1 Table of Contents

1.1 Revision History

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

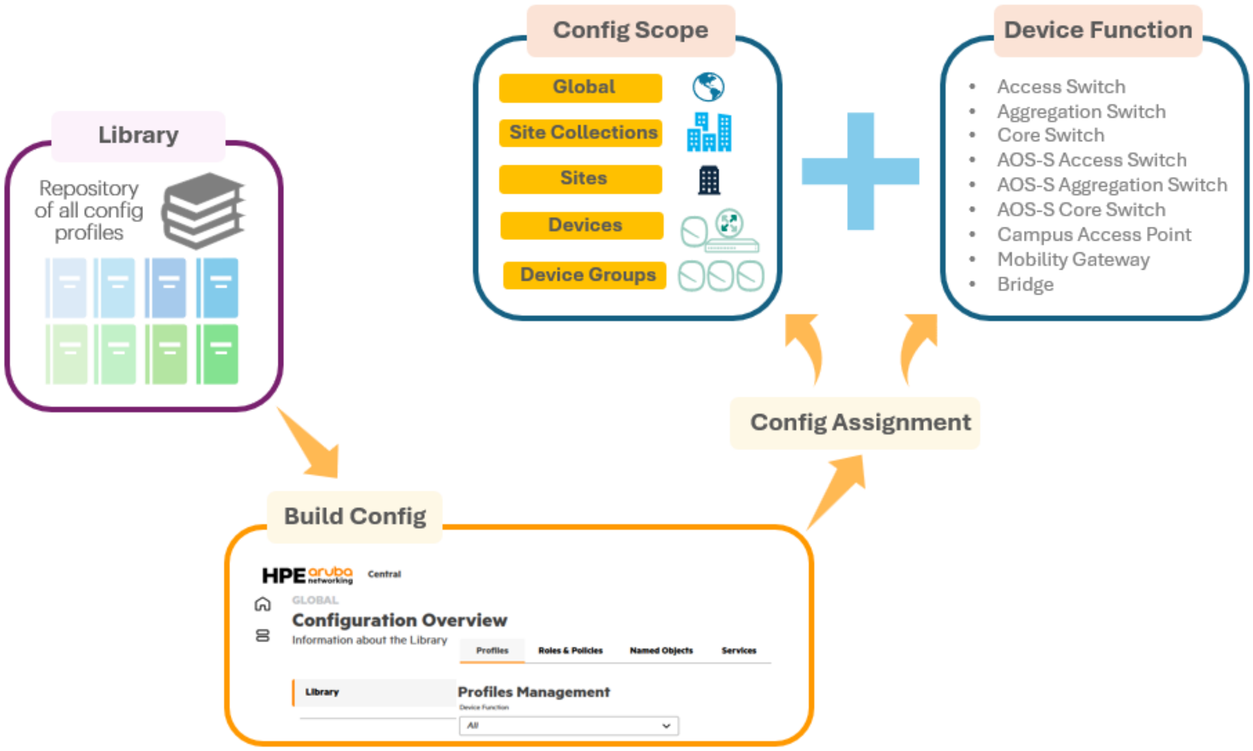
2 New Central Configuration for AOS10 Access Points - Bridge Mode

With the general availability of New Central, it is essential to understand one of its principal features: **The Hierarchical Configuration Model**. HPE Aruba Networking Central employs this model to streamline full stack network management across distributed locations. Administrators are able to develop reusable templates and policies, which minimise administrative burden, ensure uniformity, and support extensive deployments.

The hierarchical configuration model uses a top-down, multi-level structure to manage network infrastructure efficiently. It allows sharing configuration components across the network, with granular overrides permitted at lower levels for specific sites or devices, improving scalability and consistency.

Then there is “Library” as your go-to folder for handy config notes. It’s not a config level, but a central spot to store and reuse settings. This keeps things consistent and makes life easier, as you’re less likely to make mistakes.

This document continues from the previous technote, where I discussed the automatic migration of Instant AP to AOS10 and obtaining the new AOS10 configuration from Classic Central. This technote includes details of New Central configuration using various profiles needed for the configuration of AOS10 WLANs **operating in Bridge mode**.



Here we will walk through setting up a WLAN that uses 802.1x authentication with an external authentication server. I won’t dive into the details of configuring ClearPass here and assume it’s already set up and working as expected because the main thing we’re focusing on is how to get things up and running in New Central.

2.1 Things you need

- APs running AOS10 firmware version (I am using 10.7.1.1)
- Valid HPE Aruba Central account and subscriptions
- ClearPass that is already configured as external authentication server.

3 Hierarchy Scopes and Device Function

New Central uses a new hierarchical configuration model in HPE Aruba Networking Central allows administrators to create reusable configuration objects and policies that can be applied across multiple sites or groups of devices. This approach reduces administrative overhead, ensures consistency, and makes it easier to deploy and manage large-scale networks.

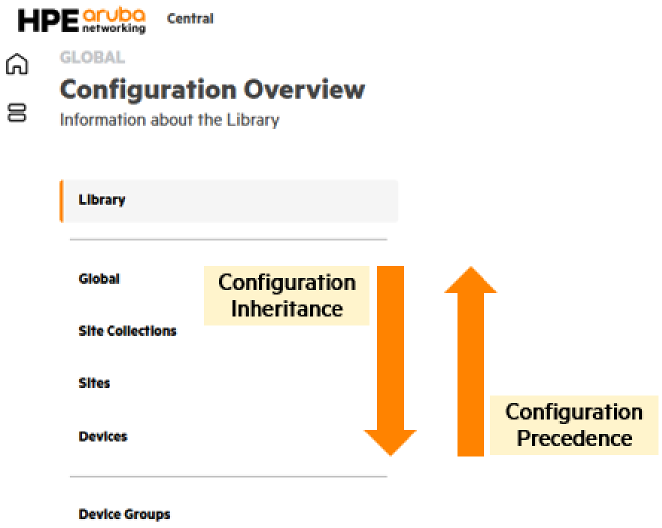
It provides 4x levels of configuration (Global, Site collections, Sites and Devices) where you can perform the configuration which gets inherited by the rest of hierarchy. So for example if you configure at the global level, the configuration will flow down to Site Collection and then to Sites and then to Devices.

Although global configurations apply universally, they can be overridden at the site collection, site, or device level to accommodate specific requirements. For example, a global authentication server group might use be used for WLAN authentication while a specific site may require a different server group for the same WLAN. And that will take precedence over the global configuration and so on.

The Global level includes all sites within the organisation and we can only have one Global level per organisation.

For Site Collection, think of it as a group of sites bundled together for easier management. Instead of configuring each site individually, you can set up certain configuration objects once and apply them across all the sites in that collection. It's a handy way to ensure multiple locations share the same settings, without having to repeat yourself for every single site.

Picture a site as the place where you set up and manage settings unique to that location. Some things like High Availability (HA) profiles for switches and gateways (including VSF, VSX, and clusters) can only be configured at the site level. These profiles are tailored specifically for each site, so you need to create and apply them right there. Also, every network setup must include at least one site it's not optional.



There is a noteworthy configuration tier known as Device Groups, which differs from those found in Classic Central. This feature enables the targeted distribution of configurations to specific devices at selected sites, rather than applying settings universally across all devices within a location. For instance, a Guest SSID may be designated only for access points situated in reception areas and meeting rooms at each site, while being excluded from corporate office spaces. Device groups are an optional component.

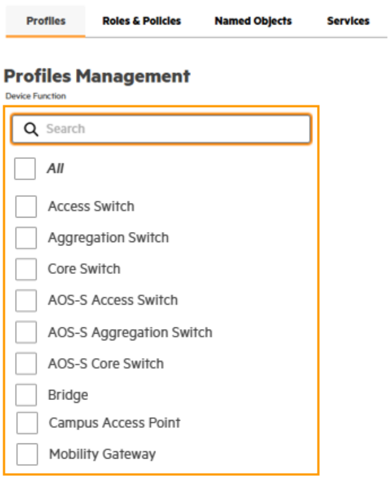
Lastly, there's the "Library", not a configuration level, but a central repository for reusable configuration objects and settings. Engineers often keep a folder containing various configuration notes tailored to specific setups or solutions. The Library works like this folder, enabling storage and reuse of common configurations across multiple devices, sites, or networks. This approach is highly beneficial, as it helps maintain consistent configurations, streamline deployment, and enhances security by reducing manual errors.

3.1 Device Function

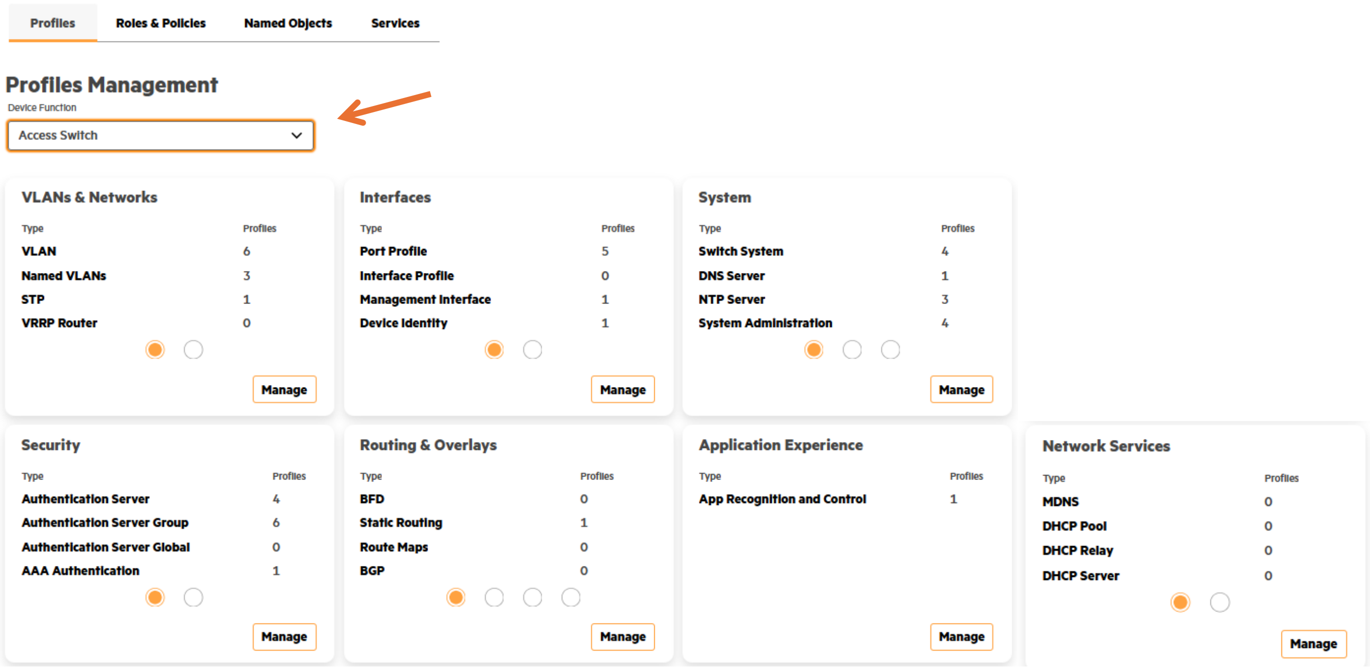
This is yet another innovating approach added to the configuration to help to ensure that the configuration is specific for various device function or personas.

Device functions enable administrators to control the assignment of profiles based on a device's role in the network. For example, an authentication profile might be applied only to access switches and not to core and aggregation switches.

Here you can see the available device functions, including specific set of personas for AOS-S switches. There will be other personas added to the list as other device types are supported under the new central configuration.



The nice thing about Device functions is that by choosing a specific type, you can view the configuration objects that are relevant to that device functions. For example here I have selected Access Switch.



Profiles Management

Device Function: Access Switch

VLANs & Networks

Type	Profiles
VLAN	6
Named VLANs	3
STP	1
VRRP Router	0

Interfaces

Type	Profiles
Port Profile	5
Interface Profile	0
Management Interface	1
Device Identity	1

System

Type	Profiles
Switch System	4
DNS Server	1
NTP Server	3
System Administration	4

Security

Type	Profiles
Authentication Server	4
Authentication Server Group	6
Authentication Server Global	0
AAA Authentication	1

Routing & Overlays

Type	Profiles
BFD	0
Static Routing	1
Route Maps	0
BGP	0

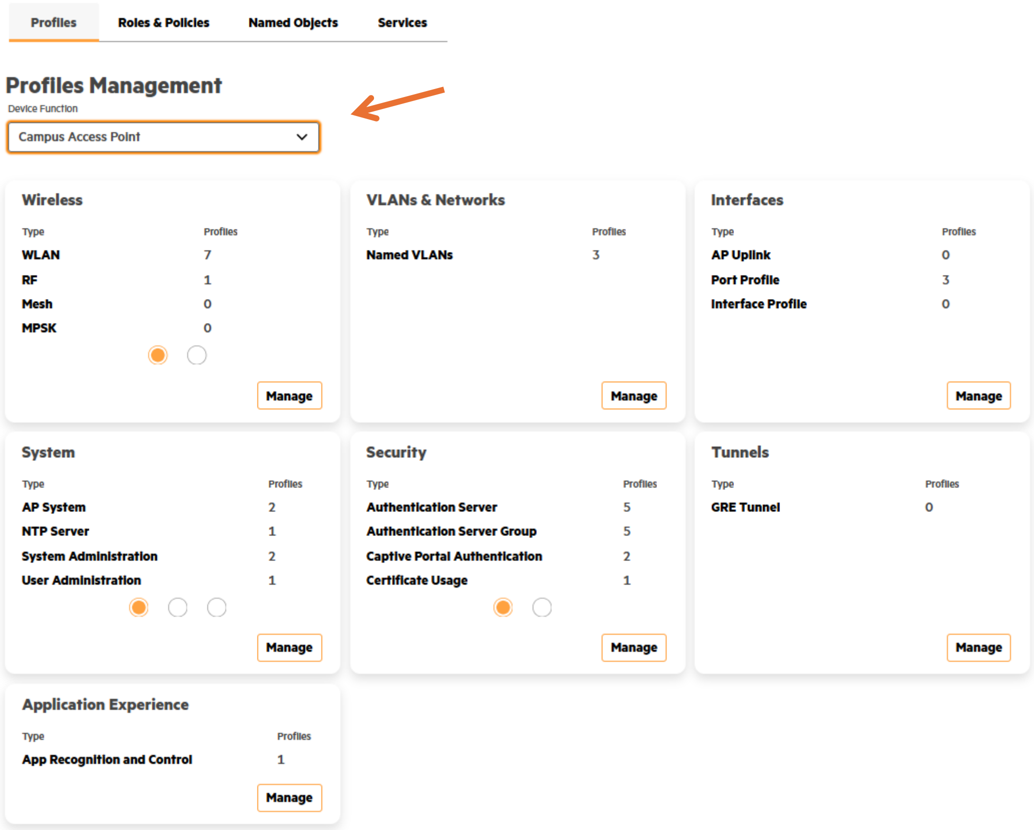
Application Experience

Type	Profiles
App Recognition and Control	1

Network Services

Type	Profiles
MDNS	0
DHCP Pool	0
DHCP Relay	0
DHCP Server	0

As compared to Campus AP seen below.



