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

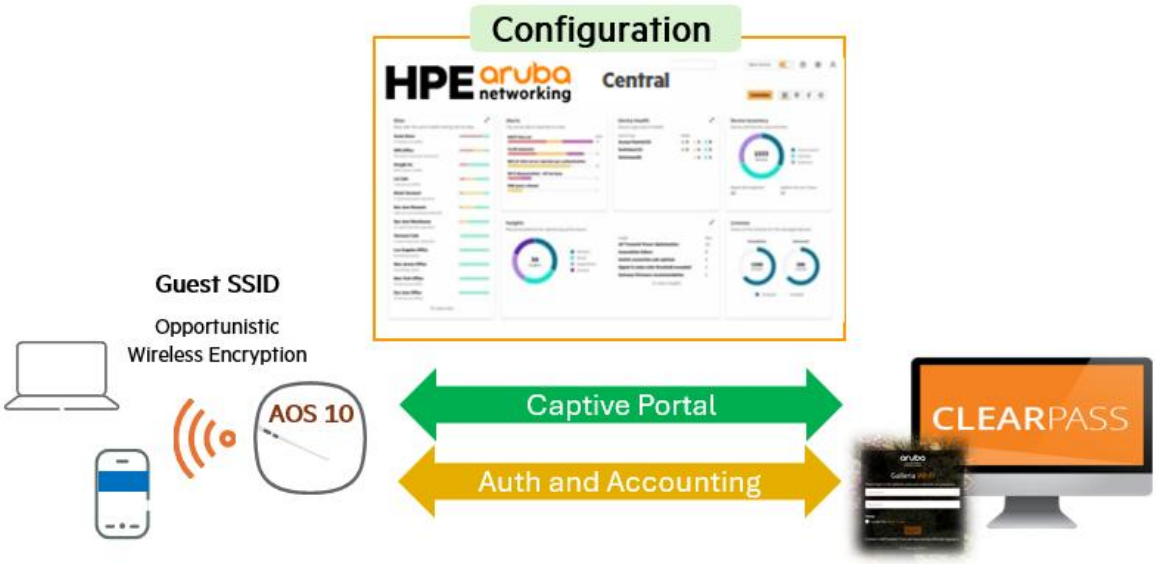
DATE	VERSION	EDITOR	CHANGES
24 Mar 2026	0.1	Ariya Parsamanesh	Initial creation
02 Apr 2026	0.2	Ariya Parsamanesh	Added the testing section

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.

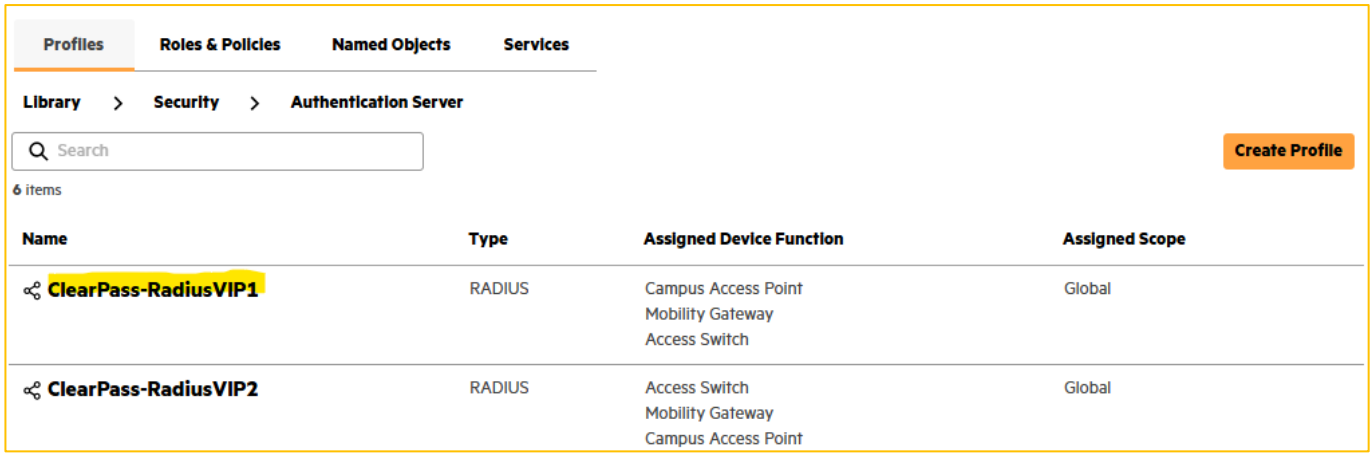
3 AOS10 AP Configuration

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.

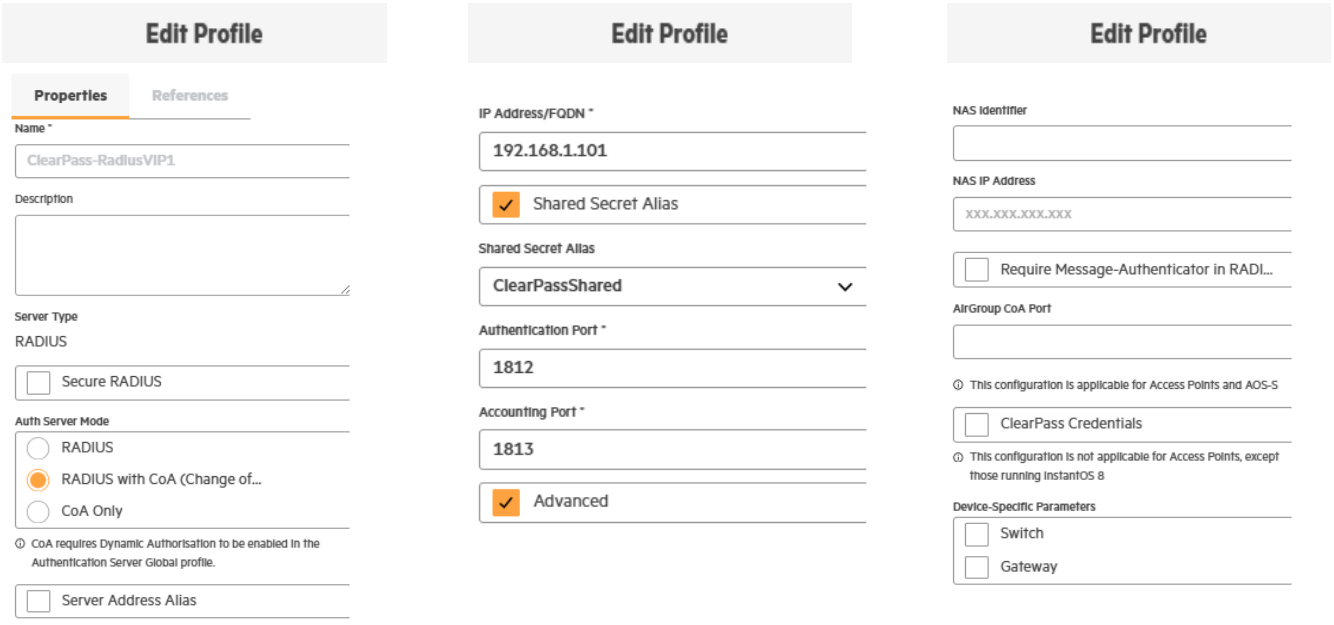
1. Configure AAA Authentication profile
2. Assign the Authentication servers to Authentication server Group
3. Captive portal Profile
4. User role and Policies (as required)
5. Configure Guest WLAN profile
6. Import Certificate for guest redirection
7. Certificate usage

