aruba
a Hewlett Packard Enterprise company

# ESP Campus Deploy

Validated Solution Guide

Aruba Solution TME

May 28, 2025

# Table of Contents

# ESP Campus Deploy

This guide provides IT professionals with prescriptive steps to deploy a Campus network outlined in the Campus Design Document for the following products:

- Aruba Central
- Aruba ClearPass Policy Manager
- Aruba Access Point 300 and 500 Series
- Aruba Gateway 7000, 7200, and 9000 Series
- Aruba CX Switching 6300, 6400, 8300, and 8400 Series

## Document Conventions

Bold text indicates a command, navigational path, or a user interface element.

Examples:

- the **show stacking** command
- Go to **Configuration > System > General**
- **Username:** *admin*

Italic text indicates important terminology, user interface input, or a table heading.

Examples:

- *Spatial streaming* is a transmission technique in MIMO wireless communication
- **Password:** *password*
- *Example: Core 1 Switch*

Code blocks indicate a variable for which you substitute a value appropriate for your environment.

Example:

- Configure the NTP servers.

```
ntp server 10.2.120.98 iburst version 3
ntp server 10.2.120.99 iburst version 3
```

# Introduction

The Aruba ESP Campus design provides wired and wireless connectivity, policy for local users, and services that extend across the network. The wired LAN interconnects the wireless APs, WAN, data center, and Internet DMZ, making it a critical part of the network. Campus networks require a high-availability design to support mission-critical applications and real-time multimedia communications that drive organizational operations.

The Aruba ESP Campus provides the following benefits:

- Specific functions of individual layers make the network easier to operate and maintain.
- Modular building blocks quickly scale as the network grows.
- Location-independent network access improves employee and guest productivity.
- Hard-to-wire locations receive network connectivity without costly construction.
- ESP Campus facilitates plug-and-play wireless deployment with wired LAN switches preconfigured to recognize APs.
- Centralized control of wireless environment is easy to manage and operate.
- Reliable wireless connectivity, including complete RF spectrum management, is available with key Aruba management features.
- Configuration, management, and operations are simplified with using cloud-based controls.
- Simple, repeatable designs are easier to deploy, manage, and maintain.

This guide outlines recommended deployment options and provides general guidance for which options to use.

## Purpose of This Guide

This deployment guide covers the Campus in the Edge Services Platform (ESP) architecture. It contains an explanation of the requirements that shaped the design and the benefits they can provide to an organization. The guide describes a single system that integrates access points, gateways, access switches, aggregation switches, core switches, cloud-based orchestration, and network management.

For design guidance, refer to volume one of this VSG:

Aruba VSG: Campus Design

### Design Goals

The overall goal is to create a readily scalable design that is easy to replicate at different sites. The components are limited to a specific set of products to help with operations and maintenance. The design has a target of sub-second failover when a network device or link between two network devices becomes unavailable. The protocols are tuned for a highly available network in all functional areas.

This guide can be used to deploy new networks. It is not intended as an exhaustive discussion of all options, but rather to present the best recommended designs, features, software, and hardware.

## Audience

This guide is written for IT professionals who need to deploy Aruba solutions for small, medium, and large campus networks. These IT professionals can serve in a variety of roles:

- Systems Engineers who need a standard set of procedures for implementing Aruba solutions.
- Project Managers who create statements of work for Aruba implementations.
- Aruba Partners who sell technology or create implementation documentation.

## Customer Use Cases

With so many wireless devices on a network, performance and availability are key. Wireless clients with different capabilities support different performance levels. If the wireless network does not self-optimize, slower clients can degrade performance for faster clients.

The Wi-Fi 5 and Wi-Fi 6 standards support speeds greater than 1 Gbps. To accommodate the increased data rates, the APs implement the IEEE 802.3bz Ethernet standard of 2.5 and 5 Gbps. An organization can achieve the higher data rates on existing building twisted-pair cabling when connecting to Aruba switches with Smart Rate ports that also support the 802.3bz Ethernet standard. To support the explosion of IoT devices and latest wireless technologies, IEEE 802.3bt Power over Ethernet (PoE) provides simplicity and cost savings by eliminating the need for dedicated power. The access layer acts as a collection point for high-performance wired and wireless devices and must have enough capacity to support the power and bandwidth needs of today as well as scale for the future as the number of devices grows.

Security is a critical part of the campus network. Users must be authenticated and granted access to the services they need to do their jobs. IoT devices must be identified using MAC authentication and profiling to prevent rogue devices from using the network. In addition to corporate-managed assets, users connect personal devices, guests need access to the Internet, and contractors need access to the Internet and the organization's internal network. This type of broad access must be accomplished while maintaining the security and integrity of the network. Connecting so many devices and user types increases the administrative burden, and the network should allow automation of device onboarding in a secure manner.

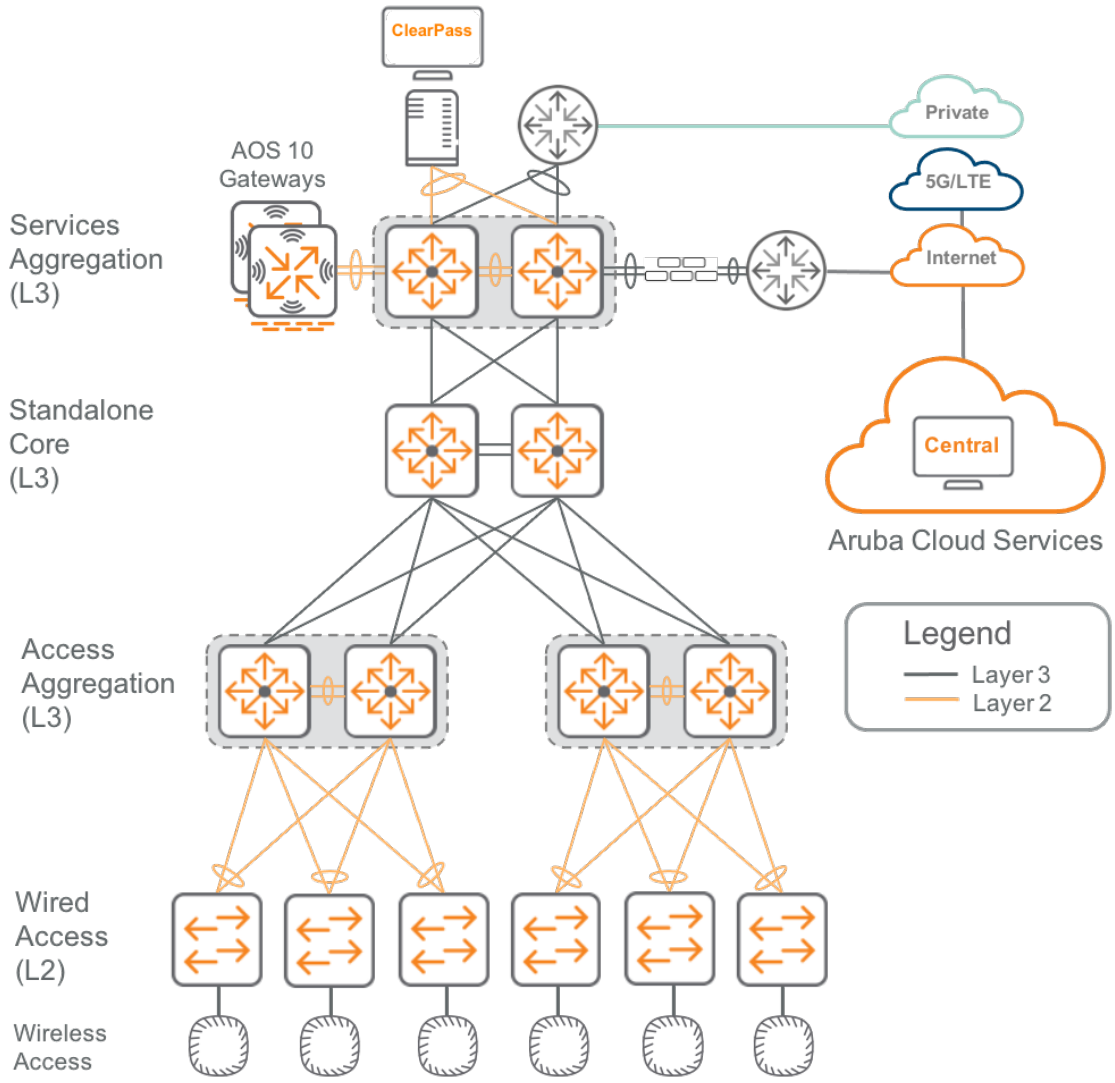
Before wireless became the primary network access method, typical network designs provided two or more wired ports per user. It was common to run two network drops to each user's desk and have additional ports for conference rooms, network printers, and other shared areas, adding up to just over two ports per user. In networks where 80% or more of the users are connecting over wireless, and wired IoT devices continue to rise, the number of wired ports in the network is closer to one per user.

# Deploying the Campus Network

The design referenced in this deployment guide is a large campus topology, described in the Aruba ESP Campus design guide. The topology implements a traditional 3-tier network using a routed core connected to an aggregation layer, which is then connected to the access layer. The access layer is deployed as Layer 2 only and default gateways are implemented at the aggregation layer. The design requires a services aggregation block connected to the core to ensure efficient delivery of services to endpoints across the campus. All switches and gateways are configured with an IP address in the management VLAN.

The connections between the core and aggregation layers are Layer 3 and consist of point-to-point interfaces using the IP address range of 172.18.X.X. Shared services such as Active Directory, DHCP, DNS, and ClearPass are connected to the services aggregation layer, which has address spaces in the 10.X.X.X range. The wireless network operates on top of the wired network using APs connected in the access switches and AOS 10 gateways dual-connected in the services aggregation switches. The physical layout of the network with switches, APs and gateways, as well as the Layer 2 and Layer 3 domains, are shown in the following diagram.

**Campus Topology**




Aruba ESP offers a breadth of services, including onboarding, provisioning, orchestration, analytics, location tracking, and management. AI Insights reveal issues before they impact users, enabling an organization to accomplish remediation tasks quickly and easily with intuitive workflow-centric navigation and views that present multiple dimensions of correlated data. Campus policies are created centrally and features such as Dynamic Segmentation enable the network administrator to implement them over an existing infrastructure.

## Planning for Deployment

Before deploying the network, it is important to identify values that can ensure consistent numbering and addressing schemes to accommodate the size of your current network, while leaving room for growth. Using a consistent approach to the physical and logical configurations streamlines network management and troubleshooting. This section provides sample values and context for choosing them. The values may require adjustment to accommodate the size of the network to be deployed.

## Central Organization

Aruba Central requires that devices are added to a group for configuration. Group configuration is managed using UI workflows and an interactive CLI editor called MultiEdit. Optionally, group configuration using a static CLI template and variable files can be enabled at the time of group creation. Enable templates only when a specific deployment use case requires them.

| Group Name | Description |
|---|---|
| SW-CORE | Core Switching - Routing services and connectivity to/from Aggregation Switching |
| SW-AGG | Aggregation Switching - Devices that connect Access Switching, handle L3 services |
| SW-ACCESS | Access Switching - Wired clients and Devices (APs, Printers, IOT) |
| WL-CAMPUS | Wireless Campus Devices - AP, Gateways |
| SW-SVCS | Services Aggregation Switching - DHCP, DNS, MRT |
| BR-SDB | Branch Sites using a Gateway (SD-Branch) - Gateway maintains VPN connections to VPN-C |
| BR-SDW | Branch Sites using a Gateway (SD-WAN) - Gateway maintains VPN connections to VPN-C |
| BR-MICRO | Branch Sites using APs only - AP maintains VPN connections to VPN-C |
| VPNC-BR | VPN Concentrators used for Branch sites - Micro and SD-Branch |

Use sites to organize devices according to the geographic location of installation.

| Site Name | Description |
|---|---|
| RSV-BLD01 | Campus Building 01 located in Roseville |
| RSV-BLD02 | Campus Building 02 located in Roseville |
| RSV-BLD03 | Campus Building 03 located in Roseville |
| RSV-DMZ | Demilitarized Zone located in Roseville |
| RSV-DC01 | Datacenter 01 located in Roseville |
| DEN-BR01 | Branch 01 located in Denver |
| SJC-BR01 | Branch 01 located in San Jose |
| WDSM-BR01 | Branch 01 located in West Des Moines |

## Device Names

Device tables within Aruba Central can be filtered and sorted by name. Establish a device naming convention that indicates the device type, role, and location to simplify the steps when a subset of devices must be analyzed within a large campus network. The examples below illustrate a naming scheme of dev type-location-role serial-unit serial.

| Device Name | Network Role | Description |
|---|---|---|
| SW-RSVDC01-CORE01-01 | Core Switch | Roseville Datacenter 1, core switch 1 |
| SW-RSVDC01-CORE01-02 | Core Switch | Roseville Datacenter 1, core switch 2 |
| SW-RSVBLD01-AG01-01 | Aggregation Switch | Roseville Building 1, aggregation switch 1, member 1 |
| SW-RSVBLD01-AG01-02 | Aggregation Switch | Roseville Building 1, aggregation switch 1, member 2 |
| SW-RSVBLD03-AG03-01 | Aggregation Switch | Roseville Building 3, aggregation switch 3, member 1 |
| SW-RSVBLD01-AC01 | Access Switch | Roseville Building 1, access switch 1 |
| SW-RSVBLD02-AC03 | Access Switch | Roseville Building 2, access switch 3 |
| GW-RSVSVC01-VPNC01 | VPNC Gateway | Roseville Services aggregation 01, VPN Concentrator 01 |
| GW-RSVSVC01-CAMPUS01 | Campus Gateway | Roseville Services aggregation 01, Campus Gateway 01 |
| AP-RSVBLD01-AG01AC01-01 | Access Point | Roseville Building 1, aggregation switch 1, access switch 1, access point 1 |
| AP-RSVBLD03-AG03AC01-01 | Access Point | Roseville Building 3, aggregation switch 3, access switch 1, access point 1 |

## IP Addressing

When a new network is deployed, it is important to take the time to design an IP addressing scheme that can adapt to the changing needs of the organization and the business it serves. Loopback interfaces on switches, DHCP pools, OSPF point-to-point links, and the routing tables that enable access across the network should be planned in a way to minimize load on operators and devices.

| IP Address Type | Description | Example |
|---|---|---|
| DHCP Pool | Devices connected to access switches. Subnets are defined by Building/Site/Agg. Subnet is injected into routing table. | 10.x.x.x/24 |
| Management Interfaces | Dedicated management network for Out-of-Band Management (OOBM) | 172.16.10.x/24 |
| VSX ISL | Only two IP addresses are needed. IPs are not injected into routing table | 10.99.99.x/30 |
| OSPF Interfaces | Each subnet needs only two IP addresses. | 172.18.10X.X/30 |

## VLAN Names and Numbers

Aruba ESP best practice is to use named VLANs. This allows the grouping of multiple VLAN numbers within a name for policy creation purposes. Choose VLAN names that describe their purpose. Establish a VLAN numbering scheme that can remain consistent through periods of growth and that can align to functional ID numbers used elsewhere in the network.

**Table 5:** Example VLAN Names used in this guide

| VLAN Name | VLAN ID | Description |
|---|---|---|
| EMPLOYEE | 3 | Authenticated employee access |
| PRINTER | 6 | LAN connected printers |
| REJECT_AUTH | 13 | Fail-through VLAN for authentication policy failures |
| MGMT_VLAN | 15 | Infrastructure device management interface VLAN |

## MAC Address Best Practices

A Locally Administered Address (LAA) should be used any time a MAC address must be configured. An LAA is a MAC that looks like one of the four examples below:

```
x2-xx-xx-xx-xx-xx
x6-xx-xx-xx-xx-xx
xA-xx-xx-xx-xx-xx
xE-xx-xx-xx-xx-xx
```

The x positions can be any valid hex value. It is helpful to create a binary representation of the associated VLAN ID using the hex positions. For more details on the LAA format, see the IEEE Tutorial Guide.

## HPE GreenLake

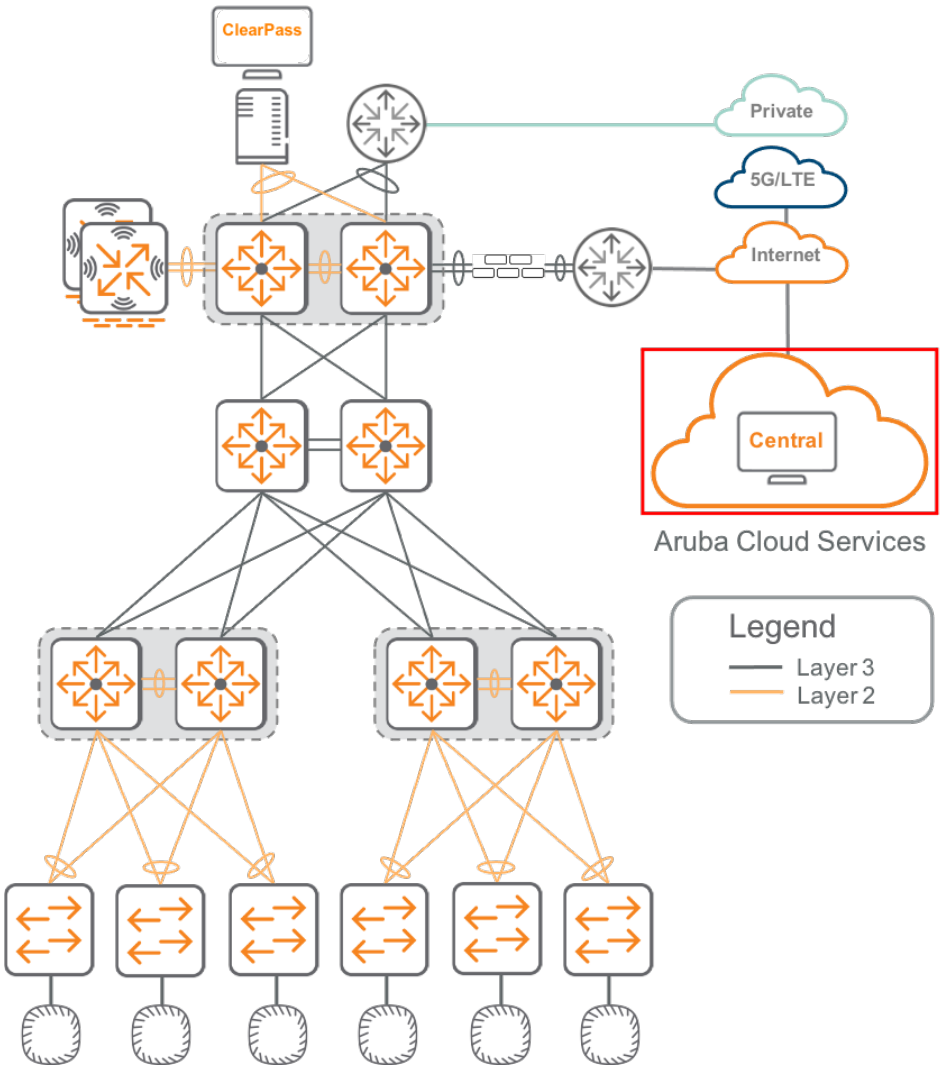
HPE GreenLake is a cloud based platform that brings a unified experience to apps and data everywhere while providing one IT operating model to orchestrate across edges, colocations, data centers, and multi-cloud. Using Aruba Central with HPE GreenLake provides a single, versatile platform to view and orchestrate critical network services along with data and compute services. Devices must be added to GreenLake with an active linked subscription to use Aruba Central. For more information on onboard devices and subscriptions, refer to GreenLake Platform .

## Aruba Central

Aruba Central, originally a standalone cloud application, has been integrated seamleassly into HPE GreenLake. This integration yields a significant enhancement in operation efficiency and resource management. Central's intuitive health dashboards and user-friendly management interface can be accessed quickly by clicking the Aruba Central icon on the HPE GreenLake dashboard.

This section provides details for configuring Aruba Central to prepare for a Campus deployment. A group must be created to configure devices with the same role, and a site must be established to monitor devices belonging to the same location, ensuring that a device is provisioned with both a group and site.

**Aruba Central**




## Go to Aruba Central from GreenLake

The following procedure guides the user to open an Aruba Central Instance from GreenLake home-page.

**NOTE:**

A central instance must be added to the company workspace before launching it.

**Step 1** Login to GreenLake and select the workspace.

**Step 2** Click the **Services** tab on the top.


**Figure 1:** services

**Step 3** Click **Launch** on Aruba Central.


**Figure 2:** launch

## Create New Groups

Aruba Central uses group and device levels for configuration tasks. A device's final configuration comprises configurations applied at both the group level and the device level. Parameters changed at the device level override the configuration inherited from the group level. Recommended best practice is to enter changes at the device level only when required, such as when configuring an IP address or name of the device. Most changes should be made at the group level to reduce configuration time and to ensure configuration consistency across the network.

**NOTE:**

A device must be provisioned to a group and assigned a license in order to receive configuration from Central.

The following procedure creates a group. This group can then be used to configure devices that have the same role.

**Step 1** Go to **Aruba Central** home page, and set the filter to **Global**.

**Step 2** On the left navigation pane in the **Maintain** section, select **Organization**.

**Step 3** Select the **Groups** tile.

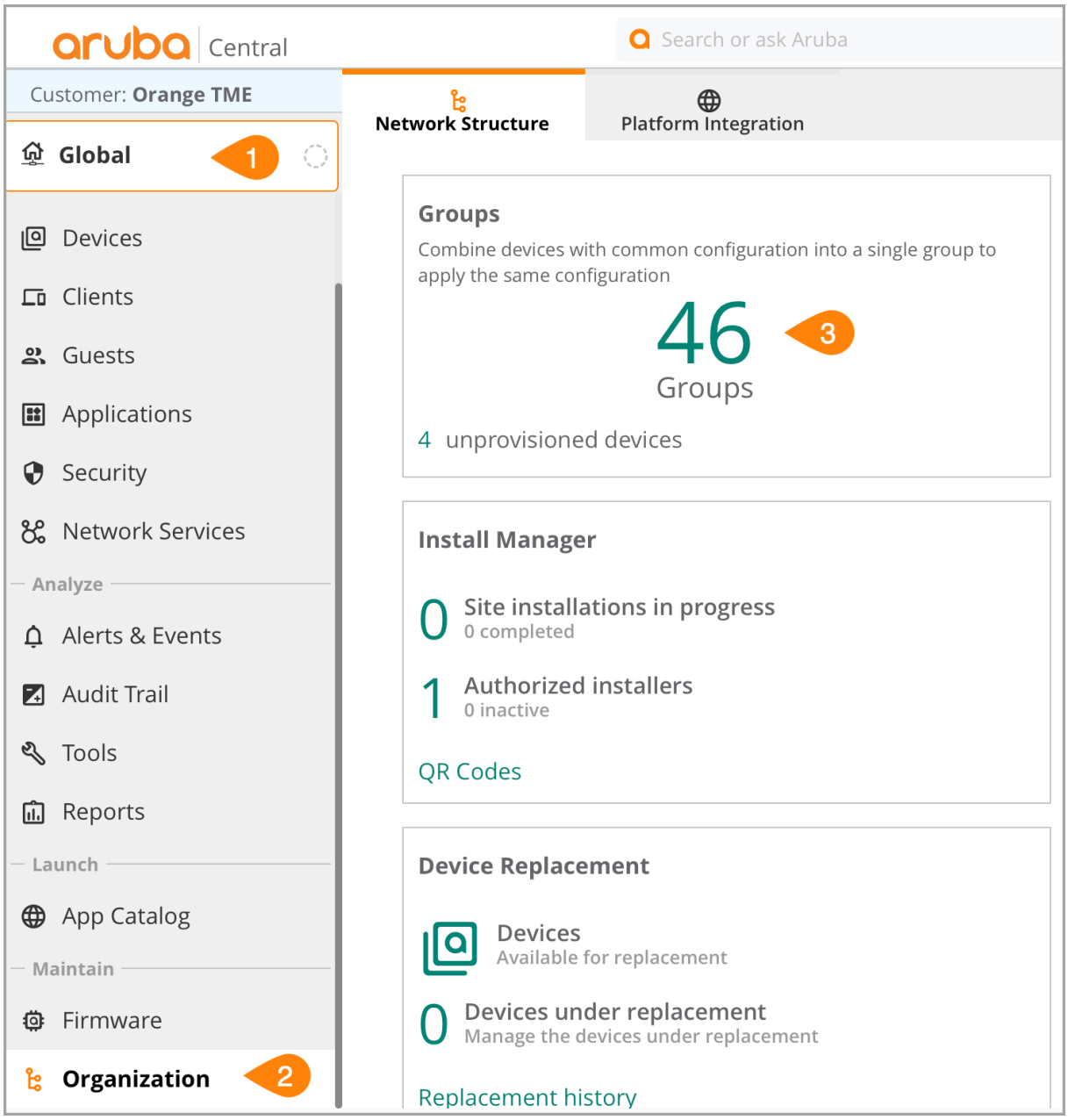



**Figure 3:** organization_group

**Step 4** Click the **+** (plus sign) to create a new group.


**Figure 4:** plus

**Step 5** Enter a **Name** for the group. Enable the toggle for **Make this group compatible with New Central**, select the appropriate checkbox in the **Group will contain** list, then click **Next**. Sample group details are:

- **Name:** *BDG9-AGG01*

- **Make this group compatible with New Central**: toggle button
- **Group will contain:** *check-mark*


**Figure 5:** add_group

**NOTE:**

For detailed instructions on how to create a template and custom variables, consult the Creating a Configuration Template section in Central online help.

**Step 6** Click **Add**.


**Figure 6:** switch_type_select

**NOTE:**

When **Access points** and **Gateways** are selected in the previous step, select the Architecture and Network role for the device types.

