

1 Table of Contents

1	Table of Contents	1
1.1	Revision History	1
2	New Central Configuration for AOS10 Access Points – Guest Bridge Mode.....	2
2.1	Things you need.....	2
3	AOS10 AP Configuration.....	3
3.1	Authentication Server Profile	3
3.2	Captive Portal Profile.....	4
3.3	WLAN Profile.....	5
3.4	Certificate Management.....	7
3.5	Certificate Usage.....	8
4	Testing	10
4.1	Audit Trail	10
4.2	AOS10 Certificate Usage.....	10
4.3	User Connectivity.....	11
4.4	References	13
5	ClearPass Configuration for Reference	14
5.1	Services - simple MAC Authentication	14
5.2	Services - Simple User Authentication with MAC Caching	15
5.3	Web Login (school)	16

1.1 Revision History

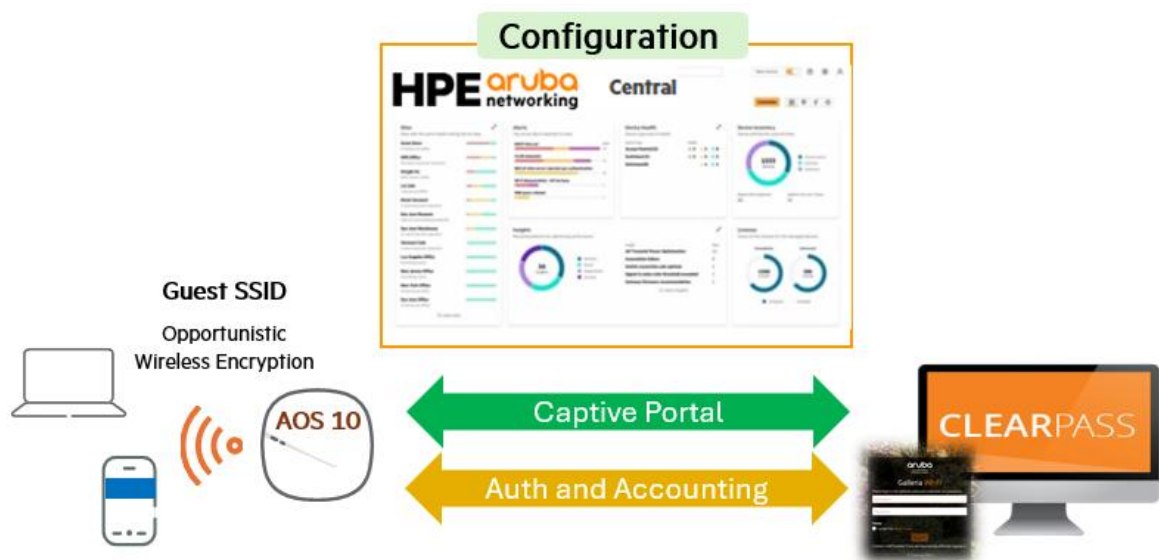
DATE	VERSION	EDITOR	CHANGES
24 Mar 2026	0.1	Ariya Parsamanesh	Initial creation
02 Apr 2026	0.2	Ariya Parsamanesh	Added the testing section

2 New Central Configuration for AOS10 Access Points – Guest Bridge Mode

Previously, I discussed one of the main features of New Central, the **Hierarchical Configuration Model**, in an earlier technote. If you remember that model helps organise configurations in a much more structured way. In this technote, I'm going to build on what we covered before, but this time, we'll focus specifically on setting up a guest WLAN. I'll be using ClearPass both as the captive portal for guests and as the authentication server, so you'll see how these components fit together in practice.

This technote will walk you through the steps to configure New Central using the different profiles required for setting up AOS10 guest WLANs, specifically **operating in Bridge mode**. We'll break down each profile and explain why it's needed, so you can follow along even if you're not familiar with all the technical terms.

The main aim here is to concentrate on configuring New Central and not get side-tracked by ClearPass setup, as we'll assume ClearPass is already set up for guest authentication and as a captive portal. This guide is especially useful if your organisation has previously configured a ClearPass guest portal for AOS10 access points using Classic Central, and now you're looking to transition to the New Central configuration.



2.1 Things you need

- APs running AOS10 firmware version (I am using 10.7.1.1)
- Valid HPE Aruba Central account and subscriptions
- AP already has a valid AP system and NTP profile
- AP has a Captive portal certificate that is in Classic Central.
- ClearPass has a valid public HTTPS server certificate and FQDN.
- ClearPass that is already configured as external authentication server and guest captive portal. It has all the needed policy manager services.

3 AOS10 AP Configuration

As mentioned earlier here I assume that the AP is already online with proper AP System, NTP and user administrator Profiles. Here we need to complete the following tasks to configure Guest WLAN with captive portal that is hosted on ClearPass.

1. Configure AAA Authentication profile
2. Assign the Authentication servers to Authentication server Group
3. Captive portal Profile
4. User role and Policies (as required)
5. Configure Guest WLAN profile
6. Import Certificate for guest redirection
7. Certificate usage

3.1 Authentication Server Profile

Since I have an existing on Premise NAC appliance (ClearPass) I'll use that as my authentication server. Note that I have two ClearPass nodes, I have already configured them for HA and have a Virtual IP (VIP) which I am using here. If you already have this configured, you can skip this section.