3.1 Authentication Server Profile

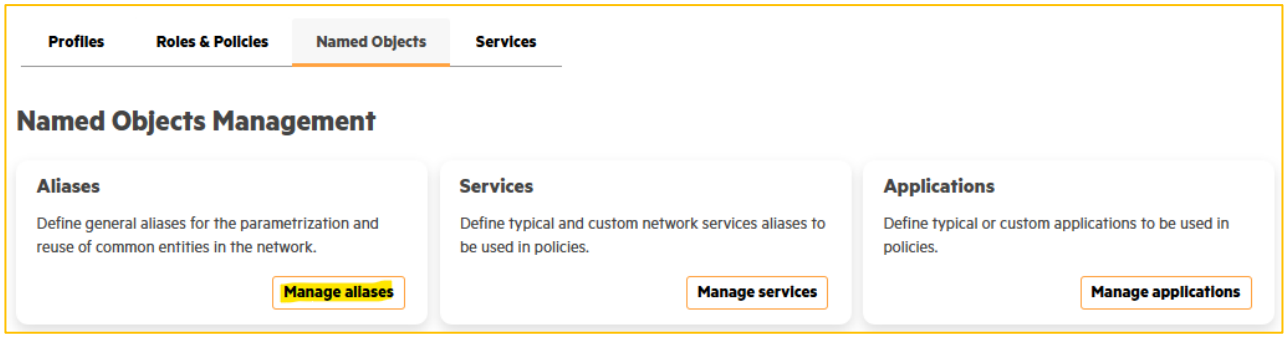
Since I have an existing on Premise NAC appliance (ClearPass) I'll use that as my authentication server. Note that I have two ClearPass nodes, I have already configured them for HA and have a Virtual IP (VIP) which I am using here. If you already have this configured, you can skip this section.

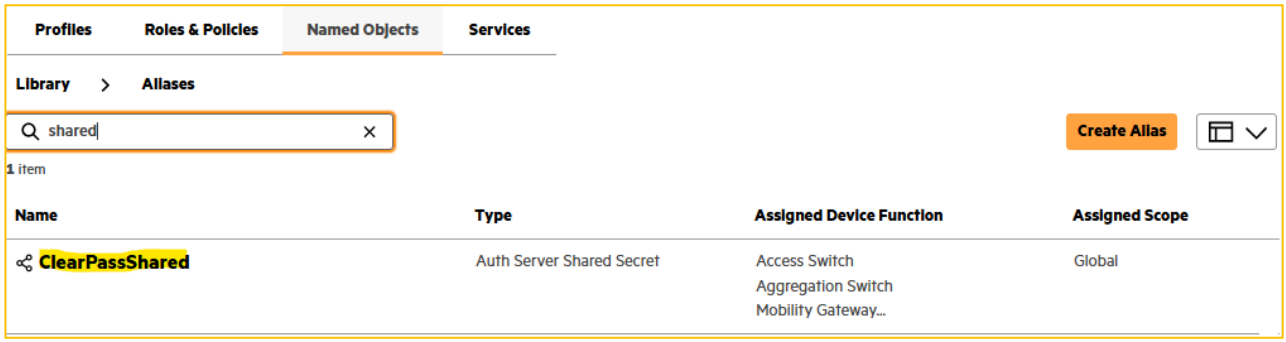


You can see below ClearPassRadiusVIP1 server. You can also select device specific parameters for switches and gateways. Note that you can use IP address or FQDN, here I am using IP addresses.



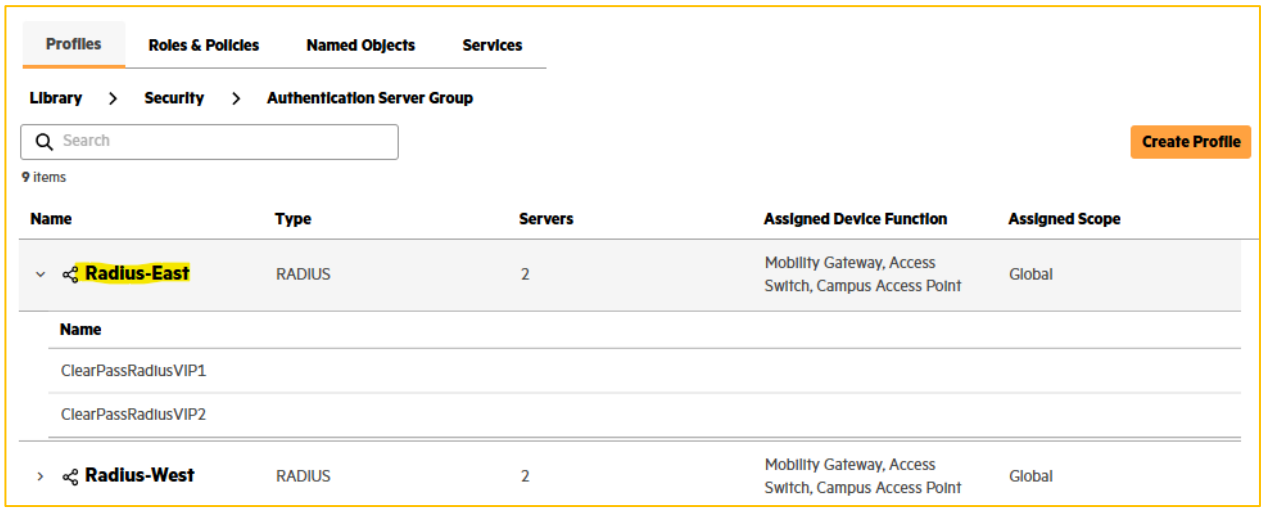
Note that I am using Radius with CoA and also “Shared Secret Alias”. Now to be able to use the “Shared Secret Alias” you need to define it first and you do that by creating an alias from Named Objects tab as shown below.





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

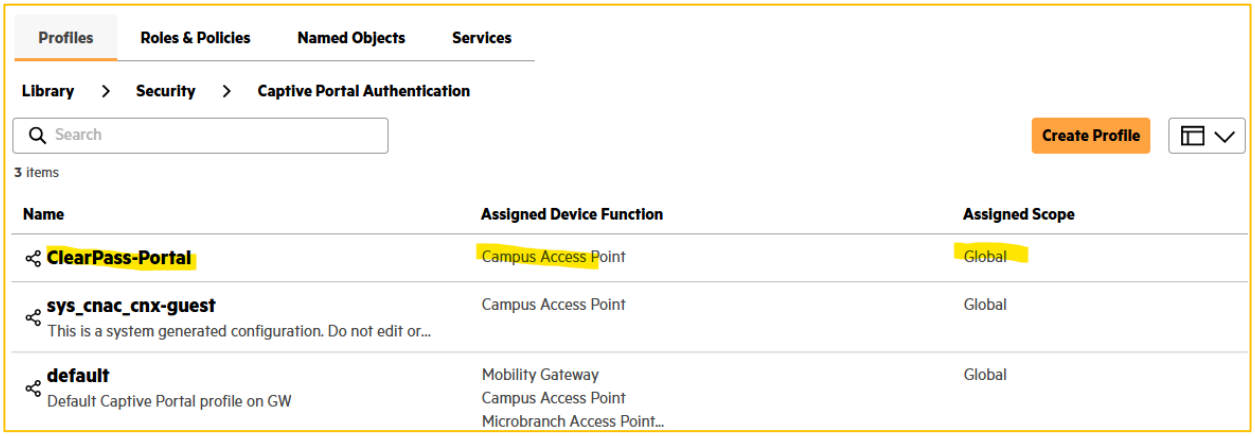
Next, we must configure Authentication server group that will include the Auth servers we just configured. Here I have two authentication server groups to distribute my auth session across my configured authentication servers and I am showing only one of them called “Radius-East” where I have added the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