**Step 7** Repeat this procedure to create all required groups.

## Set the Group Password

**Step 1** Go to **Aruba Central** and set the filter to **Global**.

**Step 2** On the left navigation pane, select **Organization** in the **Maintain** section.

**Step 3** Select the **Group** tile and click **Go to config** .

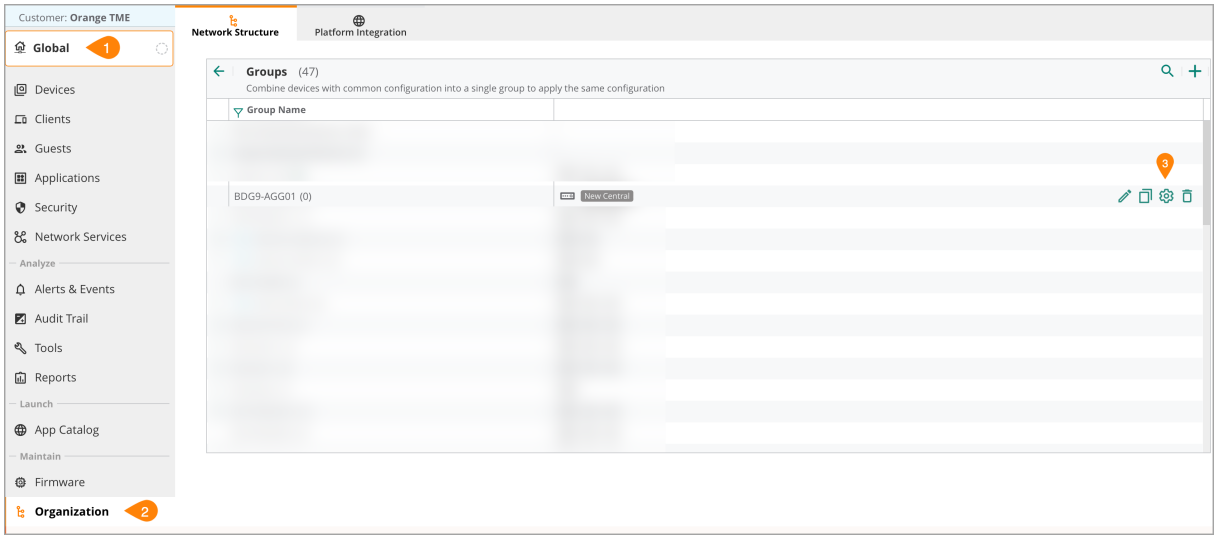



**Figure 7:** device_config

**Step 4** Provide the password. Click **Save**.


**Figure 8:** password

**NOTE:**

A device-specific Administrator password can be set at the device level of Central. To setup passwords for Access Points and Gateways, select the device tab and click to the **config** (gear) button at the top right.

## Create New Sites

Central Groups define a set of devices with shared configuration, while sites define a set of devices with a shared location. Use sites to monitor and analyze the network, and use groups to configure similar devices. Like groups, sites are created in the **Organization** navigation pane. At least one site should be defined to allow Central to generate accurate topology and reporting data.

**Step 1** Go to Aruba Central **Account Home** page, and set the filter to **Global**.

**Step 2** On the left navigation pane, select **Organization** in the **Maintain** section.

**Step 3** Click the **Sites** tab.

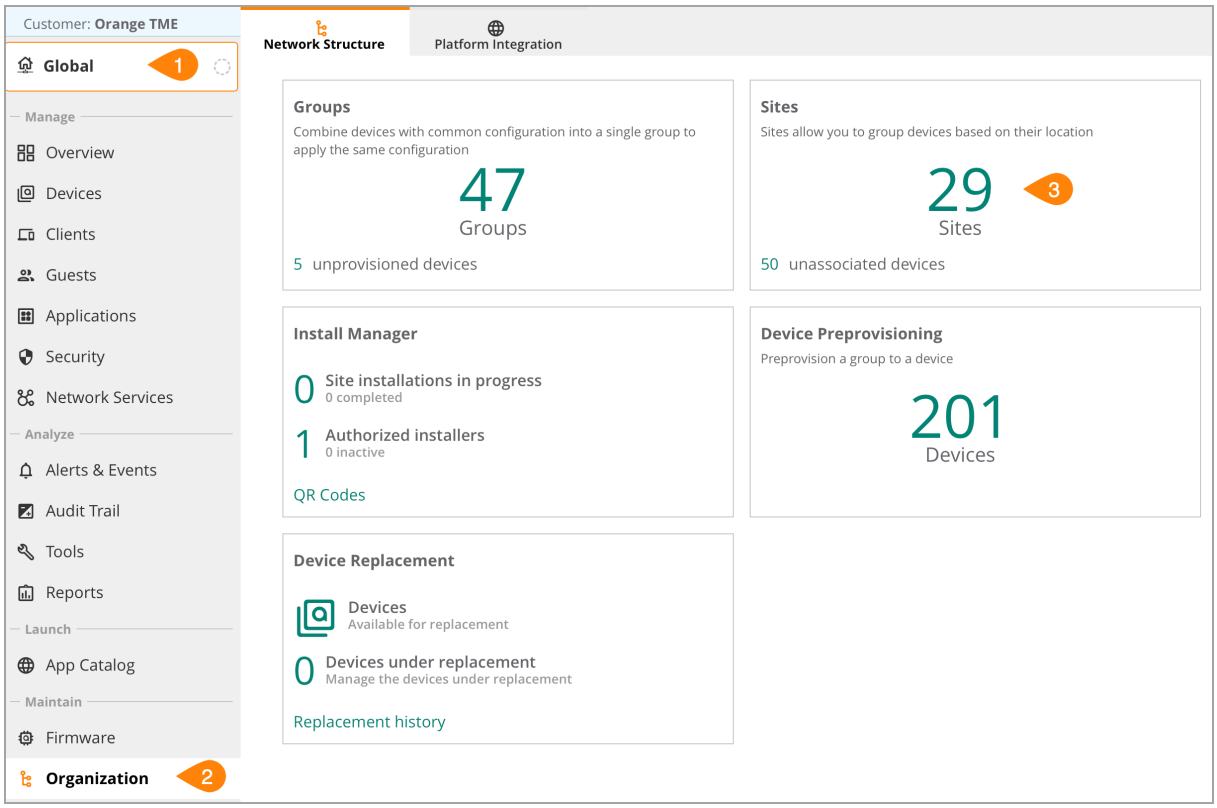



**Figure 9:** select_site_tab

**Step 4** At the bottom, click **New Site**.


**Figure 10:** new_site

**Step 5** In the **Create New Site** window, provide the site details and click **Add**. Sample the site details are shown below.

- **Site Name:** *EXAMPLE SITE*
- **Street Address:** *123 Any Street*
- **City:** *Santa Clara*
- **County:** *United States*
- **State or Province:** *California*
- **Zip/Postal Code:** *95054*

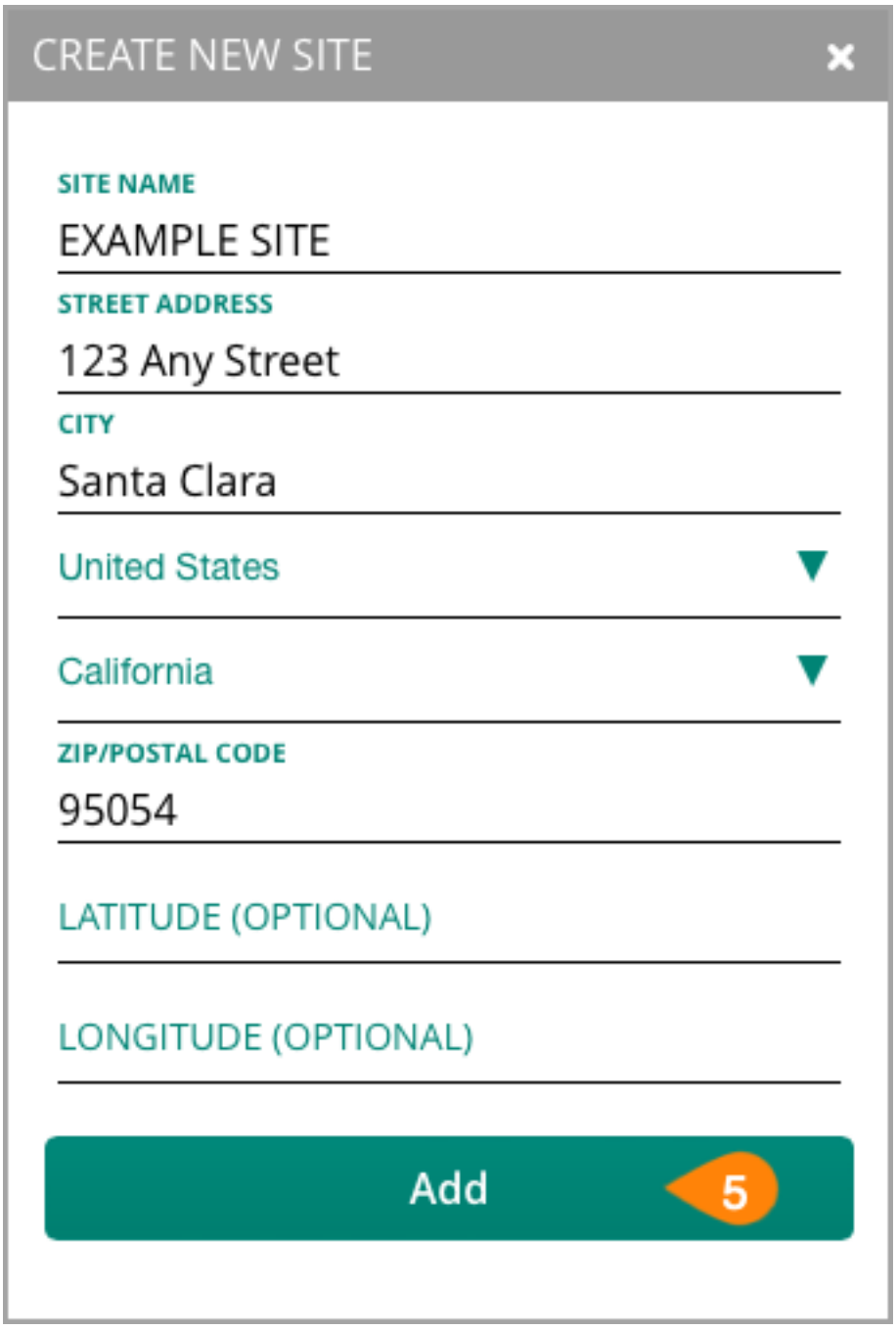



**Figure 11:** site_form

**Step 6** Repeat this procedure to create each required site.

## Manage Firmware Compliance

Enable firmware compliance to ensure that devices in a group are maintained at the same firmware level, starting when the device is first added to the group. Aruba recommends running the latest updated firmware for the initial deployment.

**Step 1** Go to the **Aruba Central** home page, and set the filter to the appropriate group.

**Step 2** On the left navigation pane, select **Firmware** in the **Maintain** section.

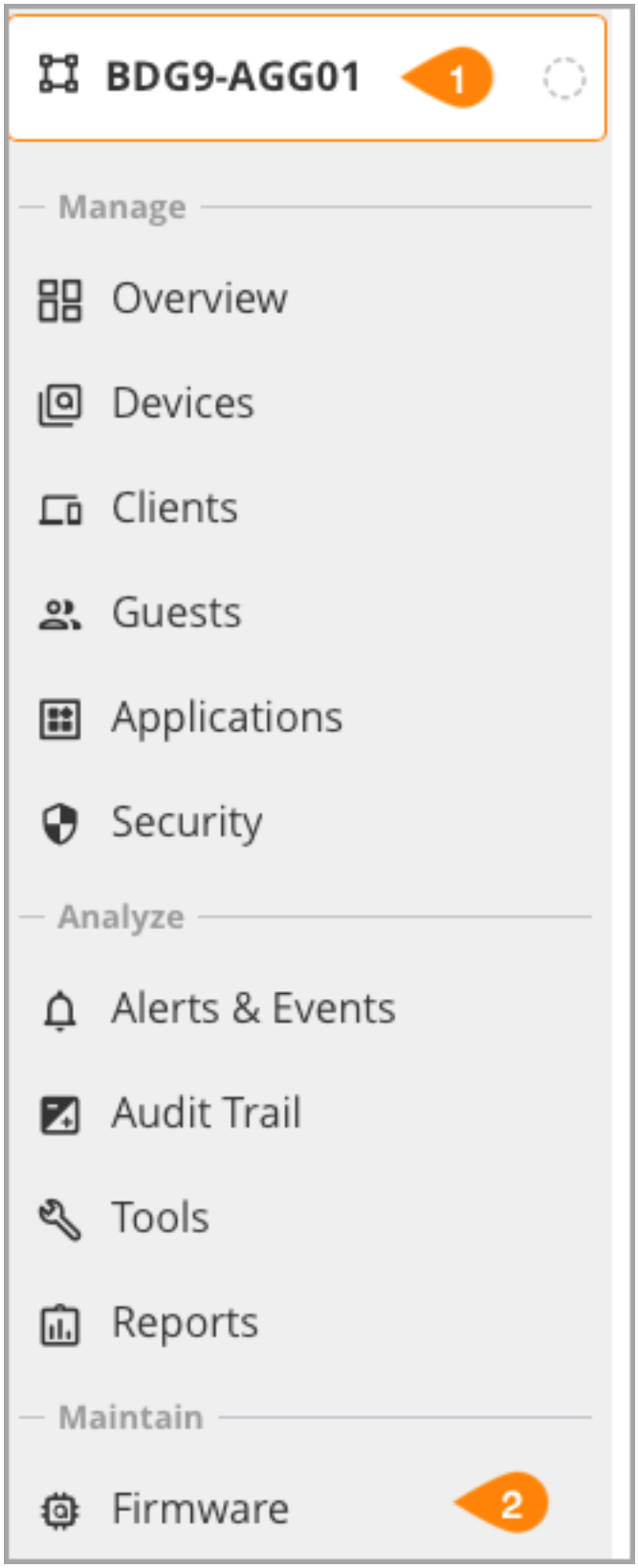



**Figure 12:** firmware

**Step 3** On the **Access Points** page at the top right, click **SET COMPLIANCE**.

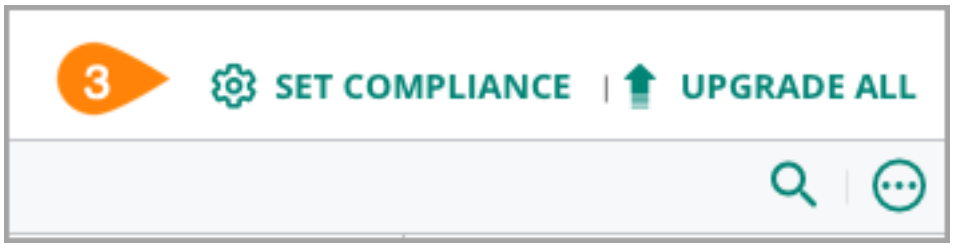



**Figure 13:** set_compliance

**Step 4** On the initial window, click the **Set firmware compliance** slider.

**Step 5** Provide the firmware details, then click **Save**. Sample firmware details are shown below.

- **Groups:** *EXAMPLE-GROUP*
- **Firmware Version:** *Latest Recommended*
- **Upgrade Type:** *Live*
- **When:** *Now*

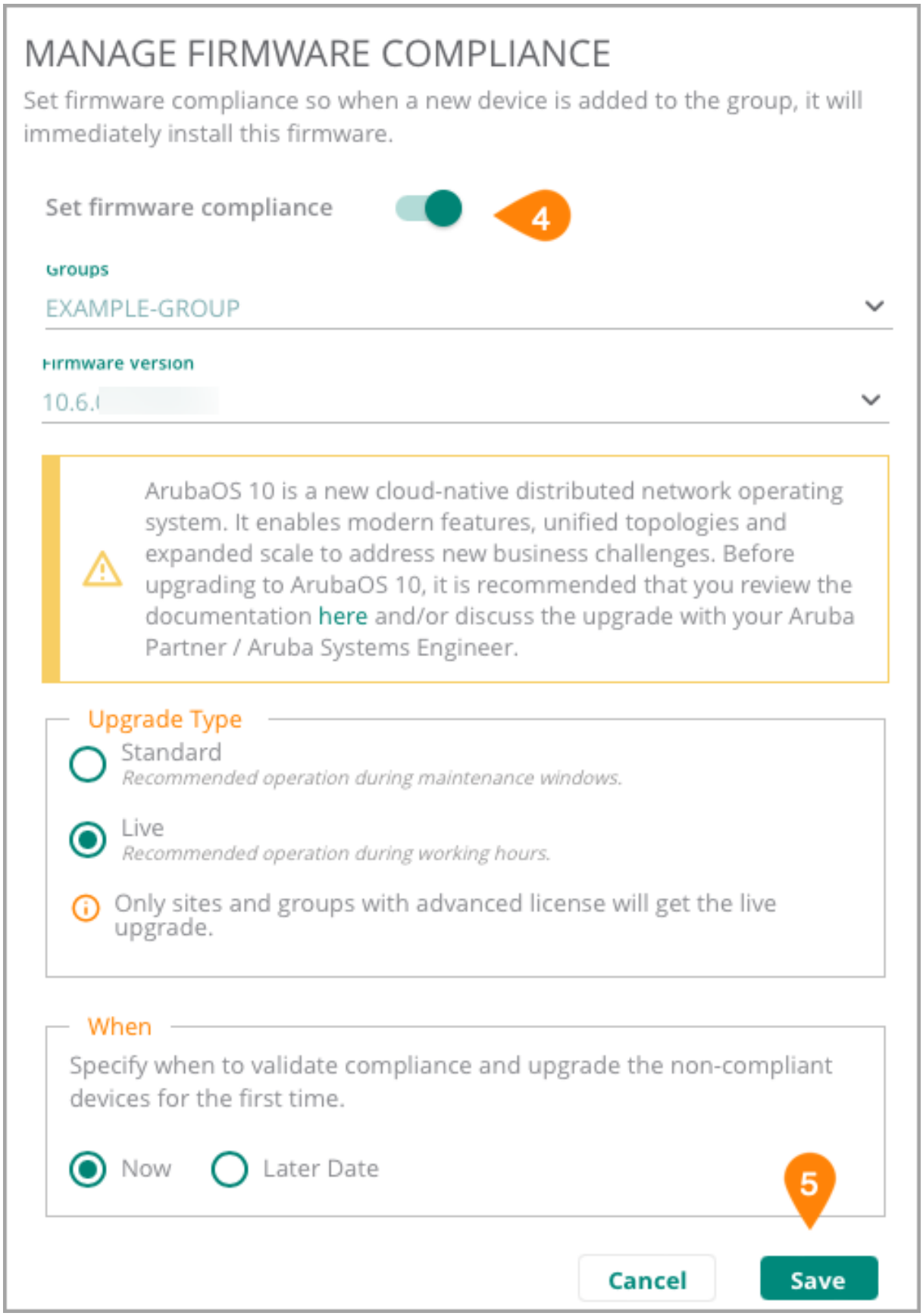



**Figure 14:** Firmware-Set-Compliance-On-Group

**Step 6** Repeat this procedure for all groups.

## Provision a Device in a Group

This procedure outlines the steps to add a device to a central group for configuration deployment.

**Step 1** Go to the **Aruba Central** home page, and set the filter to **Global**.

**Step 2** On the left navigation pane, click **Organization** in the **Maintain** section.

**Step 3** Click the **Groups** tile.

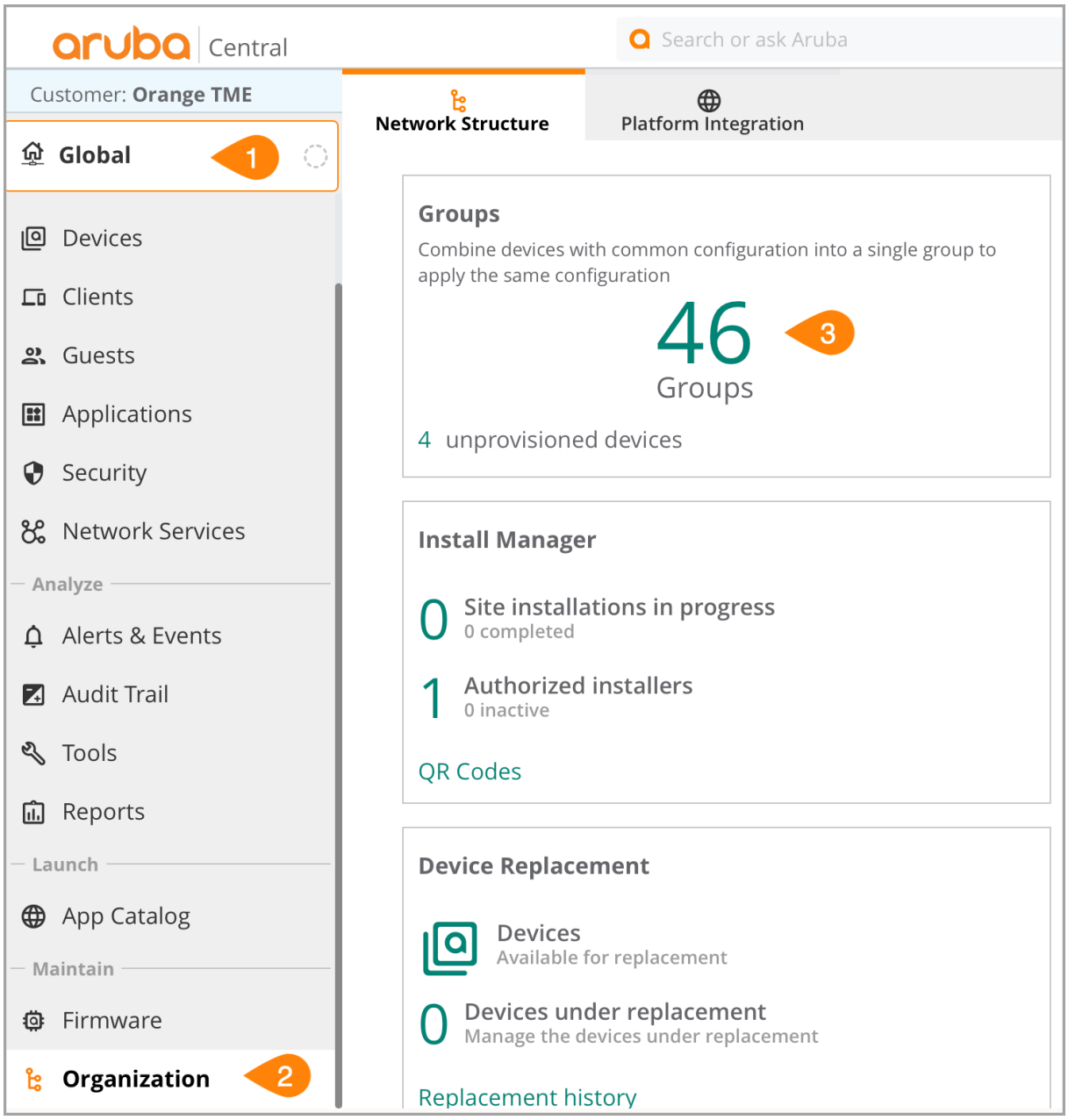



**Figure 15:** organization_group

**Step 4** Select **Unprovisioned Devices**, then select the device(s) to be pre provisioned.

**Step 5** Click the **provision** button.

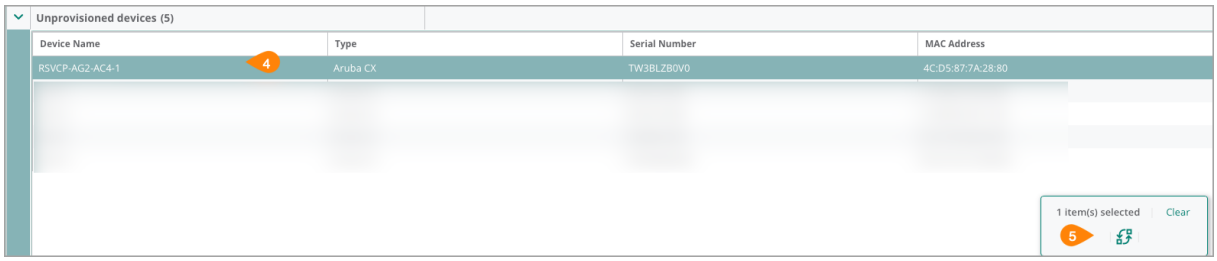



**Figure 16:** provision

**Step 6** Select the **Destination group**, then click **Move**.

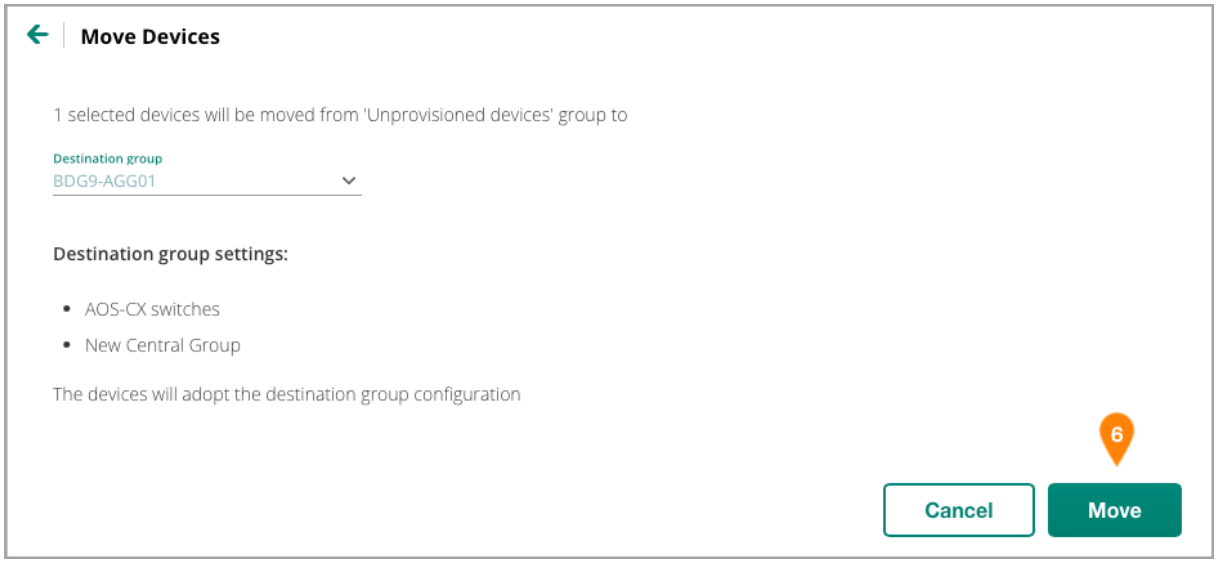



**Figure 17:** move

## Provision a Device in a Site

This procedure outlines the steps to add a device to a site for monitoring.