Name	Type	Assigned Device Function	Assigned Scope
ClearPass-RadiusVIP1	RADIUS	Campus Access Point Mobility Gateway Access Switch	Global
ClearPass-RadiusVIP2	RADIUS	Access Switch Mobility Gateway Campus Access Point	Global

You can see below ClearPassRadiusVIP1 server. You can also select device specific parameters for switches and gateways. Note that you can use IP address or FQDN, here I am using IP addresses.

Edit Profile

Properties | References

Name *
ClearPass-RadiusVIP1

Description

Server Type
RADIUS

Secure RADIUS

Auth Server Mode

RADIUS
 RADIUS with CoA (Change of...)
 CoA Only

CoA requires Dynamic Authorisation to be enabled in the Authentication Server Global profile.

Server Address Alias

Edit Profile

IP Address/FQDN *
192.168.1.101

Shared Secret Alias

Shared Secret Alias
ClearPassShared

Authentication Port *
1812

Accounting Port *
1813

Advanced

Edit Profile

NAS Identifier

NAS IP Address
xxx.xxx.xxx.xxx

Require Message-Authenticator in RADI...

AltGroup CoA Port

This configuration is applicable for Access Points and AOS-S

ClearPass Credentials

This configuration is not applicable for Access Points, except those running InstantOS 8

Device-Specific Parameters

Switch
 Gateway

Note that I am using Radius with CoA and also “Shared Secret Alias”. Now to be able to use the “Shared Secret Alias” you need to define it first and you do that by creating an alias from Named Objects tab as shown below.

The screenshot shows the 'Named Objects Management' interface with three main sections: Aliases, Services, and Applications. Each section has a brief description and a 'Manage' button.

- Aliases:** Define general aliases for the parametrization and reuse of common entities in the network. [Manage aliases](#)
- Services:** Define typical and custom network services aliases to be used in policies. [Manage services](#)
- Applications:** Define typical or custom applications to be used in policies. [Manage applications](#)

The screenshot shows the 'Allases' library with a search bar containing 'shared'. Below the search bar, there is a table with one item:

Name	Type	Assigned Device Function	Assigned Scope
ClearPassShared	Auth Server Shared Secret	Access Switch Aggregation Switch Mobility Gateway...	Global

Now that it is created and assigned to Device function and scope, it will appear as an option in the AAA Authentication Profile.

Next, we must configure Authentication server group that will include the Auth servers we just configured. Here I have two authentication server groups to distribute my auth session across my configured authentication servers and I am showing only one of them called “Radius-East” where I have added the two authentication servers called ClearPassRadiusVIP1 and VIP2.

The screenshot shows the 'Authentication Server Group' configuration interface. It displays a table with two groups:

Name	Type	Servers	Assigned Device Function	Assigned Scope
Radius-East	RADIUS	2	Mobility Gateway, Access Switch, Campus Access Point	Global
Name ClearPassRadiusVIP1 ClearPassRadiusVIP2				
Radius-West	RADIUS	2	Mobility Gateway, Access Switch, Campus Access Point	Global

Note that there is specific configuration setting just for Switches and/or gateways which is not shown here. So, you can have all those configured in one profile. And this specific configuration will one be applied to the specified device personas.

3.2 Captive Portal Profile

Once again starting from Library, we’ll configure our Captive portal profile called ClearPass-Portal that uses ClearPass. Like always with captive portal, it will redirect the guest user to a Web page on ClearPass Guest and various workflows are supported and configured on ClearPass Guest.

Profiles	Roles & Policies	Named Objects	Services
Library > Security > Captive Portal Authentication			
<input type="text" value="Search"/> Create Profile <input type="button" value=""/>			
3 items			
Name	Assigned Device Function	Assigned Scope	
ClearPass-Portal	Campus Access Point	Global	
sys_cnac_cnx-guest <small>This is a system generated configuration. Do not edit or...</small>	Campus Access Point	Global	
default <small>Default Captive Portal profile on GW</small>	Mobility Gateway Campus Access Point Microbranch Access Point...	Global	

Here is the Captive Portal Profile that I have configured. Note that I have added the URL for the captive portal and it's in FQDN format that will not cause any warning or errors. The guest captive portal URL is from ClearPass.

Name *

Description

URL

 Use HTTPS for authentication

Post Authentication Redirection URL

 Add Network Device IP in redirection URL

URL Hash key

This feature is not supported on Access Points

Retype URL Hash key

Device-Specific Parameters
 Access Point Parameters
 Gateway Parameters

Access Point Parameters
 Server Offload
 Prevent Frame Overlay

Captive Portal Failure
 Allow Internet
 Deny Internet

3.3 WLAN Profile

Starting from Library, we'll configure our guest WLAN profile called guest-CP that uses ClearPass for authentication and captive portal. When you are done, assign the Scope as you have done for the previous profiles.

