

1 Table of Contents

1	Table of Contents	1
1.1	Revision History	1
2	New Central Configuration for Tunnelled WLANs	2
2.1	Things you need.....	2
3	Roles and Policies Configuration	3
3.1	User Roles	3
4	WLAN Configuration and Testing	8
4.1	Tunnel WLAN dot1x Configuration.....	8
4.2	AP and Gateway Testing	9
4.3	Dot1x User Testing	13
4.4	Tunnel WLAN Guest Configuration.....	14
4.5	Guest User Testing.....	19
4.6	Tunnel WLAN Guest Configuration with customised User Role.....	24
4.7	User Testing with Customised User Roles	26
4.8	References	27

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
09 Jun 2026	0.1	Ariya Parsamanesh	Initial creation
23 Jun 2026	0.2	Ariya Parsamanesh	Added the testing section

2 New Central Configuration for Tunnelled WLANs

Background

This technote builds on the previous one, where I covered how to onboard and configure Mobility Gateways running HPE Aruba Networking Wireless Operating System 10 (AOS-10) using the New Central cloud-native platform. That technote also covered the basic gateway configuration, including link aggregation and clustering.

Scope

In this technote, I'll focus on the element profiles required to configure AOS-10 AP WLANs that operate in tunnel mode connecting to the mobility gateway cluster. Each profile is explained in context, including why it is needed, so the configuration is easier to follow even if you are not familiar with every technical detail.

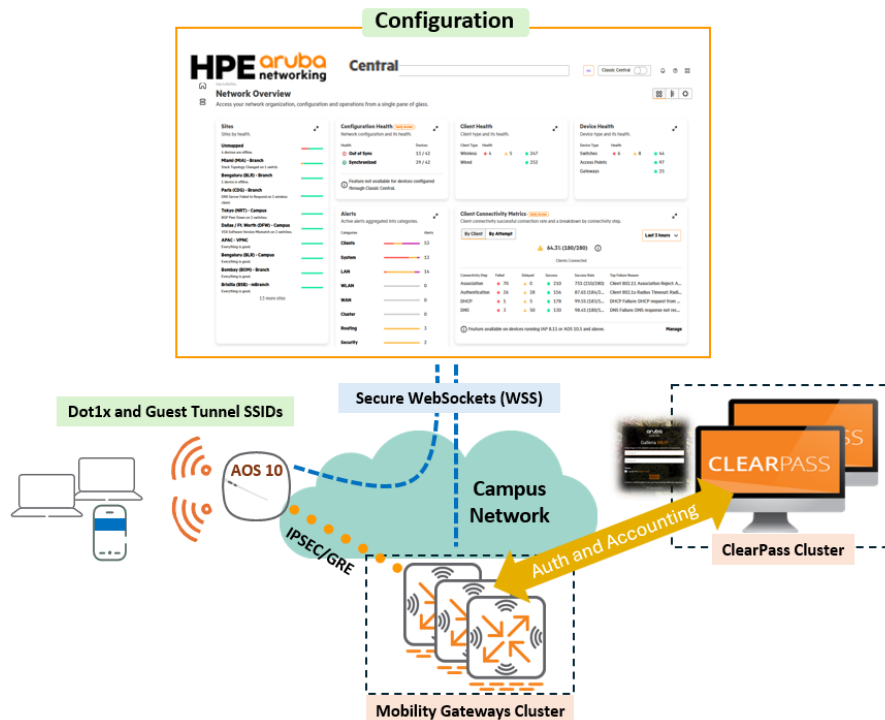
Configuration scenarios

I'll cover two tunnelled WLAN scenarios:

- A tunnelled 802.1X WLAN that derives dynamic user roles.
- A tunnelled guest WLAN that uses external captive portal services.

For both scenarios, I'll use a ClearPass cluster for authentication. ClearPass will also provide the captive portal guest services for the guest WLAN.

The focus is on configuring New Central, not on the ClearPass setup. I assume ClearPass is already configured for 802.1X authentication and guest captive portal services.



2.1 Things you need

- Couple of gateways running minimum AOS10 firmware version or 10.4.1.7 (I am using 10.7.2.5)
- AOS10 APs are already online in New Central.
- Valid HPE Aruba Central account and subscriptions
- ClearPass that is already configured as external authentication server and guest captive portal.

3 Roles and Policies Configuration

In the previous technote, where I configured the gateways, I did not cover user roles. One key point with tunnelled WLANs is that all user traffic is sent through a GRE tunnel between the AP and the gateway. While both the AP and the gateway can technically enforce policy, the best practice is to apply user traffic policy at the gateway.

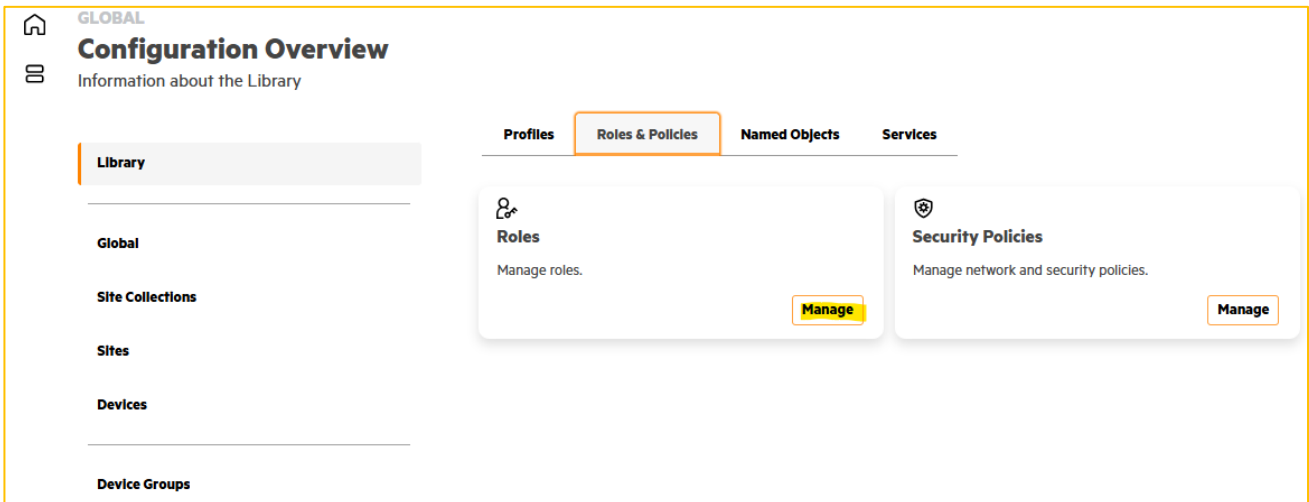
When you configure a WLAN element profile, Aruba Central automatically creates a default role for that WLAN. It then assigns that role to both the campus AP and gateway device functions. In most cases, the default role uses an allow-all policy, which allows traffic to pass from the AP to the gateway without being blocked.

For any additional roles you create, assign them only to the gateway device types and appropriate scope that are part of the WLAN. This gives the gateways the role definitions they need to enforce policy, while keeping unnecessary roles and policies off the APs. This keeps the design cleaner and easier to manage, because policy enforcement happens in one place: at the gateways.

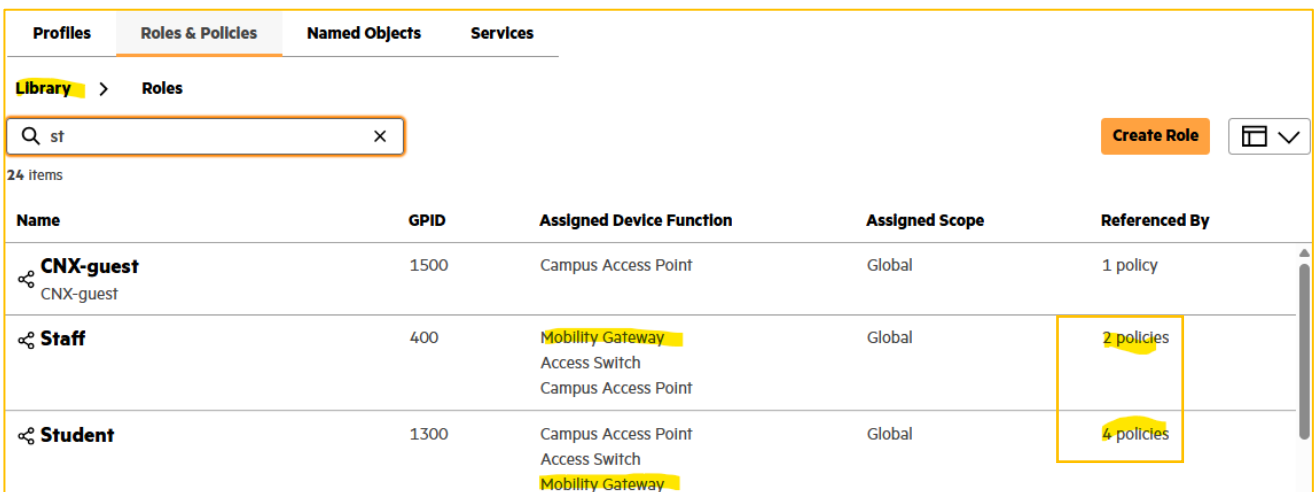
Now having said that, some of the screenshots in this technote indicates that I am assigning roles/policies to the APs and that is correct because in my lab setup I also use those roles in WLANs with bridge mode.