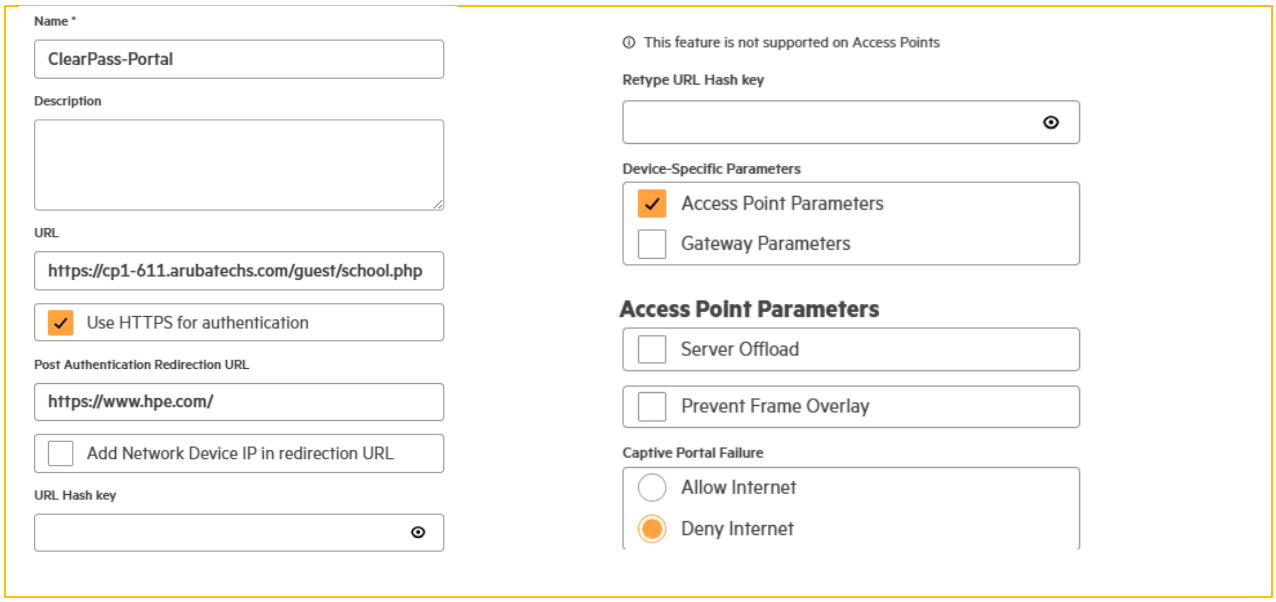
Note that there is specific configuration setting just for Switches and/or gateways which is not shown here. So, you can have all those configured in one profile. And this specific configuration will one be applied to the specified device personas.

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.

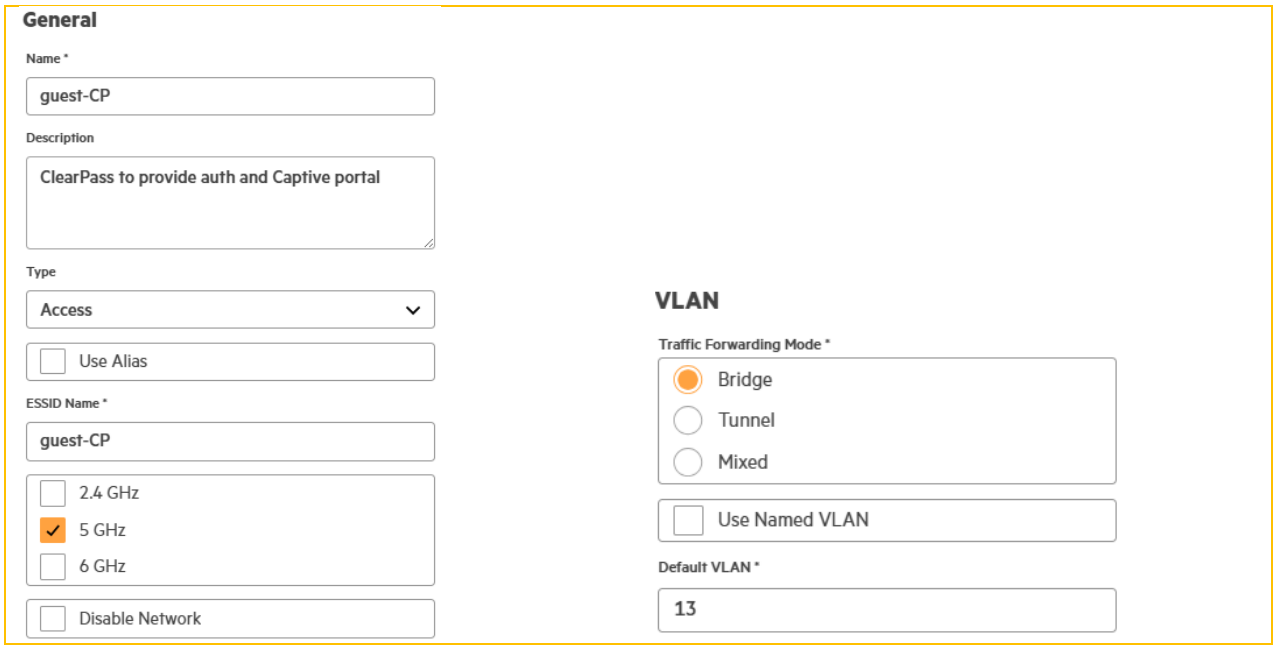


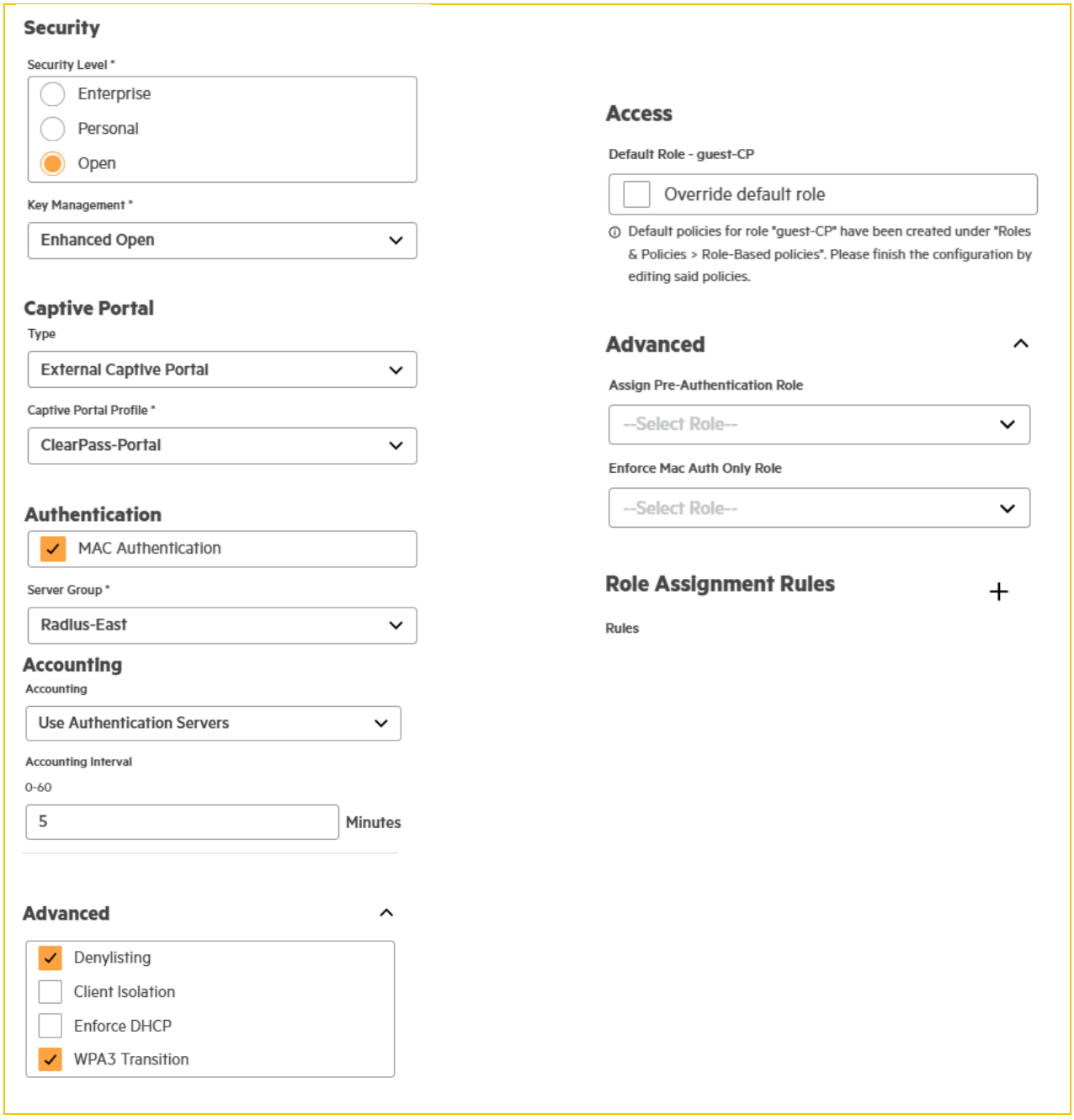
Here is the Captive Portal Profile that I have configured. Note that I have added the URL for the captive portal and it's in FQDN format that will not cause any warning or errors. The guest captive portal URL is from ClearPass.



