

# 1 Table of Contents

---

1	Table of Contents .....	1
1.1	Revision History .....	1
2	New Central Configuration for Mobility Gateways.....	2
2.1	Things you need.....	2
3	Mobility Gateway Onboarding – Green Field.....	3
3.1	Profile Categories and Configuration Checklist .....	4
3.2	Validating New Mobility Gateway .....	5
3.3	User Administrator Profile.....	6
3.4	System Administrator Profile.....	7
3.5	VLAN Profiles .....	8
3.6	Gateway System Profile.....	10
3.7	DNS and NTP Profiles.....	11
3.8	AAA Authentication Profile.....	12
3.9	Default Gateway Profile.....	14
3.10	Link Aggregation Profile.....	15
4	Onboarding Testing .....	18
4.1	Audit Trail .....	18
4.2	Configuring Hostname .....	19
4.3	LAG Operation Status .....	19
4.4	Gateway Clustering.....	22
4.5	References .....	24
5	Appendix -A .....	25
5.1	Mobility Gateway Onboarding Console bootup.....	25
5.2	Gateway Reset Procedure .....	27

## 1.1 Revision History

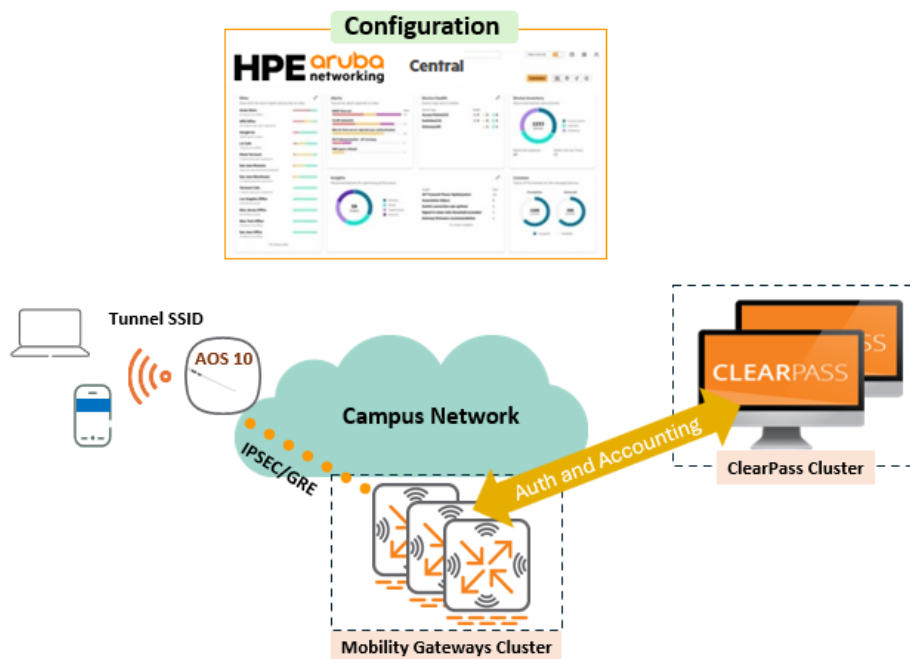
DATE	VERSION	EDITOR	CHANGES
06 Jun 2026	0.1	Ariya Parsamanesh	Initial creation
12 Jun 2026	0.2	Ariya Parsamanesh	Added the testing section

## 2 New Central Configuration for Mobility Gateways

In this technote, I'll walk through how to onboard and configure Mobility Gateways running HPE Aruba Networking Wireless Operating System 10 (AOS-10) using the New Central cloud-native platform. We'll cover pre-provisioning, firmware compliance, and the New Central configuration needed to automatically upgrade factory-default AOS8 gateways to AOS10 before pushing the required configuration.

This configuration builds on the New Central hierarchical configuration model that I covered in an earlier technote. The main benefit of this model is that it keeps configurations organised, easier to reuse, and more flexible across different levels of the network hierarchy.

I'll focus on the element profiles needed to onboard two Mobility Gateways, configure link aggregation, and then place the gateways into a high-availability cluster. This provides the foundation for the next stage: configuring AOS10 AP WLANs that operate in tunnel mode.



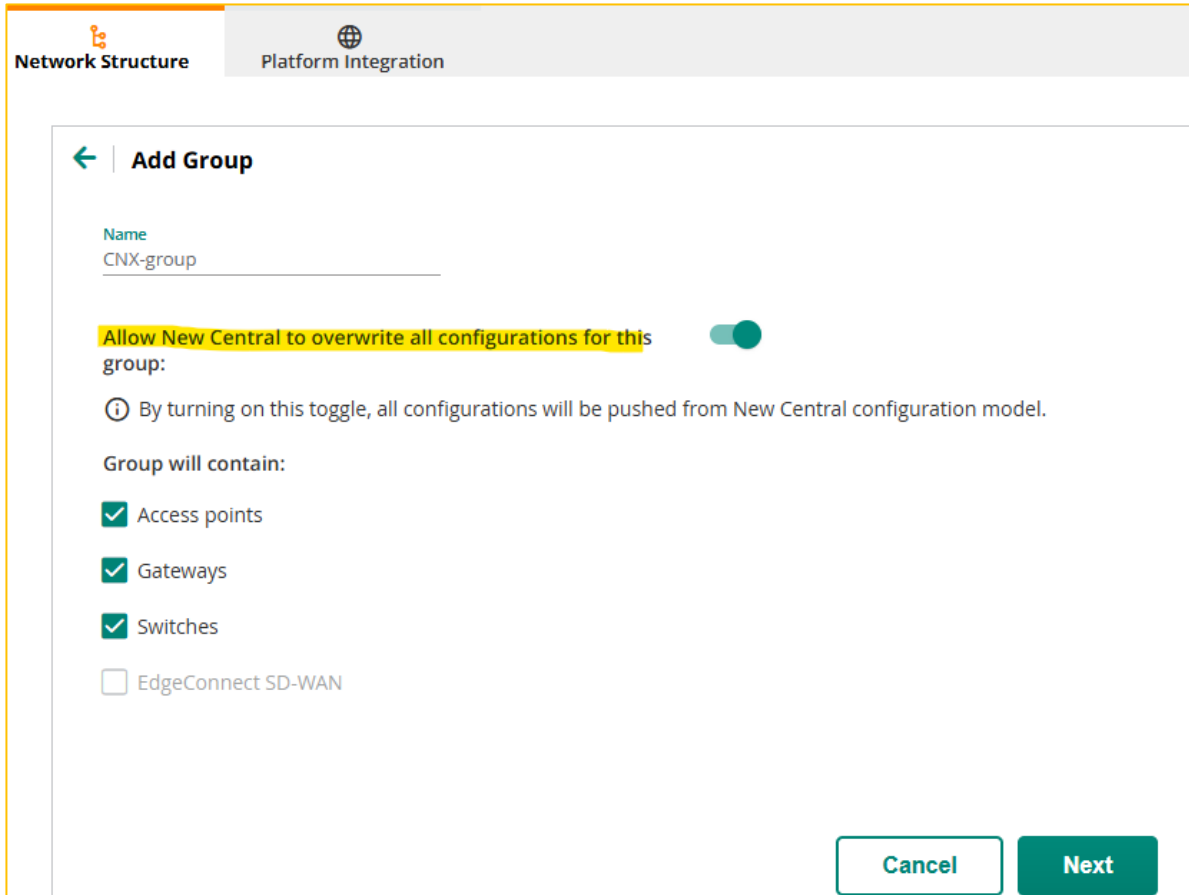
AOS-10 is a distributed network operating system that works with HPE Aruba Networking Central to manage and control access points and gateways. In AOS10, gateways no longer manage or adopt APs directly. Instead, they provide centralised data-plane services for APs and wired switches. This allows you to use policy-based forwarding to tunnel user traffic from APs and switches to the gateway cluster. All AOS10 APs and gateways are managed and adopted by Aruba Central.

### 2.1 Things you need

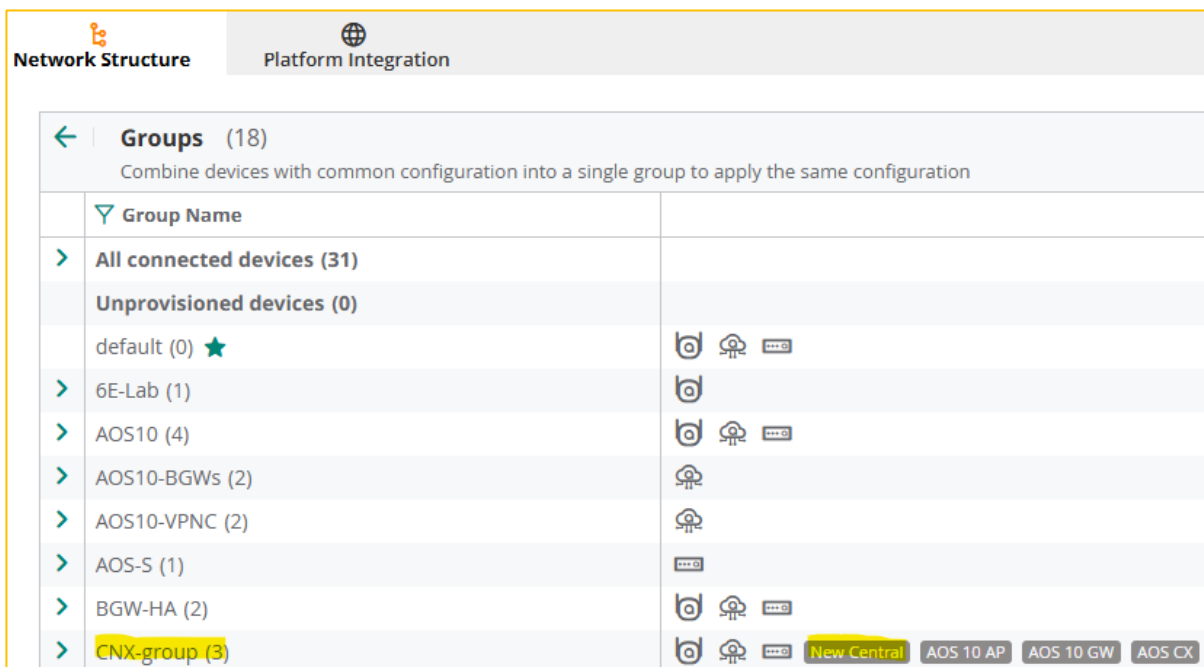
- Couple of gateways running minimum AOS10 firmware version or 10.4.1.7 (I am using factory default AOS8 8.5.0.0-1.0.7.1 gateways)
- AOS10 APs are already configured in New Central.
- Valid HPE Aruba Central account and subscriptions
- Optional ClearPass that is already configured as external authentication server. (This will be mainly used in my next technote that covered the tunnel WLAN configuration)