**Step 1** Go to the **Aruba Central** homepage, and set the filter to **Global**.

**Step 2** In the **Maintain** section, select **Organization**.

**Step 3** Click the **Sites** tile.

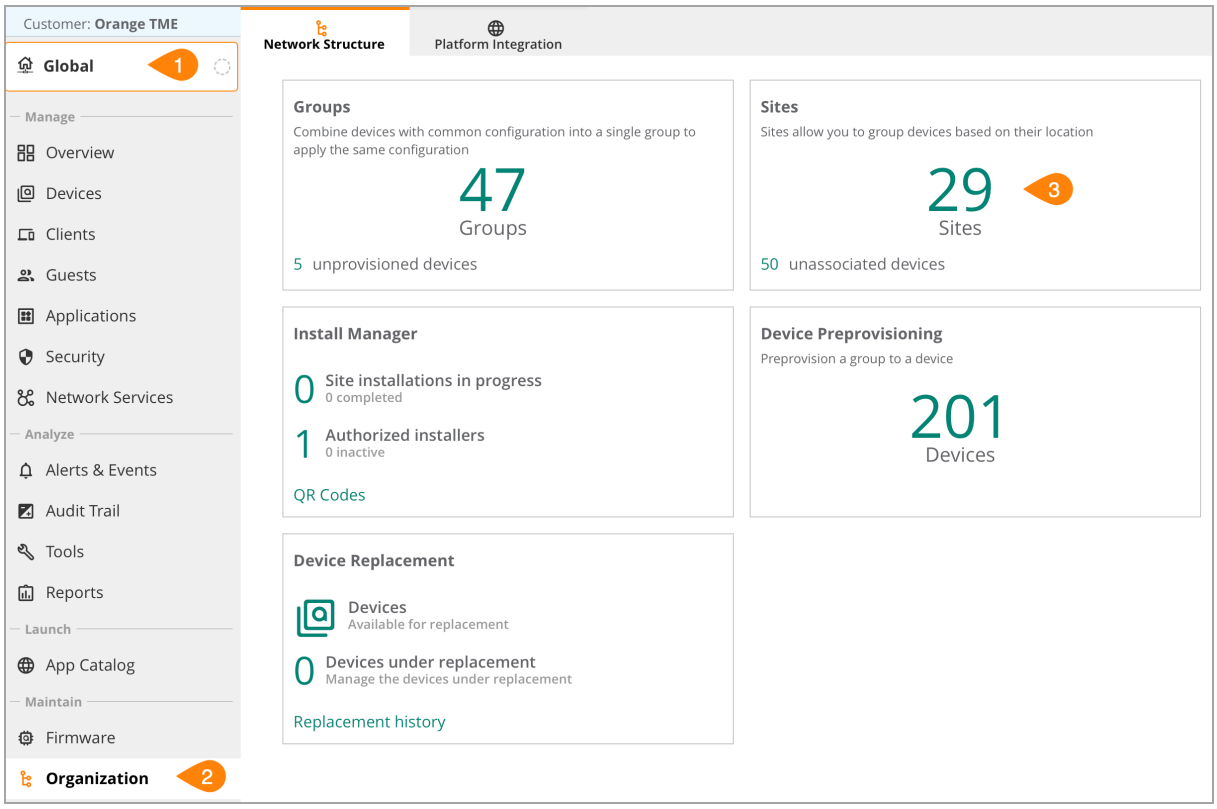



**Figure 18:** select_site_tab

**Step 4** Select the device(s) to move and drag the device to the corresponding **site**.

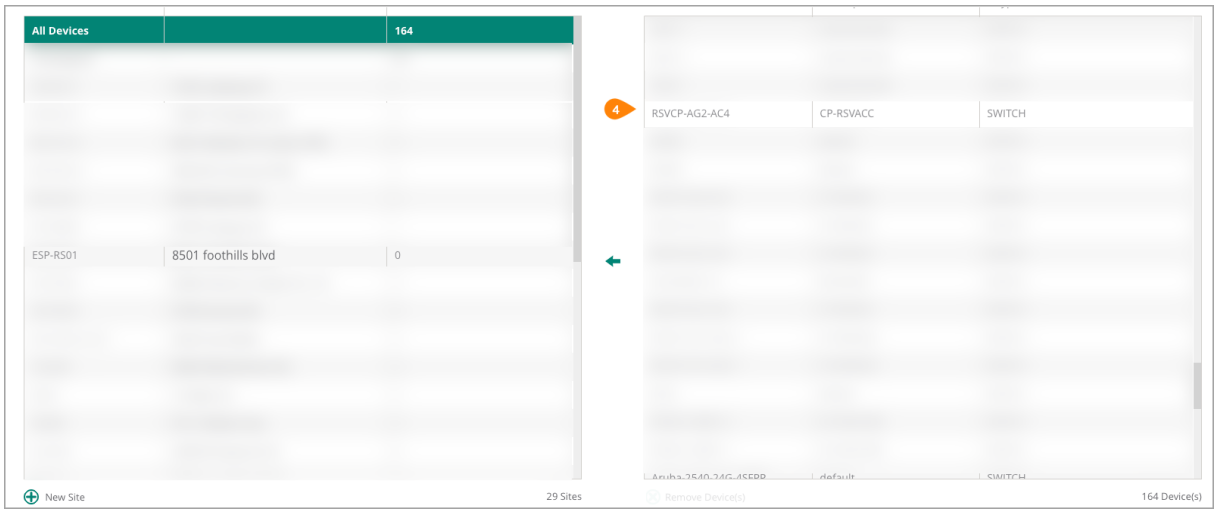



**Figure 19:** select_device

**Step 5** Click **Yes** to confirm the move.


**Figure 20:** confirm_action

# Campus Wired Connectivity

The Aruba CX switching portfolio provides a range of products for use in core, aggregation, and access layers of the campus. Aruba switches are built using a cloud-native operating system called AOS-CX. To achieve increased network resiliency and facilitate automation, AOS-CX implements a database-centric operational model. With features such as always-on PoE, Virtual Switching Framework (VSF) for access stacking, and Virtual Switching Extension (VSX) for core and aggregation redundancy, organizations can rely on Aruba CX switches for mission-critical requirements throughout the campus.

Aruba ESP for Campus offers several two-tier and three-tier designs to meet the requirements for organizations of any size. Larger organizations and those that require a flexible foundation for growth typically follow a 3-tier approach using a layer-3-only dedicated core, an aggregation layer that provides default-gateway services connected via routed links to the core, and an access layer connecting wired devices and wireless access points. Access switches typically are stacked using VSF; aggregation and core switches are paired using VSX. Access switch stacks cross-connect to aggregation pairs using Aruba's multi-chassis link aggregation (MC-LAG) capability within VSX to ensure non-blocking, fault tolerant uplink capacity.

# Preparing Campus Switches

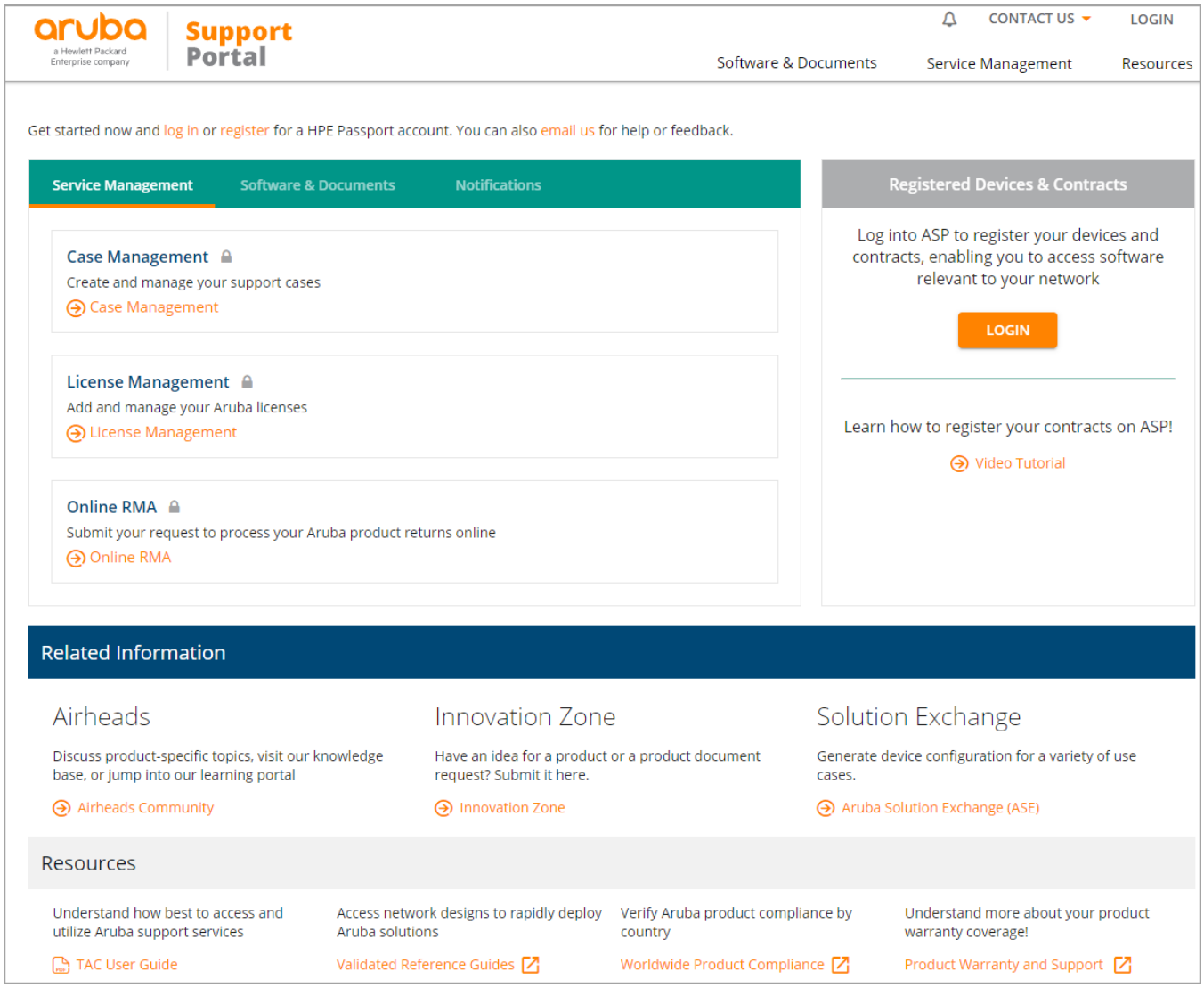
Following initial unboxing and inventory, the next step in deploying a campus network involves the physical installation of the switches. At the core and aggregation layers, verify the airflow configuration for the products to be installed to make sure they support the cooling design of the installation location. At the access layer, ensure that sufficient power and cooling are provided for the planned endpoint density and power requirements. Rack space, mechanical fasteners, patch cables, and optics or DACs are critical components to have on-hand before initiating physical installation.

## Switch Installation

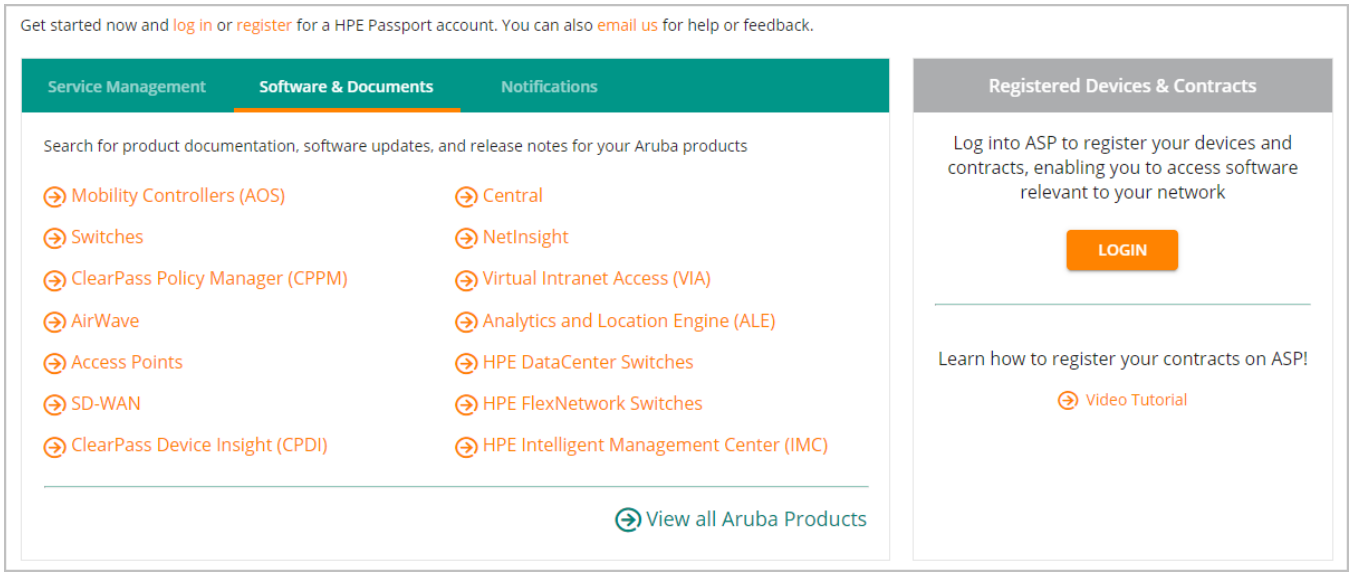
Before installing the switches, download the Aruba Installation Guide for the specific model to be deployed. Review the requirements for power, cooling, and mounting, and ensure that the required infrastructure is available at each location where campus switches will be installed.

**Step 1** Open a web browser and navigate to the Aruba Support Portal at https://asp.arubanetworks.com/.

**Step 2** On the **Support Portal** page, select the **Software & Documents** tab.



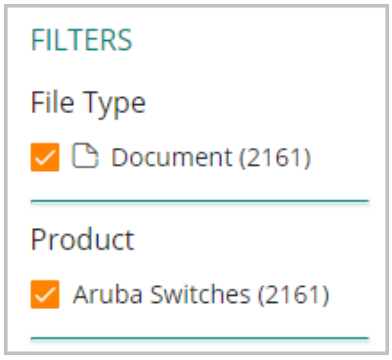

**Step 3** On the **Software & Documents** tab, select **Switches**.



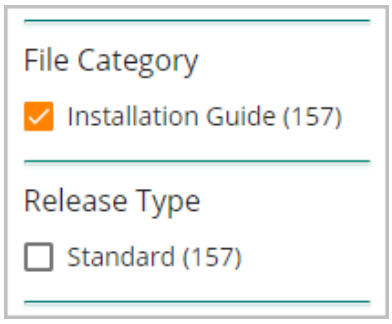

**Step 4** Select the filter options on the left.

- **File Type:** *Document*

- **Product:** *Aruba Switches*




- **File Category:** *Installation Guide*




**Step 5** Download the Installation Guide version for the switch model to be installed.

**Step 6** Complete the physical installation of switches in the racks.

**NOTE:**

Installation locations have a range of infrastructure limitations and standards. Ensure that the equipment to be installed is compatible with those parameters. If not, consult with Aruba TAC or a local SE.

**NOTE:**

In many cases, initial configuration of a switch can be completed and validated prior to permanent physical installation. Consider if a “bench configuration” methodology is appropriate to the deployment.

## Physical Cabling

Consistent port selection across the campus switching infrastructure results in increased ease of configuration management, monitoring, reporting, and troubleshooting tasks throughout the network. Document all connections and ensure that distance limitations are observed for endpoint connections, AP connections, and between switches. In most cases, a structured cabling vendor should be consulted.

In large campus environments, the ESP network may be deployed in phases. For each phase, complete all layer 1 interconnects between switches before beginning the configuration process in Central.

## Switch Profiles and Interface Groups

Aruba CX 8xxx model switches have configurable hardware that addresses a range of performance requirements at the core and aggregation layers of a campus network.

- *Switch profiles* assign system resources strategically for the deployed role. Campus-specific switch profiles include core and aggregation roles. Refer to the “Hardware forwarding table commands” section of the model-specific Aruba CX Fundamentals guide for feature details.
- *Interface groups* allocate switch ports for features that must be enabled on a group of ports at the same time. Port speeds on 8325 (all ports) and 8360-32Y4C (ports 1-4) switches are configured as port groups. In both cases, the default port speed is 25 Gb/s and must be set to 10 Gb/s to support transceivers of that speed. Refer to the “Network Ports” section of the model-specific Aruba CX Switch Series Installation and Getting Started Guide for complete, model-specific details.

## DHCP

A new switch must receive an IP address, DNS server address, and a default gateway via DHCP in order to connect with Central for successful Zero Touch provisioning.

In some settings, it may be desirable to reserve an IP address for each switch on a DHCP server. This ensures a predictable IP address for local management connections, such as SSH, while also enabling the switch to contact Aruba Central immediately on boot.

When switches are unpacked and prepared for bench configuration or rack mounting, access the orange luggage tag on the switch and record the base MAC address. The MAC address of the management interface is the base MAC + 1. For example, 02:00:00:00:00:00 becomes 02:00:00:00:00:01. Use this management MAC address for a DHCP reserved lease configuration.

## Switch Group Configuration

The following procedures configure a Central switch group with the base features required for all switches in the network. Repeat this procedure for each switch group in the network.

Group-level configured features include the host name, admin account password, Network Time Protocol (NTP), Domain Name System (DNS), Terminal Access Controller Access Control System (TACACS), and Authentication, Authorization, and Accounting (AAA) servers.

### Configure the UI Group Settings

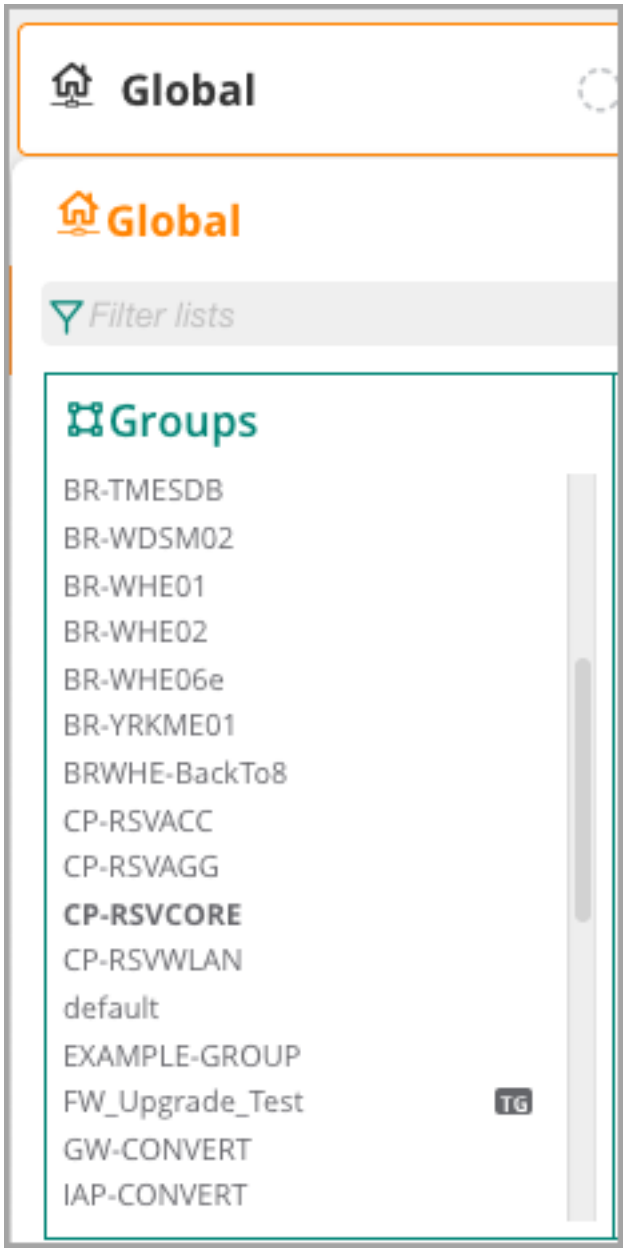
Use this procedure to configure group settings for switches. An HPE GreenLake account is required in order to access Aruba Central.

**NOTE:**

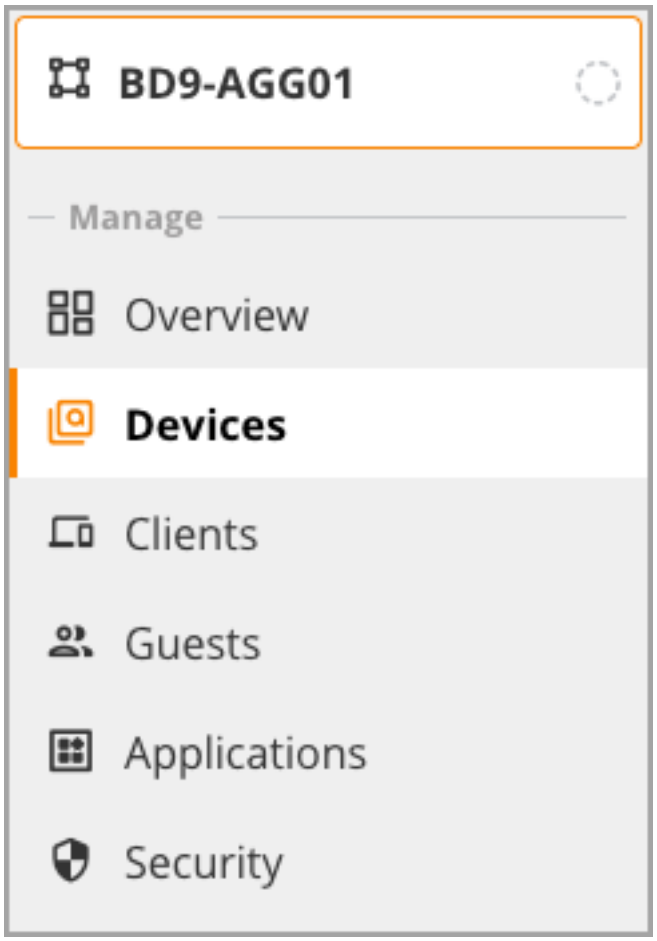
Best practice is to use the fewest groups necessary to provide logical organization for the network and consistent configuration between devices. Configuration cannot be shared among groups.