Profiles Management

Device Function: Campus Access Point

Wireless

Type	Profiles
WLAN	7
RF	1
Mesh	0
MPSK	0

VLANs & Networks

Type	Profiles
Named VLANs	3

Interfaces

Type	Profiles
AP Uplink	0
Port Profile	3
Interface Profile	0

System

Type	Profiles
AP System	2
NTP Server	1
System Administration	2
User Administration	1

Security

Type	Profiles
Authentication Server	5
Authentication Server Group	5
Captive Portal Authentication	2
Certificate Usage	1

Tunnels

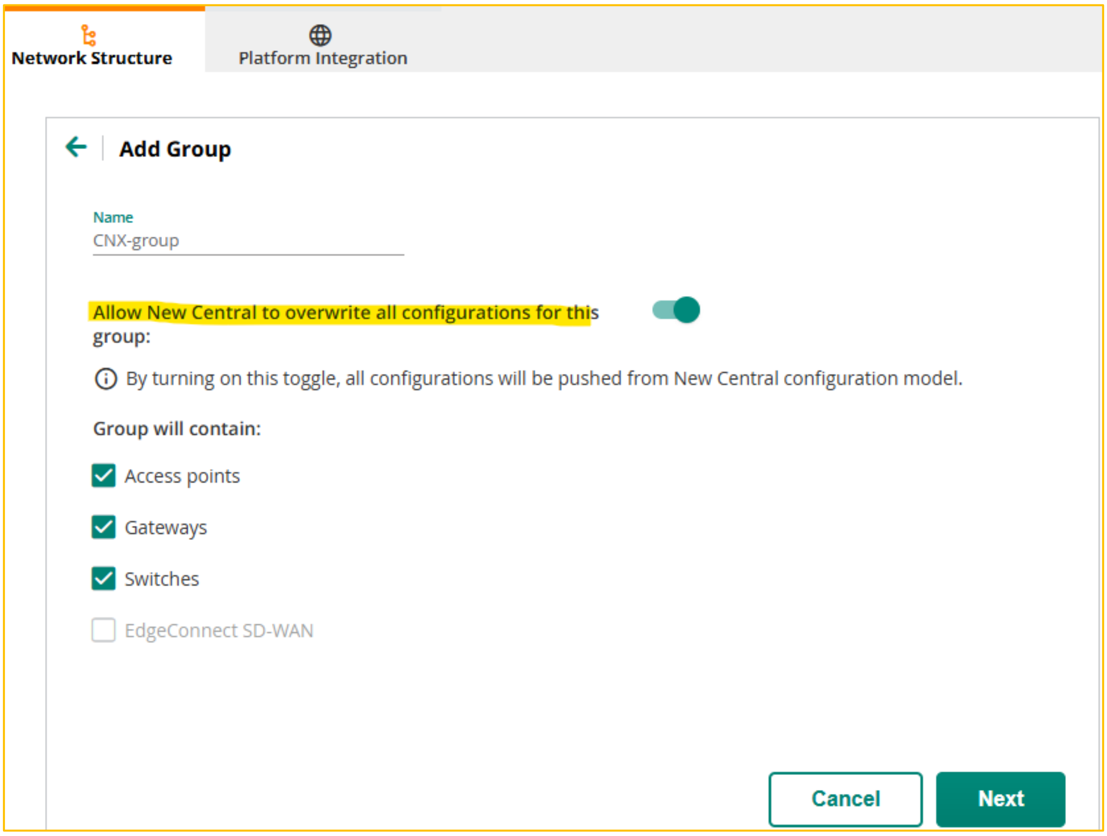
Type	Profiles
GRE Tunnel	0

Application Experience

Type	Profiles
App Recognition and Control	1

4 AOS10 AP Configuration

Now that we have explained the different hierarchical configuration scopes and device functions, we can proceed with configuring AOS 10 AP. However, before you begin with the New Central configuration, 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 switched on, 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.



Add Group

Name: CNX-group

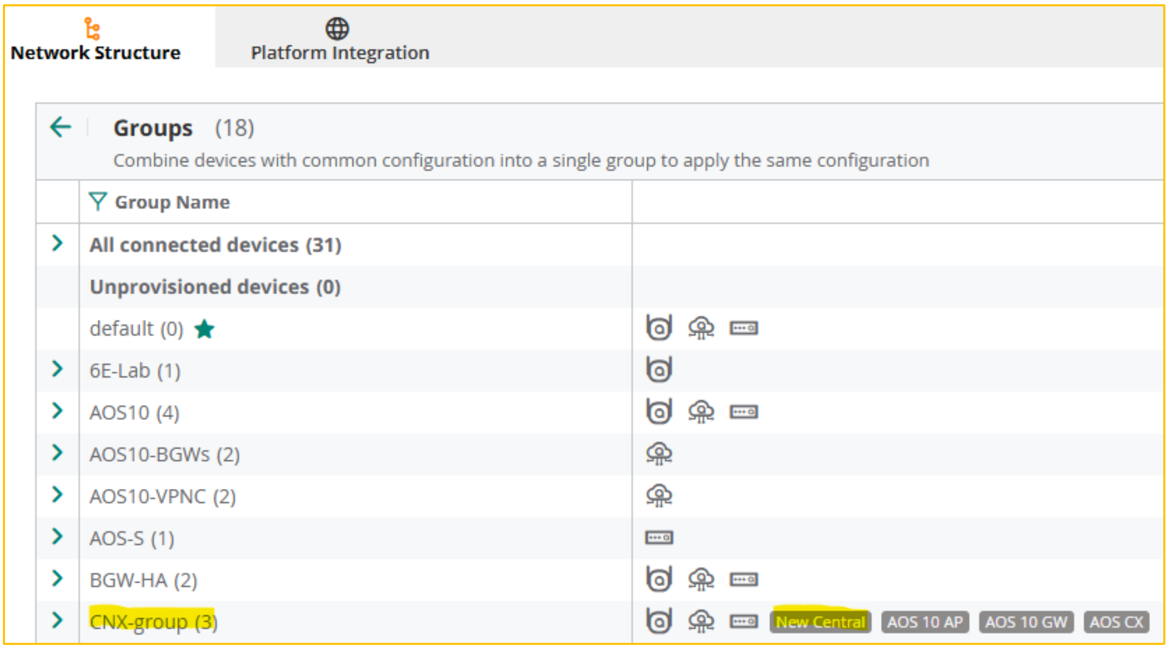
Allow New Central to overwrite all configurations for this group: ●

ⓘ By turning on this toggle, all configurations will be pushed from New Central configuration model.

Group will contain:

- ☑ Access points
- ☑ Gateways
- ☑ Switches
- □ EdgeConnect SD-WAN

And once created it should be displayed as shown below.

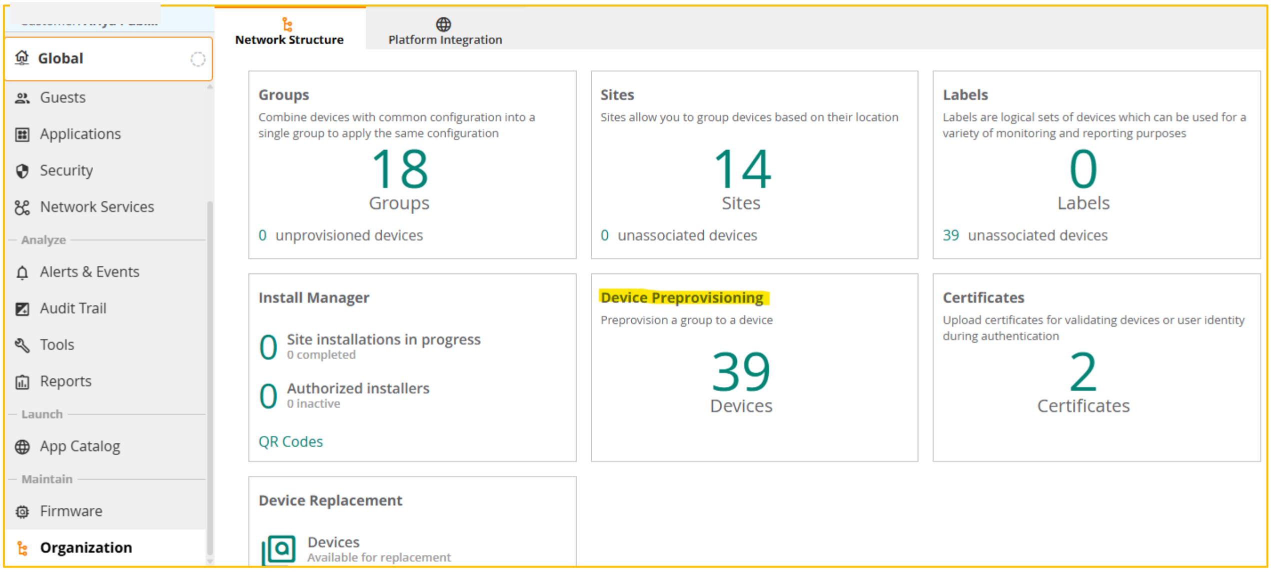


Groups (18)

Combine devices with common configuration into a single group to apply the same configuration

Group Name	
All connected devices (31)	
Unprovisioned devices (0)	
default (0) ★	
6E-Lab (1)	
AOS10 (4)	
AOS10-BGWs (2)	
AOS10-VPNC (2)	
AOS-S (1)	
BGW-HA (2)	
CNX-group (3)	New Central AOS 10 AP AOS 10 GW AOS CX

The devices should be moved to a Site which is mandatory for New central configuration. This was covered in my previous technote. Lastly you can move your APs via Device Preprovisioning to the group that you have just enabled it for New Central configuration.



Global
Guests
Applications
Security
Network Services
Analyze
Alerts & Events
Audit Trail
Tools
Reports
Launch
App Catalog
Maintain
Firmware
Organization

Network Structure
Platform Integration

Groups
Combine devices with common configuration into a single group to apply the same configuration
18
Groups
0 unprovisioned devices

Sites
Sites allow you to group devices based on their location
14
Sites
0 unassociated devices

Labels
Labels are logical sets of devices which can be used for a variety of monitoring and reporting purposes
0
Labels
39 unassociated devices

Install Manager
0 Site installations in progress
0 completed
0 Authorized installers
0 inactive
QR Codes

Device Preprovisioning
Preprovision a group to a device
39
Devices

Certificates
Upload certificates for validating devices or user identity during authentication
2
Certificates

Device Replacement
Devices
Available for replacement

4.1 Profile Categories and Configuration Checklist

AOS10 AP 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 various configuration profile categories that are available for Campus AP.

Categories	Subcategories	**Categories**	Subcategories
Wireless	WLAN RF Mesh MPSK Passpoint RTLS Wireless IDS/IPS	**Security**	Authentication Server Authentication Server Group Captive Portal Authentication Certificate Usage EST Passpoint Identity Provider
VLAN & Network	Named VLANs	**Tunnels**	GRE Tunnel
Interfaces	AP Uplink Port Profile Interface Profile	**Application Experience**	App Recognition and Control
System	AP System NTP Server System Administration User Administration Intelligent Power Management (IPM) Syslog Server Dump Server Dynamic DNS Proxy SNMP Time Range		

This is my checklist for pre-staging AOS10 AP configuration

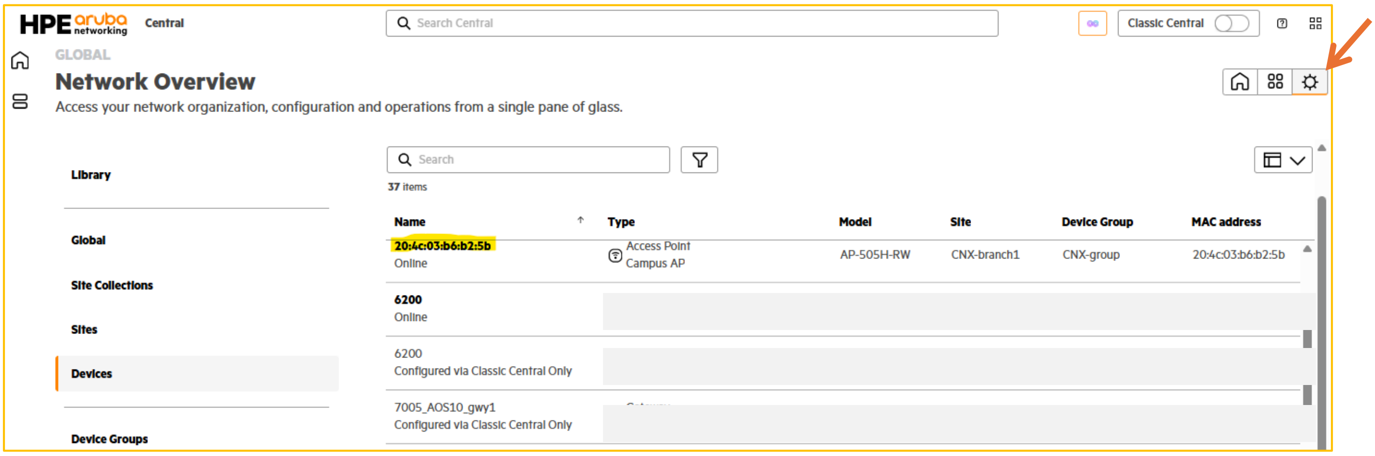
1. Ensure the newly factory defaulted AP is displayed under device configuration
2. Configure administrator password
3. AP System Profile and scope
4. NTP Profile
5. IPM Profile
6. RF Profile (if required)
7. Rename AP (if required)
8. AAA Authentication Profile
9. User Roles
10. WLAN Profile
11. Named VLAN Profile (if required)
12. AP Uplink Port Profile (if required)

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

- 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; opt for underscores or hyphens instead.
- As always it is recommended for APs to use DHCP for management.

4.2 Validating New AP

Before we start the configuration, I just want to check that the newly factory defaulted AP is listed and displayed in bold which means that it is in a group that can be configured by New Central.



GLOBAL

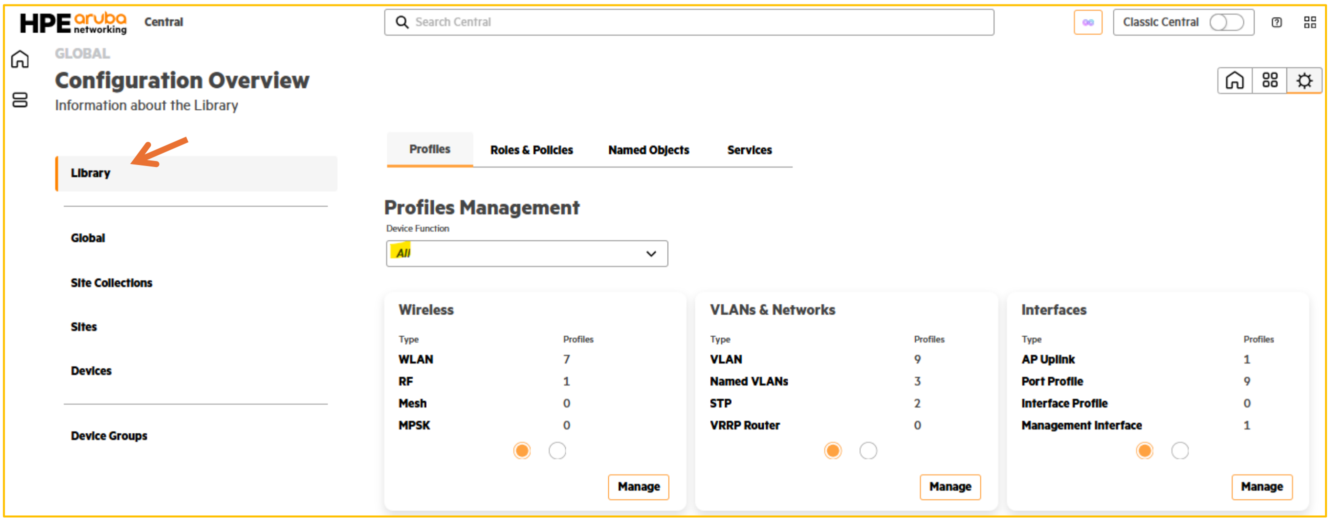
Network Overview

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

37 items

Name	Type	Model	Site	Device Group	MAC address
20:4c:03:b6:b2:5b Online	Access Point Campus AP	AP-505H-RW	CNX-branch1	CNX-group	20:4c:03:b6:b2:5b
6200 Online					
6200 Configured via Classic Central Only					
7005_AOS10_gwy1 Configured via Classic Central Only					

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



GLOBAL

Configuration Overview

Information about the Library

Profiles Management

Device Function: All

Wireless

Type	Profiles
WLAN	7
RF	1
Mesh	0
MPSK	0

VLANs & Networks

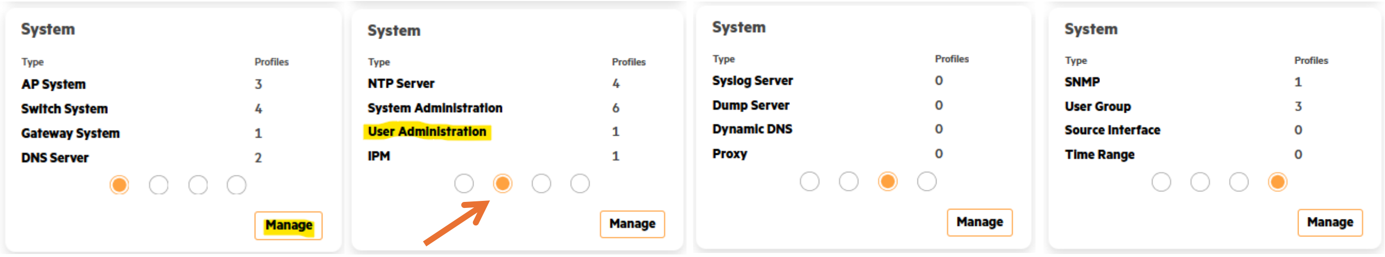
Type	Profiles
VLAN	9
Named VLANs	3
STP	2
VRRP Router	0

Interfaces

Type	Profiles
AP Uplink	1
Port Profile	9
Interface Profile	0
Management Interface	1

4.3 Administrator Password

I'll start with the system card and choose User 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.