# 3 Mobility Gateway Onboarding – Green Field

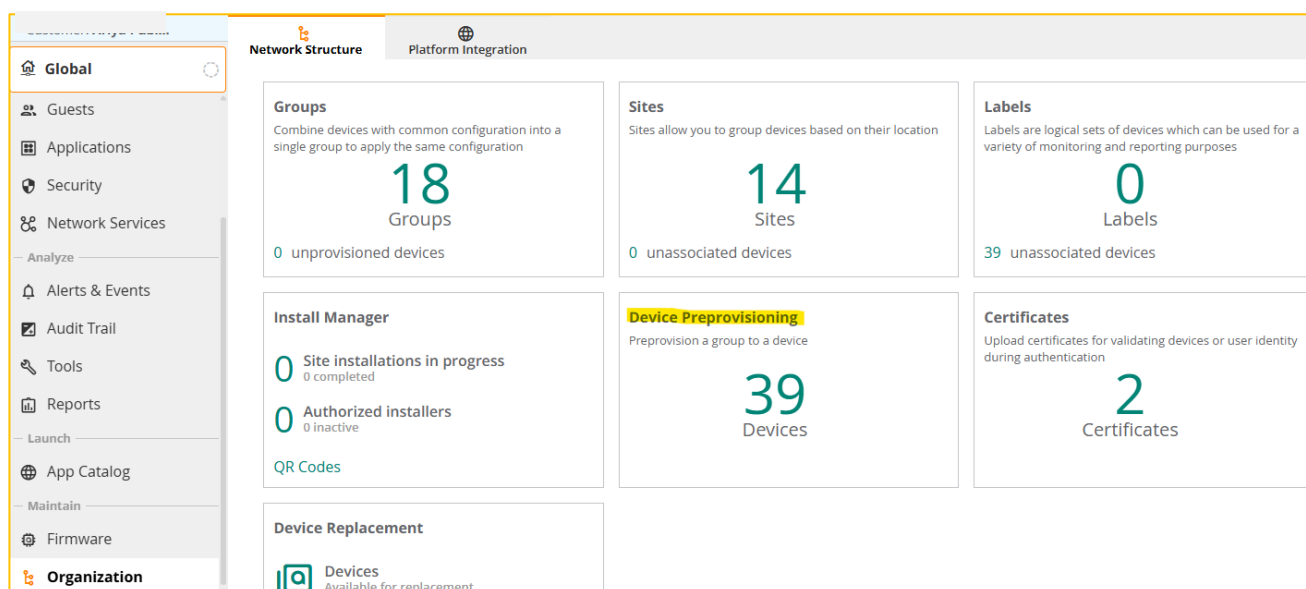
It is important to note that your APs, switches, and gateways must first belong to a device group within Classic Central. This device group must have the “Enable New Central” slider enabled, which is a setting available, only at the time you create a new group. Without this step, these devices cannot be managed or configured under the New Central platform.



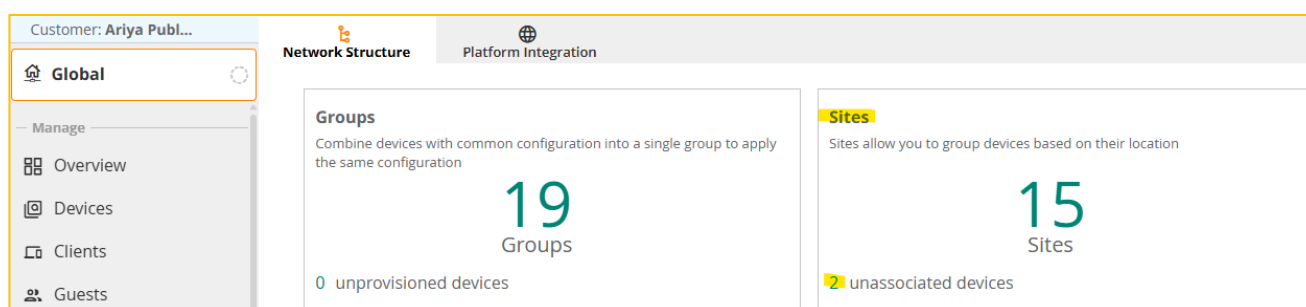
And once created it should be displayed as shown below.



You can move your Mobility gateways via Device Preprovisioning to the group that you have just enabled it for New Central configuration.



Once you have pre-provisioned the gateways to the new group which in my case is CNX-group, then you need to assign them to a Site which is mandatory for New Central configuration.



As seen above it shows that there are 2 devices that are not associated with any sites, these are my two new gateways. So, create a new Site and move the devices there for them to be visible in New Central, in my case I have added my two gateways to CNX-branch1. Once I move them to the correct site CNX-branch1, then at this point, the two gateways will be visible in New Central's device level configuration.

In order to get the gateways automatically upgraded to AOS10, I have set the gateway firmware compliance for this group to be 10.7.2.5.

The screenshot shows the 'Gateways' configuration page for the 'CNX-group'. The table below lists the gateways:

Name	Site	MAC Address	Serial	Model	Firmware Version	Recommended Version	Upgrade S...	Compliance Status
R1E	CNX-branch1	28:	C	R1B21A	Unknown	10.4.1.7_92147		Set
R1E	CNX-branch1	20:	C	R1B21A	Unknown	10.4.1.7_92147		Set

### 3.1 Profile Categories and Configuration Checklist

AOS10 AP and Gateways should be factory defaulted and generally devices must be assigned a device function. APs and gateways are automatically assigned their appropriate device function. And finally the minimum required firmware version is 10.4.1.7. So we are all good.

The table below show all the configuration profile categories that are available for mobility gateways. However not all of them are mandatory profiles to onboard the gateways. The ones that I'll use here are shown with "<<" next to it.

Categories	Subcategories	Categories	Subcategories
<b>System</b>	Gateway System << DNS Server << NTP Server << System Administration << User Administration << Syslog Server Dynamic DNS SNMP Time Range	<b>Security</b>	Authentication Server << Authentication Server Group << AAA Authentication << Captive Portal Authentication Certificate Usage EST Radius Proxy
<b>VLAN &amp; Network</b>	VLAN << Named VLANs VRRP Router STP Multicast (MGMD Global)	<b>Interfaces</b>	Port Profile Interface Profile GW Interface Profile << Management Interface Loopback Profile
<b>Tunnels</b>	GRE Tunnel GRE Tunnel Group	<b>Application Experience</b>	App Recognition and Control
<b>Network Services</b>	DHCP Pool DHCP Server	<b>Routing &amp; Overlays</b>	Static Routing << Route Maps VRF OSPF Prefix List VXLAN Tunnel VNI Community List PIM

This is my checklist for pre-staging AOS10 Mobility gateway configuration

1. Ensure the newly factory defaulted gateway is displayed under device configuration
2. Create a user administrator profile
3. Create a system administrator profile
4. Create a VLAN profile and assign scope to the profile with Enable L3 option
5. Create Gateway System Profile
6. Create DNS and NTP Profile
7. AAA Authentication Profile
8. Create Default gateway
9. Create LAG in GW interface configuration
10. Rename gateway hostname (if required)
11. Named VLAN Profile (if required)

Before we start with the pre-staging configuration, here are few points to consider

- You need to factory default the gateway if it previously part of a Classic Central group (incl default group).
- Use Library profiles for configuration settings that need to be applied throughout the hierarchy and to various device categories.
- Utilise Local profiles for settings that are specific to a device's function or its position within the hierarchy.
- Avoid using spaces in profile names instead use underscores or hyphens.

## 3.2 Validating New Mobility Gateway

Before we start the configuration, I just want to check that the newly factory defaulted gateways are listed and displayed in bold which means that it is in a group that can be configured by New Central. If the gateways have never contacted Aruba Central, then their serial number will be displayed as hostnames. This is shown below.

**GLOBAL**  
**Devices**  
 Access your network organization, configuration and operations from a single pane of glass.

**Library**

**Global**

**Site Collections**

**Sites**

**Devices**

**Devices**

Search

Clear Filters

2 results of 2 items

Name	Type	Model	Site	Device Group	MAC address
CN	Gateway	9004-RW	CNX-branch1	CNX-group	20
CN	Gateway	9004-RW	CNX-branch1	CNX-group	28

Generally, I always start all my configuration from the Library. By default, the device functions of “All” is selected. But you can choose any specific device type like Mobility gateways. This is shown below.

**GLOBAL**  
**Configuration Overview**  
 Information about the Library

**Library**

**Global**

**Site Collections**

**Sites**

**Devices**

**Device Groups**

**Profiles** Roles & Policies Named Objects Services

**Profiles Management**

Device Function

Mobility Gateway

**VLANs & Networks**

Type	Profiles
VLAN	6
Named VLANs	0
STP	1
VRRP Router	0

**Interfaces**

Type	Profiles
Port Profile	0
Interface Profile	0
Management Interface	1
Loopback Profile	1

**System**

Type	Profiles
User Administration	1
Syslog Server	0
Dynamic DNS	0
SNMP	0

### 3.3 User Administrator Profile

Navigate to the Library and create this profile as shown below. This is to set the admin password. This is needed when you SSH or console or reverse SSH to the gateways.

