 14:00:0	D			
Endpoint:Username			cpguser				
Expire	e-Time-Update:Gues	tUser	0				
Expiry	/-Check:Expiry-Action	on	0				
Post-	Auth-Check:Action		Disconnect				
Post-	Auth-Check:Action	D-l-	Disconnect and Block	Access			
- FOUL	s:Aruba:Aruba-User	- KOIE	GUEST		×		

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



Clear Cache

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.

Request Details					
Summary Input O	Accounting				
Login Status:	ACCEPT	^			
Session Identifier:	R0000013-01-601e123b				
Date and Time:	Feb 06, 2021 14:51:23 AEDT				
End-Host Identifier:	A0-88-B4-50-C0-84 (Computer / Windows / Windows)				
Username:	cpguser				
Access Device IP/Port:	192.168.1.57 (MD-1 / Aruba)				
Access Device Name:	7008-1				
System Posture Status:	System Posture Status: UNKNOWN (100)				
	Policies Used -				
Service:	GG User Authentication with MAC Caching				
Authentication Method:	PAP				
Authentication Source:	Local:localhost				
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]				
Roles:	[Guest], [User Authenticated]				
Enforcement Profiles:	GG MAC Cachina Bandwidth Limit. GG MAC Cachina Session Limit. GG Guest MAC ords ► ►I Change Status Show Configuration Export Show Logs C	✓			
Request Details					
	Access Control Capabilities -				
Select Access Control Typ	e: O Agent O SNMP I RADIUS CoA O Server Action				
RADIUS CoA Type:	[ArubaOS Wireless - Terminat ~				



Dashboard O	Bashboard o Monitoring > Live Monitoring > Access Tracker									
🛃 Monitoring 📀	Auto Refresh									
The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.										
- Jaccounting - Jaccount Activity	T [4	All Requests]	victory (192.168.1.95)	15 Last 1 day before Too	lay	Edit			
Analysis & Trending										
System Monitor	Filtor	Poquet ID	v contains v	Go Clear Filter			Show 20 records			
🗉 🛃 Profiler and Network Scan	Filter. [P	(equest 10	 contains + 							
	#	Server	Source	Username	Service	Login Status	Request Timestamp 🔻			
	1.	192.168.1.95	RADIUS	cpguser	GG MAC Authentication	ACCEPT	2021/02/06 14:59:42			
	2.	192.168.1.95	RADIUS	cpguser	GG User Authentication with MAC Caching	ACCEPT	2021/02/06 14:51:23			
	з.	192.168.1.95	RADIUS	a088b450c084	GG MAC Authentication	REJECT	2021/02/06 14:43:48			

Looking at the details of that session

Request Details			Request Details G					
Summary Input Ou	Accounting	_	Summary Input Output Accounting					
Login Status:	ACCEPT	^	Enforcement Profiles: [Allow Access Profile], GG Guest Device Profile					
Session Identifier:	R00000014-01-601e142e		System Posture Status: UNKNOWN (100)					
Date and Time:	Feb 06, 2021 14:59:42 AEDT		Audit Posture Status: UNKNOWN (100)					
End-Host Identifier:	A0-88-B4-50-C0-84 (Computer / Windows / Windows)		RADIUS Response					
Username:	cpguser							
Access Device IP/Port:	192.168.1.57 (MD-1 / Aruba)		Radius:Aruba:Aruba-User-Role Guest					
Access Device Name:	7008-1		Radius:IETF:User-Name cpguser					
System Posture Status:	UNKNOWN (100)							
	Policies Used -							
Service:	GG MAC Authentication							
Authentication Method:	MAC-AUTH							
Authentication Source:	Local:localhost							
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]							
Roles:	[Guest], [MAC Caching], [User Authenticated]							
Enforcement Profiles:	[Allow Access Profile], GG Guest Device Profile	~	~					
Showing 1 of 1-20 rec	ords ► ► Change Status Show Configuration Export Show Logs Clos	se	Showing 1 of 1-20 records ► ► Change Status Show Configuration Export Show Logs Close					

7.5 Captive Portal Server Certificate for MD

Here we'll upload a wild card public certificate to every MD which then can be used for Captive portal server certificate.

Managed Network > Lab >	7008-1 (i) Version 8.6.0.7							
	Q Dashboard	Gor	oeral Admin AirWa		tificates SNMP	Logging Profiles	More	
🔁 Mobility Master		Gei		ive crisec ce i	sincates sitility	Logging	Wore	
🔁 Managed Network (2)	WLANs	✓ Ir	nport Certificates					
	Roles & Policies		Import Certificates					
	Access Points		NAME	ТҮРЕ	FILENAME	REFERENCES	EXPIRED	
	AP Groups		master-ssh-pub-cert	PublicCert	master-ssh-pub-cert		No	
	Authentication							
			+					
			New Certificate					
	Tasks		Certificate name:	CP-server-cert				
	Redundancy		Certificate filename	clearnass info-contr	Browse			
	Maintenance			cicul pubblimo contr				
			Optional passphrase:	••••••				
			Retype passphrase:	•••••				
			Certificate format:	PEM 💙				
			Certificate type:	ServerCert	~			

Once it is submitted.