3.1 User Roles

Here I'll go through the configuration of user roles and related policies. In most cases, you want to use the same user roles for your wired and wireless users. I'll start from the library level.



I'll create two roles, Staff and Student. Let's look the roles that I created before.



Here I am showing only what is relevant to the wireless users. You can also configure parameters that are specific to LAN switches. Also note the number of policies each of the roles have.

Edit Role
×

Properties

References

Name *

Description

VLAN ID

Captive Portal Profile

Select
▼

GPID *

Dynamic Application Prioritization

Device-Specific Parameters

Switch

Gateway

Gateway Parameters

VLAN Assignment

VLAN ID
 Named VLAN

VLAN Profile

11
▼

Edit Role
×

Properties

References

Name *

Description

VLAN ID

Captive Portal Profile

Select
▼

GPID *

Dynamic Application Prioritization

Device-Specific Parameters

Switch

Gateway

Gateway Parameters

VLAN Assignment

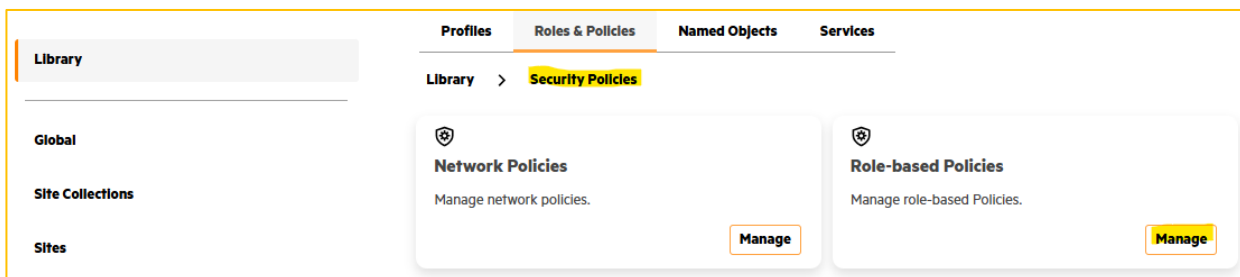
VLAN ID
 Named VLAN

VLAN Profile

12
▼

The initial VLAN-id field is empty. This is because I am using these roles exclusively for tunnelled users. That's why I have assigned Staff and Student roles to VLAN11 and 12 respectively in the gateway specific parameters. For large deployments, you can use Named VLANs instead of VLAN ID. Don't forget to assign the device function and scope.

Next, we go to the Security policies and choose Role-based Policies.



Few points about security policies

- Security Policies are still applied to scopes and device functions.
- The security policies are processed in a top-down fashion until a match is found.
- Policies can be assigned to multiple roles.
- Anything that starts with "sys_" is system generated. Shown below we have two. The sys_allow_all is an explicit allow all rule, which means all wireless traffic that is bridged locally instead of tunnelled to a gateway, will match this policy if it hasn't yet found a match.
- For "Deny all" policy, you need to explicitly create one.
- And if you decide to have "Deny all" policy then other polices with rules explicitly allowing certain traffic should be defined above it.
- The roles will only be sent to the APs, Switches and Gateways if they have at least one policy referencing it.

Profiles Roles & Policies Named Objects Services

Library > Security Policies > Role-based Policies Create Policy

Name	Rules	Assigned Device Function	Assigned Scope
> sys_central_nac This is a system generated configu...	3	Campus Access Point	Global
> basic-net-services	6	Mobility Gateway, Campus Access Point	Global
> Inappropriate-content	2	Campus Access Point, Mobility Gateway, Access Switch	Global
> Internal-nets	1	Campus Access Point, Mobility Gateway	Global
> Allow-All-Pol	1	Mobility Gateway, Campus Access Point, Access Switch	Global
> sys_allow_all Default policy to allow role to role...	8	Campus Access Point	Global

Here I have 4x policies that I created. And each policy consists of a set of rules.

Policies	Purpose	Associated User role for most of the rules
Basic-net-services	Allow access to DHCP and DNS	Student, Guest_Preauth, quarantine
Inappropriate-content	Deny access to inappropriate web categories	Staff, Student,
Internal-nets	Allow access to RFC 1918 networks	Student
Allow-All-Pol	Allow-all access	Staff, Students,

Here I have expanded the “basic-net-services” policy. Note that each rule can be assigned to multiple roles. I have just hovered my mouse over the roles and it displays all the roles that it is assigned to.

Profiles Roles & Policies Named Objects Services

Library > Security Policies > Role-based Policies Create Policy

Name	Rules	Assigned Device Function	Assigned Scope
> sys_central_nac This is a system generated configu...	3	Campus Access Point	Global
▼ basic-net-services	6	Mobility Gateway, Campus Access Point	Global
IP Version	Role: quarantine, Student, Guest_Preauth	Ice/Appl...	Category Type Action Description DSCP 802.1P
IPv4	Role: quarantine	Any	svc-bootp Net Service Allow - - -
IPv4	Role: quarantine	Any	svc-dhcp Net Service Allow - - -
IPv4	Role: quarantine	Any	svc-dns Net Service Allow - - -
IPv4	Role: quarantine	Any	svc-icmp Net Service Allow - - -
IPv4	Role: quarantine	Net Destinati...	svc-https Net Service Allow access to clea... - -
IPv4	Role: quarantine	Net Destinati...	svc-http Net Service Allow access to clea... - -
> Inappropriate-content	2	Campus Access Point, Mobility Gateway, Access Switch	Global

In another example, expanding the “inappropriate-content” policy, you see that I am denying access to Adult and gambling sites. This policy is applied to most of my roles. So here you don’t need to duplicate the rule for each user role.

The screenshot shows the 'Roles & Policies' section in Aruba Central. Under 'Role-based Policies', the 'inappropriate-content' policy is expanded to show two rules:

Source	Destination	Service/Application	Action	Description	DSCP	802.1P
Role: Staff, Student	Any	Adult and pornogra...	Deny	-	-	-
Role: Staff, Student, ...	Any	Gambling	Deny	-	-	-

A context menu is visible on the right side of the rules table, containing options: Add Rule Above, Add Rule Below, Move Down, Clone Rule Above, and Clone Rule Below.

When you hover your mouse over a rule, “...” appears and by clicking on it you can bring up the rule ordering cloning pop-up. As you are reordering the policies, the order gets synced to the devices that are associated to the user-role. You can check the rules that were pushed down to the gateways with “show right <user-role-name>” as shown below for Staff role where I am showing a part of the output that refers to the access policies.

You can use Troubleshooting section

The screenshot shows the 'Troubleshoot' section for device 'Aruba9004_1'. The 'Commands' tab is active, showing a list of available commands and a search box. Below, the 'Device Outputs' section displays the output of the 'show rights' command for the 'sys_policy_Staff' policy.

```

sys_policy_Staff
-----
Priority Source Destination Service Application Action TimeRange Log Expired Queue TOS
DisScan IPv4/6 Contract Mark Description
-----
1 any any web-cc-category adult/pornography deny Low
4
2 any any web-cc-category gambling deny Low
4
3 any any any permit Low
4
Expired Policies (due to time constraints) = 0
  
```

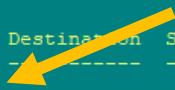
```

access-list List
-----
Position  Name                Type      Location
-----  -
1         global-sacl          session
2         apprf-staff-sacl     session
3         sys_policy_Staff    session

global-sacl
-----
Priority  Source  Destination  Service  Application  Action  TimeRange  Log  Expired  Queue  TOS  8021P  Denylist
-----  -
apprf-staff-sacl
-----
Priority  Source  Destination  Service  Application  Action  TimeRange  Log  Expired  Queue  TOS  8021P  Denylist
-----  -
sys_policy_Staff
-----
Priority  Source  Destination  Service  Application  Action  TimeRange  Log  Expired  Queue
-----  -
ription
-----
1         any    any          web-cc-category adult/pornography deny          Low
2         any    any          web-cc-category gambling    deny          Low
3         any    any          any                            permit        Low

Expired Policies (due to time constraints) = 0
(Aruba9004_1) #

```



And the snapshot of the policies for Student role as seen by the gateway. Look at the order of the rules.