**Profiles** Roles & Policies Named Objects Services

**Library** > **System** > **User Administration**

Search

**Create Profile**

Name \*

admin-gold

Username \*

admin

Password \*

\*\*\*\*\*

Retype Password \*

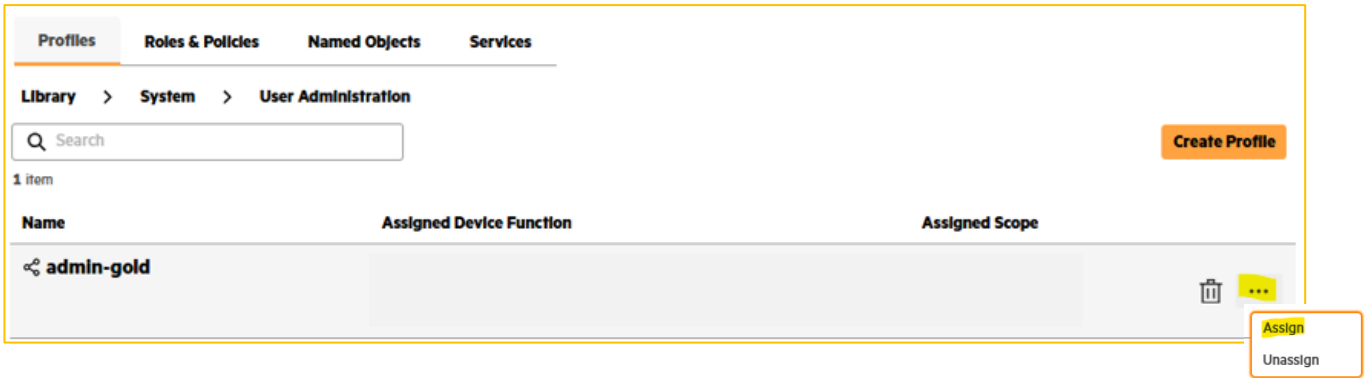
\*\*\*\*\*

Role \*

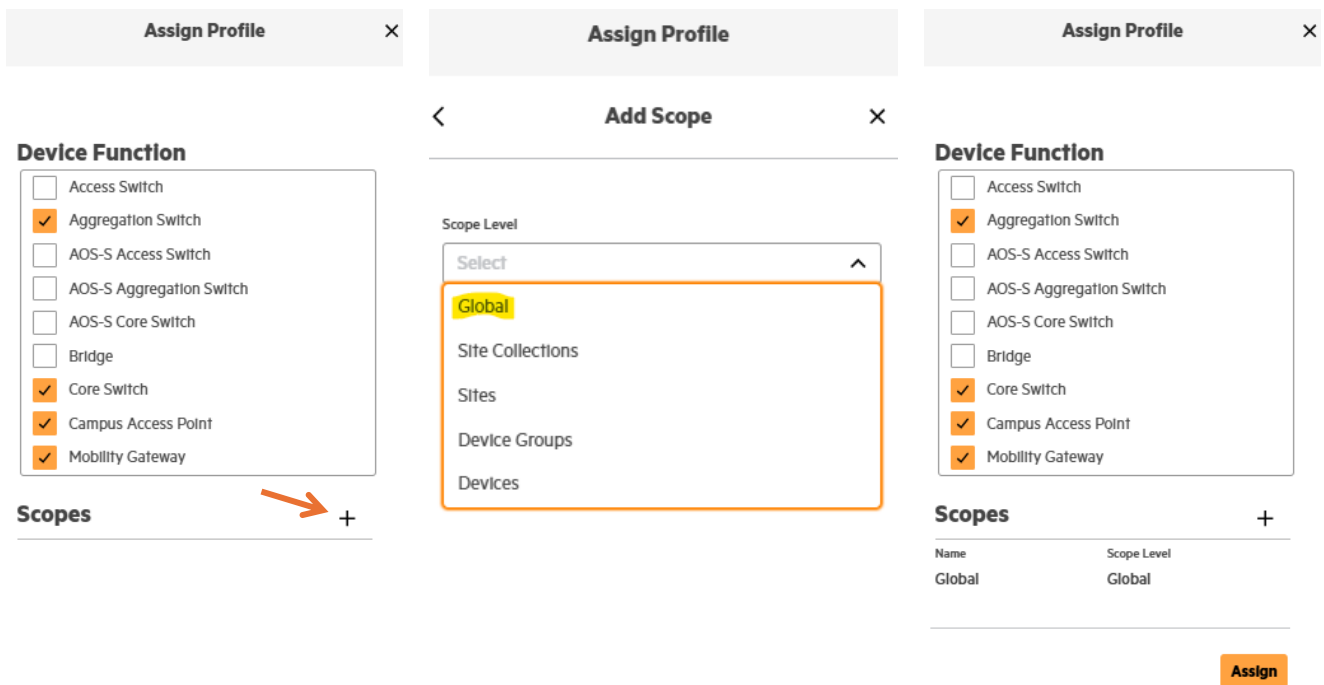
Admin

**Create**

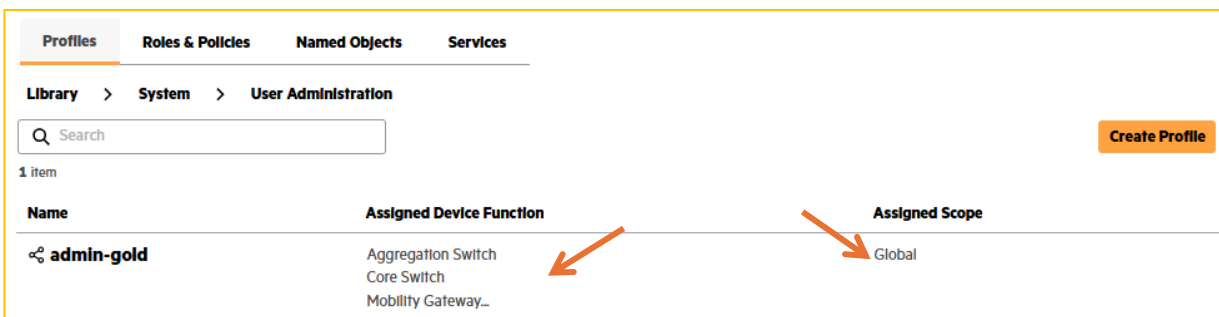
Once this is created it will be listed as shown below. The important thing to note is that it is not yet assigned to any device type and to any scope. In this state the configuration has no scope and not been applied to any device types. It's just sitting in the library.



We now need to assign it to a device function and a scope. When you hover your mouse over it you get the three dots and from there you can do both the assignments. Here I am assigning it to Aggregate switch, Core Switch, Campus access points and mobility gateway. This way I have consistency for the admin credentials. Also I have assigned to global. However, based on your policies, you can assign it to a site or site collections as well.



And once I have assigned and saved it, the assignments are shown below.



At this point the configuration will be pushed and synced with the Mobility gateway. You can go to the Audit Trail and check it.

### 3.4 System Administrator Profile

I'll start with the system card and choose System Administration to set the administrator password. Note that you can click on the radio button to go through the profiles that are available in the category.

Once you save it you can assign the device type and scope. Here I have assigned it to Mobility gateways, Access and Campus APs device function and the scope is global.

Name	Assigned Device Function	Assigned Scope
sys-admin-gold	Mobility Gateway Access Switch Campus Access Point	Global

### 3.5 VLAN Profiles

Here at the Library level, I have created a VLAN 192 and enable L3 and I'll use it as the system IP for the mobility gateway. I have also created VLAN 11-13 for my access switches and mobility gateways. These VLANs are mainly for role base access for wireless users.

VLAN Id	Descriptions	Device Types	Scope
11	Role based access	Access Switch, Mobility gateway	Global
12	Role based access	Access Switch, Mobility gateway	Global
13	Role based access	Access Switch, Mobility gateway	Global
192	System IP for mobility gateways	Mobility gateway	CNX-branch1

I am just showing VLAN 192 that will be used for system IP of the gateways. Note that we have enabled L3 and I must assign a static IP address at the device level for the gateways.

Once I have saved the VLAN profile, I will then assign it to the required scope.

VLAN ID	Name	Assigned Device Function	Assigned Scope
192	-	Mobility Gateway	CNX-branch1

Next, I need to set the IP address for VLAN 192 at the device level. When navigating to the device levels the gateways are shown by their serial numbers.

Name	Type	Model	Site	Device Group	MAC address
CN1	Gateway	9004-RW	CNX-branch1	CNX-group	20:...
CN1	Gateway	9004-RW	CNX-branch1	CNX-group	28:...

Then clicking on the first gateway that will list all the VLANs that are available for that gateway. You can see where those profiles have been assigned to, which in my case is Globa for VLAN 11-13 and CNX-branch site for VLAN 192.

Profiles	Roles & Policies	Named Objects	Services		
CN	> VLANs & Networks	> VLAN	Mobility Gateway		
<input type="text" value="Search"/> <span style="float: right;">Create Profile</span>					
6 items					
VLAN ID	Name	Inherits From	Assigned Device Function	Assigned Scope	Overrides
1	DEFAULT_VLAN_1	Global	Mobility Gateway	Global	-
11	-	Global	Mobility Gateway	Global	-
12	-	Global	Mobility Gateway	Global	-
13	-	Global	Mobility Gateway	Global	-
192	-	Site	Mobility Gateway	CNX-branch1	-

Then you click on the VLAN 192 and ensure you have checked the “save as local profile” which will then show the field for the static IP address.

Properties
References

*i* This profile is inherited from SITE. Any modification will break this inheritance and will set the profile as an override.

### General

 Save as a local profile

### Layer 3

 Enable L3  
 Admin State  
 Use IPv4 Alias  
 IPv4 Address Assignment \*  
 Static  
 DHCP  
OX device doesn't support configuring DHCP-Client on more than one VLAN  
 IPv4 Address/Prefix  
  
 Use IPv6 Alias

### Switch Layer 3 Parameters

 Switch Specific Parameters

### Gateway Layer 3 Parameters

 Gateway Specific Parameters  
 Force Operational Status Up  
 Enable Routing  
 Broadcast Multicast Optimizations  
 Suppress ARP  
 Local Proxy ARP  
 NAT Inside  
 NAT Outside  
Adjust TCP MSS

Once you save it, it will be displayed as follows. Note the half-moon icon that shows the configuration has inherited from self, meaning the device level.

VLAN ID	Name	Inherits From	Assigned Device Function	Assigned Scope
1	DEFAULT_VLAN_1	Global	Mobility Gateway	Global
11	-	Global	Mobility Gateway	Global
12	-	Global	Mobility Gateway	Global
13	-	Global	Mobility Gateway	Global
192	-	Self	Mobility Gateway	

### 3.6 Gateway System Profile

This is a mandatory profile as it sets system IP, time zone, and other custom parameters for the gateways. One cool thing is that if your sites have been configured with real addresses then the time zone parameter is automatically set based on the site's location that the gateway is in. But since I am not using real addresses for my sites then I need to set it even though it is not displayed here. We are starting at the library level.