← Managed Network > Lab > 7008-1 ① Version 8.6.0.7								
C₽ _k Q	Dashboard	Seneral Admin AirWave CPSec Certificates SNMP Logging Profiles More						
🗎 Mobility Master	Configuration							
🗁 Managed Network (2)	WLANs	master-ssh-pub-cert PublicCert master-ssh-pub-cert - No						
🗁 Lab (2)	Roles & Policies	Crestvercert Servercert Creatpostiniocontroler " No						
📼 7008-1	Access Points							
5008-2	AP Groups	+						
	Cartificata S CB samer sant Canaral Dataile							
	Services	Certificate > CP-server-cert General Details						
	Interfaces	This certificate is intended for the following purpose(s):						
	Controller	All issuance policies Forumes the identity of a remote computer						
	Issued to: * clearnass info							
	Tasks	Issued by: AlphaSSL CA - SHA256 - G2						
	Redundancy	Valid from: Nov 2, 2020 23:05:51 GMT						
	Maintenance	Valid to: Dec 4, 2021 23:05:51 GMT						

Managed Network > Lab > 7008-1 (i) Version 8.6.0.7

Dashboard	General Admin AirWave	CPSec Cert	ificates SNMP Logging	Profiles More		
	 Import Certificates 					
Roles & Policies	Import Certificates					
Access Points	NAME	ТҮРЕ	FILENAME	REFERENCES	EXPIRED	=
AB Crouns	master-ssh-pub-cert	PublicCert	master-ssh-pub-cert		No	
AF Groups	CP-server-cert	ServerCert	clearpass.info-contro	ller.pem	No	Ē
Authentication						
Services						
Interfaces	+					
Controller						
System	Certificate > CP-server-cert	General D	etalls			
Tasks	Version:		3 (0x2)			
Redundancy	Serial number:		14155746B177D8AC839BC421			
Maintenance	Signature algorithm:		sha256WithRSAEncryption			
	Issuer:		AlphaSSL CA - SHA256 - G2			
	Valid from:		Nov 2, 2020 23:05:51 GMT			
	Valid to:		Dec 4, 2021 23:05:51 GMT			
	Subject:		*.clearpass.info			
	Public key:		rsaEncryption (2048 bit)			
	Key usage:		Digital Signature, Key Encipherment			
	Thumbprint algorithm	1:	SHA1			
AnihaMM-VA 8711	Thumbprint:		39:63:DF:EA:69:4E:3B:C2:CC:6A:85:B9	:D8:06:47:57:BF:47:B6:CC		

Now you need to assign it as Captive Portal certificate.

Managed Network > Lab > 7	7008-1 🕕 Version 8.6.0.7
Dashboard	General Admin AirWave CPSec Certificates SNMP Logging Profiles More
Configuration	
WLANs	> Spanning Tree
Roles & Policies	> LACP
Access Points	> Capacity Threshold
AP Groups	
Authentication	> Phone Home
Services	✓ General
Interfaces	CAPTIVE PORTAL CERTIFICATE
Controller	Server certificate: CP-server-cert Y
System	IDP SERVER CERTIFICATE
Tasks	Server certificate: default 💙
Redundancy	
Maintenance	SSL protocol:

Checking it from the CLI

```
(7008-1) #show crypto pki serverCert
Certificates of All Nodes
_____
              Expired
Name
_____
               _____
CP-server-cert No
(7008-1) #show crypto pki serverCert CP-server-cert
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            14:15:57:46:b1:77:d8:ac:83:9b:c4:21
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=BE, O=GlobalSign nv-sa, CN=AlphaSSL CA - SHA256 - G2
        Validity
            Not Before: Nov 2 23:05:51 2020 GMT
            Not After : Dec 4 23:05:51 2021 GMT
        Subject: CN=*.clearpass.info
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c9:a2:fe:62:3a:4d:1a:51:51:60:fc:50:e6:c3:
                    61:25:4c:27:b5:50:93:44:62:47:33:9d:da:30:39:
                    ee:ee:df:46:37:31:1d:35:b3:99:04:3e:c5:df:63:
                    c3:bd:50:72:9f:93:14:9d:70:f7:ae:fb:d5:01:76:
                    22:46:c2:b5:0e:f1:b0:a2:be:c2:41:43:e9:82:bc:
                    b2:9c:eb:f2:ee:cb:e8:0e:57:52:ac:47:01:db:75:
                    51:3b:68:9c:a2:19:57:03:69:db:b1:dd:60:d7:55:
                    c3:ec:1b:e1:80:50:93:1b:92:45:6e:5c:2c:44:fb:
                    5a:55:09:1b:00:d2:63:e3:64:2e:ac:13:24:65:1b:
                    6a:3b:ad:ea:a2:46:04:cf:44:f1:81:42:fc:29:14:
                    ca:f1:77:94:d5:48:a9:ec:a7:7e:73:6b:96:a6:35:
                    4e:81:2b:4b:5f:ca:1f:b1:d0:f0:dc:11:fa:b8:e6:
                    08:bc:20:dd:74:57:1e:3f:17:15:77:29:b0:02:52:
                    c2:c1:58:ca:4c:ee:e1:fa:fe:30:a5:5a:e0:7f:e9:
                    c0:14:03:e1:78:51:40:12:7c:53:56:c2:7b:a1:44:
                    83:16:dc:d4:f0:ce:b8:c3:23:e8:b7:c1:a1:71:8b:
                    a5:45:fd:07:0a:58:19:41:96:0f:b2:05:c6:66:a0:
                    3f:91
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            Authority Information Access:
                CA Issuers - URI:http://secure2.alphassl.com/cacert/gsalphasha2g2r1.crt
                OCSP - URI:http://ocsp2.globalsign.com/gsalphasha2g2
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.4146.1.10.10
                  CPS: https://www.globalsign.com/repository/
                Policy: 2.23.140.1.2.1
            X509v3 Basic Constraints:
                CA: FALSE
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl2.alphassl.com/gs/gsalphasha2g2.crl
            X509v3 Subject Alternative Name:
                DNS:*.clearpass.info, DNS:clearpass.info
```

```
X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
           X509v3 Authority Key Identifier:
                keyid:F5:CD:D5:3C:08:50:F9:6A:4F:3A:B7:97:DA:56:83:E6:69:D2:68:F7
           X509v3 Subject Key Identifier:
               A3:ED:1B:14:AE:B1:5E:1B:1F:8E:DD:D0:64:5F:E9:5D:3D:08:F7:D9
            1.3.6.1.4.1.11129.2.4.2:
                .....u.oSv.1.1.....Q..w....).....7....u.5.Z.....FOD.
.{..+.C.9.S.~sK..[....n.iy..%... {..4.Tw..)Q%p7..eT.4....).O. .....0.[.Eg.)..6.
=....OU....CX-o...y...58.|...Im.....FOD.
   Signature Algorithm: sha256WithRSAEncryption
        b5:4f:45:1e:e7:23:42:20:c3:86:4e:97:27:85:db:5b:09:5b:
        ef:29:a9:00:72:4f:34:15:ec:75:e5:45:05:b8:2d:ef:55:76:
        e9:03:7b:46:6a:88:e5:67:b4:3b:19:f6:3a:41:61:d8:49:3e:
        23:90:08:a9:60:9f:17:ad:b0:d5:8b:99:ea:07:58:a0:ea:9f:
        13:73:64:0f:25:2d:9d:48:4d:f6:46:08:55:c3:f4:43:cc:6d:
        71:bd:e6:39:76:4b:ae:1c:7c:88:57:f5:4d:27:a3:b8:e0:db:
        8b:9b:39:b4:76:17:c8:16:a9:cf:07:36:b7:ee:b8:fd:88:bb:
        a5:9b:4f:ae:32:a9:bf:6d:16:48:c0:47:cd:aa:b6:ac:b2:6a:
        8d:60:25:26:02:38:a2:b9:68:c9:4d:a5:3d:59:0a:01:ca:fc:
        4c:ae:8a:68:51:3e:2f:87:a9:1a:f6:8a:ef:7e:24:63:ae:99:
        03:02:eb:03:97:db:20:fb:34:a7:aa:85:01:4d:de:e3:6c:bc:
        e8:6a:7d:22:e6:c4:32:b2:f6:72:05:b0:5e:68:1e:c3:af:7a:
        44:68:ac:c4:a7:e2:04:f9:7e:6b:e2:68:82:c3:6d:71:89:52:
        57:41:43:8d:7a:f8:83:e7:2f:08:2f:c8:32:27:69:97:d6:d8:
        62:8e:c7:58
```

```
(7008-1) #
```