System

Type	Profiles
AP System	3
Switch System	4
Gateway System	1
DNS Server	2

● ○ ○ ○

System

Type	Profiles
NTP Server	4
System Administration	6
User Administration	1
IPM	1

○ ● ○ ○

System

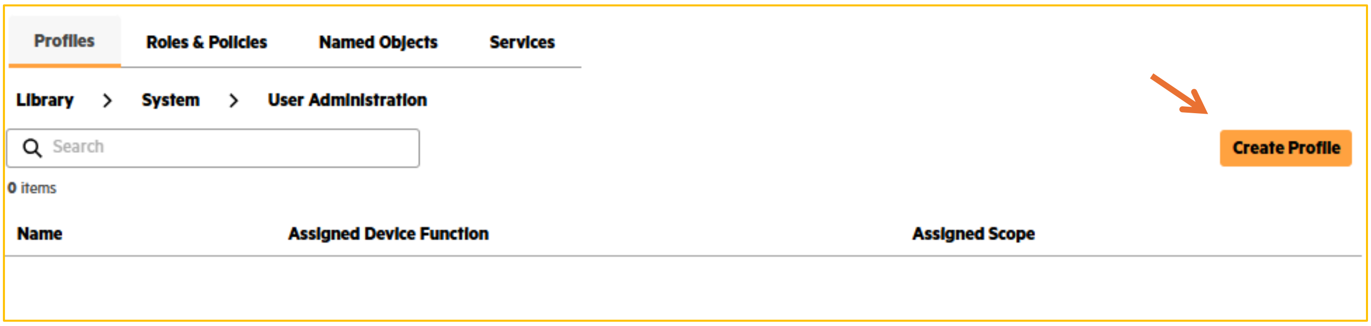
Type	Profiles
Syslog Server	0
Dump Server	0
Dynamic DNS	0
Proxy	0

○ ○ ● ○

System

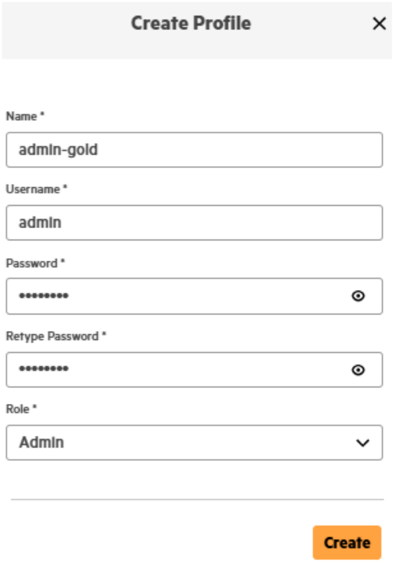
Type	Profiles
SNMP	1
User Group	3
Source Interface	0
Time Range	0

○ ○ ○ ●



0 items

Name	Assigned Device Function	Assigned Scope



Create Profile

Name * admin-gold

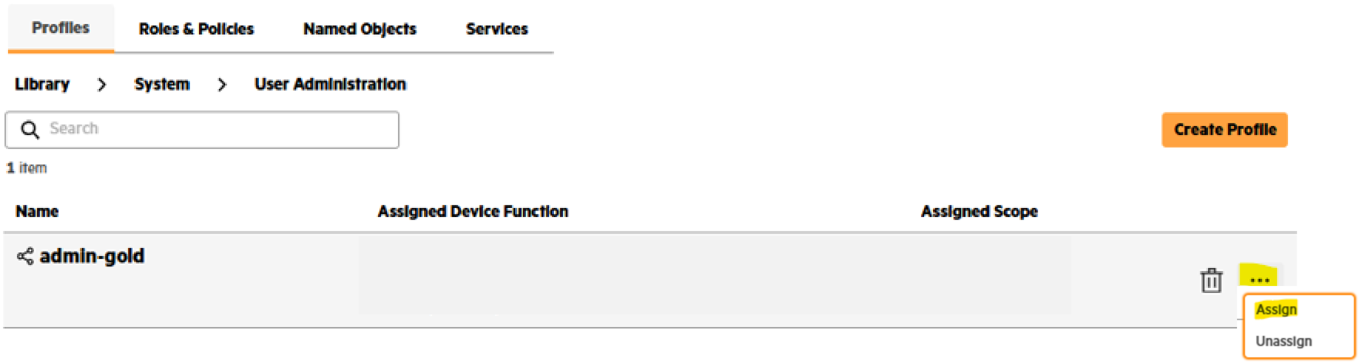
Username * admin

Password * ••••••••

Retype Password * ••••••••

Role * Admin

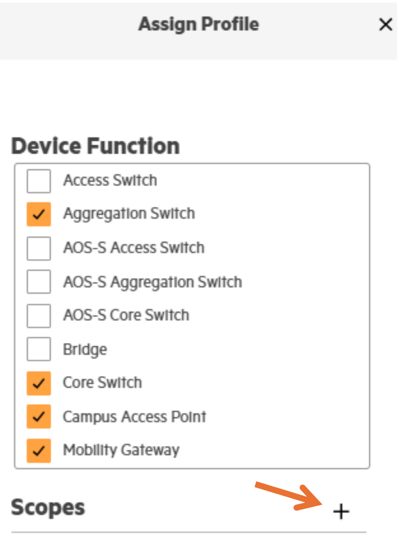
Once this is created it will be listed as shown below. The important thing to note is that it is not yet assigned to any device type and to any scope. In this state the configuration has no scope and not been applied to the AP. It's just sitting in the library.



1 item

Name	Assigned Device Function	Assigned Scope
admin-gold		

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. But based on your policies, you can assign it to a site or site collections as well.

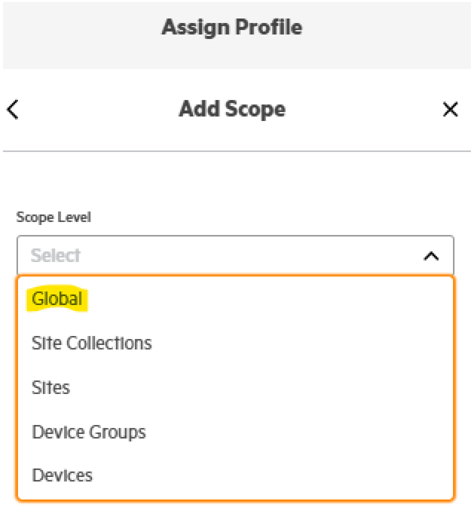


Assign Profile ✕

Device Function

- ☐ Access Switch
- ☑ Aggregation Switch
- ☐ AOS-S Access Switch
- ☐ AOS-S Aggregation Switch
- ☐ AOS-S Core Switch
- ☐ Bridge
- ☑ Core Switch
- ☑ Campus Access Point
- ☑ Mobility Gateway

Scopes +



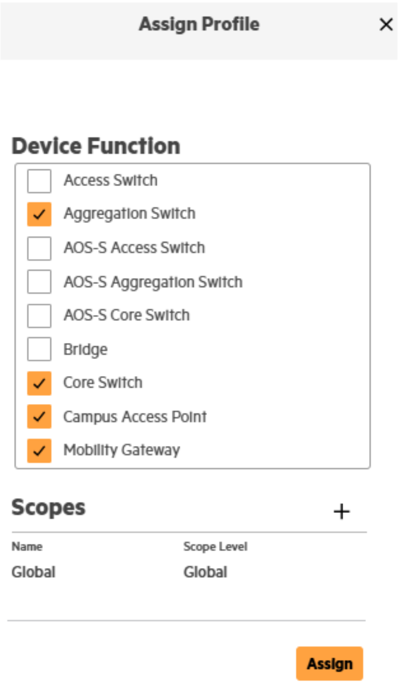
Assign Profile

‹ Add Scope ✕

Scope Level

Select

- Global
- Site Collections
- Sites
- Device Groups
- Devices



Assign Profile ✕

Device Function

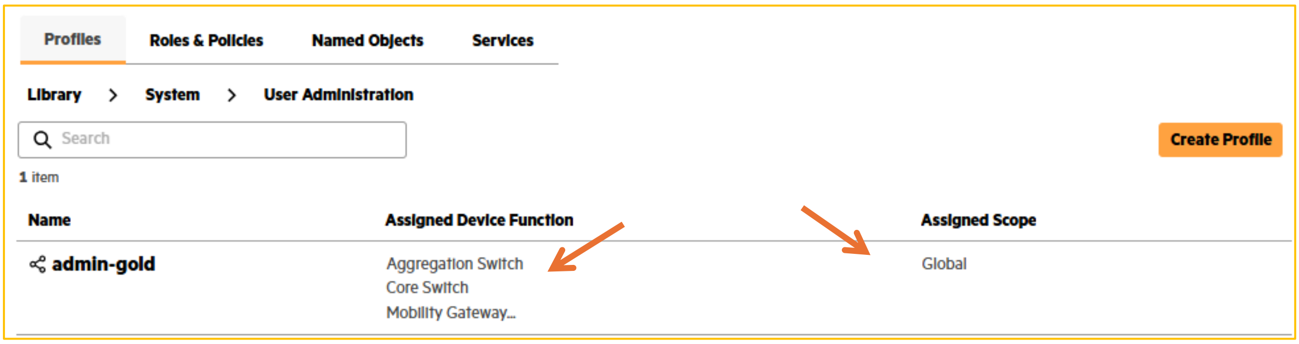
- ☐ Access Switch
- ☑ Aggregation Switch
- ☐ AOS-S Access Switch
- ☐ AOS-S Aggregation Switch
- ☐ AOS-S Core Switch
- ☐ Bridge
- ☑ Core Switch
- ☑ Campus Access Point
- ☑ Mobility Gateway

Scopes +

Name	Scope Level
Global	Global

Assign

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



Profiles | Roles & Policies | Named Objects | Services

Library > System > User Administration

Search

Create Profile

1 item

Name	Assigned Device Function	Assigned Scope
admin-gold	Aggregation Switch Core Switch Mobility Gateway...	Global

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

4.4 AP System Profile

This is a must have profile as it sets country code, time zone, and other custom parameters for the AP. One cool thing is that if your sites have been configured with real addresses then the time zone and country code parameters are automatically set based on the site's location that the AP is in.

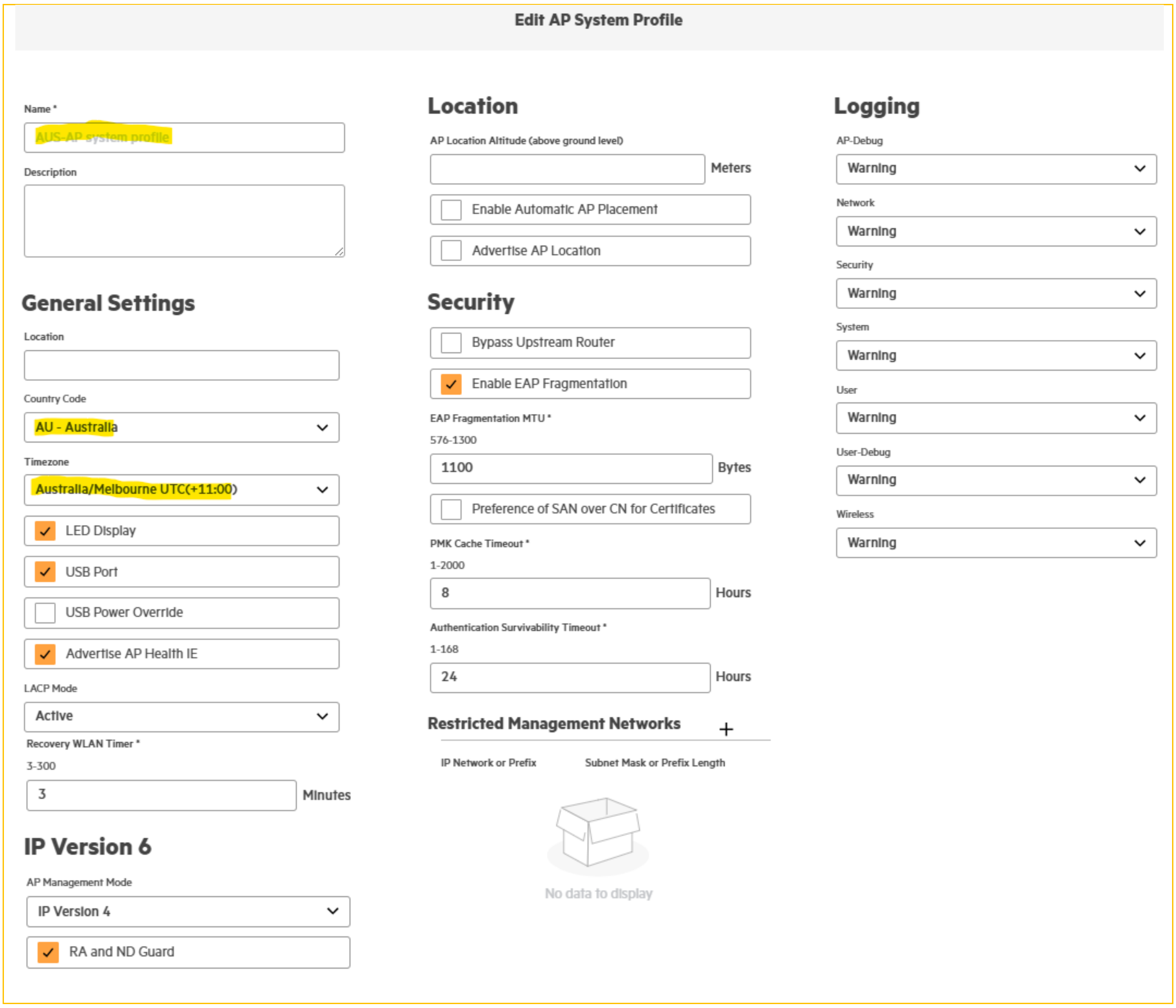
But since I am not using read addresses for my sites then I need to set it. And I have just added the country code and time zone, the rest of left as default. Of course you can change the other setting too. Here I am just configuring the minimum configuration.

You should also know that New Central supports Auto-Locate feature with “Enable Automatic AP Placement” checkbox. This uses Open Location initiative. It is also known by a number of names like IEEE 802.11MC , or Fine Time Measurement (FTM). The main concept is supporting automatic placement of an AP on the floorplan. FTM aids AP to calculate the distance between them using rounded prime. I’ll be covering this feature in upcoming technotes.

Be aware of is “Enable EAP Fragmentation” feature that is enabled by default which ensures reliable 802.1X authentication (especially EAP-TLS) by breaking large certificate chains into smaller, manageable packets.

Also in the system profile is where you can also configure your

- logging levels
- LACP mode (default is Active)
- IPv6 dual stack
- Restricted management access to the AP



Edit AP System Profile

Name *
AUS-AP system profile

Description

General Settings

Location

Country Code
AU - Australia

Timezone
Australia/Melbourne UTC(+11:00)

☑ LED Display

☑ USB Port

□ USB Power Override

☑ Advertise AP Health IE

LACP Mode
Active

Recovery WLAN Timer *
3-300
3 Minutes

IP Version 6

AP Management Mode
IP Version 4

☑ RA and ND Guard

Location

AP Location Altitude (above ground level)
Meters

□ Enable Automatic AP Placement

□ Advertise AP Location

Security

□ Bypass Upstream Router

☑ Enable EAP Fragmentation

EAP Fragmentation MTU *
576-1300
1100 Bytes

□ Preference of SAN over CN for Certificates

PMK Cache Timeout *
1-2000
8 Hours

Authentication Survivability Timeout *
1-168
24 Hours

Restricted Management Networks +

IP Network or Prefix	Subnet Mask or Prefix Length

No data to display

Logging

AP-Debug
Warning

Network
Warning

Security
Warning

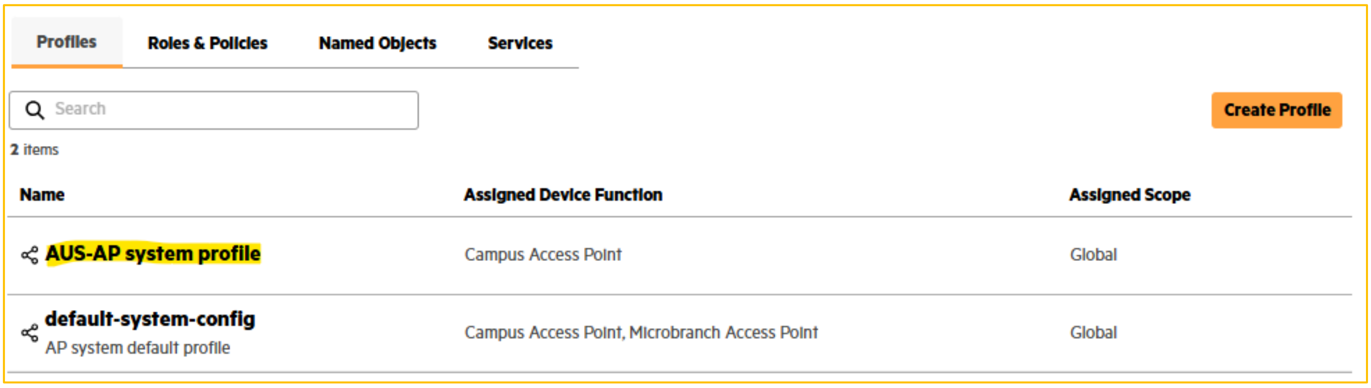
System
Warning

User
Warning

User-Debug
Warning

Wireless
Warning

And as before you need to perform the assignment too. I have assigned to Campus AP and global. But you can also assign it to Sites and Site Collections.