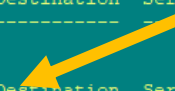
```

access-list List
-----
Position  Name                Type      Location
-----  -
1         global-sacl          session
2         apprf-student-sacl session
3         sys_policy_Student  session

global-sacl
-----
Priority  Source  Destination  Service  Application  Action  TimeRange  Log  Expired  Queue  TOS  8021P  Denylist  Mirror
-----  -
apprf-student-sacl
-----
Priority  Source  Destination  Service  Application  Action  TimeRange  Log  Expired  Queue  TOS  8021P  Denylist  Mirror
-----  -
sys_policy_Student
-----
Priority  Source  Destination  Service  Application  Action  TimeRange  Log  Expired  Queue  TOS
-----  -
ription
-----
1         any    any          svc-bootp          permit        Low
2         any    any          svc-dhcp           permit        Low
3         any    any          svc-dns            permit        Low
4         any    any          web-cc-category adult/pornography deny          Low
5         any    any          web-cc-category gambling    deny          Low
6         any    rfcl918-net  any                permit        Low
7         any    any          any                permit        Low

Expired Policies (due to time constraints) = 0
(Aruba9004_1) #

```



Key points for user roles

- User roles will not be pushed to the gateways even if the role is assigned to gateway device function and has a correct scope unless the role has a policy rule assigned to it.
- user based policies can be assigned to all the device types but only scoped at Global, site collection and sites.
- The scope needed for the user roles can be Global, Site collection/Sites and device groups that has the gateways in place.


4 WLAN Configuration and Testing

In AOS 10 tunnel mode, the access point decrypts client wireless traffic and forwards it through a GRE tunnel to the selected gateway, where it is processed and sent to the network.

Now we'll configure the tunnel WLANs for dot1x authentication and another one for Guest.

4.1 Tunnel WLAN dot1x Configuration

Here is the WLAN configuration for the tunnel WLAN that I'll call "corp-CP-Tun". This will be using ClearPass as my authentication server which I covered in the previous technote for mobility gateways.

General Name * <input type="text" value="corp-CP-Tun"/> Description <input type="text"/> Type <input type="text" value="Access"/> <input type="checkbox"/> Use Alias ESSID Name * <input type="text" value="corp-CP-Tun"/> <input type="checkbox"/> Disable Network Bands <input checked="" type="checkbox"/> 2.4 GHz <input checked="" type="checkbox"/> 5 GHz <input type="checkbox"/> 6 GHz Wi-Fi Protocols	VLAN Traffic Forwarding Mode * <input type="radio"/> Bridge <input checked="" type="radio"/> Tunnel <input type="radio"/> Mixed Primary Gateway Cluster * <input type="text" value="CNX-group:MGW_cluster_1"/> Secondary Gateway Cluster <input type="text" value="--Select Cluster--"/> <input type="checkbox"/> Use Named VLAN Default VLAN * <input type="text" value="13"/> Advanced VLAN Assignment Rules + Rules
Security Security Level * <input checked="" type="radio"/> Enterprise <input type="radio"/> Personal <input type="radio"/> Open Key Management * <input type="text" value="WPA3-Enterprise(CCM 128)"/> Authentication Server Group * <input type="text" value="Radius-East"/> <small>ⓘ Server Group is supported in APs running AOS 10.6.0.0 and above.</small> Reauthentication Interval 0-32768 <input type="text" value="0"/> Minutes <input type="checkbox"/> Perform MAC Authentication Before 802.1X <input type="checkbox"/> MAC Authentication Fail-Through	Access Default Role - <input type="checkbox"/> Override default role <small>ⓘ Default policies for role "" have been created under "Roles & Policies > Role-Based policies". Please finish the configuration by editing said policies.</small> Advanced Enforce Machine Authentication Machine Auth Only <input type="text" value="--Select Role--"/> User Auth Only <input type="text" value="--Select Role--"/> Role Assignment Rules + Rules 

Accounting

Accounting

Accounting Server group

Accounting Server Group

Radius-East

Interim RADIUS Accounting Interval

0-60

5 Minutes

Note that if you want to change the default user role for this WLAN, you can select one of the previously defined user roles from the Default Role drop-down list. This is assigned to all clients that do not have a dynamic role assignment. Scope the WLAN Profile to "Campus Access Point" device function, site and Device Group where AP is present.

Profiles Roles & Policies Named Objects Services

Library > Wireless > WLAN

CP-Tun

1 item

Name	Type	Status	Assigned Device Scope
corp-CP-Tun	Access	Enabled	Campus Access Point 2 scopes

Assigned Scopes

Name	Scope Level
CNX-group	Device Group
CNX-branch1	Site

Create Profile

Once it is assigned to the device group, then only the WLAN gets broadcasted from the AP. Note that it is not mandatory for the APs to be in the same device group as the gateway cluster. They can belong to a different device group. However, I am using the same device group for both.

4.2 AP and Gateway Testing

Before we start connecting clients to the WLAN, let's check the basics to ensure all the configuration is in place.

First check the audit trail in Central to see if all is good.

GLOBAL


Audit Trail

View the activities that impact the network.

wlan profile "corp-CP-tun" Last 30 days

19 items

Occurred On	Action	Category	Sub-Category	Destina...	Destination Name	Description
06/08/2026, 3:01:24 PM	Scope assigned	Configuration	Profiles	Global	Global	Wlan profile "corp-CP-Tun" assigned to scope "Global" for Campus Access Poin...
06/08/2026, 2:56:56 PM	Scope un-assigned	Configuration	Profiles	Global	Global	Wlan profile "corp-CP-Tun" unassigned from scope "Global" for Campus Access ...
06/08/2026, 2:55:28 PM	Scope assigned	Configuration	Profiles	Global	Global	Wlan profile "corp-CP-Tun" assigned to scope "Global" for Campus Access Poin...
06/08/2026, 2:50:02 PM	Scope assigned	Configuration	Profiles	Site	CNX-branch1	Wlan profile "corp-CP-Tun" assigned to scope "CNX-branch1" for Campus Acce...
06/08/2026, 2:50:02 PM	Scope assigned	Configuration	Profiles	Device Group	CNX-group	Wlan profile "corp-CP-Tun" assigned to scope "CNX-group" for Campus Access ...
06/08/2026, 2:49:29 PM	Profile created	Configuration	Profiles	Library	-	Wlan profile "corp-CP-Tun" created

Then I'll start from the AP, first check if the WLAN is in the BSS table. You can run all the CLI commands from commands from the Troubleshooting section 

Troubleshoot

For CNX-branch1

Tests Remote Console **Commands** Live Monitoring Support Logs History

Device Inputs

Device Type* Devices*

```
AP1# sh ap bss-table

Aruba AP BSS Table
-----
bss          ess          port ip          band/ht-mode/bandwidth  ch/EIRP/max-EIRP
type cur-cl  ap name  in-t(s)  tot-t  flags  mu-mimo  mld-mac/link-id  MBSSID Group
-----
d0:d3:e0:b2:2a:90 corp-CP-Tun  ??  10.10.10.34  5GHz/HE/80MHz  60E/21.0/23.0  ap
0      AP1      0      56s  KTWZ3  1      -
Channel followed by "*" indicates channel selected due to unsupported configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:3
Num Associations:0

Flags:      B = Beacon Protection; c = MBO Cellular Data Capable BSS; d = Deferred Delete
Pending; D = VLAN Discovered; E = Enhanced-open BSS without transition mode; I = Imminent VAP
Down; K = 802.11K Enabled; m = Agile Multiband (MBO) BSS; M = WPA3-SAE mixed mode BSS; o =
Enhanced-open transition mode open BSS; O = Enhanced-open BSS with transition mode; Q = DFS CAC
timer running; r = 802.11r Enabled; t = Broadcast TWT Enabled; T = Individual TWT Enabled; W =
802.11W Enabled; x = MBSSID Tx BSS; z = WPA3-AES-CCM128 BSS; Z = WPA3-AES-CCM128 BSS with
transition mode; 3 = WPA3 BSS;

AP1#
```