**Step 1** Login to HPE GreenLake and launch **Aruba Central**.

**Step 3** In the filter dropdown, select a switch group. In this example, the group is **CP-RSVCORE**.

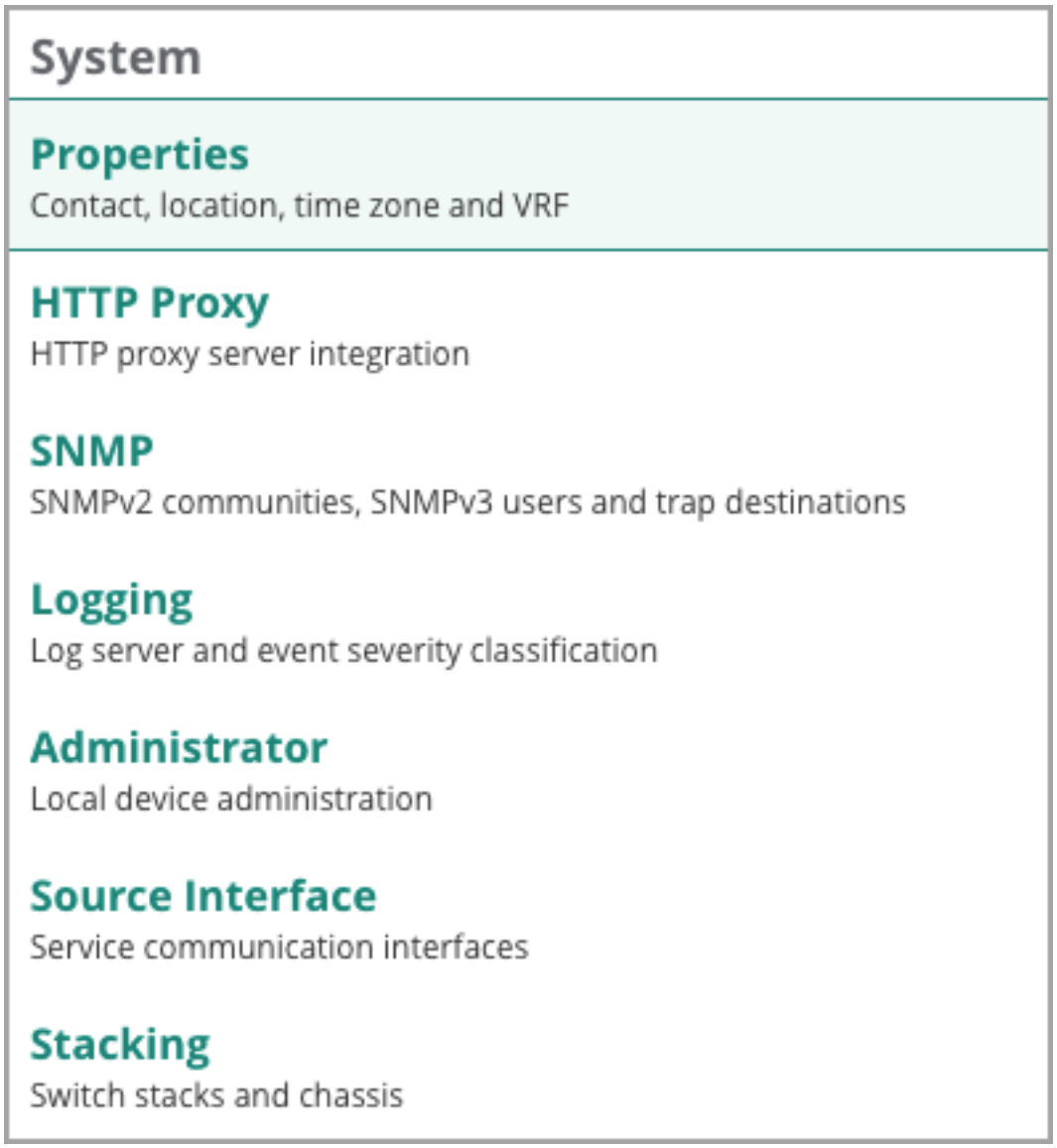



**Step 4** On the left menu, select **Devices**.

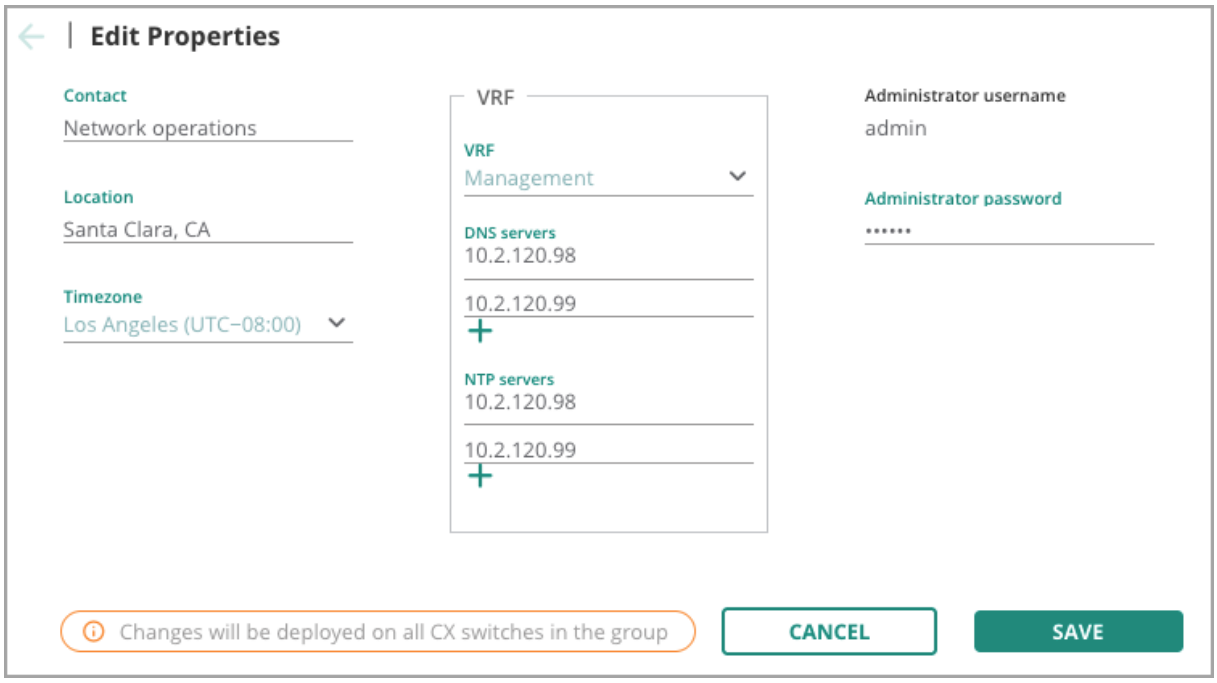



**Step 5** In the upper right of the **Switches** page, select **Config**.

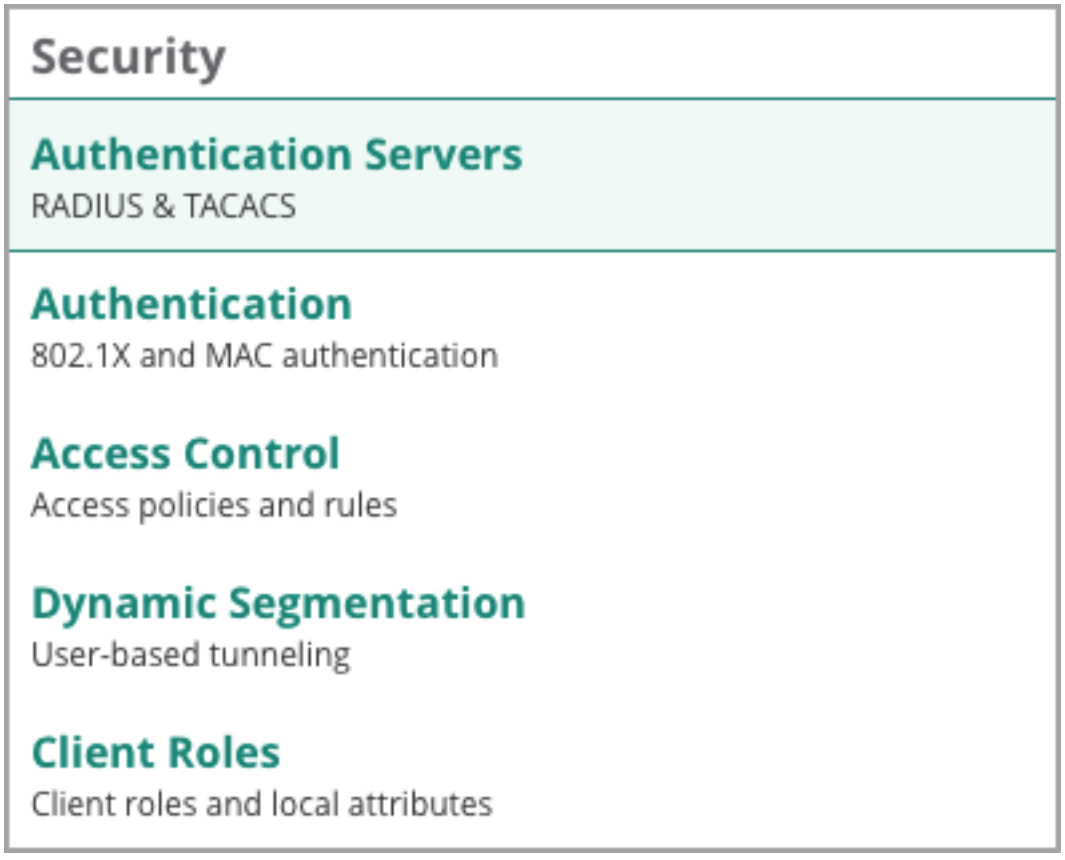

**Step 6** In the **System** tile, select **Properties**.



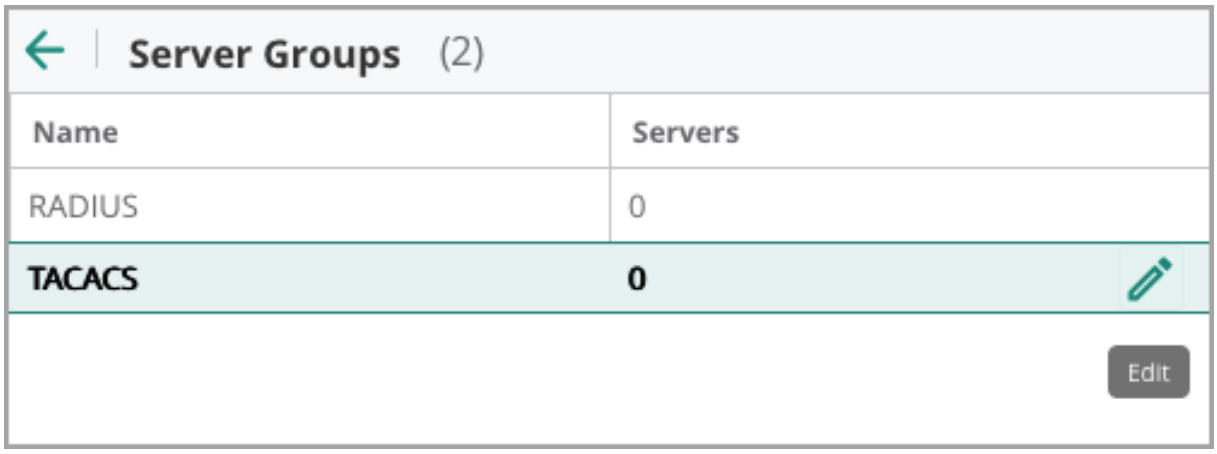

**Step 6** On the **Edit Properties** page, assign the following settings, then click **Save**. Set the VRF to the default network where DNS and NTP will be reachable. Enter a complete IP address to make the **+** (plus sign) appear for adding additional servers. - **Contact:** *Network operations* - **Location:** *Santa Clara, CA* - **Timezone:** *Los Angeles (UTC-8:00)* - **VRF:** *Management* - **DNS servers:** *10.2.120.98, 10.2.120.99* - **NTP servers:** *10.2.120.98, 10.2.120.99* - **Administrator username:** *admin* (static) - **Administrator password:** *password*




**Step 7** In the **Security** tile, select **Authentication Servers**.

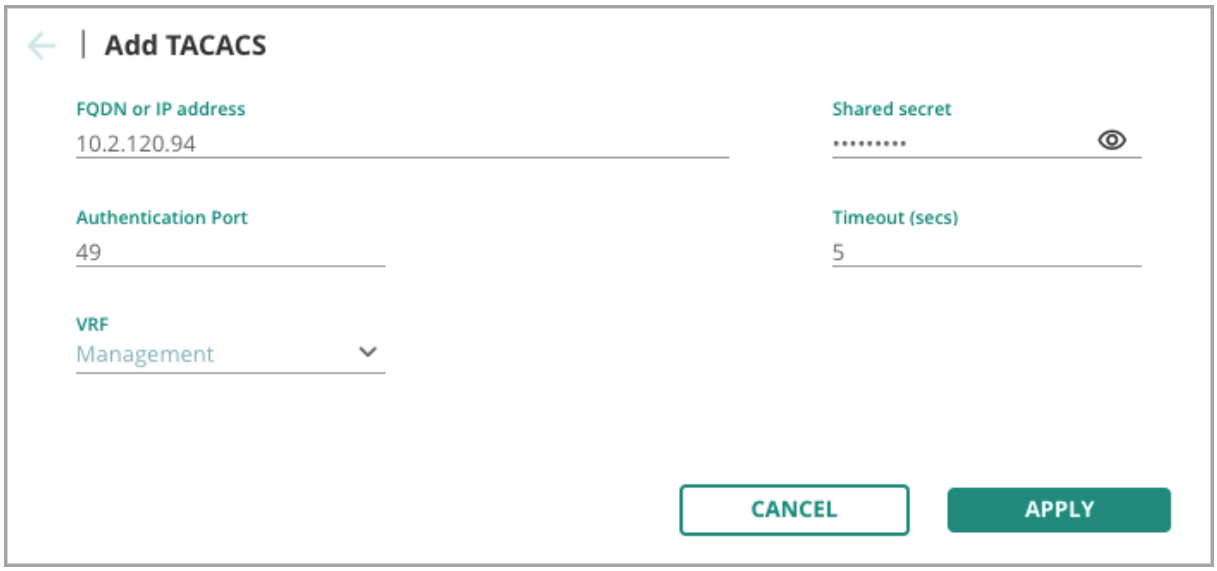



**Step 8** Mouse-over the TACACS row. At the far right, click the **Edit** (pencil) icon.




**Step 9** At the top right corner of the **TACACS Servers** table, click the **+** (plus sign), assign the following settings on the **Add TACACS** page, then click **Apply**.

- **FQDN or IP address:** *10.2.120.94*
- **Authentication Port:** *49* (default)
- **VRF:** *Management*
- **Shared secret:** *secret*
- **Timeout (secs):** *5* (default)



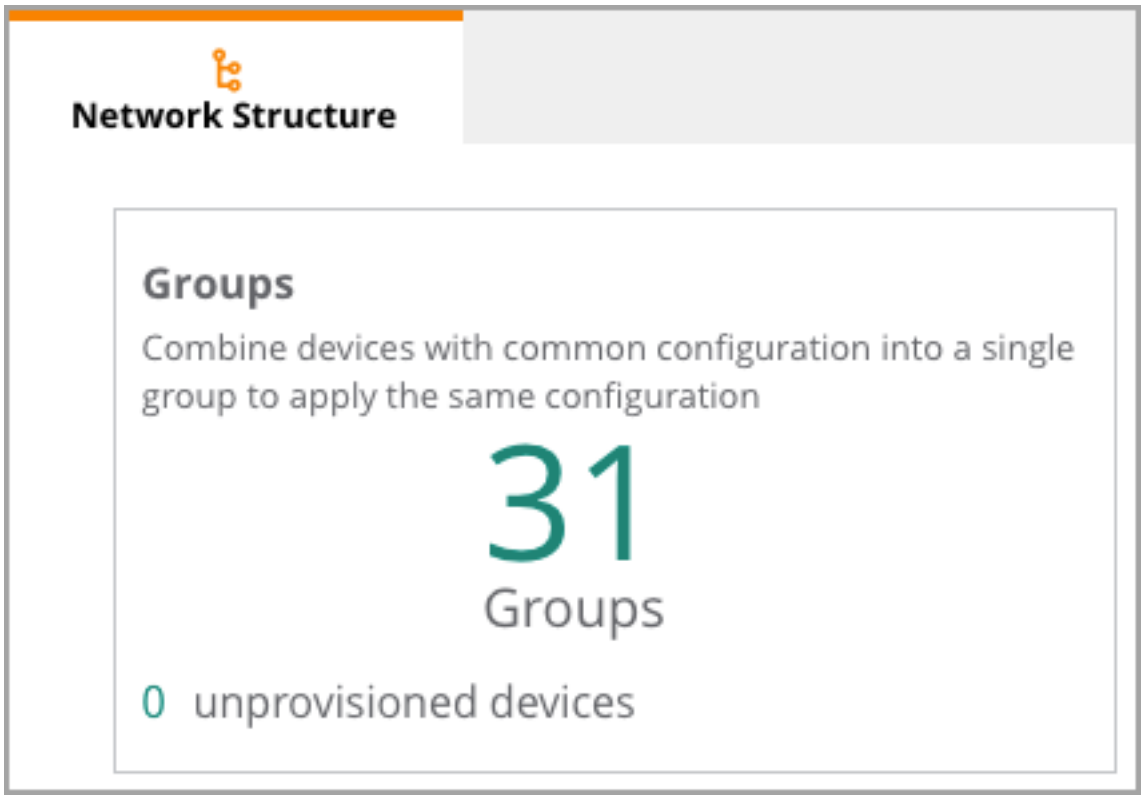

**Step 10** Add additional servers by clicking the **+** (plus sign) on the top right corner of the **TACACS Servers** table. After all servers are added, click **Save**.

## Add Switches to the Group

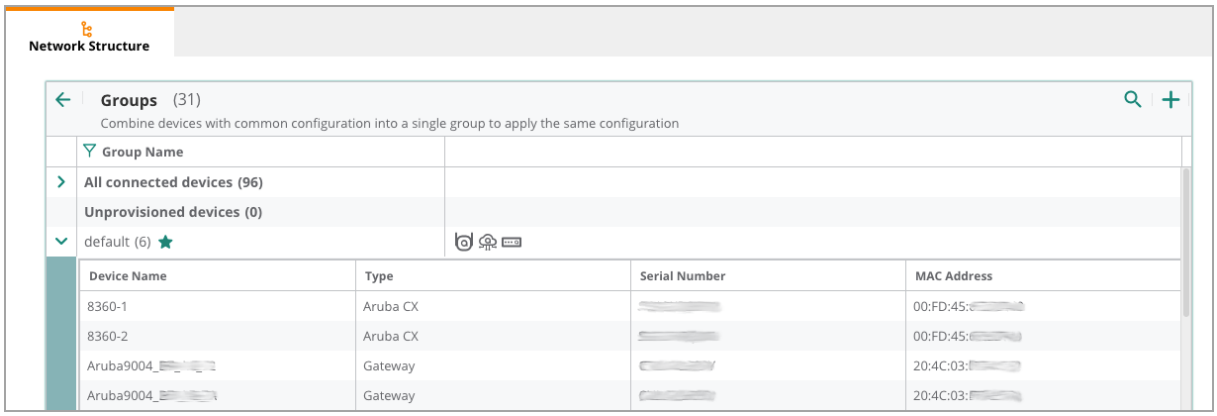
Use this procedure to assign switches to groups and synchronize initial configuration.

**Step 1** In the filter dropdown, select the **Global** group. On the left menu, select **Organization**.

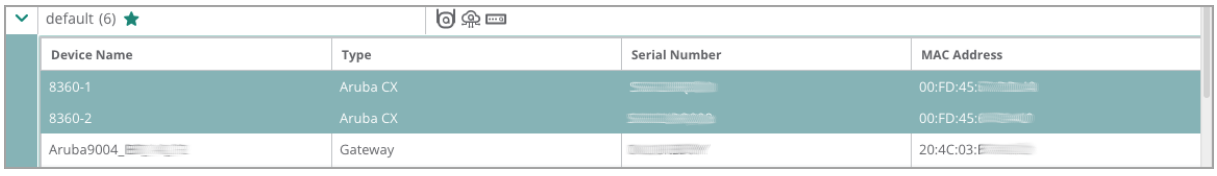
**Step 2** Select the **Groups** tile.



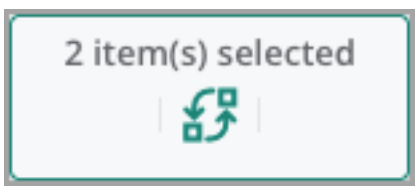

**Step 3** Expand the **> default** Group section.



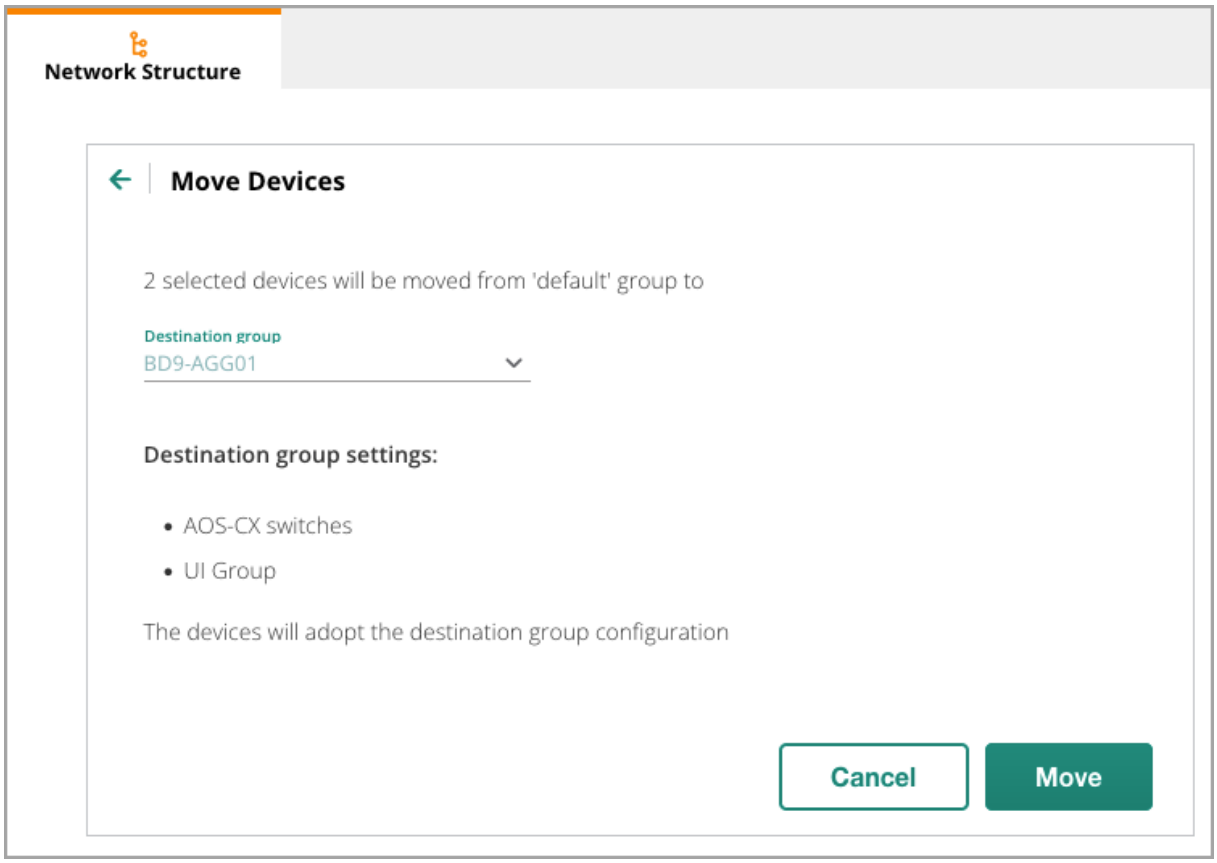

**Step 4** Select the switches to be moved.




**Step 5** In the lower right corner of the **default** Group table, begin the switch move by clicking the **Move** button.




**Step 6** Select the appropriate destination switch group for the selected switches, then click **Move**.



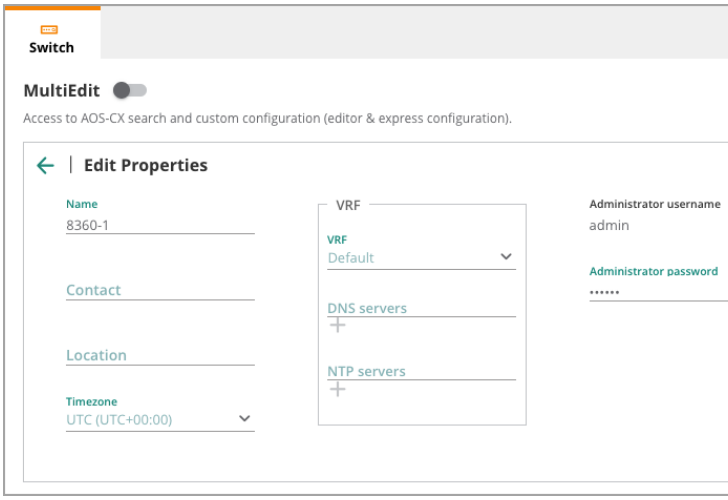

**Step 7** Confirm the move on the devices view of the destination group.

## Configure the Switch Hostname

**Step 1** In the filter dropdown, select the destination group from the preceding step. On the left menu, select **Devices**.

**Step 2** Click the **Device Name** of a recently added switch. On the left menu, select **Device**.

**Step 3** In the **System** tile, click **Properties**.




**Step 4** In the **Name** field, enter a hostname for the switch.

**Step 5** Repeat this procedure for each switch in the Group.

## Create a Template Group

Occasionally a configuration template is used to initialize the network devices to be onboarded to Central. This is accomplished by adding the new device to a Template Group. A configuration template and variables file are then associated with the group and applied to each device added to the group.

For detailed instructions on how to create a template and custom variables, consult the Creating a Configuration Template for Gateways section of the Central online help.

### *Configure the Template Group*

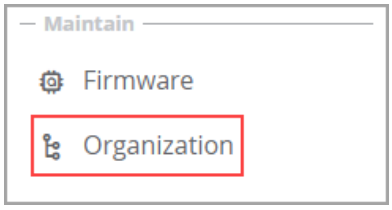
Use this procedure to create a template group.

When using a template group to configure core switches, consider creating a template group for each core switch because they have unique IP address on each interface and a single template is difficult to maintain with a long list of variables.

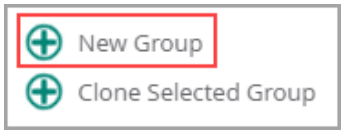
**Step 1** Navigate to **Central** and login using administrator credentials.

**Step 2** On the Aruba Central Account Home page, launch the **Network Operations** app.

**Step 3** On the left navigation pane in the **Maintain** section, select **Organization**.

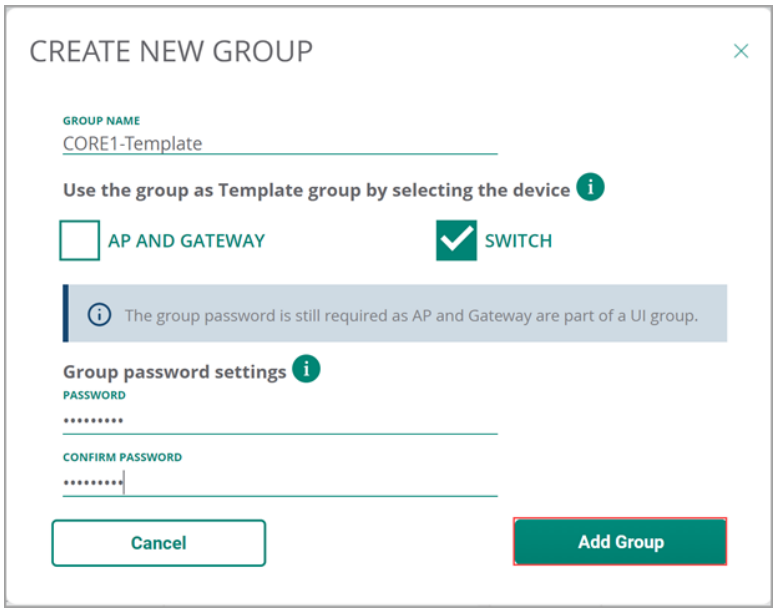



**Step 4** On the **Groups** page in the Manage Groups section, select **New Group**.




**Step 5** On the **Create New Group** page, assign the following settings, then click **Add Group**.

- **GROUP NAME:** *CORE1-Template*
- **SWITCH:** *checkmark*
- **PASSWORD:** *password*
- **CONFIRM PASSWORD:** *password*

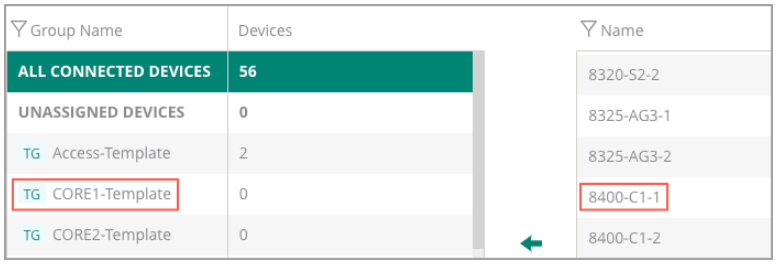



**NOTE:**

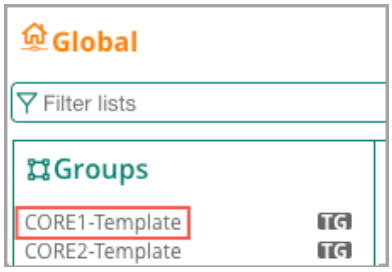
The password enables administrative access to the device's interface. This password is used as the login password for all the devices in the group, but it is not the enable password. The same password can be used across multiple groups.

### *Add Switches to a Template Group*

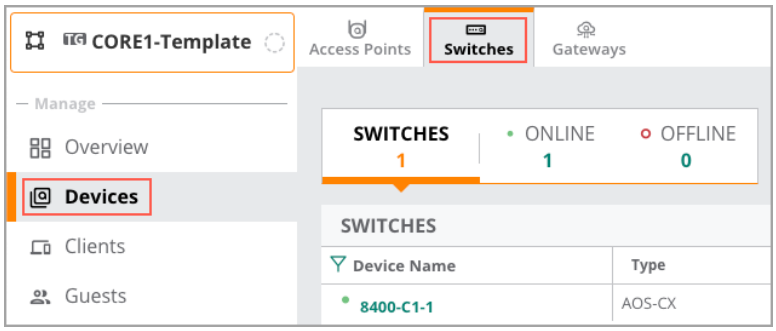
**Step 1** On the **Groups** page, in the **Manage Groups** section, drag the unassigned core switch from the left side to the template group on the right side.




**Step 2** At the top left, go to **Global > Groups**. In the **Groups** list, select **CORE1-Template**.




**Step 3** On the left menu, select **Devices**, then select **Switches**.

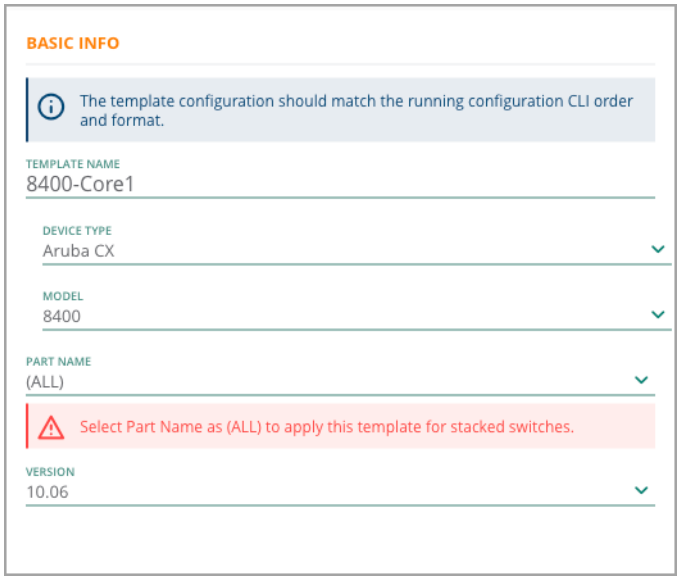



**Step 4** On the **Switches List** page in the top right, click **Config**.

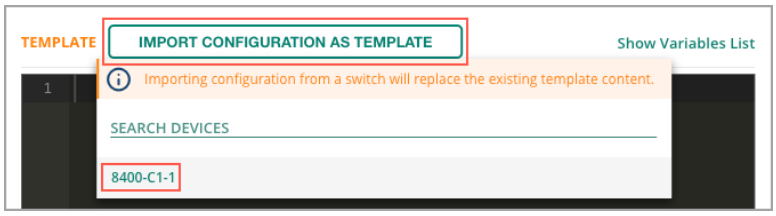

**Step 5** On the **Switches Template** section in the top right, click the **+** (plus sign).


**Step 6** On the **Add Template** window in the **BASIC INFO** section, assign the following settings, then click **Next**.