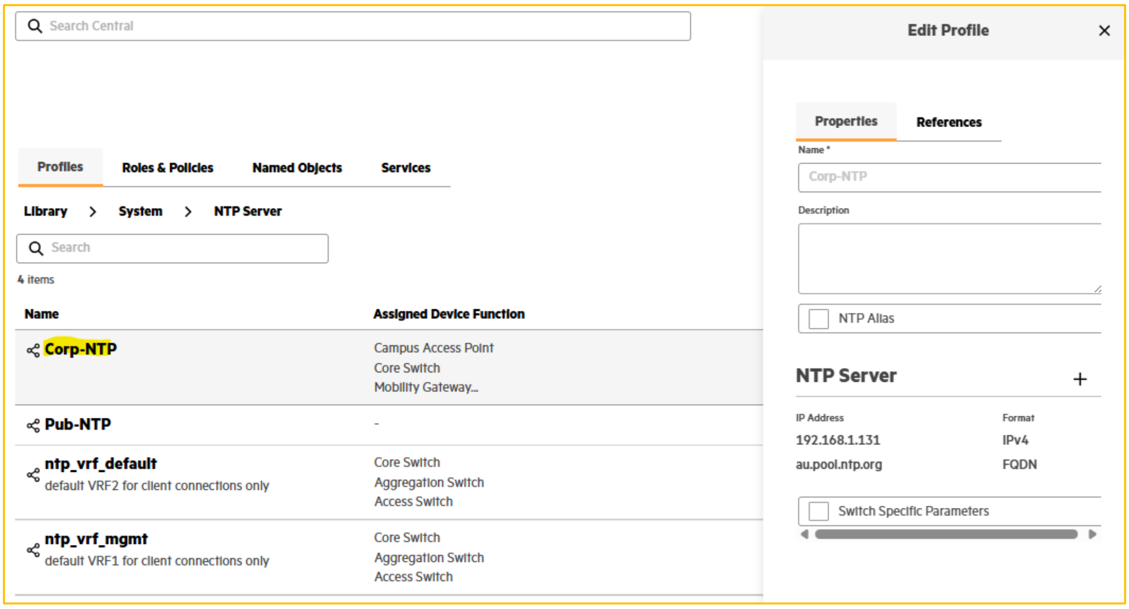


2 items

Name	Assigned Device Function	Assigned Scope
AUS-AP system profile	Campus Access Point	Global
default-system-config AP system default profile	Campus Access Point, Microbranch Access Point	Global

4.5 NTP Profile

Next on my checklist is setting the NTP profile. I have configured one called Corp-NTP. Again all these common network objects like NTP can be assigned to all your device functions. Here 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 organization's configuration standards.



4 items

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

Name *: Corp-NTP

Description:

□ NTP Alias

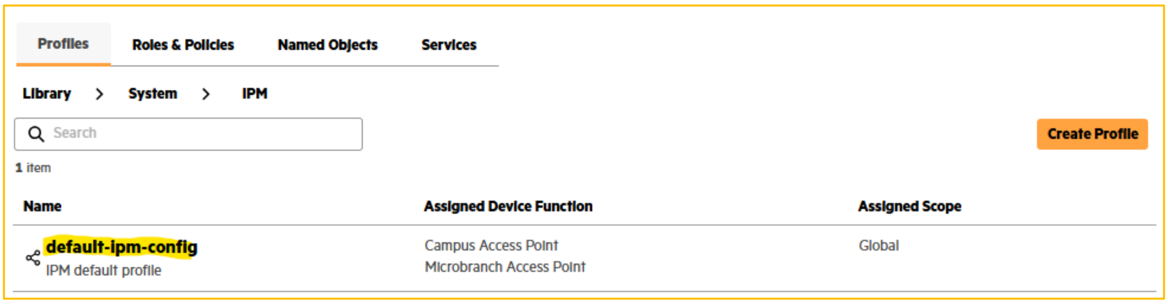
NTP Server +

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

□ Switch Specific Parameters

4.6 Intelligent Power Management

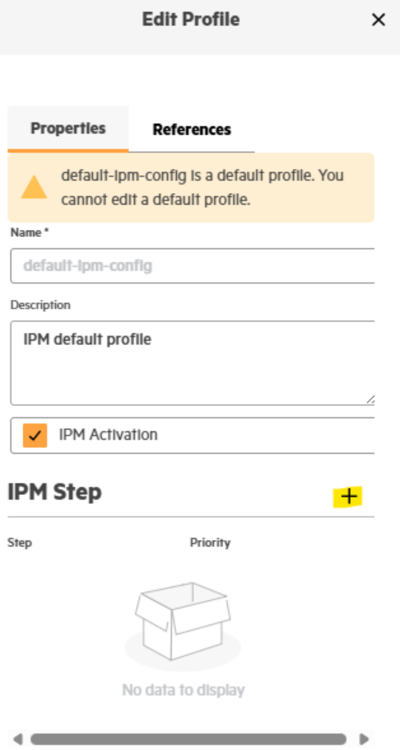
This is a system generated default profile that enables IPM.



1 item

Name	Assigned Device Function	Assigned Scope
default-ipm-config IPM default profile	Campus Access Point Microbranch Access Point	Global

You cannot modify any default profiles. You need to create a new one if you need to change it. Here are the options for setting IPM. Here I am using the default IPM profile.



default-ipm-config is a default profile. You cannot edit a default profile.

Name *: default-ipm-config

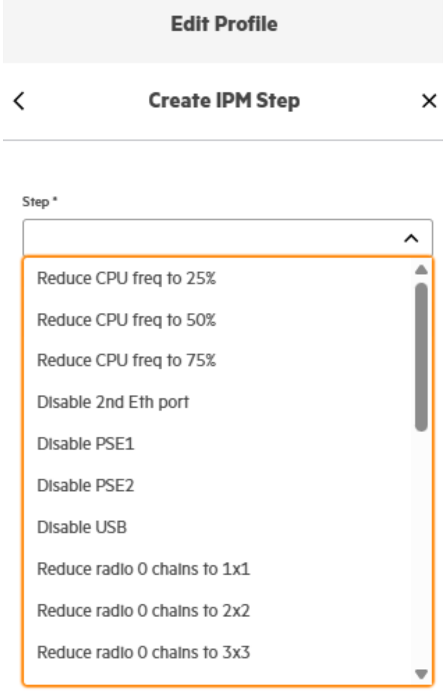
Description: IPM default profile

☑ IPM Activation

IPM Step +

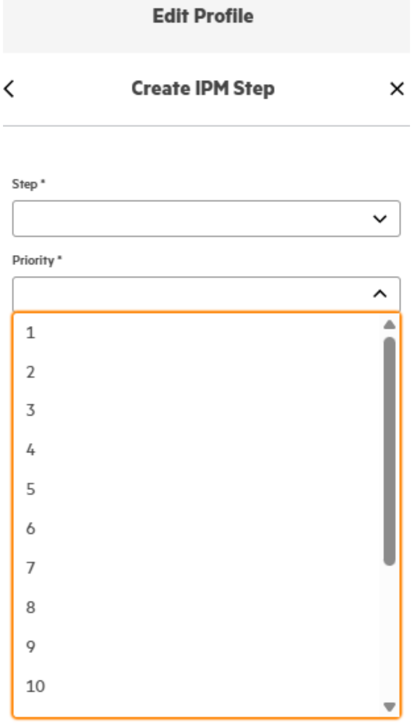
Step	Priority

No data to display



Step *

- Reduce CPU freq to 25%
- Reduce CPU freq to 50%
- Reduce CPU freq to 75%
- Disable 2nd Eth port
- Disable PSE1
- Disable PSE2
- Disable USB
- Reduce radio 0 chains to 1x1
- Reduce radio 0 chains to 2x2
- Reduce radio 0 chains to 3x3



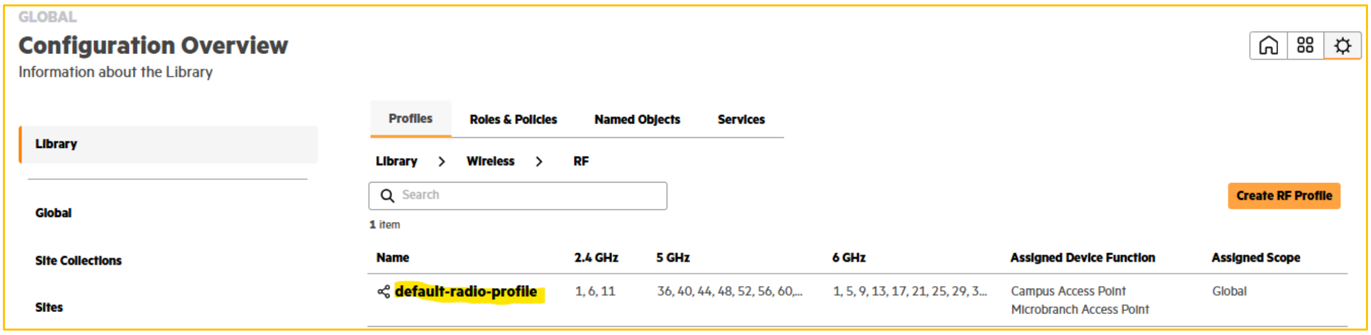
Step *

Priority *

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10

4.7 RF Profile

Here too, there is default RF profile that gets created based on your APs. Again you cannot edit the default profiles but you can create a new one based on your specific requirements. Here I am just using the default profile.



GLOBAL

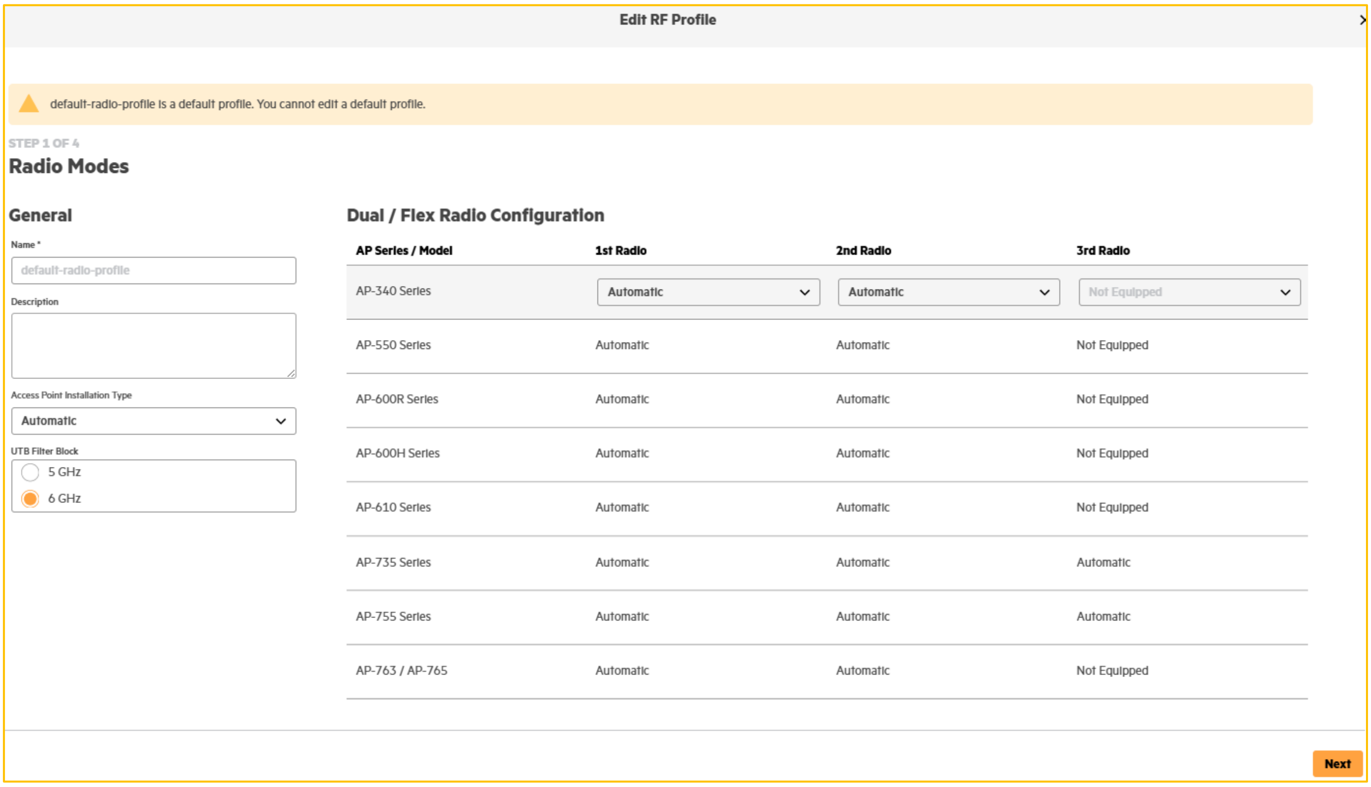
Configuration Overview

Information about the Library

1 item

Name	2.4 GHz	5 GHz	6 GHz	Assigned Device Function	Assigned Scope
default-radio-profile	1, 6, 11	36, 40, 44, 48, 52, 56, 60,...	1, 5, 9, 13, 17, 21, 25, 29, 3...	Campus Access Point Microbranch Access Point	Global

I am showing the screenshots just to display the configuration depth that you can do here. You can configure ultra band filter for 6GHz, flex radio settings just to mention a few.



Edit RF Profile

default-radio-profile is a default profile. You cannot edit a default profile.