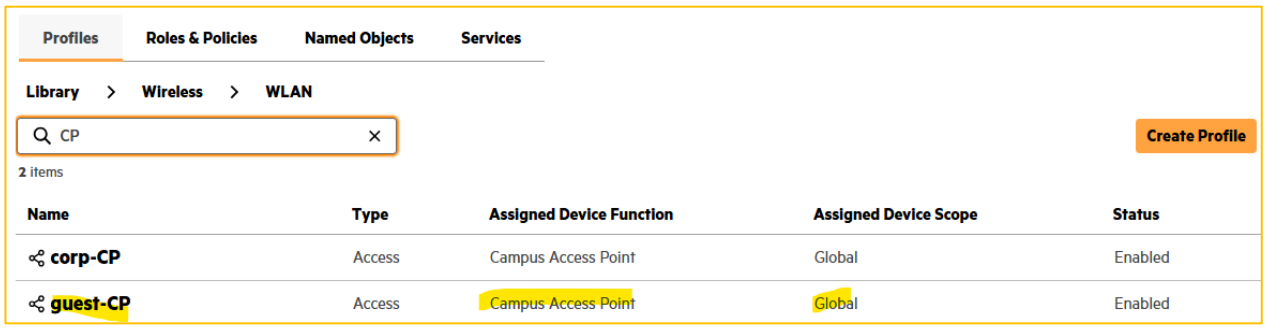
3.3 WLAN Profile

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.





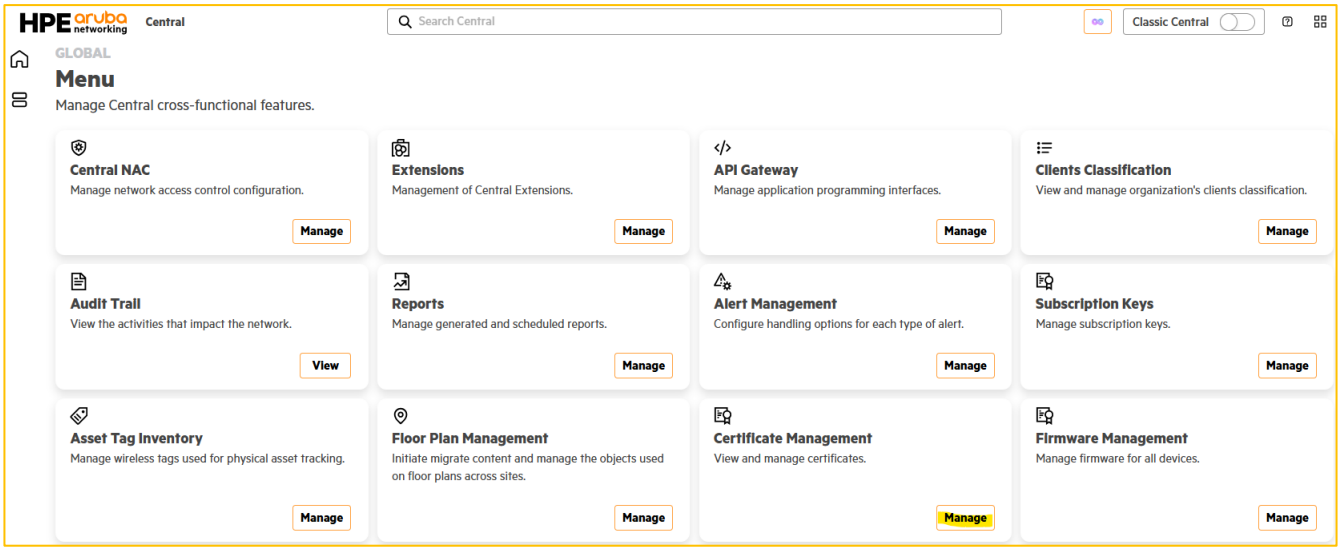
And once it is saved it will be displayed as shown below.



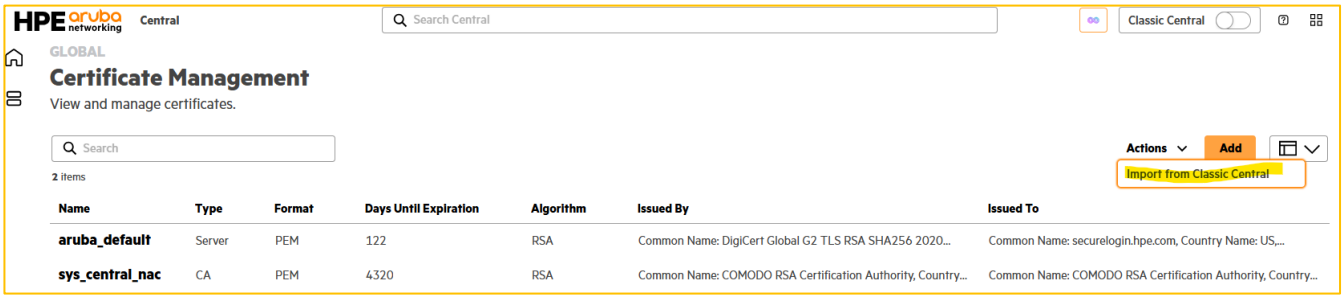
You can also change the default role, though it will usually match the WLAN profile name unless you specify otherwise. Additionally, I chose not to set a pre-auth user role since I'll be using the default pre-auth role, but you do have the option to assign one if desired.

3.4 Certificate Management

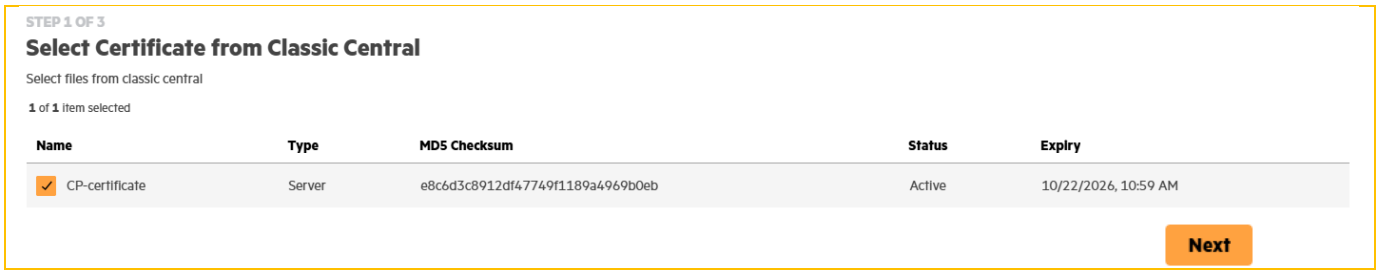
One of the key aspects of any external captive portal configuration is to assign a publicly signed server certificate to the APs so that when the APs perform the HTTPS redirection, the user browser does not complain with warning or even fail. So here we go to the Certificate Management section to import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