### Create Profile

Name \*  
gateway-sys-prof

Description

Location

Contact

Use IPv6 System VLAN Alias

IPv6 System IP  
None

Please set the System-IP for the gateway to enable full functionality

Source Interface Type

None  
 Loopback  
 VLAN

### General

Timezone \*  
Automatic (from site)

LCD Menu

LCD Maintenance

GPS

Use IPv4 System VLAN Alias

**System IP**  
VLAN 192

### Security

FIPS Compliance

### Authentication Timers

User Idle Timeout  
5 Minutes

Authentication Server Dead Time  
10 Minutes

Logon User Lifetime  
5 Minutes

### RADIUS Client

NAS Interface Type

None  
 IP Address  
 VLAN

### Firewall

Firewall Options

Deny Inter User Bridging  
 Deny Inter User Traffic  
 IPv6 Processing  
 Trust Client Voice QOS

Jumbo Frames Processing

Jumbo Frames MTU  
1789-9216  
Bytes

### Logging

Category Subcategory Process Logging Level

No data to display

Here, I have just added system IP VLAN and time zone, the rest of left as default. Of course you can change the other setting too. Here I am just configuring the minimum configuration.

And as before you need to perform the assignment too. I have assigned to Mobility Gateway and Site level. But you can also assign it to Sites and Site Collections.

### Configuration Overview

Information about the Library

Library

Global

Site Collections

Sites

Profiles Roles & Policies Named Objects Services

Library > System > Gateway System

Search

1 item

Name	Assigned Device Function	Assigned Scope
gateway-sys-prof	Mobility Gateway	CNX-branch1

Create Profile

## 3.7 DNS and NTP Profiles

Next on my checklist is setting the DNS and NTP profiles. I have configured one called Corp-DNS and Corp-NTP. Again, all these common network objects like DNS and NTP can be assigned to all your device functions. I have assigned it to all my device functions and global scope. You can set up an additional profile for a site or site collection that takes precedence over the global profile.

This lets you standardise configurations at different levels to suit your needs. Importantly, if you delete the site-level/site collection profile, the global profile is instantly applied, ensuring compliance with your organisation's configuration standards.

### GLOBAL Configuration Overview

Information about the Library

Library

Global

Site Collections

Sites

Devices

Profiles Roles & Policies Named Objects Services

Library > System > DNS Server

Search

2 items

Name	Assigned Device Function	Assigned Scope
Corp-DNS	Aggregation Switch Mobility Gateway Core Switch...	global
Pub-DNS	-	-

Create Profile

**Properties**   **References**

Name \*

Description

Domain Name

Domain List

+

Note: domain-name will be ignored when both domain-name and domain list are configured

 DNS Alias


### DNS Servers

GW, AOS-S supports a maximum of 6, 4 DNS servers respectively and CX supports a maximum of 3 DNS servers per VRF.

IP Address	Format
192.168.1.131	IPv4

### DNS Static Hosts

GW and CX Supports Maximum of 200 and 6 Static Hosts Respectively

Hostname	VRF Profile
 No data to display	

And here is the NTP Profile.

Search Central

**Profiles**   **Roles & Policies**   **Named Objects**   **Services**

Library > System > NTP Server

Search

4 items

Name	Assigned Device Function
Corp-NTP	Campus Access Point Core Switch Mobility Gateway...
Pub-NTP	-
ntp_vrf_default <small>default VRF2 for client connections only</small>	Core Switch Aggregation Switch Access Switch
ntp_vrf_mgmt <small>default VRF1 for client connections only</small>	Core Switch Aggregation Switch Access Switch

**Edit Profile** ×

**Properties**   **References**

Name \*

Description

 NTP Alias

### NTP Server

IP Address	Format
192.168.1.131	IPv4
au.pool.ntp.org	FQDN

 Switch Specific Parameters

### 3.8 AAA Authentication Profile

This is not mandatory for onboarding gateways but eventually I'll be requiring it and hence it is configured here. Since I have an existing on premise NAC appliance (ClearPass) I'll use that as my authentication server. You can also configure TACACS authentication servers too. But here I am just showing RADIUS auth servers.

**Profiles**   **Roles & Policies**   **Named Objects**   **Services**

Library > Security > Authentication Server

Search Create Profile

6 items

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

I am showing ClearPassRadiusVIP1 server. You can also select device specific parameters for switches and gateways.

### Edit Profile

**Properties**   **References**

Name \*

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 \*

Shared Secret Alias

Shared Secret Alias

Authentication Port \*

Accounting Port \*

Advanced

### Edit Profile

NAS Identifier

NAS IP Address

Require Message-Authenticator in RADI...

AirGroup 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

Next, I must configure Authentication server group that will include the Auth servers we just configured. I have two authentication server groups to distribute my auth session across the Authentication servers I have configured. Now focusing on Radius-East Server group. Note that I am using Radius with CoA and “Shared Secret Alias”.

You can create an alias from Named Objects tab as shown below.

**Profiles**   **Roles & Policies**   **Named Objects**   **Services**

### Named Objects Management

**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](#)

**Profiles**   **Roles & Policies**   **Named Objects**   **Services**

Library > **Aliases**

Q shared | [Create Alias](#)

1 item

Name	Type	Assigned Device Function	Assigned Scope
🔗 <b>ClearPassShared</b>	Auth Server Shared Secret	Access Switch Aggregation Switch Mobility Gateway...	Global

I need to add the authentications servers to the auth server groups where I have added my two ClearPass nodes.

**Profiles**   **Roles & Policies**   **Named Objects**   **Services**

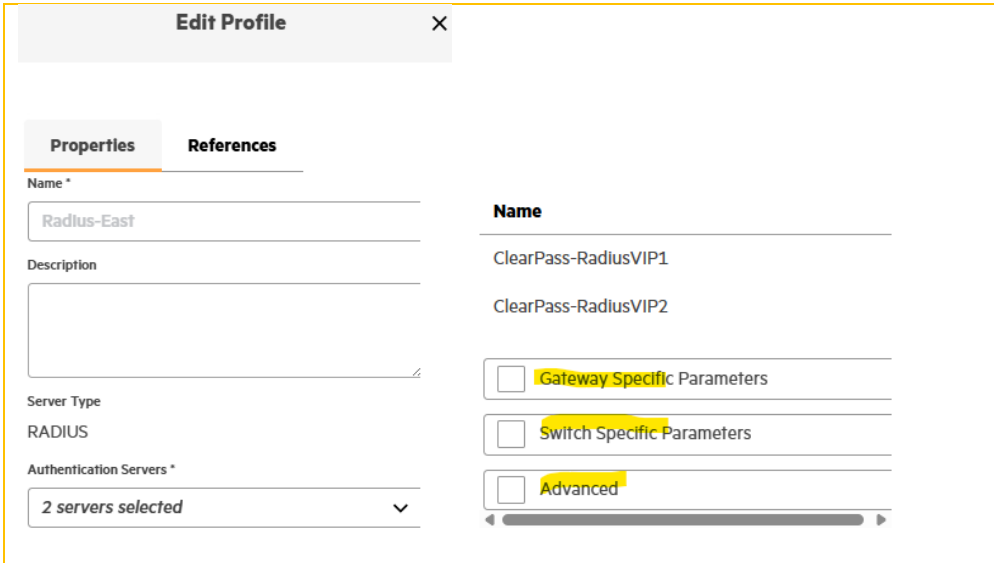
Library > **Security** > **Authentication Server Group**

Q Search | [Create Profile](#)

9 items

Name	Type	Servers	Assigned Device Function	Assigned Scope
🔗 <b>Radius-East</b>	RADIUS	2	Mobility Gateway, Access Switch, Campus Access Point	Global
<p><b>Name</b></p> <p>ClearPassRadiusVIP1</p> <p>ClearPassRadiusVIP2</p>				
> 🔗 <b>Radius-West</b>	RADIUS	2	Mobility Gateway, Access Switch, Campus Access Point	Global

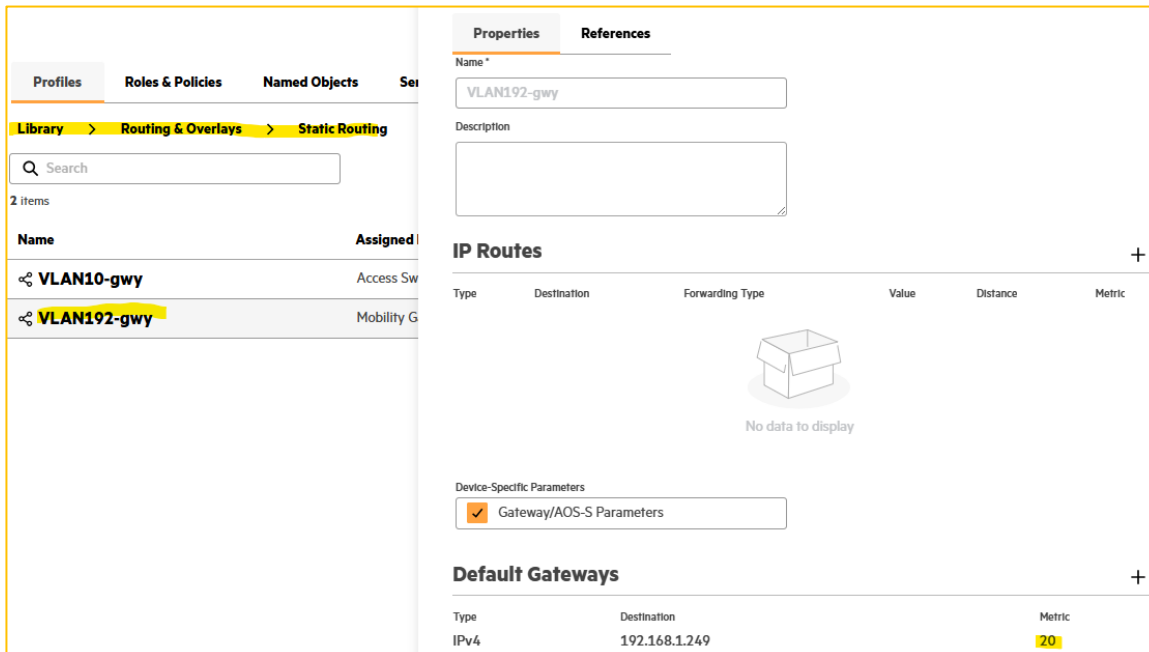
You see that there is specific configuration setting just for Switches and/or gateways. So you can have all those collected in one profile. And this specific configuration will one be applied to the specified device personas.



### 3.9 Default Gateway Profile

For onboarding of the gateways, I am planning to use one of the interfaces say 0/0/0 as an out of band mgmt. port, this is because it has DHCP enabled and its on VLAN1. I also ensure that the rest of the interfaces are not connected. Then once the gateway is up and has contacted Aruba Central which then will enforce the firmware upgrade to the compliance version we have set to, then I'll start the device level configuration like IP addressing for VLAN 192 and LACP interfaces. Then I disconnect the OOBM interface and connect the production interface which in my case is 0/0/2 and 0/0/3.

Here, I am setting the default gateway for the production network.