7.6 General Operation

So now when the wildcard cert is imported as captive portal cert for Controllers, it will replace the asterisk "*" in the CN of the cert with "captiveportal-login".

So in ClearPass Guest weblogin or self-registration page instead of using securelogin.arubanetworks.com, now we should be using "captiveportal-login.clearpass.info".

aruba	ClearPass Guest						
🖣 Guest 🛛 🛛 🛛	Home » Configuration	ome » Configuration » Pages » Web Logins					
🔊 Devices 🔹 💿	Web Login (sch	Veb Login (school)					
📳 Onboard 🔹 💿							
🔨 Configuration 📀	Use this form to make	changes to the Web Login school .					
- 🍣 Authentication		Web Login Editor					
∃ 🥑 Content Manager – 🙀 Private Files	* Name:	school Enter a name for this web login page.					
- 🎯 Public Files - 🔐 Guest Manager	Page Name:	School Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".					
Hotspot Manager H	Description:						
- III Forms - III List Views	* Vendor Settings:	Aruba Select a predefined group of settings suitable for standard network configurations.					
- Web Logins	Controller-initiated — Guest browser performs HTTP form submit Login Method: 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.						
Receipts MS Services	* Address:	captiveportal-login.clearpass.info Enter the IP address or hostname of the vendor's product here.					
Translations	Secure Login:	Use vendor default V Select a security option to apply to the web login process.					

Now with all this in place, the users should not see any browser warning for the initial redirection to the captive portal page.

8 Guest Access with Terms of use

This objective here is to have an anonymous weblogin for guests to just accept the terms of use.

Create a new web login with the following:

- Authentication: Anonymous Do not require a username or password
- Auto-Generate: Checked
- Terms: Checked
- Anonymous User: Choose a unique username of your choice. It will not be visible outside the account list. Say you chose "cpguser"
- Pre-Auth Check: Local match a local account

🗣 Guest 🔹 🔍	Home » Configuration >	Pages » Web Logins								
gi ¹⁾ Devices 🔹 🔹	Web Login (Far	ncv Terms and Conditions Only)								
- i Onboard O	, (Use this form to make changes to the Web Login Fancy Terms and Conditions Only.								
Configuration 📀	Use this form to make	changes to the Web Login Fancy Terms and Conditions Only.								
- Station		Web Login Editor								
🖃 🍯 Content Manager	*	Fancy Terms and Conditions Only								
- 🤷 Private Files	[∞] Name:	Enter a name for this web login page.								
- 🥹 Public Files - 🕰 Guest Manager	Page Name:	t_and_1 Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".								
Hotspot Manager Second Secon	Description:									
- 🍈 Forms - 🛄 List Views	* Vendor Settings:	Aruba Select a predefined group of settings suitable for standard network configurations.								
—:∯ Self-Registrations —∰ Web Logins — ≷ Web Pages	Login Method:	Controller-initiated — Guest browser performs HTTP form submit 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:	Captiveportai-login.clearpass.info Enter the IP address or hostname of the vendor's product here.								
ITranslations	Secure Login:	Use vendor default V 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 page	, arameters passed in the initial redirect.								
	Security Hash:	Do not check – login will always be permitted 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 th	e behaviour and content of the login form.								
	Authentication:	Anonymous – Do not require a username or password Select the authentication requirement. 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.								
	Auto-Generate:	Create a new anonymous account The account will be created without a session limit or expiration time, and with the Guest role (ID 2). Enter a value for 'Anonymous User' to use a specific username, or leave blank to randomly generate a username.								
	* Anonymous User:	anonyguest The account to use for anonymous authentication. The password will be visible within the HTML It is recommended to increase the account Session Limit to the number of guests you wish to support.								
	Prevent CNA:	Enable bypassing the Apple Captive Network Assistant 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:	Local — match a local account								
	Terms:	Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.								
	CAPTCHA:	None ~ Select a CAPTCHA mode.								