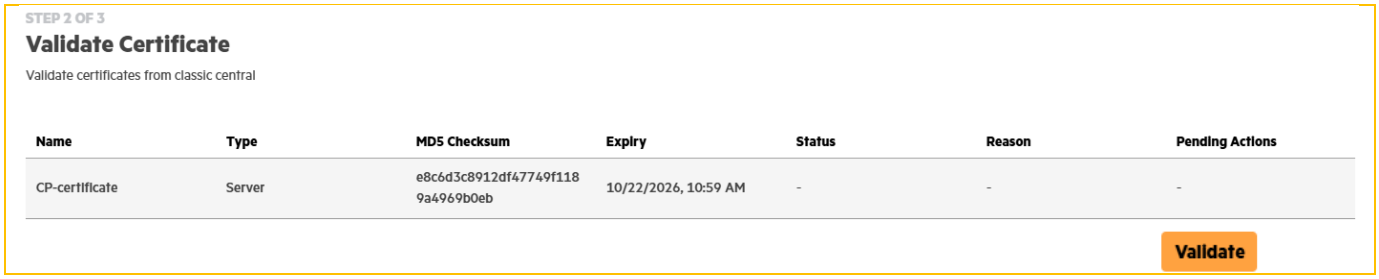


Here you'll notice that we are going to import the certificate from Classic Central. So here the assumption is that we were using Classic Central for AOS10 guest WLAN with ClearPass as captive portal and now we want to use the same certificate for New Central configuration. Alternatively, you can add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

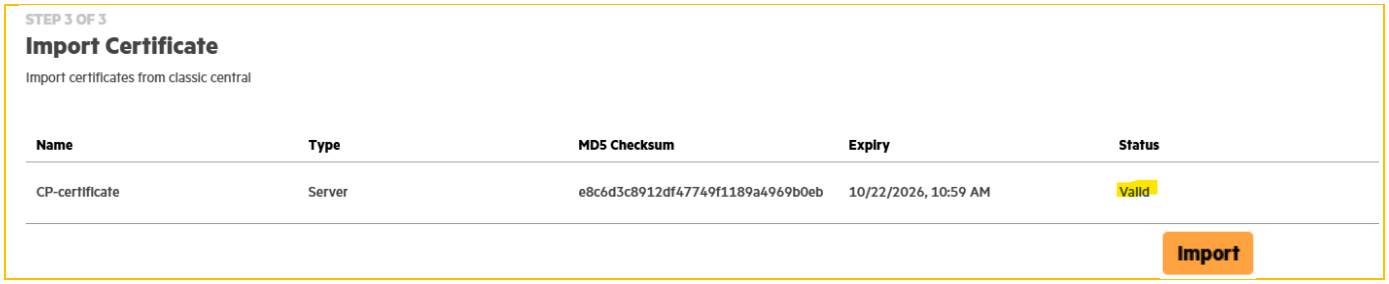


The import from Classic Central involves three steps process that are shown here.

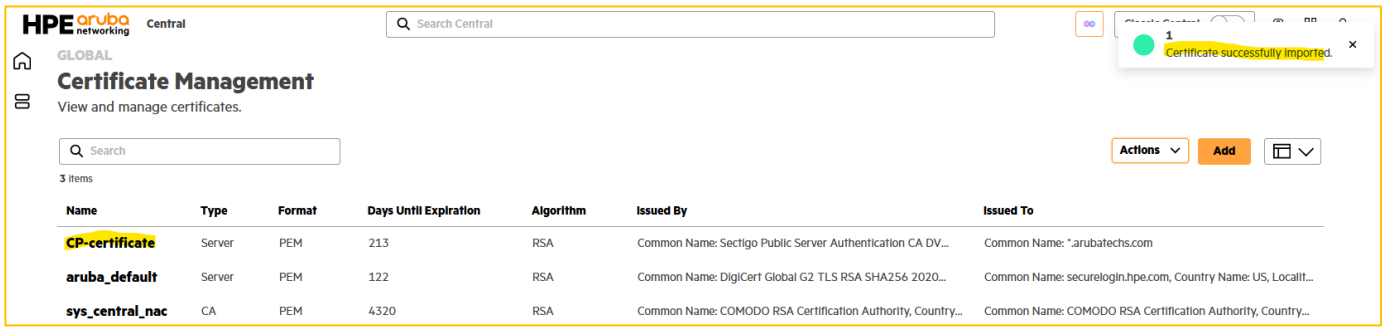




Once you click on the "Validate" button, the certificate gets validated as shown below.

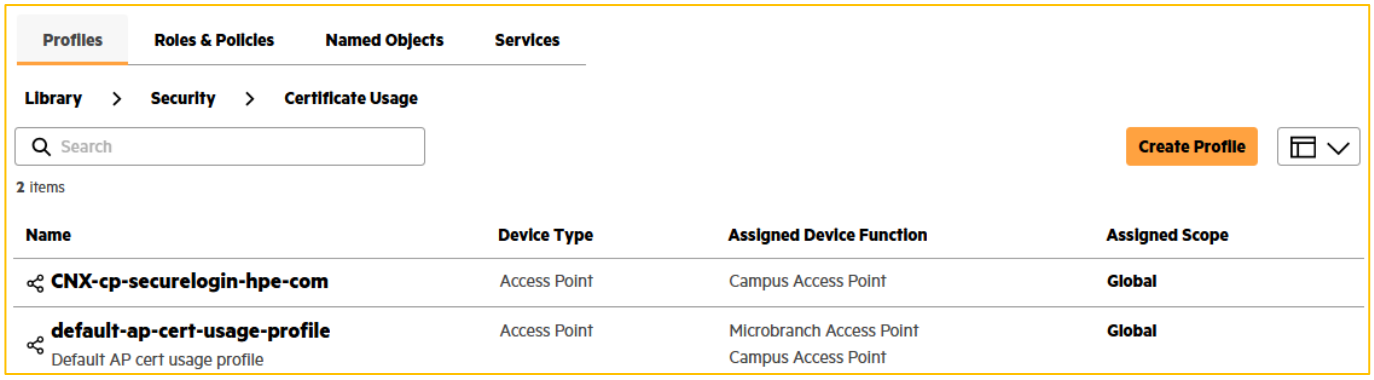


After clicking on the “Import” button, it gets added to the certificates that can be used.