In my setup, the default gateway for the OOBM and the production networks are different. So, to ensure my connectivity is not disrupted when I switch between OOBM and production network of my gateways, I had to change the default route metric.

Note that the metric for this default gateways is 20 and it is higher than the one the gateway receives from DHCP on its 0/0/0. This way you can ensure you have connectivity when the OOBM interface is connected again. The default gateway metric is 10 for the DHCP enabled interface. I have now assigned it to CNX-branch1.

Profiles Roles & Policies Named Objects Services

Library > Routing & Overlays > Static Routing

Q 192 X Create Profile

1 item

Name	Assigned Device Function	Assigned Scope
VLAN192-gwy	Mobility Gateway	CNX-branch1

### 3.10 Link Aggregation Profile

This is to configure port channel or Link Aggregation (LAG) for the gateways. You need to navigate to device level > Interfaces > GW Interface Configuration

GATEWAY Network config management for this scope

Profiles Roles & Policies Named Objects Services

Library

Global

Site Collections

Sites

CNX-branch1 X

Devices

CN X

Device Groups

CNX-group X

#### Profiles Management

Type	Profiles
VLAN	6
Named VLANs	0
STP	1
VRPP Router	0

Manage

Type	Profiles
Port Profile	0
GW Interface Configuration	4
Management Interface	0
Loopback Profile	1

Manage

Type	Profiles
System Information	1
Gateway System	1
DNS Server	1
NTP Server	1

Manage

Type	Profiles
Authentication Server	6
Authentication Server Group	5
AAA Authentication	11
Captive Portal Authentication	3

Manage

Type	Profiles
GRE Tunnel	0
GRE Tunnel Group	0

Manage

Type	Profiles
Static Routing	1
Route Maps	0
VRF	1
OSPF	0

Manage

Before you add the interface to the LAG profile ensure LLDP Transmit/Receive are enabled on the individual interfaces. This is so that you get a correct topology when you monitor your site in New Central.

Profiles Roles & Policies Named Objects Services

CN Interfaces > GW Interface Configuration Mobility Gateway

Ports LAGs

Q Search

4 items

Port	Admin Status	Speed/Duplex	Port Profile
0/0/0	Enabled	Auto Auto	-
0/0/1	Enabled	Auto Auto	-
0/0/2	Enabled	Auto Auto	-

0 1 2 3 4

<input type="checkbox"/> PoE	
<input type="checkbox"/> Jumbo MTU	
<input type="checkbox"/> Spanning Tree	
<input checked="" type="checkbox"/> LLDP Config	
<input checked="" type="checkbox"/> LLDP Transmission	
Transmit Interval	30
Transmit Hold	4
Fast Transmit Interval	1
Fast Transmit Count	4
<input checked="" type="checkbox"/> LLDP Receive	
<input checked="" type="checkbox"/> LLDP-MED	

Once you have done this for both 0/0/2 and 0/0/3, then proceed to LAG tab and click on port-channel 0.

Profiles Roles & Policies Named Objects Services

CN > Interfaces > GW Interface Configuration Mobility Gateway

Ports LAGs

Search

8 items

0 1 2 3 4

Name	Ports	Admin State	Protocol	VLAN Mode	VLAN	Description
0	-	Yes	-	Access	1	-
1	-	Yes	-	Access	1	-

Legend

- Connected
- Error
- Disabled
- Not Connected
- Uplink

Select Information to Display

Neighbor Type

Edit LAG

LAG

Configure Link Aggregation ( LAG ) for ports.

General

Ports



LAG ID \*

2

Edit LAG

Add Port to LAG

Ports

2 Items selected

- Select All
- 0/0/0
- 0/0/1
- 0/0/2
- 0/0/3

View Selection

Add

Edit LAG

LAG

Configure Link Aggregation ( LAG ) for ports.

General

Ports

0/0/2

0/0/3

LAG ID \*

0

Description

Admin State

Protocol \*

LACP

Mode \*

Active

Passive

Network Parameters

VLAN Mode \*

Access

Trunk

Native VLAN \*

192

Allowed VLANs \*

11-13,192

VLAN Security

VLAN	Client Authentication	Policy
11-13	false	-
192	false	-

Jumbo MTU

Spanning Tree

Once it is saved, you'll see the following screenshot.

The screenshot shows a network configuration interface with the following elements:

- Navigation tabs: Profiles, Roles & Policies, Named Objects, Services.
- Breadcrumbs: CN > Interfaces > GW Interface Configuration (Mobility Gateway).
- Sub-tabs: Ports, LAGs.
- Search bar: Q Search.
- Item count: 8 items.
- Visual indicator: A row of 5 boxes labeled 0, 1, 2, 3, 4, with box 4 highlighted.
- Table with columns: Name, Ports, Admin State, Protocol, VLAN Mode, VLAN, Description.
- Legend: Connected (green), Error (red), Disabled (grey), Not Connected (light grey), Uplink (dotted).
- Select Information to Display: Neighbor Type (dropdown).

Name	Ports	Admin State	Protocol	VLAN Mode	VLAN	Description
0	0/0/2, 0/0/3	Yes	LACP	Trunk	NATIVE: 192	-
1	-	Yes	-	Access	1	-

It goes without saying that you need to configure the LAN switch ports that connect to the gateways as LACP as well. And just for completeness here is the configuration of the CX switch that connects to this gateway.

```
interface lag 250
  no shutdown
  no routing
  vlan trunk native 192
  vlan trunk allowed 11-13,192
  lacp mode active
  lacp rate fast
!
interface 1/1/11
  no shutdown
  lag 250
!
interface 1/1/12
  no shutdown
  lag 250
```

# 4 Onboarding Testing

Here I am using a brand new 9004 mobility gateway which it seems was shipped with ArubaOS Version 8.5.0.0-1.0.7.1. I first connect the interface 0/0/0 to my network, by default this interface is enabled for DHCP.


The gateway will reach out to Aruba Central and will and will go through the following tasks and it

- Starts Zero Touch Provisioning (ZTP) auto provision
- Reaches out to device.arubanetworks.com which informs it to go to a specific instant of Aruba Central
- Will then reach out to device-apacsouth.central.arubanetworks.com
- GreenLake will check if the device is in the inventory and has a valid subscription.
- Then the device will be assigned to the Device Preprovisioning group. In our case it is CNX-branch1
- Then the device will be automatically upgraded to 10.7.2.5 version. This is because I configure firmware compliance.

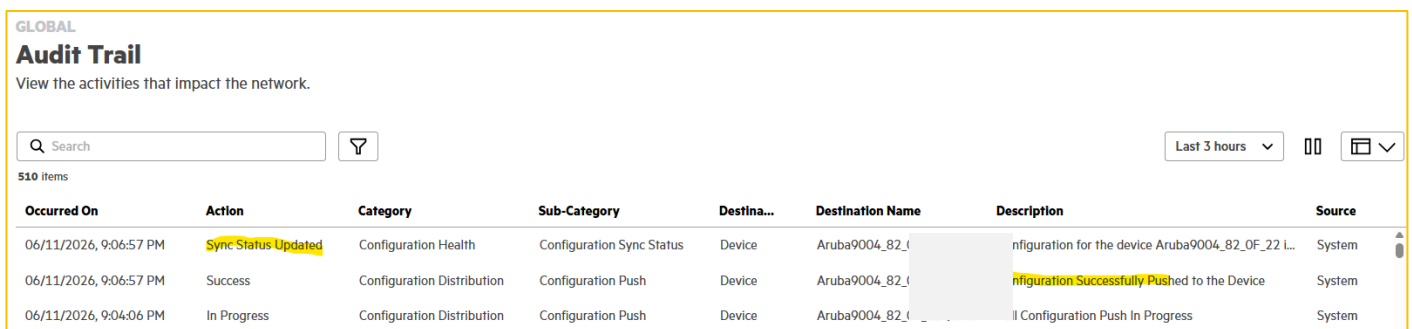
For complete gateway onboarding console bootup, refer to Appendix A.

## 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 also search for specific strings.

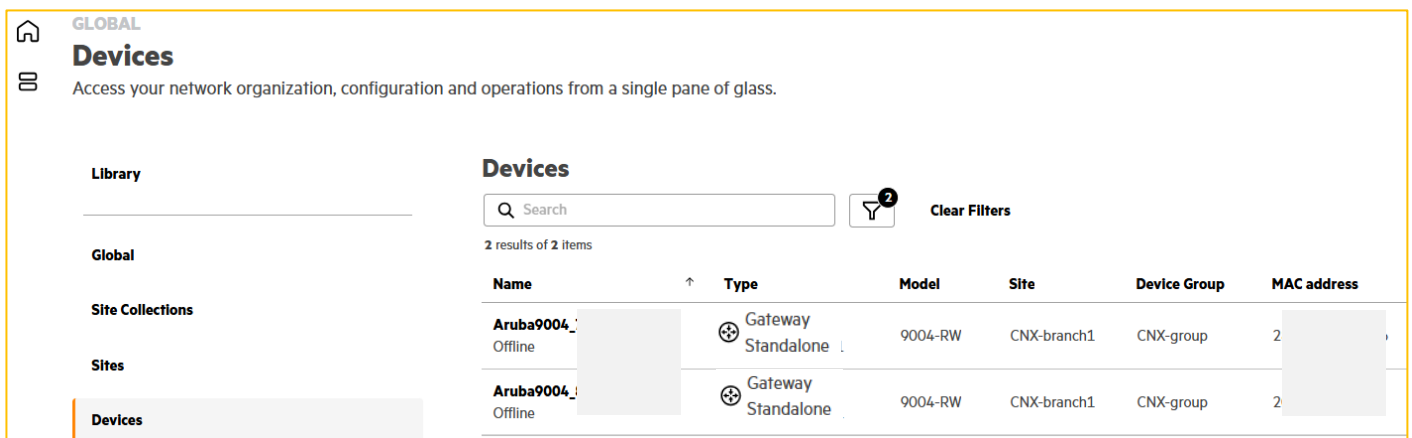
Here you'll see that the configuration was successfully pushed.



The screenshot shows the 'Audit Trail' section of the network management interface. It includes a search bar, a filter icon, and a dropdown menu set to 'Last 3 hours'. Below the search bar, it indicates '510 items'. The main content is a table with the following columns: Occurred On, Action, Category, Sub-Category, Destina..., Destination Name, Description, and Source. Three rows of data are visible, showing configuration sync status updates and successful pushes.