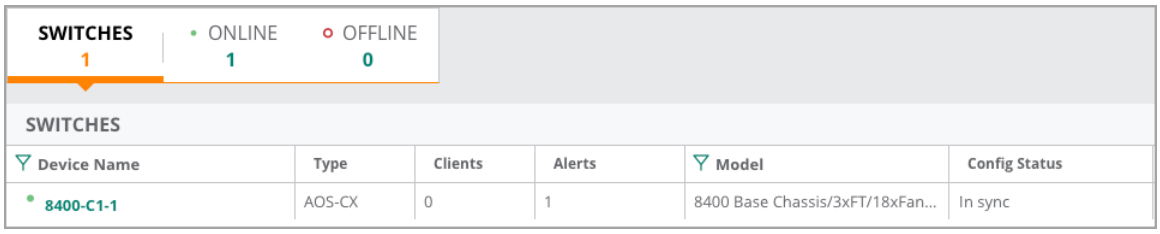
- **Template Name:** *8400-Core1*
- **Device Type:** *Aruba CX*
- **Model:** *8400*
- **Part Name:** *(ALL)*
- **Version:** *10.06*




**Step 7** In the **TEMPLATE** section, select **Import Configuration as Template**. Select **8400-C1-1**, then click **Save**.




**Step 8** On the left menu, go to **Devices > Switches > List**, and verify that the **Config Status** is “In sync”.



# Wired Core Configuration

The most critical point of connectivity in a campus LAN, the network core is designed for simplicity and reliability. Relative to the rest of the network, the core provides high-speed, high-bandwidth, Layer 3 connectivity between the various aggregation points across the campus.

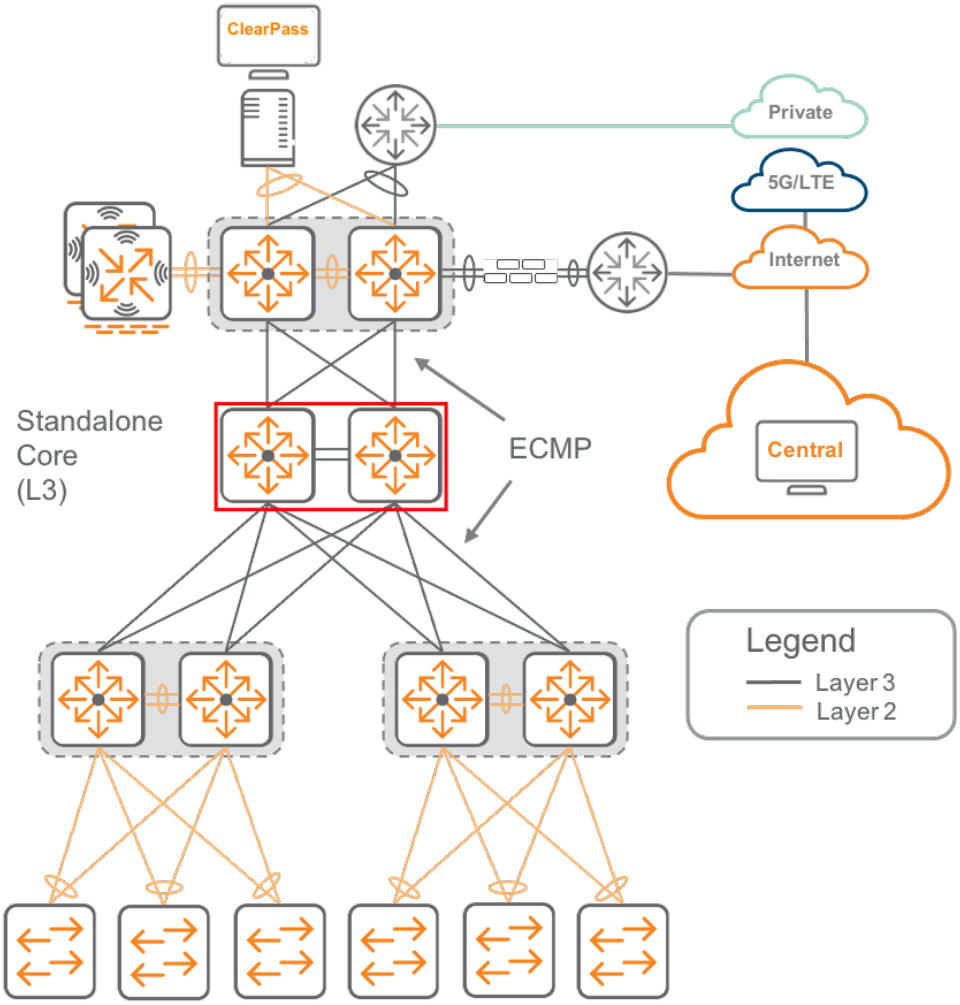
The network core also provides services aggregation functions when needed. Deciding where to locate network services, such as gateway devices, depends on the number of access aggregation switches and where user applications are hosted. Refer to the ESP Campus Design Validated Solution Guide for further discussion.

## Configure the Core Switch Group

The following procedures describe the creation of a core switch configuration in CLI format. The switch configuration can be created offline in a text editor and copied into MultiEdit, or it can be typed directly in MultiEdit in a UI group of Central. Switches in the group receive the configuration when synchronized to Central.

The figure below shows the standalone core switches in the Aruba ESP Campus.

**Wired Core**




## Enable MultiEdit for the Group

The base configuration of the switch was previously described in the Switch Group Configuration section of this guide. The following procedure completes the switch configuration using the Aruba Central MultiEdit tool, a CLI-based configuration editor built into Central.

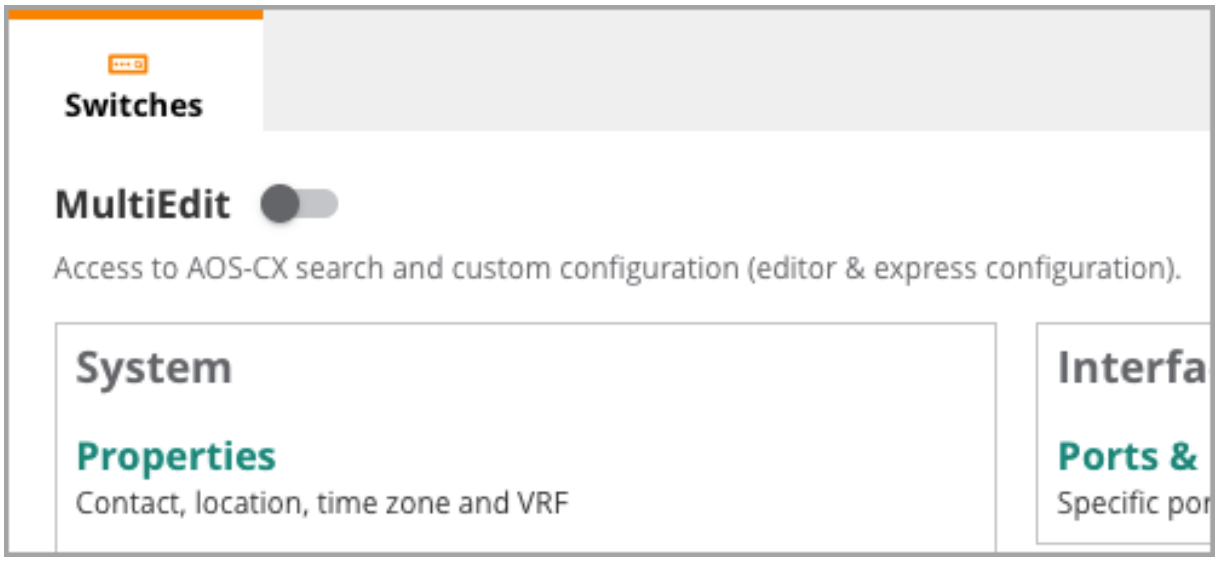
**Step 1** Go to **Central** and login using administrator credentials.

**Step 2** On the Aruba Central Account Home page, launch the **Network Operations** app.

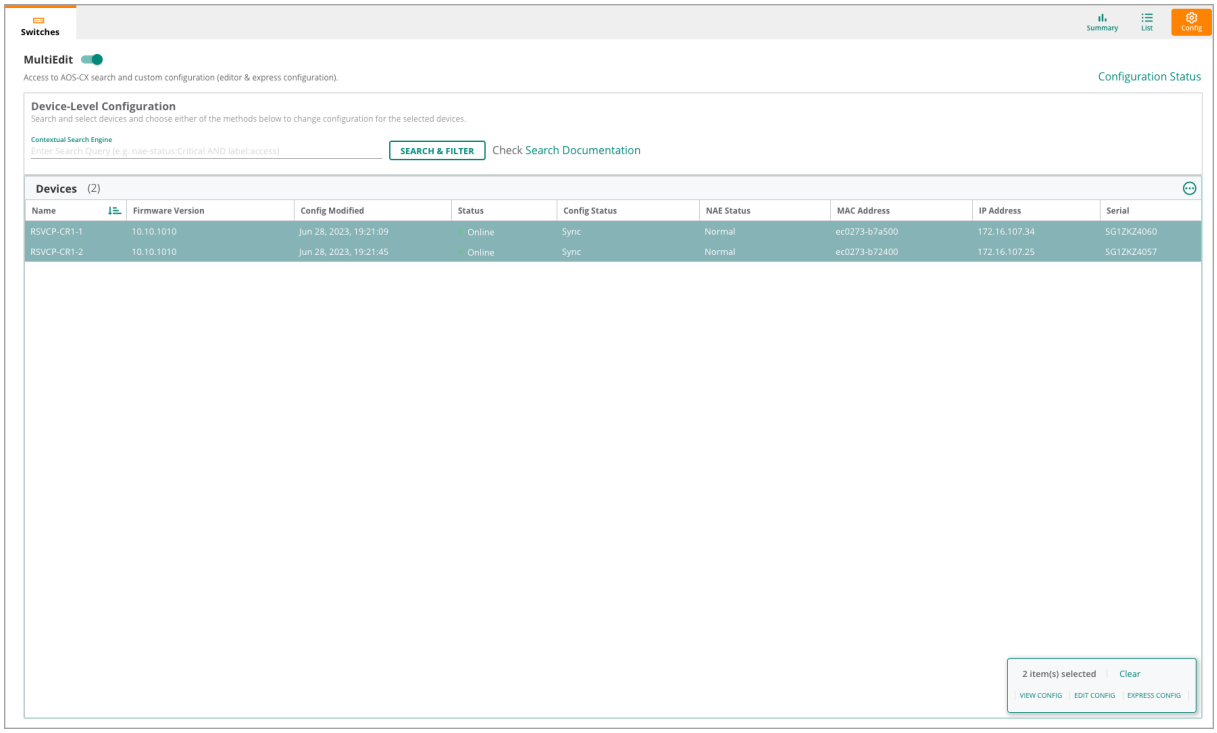
**Step 3** In the filter dropdown, select a core switch **Group** name. On the left menu, select **Devices**.

**Step 4** In the upper right of the **Switches** page, select **Config**.

**Step 5** In the upper left of the **Switches** page, move the slider right to enable **MultiEdit**.




**Step 6** Select the devices for editing. In the lower right window, click **EDIT CONFIG**.

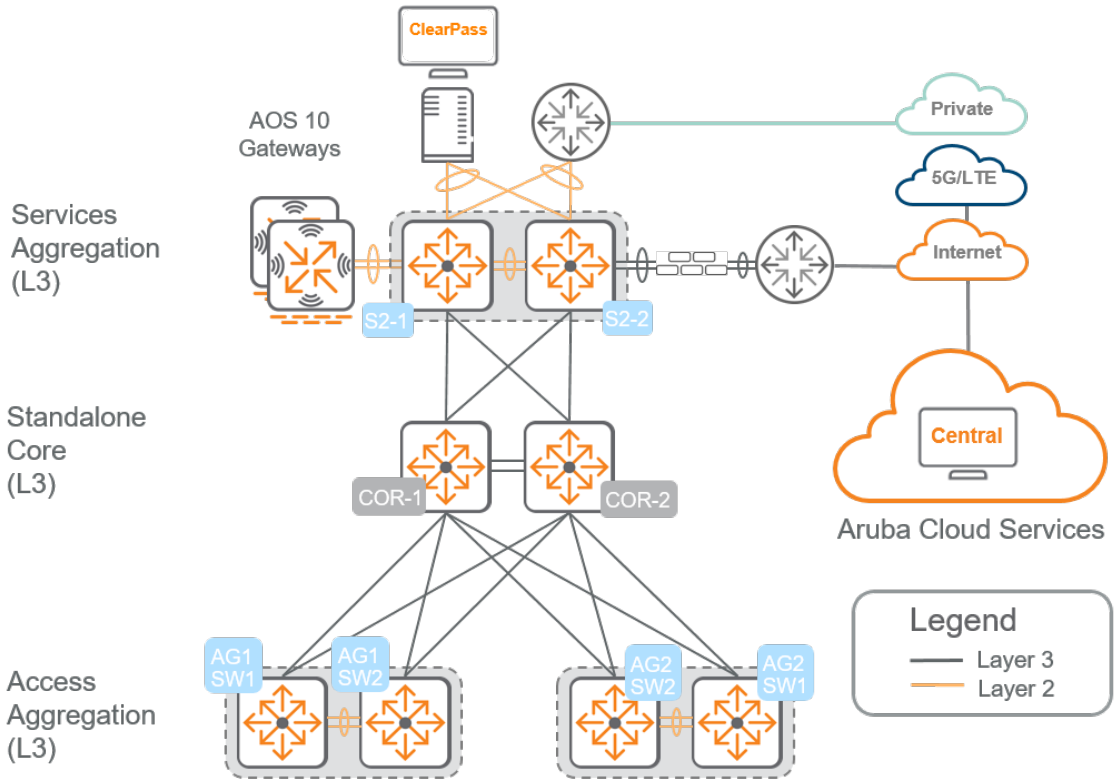



## Configure Routers and Loopback Interfaces

In the following procedure, Open Shortest Path First (OSPF) routing is configured and neighbor relationships are established between aggregation and core switches by configuring point-to-point IP links using /31 subnets. Then, Protocol Independent Multicast-Sparse Mode (PIM-SM) routing is enabled on the same links to ensure that multicast streams coming from the core can flow to the access VLANs. Loopback interfaces are created for the routers.

The figure below can be used as a reference point for the implemented configuration.

**OSPF Topology**




**NOTE:**

After pasting a configuration in the MultiEdit window, right-click any device-specific values. A **Modify Parameters** window appears on the right to allow input of individual device values when entering configuration for multiple devices.

**Step 1** Configure the global OSPF routing instance with area 0 and enable passive-interface default to avoid unwanted OSPF adjacencies. Use a pre-allocated loopback IP address as the router-id. When a chassis has redundant management modules, enable **graceful-restart**.

```
router ospf 1
  area 0
  passive-interface default
  router-id 10.0.0.1
  redistribute bgp
  graceful-restart restart-interval 30
```

**Step 2** Configure multicast routing globally.

```
router pim
  enable
```

**Step 3** Configure OSPF on the loopback interface. Create the loopback 0 interface and configure the IP address using the router ID from the earlier step. Enable OSPF with area 0.

```
interface loopback 0
  ip address 10.0.0.1/32
  ip pim-sparse enable
  ip ospf 1 area 0
```

**Step 4** Create a new loopback interface with the Anycast IP address. Enable PIM-SM and OSPF.

```
interface loopback 1
  ip address 10.0.0.100/32
  ip pim-sparse enable
  ip ospf 1 area 0
```

## Configure Multicast Routing

In the following procedure, the core is configured as a rendezvous point (RP) candidate using the loopback 1 anycast IP address and a bootstrap router (BSR) candidate using the loopback 0 IP address. Then MSDP is configured to share multicast group source addresses.

**Step 1** Configure the RP candidate source IP interface using loopback 1, and the BSR candidate source IP interface using loopback 0. Set the RP-candidate group prefix and the BSR-candidate priority.

**Example: Core 1 Switch**

```
router pim
    enable
    rp-candidate source-ip-interface loopback1 group-prefix 224.0.0.0/4
    bsr-candidate source-ip-interface loopback0
    bsr-candidate priority 1
```

**Example: Core 2 Switch**

```
router pim
    enable
    rp-candidate source-ip-interface loopback1 group-prefix 224.0.0.0/4
    bsr-candidate source-ip-interface loopback0
```

**NOTE:**

The RP candidate group prefix should be adjusted based on the IP design of the local network. The 224.0.0.0/4 prefix assigns all multicast groups to the RP.

**Step 2** Configure MSDP globally. The MSDP peer is the IP address of the loopback 0 interface on the adjacent core switch. The local loopback 0 interface is the connect-source.

**Example: Core 1 Switch**

```
router msdp
 enable
 ip msdp peer 10.0.0.2
     connect-source loopback0
     enable
     mesh-group RSVCP
```

**Example: Core 2 Switch**

```
router msdp
 enable
 ip msdp peer 10.0.0.1
     connect-source loopback0
     enable
     mesh-group RSVCP
```

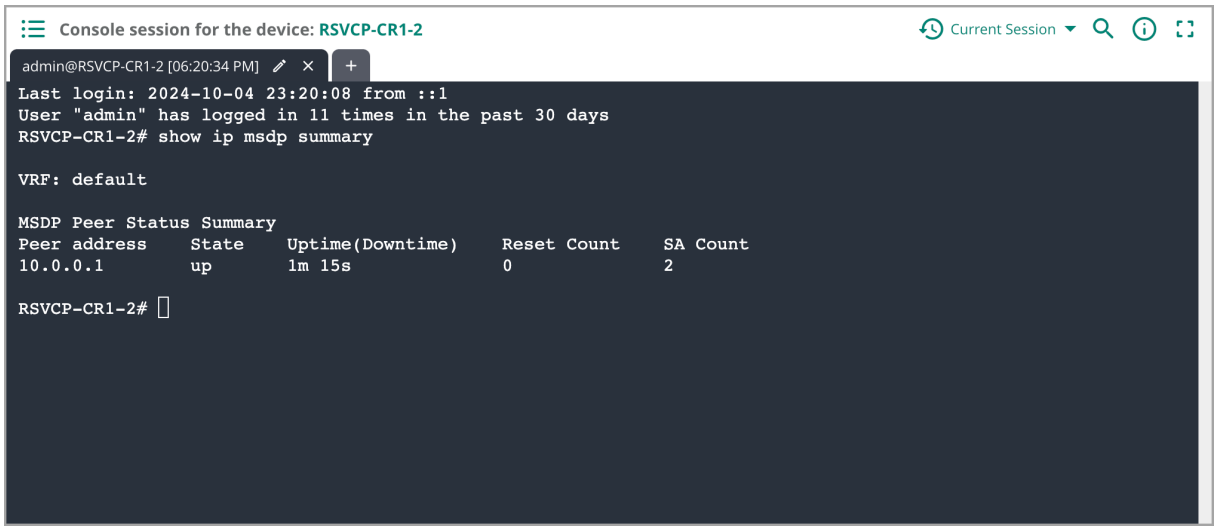
**NOTE:**

The mesh-group must be specified to exchange multicast group source address (SA) information, even when only two switches are participating in MSDP. An MSDP peer relationship will form without the mesh-group specificiation, but no SA information will be exchanged.

At the bottom right of the MultiEdit window, click **Save**.


### *Verify MSDP*

**Step 3** In a **Remote Console** window, type the command `show ip msdp summary`, then press ENTER. The output shown below indicates that MSDP source address (SA) information is sent from Core 1 to Core 2.




**NOTE:**

Execute the **show ip msdp summary** on both core routers when a multicast source is active to verify SA information is exchanged. The **SA Count** value on at least one core router should be above zero.

## Configure Switch Interfaces

Next, each physical interface connected to an aggregation switch is configured for OSPF and PIM-SM routing.

**Step 1** Configure OSPF and PIM-SM on the physical interfaces. Configure a large IP MTU, turn off OSPF passive mode, set the OSPF network to point-to-point, and enable OSPF using the router process and area.

```
interface 1/1/1
  description CORE_TO_AGG1
  no shutdown
  mtu 9198
  ip address 172.18.103.1/31
  ip mtu 9198
  no ip ospf passive
  ip ospf network point-to-point
  ip ospf 1 area 0
  ip pim-sparse enable
```

**Step 2** Repeat the previous step for each interface between the core and aggregation switches.

**Example: Core 1 Switch**

| Core 1 IP Address | Subnet | Peer Device |
|---|---|---|
| 172.18.100.0 | 172.18.100.0/31 | Core-2 |
| 172.18.100.2 | 172.18.100.2/31 | Core-2 |
| 172.18.106.1 | 172.18.106.0/31 | S2-1 |
| 172.18.106.5 | 172.18.106.4/31 | S2-2 |
| 172.18.102.1 | 172.18.102.0/31 | AG2-1 |
| 172.18.102.5 | 172.18.102.4/31 | AG2-2 |
| 172.18.103.1 | 172.18.103.0/31 | AG1-1 |
| 172.18.103.5 | 172.18.103.4/31 | AG1-2 |

**Example: Core 2 Switch**

| Core 2 IP Address | Subnet | Peer Device |
|---|---|---|
| 172.18.100.1 | 172.18.100.0/31 | Core-1 |
| 172.18.100.3 | 172.18.100.2/31 | Core-1 |
| 172.18.106.3 | 172.18.106.2/31 | S2-1 |
| 172.18.106.7 | 172.18.106.6/31 | S2-2 |
| 172.18.102.3 | 172.18.106.2/31 | AG2-1 |
| 172.18.102.7 | 172.18.102.6/31 | AG2-2 |
| 172.18.103.3 | 172.18.103.2/31 | AG1-1 |
| 172.18.103.7 | 172.18.103.6/31 | AG1-2 |

## Configure Data Center Connectivity

Many campuses have a locally attached data center. With this arrangement, routing must be established between the two networks so that clients in the campus can access applications in the data center. In the OWL, Corp. campus, BGP is used to peer with the data center border to learn the routes needed by clients.

**Step 1** Create VLANs and SVIs for peering between the campus core and data center border. Each VLAN SVI becomes the BGP neighbor and participates in OSPF for the campus.

```
vlan 2011
    name DC1_FB1_PROD_LF1-1
vlan 2013
    name DC1_FB1_PROD_LF2-1

...

interface vlan 2011
    description DC1_FB1_PROD_LF1-1
    ip mtu 9198
    ip address 172.18.100.63/31
    ip ospf 1 area 0.0.0.0
    ip ospf passive
interface vlan 2013
    description DC1_FB1_PROD_LF2-1
    ip mtu 9198
    ip address 172.18.100.67/31
    ip ospf 1 area 0.0.0.0
    ip ospf passive
```

**Step 2** Configure the physical interfaces connected to the data center border to trunk the VLANs created above.

```
interface 1/3/5
    description RSVDC-FB1-LF1-1
    no shutdown
    mtu 9198
    no routing
    vlan trunk native 1
    vlan trunk allowed 2011
interface 1/3/6
    description RSVDC-FB1-LF1-2
    no shutdown
    mtu 9198
    no routing
    vlan trunk native 1
    vlan trunk allowed 2013
```

**Step 3** Configure the BGP router to peer with the routers running on the data center border switches.

```
router bgp 65000
    bgp router-id 10.0.0.1
    neighbor 172.18.100.62 remote-as 65001
    neighbor 172.18.100.62 fall-over bfd
    neighbor 172.18.100.66 remote-as 65001
    neighbor 172.18.100.66 fall-over bfd
    address-family ipv4 unicast
        neighbor 172.18.100.62 activate
        neighbor 172.18.100.62 default-originate
        neighbor 172.18.100.66 activate
        neighbor 172.18.100.66 default-originate
    exit-address-family
```

**Step 4** At the bottom right of the MultiEdit window, click **Save**.

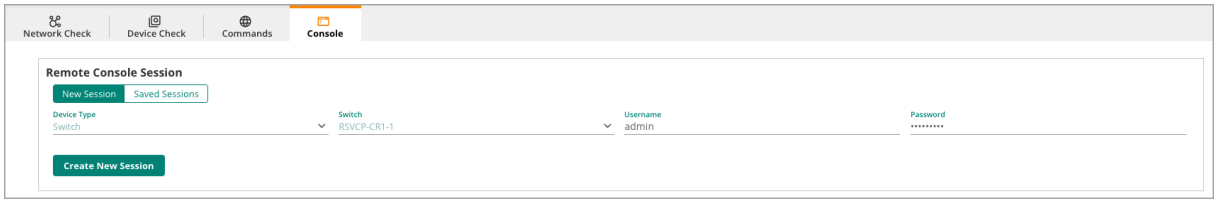

### *Verify BGP Operation*

Central provides a remote console capability that allows for CLI access on any managed switch. Use this to run CLI **show** commands at validation steps throughout this guide.

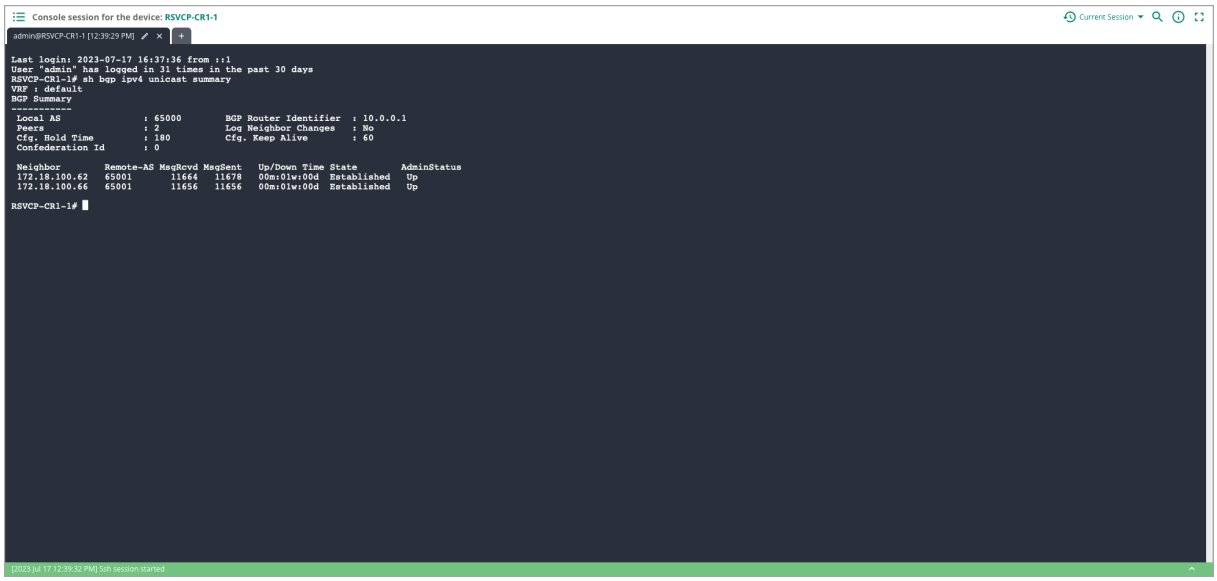
**Step 1** On the left menu, select **Tools**.