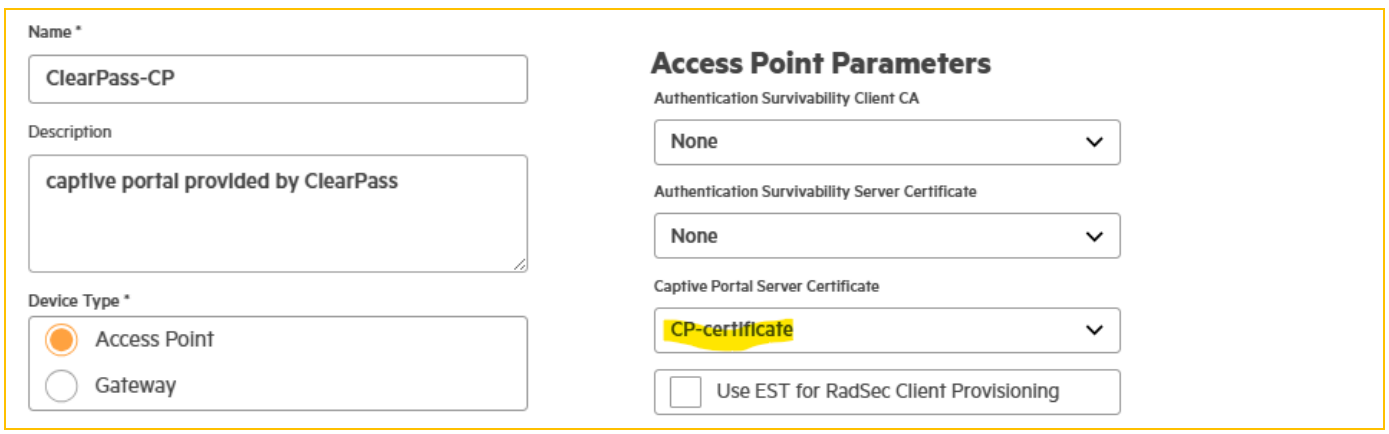


3.5 Certificate Usage

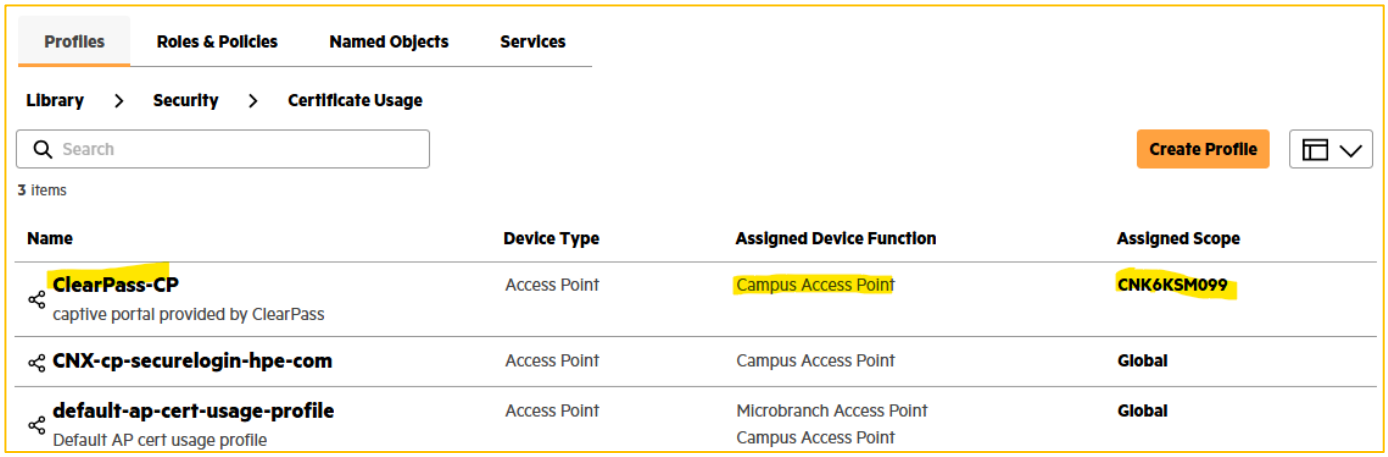
The last step of the certificate management is assigning its usage for captive portal purposes. So again, from Library we will create a certificate usage profile.



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.



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

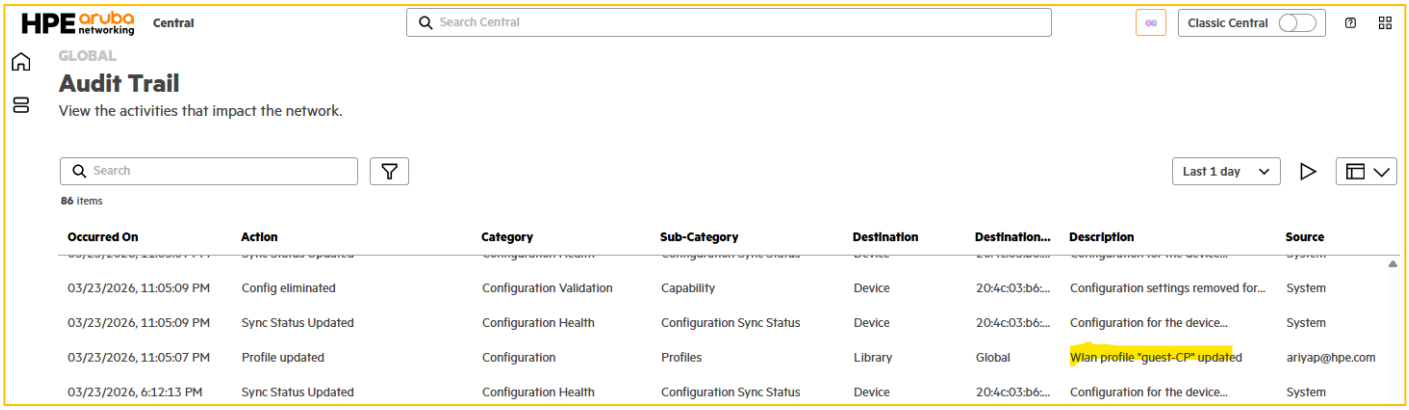


Note that I have not assigned any Authentication role all that will be handled by

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.



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.

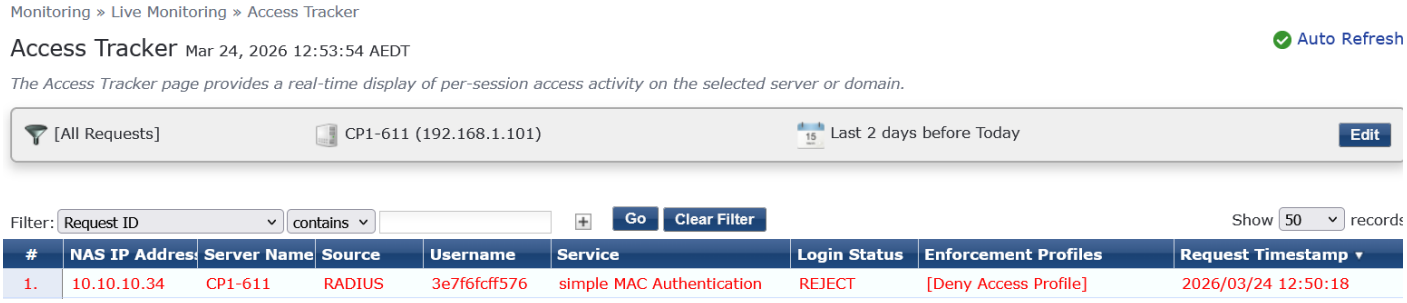

```
20:4c:03:b6:b2:5b# sh cert assignment

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.

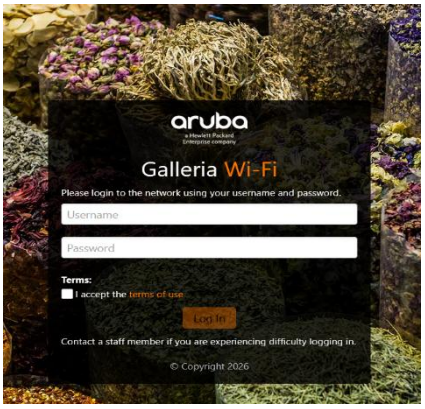
```
20:4c:03:b6:b2:5b# sh cert assignment

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.



#	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



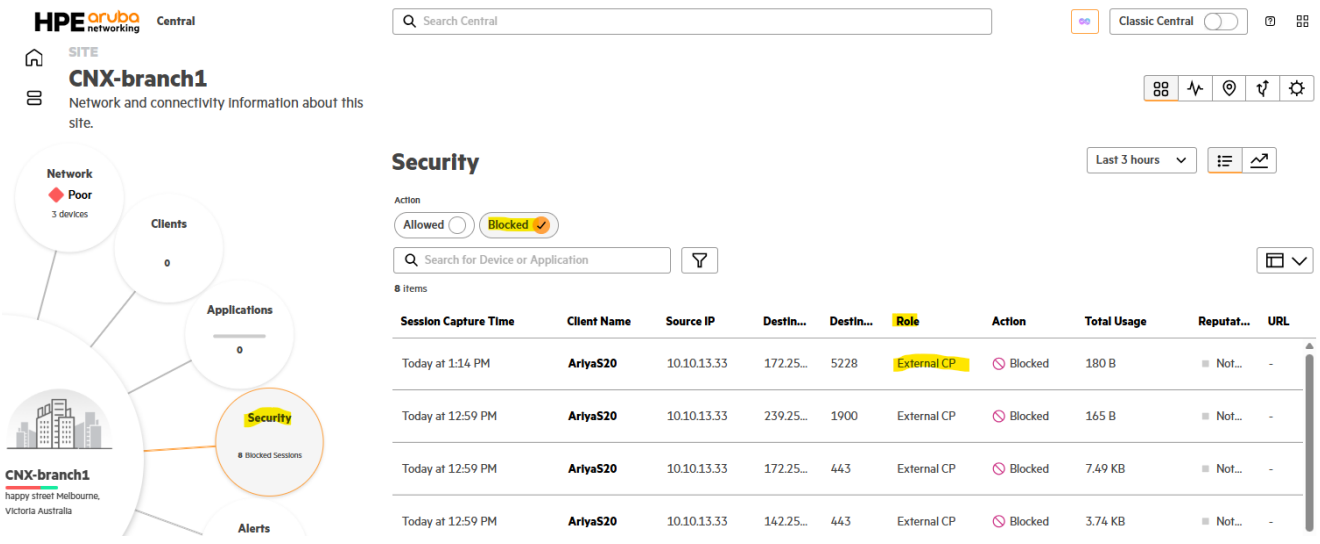
A MAC authentication failure shown above is expected. The client is placed in a captive portal user role and redirected to the configured Guest captive portal URL.