Occurred On	Action	Category	Sub-Category	Destina...	Destination Name	Description	Source
06/11/2026, 9:06:57 PM	Sync Status Updated	Configuration Health	Configuration Sync Status	Device	Aruba9004_B2_...	nfiguration for the device Aruba9004_B2_OF_22 L...	System
06/11/2026, 9:06:57 PM	Success	Configuration Distribution	Configuration Push	Device	Aruba9004_B2_...	nfiguration Successfully Pushed to the Device	System
06/11/2026, 9:04:06 PM	In Progress	Configuration Distribution	Configuration Push	Device	Aruba9004_B2_...	ll Configuration Push In Progress	System

And the gateways will be displayed as shown below. Note that the hostname is now changed to their factory defaulted hostname like Aruba9004\_xx\_xx\_xx, where the xx are the MAC address.



The screenshot shows the 'Devices' section of the network management interface. It includes a search bar, a filter icon with a '2' notification, and a 'Clear Filters' button. Below the search bar, it indicates '2 results of 2 items'. The main content is a table with the following columns: Name, Type, Model, Site, Device Group, and MAC address. Two rows of data are visible, showing gateway devices in a standalone configuration.

Name	Type	Model	Site	Device Group	MAC address
Aruba9004_... Offline	Gateway Standalone	9004-RW	CNX-branch1	CNX-group	2...
Aruba9004_... Offline	Gateway Standalone	9004-RW	CNX-branch1	CNX-group	2...

## 4.2 Configuring Hostname

At this stage the mobility gateway has the configuration but has a default hostname. So, from the device level, I'll first add the hostname.

The screenshot shows the configuration page for 'sys-system-info-profile'. The breadcrumb navigation is 'Aruba9004\_1 > System > System Information > Mobility Gateway'. The 'Name' field contains 'sys-system-info-profile'. The 'Hostname' field is highlighted with an orange border and contains 'Aruba9004\_1'. Below the form is a table with one row:

Name	Inherits From	Assigned Device Function
sys-system-info-profile	Self	Mobility Gateway

Once I update it, it will get refreshed and shown below

The screenshot shows the configuration page for 'sys-system-info-profile' after an update. The breadcrumb navigation is 'Aruba9004\_1 > System > System Information > Mobility Gateway'. The 'Name' field contains 'sys-system-info-profile'. The 'Assigned Device Function' is 'Mobility Gateway'. The 'Assigned Scope' field now contains 'Aruba9004\_1'. Below the form is a table with one row:

Name	Inherits From	Assigned Device Function	Assigned Scope
sys-system-info-profile	Self	Mobility Gateway	Aruba9004_1

## 4.3 LAG Operation Status

Note that so far the gateways are connected with their so called OOBM port (I am using interface 0/0/0). Once the configuration is synchronised, I'll disconnect the interface 0/0/0 and connect the 0/0/2 and 0/0/3 which are part of the LAG that connects to the real production network. (The other way you can do this is, connect all the gateways ports to the respective LAN switches and control which ports will be operational from your LAN switch.)

Here is when the OOBM interface is still connected.

```
(Aruba9004_1) #show port status

Port Status
-----
Slot-Port  PortType  AdminState  OperState  PoE  Trusted  SpanningTree  PortMode  Speed  Duplex  PortError
-----
0/0/0      GE        Enabled     Up         N/A  Yes      Forwarding    Access    1 Gbps Full    -
0/0/1      GE        Enabled     Down      N/A  Yes      Disabled      Access    Auto   Auto    -
0/0/2      GE        Enabled     Down      N/A  N/A      N/A           PC0       Auto   Auto    -
0/0/3      GE        Enabled     Down      N/A  N/A      N/A           PC0       Auto   Auto    -
PC0        PC        Enabled     Down      N/A  Yes      Discarding    Trunk     N/A    N/A     -

(Aruba9004_1) #
```

```
(Aruba9004_1) #show ip interface b

Interface          IP Address / IP Netmask      Admin  Protocol  VRRP-IP
-----
vlan 13            unassigned / unassigned             up     down
vlan 4094          10.10.30.34 / 255.255.255.0           up     up
vlan 192           192.168.1.241 / 255.255.255.0           up     up
vlan 1             unassigned / unassigned             up     down
loopback           unassigned / unassigned             up     up

DHCP is enabled on VLAN(s) 4094
(Aruba9004_1) #
```

Also note the default route that it is point to the default gateway on my onboarding VLAN (VLAN30). See the metric for this default route is 10 and that's why it is showing here even though there is another static default route to VLAN192 gateway but with higher metric.

```
(Aruba9004_1) #show ip route

Codes: C - Connected, O - OSPF, IA - OSPF Inter Area, E1 - OSPF External Type 1, R -
RIP
      E2 - OSPF External Type 2, N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA
External Type 2
      B I - BGP Interior, B E - BGP Exterior, EV - BGP EVPN, S - Static
      U - BGW Peer Uplink, M - Management, Ru - Route Usable, * - Candidate Default
      V - RAPNG VPN/Branch, I - Crypto-Cfgset, N - Not Redistributed, Bc - Cloud
Overlay Protocol

S*   0.0.0.0/0 [50/10] via 10.10.30.1
C    192.168.1.0/24 is directly connected, VLAN192
C    10.10.30.0/24 is directly connected, VLAN4094

(Aruba9004_1) #
```

This is when I connect the LAG interfaces and disconnect the OOBM interface.

```
(Aruba9004_1) #show port status

Port Status
-----
Slot-Port  PortType  AdminState  OperState  PoE  Trusted  SpanningTree  PortMode  Speed  Duplex  PortError
-----
0/0/0      GE        Enabled     Down       N/A  Yes      Disabled      Access    Auto   Auto   -
0/0/1      GE        Enabled     Down       N/A  Yes      Disabled      Access    Auto   Auto   -
0/0/2      GE        Enabled     Up         N/A  N/A      N/A           PC0       1 Gbps Full  -
0/0/3      GE        Enabled     Up         N/A  N/A      N/A           PC0       1 Gbps Full  -
PC0        PC        Enabled     Up         N/A  Yes      Forwarding    Trunk     1 Gbps N/A    -

(Aruba9004_1) #
```

Note that the onboarding VLAN disappears as it is not up.

```
(Aruba9004_1) #show ip interface b

Interface                IP Address / IP Netmask      Admin  Protocol  VRRP-IP
vlan 13                  unassigned / unassigned      up     up
vlan 4094                 unassigned / unassigned      up     down
vlan 192                  192.168.1.241 / 255.255.255.0 up     up
vlan 1                    unassigned / unassigned      up     down
loopback                 unassigned / unassigned      up     up

DHCP is enabled on VLAN(s) 4094

(Aruba9004_1) #
```

And the default route changes to 192.168.1.249 with the metric of 20.

```
(Aruba9004_1) #show ip route

Codes: C - Connected, O - OSPF, IA - OSPF Inter Area, E1 - OSPF External Type 1, R -
RIP
      E2 - OSPF External Type 2, N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA
External Type 2
      B I - BGP Interior, B E - BGP Exterior, EV - BGP EVPN, S - Static
      U - BGW Peer Uplink, M - Management, Ru - Route Usable, * - Candidate Default
      V - RAPNG VPN/Branch, I - Crypto-Cfgset, N - Not Redistributed, Bc - Cloud
Overlay Protocol

S*   0.0.0.0/0 [50/20] via 192.168.1.249
C    192.168.1.0/24 is directly connected, VLAN192

(Aruba9004_1) #
```

Here I want to check the status of the link aggregation interfaces which you can use a remote console from New Central and run these commands.

```
(Aruba9004_1) #show interface port-channel 0

Port-Channel 0 is administratively up, Link is up, Line protocol is up
Hardware is Port-Channel, address is 20:4C:03:1A:2F:74 (bia 20:4C:03:1A:2F:74)
Description: Link Aggregate (LACP)
Spanning Tree is Forwarding
Switchport priority: 0
Jumbo Support is enabled on this interface MTU 9216
Member port(s):
  GE 0/0/2, Admin is up, Link is up, Line protocol is up
  GE 0/0/3, Admin is up, Link is up, Line protocol is up
Speed :2 Gbps
Interface index: 8195
Last clearing of "show interface" counters 0 day 0 hr 41 min 50 sec
link status last changed 0 day 0 hr 7 min 54 sec
 35462 packets input, 31617886 bytes
  Received 9768 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input error bytes, 0 CRC, 0 frame
 2419 multicast, 23275 unicast
 4674 packets output, 613856 bytes
  0 output errors bytes, 0 deferred
  0 collisions, 0 late collisions, 0 throttles
Port-Channel 2 is TRUSTED

Statistics for member port: GE 0/0/2
 8630 packets input, 2975839 bytes
  Received 4453 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input error bytes, 0 CRC, 0 frame
 1527 multicast, 2650 unicast
 1883 packets output, 335108 bytes
  0 output errors bytes, 0 deferred
  0 collisions, 0 late collisions, 0 throttles
Statistics for member port: GE 0/0/3
26832 packets input, 28642047 bytes
  Received 5315 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input error bytes, 0 CRC, 0 frame
  892 multicast, 20625 unicast
 2791 packets output, 278748 bytes
  0 output errors bytes, 0 deferred
  0 collisions, 0 late collisions, 0 throttles

(Aruba9004_1) #
```