Next, I'll use this command is to check the tunnel configuration that was pushed to the AP.

```
AP1# sh overlay tunnel config

Overlay Tunnel Config
Cluster MGW_cluster_1 - Zone 0
-----
Index  UAC IP          Tunnel Type  Heartbeat  MTU  Vlan List
-----
0      192.168.1.241  GRE         Enabled    1500  1,10-13,192,4094
1      192.168.1.242  GRE         Enabled    1500  1,10-13,192,4094

AP1#
```

Here you can check that tunnels are created.

```
AP1# sh ata current-cfg

Current Central is Up
Microbranch AP is Disabled
Microbranch System IP is 0.0.0.0/::
[Current Configuration For cluster(MGW_cluster_1)]
<Tunnel list>
----pub_ip=192.168.1.241, local_ip=192.168.1.241, vlan=1,10-13,192,4094, mcast=0, Tun_Type=GRE,
peer_device_type=Gateway
key_exp=129600, dstNatt=4500, HBT_interval=3, HBT_Threshold=10
----pub_ip=192.168.1.242, local_ip=192.168.1.242, vlan=1,10-13,192,4094, mcast=0, Tun_Type=GRE,
peer_device_type=Gateway
key_exp=129600, dstNatt=4500, HBT_interval=3, HBT_Threshold=10
<SSID list for primary>
----ssid=corp-CP-Tun, type=0

AP1#
```

You can also check the stats for IPSEC tunnels that are created from the AP to the gateways. One tunnel for each gateway.

```
AP1# sh crypto ipsec stats

IPSEC STATS
-----
MAP NAME                IP ADDR          DEVNAME  TX/RX PACKETS  TX/RX BYTES      TX/RX DROPS  TX/RX
ERRORS
-----
-----
---
gw-ipsecmap-20:4c:03:82:0f:22  192.168.1.241  tun1    12976/12976    1433138/1424874  0/0          0/0
gw-ipsecmap-28:de:65:73:85:96  192.168.1.242  tun0    363/361        40007/39628      0/0          0/0
Total IPSEC Count: 2

AP1#
```

Now we'll check the tunnels from the gateways starting with the status of tunnel orchestrator.

```
(Aruba9004_1) #show crypto oto

OTO Status
Channel state:          CONNECTED
Channel UP since:      Thu Jun  4 09:30:16 2026
Channel Up count:      1
Channel Down count:    0
Keepalive Interval:    60
#Create Channel:       1
#Delete Channel:       0
#KeepAlive Sent:       205
#KeepAlive Received:   187
#KeepAlive Pending:    0
Create Spec:           2
Update Spec Sent/Recv: 0/0
Delete Spec:           0
Device Spec:           3
Resync Event Sent:     17
Ike Event Sent:        1
Peer Down DPD/HCM/OTO: 0/0/0
BG-SRC Learn/OnRekey: 1/0
BG-SRC Err SPI/Map/Vlan/B-Mesh: 0/0/0/0
Rekey Request/Done/Abort/Fake: 0/0/0/0
State Update Event Sent: 1
Down Event Sent:       0/0
HCM Message Lookup (Success/Fail): 0/0
HCM Message Drops No (VpnIP/ProbeIP): 0/0
Survival-map Cleanup Total/Last: 0/0
Tunnel State Trigger: HCM
SPI Costly:            0
Loop Time/Amon Time(ms): 0/0
Survival Map Lookup/Time(ms): 1/0

(Aruba9004_1) #
```

Here we see that the tunnel is up and operational.

```
(Aruba9004_1) #show tunnelmgr tunnel-list

Tunnelmgr Table Dump
-----
Tunnel ID                Map ID  Peer IP      Peer MAC          Device-Type  Secure-Mode
Status GRE ID Mtu
-----
-----
fb42e94e-c9ca-459a-a5d3-7792daf67b1b  0x70001  10.10.10.34  20:4c:03:b6:b2:5b  AP           No          UP
12          1500

Total Entries:  1 Up: 1

(Aruba9004_1) #
```

Finally checking the IPSEC tunnels, we notice that there is a tunnel to the AP and another between the gateways on the clusters.

```
(Aruba9004_1) #show crypto ipsec sa
```

```

Tunnel Service SA Information
-----
Initiator IP      Responder IP      SPI (IN/OUT)      Flags
Start Time        Tunnel Type      Inner IP           -----
-----
10.10.10.34      192.168.1.241    94e8c000/fe740000 UT1t
Jun  7 13:43:04  AP              10.10.10.34

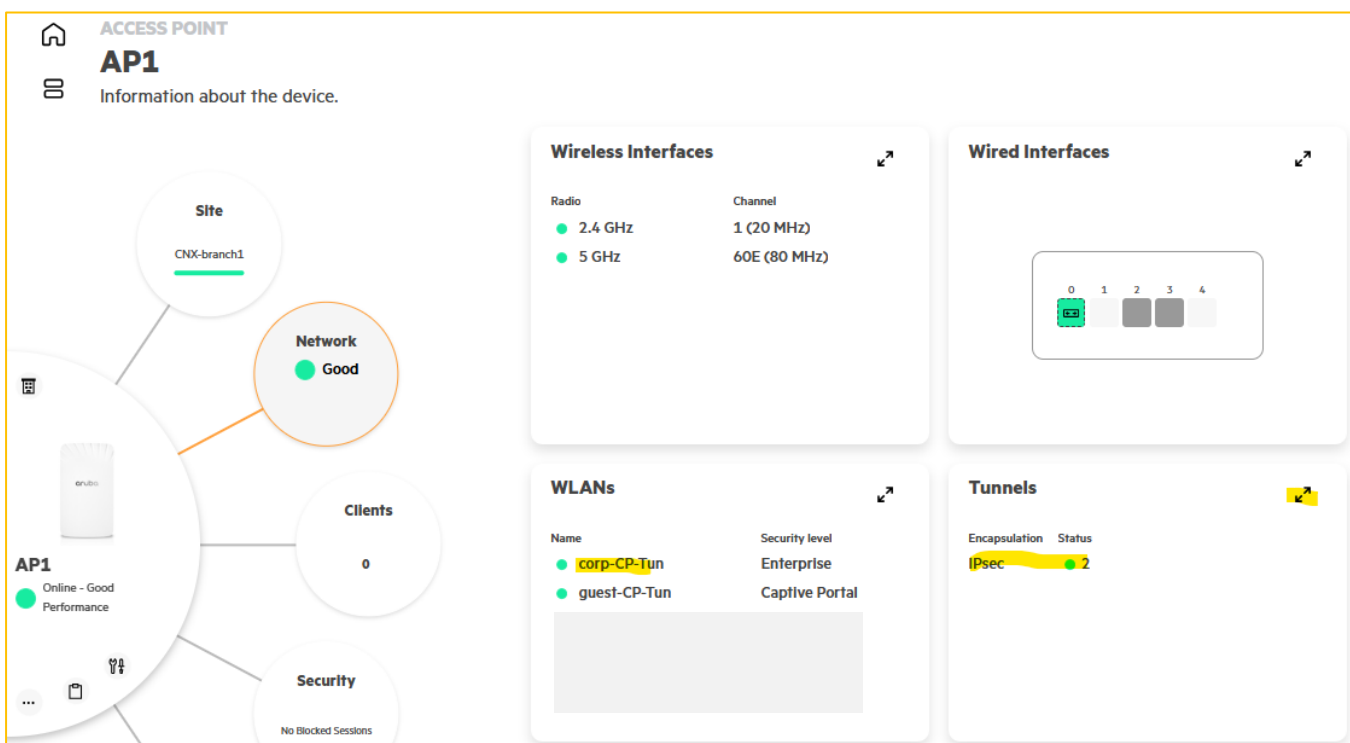
IPSEC SA (V2) Active Session Information
-----
Initiator IP      Responder IP      SPI (IN/OUT)      Flags
Start Time        Tunnel Type      Inner IP           -----
-----
192.168.1.242    192.168.1.241    f7b6f200/f5927f00 T2
Jun  7 16:00:48  N/A              -

Flags: T = Tunnel Mode; E = Transport Mode; U = UDP Encap
       L = L2TP Tunnel; N = Nortel Client; C = Client; 2 = IKEv2
       l = uplink load-balance; t = Tunnel Service; P = Reverse-Pinning Enabled
Total IPSEC SAs: 2

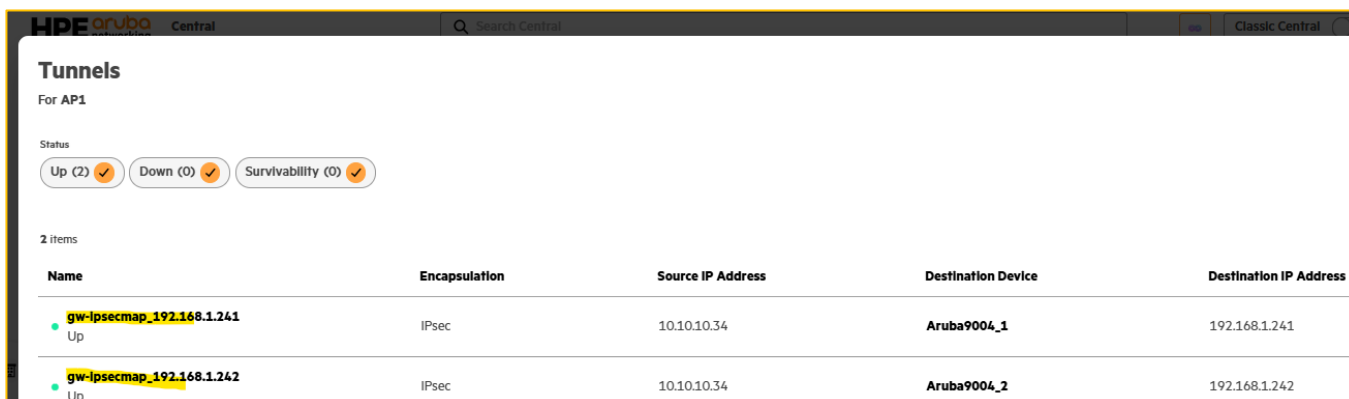
(Aruba9004_1) #