STEP 1 OF 4

Radio Modes

General

Name *: default-radio-profile

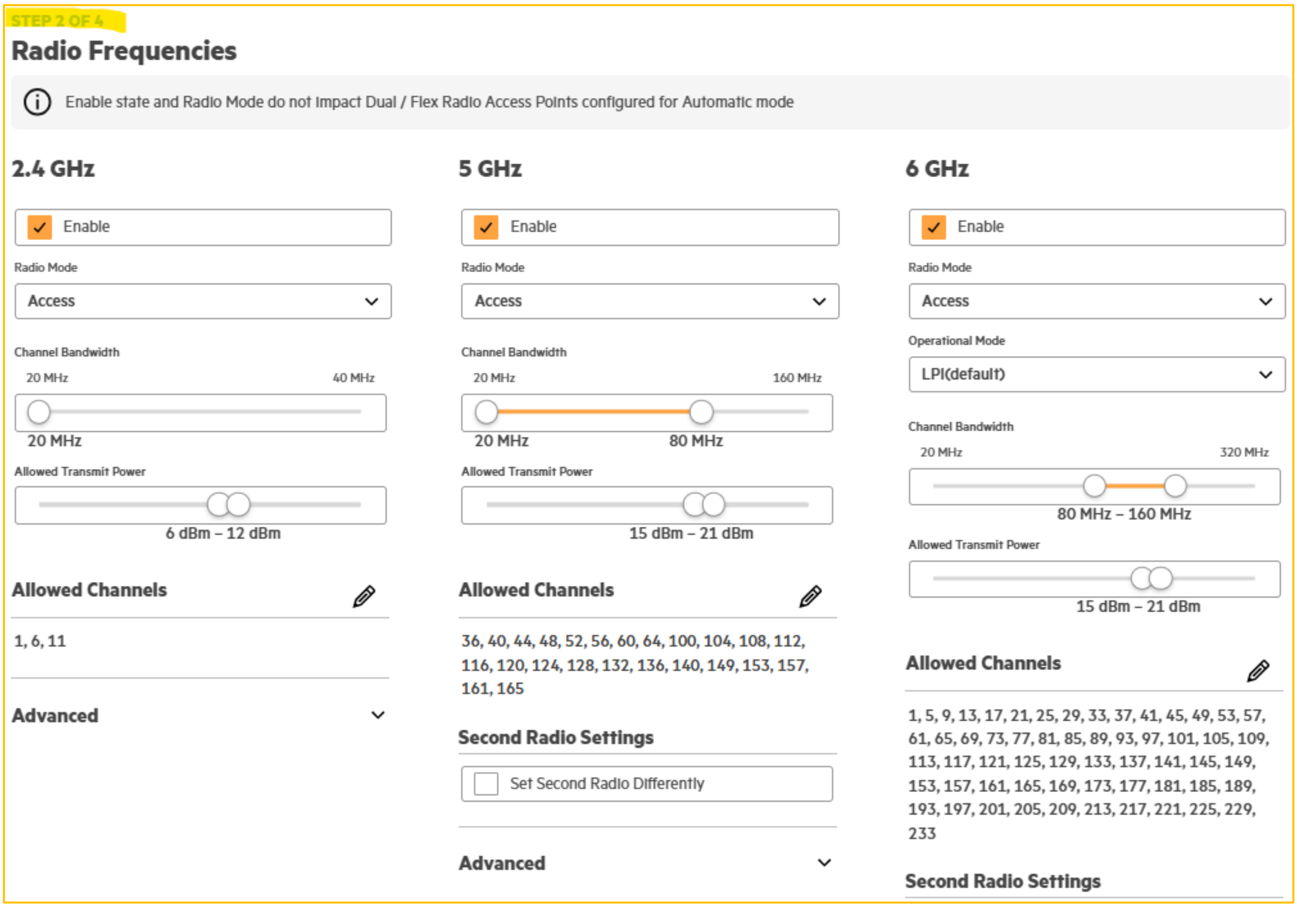
Description:

Access Point Installation Type: Automatic

UTB Filter Block: ○ 5 GHz ● 6 GHz

Dual / Flex Radio Configuration

AP Series / Model	1st Radio	2nd Radio	3rd Radio
AP-340 Series	Automatic	Automatic	Not Equipped
AP-550 Series	Automatic	Automatic	Not Equipped
AP-600R Series	Automatic	Automatic	Not Equipped
AP-600H Series	Automatic	Automatic	Not Equipped
AP-610 Series	Automatic	Automatic	Not Equipped
AP-735 Series	Automatic	Automatic	Automatic
AP-755 Series	Automatic	Automatic	Automatic
AP-763 / AP-765	Automatic	Automatic	Not Equipped



STEP 2 OF 4

Radio Frequencies

ⓘ Enable state and Radio Mode do not impact Dual / Flex Radio Access Points configured for Automatic mode

2.4 GHz

☑ Enable

Radio Mode: Access

Channel Bandwidth: 20 MHz – 40 MHz; selected: 20 MHz

Allowed Transmit Power: 6 dBm – 12 dBm

Allowed Channels

1, 6, 11

Advanced

5 GHz

☑ Enable

Radio Mode: Access

Channel Bandwidth: 20 MHz – 160 MHz; selected: 20 MHz – 80 MHz

Allowed Transmit Power: 15 dBm – 21 dBm

Allowed Channels

36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165

Second Radio Settings

☐ Set Second Radio Differently

Advanced

6 GHz

☑ Enable

Radio Mode: Access

Operational Mode: LPI(default)

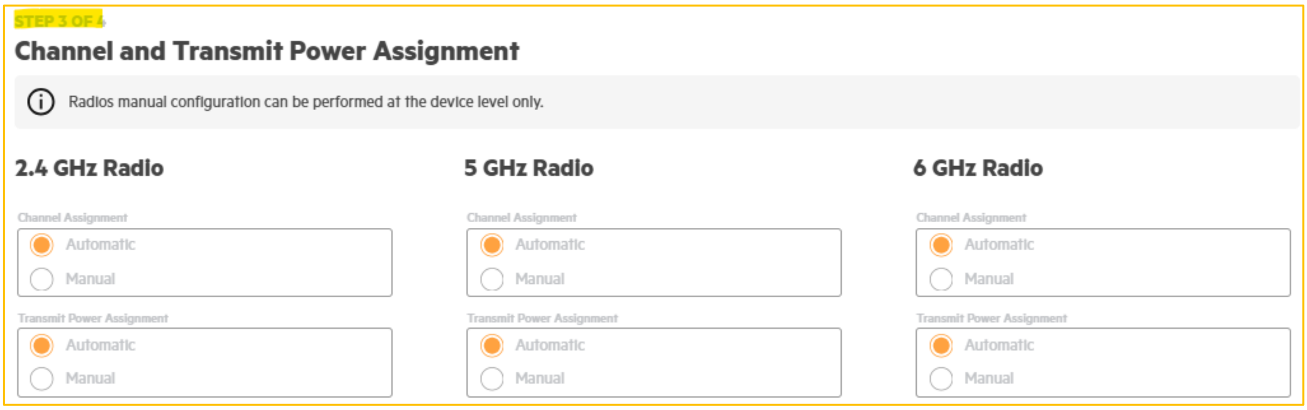
Channel Bandwidth: 20 MHz – 320 MHz; selected: 80 MHz – 160 MHz

Allowed Transmit Power: 15 dBm – 21 dBm

Allowed Channels

1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93, 97, 101, 105, 109, 113, 117, 121, 125, 129, 133, 137, 141, 145, 149, 153, 157, 161, 165, 169, 173, 177, 181, 185, 189, 193, 197, 201, 205, 209, 213, 217, 221, 225, 229, 233

Second Radio Settings



STEP 3 OF 4

Channel and Transmit Power Assignment

ⓘ Radios manual configuration can be performed at the device level only.

2.4 GHz Radio

Channel Assignment: ● Automatic ○ Manual

Transmit Power Assignment: ● Automatic ○ Manual

5 GHz Radio

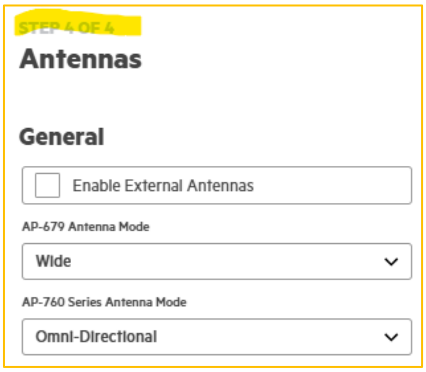
Channel Assignment: ● Automatic ○ Manual

Transmit Power Assignment: ● Automatic ○ Manual

6 GHz Radio

Channel Assignment: ● Automatic ○ Manual

Transmit Power Assignment: ● Automatic ○ Manual



STEP 4 OF 4

Antennas

General

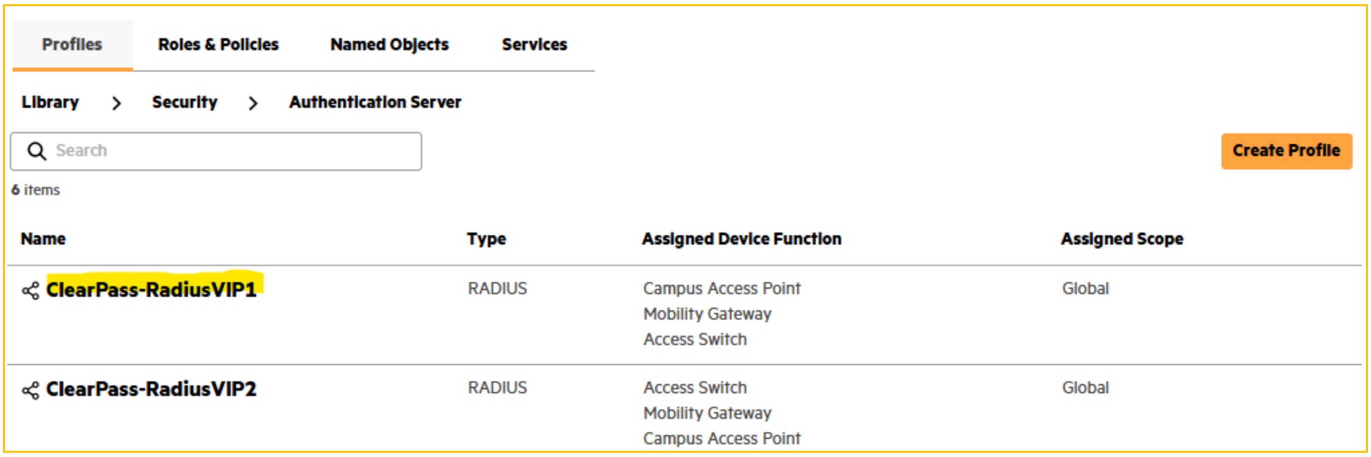
☐ Enable External Antennas

AP-679 Antenna Mode: Wide

AP-760 Series Antenna Mode: Omni-Directional

4.8 AAA Authentication Profile

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

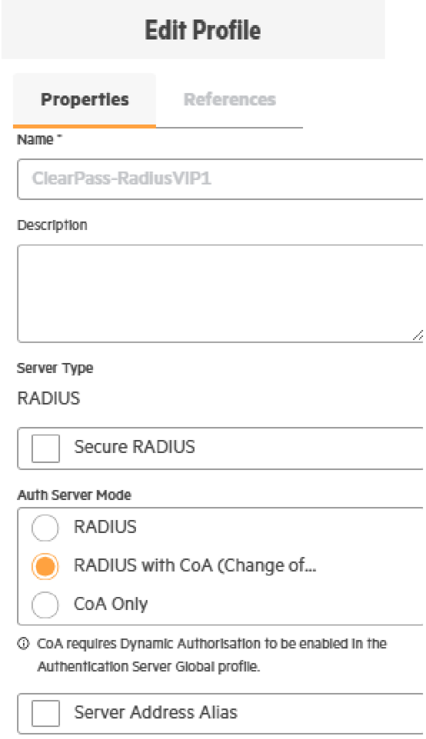
Search

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

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



Edit Profile

Properties | References

Name *

ClearPass-RadiusVIP1

Description

Server Type

RADIUS

□ Secure RADIUS

Auth Server Mode

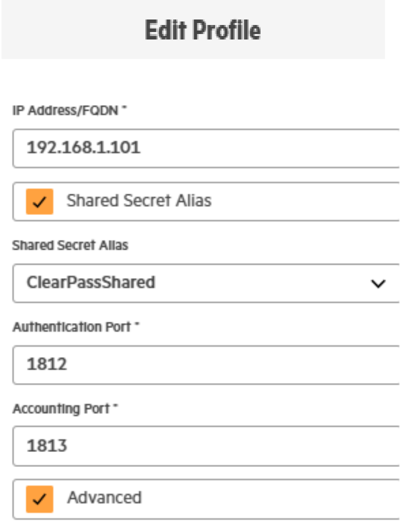
○ RADIUS

● RADIUS with CoA (Change of...

○ CoA Only

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

□ Server Address Alias



Edit Profile

IP Address/FQDN *

192.168.1.101

☑ Shared Secret Alias

Shared Secret Alias

ClearPassShared

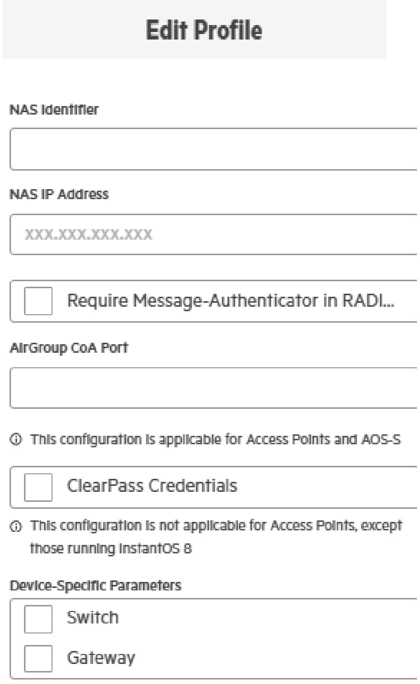
Authentication Port *

1812

Accounting Port *

1813

☑ Advanced



Edit Profile

NAS Identifier

NAS IP Address

xxx.xxx.xxx.xxx

□ Require Message-Authenticator in RADI...

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

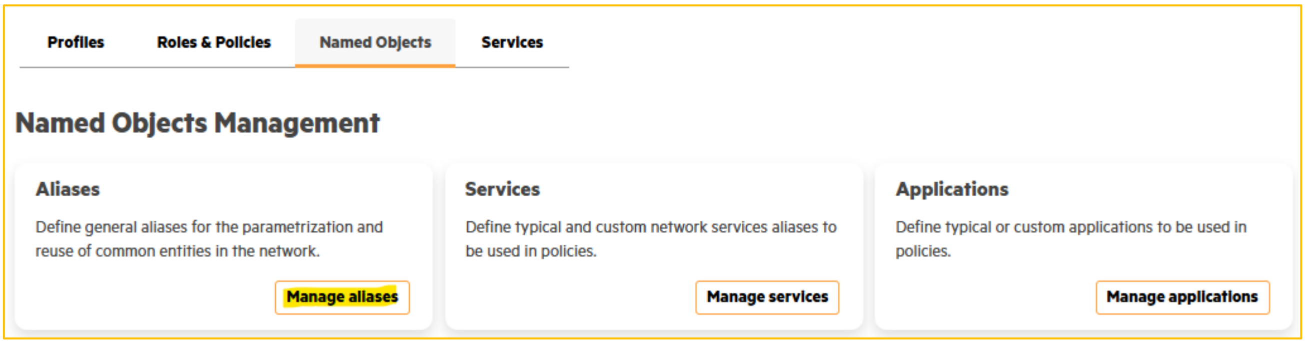
Device-Specific Parameters

□ Switch

□ Gateway

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

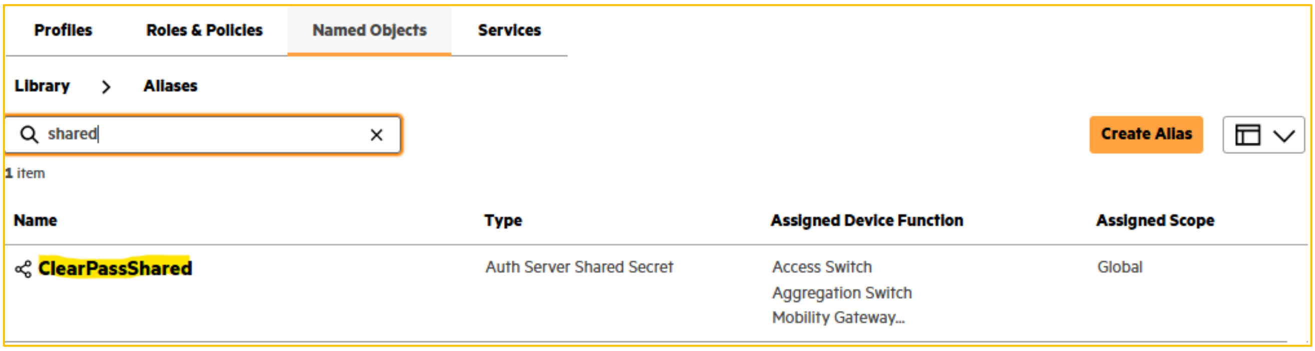
Define typical and custom network services aliases to be used in policies.

Manage services

Applications

Define typical or custom applications to be used in policies.