General

Name *

Description

Type

Use Alias

ESSID Name *

2.4 GHz
 5 GHz
 6 GHz

Disable Network

VLAN

Traffic Forwarding Mode *
 Bridge
 Tunnel
 Mixed

Use Named VLAN

Default VLAN *

Security

Security Level *

Enterprise
 Personal
 Open

Key Management *

Enhanced Open

Captive Portal

Type

External Captive Portal

Captive Portal Profile *

ClearPass-Portal

Authentication

MAC Authentication

Server Group *

Radius-East

Accounting

Accounting

Use Authentication Servers

Accounting Interval

0-60

5 Minutes

Advanced

Denylisting
 Client Isolation
 Enforce DHCP
 WPA3 Transition

Access

Default Role - guest-CP

Override default role

ⓘ Default policies for role "guest-CP" have been created under "Roles & Policies > Role-Based policies". Please finish the configuration by editing said policies.

Advanced

Assign Pre-Authentication Role

--Select Role--

Enforce Mac Auth Only Role

--Select Role--

Role Assignment Rules

Rules

And once it is saved it will be displayed as shown below.

Profiles Roles & Policies Named Objects Services

Library > Wireless > WLAN

Q CP x Create Profile

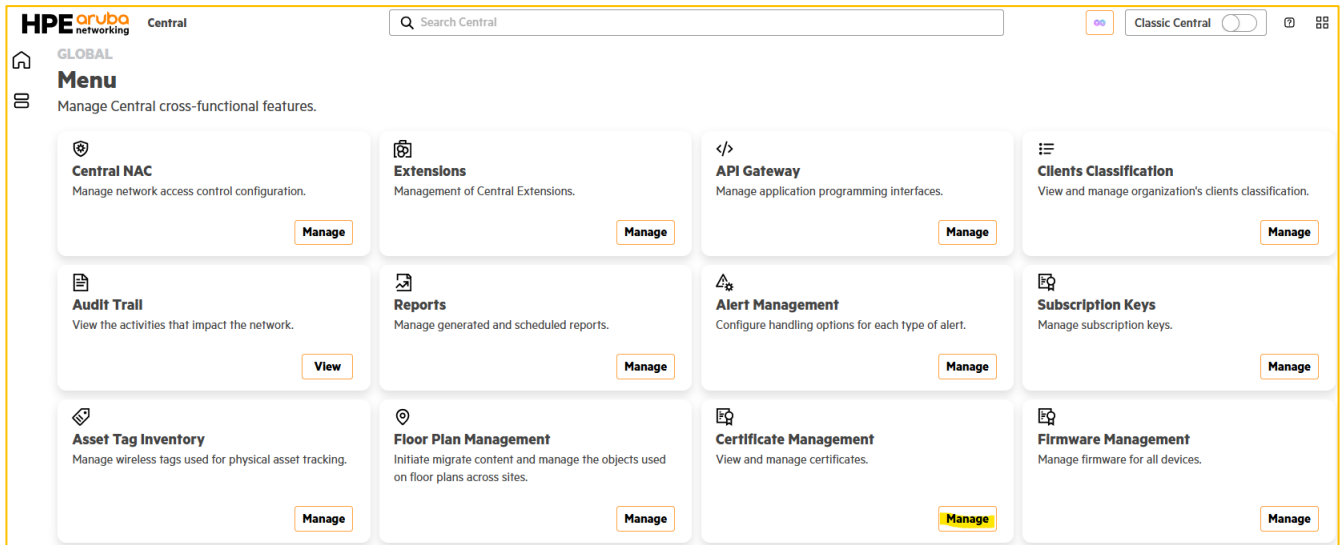
2 items

Name	Type	Assigned Device Function	Assigned Device Scope	Status
corp-CP	Access	Campus Access Point	Global	Enabled
guest-CP	Access	Campus Access Point	Global	Enabled

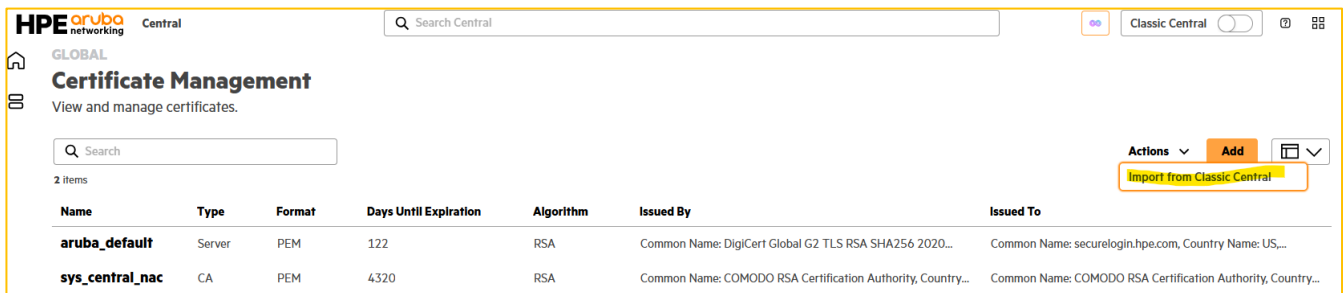
You can also change the default role, though it will usually match the WLAN profile name unless you specify otherwise. Additionally, I chose not to set a pre-auth user role since I'll be using the default pre-auth role, but you do have the option to assign one if desired.