```

You can also check all this from the Web UI.



You can expand Tunnel card to get the details.

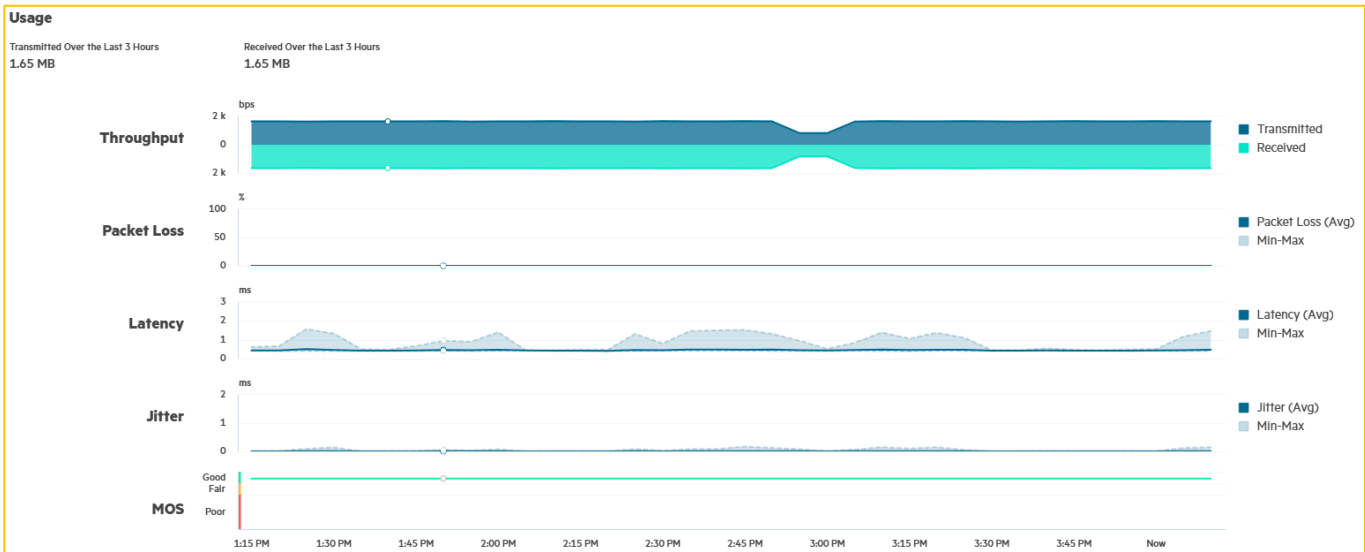


You can also get the performance of each tunnel.

← gw-ipsecmap_192.168.1.241

Properties

Destination Device Aruba9004_1	Encapsulation IPsec	Destination IP Address 192.168.1.241	Destination Cluster MGW_cluster_1	High Availability -	Peer Type Gateway
Authentication SHA-256	Encryption AES	In SPI 9323134	Out SPI 14560335	Source IP Address 10.10.10.34	Uptime 1h 2m 16s
Last Change Reason Unknown					



4.3 Dot1x User Testing

Now we get two laptops to connect to the tunnels dot1x WLAN with staff and student credentials respectively. As shown below both could connect successfully and assigned to the correct user-role and are in the correct VLANs.

SITE CNX-branch1
Network and connectivity information about this site.

Network Poor 4 devices

Clients 2

Applications 31

Security 3 Blocked Sessions

Clients

Status: Connected (2) ✓, Failed (0), Connecting (0), Disconnected (1), Blocked (0)

Type: Wireless (2) ✓, Wired (1), Remote (0)

Name	Type	MAC Address	IP Address	VLAN	Tunneling	Tunnel ID	Role
staff1 Connecte...	Wireless	d0:abd5:c2:06:55	10.10.11.48 fe80:0:0:17cf:63e1:5ae5:fe98	11	Overlay	0	Staff
student1 Connecte...	Wireless	f0:d5:bf:4b:67:11	10.10.12.45 fe80:0:0:0eac:6491f:8fa8:1aa5	12	Overlay	0	Student

ClearPass access tracker shows AP's IP address as NAS-Identifier and Gateway' IP address as the NAS-IP-Address. So, all the authentication requests are coming from the gateway. This is important as ClearPass always sends RADIUS CoA to the NAS IP address.

Summary	Input	Output	Accounting
Username:	staff1		
End-Host Identifier:	D0-AB-D5-C2-06-55 (Operating System / Microsoft / Windows)		
Access Device IP (Port):	192.168.1.241		
Access Device Name:	10.10.10.34 (AOS10-gateway3 / Aruba)		
RADIUS Request			
Radius:Aruba:Aruba-AP-Group	CNX-group		
Radius:Aruba:Aruba-AP-MAC-Address	204c03b6b25b		
Radius:Aruba:Aruba-Device-MAC-Address	d0abd5c20655		
Radius:Aruba:Aruba-Essid-Name	corp-CP-Tun		
Radius:Aruba:Aruba-Location-Id	20:4c:03:b6:b2:5b		
Radius:IETF:Called-Station-Id	204c03b6b25b		
Radius:IETF:Calling-Station-Id	d0abd5c20655		
Radius:IETF:Framed-MTU	768		
Radius:IETF:Location-Capable	9		
Radius:IETF:NAS-Identifier	10.10.10.34		
Radius:IETF:NAS-IP-Address	192.168.1.241		
Radius:IETF:NAS-Port	0		
Radius:IETF:NAS-Port-Type	19		
Radius:IETF:Service-Type	2		

Here is the view from HPE Aruba Central.

The screenshot displays the HPE Aruba Central interface for a client named 'staff1'. The main dashboard includes a 'Health' section with a timeline showing the client is connected since June 22, 2026, at 11:32 AM. The 'Connectivity Performance' section shows 0 bps throughput and 44 dB signal quality. The 'Properties' section lists details such as Host Name (DESKTOP-PJA3PBF), MAC Address (d0abd5c2:06:55), and IP Address (10.10.11.48). A network diagram at the bottom illustrates the client's connection path through an AP1, a switch, and finally to the Internet.

4.4 Tunnel WLAN Guest Configuration

In this section I'll cover basic tunnel WLAN for Guest using external captive portal.

The order of tasks is

1. Configure Captive Portal Authentication profile
2. Configure Captive Portal Server Certificate (optional)
3. Configure your Names Object Aliases (optional)
4. Configure Pre-authentication User role
5. Configure role policies for the Pre-authentication User role.
6. Configure the Guest WLAN profile

Captive Portal Authentication profile

You need to navigate to Library>> Profiles>>Security >> Captive Portal Authentication to

And here is my configuration.