Manage applications

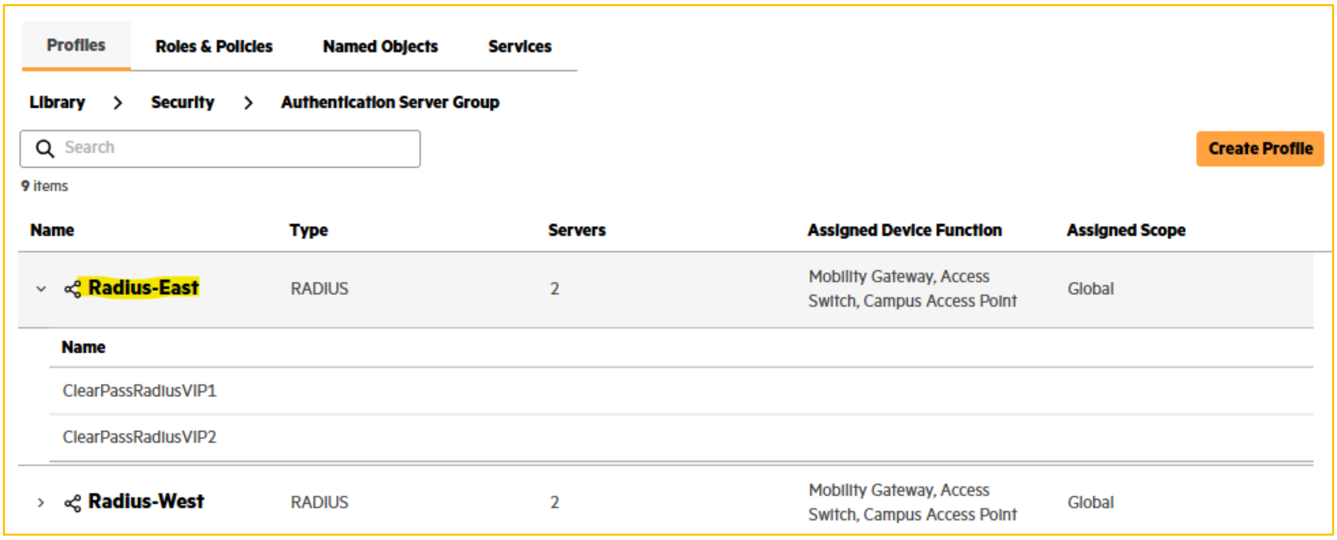


shared

1 item

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

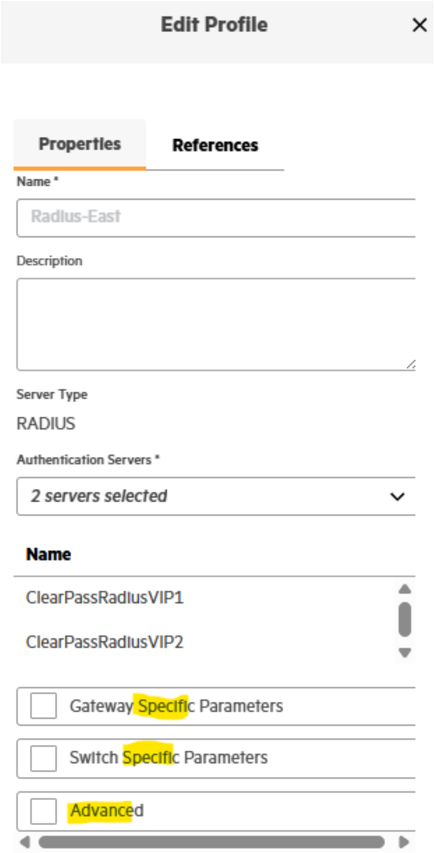
Now we need to add the authentications servers to the auth server groups where I have added my two ClearPass nodes.



9 items

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

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.



Name *
Radius-East

Description

Server Type
RADIUS

Authentication Servers *
2 servers selected

Name
ClearPassRadiusVIP1
ClearPassRadiusVIP2

□ Gateway Specific Parameters

□ Switch Specific Parameters

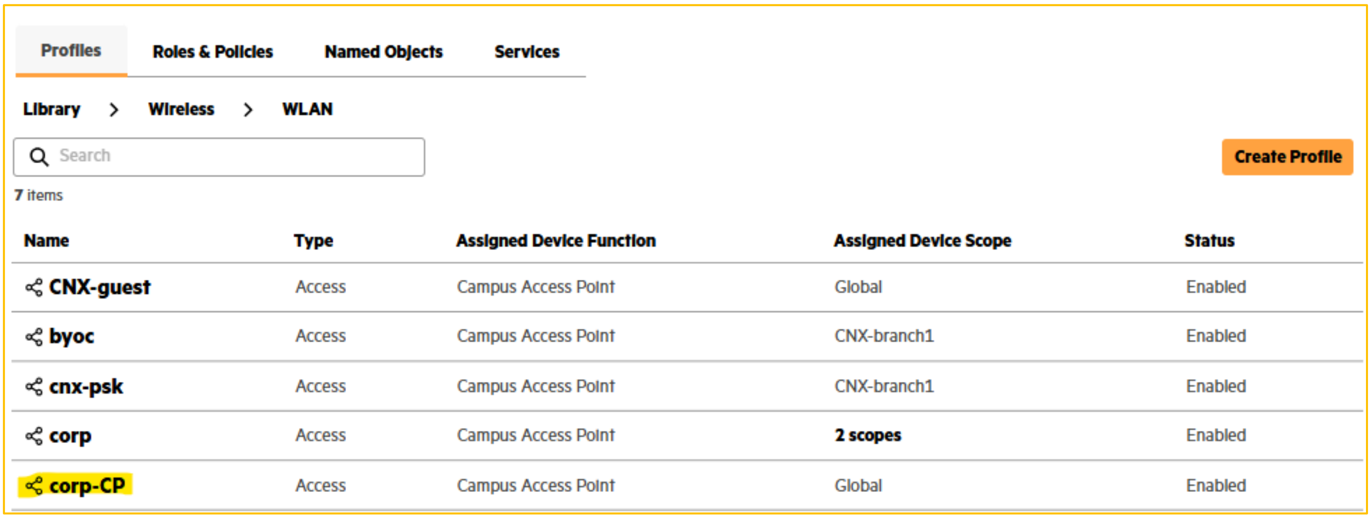
□ Advanced

4.9 WLAN Profile

Now we’ll configure our 802.1x WLAN profile called corp-CP that uses ClearPass for authentication.

You can use create a new WLAN profile by clicking n “Create Profile” for each SSID you will be broadcasting. Note that under each heading, there is the “Advanced” option that can be expanded and provides more configuration options like (Broadcast/Multicast filter, Data Rates, etc).

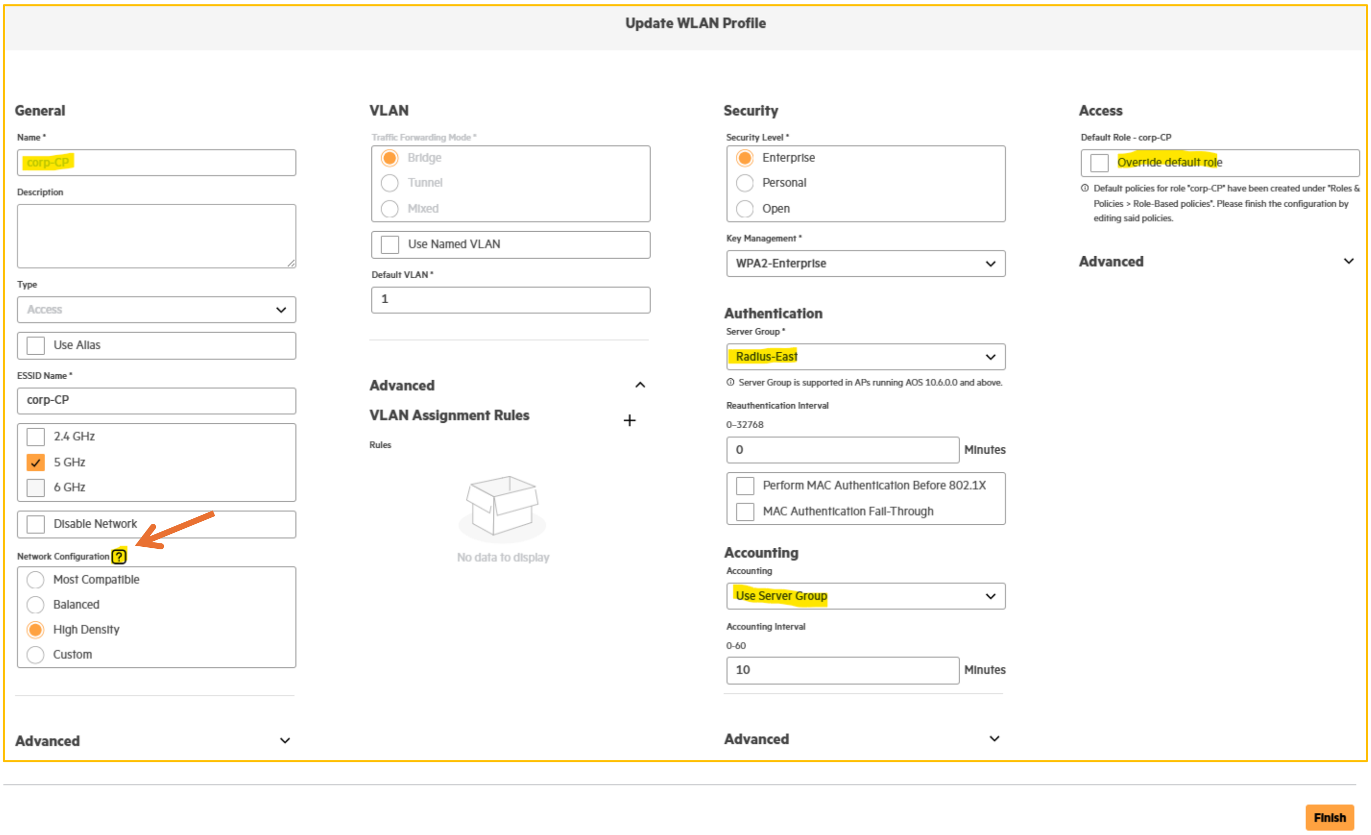
When you are done, assign the Scope as you have done for the previous profiles.



7 items

Name	Type	Assigned Device Function	Assigned Device Scope	Status
CNX-guest	Access	Campus Access Point	Global	Enabled
byoc	Access	Campus Access Point	CNX-branch1	Enabled
cnx-psk	Access	Campus Access Point	CNX-branch1	Enabled
corp	Access	Campus Access Point	2 scopes	Enabled
corp-CP	Access	Campus Access Point	Global	Enabled

Note that under “Network configuration”, I have chosen “High Density”. If you are curious about what this is all about you can click on the “?” icon



Update WLAN Profile

General

Name *: corp-CP

Description:

Type: Access

□ Use Alias

ESSID Name *: corp-CP

□ 2.4 GHz
☑ 5 GHz
□ 6 GHz

□ Disable Network

Network Configuration ?
○ Most Compatible
○ Balanced
● High Density
○ Custom

VLAN

Traffic Forwarding Mode *
● Bridge
○ Tunnel
○ Mixed

□ Use Named VLAN

Default VLAN *: 1

VLAN Assignment Rules +

Rules

No data to display

Security

Security Level *
● Enterprise
○ Personal
○ Open

Key Management *: WPA2-Enterprise

Authentication

Server Group *: Radius-East

ⓘ Server Group is supported in APs running AOS 10.6.0.0 and above.

Reauthentication Interval
0–32768
0 Minutes

□ Perform MAC Authentication Before 802.1X
□ MAC Authentication Fall-Through

Accounting

Accounting: Use Server Group

Accounting Interval
0-60
10 Minutes

Access

Default Role - corp-CP

□ Override default role

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

Clicking on the “?” as shown above will give you the following Configuration setting for High Density

- G and A Basic Data Rates: 24, 36
- Transmit rates include all available rates from 24 and above (inclusive)
- Broadcast filter: ARP
- IPv6 RA and ND Optimization: Convert to Unicast

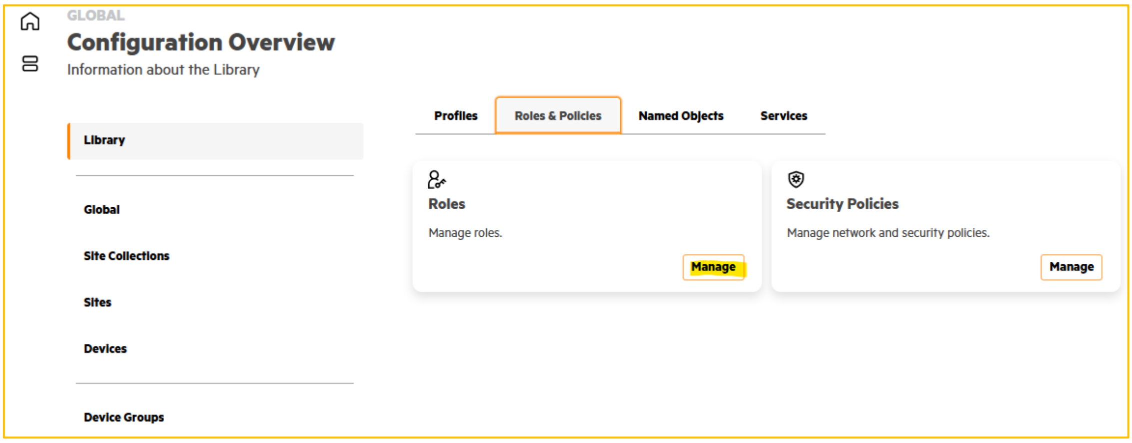
- Disable DMO
- 11r and 11k Enabled
- Enable OKC, PMK caching 11r: Disabled

Another thing is that you can override the default role, but by default it will be the name of the WLAN profile.

Since I want to show only wireless users connecting to corp-CP WLAN in bridge mode, I don't need to configure VLANs for the APs. Obviously it is needed for wired clients and you need to configure VLAN Profiles.

4.10 User Roles

The final piece is to configure user roles and related policies. In most cases, you want to use the same user roles for your wired and wireless users.



GLOBAL

Configuration Overview

Information about the Library

Library

Global

Site Collections

Sites

Devices

Device Groups

Profiles | Roles & Policies | Named Objects | Services

Roles

Manage roles.

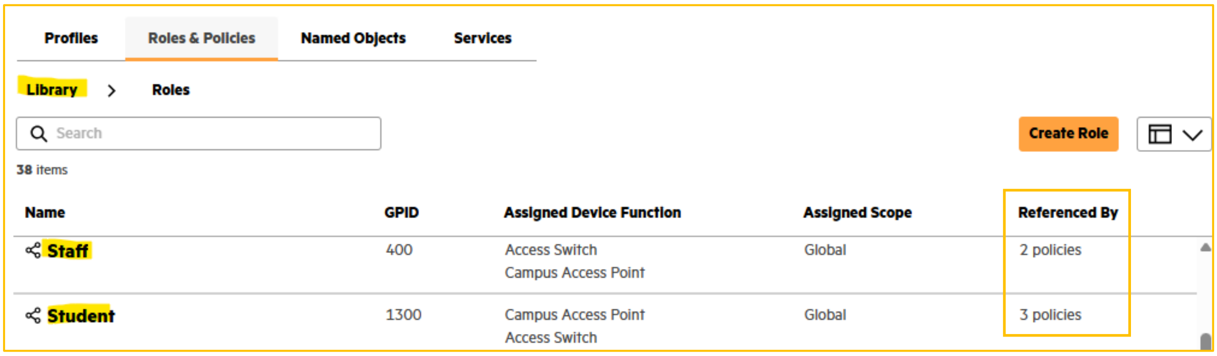
Manage

Security Policies

Manage network and security policies.