3.4 Certificate Management

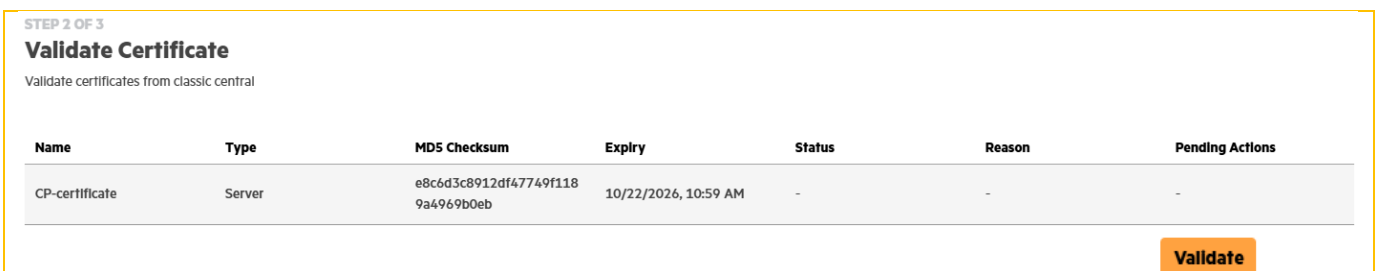
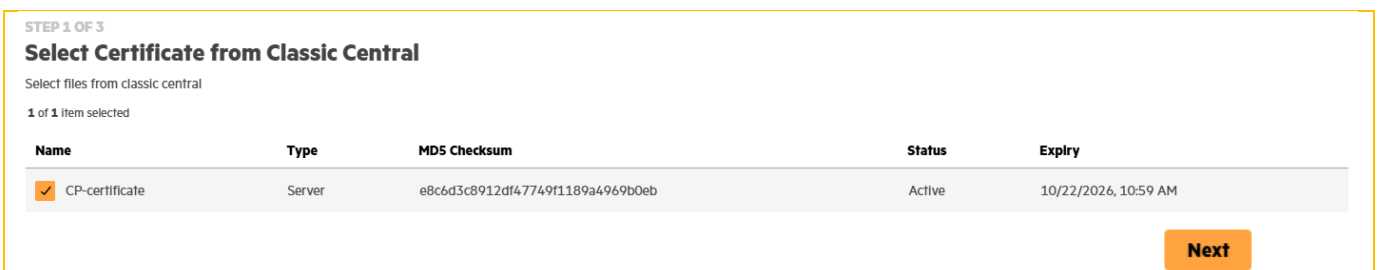
One of the key aspects of any external captive portal configuration is to assign a publicly signed server certificate to the APs so that when the APs perform the HTTPS redirection, the user browser does not complain with warning or even fail. So here we go to the Certificate Management section to import the Server certificate for Captive portal.



Here you'll notice that we are going to import the certificate from Classic Central. So here the assumption is that we were using Classic Central for AOS10 guest WLAN with ClearPass as captive portal and now we want to use the same certificate for New Central configuration. Alternatively, you can add your certificate in PEM format as well.



The import from Classic Central involves three steps process that are shown here.



Once you click on the "Validate" button, the certificate gets validated as shown below.

STEP 3 OF 3

Import Certificate

Import certificates from classic central

Name	Type	MDS Checksum	Expiry	Status
CP-certificate	Server	e8c6d3c8912df47749f1189a4969b0eb	10/22/2026, 10:59 AM	Valid

Import

After clicking on the “Import” button, it gets added to the certificates that can be used.

HPE aruba Central Certificate Management

View and manage certificates.

3 Items

Name	Type	Format	Days Until Expiration	Algorithm	Issued By	Issued To
CP-certificate	Server	PEM	213	RSA	Common Name: Sectigo Public Server Authentication CA DV...	Common Name: *arubatechs.com
aruba_default	Server	PEM	122	RSA	Common Name: DigiCert Global G2 TLS RSA SHA256 2020...	Common Name: securelogin.hpe.com, Country Name: US, Localit...
sys_central_nac	CA	PEM	4320	RSA	Common Name: COMODO RSA Certification Authority, Country...	Common Name: COMODO RSA Certification Authority, Country...

Notification: Certificate successfully imported.

3.5 Certificate Usage

The last step of the certificate management is assigning its usage for captive portal purposes. So again, from Library we will create a certificate usage profile.

Profiles Roles & Policies Named Objects Services

Library > Security > Certificate Usage

2 items

Name	Device Type	Assigned Device Function	Assigned Scope
CNX-cp-securelogin-hpe-com	Access Point	Campus Access Point	Global
default-ap-cert-usage-profile Default AP cert usage profile	Access Point	Microbranch Access Point Campus Access Point	Global

Create Profile

The new profile name is ClearPass-CP and this is profile where you can assign certificates for all the services that require one like RadSec or AP 802.1X Server CA (Uplink), etc. I am showing only the Captive portal server certificate.

Name *
ClearPass-CP

Description
captive portal provided by ClearPass

Device Type *
 Access Point
 Gateway

Access Point Parameters

Authentication Survivability Client CA
None

Authentication Survivability Server Certificate
None

Captive Portal Server Certificate
CP-certificate

Use EST for RadSec Client Provisioning


The rest of the field that I have not shown are left as default.