**Step 2** On the **Console** tab, assign the following settings, then select **Create New Session**.

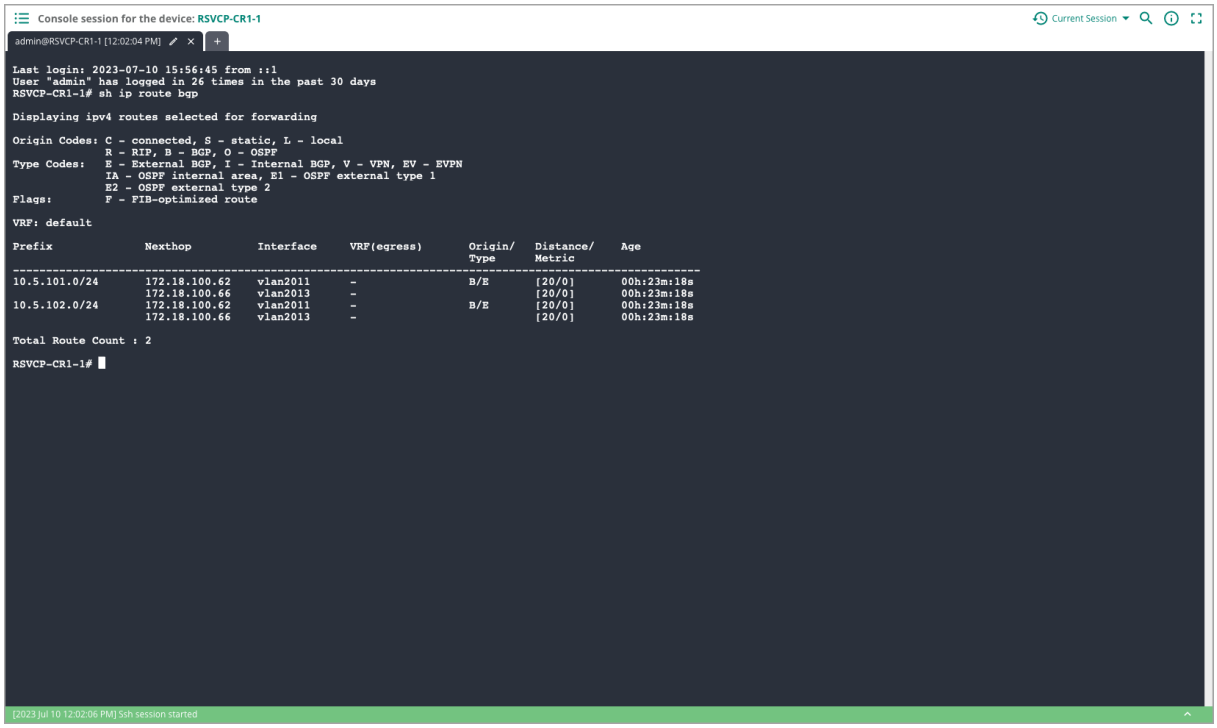
- **Device Type:** *Switch*
- **Switch:** *Device name*
- **Username:** *admin*
- **Password:** *password*




**Step 3** In the **Remote Console** window, type the command `show bgp ipv4 unicast summary`, then press ENTER. The output shown below indicates healthy BGP sessions to data center border switches.




**Step 4** In the **Remote Console** window, type the command *show ip route bgp*, then press ENTER. The output shown below shows the routes learned from the data center border switches.




## Configure Internet Connectivity

**Step 1** Configure an interface on each switch to provide Internet connectivity. In the OWL, Corp. campus, internet service is provided through a firewall running OSPF. The core switches use OSPF to peer with the firewall and learn the default route.

```
interface 1/3/11
    description RSVCP-INET
    no shutdown
    mtu 9198
    routing
    ip mtu 9000
    ip address 192.168.8.9/31
    ip ospf 1 area 0.0.0.0
    no ip ospf passive
    ip ospf network point-to-point
```

**NOTE:**

Devices in the group automatically synchronize the new configuration. Synchronization status is updated on the **Configuration Status** page. Process step execution can be observed by clicking **Audit Trail** on the left menu. Verification of OSPF routing is performed during aggregation switch deployment.

# Access and Services Aggregation Configuration

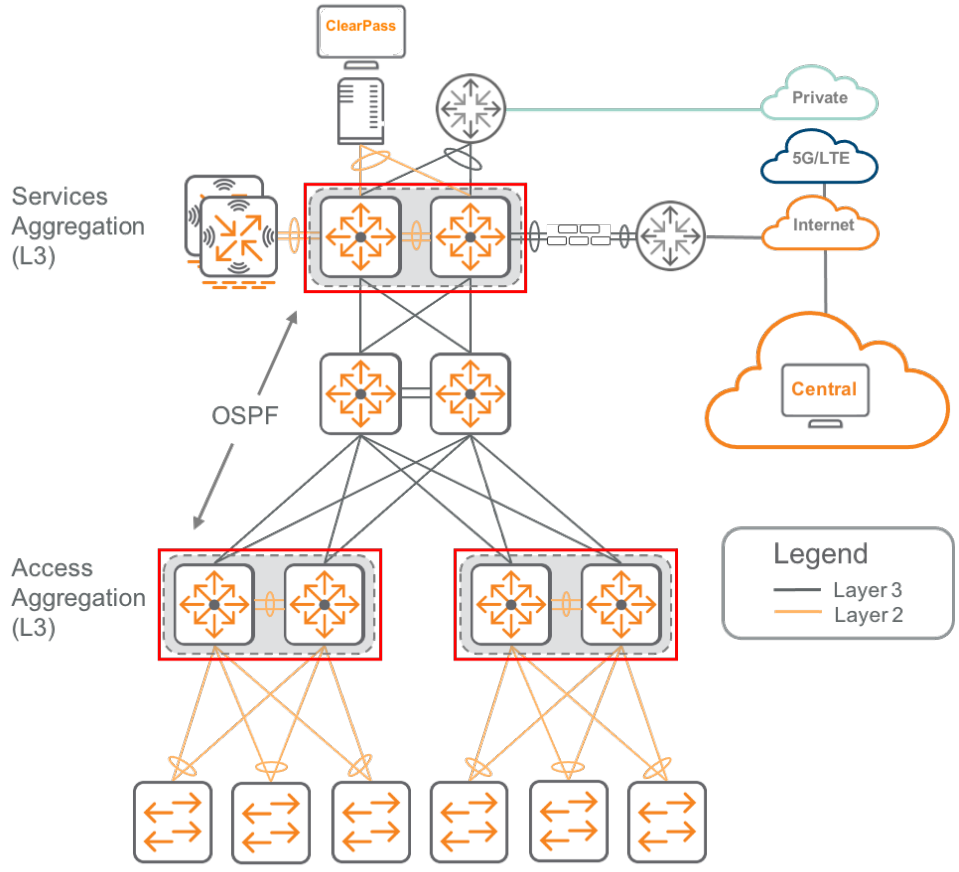
The access-aggregation layer provides default gateway services to the layer 2 access switches and consolidates bandwidth from the lower speed access ports into high-speed uplinks to the core. The services-aggregation layer provides a function similar to the gateways, policy servers, and WAN or Internet gateways.

## Configure the Aggregation Switch Groups

The following procedures describe the creation of an aggregation switch configuration in CLI format. The switch configuration may be created offline in a text editor and copied into MultiEdit or it may be typed directly in MultiEdit in a UI group of Central. Switches in the group receive the configuration when synchronized to Central.

The following figure shows the access aggregation and services aggregation switches in the ESP Campus.

**Wired Aggregation**



## Enable MultiEdit for the Group

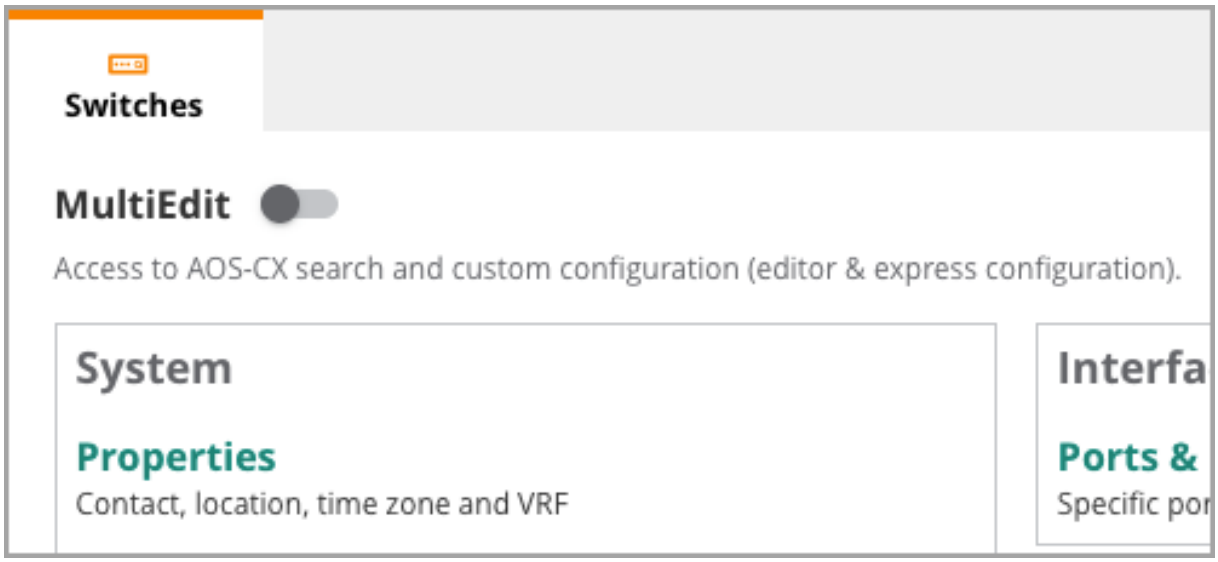
The base configuration of the switch was previously described in the Switch Group Configuration section of this guide. The following procedure completes the switch configuration using the Aruba Central MultiEdit tool, a CLI-based configuration editor built into Central.

**Step 1** Login to **HPE Greenlake** and navigate to **Aruba Central**.

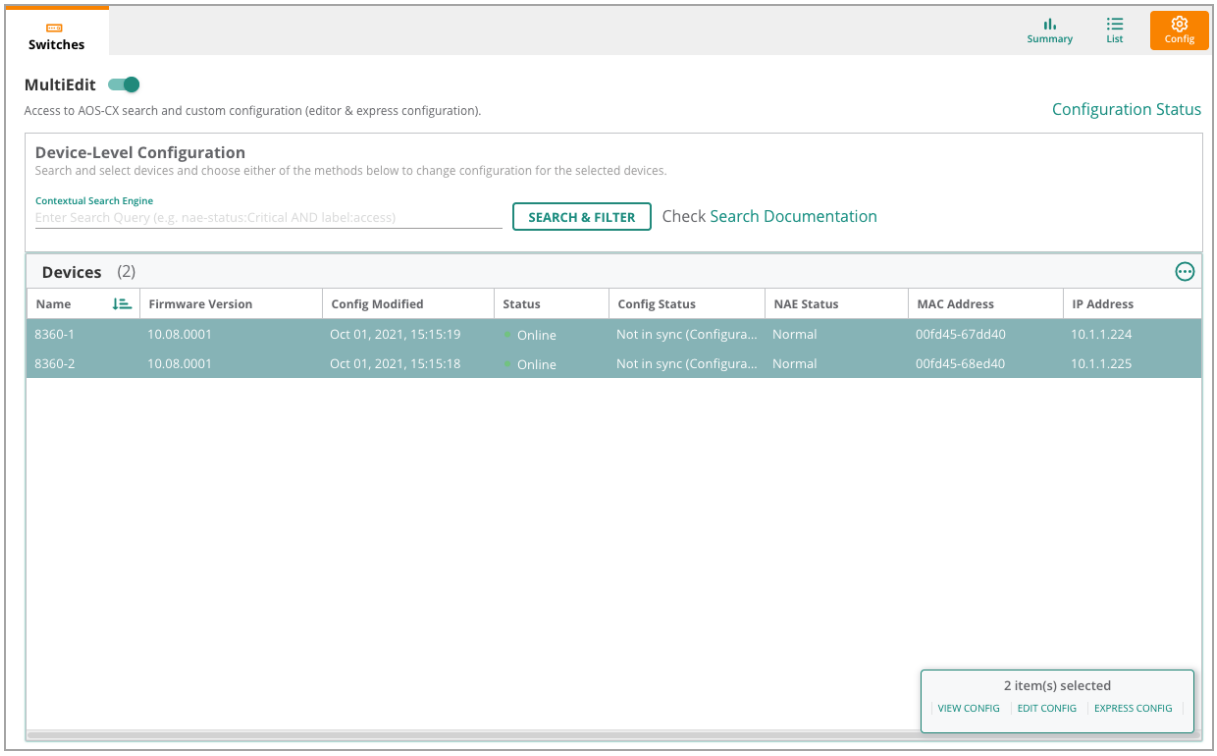
**Step 2** In the filter dropdown, select an aggregation switch **Group** name. On the left menu, select **Devices**.

**Step 3** In the upper right of the **Switches** page, select **Config**.

**Step 4** In the upper left of the **Switches** page, move the slider right to enable **MultiEdit**.




**Step 5** Select the devices for editing. In the lower right window, click **EDIT CONFIG**.



**NOTE:**

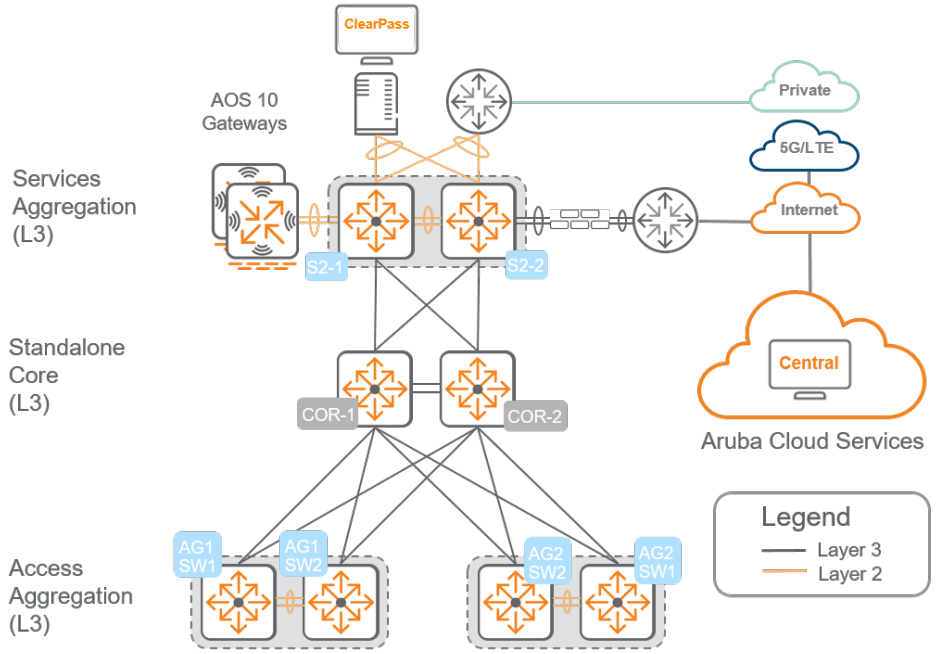
The following steps provide a chunk of configuration that can be pasted into the MultiEdit window. After pasting the configuration chunk, right-click any device-specific values. A **Modify Parameters** window appears on the right to allow input of individual device values.

## Configure OSPF and Multicast Routing

In the following steps, OSPF routing is configured to peer on point-to-point IP links using interface addresses in a /31 subnet. Then, PIM-Sparse Mode is enabled on the same links to ensure that multicast streams coming from the core can flow to the access VLANs.

The figure below can be used as a reference point for the implemented configuration.

**OSPF Topology**




**NOTE:**

The switch configuration is formatted automatically on input. Paste CLI at the begining, end, or on a new line anywhere in the configuration.

**Step 1** Configure the global OSPF routing instance with area 0 and enable passive-interface default to avoid unwanted OSPF adjacencies. Use a pre-allocated loopback IP address as the router-id.

```
router ospf 1 area 0
  passive-interface default
  router-id 10.0.3.1
```

When creating a template for chassis switch configuration, enable graceful restart.

```
graceful-restart restart-interval 30
```

**Step 2** Configure the global multicast routing instance.

```
router pim
  enable
  active-active
```

**Step 3** Create the loopback 0 interface and use a pre-allocated IP address. This should match the one used as the OSPF router-id. Enable OSPF in area 0 and PIM sparse mode on the interface.

```
interface loopback 0
  ip address 10.0.3.1/32
  ip ospf 1 area 0
  ip pim-sparse enable
```

**Step 4** Configure OSPF and PIM-SM on the physical interfaces. Configure a large IP MTU, turn off passive mode, associate the OSPF router instance from above, and enable PIM sparse mode on the interface.

```
interface 1/1/1
description AG1_TO_CORE
no shutdown
ip mtu 9198
ip address 172.18.103.0/31
no ip ospf passive
ip ospf network point-to-point
ip ospf 1 area 0
ip pim-sparse enable
```

**Step 5** Repeat the previous step for each interface connected between the aggregation and core switches.

**Example: Aggregation 1 Switches**

| AG1 IP Address | Subnet | Source Device | Peer Device |
|---|---|---|---|
| 172.18.103.0 | 172.18.103.0/31 | AG1-SW1 | Core 1 |
| 172.18.103.4 | 172.18.103.4/31 | AG1-SW2 | Core 1 |
| 172.18.103.2 | 172.18.103.2/31 | AG1-SW1 | Core 2 |
| 172.18.103.6 | 172.18.103.6/31 | AG1-SW2 | Core 2 |

**Example: Aggregation 2 Switches**

| AG2 IP Address | Subnet | Source Device | Peer Device |
|---|---|---|---|
| 172.18.102.0 | 172.18.102.0/31 | AG2-SW1 | Core 1 |
| 172.18.102.4 | 172.18.102.4/31 | AG2-SW2 | Core 1 |
| 172.18.102.2 | 172.18.102.2/31 | AG2-SW1 | Core 2 |
| 172.18.102.6 | 172.18.102.6/31 | AG2-SW2 | Core 2 |

**Example: Service Aggregation Switches**

| Service AG IP Address | Subnet | Source Device | Peer Device |
|---|---|---|---|
| 172.18.106.0 | 172.18.106.0/31 | S2-1 | Core 1 |
| 172.18.106.4 | 172.18.106.4/31 | S2-2 | Core 1 |
| 172.18.106.2 | 172.18.106.2/31 | S2-2 | Core 2 |
| 172.18.106.6 | 172.18.106.6/31 | S2-1 | Core 2 |

**Step 6** At the bottom right of the MultiEdit window, click **Save**.


**Step 7** When **Config Status** has returned to the “Sync” state for the modified devices, select **List** from the upper right.

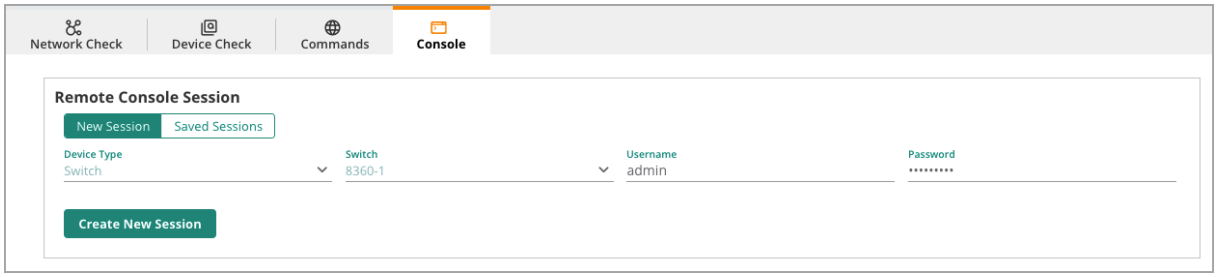

## Verify OSPF Operation

Central provides a remote console capability that allows for CLI access on any managed switch. Use this to run CLI **show** commands at validation steps throughout this guide.

**Step 8** On the left menu, select **Tools**.

**Step 9** On the **Console** tab, assign the following settings, then select **Create New Session**.

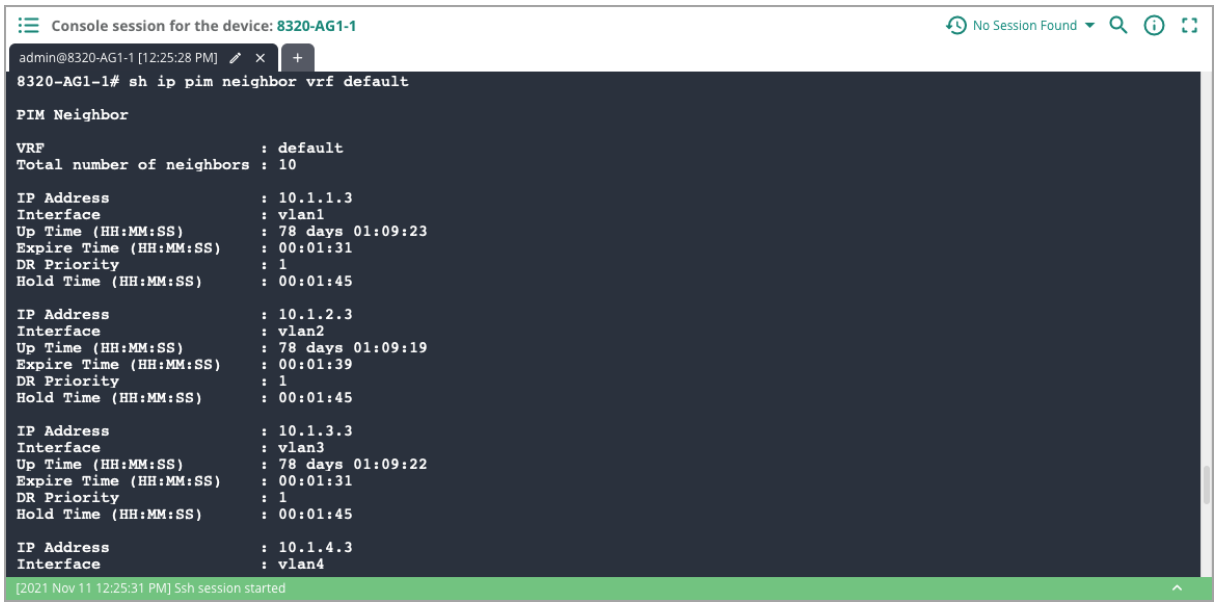
- **Device Type:** *Switch*
- **Switch:** *Device name*
- **Username:** *admin*
- **Password:** *password*




**Step 10** In the **Remote Console** window, type the command `show ip ospf neighbors`, then press ENTER. The output shown below indicates healthy OSPF sessions to core switches.


## Verify Multicast Operation

**Step 11** In a **Remote Console** window, type the command *show ip pim neighbor vrf default*, then press ENTER. The output shown below indicates multicast routing is running on configured VLANs.




## Plan MAC Addresses

A Locally Administered Address (LAA) should be used when assigning a VSX system-mac and active gateway MAC addresses in upcoming procedures. An LAA is a MAC in one of the four formats shown below:

```
x2-xx-xx-xx-xx-xx
x6-xx-xx-xx-xx-xx
xA-xx-xx-xx-xx-xx
xE-xx-xx-xx-xx-xx
```

The *x* positions can contain any valid hex value. For more details on the LAA format, see the IEEE tutorial guide.

**Step 1** Determine VSX System MAC addresses.

Each VSX pair uses a VSX system MAC address for control plane protocols such as Spanning-Tree and Link Aggregation Control Protocol (LACP). The same VSX MAC address is configured on both VSX pair members, and it must be unique per pair.

The following values are assigned to VSX pairs in this guide:

| VSX Pair | VSX System MAC |
|---|---|
| RSVCP-CR1-AG1 | 02:01:00:00:01:00 |
| RSVCP-CR1-AG2 | 02:01:00:00:02:00 |
| RSVCP-CR1-AG3 | 02:01:00:00:03:00 |
| RSVCP-CR1-SS2 | 02:01:00:00:04:00 |

**Step 2** Determine Active Gateway MAC addresses.

An active gateway IP provides Layer 3 gateway redundancy across members of a VSX pair. The active gateway MAC associates a virtual MAC address with an active gateway IP. Only a small number of unique virtual MAC assignments may be configured per switch. The same active gateway MAC address should be re-used for each active gateway IP assignment.

The following MAC values are assigned in this guide:

| VSX Pair | Active Gateway MAC for all subnets/VLANs on VSX Pair |
|---|---|
| RSVCP-CR1-AG1 | A2:01:00:00:00:01 |
| RSVCP-CR1-AG2 | A2:02:00:00:00:01 |
| RSVCP-CR1-AG3 | A2:03:00:00:00:01 |
| RSVCP-CR1-SS2 | A2:04:00:00:00:01 |

## Configure VSX

VSX is a redundancy protocol used to combine the Layer 2 data plane of two AOS-CX switches into a single logical switch fabric. Management and control plane functions remain independent. VSX is supported on 6400, 8400, and 83xx switch models.

Spanning tree should be enabled with aggregation switches acting as the root bridge. Gateways and access switches are configured with high bridge IDs to prevent them from becoming a root bridge.

Use this procedure to configure VSX on each switch.

**Step 1** Configure a LAG interface to be used as the inter-switch link (ISL) for the VSX pair. Allow all VLANs on this LAG for simplified configuration management.

```
interface lag 256
  no shutdown
  no routing
  vlan trunk native 1
  vlan trunk allowed all
  lacp mode active
```

**Step 2** Configure the ports of the LAG interface. A minimum of two ports is required and a maximum of eight are supported. The CLI below shows example interface numbers. To simplify the copy-paste procedure, copy only the configuration lines below the interface and paste them under the correct interface in MultiEdit.

```
interface 1/1/49
  description ISL_INTERFACE
  no shutdown
  lag 256
  mtu 9198
interface 1/1/50
  description ISL_INTERFACE
  no shutdown
  lag 256
  mtu 9198
```

**Step 3** Enable the VSX instance with the ISL LAG interface, the management IP information and VRF for the keep-alive session, a primary or secondary role, and shared system-mac. Primary and secondary examples are shown for clarity. Paste the configuration into MultiEdit one time only, then edit individual switch values as needed.