Manage

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



Profiles | Roles & Policies | Named Objects | Services

Library > Roles

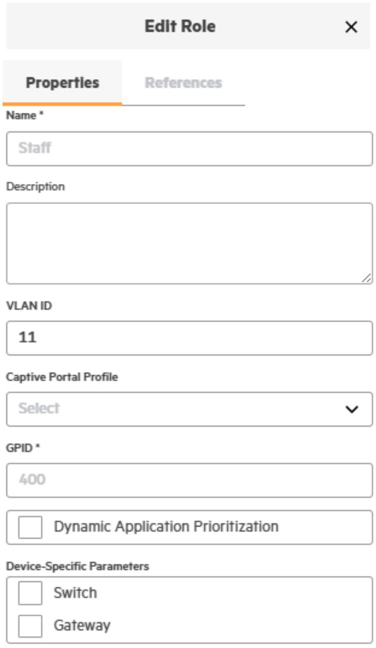
Search

Create Role

38 items

Name	GPID	Assigned Device Function	Assigned Scope	Referenced By
Staff	400	Access Switch Campus Access Point	Global	2 policies
Student	1300	Campus Access Point Access Switch	Global	3 policies

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 *: Staff

Description:

VLAN ID: 11

Captive Portal Profile: Select

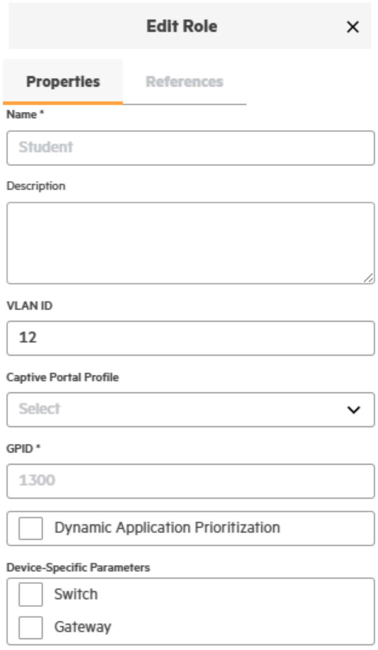
GPID *: 400

□ Dynamic Application Prioritization

Device-Specific Parameters

□ Switch

□ Gateway



Edit Role

Properties | References

Name *: Student

Description:

VLAN ID: 12

Captive Portal Profile: Select

GPID *: 1300

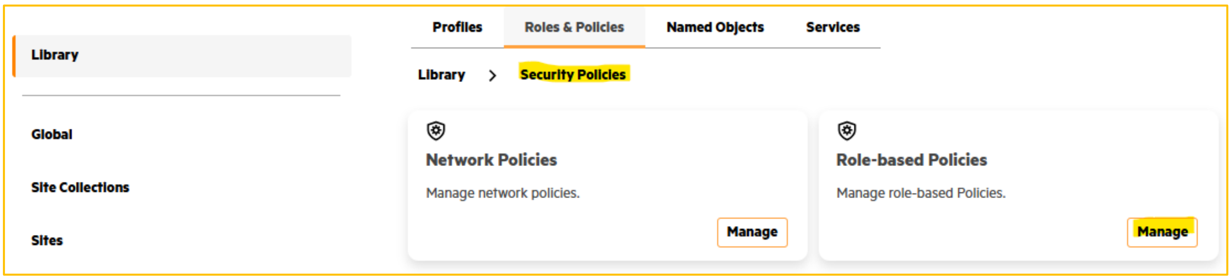
□ Dynamic Application Prioritization

Device-Specific Parameters

□ Switch

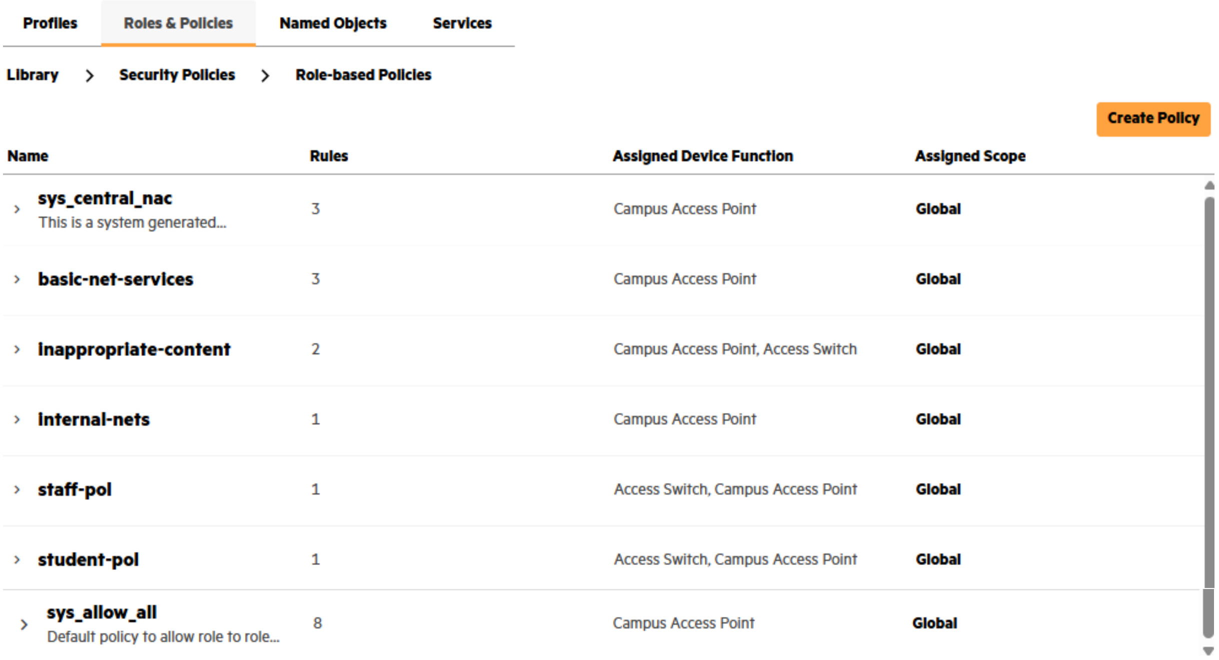
□ Gateway

So I have assigned Staff role to VLAN11 and Student Role to VLAN 12. 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.
- Ans if you decide to have "Deny all" policy then other polices with rules explicitly allowing certain traffic should be defined above it.

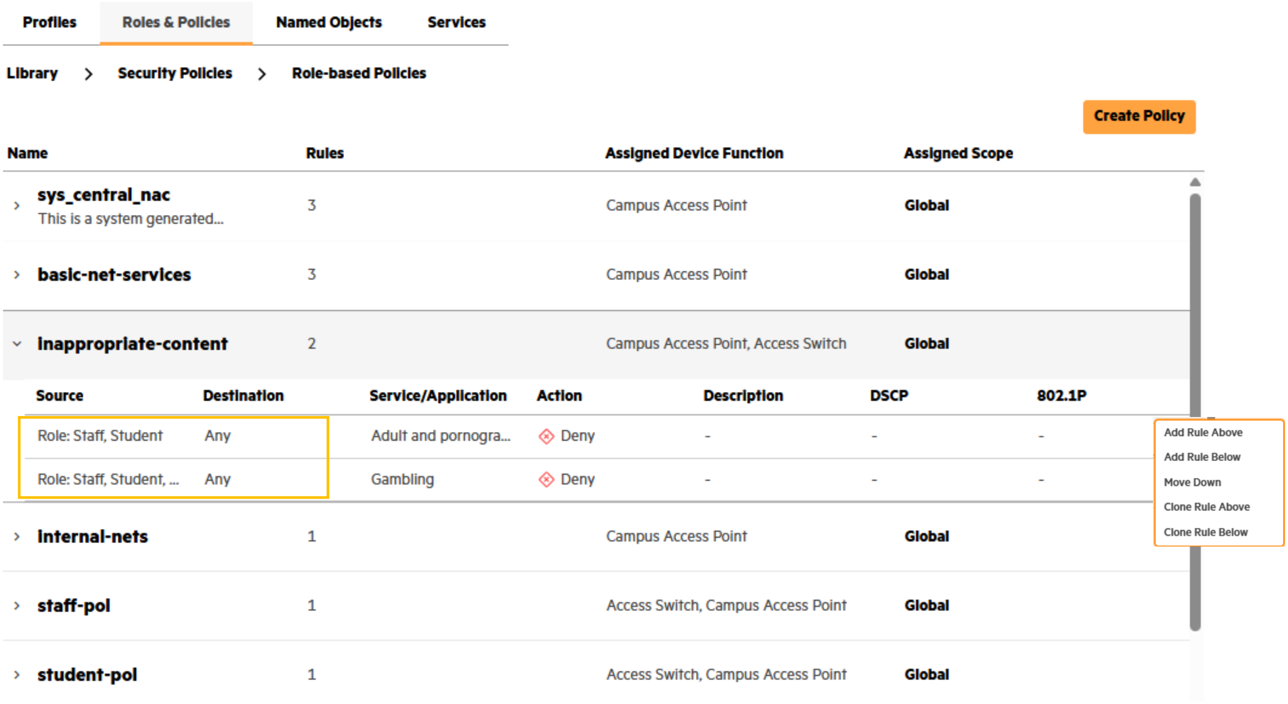


Name	Rules	Assigned Device Function	Assigned Scope
sys_central_nac This is a system generated...	3	Campus Access Point	Global
basic-net-services	3	Campus Access Point	Global
inappropriate-content	2	Campus Access Point, Access Switch	Global
internal-nets	1	Campus Access Point	Global
staff-pol	1	Access Switch, Campus Access Point	Global
student-pol	1	Access Switch, Campus Access Point	Global
sys_allow_all Default policy to allow role to role...	8	Campus Access Point	Global

Here I have 5x policies that I created.

Policies	Purpose	User role associated
Basic-net-services	Allow access to DHCP and DNS	Student
inappropriate-content	Deny access to inappropriate web categories	Staff, student
internal-nets	Allow access to RFC 1918 networks	Student
Staff-pol	Allow-all access	Staff
Student-pol	Deny-all access	Student

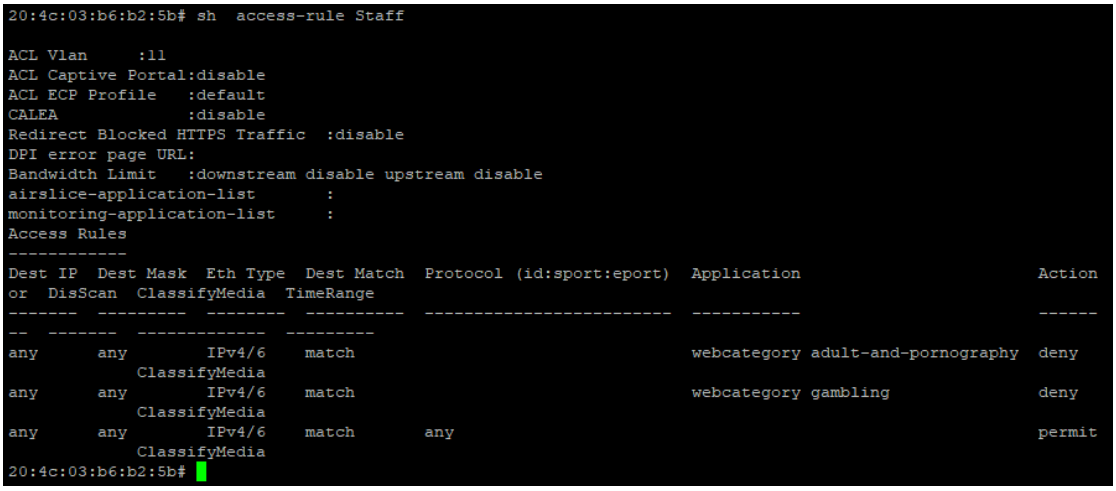
Expanding the "inappropriate-content" , you see that I am denying access to Adult and gambling sites. This policy is applied to most of my roles. So here you don't need to duplicate for each user role.



Name	Rules	Assigned Device Function	Assigned Scope
› sys_central_nac This is a system generated...	3	Campus Access Point	Global
› basic-net-services	3	Campus Access Point	Global
˅ inappropriate-content	2	Campus Access Point, Access Switch	Global
› internal-nets	1	Campus Access Point	Global
› staff-pol	1	Access Switch, Campus Access Point	Global
› student-pol	1	Access Switch, Campus Access Point	Global

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

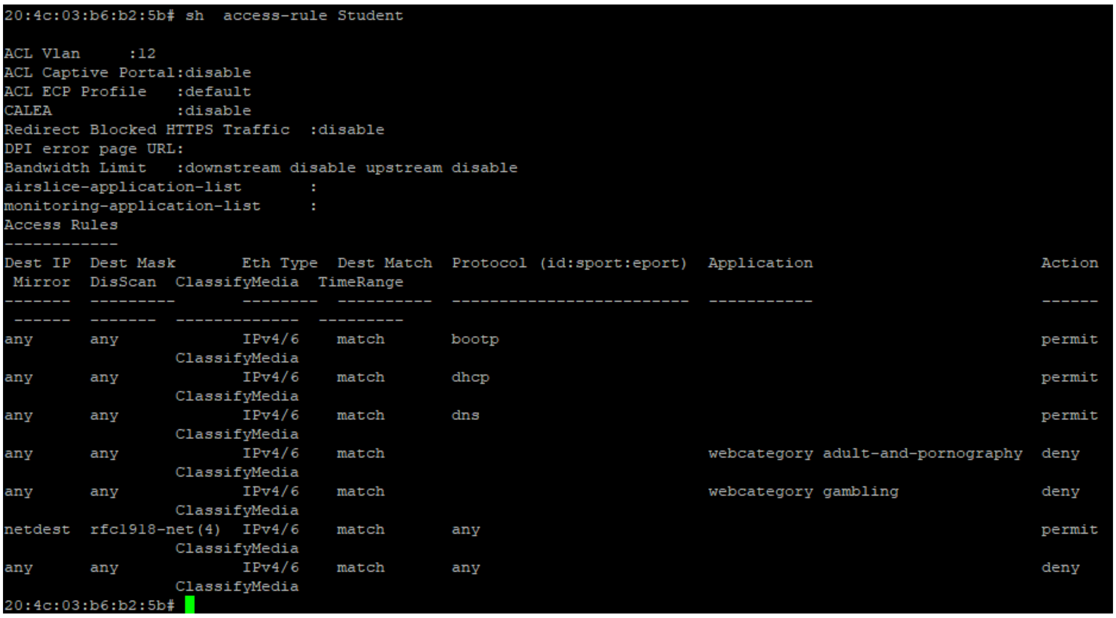
When you hover your mouse over a rule, "**...**" appears and by clicking on it you can bring up the rule ordering cloning pop-up. As you are reordering the policies, the order gets synced to the AP. You can check the rules that were pushed down to the AP as shown below for Staff role.



```
20:4c:03:b6:b2:5b# sh  access-rule Staff

ACL Vlan     :11
ACL Captive Portal:disable
ACL ECP Profile   :default
CALEA             :disable
Redirect Blocked HTTPS Traffic  :disable
DPI error page URL:
Bandwidth Limit   :downstream disable upstream disable
airslice-application-list       :
monitoring-application-list     :
Access Rules
------------
Dest IP  Dest Mask  Eth Type  Dest Match  Protocol (id:sport:eport)  Application                        Action
or  DisScan  ClassifyMedia  TimeRange
-------  ---------  --------  ----------  -------------------------  -----------                        ------
--  -------  -------------  ---------
any      any        IPv4/6    match                                  webcategory adult-and-pornography  deny
             ClassifyMedia
any      any        IPv4/6    match                                  webcategory gambling               deny
             ClassifyMedia
any      any        IPv4/6    match       any                                                           permit
             ClassifyMedia
20:4c:03:b6:b2:5b# █
```

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



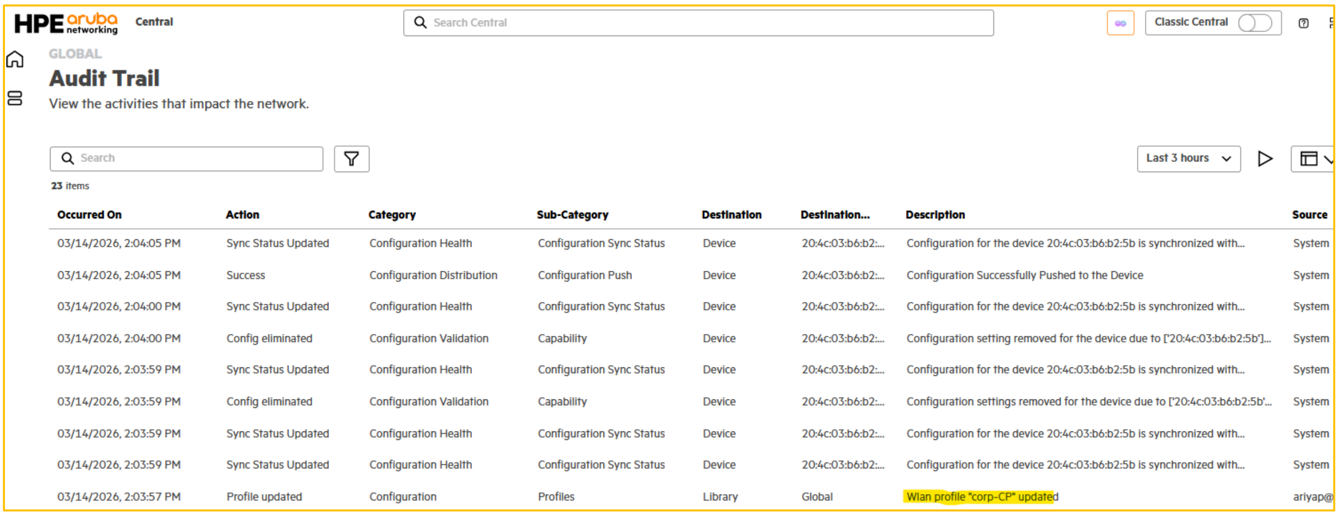
```
20:4c:03:b6:b2:5b# sh  access-rule Student

ACL Vlan     :12
ACL Captive Portal:disable
ACL ECP Profile   :default
CALEA             :disable
Redirect Blocked HTTPS Traffic  :disable
DPI error page URL:
Bandwidth Limit   :downstream disable upstream disable
airslice-application-list       :
monitoring-application-list     :
Access Rules
------------
Dest IP  Dest Mask       Eth Type  Dest Match  Protocol (id:sport:eport)  Application                        Action
 Mirror  DisScan  ClassifyMedia  TimeRange
-------  ---------       --------  ----------  -------------------------  -----------                        ------
 ------  -------  -------------  ---------
any      any             IPv4/6    match       bootp                                                         permit
                  ClassifyMedia
any      any             IPv4/6    match       dhcp                                                          permit
                  ClassifyMedia
any      any             IPv4/6    match       dns                                                           permit
                  ClassifyMedia
any      any             IPv4/6    match                                  webcategory adult-and-pornography  deny
                  ClassifyMedia
any      any             IPv4/6    match                                  webcategory gambling               deny
                  ClassifyMedia
netdest  rfc1918-net(4)  IPv4/6    match       any                                                           permit
                  ClassifyMedia
any      any             IPv4/6    match       any                                                           deny
                  ClassifyMedia
20:4c:03:b6:b2:5b# █
```

5 Testing

5.1 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.