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.

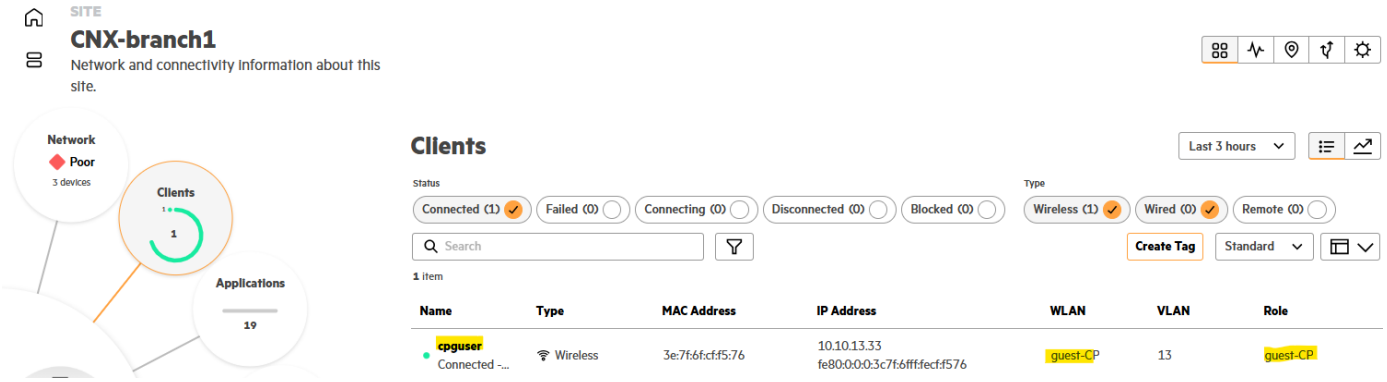
Here you can see the user role that was assigned.

```
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:fecf: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 Addres	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

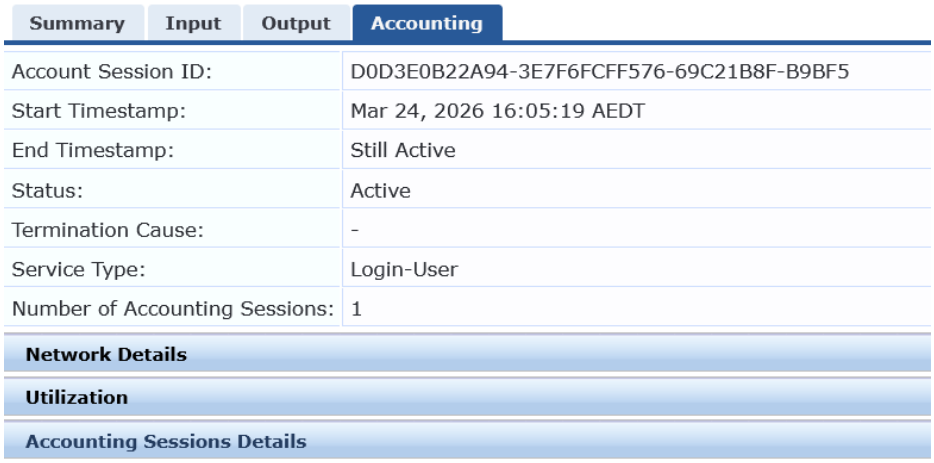
◀ Showing 2 of 1-22 records ▶ | Change Status | Show Configuration | Export | Show Logs | Close

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.



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:fecf: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: Name contains Go Clear Filter Hit Count for Current hour Show 50 records

#	Order	Name	Type	Template	Hit Count	Status
14.	14	--------Guest -Mac Auth Wireless Services----------	RADIUS	Cisco Web Authentication Proxy	0	
15.	15	simple MAC Authentication	RADIUS	MAC Authentication	1	
16.	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:	gg MAC Authentication
Description:	MAC Authentication bypass for captive portal users
Type:	MAC Authentication
Status:	Disabled
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: [Allow All MAC AUTH] — Move Up ↑ | Move Down ↓ | Remove | View Details | Modify

--Select to Add--