**NOTE:**

The management (mgmt) interface is used as a keep-alive interface for VSX. Ensure that the mgmt IP interface of the secondary switch is reachable from the primary switch and vice versa.

**NOTE:**

The system MAC must be the same value on each switch in the VSX pair, but otherwise unique within the network.

**Example: Primary VSX Switch**

```
vsx
  inter-switch-link lag 256
  keepalive peer 172.16.108.58 source 172.16.108.56 vrf mgmt
  role primary
  system-mac 02:01:00:00:01:00
```

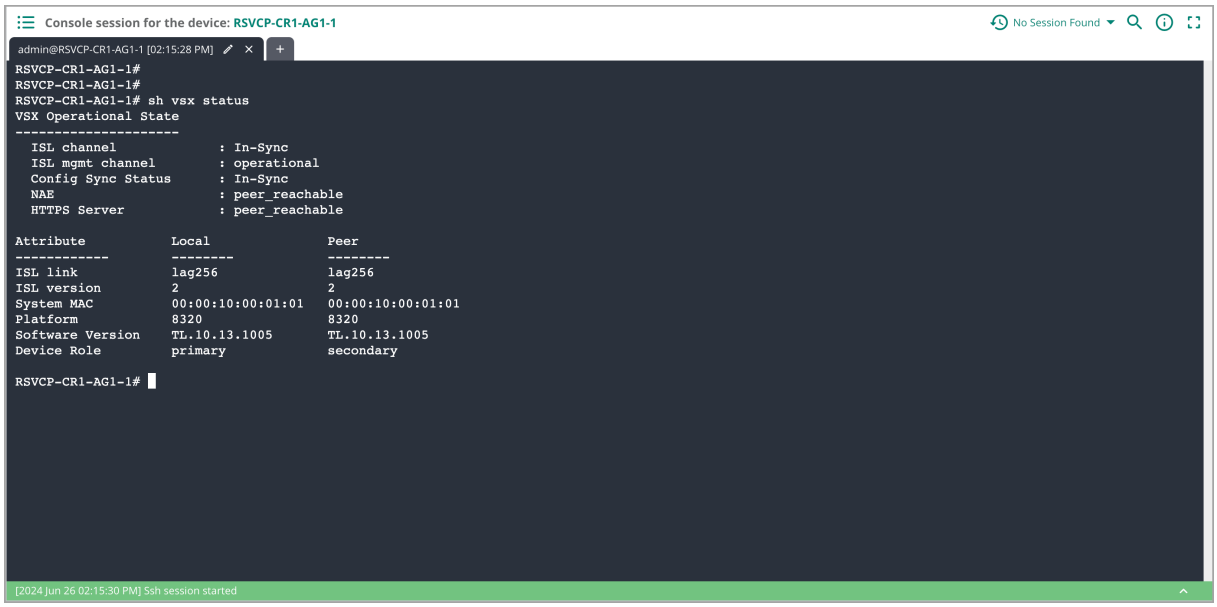
**Example: Secondary VSX Switch**

```
vsx
  inter-switch-link lag 256
  keepalive peer 172.16.108.56 source 172.16.108.58 vrf mgmt
  role secondary
  system-mac 02:01:00:00:01:00
```

**Step 4** At the bottom right of the MultiEdit window, click **Save**.


## Validate VSX Configuration

**Step 5** In a Remote Console window, type the command *show vsx status*, then press enter. The output shown below indicates a healthy VSX deployment.




## Configure the Access VLANs

The Layer 3 aggregation switch is the default gateway for access switches and advertises the interface VLAN routes to the rest of the network.

Use this procedure to configure the VLANs for the aggregation switches.

**Step 1** If needed, select **Devices** from the left menu, click **Config** in the upper right, and, with MultiEdit enabled, begin a new **Edit Config** session.

**Step 1** Define the access VLAN numbers and names, and enable IGMP snooping.

```
vlan 2
  name ZTP_NATIVE
  ip igmp snooping enable
vlan 3
  name EMPLOYEE
  ip igmp snooping enable
...
vlan 14
  name CRITICAL_AUTH
  ip igmp snooping enable
vlan 15
  name MGMT
  ip igmp snooping enable
```

**Step 3** Configure the VLAN and IP services. Configure a large IP MTU, set DHCP IP helper addresses, associate the OSPF router instance from above, enable PIM-SM, and enable IGMP on the interface.

```
interface vlan 2
  description ZTP_NATIVE
  ip mtu 9198
  ip address 10.2.2.2/24
  ip helper-address 10.2.120.98
  ip helper-address 10.2.120.99
  ip ospf 1 area 0.0.0.0
  ip igmp enable
  ip pim-sparse enable
```

**NOTE:**

The **ip helper-address** command enables the forwarding of DHCP requests from endpoints to DHCP servers on other subnets. Multiple DHCP servers can be defined.

**Step 4** Repeat the previous step for each VLAN.

**Step 5** At the bottom right of the MultiEdit window, click **Save**.


**Example: Access Aggregation**

| VLAN Name | VLAN ID | Access Agg 1 | Access Agg 2 | Network/Mask | Reserved Active gateway IP | Reserved Active gateway MAC address | IP helper address |
|---|---|---|---|---|---|---|---|
| ZTP_NATIVE | 2 | 10.2.2.2 | 10.2.2.3 | 10.2.2.0/24 | 10.2.2.1 | A2:01:00:00:00:01 | 10.2.120.98 10.2.120.99 |
| EMPLOYEE | 3 | 10.2.3.2 | 10.2.3.3 | 10.2.3.0/24 | 10.2.3.1 | A2:01:00:00:00:01 | 10.2.120.98 10.2.120.99 |
| VISITOR | 12 | 10.2.12.2 | 10.2.12.3 | 10.2.12.0/24 | 10.2.12.1 | A2:01:00:00:00:01 | 10.2.120.98 10.2.120.99 |
| REJECT_AUTH | 13 | 10.2.13.2 | 10.2.13.3 | 10.2.13.0/24 | 10.2.13.1 | A2:01:00:00:00:01 | 10.2.120.98 10.2.120.99 |
| CRITICAL AUTH | 14 | 10.2.14.2 | 10.2.14.3 | 10.2.14.0/24 | 10.2.14.1 | A2:01:00:00:00:01 | 10.2.120.98 10.2.120.99 |
| MGMT | 15 | 10.2.15.2 | 10.2.15.3 | 10.2.15.0/24 | 10.2.15.1 | A2:01:00:00:00:01 | 10.2.120.98 10.2.120.99 |

**Example: Service Aggregation 1**

| VLAN Name | VLAN ID | Service Agg 1 | Service Agg 2 | Network/Mask | Reserved Active Gateway IP | Reserved Active gateway MAC | IP helper address |
|---|---|---|---|---|---|---|---|
| EMPLOYE | 103 | 10.6.103. | 10.6.103. | 10.6.103. | 10.6.103.1 | A2:04:00:00:00: | 10.2.120.98<br>10.2.120.99 |
| VISITOR | 112 | 10.6.112.2 | 10.6.112.3 | 10.6.112.0/24 | 10.6.112.1 | A2:04:00:00:00:01 | 10.2.120.98<br>10.2.120.99 |
| REJECT_A | 113 | 10.6.113.2 | 10.6.113.3 | 10.6.113.0 | 10.6.113.1 | A2:04:00:00:00: | 10.2.120.98<br>10.2.120.99 |
| CRITICAL_AUTH | 114 | 10.6.114.2 | 10.6.114.3 | 10.6.114.0/24 | 10.6.114.1 | A2:04:00:00:00:01 | 10.2.120.98<br>10.2.120.99 |
| MGMT | 115 | 10.6.115.2 | 10.6.115.3 | 10.6.115.0 | 10.6.115.1 | A2:04:00:00:00: | 10.2.120.98<br>10.2.120.99 |

## Configure VLAN Active Gateways

An active gateway provides the ability to have a default route through either switch in a VSX pair with each switch using the same local MAC address and IP address.

**Step 1** Configure an active gateway on each VLAN using a local MAC address and IP address unique to the VLAN. If the VLAN is configured already according to the steps above, it is only necessary to paste the **active-gateway** lines.

**Example: VLAN 2 on Primary VSX Switch**

```
interface vlan 2
  active-gateway ip mac a2:01:00:00:00:01
  active-gateway ip 10.2.2.1
  description ZTP_Native
  ip mtu 9198
  ip address 10.2.2.2/24
  ip helper-address 10.2.120.98
  ip helper-address 10.2.120.99
```

**Example: VLAN 2 on Secondary VSX Switch**

```
interface vlan 2
  active-gateway ip mac a2:01:00:00:00:01
  active-gateway ip 10.2.2.1
  description ZTP_Native
  ip mtu 9198
  ip address 10.2.2.3/24
  ip helper-address 10.2.120.98
  ip helper-address 10.2.120.99
```

## Configure Spanning Tree

For the widest possible interoperability, configure Multiple Spanning Tree Protocol (MSTP) as the loop protection protocol.

**Step 1** Configure spanning tree globally and set the highest priority to ensure the aggregation switches are the root.

```
spanning-tree
spanning-tree priority 0
```

**NOTE:**

MSTP is the default spanning-tree protocol on an Aruba CX switch and is selected simply by enabling spanning-tree.

## Configure the Multi-Chassis LAG Interfaces

Configure an MC-LAG interface for each downstream access switch to enable uplink to both switches in the VSX pair without blocking.

**Step 1** Enable spanning tree root guard and LACP fallback to allow for safe ZTP of access switches. Assign a native VLAN of two and trunk the allowed access VLANs previously created. Enable LACP active and LACP fallback to facilitate access switch provisioning. Enable PIM-SM routing.

```
interface lag 1 multi-chassis
  no shutdown
  no routing
  vlan trunk native 2
  vlan trunk allowed 1-3,5-6,13-15
  lacp mode active
  lacp fallback
  spanning-tree root-guard
```

**Step 2** Repeat the previous step for each MC-LAG interface required for the connected access switches.

**Step 3** Configure the ports of the LAG interface. The CLI below shows example interface numbers. To simplify the copy and paste procedure, copy only the configuration lines below the interface and paste them under the correct interface in MultiEdit.

```
interface 1/1/1
  description DOWNLINK_TO_ACCESS_SW_OR_CTRL
  no shutdown
  lag 1
  mtu 9198
```

**Step 4** Repeat the previous step for each MC-LAG interface.

**Step 5** At the bottom right of the MultiEdit window, click **Save**.


Devices in the group automatically synchronize the new configuration. Synchronization status is updated on the **Configuration Status** page and process step execution can be observed by clicking **Audit Trail** on the left menu.

# Wired Access Configuration

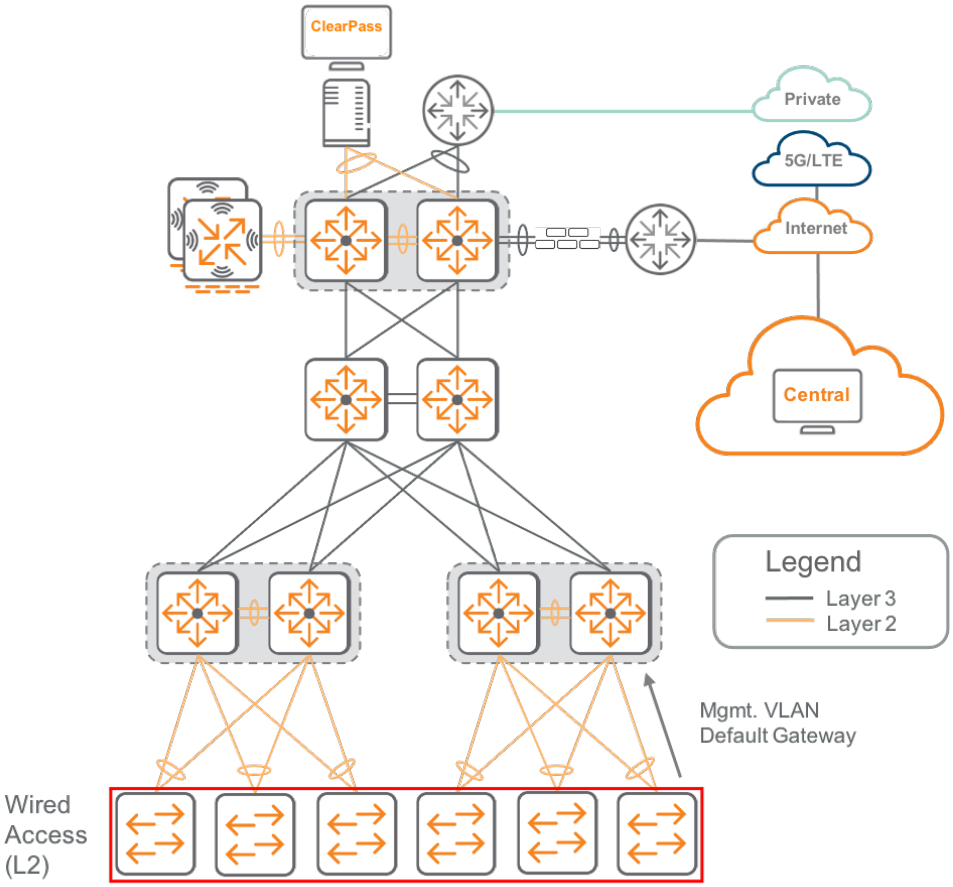
The access layer provides wired and wireless devices with Layer 2 connectivity to the network. It plays an important role in protecting users, application resources, and the network itself from human error and malicious attacks. This protection includes controlling the devices allowed on the network, ensuring that connected devices cannot provide unauthorized services to end users, and preventing unauthorized devices from taking over the role of other devices on the network.

## Configure the Access Switch Groups

The following procedures describe the configuration of individual and stacked access layer switches using a UI Group. The base configuration of the switches was described previously in the Switch Group Configuration section of this guide.

The following procedure completes the switch configuration using an Central UI Group. The figure below shows the access switches in the Campus.

**Wired Access**



## Configure a Standalone Switch

Connect a standalone switch to a network segment where it can receive a DHCP lease, which includes DNS servers and a valid route toward the Internet. CX 6000 series switches are factory-configured to request DHCP on any front panel interface or on the dedicated management port. After a new switch can reach Central, it automatically associates to the correct organization based on information from the time of purchase.

## Configure a Switch Stack

Follow this procedure to configure a group of switches for VSF stacking. Begin by cabling the stacking ports in a ring or daisy chain topology. The recommended stack ports for a 24-port model are 25 and 26, or ports 49 and 50 on 48-port models. To perform auto-stacking using Central, connect one switch in the stack to a network with DHCP service providing Internet reachability. This switch serves as the stack conductor after the stack is formed.

**NOTE:**

VSF stacking is supported on CX 6300 and 6200 model switches only.A switch must be added to a group before VSF configuration can continue.

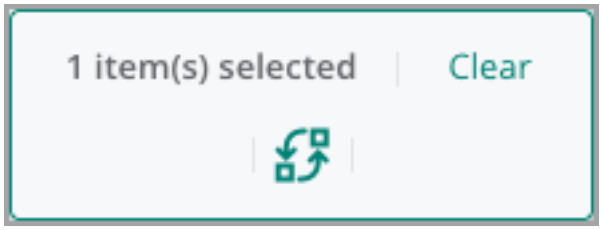
**CAUTION:**

Make sure the switches are in factory default state before auto stacking.

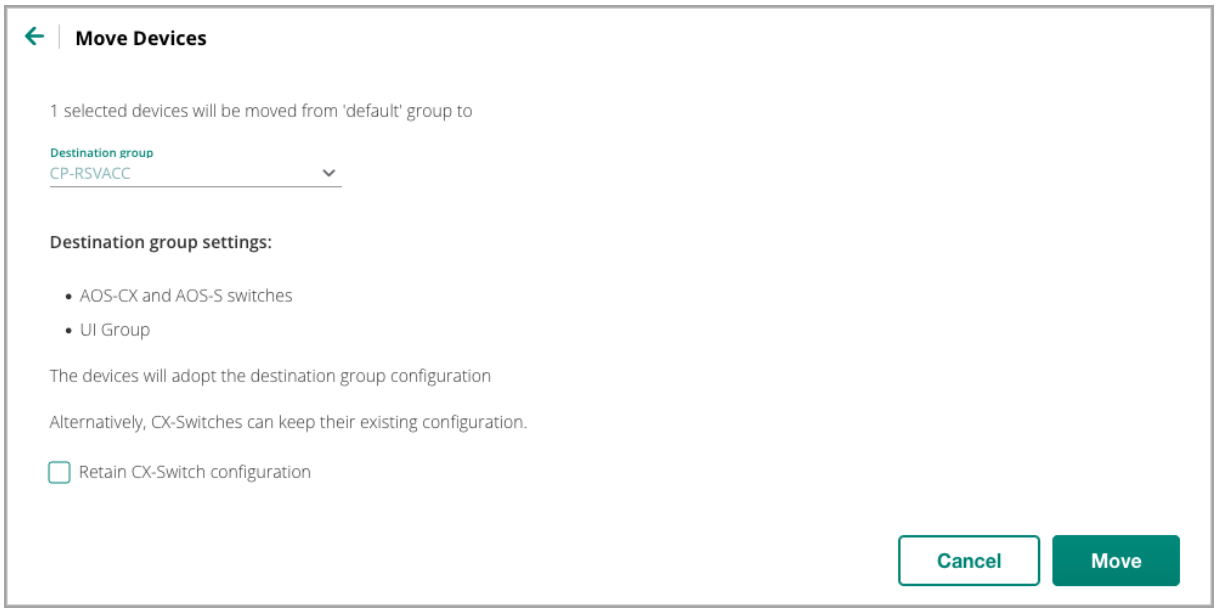
**Step 1** Login to **HPE Greenlake** and navigate to **Central**.

**Step 2** In the filter dropdown, select **Global**, if it is not already selected. On the left menu, select **Organization**.

**Step 3** Expand the **Unprovisioned devices** group, highlight the switch directly connected to the network, then click the **Move Devices** button at the lower right in the window.




**Step 4** In the **Destination group** dropdown, select the correct access switching **Group** for the stack, then click **Move**.

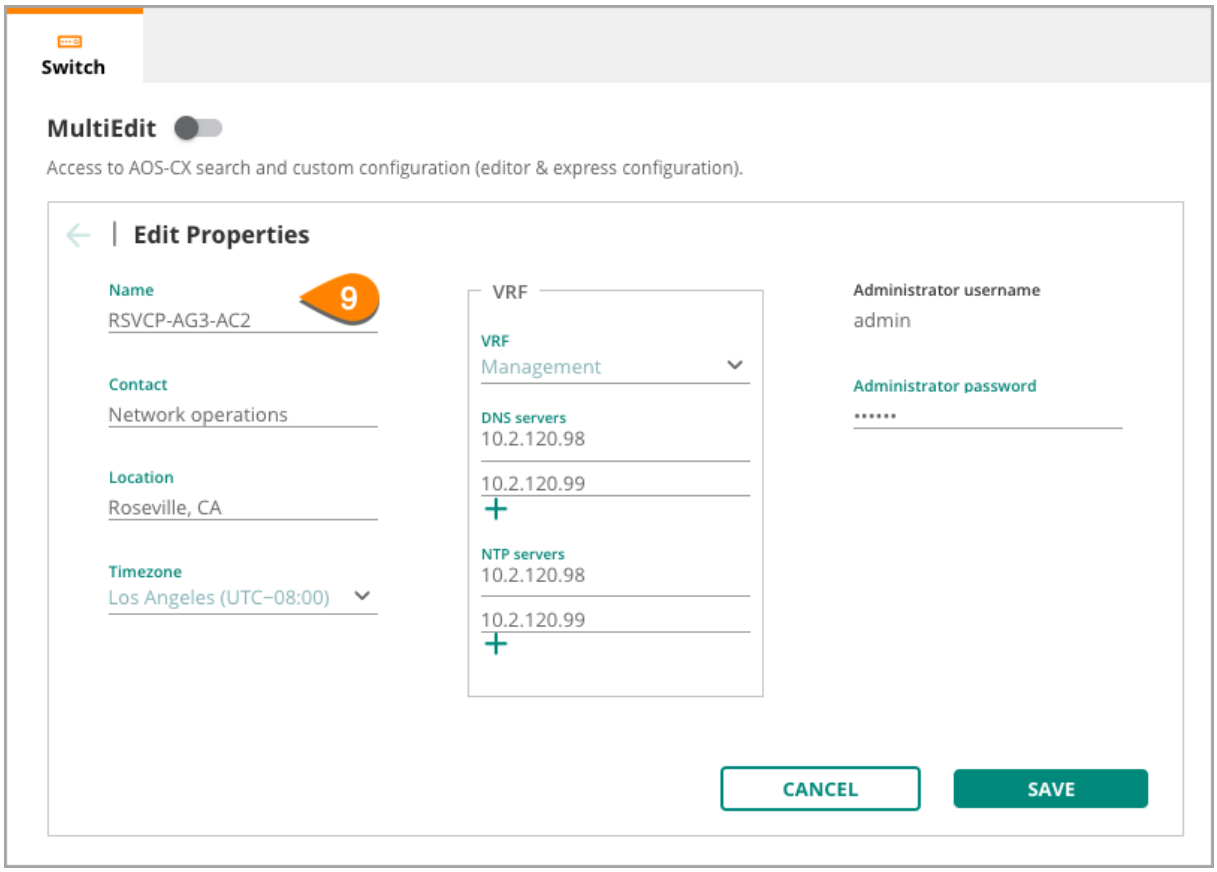



**Step 5** In the filter dropdown, select the access switch **Group** name. On the left menu, select **Devices**.

**Step 6** Select the new switch, using the serial number if multiple new switches are being added. On the left menu, select **Device**.

**Step 7** On the **Switch** page in the **System** tile, select **Properties**.

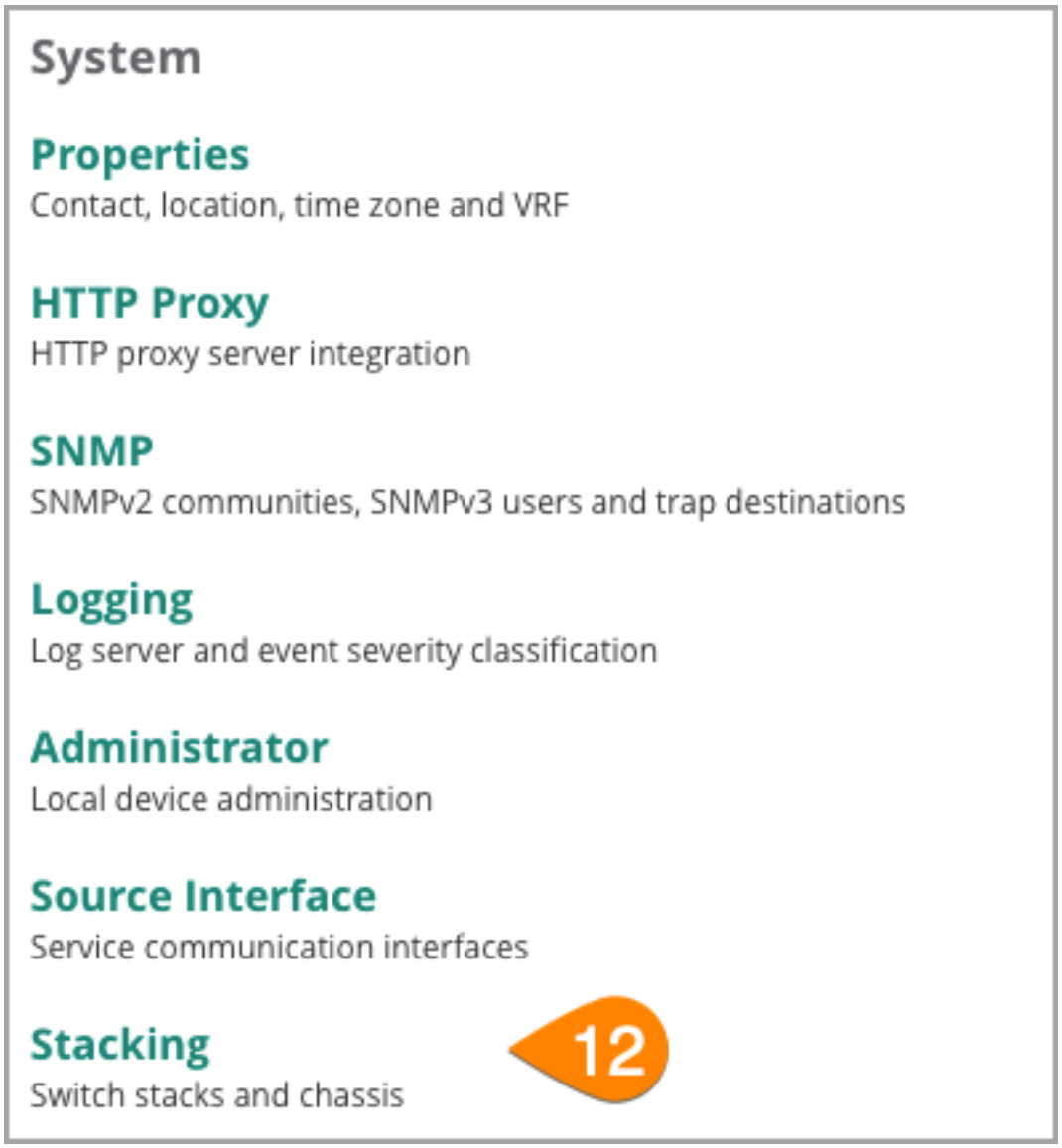
**Step 8** On the **Edit Properties** page, enter a **Name** for the new switch, leave the group inherited properties unchanged, then click **SAVE**.