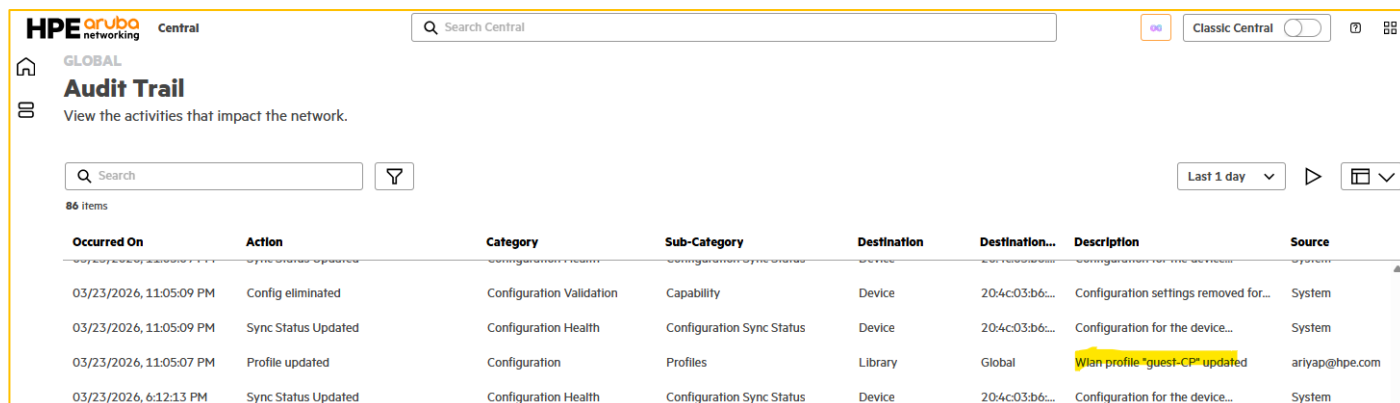
Profiles	Roles & Policies	Named Objects	Services
Library > Security > Certificate Usage			
<input type="text" value="Search"/>			<input type="button" value="Create Profile"/> <input type="button" value="Filter"/>
3 items			
Name	Device Type	Assigned Device Function	Assigned Scope
ClearPass-CP <small>captive portal provided by ClearPass</small>	Access Point	Campus Access Point	CNK6KSM099
CNX-cp-securelogin-hpe-com	Access Point	Campus Access Point	Global
default-ap-cert-usage-profile <small>Default AP cert usage profile</small>	Access Point	Microbranch Access Point Campus Access Point	Global

Note that I have not assigned any Authentication role all that will be handled by

4 Testing

4.1 Audit Trail

Let's have a quick look at the audit trail to see some of the changes we have made. To navigate to it, you need to click on the burger icon  and then choose **Audit Trail**. There you can change the duration and search for specific strings.




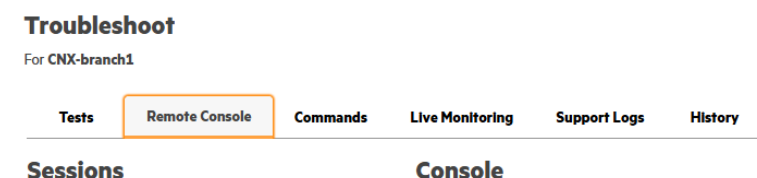
The screenshot shows the HPE Aruba Central interface for the 'Audit Trail' section. It includes a search bar, a filter icon, and a dropdown for 'Last 1 day'. Below is a table with 86 items, showing configuration changes for various devices and profiles.

Occurred On	Action	Category	Sub-Category	Destination	Destination...	Description	Source
03/23/2026, 11:05:09 PM	Config eliminated	Configuration Validation	Capability	Device	20:4c:03:b6...	Configuration settings removed for...	System
03/23/2026, 11:05:09 PM	Sync Status Updated	Configuration Health	Configuration Sync Status	Device	20:4c:03:b6...	Configuration for the device...	System
03/23/2026, 11:05:07 PM	Profile updated	Configuration	Profiles	Library	Global	Wifi profile "guest-CP" updated	ariyap@hpe.com
03/23/2026, 6:12:13 PM	Sync Status Updated	Configuration Health	Configuration Sync Status	Device	20:4c:03:b6...	Configuration for the device...	System

It is a good idea to always check that the configuration of the AP is in sync.

4.2 AOS10 Certificate Usage

Next it is important to double check the captive portal server certificate that was pushed to the AP. You can get CLI access by using the troubleshooter icon  from the site monitoring page. This is before Certificate usage profile was assigned to the AP.



The screenshot shows the 'Troubleshoot' interface for 'CNX-branch1'. The 'Remote Console' tab is selected, and the 'Sessions' and 'Console' sections are visible.

```
20:4c:03:b6:b2:5b# sh cert assignment
cert assignment
-----
Application          Cert type          Cert name
-----
captive-portal      ServerCert        aruba_default
20:4c:03:b6:b2:5b#
```

And this is after it was synced.

```
20:4c:03:b6:b2:5b# sh cert assignment
cert assignment
-----
Application          Cert type          Cert name
-----
captive-portal      ServerCert        CP-certificate
20:4c:03:b6:b2:5b#
```

4.3 User Connectivity

Let's check ClearPass access tracker after getting a client connected to guest-CP WLAN. As you see since we had configured MAC auth on the WLAN profile as well, there is a failed MAC auth.