Default Destination	he destination clients will redirect to after login.							
* o (hum								
Default ORL:	Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.							
Override Destination: If selected, the client's default destination will be overridden regardless of its value.								
Login Page Options for controlling the look and feel of the login page.								
* Skin:	ClearPass Guest 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).							
Header HTML:	<pre>(Imwa_cooklecheck) {if Serrmsg}escape){/nwa_ chead> Serrmsg}escape){/nwa_</pre>	icontext){/if}						
	<pre><form accept-charset="UTF-8" enctype="applica
novalidate=" method="POST" novalidate"=""></form></pre>	tion/x-www-form-urlencoded"						
	{if \$radius weblogin.username auth == 'anonymous'} <div styl<="" td=""><td>e="display:none;">{/if}</td></div>	e="display:none;">{/if}						
	HTML template code displayed before the login form.	ildert						
Footer HTML:	<pre>{Inwa text id=7979) Contact a staff member if you are experiencing difficulty logging in. (/nwa_text)</pre>							
	HTML template code displayed after the login form.	Insert V						
Footer HTML:	<pre>{nwa_text id=7979} Contact a staff member if you are experiencing difficulty logging in. Footer HTML: {/nwa_text}</pre>							
	HTML template code displayed after the login form.	Insert v						
Login Message:	<pre>{nwa_text id=7978} Logging in, please wait {/nwa_text}</pre>	.11						
	HTML template code displayed while the login attempt is in progress.	Insert v						
* Login Delay:	0 🔄 The time in seconds to delay while displaying the login message.							
Advertising Services Enable advertising conte	ent on the login page.							
Advertising:	Enable Advertising Services content							
Cloud Identity								
Optionally present guest	ts with various cloud identity / social login options.							
Enabled:	Enable logins with cloud identity / social network credentials							
Multi-Factor Authenti Require a secondary fac	ication ctor when authenticating.							
Provider:	No multi-factor authentication \sim							
Network Login Acces Controls access to the lo	55 ogin page.							
Allowed Access		.*						
Allowed Access.	Enter the IP addresses and networks from which logins are permitted.							
Denied Access:	Denied Access:							
* Deny Behavior:	* Denv Behavior: Send HTTP 404 Not Found status							
	Select the response of the system to a request that is not permitted.							
Post-Authentication Actions to perform after	Post-Authentication							
Health Check:	Require a successful OnGuard health check If selected, the guest will be required to pass a health check prior to accessing the	: network.						
Update Endpoint:	Mark the user's MAC address as a known endpoint If selected, the endpoint's attributes will also be undated with other data is from the	e user account.						
	The selection, the emploint's attributes will also be updated with other details from the							
	a Save Changes Save and Reload							

Here is the HTML code in the header section.

```
{nwa_cookiecheck}
{if $errmsg}{nwa_icontext type=error}{$errmsg|escape}{/nwa_icontext}{/if}
<head>
<title>Public wireless Internet access</title>
</head>
<body>
<div align="center" width="100%">
<form method="POST" accept-charset="UTF-8" enctype="application/x-www-form-urlencoded"
novalidate="novalidate">
```

{if \$radius weblogin.username auth == 'anonymous'}<div style="display:none;">{/if} <label for="username">Username:</label>
 <input type="text" style="width: 200px;" autocapitalize="off" autocorrect="off" spellcheck="false" id="username" name="username" value="{\$username|escape}">
 {if \$username error}{\$username error|escape}
{/if} {if \$radius weblogin.username auth == 'username'}<div style="display:none;">{/if} <q> <label for="password">Password:</label>
 <input type="password" style="width: 200px;" id="password" name="password">
 {if \$password error}{\$password error|escape}
{/if} {if \$radius weblogin.username auth}</div>{/if} <q> {if \$url error}{\$url error|escape}
{/if} {if \$radius weblogin.login terms require} Company X
br/>Guest Wireless Access Acceptable Use Policy This Policy is a guide to the acceptable use of the Company X Guest Wireless network facilities and services. Any individual connected to the Guest Wireless Network in order to use it directly or to connect to any other network(s), must comply with this policy, the stated purposes and Acceptable Use policies of any other network(s) or host(s) used, and all applicable laws, rules, and regulations. COMPANY C MAKES NO REPRESENTATIONS OR WARRANTIES CONCERNING THE AVAILABILITY OR SECURITY OF THE GUEST WIRELESS NETWORK, AND ALL USE IS PROVIDED ON AN AS-IS BASIS. BY USING THE GUEST WIRELESS NETWORK YOU AGREE TO DEFEND, INDEMNIFY, AND HOLD HARMLESS COMPANY C FOR ANY LOSSES OR DAMAGES THAT MAY RESULT FROM YOUR USE OF THE GUEST WIRELESS NETWORK. Company C takes no responsibility and assumes no liability for any content uploaded, shared, transmitted, or downloaded by you or any third party, or for anything you may encounter or any data that may be lost or compromised while connected to the Guest Wireless Network. Company C reserves the right to disconnect any user at any time and for any reason. The Guest Wireless Network is provided as a courtesy to allow our quests access to the internet. Users will not be given access to the Company X intranet or permission to install any software on our computers.
<label for="visitor accept terms"><input type="checkbox"</pre> name="visitor accept terms" id="visitor accept_terms" />I Accept</label></br /> {if \$visitor accept terms error}{\$visitor_accept_terms_error|escape}
{/if} {/if} <input type="submit" style="width: 200px;" id="submit" name="submit" value="Log in"> </form> </div> </body>

And this is how it looks.





Contact a staff member if you are experiencing difficulty logging in.