You can also use this command to check the LACP interfaces.

```
(Aruba9004_2) #show lacp summary

LACP 0
LACP Counter Table
-----
Port          PDUTx  PDURx  MrkTx  MrkRx  MrkRspTx  MrkRspRx  ErrPktRx  Age  Ena  Dis
-----
GE 0/0/2      6       7       0       0       0         0         0         63s  1   0
GE 0/0/3      7       8       0       0       0         0         0         66s  1   0

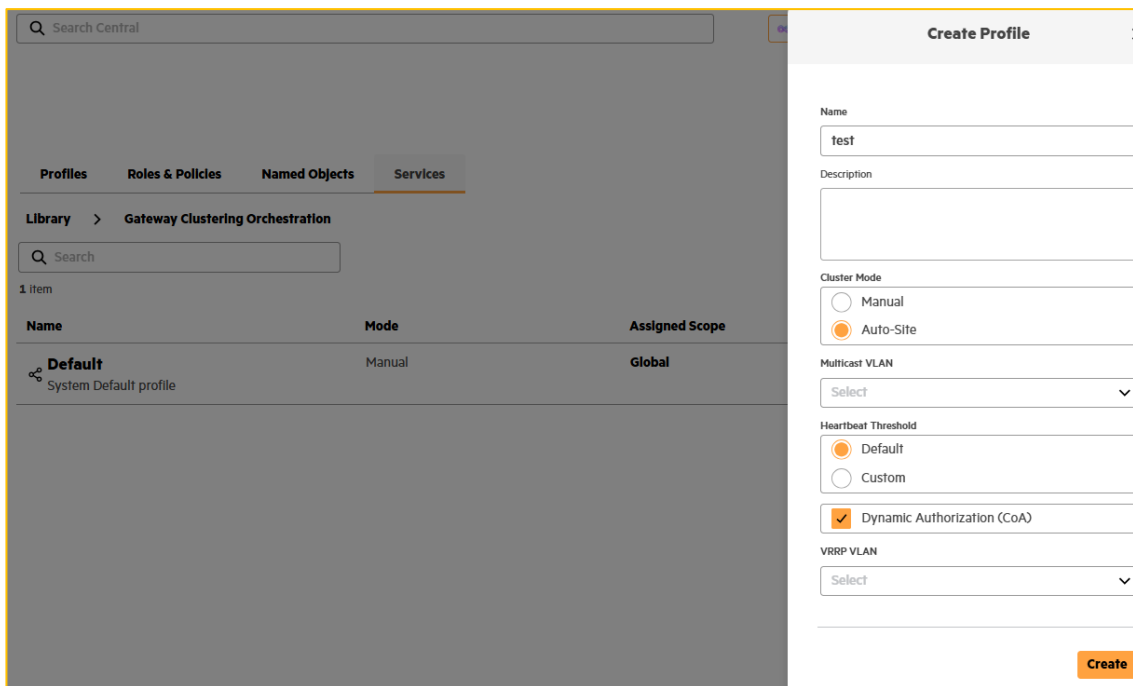
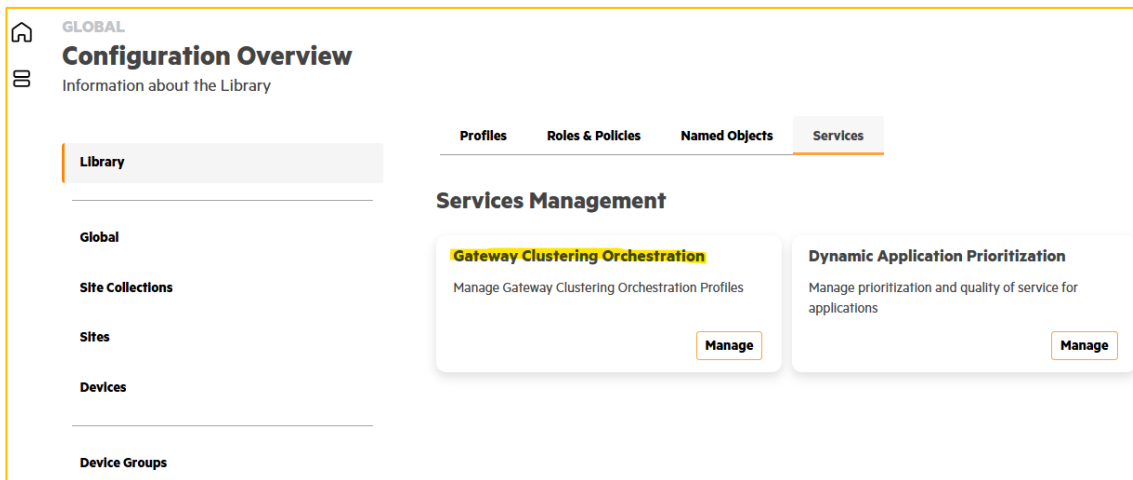
LACP Neighbor Table
-----
Port          Flags  Pri  OperKey  State  Num  Dev Id
-----
GE 0/0/2     SA     1    0xfa    0x3d  0xa  94:60:D5:DA:5A:20
GE 0/0/3     SA     1    0xfa    0x3d  0xb  94:60:D5:DA:5A:20

LACP Internal Table
-----
Port          Flags  Pri  AdminKey  OperKey  State  Num  Status
-----
GE 0/0/2     SA     255  0x1      0x1     0x3d  0x3  up
GE 0/0/3     SA     255  0x1      0x1     0x3d  0x4  up

(Aruba9004_2) #
```

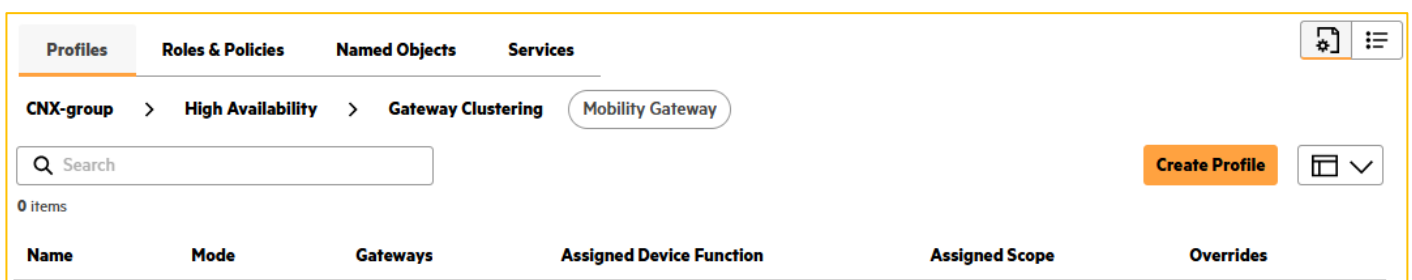
## 4.4 Gateway Clustering

We have auto clustering that should be enabled/available for almost all of Central accounts. One way to see if it is enabled for you is by having "Gateways Clustering Orchestration" card. If you don't see this card, please contact your HPE Networking SE and he can look into it for you.



In the above approach once the profile is created, you need to assign it to global, site collections or sites scope. And when you configure the WLAN profile, you need to select "AUTO-SITE-CLUSTER-MGW" as the gateway cluster. With Auto-site clustering, you can do all this **before any gateways are onboarded**.

But in my case, I must use manual clustering at the device group level. This is because I have SD-Branch gateways in my Classic account and currently the gateway cluster orchestration tile is not available for these accounts. So as shown below I navigate to device group, and the group name is called CNX-group.



**Create Profile**
✕

Create as a local profile

Device Function

Mobility Gateway

Name

Description

Cluster Mode

 Manual
  Automatic

IP Mode\*

 IPv4
  IPv6

Default Gateway Mode

Multicast VLAN

Heartbeat Threshold

 Default
  Custom

**Gateway Clustering** +

Using VRRP IP addresses that match existing custom VRRP profiles will cause those profiles to be deleted.

Name	VRRP IP
Aruba9004_1	-
Aruba9004_2	-

Once it is saved, it gets displayed as shown below.

**Profiles**
Roles & Policies
Named Objects
Services

CNX-group > High Availability > Gateway Clustering > Mobility Gateway

1 item

Name	Mode	Gateways	Assigned Device Function	Assigned Scope	Overrides
MGW_cluster_1	Manual	2	Mobility Gateway	CNX-group	-

At this point, if you want to check the cluster status at the CLI level by using a remote console to the gateways.

**Troubleshoot**

For CNX-branch1

Tests
Remote Console
Commands
Live Monitoring
Support Logs
History

**Sessions**

admin@Aruba9004\_2

SSH session started

**Console**

(Aruba9004\_2) #show lc-cluster group-membership

```
Cluster Enabled, Profile Name = "MGW_cluster_1"
Heartbeat Threshold = 2000 msec
Cluster Info Table
-----
Type IPv4 Address Priority Connection-Type STATUS
-----
peer 192.168.1.241 128 L2-Connected CONNECTED (Member)
self 192.168.1.242 128 N/A CONNECTED (Leader)
(Aruba9004_2) #
```

```
(Aruba9004_1) #show lc-cluster group-membership

Cluster Enabled, Profile Name = "MGW_cluster_1"
Heartbeat Threshold = 2000 msec
Cluster Info Table
-----
Type IPv4 Address Priority Connection-Type STATUS
-----
self 192.168.1.241 128 N/A CONNECTED (Member)
peer 192.168.1.242 128 L2-Connected CONNECTED (Leader)

(Aruba9004_1) #
```

You can also check the cluster status from New Central by navigating to the site >> Network and then clicking on the cluster name, which is in bold, shown below.

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

**Devices**

Status: Online (4) Offline (0) Type: Access Point (1) Gateway (2) Switch (1) Bridge (0)

Search: [ ] Filter: [ ]

4 items

Name	Type	MAC Address	IP Address	Model	Connected To
204c03b6b25b Online - Good Performance	Access Point Standalone	204c03b6b25b	10.10.10.34	AP-505H	6200 Port 1/1/1
6200 Online - Good Performance	Switch Standalone	ec:67:94:d4:79:c0	10.10.10.11 fd14:5f94:8156:...	CX-6200F	-
Aruba9004_1 Online - Good Performance	Gateway Cluster (Member) MGW_cluster_1	204c03820f22	192.168.1.241	A9004	-
Aruba9004_2 Online - Good Performance	Gateway Cluster (Leader) MGW_cluster_1	28:de:65:73:85:96	192.168.1.242	A9004	-

Here you can view the cluster member details and its capacity.

**GATEWAY CLUSTER**  
**MGW\_cluster\_1**  
Information about the cluster.

**Health**  
Online - Good Performance  
Configuration Status: 2 Synchronized, 0 Unsynchronized

**System**  
CPU: Good, Memory: Good, Temperature: Good, Fans: None, Power Supplies: 2 up of 2

**Cluster**  
Member: Aruba9004\_1 (Member, CNX-branch1), Aruba9004\_2 (Leader, CNX-branch1)

**Capacity**  
Last 3 Hours  
Clients: 0%, Devices: 0%

Here you can see the how the tunnel clients are being distributed across your cluster.