Monitoring » Live Monitoring » Access Tracker

Access Tracker Mar 24, 2026 12:53:54 AEDT

Auto Refresh

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

[All Requests] CP1-611 (192.168.1.101) Last 2 days before Today Edit

Filter: Request ID contains [] Go Clear Filter Show 50 records

#	NAS IP Address	Server Name	Source	Username	Service	Login Status	Enforcement Profiles	Request Timestamp
1.	10.10.10.34	CP1-611	RADIUS	3e7f6fcff576	simple MAC Authentication	REJECT	[Deny Access Profile]	2026/03/24 12:50:18

A MAC authentication failure shown above is expected. The client is placed in a captive portal user role and redirected to the configured Guest captive portal URL.

By default without pre-authentication user roles, guests are assigned the default "External CP" user role, which only permits DHCP, DNS, and access to redirect URL. If you need to customise access, you need to create your own pre-authentication user role with the relevant role policies and assign it in the WLAN profile.



Here you can see the user role that was assigned.

```
20:4c:03:b6:b2:5b# sh clients

Client List
-----
Name          IP Address  MAC Address  OS  ESSID  Access
Point        Channel    Type         Role  IPv6 Address  Signal (dB)  Speed
(Mbps)
-----
3e7f6fcff576 10.10.13.33 3e:7f:6f:cf:f5:76 NOFP _owetm_guest-CP3871538578
20:4c:03:b6:b2:5b 60E a-HE External CP fe80::3c7f:6fff:febf:f576 45 (good)
960 (good)
Number of Clients :1
Info timestamp    :21961

20:4c:03:b6:b2:5b#
```

And from the Aruba Central we see that it is indeed the case.

And once the user accepts the terms and type in their credentials, they successfully get connected to the guest network and are assigned the default guest role which is the name of the WLAN SSID.

Now checking ClearPass access tracker.

#	NAS IP Address	Server Name	Source	Username	Service	Login Status	Enforcement Profiles	Request Timestamp
1.	10.10.10.34	CP1-611	RADIUS	cpguser	Simple User Authentication with MAC Caching	ACCEPT	gg MAC Caching Session Limit, gg Guest MAC Caching, [Update Endpoint Known], gg MAC Caching Do Expire, gg MAC Caching Expire Post Login, gg Aruba cnx-guest access, gg MAC Caching Session Timeout	2026/03/24 15:21:31
2.	10.10.10.34	CP1-611	RADIUS	3e7f6fcff576	simple MAC Authentication	REJECT	[Deny Access Profile]	2026/03/24 15:21:18

Summary	Input	Output	Accounting	RADIUS Dynamic Authorization
Enforcement Profiles:		gg MAC Caching Session Limit, gg Guest MAC Caching, [Update Endpoint Known], gg MAC Caching Do Expire, gg MAC Caching Expire Post Login, gg Aruba cnx-guest access, gg MAC Caching Session Timeout		
System Posture Status:		UNKNOWN (100)		
Audit Posture Status:		UNKNOWN (100)		
RADIUS Response				
Endpoint:Guest Role ID		2		
Endpoint:MAC-Auth Expiry		2026-03-25 15:00:00		
Endpoint:Username		cpguser		
Expire-Time-Update:GuestUser		0		
Expiry-Check:Expiry-Action		0		
Post-Auth-Check:Action		Disconnect and Block Access		
Radius:Aruba:Aruba-User-Role		new-guest		
Radius:IETF:Session-Timeout		0		
Radius:IETF:User-Name		cpguser		
Session-Check:Active-Session-Count		10		
Status-Update:Endpoint		Known		

Note that from the above screenshot we see that ClearPass is sending back a user-role called “new-guest” and since it was not configured as a use role, Central is ignoring it and assigning the default user role to it.

We need to test the CoA which you can easily do by clicking on “Change Status”. And that will result in a wireless terminate that forces the client to re-connect and this time the MAC auth service will be successful. This way we are also testing MAC caching feature.

2.	10.10.10.34	CP1-611	RADIUS	cpguser	simple MAC Authentication	ACCEPT	gg Aruba cnx-guest access, gg MAC Auth Session Timeout	2026/03/24 15:37:06
3.	10.10.10.34	CP1-611	RADIUS	cpguser	Simple User Authentication with MAC Caching	ACCEPT	gg MAC Caching Session Limit, gg Guest MAC Caching, [Update Endpoint Known], gg MAC Caching Do Expire, gg MAC Caching Expire Post Login, gg Aruba cnx-guest access, gg MAC Caching Session Timeout	2026/03/24 15:32:37
4.	10.10.10.34	CP1-611	RADIUS	3e7f6fcff576	simple MAC Authentication	REJECT	[Deny Access Profile]	2026/03/24 15:32:04

Lastly always check if you have got the RADIUS accounting working correctly. So clicking on the “simple MAC authentication” session, you should see the “Accounting” tab that indicates, ClearPass is receiving accounting records from the AP.