Now checking the guest account, we see the new account for anonymous guest users that was automatically generated.

aruba	ClearPass Guest						
😳 Guest 📀	Home » Guest » Manag	e Accounts					
- Su Active Sessions - Screate Account - Create Multiple	Manage Guest Accounts						
Export Accounts Torrest Accounts Manage Accounts	Quick Help Filter:		Create		More Options		
- 📲 Manage Multiple Accounts	△ Username	Role	State	Activation	Expiration		
	🔒 anonyguest	[Guest]	Active	2 minutes ago	No expiry		
	g cpguser	[Guest]	Active	2 days ago	No expiry		
	C Refresh			1	Showing 1 – 2 of 2 20 rows per page v		

To use this captive portal page, we'll create a new controller captive portal profile so that it is pointing to this URL and then assign it in the initial user-role guest-logon.

Aruba-MM1	TER CONTROLLERS ACCESS POINTS CLIENTS ALERTS 1 ○ 1 ○ 0 ○ 1 ○				
Managed Network > Lab >					
C A Q	Dashboard Configuration	Auth Servers AAA Profiles L2 Authentication	L3 Authentication User Rules Advanced		
🔁 Managed Network (2)	WLANs	L3 Authentication	Captive Portal Authentication Profile: New Profile		
🗁 Lab (2)	Roles & Policies	O 🕞 Captive Portal Authentication	Captive Portal Authoptication Profile:		
5 7008-1	Access Points	⊕ Guest_cppm_prof			
5 7008-2	AP Groups	🕀 🖻 default			
	Authentication	Stateful Kerberos Authentication			
	Services	⊕			
	Interfaces	VIA Authentication			
	Controllers	⊕			
	System	⊕			
	Tasks	⊕			
	Redundancy	WISPr Authentication			
	IoT				
	Maintenance				

Auth Servers	AAA Profiles	L2 Authentication	L3 /	Authentication	User Rules	Advanced					
L3 Authentic	L3 Authentication				Captive Portal Authentication Profile: New Profile						
O 🗗 Captive Portal Authentication				Profile name:		iuest_terms_CP_	Prof				
⊕ Guest_cppm_prof				Default Role:			guest	~			
⊕ 🗖	default				_ /						
🕀 🖻 Sta	teful Kerberos Auth	entication		Default Guest	Role:		guest	×			
🕀 🖻 Sta	teful NTLM Authent	cation		Redirect Pause	2:		1	sec			
🕀 🖻 VIA	Authentication			User Login:							
	Connection			Guest Login:							
🕀 🖻 VIA	Web Authentication	1		Logout popup							
🕀 🖻 VPI	N Authentication			Use HTTP for a	authentication:		_				
⊕ 🖻 WI	SPr Authentication			Logon wait mi	nimum wait:	5	sec				
				Logon wait ma	iximum wait:	10	sec				
				logon wait CPU	J utilization thresh	nold:	60	%			
				Max Authentic	ation failures:		0				
				Show FQDN:							
				Authentication	Protocol:		PAP 🗸				
				Login page:			victory.clearpass.inf	ic.			

The login page is "https://victory.clearpass.info/guest/t_and_1.php?"

Auth Servers AAA Profiles L2 Authentication	L3 Authentication User Rules Advanced
L3 Authentication	Server Group: Guest_dot1_svg
Captive Portal Authentication	
⊕ Guest_cppm_prof	Server Group: Guest_dot1_svg V
Guest_terms_CP_Prof	Fail Through:
🕞 Server Group	Load Balance:
⊕ default	
⊕ ➡ Stateful Kerberos Authentication	
⊕ ➡ Stateful NTLM Authentication	
VPN Authentication	

Now changing the guest-logon role to point to the new created captive portal profile.

Role	s Policies Applications Aliases		
on -			
6	suest-guest-logon	28 Kules	
Policies	tan	2 Rules 2 Bulas	
oints			
G	uest-guest-logon Policies Bandwidth	Captive Portal More	Show
	> Network		
	> VPN		
	 Authentication 		
	IDP profile:	-None- 👻	
	Stateful NTLM profile:	-None-	
	stateful Kerberos profile:	None. Y	
	staterur kerberos prome.	-NORE-	
	WISPr profile:	-None- 💙	
	Captive portal profile:	Guest_terms_CP_Prof	
	Captive portal check for accounting:		

Now when a client connects to the guest WLAN network, it will use the T&Cs weblogin and after the user accepts the terms, they get access to the network.

aruba	MOBILITY MASTER Aruba-MM1		CONTROLLE ⊙ 1 ①	RS ACCESS POINTS 0 ⊙ 1 0	CLIENTS AL	erts 0			admin 🗸	
Managed Networ	k >							🔅 Search		0,
Dashboard Overview	A 1 client	\$ 2 w	VLANS	3.95 мв	((q)) 2 Radios					
Infrastructure	Wireless Clients 1								∇	iii
Traffic Analysis		10 4000500		2015	010	1104.05	14/1 4.51			
Security Services	> anonyguest	192.168.1.123	Good 5 GHz	guest	44 dB	-	Guest	20:4c:03:5c:05:6e		

And this is what we see in access tracker.

Access Tracker Feb 07, 2021 17:06:35 AEDT

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

[All Requests]	victory (192.168.1.95)	Last 1 day before Today	Edit

Filter: Re	equest ID $$	ins 🗸	Go Clear Filter			Show 20 \sim records
#	Server	Source	Username	Service	Login Status	Request Timestamp 🔹
1.	192.168.1.95	RADIUS	anonyguest	GG User Authentication with MAC Caching	ACCEPT	2021/02/07 17:02:37
2.	192.168.1.95	RADIUS	a088b450c084	GG MAC Authentication	REJECT	2021/02/07 17:02:21

🔗 Auto Refresh

9 Guest Operator

In this section we'll configure a Guest operator or receptionist that can assist in creating only guest user accounts. We'll allow any user in AD user group called receptionist to be able to do this. Note that ClearPass Policy Manager has already joined the AD domain.

9.1 ClearPass Guest Operator Configuration

Open the Guest application by clicking the ClearPass Guest Link in the dashboard's Quick Links box for the URL redirection to ClearPass Guest.