**GATEWAY CLUSTER**  
**MGW\_cluster\_1**  
Information about the cluster.

**Gateway Cluster Members List**

Status: Online (2) Offline (0)

Search: [ ] Filter: [ ]

2 items

Name	Role	Access point	Switch	Client	Tunnel	Model	IP Address
Aruba9004_1 Online - Good Perf...	Member	1 Active 0 Standby	0 Active 0 Standby	1 Active 0 Standby	1 GRE, 2 IPsec	A9004	192.168.1.241
Aruba9004_2 Online - Good Perf...	Leader	0 Active 1 Standby	0 Active 0 Standby	0 Active 1 Standby	1 GRE, 2 IPsec	A9004	192.168.1.242

## 4.5 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 Appendix -A

## 5.1 Mobility Gateway Onboarding Console bootup

These are the console bootup logs of a mobility gateway during onboarding.

```
Decompressing Linux... Parsing ELF... done.
Booting the kernel.
[ 0.000000] Command line: BOOT_IMAGE=/uImage0 rdinit=/sbin/init console=tty1 console=ttyS0,9600
acpi_osi=Linux tpm_tis.interrupts=0 quiet
P00
[ 0.081135] irq 27: nobody cared (try booting with the "irqpoll" option)
[ 0.082000] handlers:
[ 0.082000] [<ffffffff81336e50>] intel_gpio_irq
[ 0.082000] Disabling IRQ #27
[06:27:59]:...Starting rcS...

Aruba Networks
ArubaOS Version 8.5.0.0-1.0.7.1 (build 72342 / label #72342)
Built by p4build@pr-hpn-build05 on 2019-09-20 at 15:32:42 UTC (gcc version 4.9.4)
(c) Copyright 2019 Hewlett Packard Enterprise Development LP.

[06:27:59]:Starting device manager [ OK ]

<<<<< Welcome to Aruba Networks - Aruba A9004 >>>>>

[06:28:01]:Probing for real-time clock [ OK ]

<output removed>

[06:28:42]:rcS Done(43 sec)

[06:28:42]:Starting OS services [ OK ]

Starting ztp
Starting ztp auto provision
Starting auto provisioning
Registered for NTP Sync
Initiated DHCP, awaiting DHCP response

Auto-provisioning is in progress. It requires DHCP and Activate servers
Choose one of the following options to override or debug auto-provisioning...
'enable-debug' : Enable auto-provisioning debug logs
'disable-debug' : Disable auto-provisioning debug logs
'mini-setup' : Start mini setup dialog. Provides minimal customization and requires DHCP server
'full-setup' : Start full setup dialog. Provides full customization
'static-activate' : Provides customization for static or PPPOE ip assignment. Uses activate for master
information

Enter Option (partial string is acceptable):

Received DHCP response, My IP = 10.10.30.34, Master = none, Mask = 255.255.255.0, GW = 10.10.30.1, DNS =
192.168.1.131, Country code = none, Physical Port = 0
DNS server name 192.168.1.131 assigned to info structure..
Master info not received, trying activate
curl: (6) Could not resolve host: device.arubanetworks.com
Provisioning Parameters not received from Activate, will retry after 30 seconds
% Total % Received % Xferd Average Speed Time Time Current
% Total % Received % Xferd Average Speed Time Time Current
100 2630 0 0 100 2630 0 1795 0:00:01 0:00:01 --:--:-- 1793
Received Activate response, Central = device-apacsouth.central.arubanetworks.com
Master = auto-discovered from Activate
INFO: Backing up existing config dir.
Valid country code not specified, using default CA
Uplink Port : gigabitethernet 0/0/0
Adding gigabitethernet 0/0/0 as switchport to vlan 4094
Processes will restart now
Restarting profmgr...

<output removed>

[05:45:35]:Waiting for Controller IP [ DONE ]
[05:45:39]:Initializing AAA [ DONE ]
[05:45:39]:Initializing Controller management [ DONE ]

User:

[05:47:57]:Starting rebootme
[05:47:57]:Shutdown processing started
[05:47:59]:Starting database backup
[05:47:59]:Syncing data...
```

```

....
[05:48:03]:done.
[05:48:03]:Shutting down database server
[05:48:06]:kill all process
[05:48:08]:Sending SIGSTP to all processes, except init process
[05:48:08]:Sending SIGKILL to all processes, except init process
[05:48:08]:kill all process again
[05:48:09]:Rebooting ...
The system is going down NOW !!
Sending SIGTERM to all processes.
Sending SIGKILL to all processes.
Please stand by while rebooting the system.
[ 403.251675] reboot: Restarting system

Aruba Networks

Use the ^ and v keys to select which entry is highlighted.
The highlighted entry will be executed automatically in 0s.
Booting `RAICILLA-AOS-P0'

Booting from storage
Loading Kernel...
Signer Cert OK .
Policy Cert OK.
RSA Signature verified using SHA256 Message Digest.
Aruba Image found
ARUBA Img Size:0xa1d35e0
CPLD_GRUB_GOOD:0x0
New CPLD_GRUB_GOOD:0x1
early console in extract kernel
input_data: 0x0000000012e1a411
input_len: 0x000000000a1c3b88
output: 0x00000000f000000
output_len: 0x00000000db8aa48
kernel_total_size: 0x00000000e026000
needed_size: 0x00000000e200000
trampoline_32bit: 0x000000000086000

Decompressing Linux... Parsing ELF... done.
Booting the kernel.
[ 0.000000] Command line: BOOT_IMAGE=/uImage0 rdinit=/sbin/init console=tty1 console=ttyS0,9600
acpi_osi=Linux tpm_tis.interrupts=0 quiet
P00
P00
[ 0.368756] irq 27: nobody cared (try booting with the "irqpoll" option)
[ 0.369705] handlers:
[ 0.369705] [<00000000ecf1ea5c>] intel_gpio_irq
[ 0.369705] Disabling IRQ #27
[ 1.354311] platform testcase-data:testcase-device2: IRQ index 0 not found
[06:35:58]:...Starting rcS...

HPE Aruba Networking
AOS-10 Version 10.7.2.5 SSR (build 95489 / label #95489)
Built by jenkins@ae31184c5917 on 2026-04-03 at 19:36:59 UTC (gcc version 10.3.0)
(c) Copyright 2026 Hewlett Packard Enterprise Development LP.

[06:35:58]:Starting device manager [ OK ]

<<<<< Welcome to HPE Aruba Networking - Aruba A9004 >>>>>
[06:36:00]:Probing for real-time clock [ OK ]

<output removed>

[06:36:11]:Grub is Upgraded to Latest... [ OK ]

#####
#####
##### BIOS upgrade will reboot the Board 3 times #####
##### Complete process will take approx. 15 minute #####
##### Don't interrupt the Board Power until Upgrade Process completed #####
##### Current BIOS Version:9004.0015 #####
##### New BIOS Version:9004.0026 #####
#####
#####

Rebooting the board for bios upgrade...
[06:36:17]:Starting rebootme

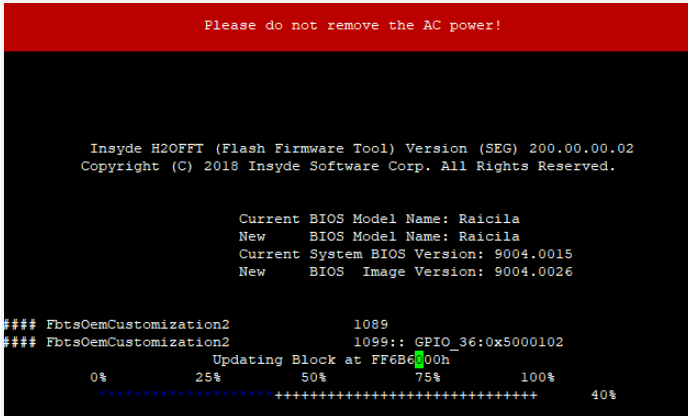
[06:36:17]:Starting database backup
[06:36:17]:Shutdown processing started
[06:36:17]:Syncing data...
sh: you need to specify whom to kill
[06:36:17]:Killing ofa

```

```

[06:36:17]:done.
[06:36:17]:Shutting down database server
[06:36:17]:kill all processes
[06:36:17]:Sending SIGSTP to all processes, except init and pgsq processes
[06:36:17]:Sending SIGKILL to all processes, except init and pgsq processes
[06:36:17]:kill all processes again
[06:36:18]:Rebooting ...
Requesting system reboot
[ 22.484234] reboot: Restarting system
[ 22.531202] reboot: Disabling all VMX...
[ 22.579793] reboot: (reboot_mode:0, reboot_type:97)
[ 22.639846] reboot: ACPI Reset is triggering.

```



```

Aruba Networks
Configuring GPIO for Raicilla 9004
POST CODE: 000000C2

```

<output removed>

```

Checking BIOS code integrity...
BIOS code integrity check Passed !!!

```

<output removed>

```

Decompressing Linux... Parsing ELF... done.
Booting the kernel.
[ 0.000000] Command line: BOOT IMAGE=/uImage0 rdinit=/sbin/init console=tty1 console=ttyS0,9600
acpi_osi=Linux tpm tis.interrupts=0 quiet processor.max_cstate=1 intel_idle.max_cstate=0 idle=poll
intel_pstate=disable intel_iommu=on iommu=pt
P00
[ 0.474081] irq 27: nobody cared (try booting with the "irqpoll" option)
[ 0.475034] handlers:
[ 0.475034] [<00000000776f0ddd>] intel gpio irq
[ 0.475034] Disabling IRQ #27
[ 1.282977] platform testcase-data:testcase-device2: IRQ index 0 not found
[06:44:26]:...Starting rcS...

```

```

HPE Aruba Networking
AOS-10 Version 10.7.2.5 SSR (build 95489 / label #95489)
Built by jenkins@ae31184c5917 on 2026-04-03 at 19:36:59 UTC (gcc version 10.3.0)
(c) Copyright 2026 Hewlett Packard Enterprise Development LP.

```

```

[06:44:26]:Starting device manager [ OK ]
<<<<< Welcome to HPE Aruba Networking - Aruba A9004 >>>>>
[06:44:28]:Probing for real-time clock [ OK ]

```

<output removed>

```

[06:45:56]:Initializing CFGM [ DONE ]
[06:45:56]:Waiting for Controller IP [ DONE ]
[06:46:00]:Initializing AAA [ DONE ]
[06:46:00]:Initializing Controller management [ DONE ]
In process of syncing configuration with Central. User login configured from Central will be enabled after
the sync. It may take some time.

```

User:

## 5.2 Gateway Reset Procedure

Sometimes you may need to reset a gateway and bring it back into New Central cleanly. The process below walks through the steps I use.

- Disconnect the gateway and wait until it shows as offline in New Central.

- Go to the site, open the Network view, and delete the gateway from there.
- In Classic Central, delete the gateway from the Global > Device > Gateway list.
  - At this point, the gateway should no longer appear under device configuration in New Central.
  - It should also be removed from the site and from the pre-provisioning group.
- Add the gateway back to the CNX-branch1 pre-provisioning group.
- Assign the gateway to the appropriate site.
  - Once this is done, the gateway should appear again under device configuration in New Central.
- If you have console access, you can reset the gateway by running the write erase all command. Alternatively, press and hold the reset button on the front of the 9004 gateways for about 5 to 10 seconds.