The last part of the URL is .php The Captive portal URL is from ClearPass guest web-login page.

Note with captive portals in tunnel mode and with AOS10, all the redirections are handled by the APs and hence you don't need captive portal certificates for the gateways.

Captive Portal Server Certificate (Optional)

Here I am using a wild card server certificate that I will assign it as the captive port certificate for the APs. You can navigate to Certificate management and upload your PEM server certificate along with the full trust chain. You can also import your existing server certificates from Classic Central if you already had one there.

This is how it should look like once you have added the certificate.

Name	Type	Format	Days Until Expiration	Algorithm	Issued By	Issued To
CP-certificate	Server	PEM	131	RSA	Common Name: Sectigo Public Server Authentication CA DV R...	Common Name: *.arubatechs.com

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

Profiles	Roles & Policies	Named Objects	Services
Library > Security > Certificate Usage			
<input type="text" value="Search"/>			<input type="button" value="Create Profile"/>
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

Here I'll create a new profile name "ClearPass-CP" and this is profile where you can assign certificates for all the services that requires it like RadSec or AP 802.1X Server CA (Uplink), etc. I am showing only the Captive portal server certificate.

Name *

Description

Device Type *
 Access Point
 Gateway

Access Point Parameters

Authentication Survivability Client CA

Authentication Survivability Server Certificate

Captive Portal Server Certificate

Use EST for RadSec Client Provisioning

The rest of the field that I have not shown are left as default. Once it is saved it will be listed as shown below where you can assign to the APs.

Profiles	Roles & Policies	Named Objects	Services
Library > Security > Certificate Usage			
<input type="text" value="Search"/>			<input type="button" value="Create Profile"/>
3 items			
Name	Device Type	Assigned Device Function	Assigned Scope
CNX-cp-securelogin-hpe-com	Access Point	Campus Access Point	Global
ClearPass-CP captive portal provided by ClearPass	Access Point	Campus Access Point	AP1
default-ap-cert-usage-profile Default AP cert usage profile	Access Point	Campus Access Point	Global

Remember that this is optional as all the APs can use the certificate that is called aruba_default that has Common Name as "securelogin.hpe.com", see below.

GLOBAL Certificate Management							
View and manage certificates.							
<input type="text" value="Search"/>							<input type="button" value="Add"/>
4 items							
Name	Type	Format	Days Until Expiration	Algorithm	Issued By	Issued To	
CP-certificate	Server	PEM	131	RSA	Common Name: Sectigo Public Server Authentication CA DV R...	Common Name: *.arubatechs.com	
aruba_default	Server	PEM	40	RSA	Common Name: DigiCert Global G2 TLS RSA SHA256 2020 C...	Common Name: securelogin.hpe.com, Country Name:	

Names Object Aliases (Optional)

Here I am configuring an alias for my ClearPass Guest nodes as they have the captive portal pages.

Name	Type	Assigned Device Function	Assigned Scope
ClearPass	Network Destination	Mobility Gateway Access Switch Campus Access Point	Global

Edit Alias [Close]

Type	Condition
Host	192.168.1.102
Host	192.168.1.101

Take a note of the assigned device types and scope.

Pre-authentication User Role

Here we'll configure the pre authentication user role for the Guest WLAN. Just like with Instant APs,

Name	GPID	Assigned Scope	Referenced By
Guest_Preauth	2200	2 scopes	1 policy
Guest_Preauth2	2400	2 scopes	1 policy

Edit Role [Close]

Profile	Type
guest-CP-Tun	WLAN AAA
guest-CP-Tun_17808963701...	Authentication

Note that initially when you create this user role, “Captive Portal Profile” field is empty. However, it will only get populated with the corresponding profile when you use this user role as “Assign Pre-Authentication Role” in a WLAN profile that has a captive portal profile.

Role Policies for the Pre-authentication User Role

Here I am using allow-all-pol that I created for this “Guest_Preauth2” user role. With role-based policies, one thing that is different here is that you can assign a rule to multiple user roles.

Name	Rules	Assigned Device Function	Assigned Scope
> basic-net-services	7	Mobility Gateway, Campus Access Point	Global
> inappropriate-content	2	Campus Access Point, Mobility Gateway, Access Switch	Global
> internal-nets	1	Campus Access Point, Mobility Gateway	Global
▼ Allow-All-Pol	1	Mobility Gateway, Campus Access Point, Access Switch	Global

IP Verison	Source	Destination	Service/App...	Category Type	Action	Description	DSCP	802.1P
IPv4	Role: Guest_P...	Any	Any	-	Allow	-	-	-

Role: Staff, Guest_Preauth2, Student

Here I have assigned this Allow-all rule to multiple use-roles and one of them is Guest_Preauth2

Note that even though we have allow-all policy for pre-auth role, AOS 10 has automatic allowances based on the captive portal profile. It allows HTTPS/HTTP to the captive portal target and DHCP/DNS. In the last section I’ll use a different pre-authentication user role which will have a specific allow access rules. But for the time being we’ll use this allow all policy.

Guest WLAN profile

And finally, we need to configure the WLAN profile and reference the captive portal profile and pre-authentication role we created earlier.

Wi-Fi Protocols

- Wi-Fi 4 (802.11n)
- Wi-Fi 5 (802.11ac)
- Wi-Fi 6 (802.11ax)
- Wi-Fi 7 (802.11be)

Network Configuration ?

- Most Compatible
- Balanced
- High Density
- Custom

Reauthentication Interval
0-32768
180 Minutes

Accounting

Accounting
Accounting Server group ▼

Accounting Server Group
Radius-East ▼

Interim RADIUS Accounting Interval
0-60
5 Minutes

After creating the WLAN SSID Profile shared object, assign it to the "Mobility AP" device function and the scope is Global and to the device group where the AP is present, same as the other tunnelled WLAN which we configured.

Profiles	Roles & Policies	Named Objects	Services
<input type="text" value="tun"/> × Create Profile			
2 items			
Name	Type	Status	Assigned Device Scope
corp-CP-Tun	Access	Enabled	3 scopes
guest-CP-Tun	Access	Enabled	2 scopes

Assigned Scopes ×

Name	Scope Level
Global	Global
CNX-group	Device Group

Assigned Device Scope

Campus Access Point

So now when we go back and check the Guest_Preauth2 user role, we'll see the corresponding captive portal profile.

Properties References

Name *

Guest_Preauth2

Description

VLAN ID

Captive Portal Profile

ClearPass-Portal-Tun ▼

GPID *

2400

Dynamic Application Prioritization

Device-Specific Parameters

Switch

Gateway

4.5 Guest User Testing

Before we get a guest client to connect, let's check the basic configurations that were pushed to the AP and gateways. Remember all the redirection happens from the AP and not the gateways. Again, you can use the troubleshooting page for remote console or running several CLI commands.

Here is the access policy for Guest_Preauth2 user role at the AOS10 AP.

```
AP1# sh access-rule Guest_Preauth2
ACL Vlan      :
ACL Captive Portal:external
ACL ECP Profile  :ClearPass-Portal-Tun
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
AP1#

```

Next, I'll check the captive portal profile. Note that it looks very similar to an Instant AP configuration.

```

AP1# sh external-captive-portal ClearPass-Portal-Tun

Name           :ClearPass-Portal-Tun
Server         :cpl-611.arubatechs.com
Port          :443
Url            :/guest/school.php
Auth Text     :
Redirect Url   :https://www.hpe.com/us/en/home.html
Server Fail Throth  :Disable
Disable Auto Allowlist :Enable
Use HTTPS     :Yes
Server Offload  :No
Prevent Frame Overlay :Disable
In Used       :Yes
Redirect Mode  :Yes
Switch IP     :No
AP1#