Navigate to Home » Administration » Operator Logins » Profiles

aruba		ClearPass Guest
🚑 Guest	• Home » Administration » Operator Logins	» Profiles
👔 Devices	 Operator Profiles 	
🚛 🛛 Onboard	•	
🔦 Configuration	 ClearPass Guest supports role-based acc perform as well as global settings such 	isess control through the use of operator profiles. Each operator is as the look and feel of the user interface.
S Administration	•	as the look and reel of the user interface.
API Services	Some operator profile settings may be o	verridden in the operator's account settings. These customized ε
- 🎒 API Clients	Use this list view to define new operator	profiles, and to make changes to existing operator profiles.
API Explorer	△ Name	Description
└- SOAP Web Services ⊕- (♈) Aruba Integrations	🛔 API Guest Operator	Operators with this profile can use the API to manage guest accounts.
	BYOD Operator	Operators with this profile can view and manage their own provisioned devices.
- 🗞 Extensions 🖃 👘 Import Configuration	Device Registration	Operators with this profile can self-provision their devices, for use with MAC authentication and AirGroup sharing.
Operator Logins Login Configuration	🏨 Help Desk	Operators with this profile can troubleshoot problems reported by end users.
- Profiles	Network Administrator	Operators with this profile can view and configure network- related settings.
- 🙀 Translation Rules	🚊 Null Profile	Default profile with no permissions.
- © Plugin Manager 	Operations and Marketing	Operators with this profile can configure guest workflows, manage print templates and control other application customization options.
	Read-only Administrator	Operators with this profile have read-only access to the entire system.
	Receptionist	Operators with this profile are limited to creating new accounts and sending receipts only, and will see the create account form on login.
	🚺 Show Details 📴 Edit 😵 Delete 🛽	Duplicate 🍕 Show Usage
	Super Administrator	Default administrative profile.
	10 operator profiles 🖒 Reload	Show all rows

For each profile that is needed, there must be a corresponding Translation Rule for operator logins to receive the correct profile. Here we'll be using "Receptionist" profile. The profile basically selects what functions are allowed.

Edit Operator Profile (Receptionist)

Use this form to make changes to the operator profile Receptionist.

	Operator Pr	ofile Editor				
* Name:	Receptionist Enter a name for this operator profile.					
Description:	Operators with this profile are limited to creating new accounts and sending receipts only, and will see the create account form on login.					
	Comments or descriptive text about the operator pr	file.				
Access These options control wh	nat operators with this profile are permitted to do.					
Enabled:	Allow operator logins If unchecked, operators with this profile will not be able to log in.					
	C Operator Privileges					
	🚱 Administrator	No Access V				
	Select operator permissions for system admini	stration and management tasks.				
	Advertising Services	No Access V				
	Select operator permissions for managing adv	ertising content and services.				
	API Services No Access V					
	Select operator permissions for API access and management.					
	(P) Aruba Integrations	No Access ~				
	Select operator permissions for access to Arub	a integrations.				
	gr Devices	No Access V				
	Select operator permissions for managing devi	ces on a network.				

	Guest Manager Custom
	Select operator permissions for managing guest users for a network.
	Active Sessions ■ No Access Read Only Full Operators with the Active Sessions privilege may disconnect active sessions or change authorization for user accounts
	Active Sessions History No Access Read Only Operators with the Active Sessions History privilege may view the historical login access of the user accounts.
	∆ Change Expiration
	Operators with this privilege may change expiration times of guest accounts.
	Operators with this privilege may create groups of new guest accounts.
	Create New Guest Account O No Access Read Only Full
	Control and the provide interview of the control of the contr
	Operators with this privilege may make changes to multiple guest accounts at once.
	Operators with this privilege may export a list of guest accounts.
	No Access Read Only Full Operators with this privilege can change all properties of quest user accounts
	▲ Import Guest Accounts ● No Access ○ Read Only ○ Full
	Operators with this privilege may create new guest accounts from a data source.
	Operators with this privilege may customize fields, forms and views within the application.
	Manage Guest Accounts No Access Read Only Full Operators with this privilege can view a list of guest accounts
	🚵 Manage Print Templates 💿 No Access 🔿 Read Only 🔿 Full
	Operators with this privilege may manage templates used to generate guest account receipts.
	Operators with this privilege may disable or remove guest accounts.
	Reset Password No Access Read Only Full Operators with this privilege may reset quest account passwords.
Privileges:	
	Operators with this privilege have the Show Details action under Manage Accounts to see all attributes for an account
	Operators with the View Passwords privilege may display the passwords for guest accounts.
	Hotspot Manager No Access
	Select operator permissions for managing self-provisioned guest access.
	Select operator permissions for Insight application
	Phone Services No Access
	Select operator permissions for 1P phone administration and management tasks.
	Select operator permissions for managing Onboard device provisioning.
	Select permissions for managing local operator logins.
	1 Pass Services No Access
	Select operator permissions for managing digital passes.
	Select operator permissions for platform administration tasks.
	Policy Manager Select operator permissions for Policy Manager
	SMS Services Custom V
	Select operator permissions for access to SMS services.
	Operators with this privilege may configure advanced settings for SMS services.
	▲ Send SMS Messages Operators with this privilege may send SMS messages from the application.
	▲ Send SMS Receipts O No Access O Read Only ● Full
	Operators with this privilege can send SMS receipt messages after creating a visitor account.
	Select operator permissions for SMTP services
	∆ Configure SMTP Services No Access ○ Read Only ○ Full
	Operators with this privilege may configure SMTP settings.
	Operators with this privilege may send SMTP messages from the application.
	Support Services No Access V
	Select operator permissions for access to support services. Translation Assistant No Access V Select operator permissions for tasks related to translation. Select operator permissions for tasks related to translation. Select operator permissions for tasks related to translation.
	Show descriptions Select the privileges that will be granted to this operator login.
	Name
	ClearPass Policy Manager
	[Contractor]
User Roles:	[Guest]
	[Employee]
	10 rows per page \checkmark
	10 rows per page Select the visitor account roles that these operators are permitted to use.