Summary	Input	Output	Accounting
Account Session ID:	D0D3E0B22A94-3E7F6FCFF576-69C21B8F-B9BF5		
Start Timestamp:	Mar 24, 2026 16:05:19 AEDT		
End Timestamp:	Still Active		
Status:	Active		
Termination Cause:	-		
Service Type:	Login-User		
Number of Accounting Sessions:	1		
Network Details			
Utilization			
Accounting Sessions Details			

Here we do a remote console to the AP and run a few CLI commands.

```
20:4c:03:b6:b2:5b# sh clients

Client List
-----
Name      IP Address  MAC Address  OS      ESSID      Access Point
Channel  Type  Role      IPv6 Address  Signal (dB)  Speed (Mbps)
-----  -----  -
cpguser  10.10.13.33  3e:7f:6f:cf:f5:76  Linux  owetm_guest-CP3871538578  20:4c:03:b6:b2:5b
60E      a-HE  guest-CP  fe80::3c7f:6fff:febf:f576  51(good)  1080(good)
Number of Clients      :1
Info timestamp        :25770

20:4c:03:b6:b2:5b#
20:4c:03:b6:b2:5b# show access-rule guest-CP

ACL Vlan      :
ACL Captive Portal:disable
ACL ECP Profile :default
CALEA          :disable
Redirect Blocked HTTPS Traffic :disable
DPI error page URL:
Bandwidth Limit :downstream disable upstream disable
airslice-application-list      :
monitoring-application-list    :
Access Rules
-----
Dest IP  Dest Mask  Eth Type  Dest Match  Protocol (id:sport:eport)  Application  Action  Log
TOS  802.1P  Denylist  App Throttle (Up:Down)  Mirror  DisScan  ClassifyMedia  TimeRange
-----  -----  -
any      any      IPv4/6  match      any      permit
ClassifyMedia

20:4c:03:b6:b2:5b#
```

4.4 References

For comprehensive configuration detail in New Central you can refer to Validated Solution Guide - [Central Configuration Example](#)

You can also refer to the [Central Online documentation](#).

5 ClearPass Configuration for Reference




For completeness I have included the ClearPass authentication and guest captive portal configuration. Details and explanation on these services are omitted, as the focus is on New Central configuration. Screenshots are included for reference.

Services

-  Add
-  Import
-  Export All

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

Filter: contains Hit Count for Show records

#	Order	Name	Type	Template	Hit Count	Status
14.	<input type="checkbox"/>	14 -----Guest -Mac Auth Wireless Services-----	RADIUS	Cisco Web Authentication Proxy	0	
15.	<input type="checkbox"/>	15 simple MAC Authentication	RADIUS	MAC Authentication	1	
16.	<input type="checkbox"/>	16 Simple User Authentication with MAC Caching	RADIUS	RADIUS Enforcement (Generic)	0	

5.1 Services - simple MAC Authentication

Summary Service Authentication Authorization Roles Enforcement

Name:

Description:

Type:

Status:

Monitor Mode: Enable to monitor network access without enforcement

More Options: Authorization Audit End-hosts Profile Endpoints Accounting Proxy

Service Rule

Matches ANY or ALL of the following conditions:

	Type	Name	Operator	Value
1.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
2.	Connection	SSID	CONTAINS	uest

Summary Service Authentication Authorization Roles Enforcement

Authentication Methods:

--Select to Add--

Authentication Sources:

Summary Service Authentication Authorization Roles Enforcement

Authentication Methods:

--Select to Add--

Authentication Sources:

Summary Service Authentication Authorization Roles Enforcement

Authorization Details:

Authorization sources from which role mapping attributes are fetched (for each Authentication Source)

Authentication Source	Attributes Fetched From
1. [Endpoints Repository] [Local SQL DB]	[Endpoints Repository] [Local SQL DB]

Additional authorization sources from which to fetch role-mapping attributes -

Summary	Service	Authentication	Authorization	Roles	Enforcement
Role Mapping Policy: <input type="text" value="simple MAC Authentication Role Mapping"/> <input type="button" value="Modify"/>					
Role Mapping Policy Details					
Description:					
Default Role: [Other]					
Rules Evaluation Algorithm: evaluate-all					
Conditions			Role		
1. (Authorization:[Endpoints Repository]:Unique-Device-Count EXISTS) AND (Authorization:[Time Source]:Now DT LESS_THAN %{Endpoint:MAC-Auth Expiry}) AND (Authorization:[Guest User Repository]:AccountExpired EQUALS false) AND (Authorization:[Guest User Repository]:AccountEnabled EQUALS true)			[MAC Caching]		
2. (Endpoint:Guest Role ID EQUALS 1)			[Contractor]		
3. (Endpoint:Guest Role ID EQUALS 2)			[Guest]		
4. (Endpoint:Guest Role ID EQUALS 3)			[Employee]		