```

Here is the similar command to see user-based policies at the gateway.

```

(Aruba9004_1) #show rights Guest_Preauth2

Valid = 'Yes'
CleanedUp = 'No'
Derived Role = 'Guest_Preauth2'
  Up BW:No Limit   Down BW:No Limit
  L2TP Pool = default-l2tp-pool
  PPTP Pool = default-pptp-pool
  Number of users referencing it = 0
  Periodic reauthentication: Disabled
  DPI Classification: Enabled
  Youtube education: Disabled
  Web Content Classification: Enabled
  IP-Classification Enforcement: Enabled
  ACL Number = 107/0
  Openflow: Enabled
  Global Role Tag: 2400
  Enforce Dhcp: Disabled
  Max Sessions = 65535

  Check CP Profile for Accounting = TRUE

Application Exception List
-----
Name  Type
----  ---

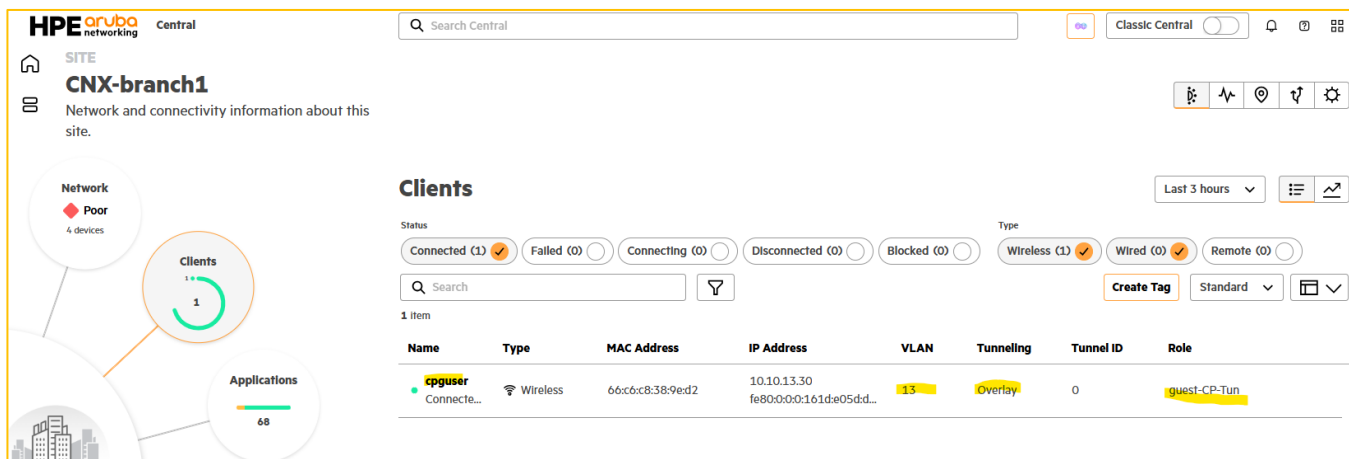
Application BW-Contract List
-----
Name  Type  BW Contract  Id  Direction
----  ---  -
-----

access-list List
-----
Position  Name                                     Type      Location
-----  -
1         global-sacl                               session
2         apprf-guest_preauth2-sacl                session
3         sys_policy_Guest_Preauth2                session

global-sacl
-----

```


And this one is Aruba Central view after successful authentication. The final user role for a successful guest is “guest-CP-Tun”. This is because by default the user role with the name of the WLAN will be assigned. If ClearPass would have sent back a user role that is also configured in New Central, then that would be the assigned user role.



Here is the familiar access tracker view from ClearPass.

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.	192.168.1.241	CP1-611	RADIUS	cpguser	simple MAC Authentication	ACCEPT	gg Aruba cnx-guest access, gg MAC Auth Session Timeout	2026/06/09 14:00:09
2.	192.168.1.241	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	2026/06/09 13:57:12
3.	192.168.1.241	CP1-611	RADIUS	66c6c8389ed2	simple MAC Authentication	REJECT	[Deny Access Profile]	2026/06/09 13:56:01

Note that always the first MAC authentication fails as the guest user has not registered or logged in. Then the guest user’s credentials get authenticated by the ClearPass’s MAC caching service. And finally, when I issue a CoA for this user, the user gets disconnected and it reconnects but this time it will pass the MAC authentication and will not get redirected to the captive portal. (note that we had enable MAC authentication got the Guest WLAN profile.

This is the access tracker request session 2 (successful guest user authentication)

Summary	Input	Output	Accounting	RADIUS Dynamic Authorization
Login Status:	ACCEPT			
Session Identifier:	R00000011-05-6a278f18			
Date and Time:	Jun 09, 2026 13:57:12 AEST			
End-Host Identifier:	66-C6-C8-38-9E-D2			Open in Central
End-Host Profile:	Operating System / Microsoft / Windows			
End-Host Status:	Known			
Username:	cpguser			
Access Device IP (Port):	192.168.1.241			
Access Device Name:	AOS10-gateway3 (AOS10-gateway3 / Aruba)			
System Posture Status:	UNKNOWN (100)			
Policies Used -				
Service:	Simple 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 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			
Service Monitor Mode:	Disabled			

And this is access tracker request session 1 (successful MAC auth after CoA)

Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R00000012-05-6a278fc9		
Date and Time:	Jun 09, 2026 14:00:09 AEST		
End-Host Identifier:	66-C6-C8-38-9E-D2	Open in Central	
End-Host Profile:	Operating System / Microsoft / Windows		
End-Host Status:	Known		
Username:	cpguser		
Access Device IP (Port):	192.168.1.241		
Access Device Name:	AOS10-gateway3 (AOS10-gateway3 / Aruba)		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	simple 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:	gg Aruba cnx-guest access, gg MAC Auth Session Timeout		
Service Monitor Mode:	Disabled		
Online Status:	✔ Online		

This is the client view from the AP.

```
AP1# sh client
Client List
-----
Name      IP Address  MAC Address      OS      ESSID          Access Point      Channel  Type
Role      IPv6 Address
-----  -
-----  -
cpguser   10.10.13.30 66:c6:c8:38:9e:d2 Win 10  guest-CP-Tun  20:4c:03:b6:b2:5b 60E      AC
guest-CP-Tun fe80::161d:e05d:dbf9:172a 47 (good) 144 (good)
Number of Clients :1
Info timestamp   :13025
AP1#
```

```
AP1# sh datapath user
Datapath User Table Entries
-----
Flags: P - Permanent
       R - ProxyARP to User, N - VPN, L - local, I - Intercept, D - Deny local routing
       M - User Media Classified, K - OS known, S - Simulated Client
FM(Forward Mode): B - Underlay, O - Overlay S - Microbranch, N - N/A

Vlan  IP      MAC      ACLs      Contract  Location  Age  Sessions  Flags
-----  -
-----  -
10.10.10.34 20:4C:03:B6:B2:5B 105/0/108 0/0 0 0 7/65535 P
1 B 0 0 -
0.0.0.0 66:C6:C8:38:9E:D2 192/0/0 0/0 0 0 0/65535 PK
13 O 0 0 192.168.1.241
10.10.13.30 66:C6:C8:38:9E:D2 192/0/0 0/0 0 0 4/65535 K
13 O 0 0 192.168.1.241
172.31.98.1 20:4C:03:B6:B2:5B 105/0/0 0/0 0 37 0/65535 P
3333 B 0 0 -
AP1#
```

This is the client view form the gateway.

```
(Aruba9004_1) #show user
This operation can take a while depending on number of users. Please be patient ....
```

```

Users
-----
IP           MAC           Name           Role           Age (d:h:m)   Auth   VPN link           Connected
To           Roaming       Essid/Bssid/Phy Profile
mode        Type         Host Name     User Type
-----
10.10.13.30  66:c6:c8:38:9e:d2  cpguser       guest-CP-Tun   00:00:16     MAC           N/A
Wireless    guest-CP-Tun/20:4c:03:b6:b2:5b/N/A  guest-CP-Tun_1780896370157002794_ dtunnel
Win 10      WIRELESS

User Entries: 1/1
Curr/Cum Alloc:1/10 Free:0/9 Dyn:1 AllocErr:0 FreeErr:0
(Aruba9004_1) #

```

You can also check the user session from the WebUI from security planet.

4.6 Tunnel WLAN Guest Configuration with customised User Role

Here I have configured ClearPass to send back “new-guest” after a successful guest login.

Now I’ll create this “new-guest” user role in New Central and assign it to the device types and sites. Note that it is not reference by anything, that’s because I have not yet assigned it to a user role policy rule.

But once I have assigned a role-based policy rule to it, it will be displayed as shown below.

I configured a new pre-authentication user role “Guest_Preauth”.

Here are the rules that are assigned to the “Guest_Preauth” role. Note that the rules are assigned to both “Guest_Preauth” and “quarantine” roles.