* Operator Filter:	No operator filter Select the default operator filtering to apply to guest accounts.
User Account Filter:	Enter a comma-delimited list of field=value pairs to create an account filter.
Session Filter:	Enter a comma-delimited list of field=value pairs to create a session filter.
Guest Account Limit:	Maximum number of guests the operator can create. Leave blank for no limit.
Device Account Limit:	Maximum number of devices the operator can create. Leave blank for no limit.
User Interface These options control th	e visual appearance and behavior of the application.
Skin:	Choose the skin to use for operators with this profile.
Start Page:	Create New Guest Account V The initial page to show this operator after logging in.
Language:	Auto-detect Select the default language to use for operators with this profile.
Time Zone:	[Default) Select the default time zone for operators with this profile.
Customization:	Override the application's forms and views If checked, you can specify different default forms and views to use.
	Save Changes

You can edit the profile based on your requirements. We have enabled "Read Only" for

- Active Sessions
- List devices
- List Guest Accounts

And full access for "Create New Guest Account".

Now navigate to Translation rules. Home » Administration » Operator Logins » Translation Rules





So once the receptionist user, type in their user credentials, the request should match a ClearPass Policy manager service,

- the service will check against AD user group "Receptionist"
- if the user credential and user group membership is correct then an enforcement profile will be executed to send back an attribute called "Receptionist"
- that should match a translation rule (as shown above) and the appropriate operator profile will be selected.

Now going back to ClearPass Policy manager, we'll create the following enfocemenet profile

E Dashboard		Configuration » Enforcement » Profiles » Add Enforcement Profile				
Monitoring	0	Enforce	ment Pro	ofiles		
Configuration	0	Profile	Attributes	Summary		
- 🛱 Service Templates & Wiza	ards	Template:		Generic Application Enforcement		
		Name:		Guest Operator Login		
Methods		Description				
Sources		Description				
E- Q Identity						
-🛱 Single Sign-On (SS	0)	Type:		Application		
—🛱 Local Users		Action:		Accept O Reject O Drop		
- 🛱 Endpoints		Device Grou	ıp List:	Remove		
- C Static Host Lists				View Details		
				Modify		
				✓		
🖃 💐 Enforcement						
- ☆ Profiles 						
- 🛱 Policy Simulation						
Profile Attributes S	Gummary					
Profile:						
Template:	Generic Application	n Enforcemer	nt			
Name:	Guest Operator Log	gin				
Description:						
Type: Application						
Action: Accept						
Device Group List: -						
Attributes:						
Attribute Name				Attribute Value		
1. admin_privileges			= Receptionist			

Configuration » Enforcement » Profiles

Enforcement Profiles

Each enforcement policy contains enforcement profiles that match conditions (role, posture, and time) to actions (enforcement profiles).

Filter: Na	ame	✓ contains ✓ oper +	Go Clear Filte	
#		Name 🔺	Туре	Description
1.		Guest Operator Login	Application	
2.		[Operator Login - Admin Users]	Application	Enforcement profile for Guest admin logins
з.		[Operator Login - Local Users]	Application	Enforcement profile for Guest operator logins
Showing	1-3 of	3		

Next, we'll create a enforcement policy that will use the above enforcement profile.

Dashboard	Configuration » Enforcement » Policies » Edit - Ariya Guest Operator Logins			
Monitoring •	Enforcement Policies - Ariya Guest Operator Logins			
🝰 Configuration 📀	Summary Enforcement	t Rules		
 —	Enforcement:			
	Name:	Ariya Guest Operator Logins		
🎝 Methods	Description:			
- 🛱 Sources	Enforcement Type:	Application		
- Q Identity	Default Profile:	[Deny Application Access Profile]		
☆ Single Sign-On (SSO) ☆ Local Users	Rules:			
- 🛱 Endpoints	Rules Evaluation Algorithm:	First applicable		
- 🛱 Static Host Lists	Conditions		Actions	
- 🎝 Roles - 🎝 Role Mappings	1. (Authorization:Ariya Al	D:memberOf CONTAINS reception)	Guest Operator Login	
🖭 🖶 Posture				
Enforcement				
—🎝 Policies				
- 🛱 Profiles				

And finally the new service that will be used to classify the authentication request.

Configuration » Services » Edit - Ariya Guest Operator Logins

Services - Ariya	Guest Operator Logins						
Summary Service	Authentication Roles Enforce	ement					
Name:	Ariya Guest Operator Logins						
Description:	Authentication Service for Application						
Туре:	Aruba Application Authentication						
Status:	Enabled						
Monitor Mode:	Enable to monitor network ac	ess without enforcement					
More Options:	Authorization						
		Service Rule					
Matches O ANY or 🔘	ALL of the following conditions:						
Туре	Nan	e Oper	ator Value				
1. Application	Nam	EQUA	LS Guest				
2. Authentication	Туре	NOT_	EQUALS SSO				
3. Click to add							
Summary Service	Authentication Roles Enfo	cement					
Authentication Sources	Ariva AD [Active Directory]	^					
		Maya IIn A					
		Mays David					
		Move Down ↓					
		Remove					
		View Details					
		Modify					
		\sim					
	Select to Add	~					
Strip Username Rules:	Enable to specify a comma	separated list of rules to strip username prefixe	s or suffixes				
Summary Service	Authentication Roles Enforce	ment					
Role Mapping Policy:	Select	✓ Modify					
		Role Manning Policy De	tails				
Description:							
Default Role:	-						
Rules Evaluation Algorith	m: -						
Conditions			Role				
Summary Service	Authentication Roles Enforceme	i l					
Use Cashed Besulter							
Ose Cached Results:	Li use cacheu koles anu Posture attributes from previous sessions						
Enforcement Policy.	Ariya Guest Operator Logins V Modify						
		Enforcement Policy Details					
Description:							
Default Profile:	[Deny Application Access Profile]						
Rules Evaluation Algorithm	first-applicable						
Conditions		En	forcement Profiles				
1 (Authorization: Ariv	(Authorization: Ariva AD: member Of CONTAINS recention) Guest Operator Login						

The last thing is to reorder the services and disable the default [guest operator logins] service.