Summary	Service	Authentication	Authorization	Roles	Enforcement
Use Cached Results: <input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions					
Enforcement Policy: <input type="text" value="simple MAC Authentication Enforcement Policy"/> <input type="button" value="Modify"/> Add New Enforcement Policy					
Enforcement Policy Details					
Description:					
Default Profile: [Deny Access Profile]					
Rules Evaluation Algorithm: first-applicable					
Conditions			Enforcement Profiles		
1. (Tips:Role MATCHES_ALL [MAC Caching]) [Guest] AND (Connection:SSID CONTAINS guest-CP)			gg Aruba cnx-guest access, gg MAC Auth Session Timeout		
6. (Tips:Role MATCHES_ANY [Guest]) [Contractor] [Employee] AND (Connection:SSID EQUALS guest)			[Allow Access Profile], Aruba Redirect access		

5.2 Services - Simple User Authentication with MAC Caching

Summary	Service	Authentication	Authorization	Roles	Enforcement
Name: <input type="text" value="Simple User Authentication with MAC Caching"/>					
Description: <input type="text" value="Captive Portal authentication with MAC Caching"/>					
Type: RADIUS Enforcement (Generic)					
Status: Enabled					
Monitor Mode: <input type="checkbox"/> Enable to monitor network access without enforcement					
More Options: <input checked="" type="checkbox"/> Authorization <input type="checkbox"/> Posture Compliance <input type="checkbox"/> Audit End-hosts <input type="checkbox"/> Profile Endpoints <input type="checkbox"/> Accounting Proxy					
Service Rule					
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:					
Type	Name	Operator	Value		
1. Radius:IETF	Calling-Station-Id	EXISTS			
2. Connection	Client-Mac-Address	NOT_EQUALS	%{Radius:IETF:User-Name}		
3. Connection	SSID	CONTAINS	uest		

Summary	Service	Authentication	Authorization	Roles	Enforcement
Authentication Methods:					
<div style="border: 1px solid #ccc; padding: 5px; display: flex; align-items: flex-start;"> <div style="flex: 1;"> <p>[PAP]</p> <p>[MSCHAP]</p> <p>[CHAP]</p> </div> <div style="flex: 0.5; text-align: center; margin-left: 10px;"> <input type="button" value="Move Up ↑"/> <input type="button" value="Move Down ↓"/> <input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/> </div> </div>					
<input type="text" value="--Select to Add--"/>					
Authentication Sources: <input type="text" value="[Guest User Repository] [Local SQL DB]"/>					

Summary	Service	Authentication	Authorization	Roles	Enforcement
Authorization Details: Authorization sources from which role mapping attributes are fetched (for each Authentication Source)					
Authorization Source		Attributes Fetched From			
1.	[Guest User Repository] [Local SQL DB]	[Guest User Repository] [Local SQL DB]			
2.	AD1 [Active Directory]	AD1 [Active Directory]			
Additional authorization sources from which to fetch role-mapping attributes -					
[Endpoints Repository] [Local SQL DB]		[Remove]		Add New .	
[Time Source] [Local SQL DB]		[View Details]			

Summary	Service	Authentication	Authorization	Roles	Enforcement
Role Mapping Policy: simple User Authentication with MAC Caching Role Mapping Modify					
Role Mapping Policy Details					
Description:					
Default Role:	[Other]				
Rules Evaluation Algorithm:	evaluate-all				
Conditions					Role
1.	(GuestUser:Role ID EQUALS 1)				[Contractor]
2.	(GuestUser:Role ID EQUALS 2)				[Guest]
3.	(GuestUser:Role ID EQUALS 3)				[Employee]

Summary	Service	Authentication	Authorization	Roles	Enforcement
Use Cached Results: <input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions					
Enforcement Policy: simple User Authentication with MAC Caching Enforcement Policy Modify Add New Enforcement Policy					
Enforcement Policy Details					
Description:					
Default Profile:	[Allow Access Profile]				
Rules Evaluation Algorithm:	first-applicable				
Conditions					Enforcement Profiles
1.	(Authorization:[Endpoints Repository]:Unique-Device-Count GREATER_THAN 10)				[Deny Access Profile]
7.	(Tips:Role EQUALS [Guest]) AND (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday) AND (Connection:SSID CONTAINS guest-CP)				gg Aruba cnx-guest access, gg MAC Caching Session Timeout, gg MAC Caching Session Limit, gg Guest MAC Caching, [Update Endpoint Known], gg MAC Caching Do Expire, gg MAC Caching Expire Post Login

5.3 Web Login (school)

And finally Home » Configuration » Pages » Web Logins

Web Login Editor	
* Name:	school <small>Enter a name for this web login page.</small>
Page Name:	school <small>Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".</small>
Description:	for AOS-10 Lab <small>Comments or descriptive text about the web login.</small>
* Vendor Settings:	Aruba <small>Select a predefined group of settings suitable for standard network configurations.</small>
Login Method:	Controller-initiated — Guest browser performs HTTP form submit <small>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.</small>
* Address:	captiveportal-login.arubatechs.com <small>Enter the hostname (FQDN) of the vendor's product here. When using Secure Login over HTTPS, this name should match the name of the HTTPS certificate installed on your device.</small>
Secure Login:	Use vendor default <small>Select a security option to apply to the web login process.</small>
Dynamic Address:	<input type="checkbox"/> The controller will send the IP to submit credentials <small>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.</small>

Note that AP is using wildcard certificate as its captive portal certificate.