GLOBAL

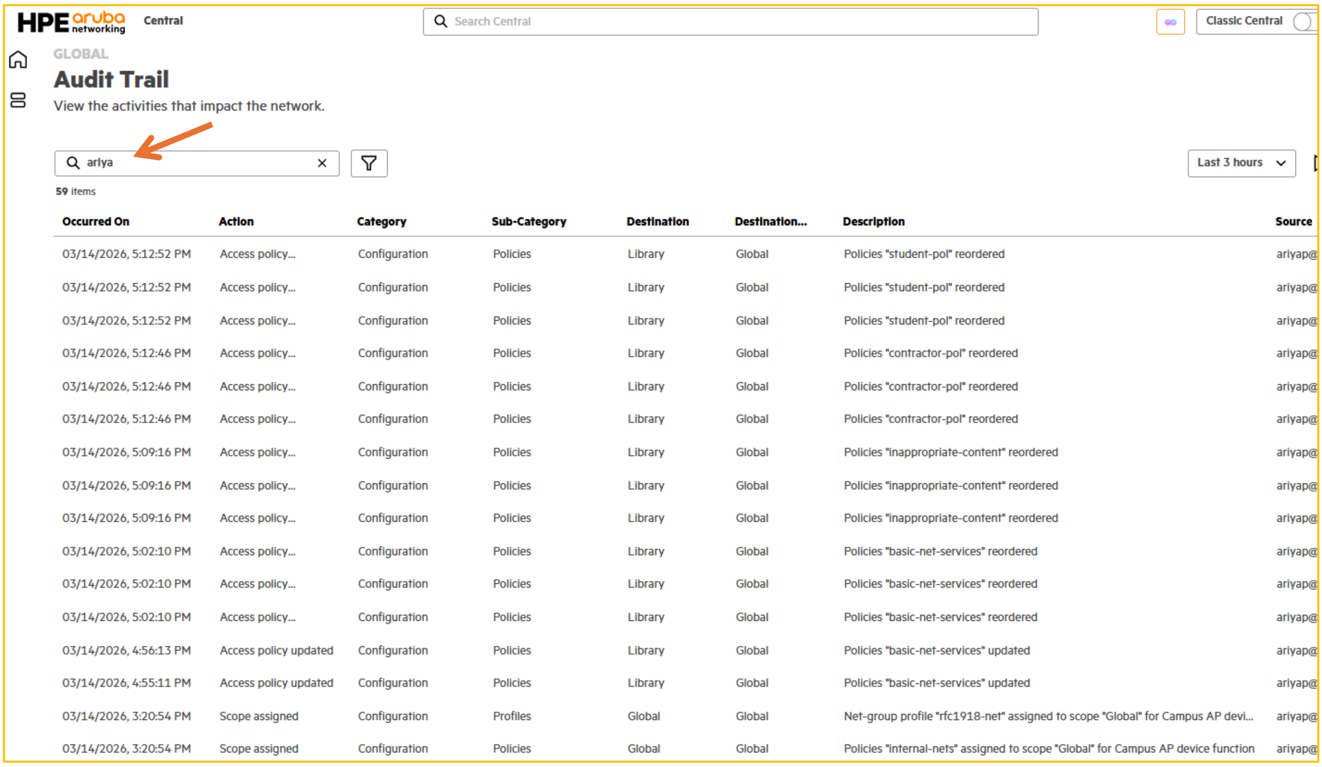
Audit Trail

View the activities that impact the network.

23 items

Occurred On	Action	Category	Sub-Category	Destination	Destination...	Description	Source
03/14/2026, 2:04:05 PM	Sync Status Updated	Configuration Health	Configuration Sync Status	Device	20:4c:03:b6:b2:...	Configuration for the device 20:4c:03:b6:b2:5b is synchronized with...	System
03/14/2026, 2:04:05 PM	Success	Configuration Distribution	Configuration Push	Device	20:4c:03:b6:b2:...	Configuration Successfully Pushed to the Device	System
03/14/2026, 2:04:00 PM	Sync Status Updated	Configuration Health	Configuration Sync Status	Device	20:4c:03:b6:b2:...	Configuration for the device 20:4c:03:b6:b2:5b is synchronized with...	System
03/14/2026, 2:04:00 PM	Config eliminated	Configuration Validation	Capability	Device	20:4c:03:b6:b2:...	Configuration setting removed for the device due to ['20:4c:03:b6:b2:5b']...	System
03/14/2026, 2:03:59 PM	Sync Status Updated	Configuration Health	Configuration Sync Status	Device	20:4c:03:b6:b2:...	Configuration for the device 20:4c:03:b6:b2:5b is synchronized with...	System
03/14/2026, 2:03:59 PM	Config eliminated	Configuration Validation	Capability	Device	20:4c:03:b6:b2:...	Configuration settings removed for the device due to ['20:4c:03:b6:b2:5b'...	System
03/14/2026, 2:03:59 PM	Sync Status Updated	Configuration Health	Configuration Sync Status	Device	20:4c:03:b6:b2:...	Configuration for the device 20:4c:03:b6:b2:5b is synchronized with...	System
03/14/2026, 2:03:59 PM	Sync Status Updated	Configuration Health	Configuration Sync Status	Device	20:4c:03:b6:b2:...	Configuration for the device 20:4c:03:b6:b2:5b is synchronized with...	System
03/14/2026, 2:03:57 PM	Profile updated	Configuration	Profiles	Library	Global	Wlan profile "corp-CP" updated	ariyap@

And here is the audit trail for some of the policies that I was updating



GLOBAL

Audit Trail

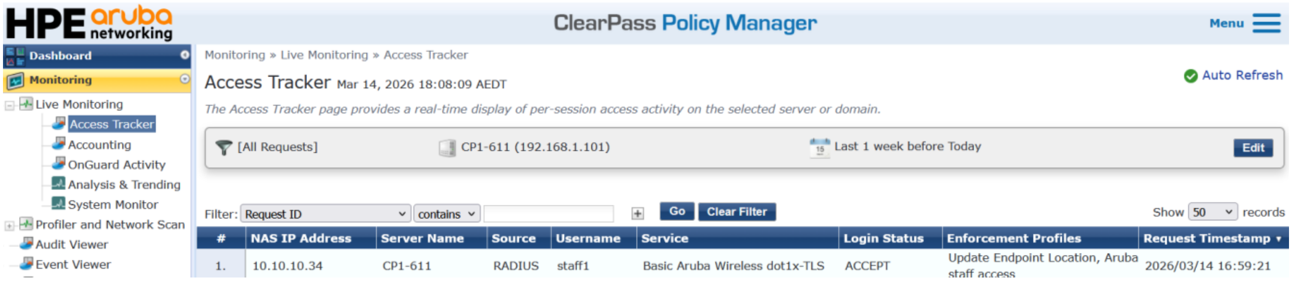
View the activities that impact the network.

59 items

Occurred On	Action	Category	Sub-Category	Destination	Destination...	Description	Source
03/14/2026, 5:12:52 PM	Access policy...	Configuration	Policies	Library	Global	Policies "student-pol" reordered	ariyap@
03/14/2026, 5:12:52 PM	Access policy...	Configuration	Policies	Library	Global	Policies "student-pol" reordered	ariyap@
03/14/2026, 5:12:52 PM	Access policy...	Configuration	Policies	Library	Global	Policies "student-pol" reordered	ariyap@
03/14/2026, 5:12:46 PM	Access policy...	Configuration	Policies	Library	Global	Policies "contractor-pol" reordered	ariyap@
03/14/2026, 5:12:46 PM	Access policy...	Configuration	Policies	Library	Global	Policies "contractor-pol" reordered	ariyap@
03/14/2026, 5:12:46 PM	Access policy...	Configuration	Policies	Library	Global	Policies "contractor-pol" reordered	ariyap@
03/14/2026, 5:09:16 PM	Access policy...	Configuration	Policies	Library	Global	Policies "inappropriate-content" reordered	ariyap@
03/14/2026, 5:09:16 PM	Access policy...	Configuration	Policies	Library	Global	Policies "inappropriate-content" reordered	ariyap@
03/14/2026, 5:09:16 PM	Access policy...	Configuration	Policies	Library	Global	Policies "inappropriate-content" reordered	ariyap@
03/14/2026, 5:02:10 PM	Access policy...	Configuration	Policies	Library	Global	Policies "basic-net-services" reordered	ariyap@
03/14/2026, 5:02:10 PM	Access policy...	Configuration	Policies	Library	Global	Policies "basic-net-services" reordered	ariyap@
03/14/2026, 5:02:10 PM	Access policy...	Configuration	Policies	Library	Global	Policies "basic-net-services" reordered	ariyap@
03/14/2026, 4:56:13 PM	Access policy updated	Configuration	Policies	Library	Global	Policies "basic-net-services" updated	ariyap@
03/14/2026, 4:55:11 PM	Access policy updated	Configuration	Policies	Library	Global	Policies "basic-net-services" updated	ariyap@
03/14/2026, 3:20:54 PM	Scope assigned	Configuration	Profiles	Global	Global	Net-group profile "rfc1918-net" assigned to scope "Global" for Campus AP devi...	ariyap@
03/14/2026, 3:20:54 PM	Scope assigned	Configuration	Policies	Global	Global	Policies "internal-nets" assigned to scope "Global" for Campus AP device function	ariyap@

5.2 User Connectivity

Let's check ClearPass access tracker after getting a client connected to corp-CP WLAN.



Monitoring » Live Monitoring » Access Tracker

Access Tracker Mar 14, 2026 18:08:09 AEDT

Auto Refresh

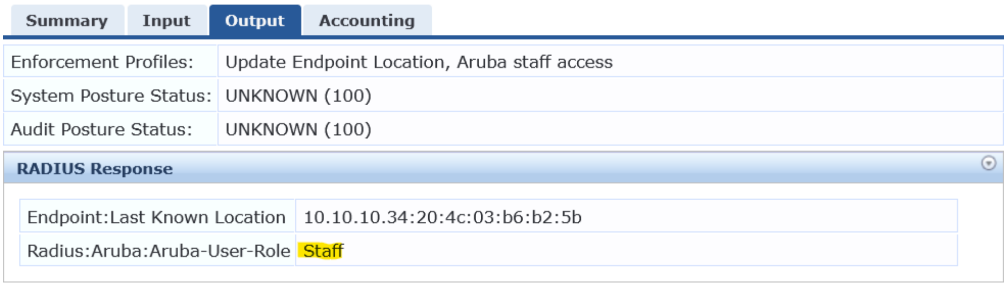
The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[All Requests] CP1-611 (192.168.1.101) Last 1 week before Today Edit

Filter: Request ID contains Go Clear Filter Show 50 records

#	NAS IP Address	Server Name	Source	Username	Service	Login Status	Enforcement Profiles	Request Timestamp ▾
1.	10.10.10.34	CP1-611	RADIUS	staff1	Basic Aruba Wireless dot1x-TLS	ACCEPT	Update Endpoint Location, Aruba staff access	2026/03/14 16:59:21

The authentication is successful and it is sending back Staff user role.



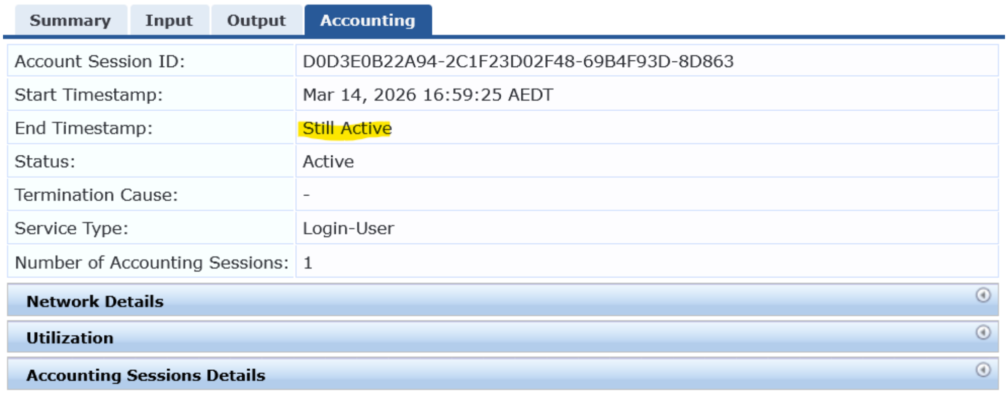
Summary Input **Output** Accounting

Enforcement Profiles:	Update Endpoint Location, Aruba staff access
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Endpoint:Last Known Location	10.10.10.34:20:4c:03:b6:b2:5b
Radius:Aruba:Aruba-User-Role	Staff

This is to show that it is receiving RADIUS accounting records as well.



Summary Input Output **Accounting**

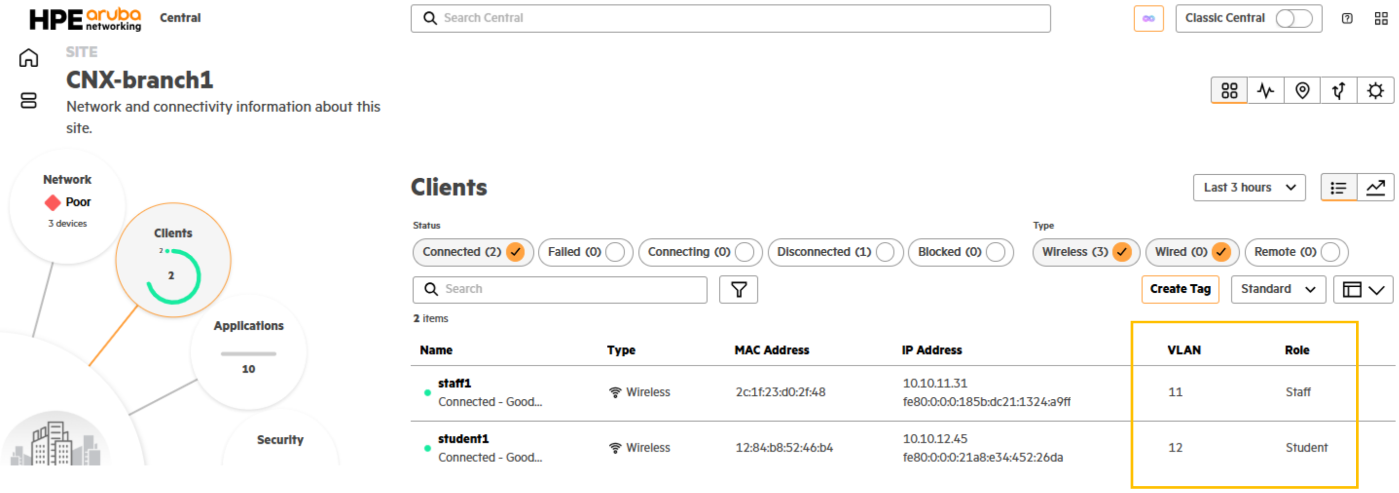
Account Session ID:	D0D3E0B22A94-2C1F23D02F48-69B4F93D-8D863
Start Timestamp:	Mar 14, 2026 16:59:25 AEDT
End Timestamp:	Still Active
Status:	Active
Termination Cause:	-
Service Type:	Login-User
Number of Accounting Sessions:	1

Network Details

Utilization

Accounting Sessions Details

Now we'll check the client planet in New Central site dashboard for CNX-branch1.



CNX-branch1

Network and connectivity information about this site.

Clients

Last 3 hours

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

Type: Wireless (3) ✓ Wired (0) ✓ Remote (0) ○

Search Create Tag Standard

2 items

Name	Type	MAC Address	IP Address	VLAN	Role
staff1 Connected - Good...	Wireless	2c:1f:23:d0:2f:48	10.10.11.31 fe80:0:0:0:185b:dc21:1324:a9ff	11	Staff
student1 Connected - Good...	Wireless	12:84:b8:52:46:b4	10.10.12.45 fe80:0:0:0:21a8:e34:452:26da	12	Student

It looks like the clients are in the correct Role and VLAN.

5.3 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.