Authentication Sources: [Endpoints Repository] [Local SQL DB]

Summary | Service | Authentication | Authorization | Roles | Enforcement

Authentication Methods: [Allow All MAC AUTH] — Move Up ↑ | Move Down ↓ | Remove | View Details | Modify

--Select to Add--

Authentication Sources: [Endpoints Repository] [Local SQL DB]

Summary | Service | Authentication | Authorization | Roles | Enforcement

Authorization Details:

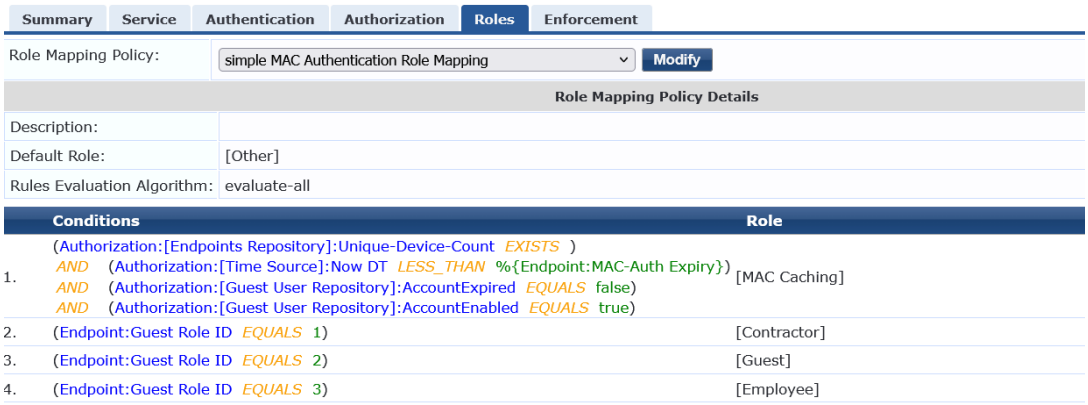
Authorization sources from which role mapping attributes are fetched (for each Authentication Source)

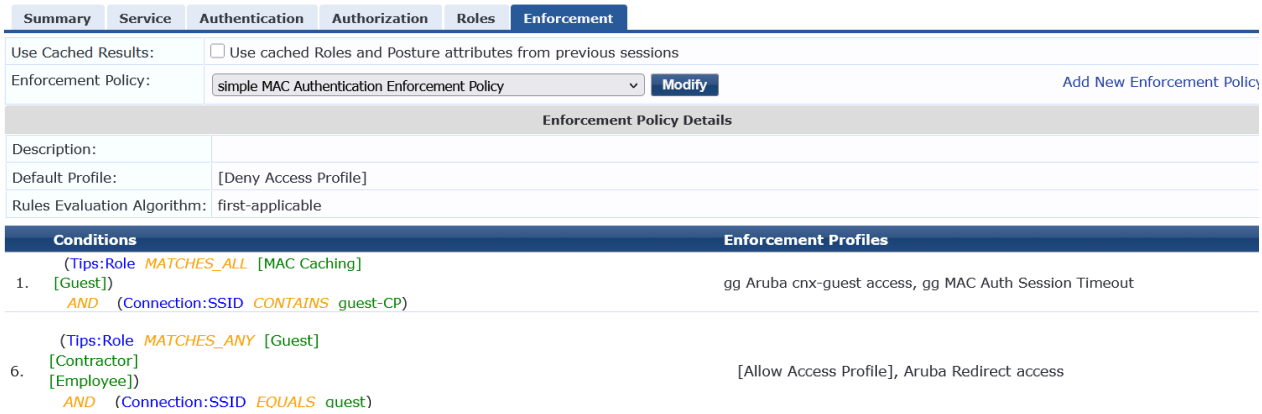
	Authentication Source	Attributes Fetched From
1.	[Endpoints Repository] [Local SQL DB]	[Endpoints Repository] [Local SQL DB]

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

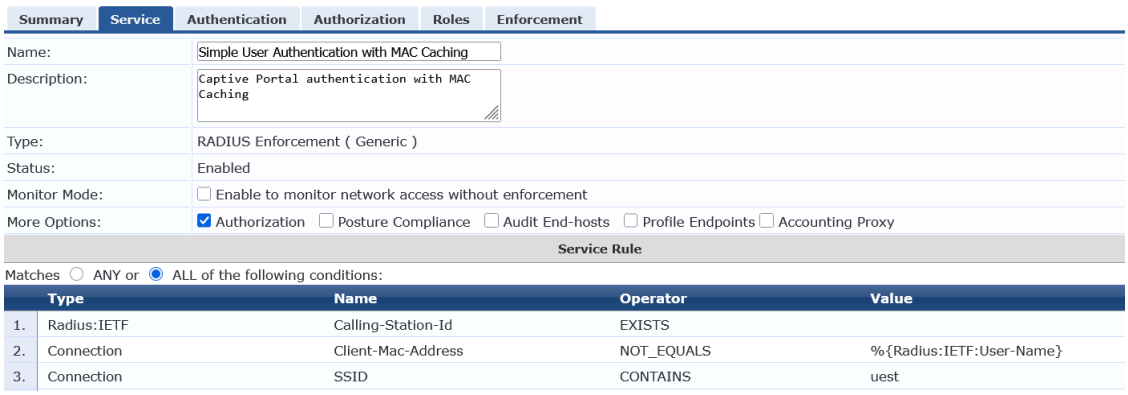
[Time Source] [Local SQL DB]
[Guest User Repository] [Local SQL DB]

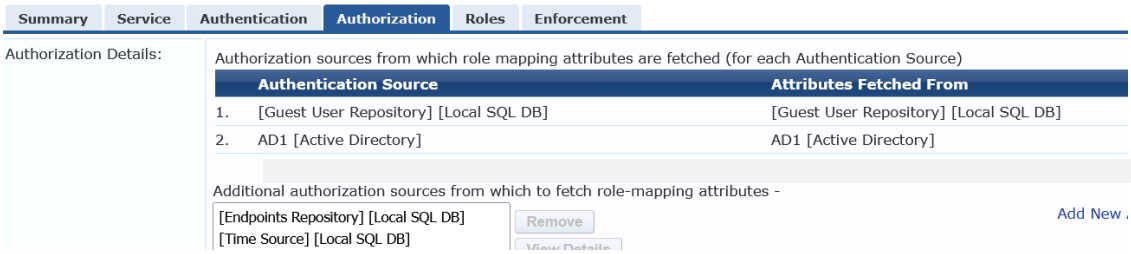
Remove

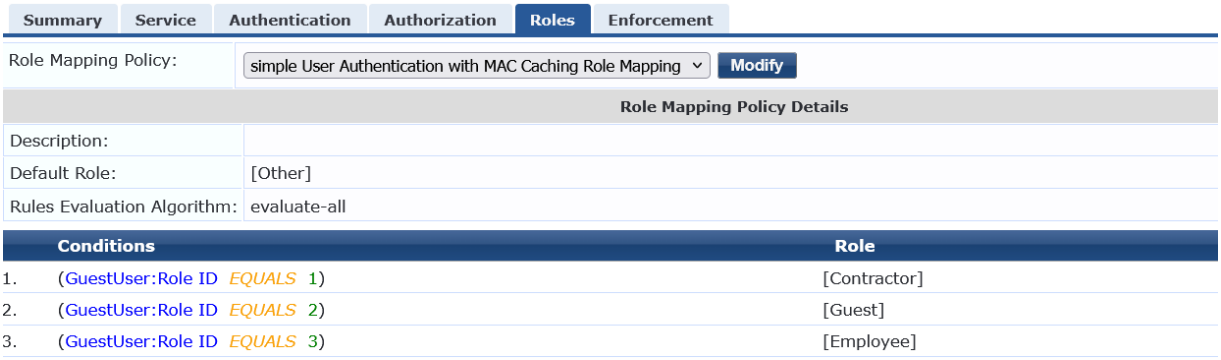


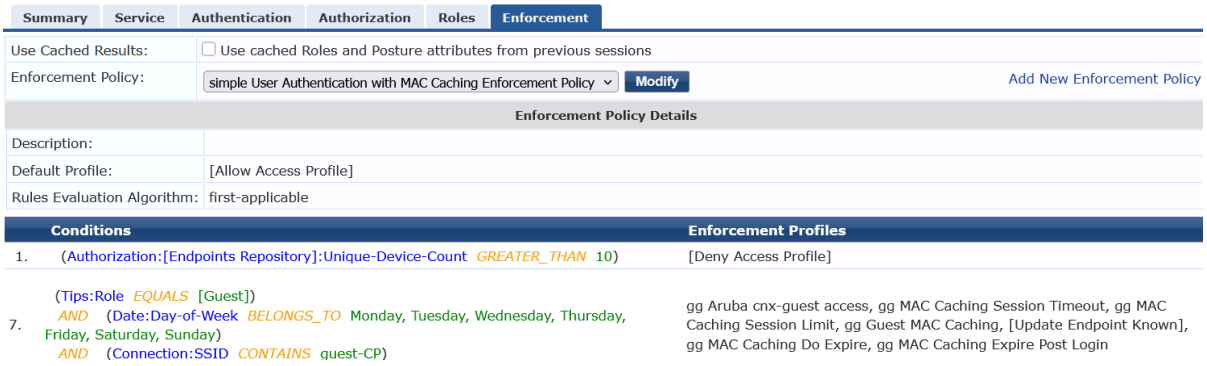


5.2 Services - Simple User Authentication with MAC Caching



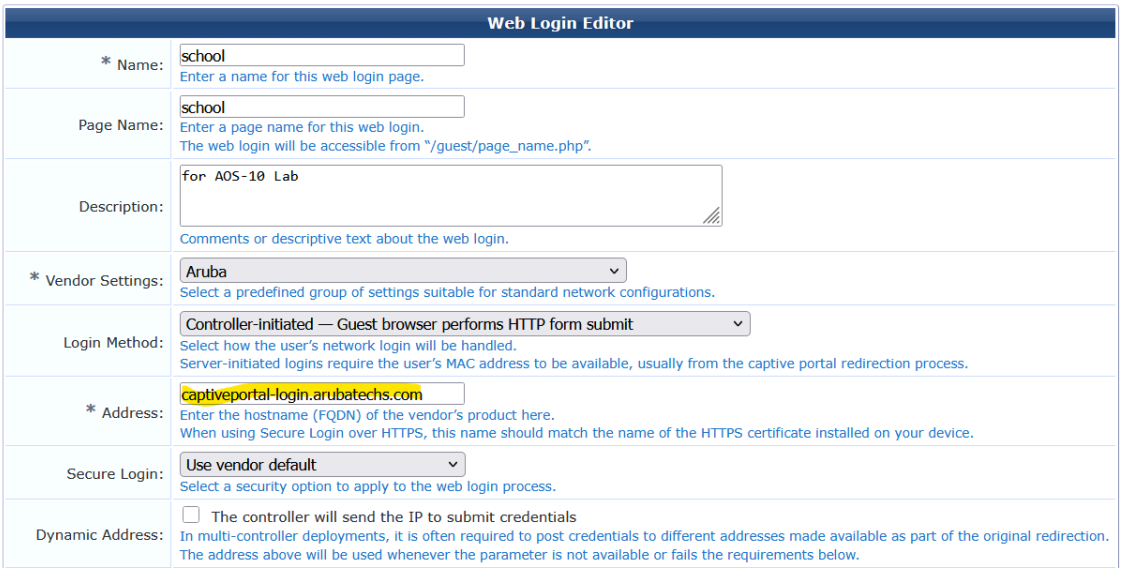






5.3 Web Login (school)

And finally Home » Configuration » Pages » Web Logins



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