Profiles								
Roles & Policies		Named Objects		Services				
Library > Security Policies > Role-based Policies								
Name	Rules	Assigned Device Function			Assigned Scope			
> sys_central_nac This is a system generated configu...	3	Campus Access Point			Global			
▼ basic-net-services	6	Mobility Gateway, Campus Access Point			Global			
IP Version	Source	Destination	Service/Appli...	Category Type	Action	Description	DSCP	802.1P
IPv4	Role: quaranti...	Any	svc-bootp	Net Service	Allow	-	-	-
IPv4	Role: quaranti...	Any	svc-dhcp	Net Service	Allow	-	-	-
IPv4	Role: quaranti...	Any	svc-dns	Net Service	Allow	-	-	-
IPv4	Role: quaranti...	Any	svc-icmp	Net Service	Allow	-	-	-
IPv4	Role: quaranti...	Net Destinati...	svc-https	Net Service	Allow	access to clea...	-	-
IPv4	Role: quaranti...	Net Destinati...	svc-http	Net Service	Allow	access to clea...	-	-

Role: quarantine, Guest_Preauth

I have also assigned the allow-all rule to “new-guest” role.

Profiles								
Roles & Policies		Named Objects		Services				
Library > Security Policies > Role-based Policies								
Name	Rules	Assigned Device Function			Assigned Scope			
> sys_central_nac This is a system generated configu...	3	Campus Access Point			Global			
> basic-net-services	6	Mobility Gateway, Campus Access Point			Global			
> inappropriate-content	2	Campus Access Point, Mobility Gateway, Access Switch			Global			
> internal-nets	1	Campus Access Point, Mobility Gateway			Global			
▼ Allow-All-Pol	1	Mobility Gateway, Campus Access Point, Access Switch			Global			
IP Version	Source	Destination	Service/Appli...	Category Type	Action	Description	DSCP	802.1P
IPv4	Role: Staff, Gu...	Any	Any	-	Allow	-	-	-

Role: Staff, Guest_Preauth2, Student, new-guest

Finally, we need to change the pre-authentication role in the guest-CP-Tun WLAN profile to use “Guest_Preauth” that we just created.

General Name * <input type="text" value="guest-CP-Tun"/> Description <input type="text"/> Type <input type="text" value="Access"/> <input type="checkbox"/> Use Alias ESSID Name * <input type="text" value="guest-CP-Tun"/> <input type="checkbox"/> Disable Network	VLAN Traffic Forwarding Mode * <input type="radio"/> Bridge <input checked="" type="radio"/> Tunnel <input type="radio"/> Mixed Primary Gateway Cluster * <input type="text" value="CNX-group:MGW_cluster_1"/> Secondary Gateway Cluster <input type="text" value="--Select Cluster--"/> <input type="checkbox"/> Use Named VLAN Default VLAN * <input type="text" value="13"/>	Security Security Level * <input type="radio"/> Enterprise <input type="radio"/> Personal <input checked="" type="radio"/> Open Key Management * <input type="text" value="Open"/> Captive Portal Type <input type="text" value="External Captive Portal"/> Captive Portal Profile * <input type="text" value="ClearPass-Portal-Tun"/>	Access Default Role - <input type="checkbox"/> Override default role <small>Default policies for role "" have been created under "Roles & Policies > Role-Based policies". Please finish the configuration by editing said policies.</small> Advanced Assign Pre-Authentication Role * <input type="text" value="Guest_Preauth"/> Enforce Mac Auth Only Role <input type="text" value="--Select Role--"/> Role Assignment Rules <input type="text" value="Rules"/>
--	---	---	--

4.7 User Testing with Customised User Roles

Before we get a guest client to connect, let's check the basic configurations that were pushed to the AP and gateways. From the troubleshooting page I remote console to the AP and ran this command to see the access policy for Guest_Preauth user role.

```

API# sh access-rule Guest_Preauth

ACL Vlan      :
ACL Captive Portal:external
ACL ECP Profile :ClearPass-Portal-Tun
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
-----
any      any             IPv4/6    match       bootp                    permit
any      any             IPv4/6    match       dhcp                     permit
any      any             IPv4/6    match       dns                       permit
any      any             IPv4/6    match       icmp                      permit
netdest  ClearPass-VIP (3) IPv4/6    match       https                     permit
netdest  ClearPass-VIP (3) IPv4/6    match       http                      permit
API#
  
```

Now let's get a user to connect to the guest-CP-Tun WLAN. It is seen that it gets a correct pre authentication user role.

The screenshot shows the network management interface for site **CNX-branch1**. On the left, a dashboard indicates 'Network Good' with 4 devices, 'Clients 1', and 'Applications 1'. The main 'Clients' section shows a filter for 'Connected (1)' and 'Wireless (1)'. A table lists one client:

Name	Type	MAC Address	IP Address	VLAN	Tunneling	Tunnel ID	Role
66c6c83...	Wireless	66:c6:c8:38:9ed2	10.10.13.30	13	Overlay	0	Guest_Preauth

After being redirected to the captive portal and entering valid credentials, the user is successfully authenticated and granted network access. Note the new user role.

The screenshot shows the network management interface for site **CNX-branch1**. The 'Clients' section now shows 2 connected clients. The table lists two clients:

Name	Type	MAC Address	IP Address	VLAN	Tunneling	Tunnel ID	Role
66c6c83...	Wireless	66:c6:c8:38:9ed2	10.10.13.30	13	Overlay	0	Guest_Preauth
cpuser	Wireless	66:c6:c8:38:9ed2	10.10.13.30	13	Overlay	0	new-guest

You can click on the username to get more information about it. Clicking it will change the context as shown below.

CLIENT
cpguser
Information about the client.

Site
CNX-branch1

Network
Good
AP1

Applications
49

Security
18 Blocked Sessions

Health
Last 3 Hrs

10:30 AM 10:45 AM 11:00 AM 11:15 AM 11:30 AM 11:45 AM 12:00 PM 12:15 PM 12:30 PM 12:45 PM 1:00 PM Now

● Connected, Good Performance

Connected Since
June 22, 2026 1:19 PM

Properties

Host Name	66:c6:c8:38:9ed2	User Name	cpguser
MAC Address	66:c6:c8:38:9ed2	Type	Wireless
IP Address	10.10.13.30	Global Unicast IPv6 Address	-
Link Local IPv6 Address	fe80:0:0:0:161de05d:d...	Access Role	new-guest

Connectivity Performance

Throughput	0 bps	Retry Frames	0 %
Signal Quality	51 dB	Transmit/Receive Rate	0 bps

Connectivity

cpguser → guest-CP-Tun → AP1 → 6200 → Aruba9906.1 → Internet

You can then check the health metric icon.

CLIENT
cpguser
Health Metrics Early Access

Health
Last 3 hours

10:30 AM 10:45 AM 11:00 AM 11:15 AM 11:30 AM 11:45 AM 12:00 PM 12:15 PM 12:30 PM 12:45 PM 1:00 PM Now

Wireless **Alerts** **Events**

Impact
Negative (0) Neutral (1) Positive (4)

Search

5 items

Occurred	Event	Category	Description	Reason	Device Host Name
06/22/2026, 1:19:42 PM	Client DHCP Acknowledge	Clients	DHCP acknowledgement received from DHC...	-	AP1
06/22/2026, 1:19:42 PM	Client Onboarding Success	Clients	Onboarding success for client 66:c6:c8:38:9e...		
06/22/2026, 1:15:52 PM	Client 802.11 De-authentica...	Clients	De-authentication sent from client 66:c6:c8:...		
06/22/2026, 12:24:04 PM	Client Onboarding Success	Clients	Onboarding success for client 66:c6:c8:38:9e...		
06/22/2026, 12:23:28 PM	Client DHCP Acknowledge	Clients	DHCP acknowledgement received from DHC...		

Client DHCP Acknowledge ×

06/22/2026, 1:19:42 PM

Description
DHCP acknowledgement received from DHCP server 192.168.1.131 for client 66:c6:c8:38:9ed2 associated to BSSID d0:d3:e0:b2:2a:91 on channel 60E of AP hostname AP1

Category
Clients

Details

Source	66:c6:c8:38:9ed2	Client MAC Address	66:c6:c8:38:9ed2
AP MAC Address	20:4c:03:b6:b2:5b	AP Hostname	AP1
Band Frequency	5 GHz	Client VLAN	13
Client IP Address	10.10.13.30	Client IP Mask	255.255.255.0
Client Phy-Capabilities	5GHz-VHT-80sgl-2ss	Client SNR	44 dB
SSID name	guest-CP-Tun	BSSID	d0:d3:e0:b2:2a:91
Channel	60E	DHCP Server IP Address	192.168.1.131
Lease Time	4 hours	Latency	12 ms
Gateway IP Address	10.10.13.1	DNS Server IP Address	192.168.1.131

Then clicking in the individual events will provide more info like lease time, latency, the DNS server that the client is using as shown here.

4.8 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](#).