Dashboard O	Configur	Configuration » Services				
Monitoring O	Monitoring OServices					
🔏 Configuration 💿						Limport
🏠 Service Templates & Wizards 🙀 <mark>Services</mark>	This pag	e shows the curre	ent list and order of services that ClearPass follows	during authentication and authorization.		
- Authentication	Filter: N	ame	✓ contains ✓ +	Go Clear Filter		Show 20 v records
Methods	#	Order 🔺	Name	Туре	Template	Status
	1.	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	0
- 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	0
- 🛱 Endpoints	4.	4	[Guest Operator Logins]	Application	Aruba Application Authentication	0
- 🔅 Static Host Lists	5.	5	[Insight Operator Logins]	Application	Aruba Application Authentication	0
- C Role Mappings	6.	6	Ariya Guest Operator Logins	Application	Aruba Application Authentication	0
	7.	7	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	S
B Enforcement	8.	8	AA Aruba 802.1X Wireless	RADIUS	Aruba 802.1X Wireless	S
- 🛱 Policies	9.	9	GG MAC Authentication	RADIUS	MAC Authentication	S
- 🛱 Profiles	10.	10	GG User Authentication with MAC Caching	RADIUS	RADIUS Enforcement (Generic)	
	Showing	1-10 of 10			Reorder	Copy Export Delete

Now we'll test it out. The URL that the operators need to browse to is <u>https://victory.clearpass.info/guest/</u> And the user used the following credentials and authenticates successfully.

aruda	ClearPass Guest	
	Operator Login	
	Password:	
	Log In	
aruba	ClearPass Guest	Menu
Guest	O Home » Guest » Create Account	
- 🤗 Create Account	Create Guest Account	
— 🔩 Manage Multiple Accounts	✓ Last successful login from 192.168.1.128 on Sunday, 07 February 2021, 5:42 PM	
	1 No failed attempts since last successful login	
	New guest account being created by reception1 .	
	Create New Guest Account	
	* Guest's Name of the guest.	
	* Company Name: Company name of the guest.	
	* Email Address: The quest's email address. This will become their username to log into the network.	
	Account Activation: Now	
	Account Expiration: 1 day from now	
	Select an option for changing the expiration time of this account.	
	Account Kole: Role to assign to this account.	
	Password: 509417	
	Notes:	
	* Terms of Use: \Box I am the sponsor of this account and accept the terms of use	
	Create	

Now the reception user can create the guest account, the details can be emailed to the guest user as well. Here is the authentication session in access tracker

Subboard Monitoring » Live Monitoring » Access Tracker							
Monitoring G	Acces	ss Tracker Feb	07, 2021 17:48:38 AEDT				Auto Refresh
Live Monitoring Access Tracker	The Acc	cess Tracker page p	provides a real-time display of per-sessio	on access activity on the selected se	erver or domain.		
	۹ 💎	All Requests]	victory (192.168.	1.95)	Last 1 day before Too	day	Edit
Analysis & Trending							
	Filter:	Request ID	✓ contains ✓	Go Clear Filter			Show 20 v records
	#	Server	Source	Username	Service	Login Status	Request Timestamp 🔻
	1.	192.168.1.95	Application	reception1	Ariya Guest Operator Logins	ACCEPT	2021/02/07 17:42:22
— 纋 Data Filters — 纋 Blacklisted Users	2.	192.168.1.95	RADIUS	anonyguest	GG User Authentication with MAC Caching	ACCEPT	2021/02/07 17:02:37
	з.	192.168.1.95	RADIUS	a088b450c084	GG MAC Authentication	REJECT	2021/02/07 17:02:21

Request Details

Summary Input Ou	tput			
Login Status:	АССЕРТ			
Session Identifier:	W0000001-01-601f8bcd			
Date and Time:	Feb 07, 2021 17:42:22 AEDT			
End-Host Identifier:	-			
Username:	reception1			
Access Device IP/Port:	-			
Access Device Name:	-			
System Posture Status:	UNKNOWN (100)			
	Policies Used -			
Service:	Ariya Guest Operator Logins			
Authentication Method:	Not applicable			
Authentication Source:	Ariya AD			
Authorization Source:	Ariya AD			
Roles:	[User Authenticated]			
Enforcement Profiles:	Guest Operator Login			
I ≤ Showing 1 of 1-9 record	ds ► ►I Change Status Show Configuration Export Show Logs Close			

1	Summary	Input	Output		
ι	Jsername:		reception1		
End-Host Identifier: -		-			
1	Access Device	e IP/Port:	-		
	Authorization	Attribute	5		
	Authorizatio	n:Ariya Al	D:Account Expires	9223372036854775807 [30828-09-14 12:48:05 AEST]	
	Authorization:Ariya AD:memberOf		D:memberOf	CN=Receptionist,CN=Users,DC=wlan,DC=net	
	Authorization: Ariya AD: Name		D:Name	reception1	
	Authorization:Ariya AD:UserDN		D:UserDN	CN=reception1,CN=Users,DC=wlan,DC=net	
L					
	Computed At	ttributes			۲

Summary	Input	Output			
Enforcement Profiles: Guest Operator Login					
System Posture Status: UNKNOWN (100)			/N (100)		
Application Response					
Application:	admin_priv	vileges Re	ceptionist		

You can customise all the fields in this form which is outside the scope of this guide.

This is the dashboard that you can access through MM and here we are showing the basic information that is displayed. Please refer to the user guide for the details.





Next, check part 3 of this document.