**Step 9** Use the green left arrow on the filter menu to return to the **Switches** page.


**Step 10** On the upper right of the **Switches** page, select **Config**.

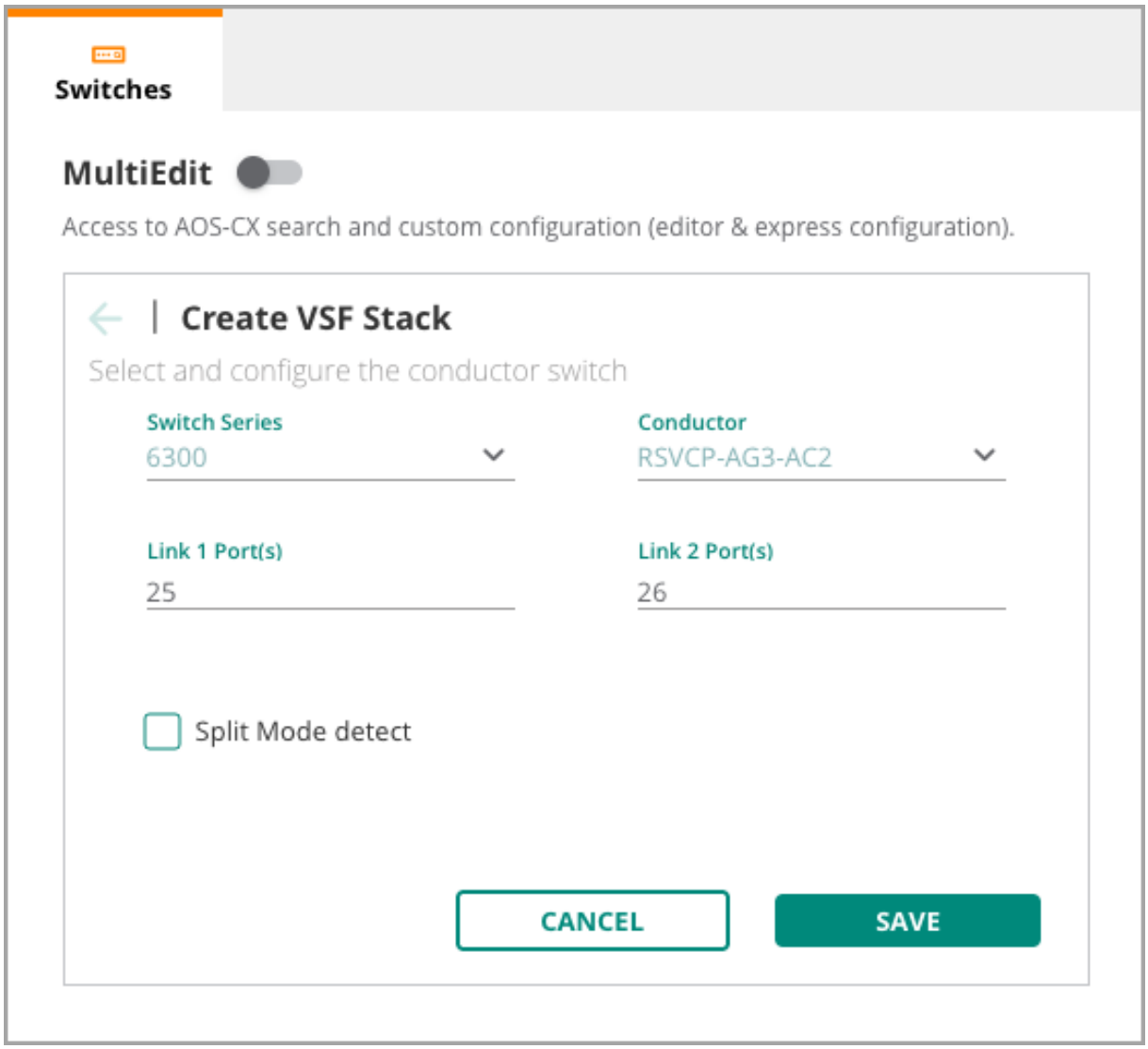
**Step 11** On the **Switches** page in the **System** tile, select **Stacking**.



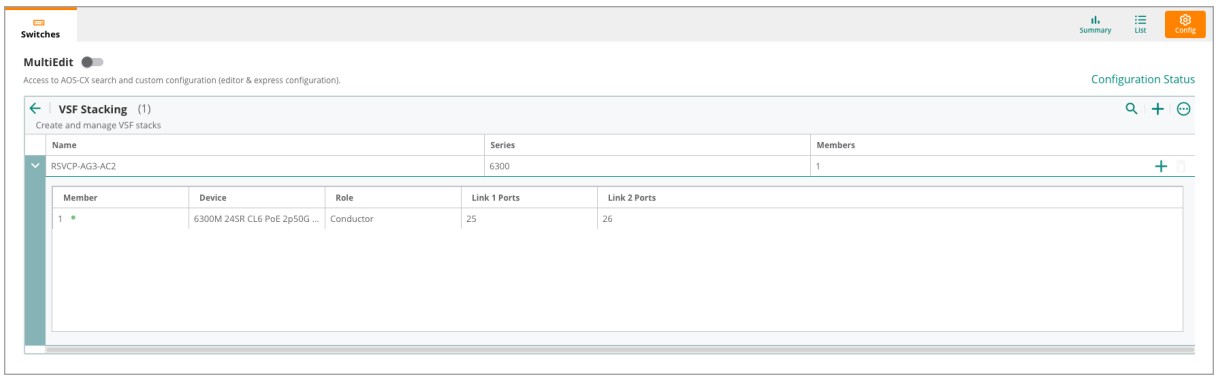

**Step 12** Create a new VSF stack by clicking the **+** (plus sign) at the upper right of the table.

**Step 13** In the **Create VSF Stack** window, assign the following settings, then click **SAVE**.

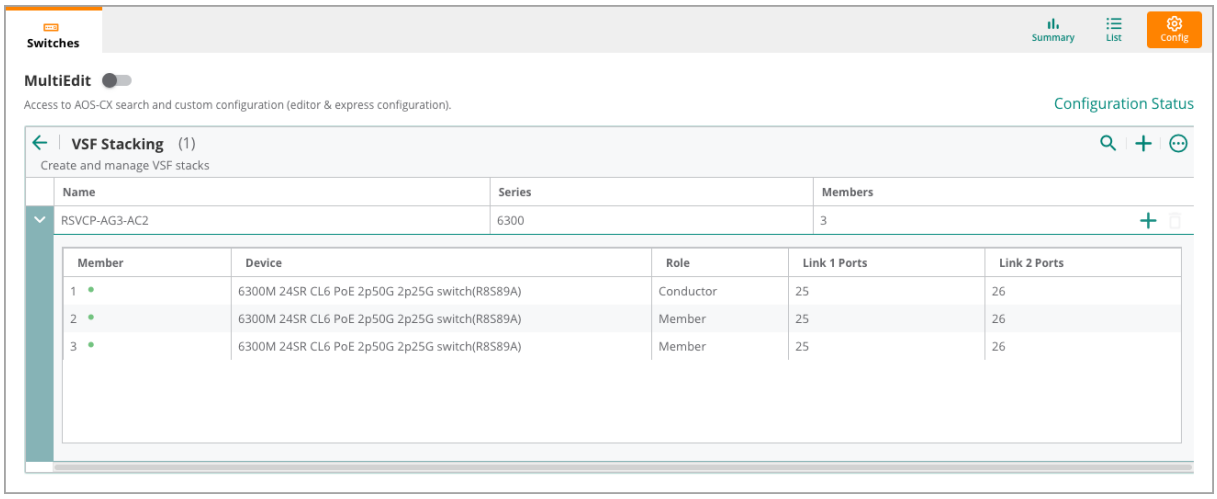
- **Switch Series:** *6300*
- **Conductor:** *RSVCP-AG3-AC2*
- **Link 1 Port(s):** *25*
- **Link 2 Port(s):** *26*
- **Split Mode detect:** *Unchecked*



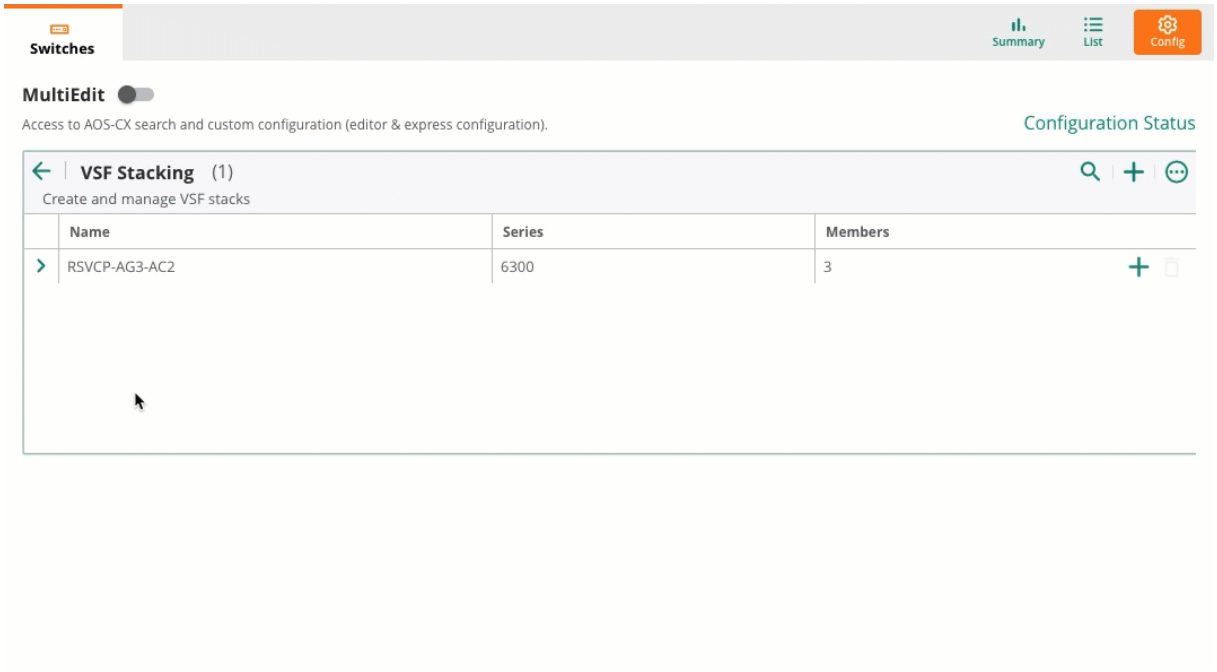

**Step 14** A VSF stack named with the serial number of the switch selected above is now listed in **VSF Stacking** with a single conductor.




**Step 15** Wait approximately five minutes for the stack to self-configure, then refresh the **VSF Stacking** page and confirm that all stack members are present.




**Step 16** At the right side of a member row, click the **Edit** icon, check the box for **Standby conductor**, then click **Save**.



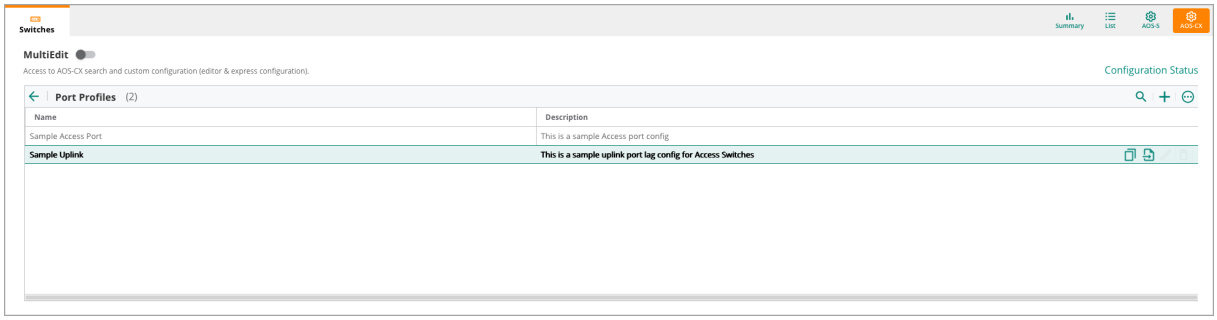

## Configure the Uplink LAG Interface

Configure link aggregation groups (LAGs) on redundant links to the aggregation switches for fault tolerance and increased capacity. By default, the uplink trunks use source and destination IP address, protocol port number, and device MAC addresses to load-balance traffic between grouped physical links. Use the Port Profiles feature of Central to apply the same port level configurations to multiple switches, or switch stacks, at the same time.

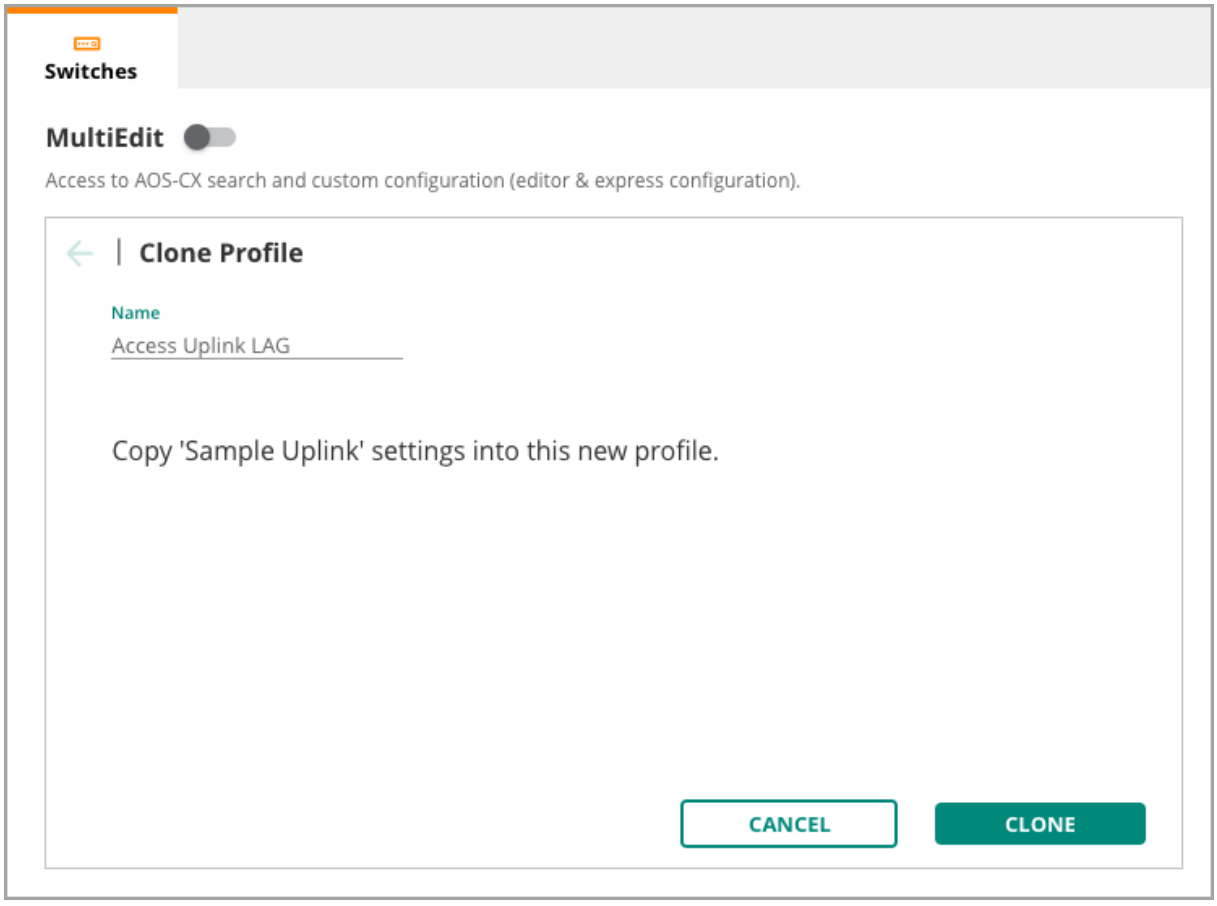
**Step 1** Connect a second link to the standalone switch or VSF stack.

**Step 2** In the device table, click the left arrow at the top left to return to the **Switches** page. Select **Port Profiles** in the **Interfaces** tile.

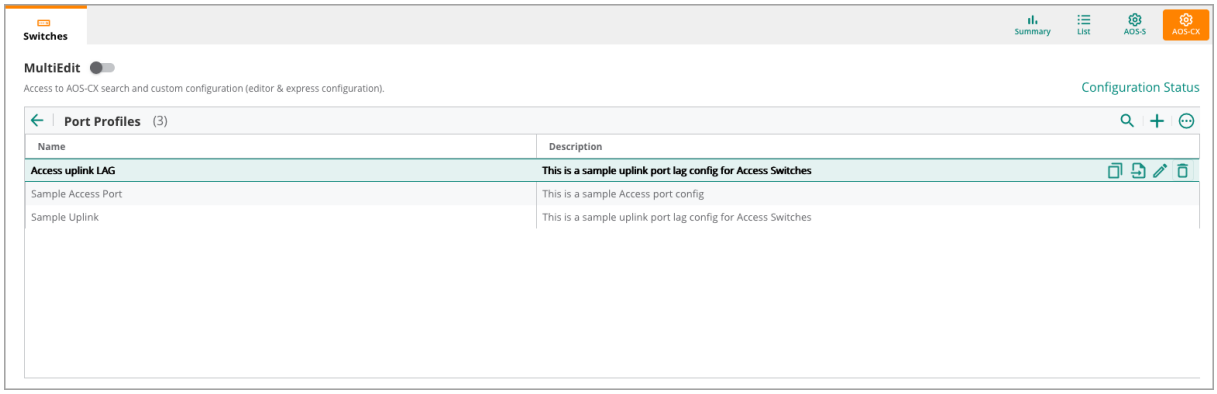

**Step 3** To clone the **Sample Uplink** profile, click the **Clone** icon visible when the row is highlighted.




**Step 4** Name the new port profile and click the **Clone** button.



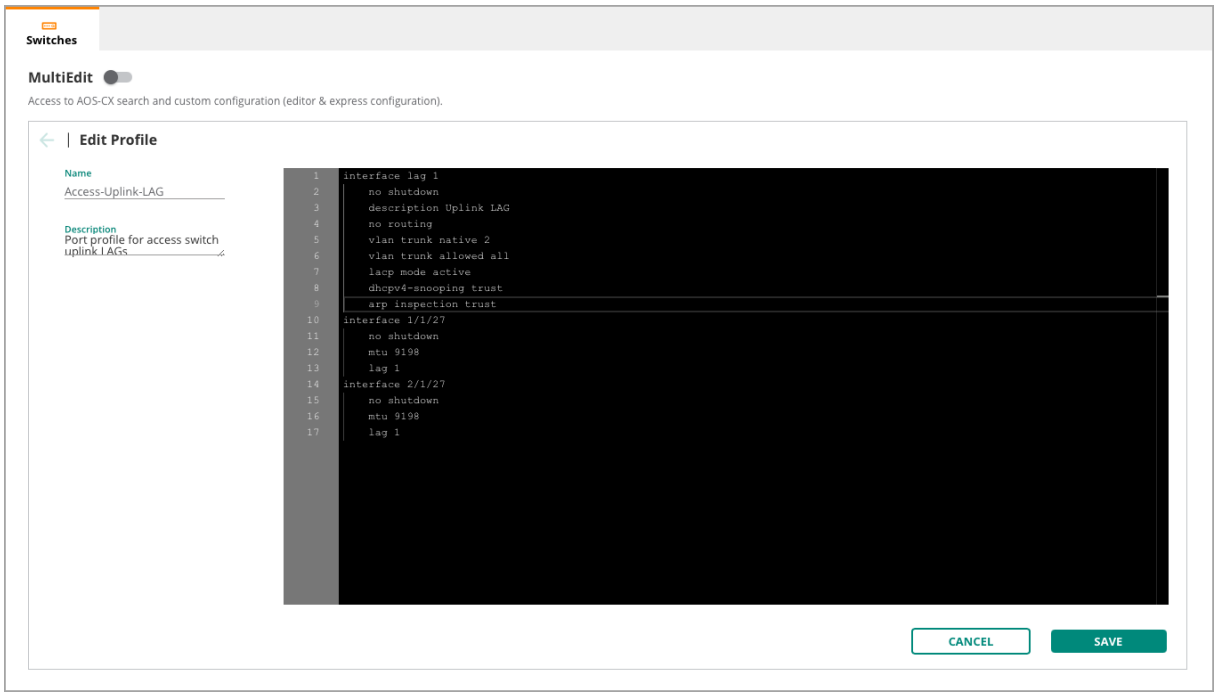

**Step 5** To edit the new profile, highlight the new row and click the **Edit** (pencil) icon.




**Step 6** In the **Edit Profile** window, enter the following LAG configuration, then click **Save**.

- **Name:** *Access uplink LAG*
- **Description:** *Port profile for access switch uplink LAGs*
- **CLI**:

```
interface lag 1
    no shutdown
    description Uplink LAG
    no routing
    vlan trunk native 2
    vlan trunk allowed all
    lacp mode active
    arp inspection trust
    dhcpv4-snooping trust
interface 1/1/27
    no shutdown
    mtu 9198
    lag 1
interface 2/1/27
    no shutdown
    mtu 9198
    lag 1
```

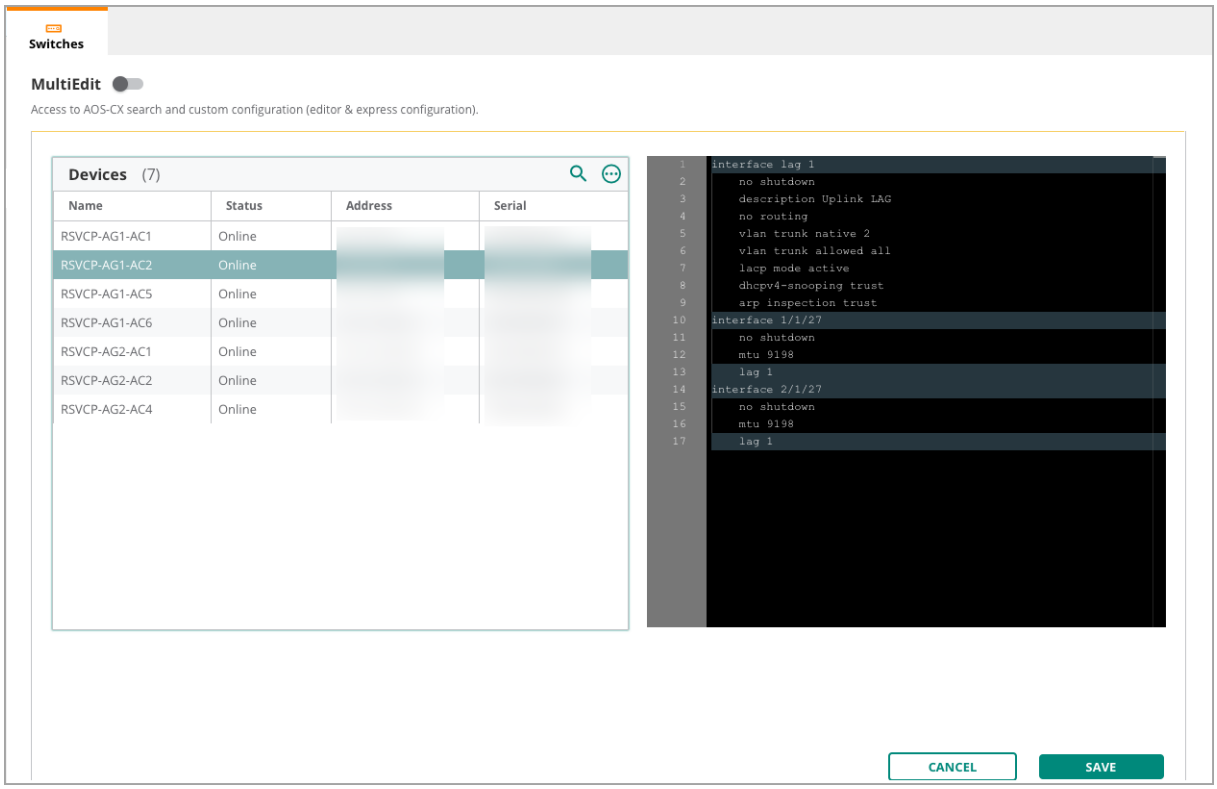



**CAUTION:**

DHCP snooping and ARP inspection must be trusted on the LAG interface to allow clients to receive DHCP addresses from the centralized DHCP servers on the network.

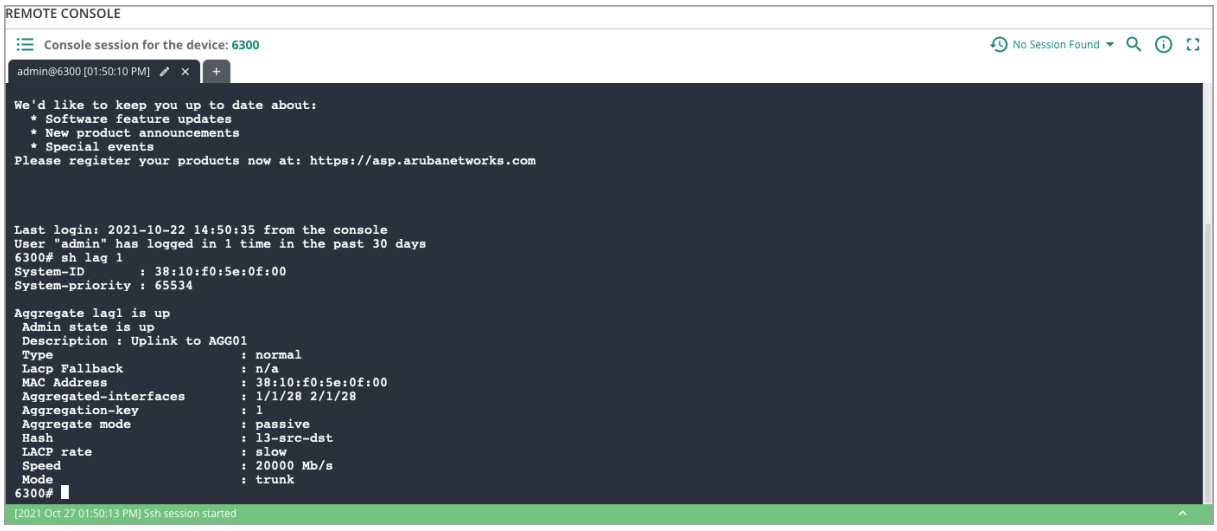
**Step 7** To apply the profile, highlight the profile row and click the **Apply** icon.

**Step 8** On the **Apply** screen, select the switches for LAG configuration, and click **Save**.




### *Verify LAG Operation*

**Step 9** Open a Remote Console window, type the command *`show lag 1`*, then press ENTER. The output shown below indicates a healthy, two-port LAG.




## Enable MultiEdit for the Group

**Step 1** In the upper left of the **Switches** page, move the slider right to enable **MultiEdit**.

**Step 2** Select the devices for editing. In the lower right window, click **EDIT CONFIG**.

The following steps provide configuration text that can be pasted into the MultiEdit window. After pasting the configuration, right-click any device-specific values. A **Modify Parameters** window appears on the right, allowing input of individual device values.

**NOTE:**

Interface configuration can optionally be performed using the Port Profiles feature documented later in this guide. This method is of particular interest to large installations with port configurations replicated across switches.

## Configure the Access VLANs

Access switches are configured with the same VLANs created on the aggregation switches in addition to an in-band management interface and a VLAN for User-Based Tunneling (UBT).

Both DHCP snooping and ARP inspection must be enabled to inspect traffic, prevent common attacks, and facilitate DHCP services across subnets. IGMP snooping is enabled and is required for Dynamic Multicast Optimization (DMO).

**NOTE:**

DHCP snooping must be enabled both globally and under each VLAN. ARP inspection is enabled only under the VLAN, but it does not take effect unless DHCP snooping also is enabled.

**Example: Access VLANs**

| VLAN Name | ZTP_NATIVE | EMPLOYEE | CAMERA | PRINTER | REJECT_AUTH | CRITICAL_AUTH | MGMT | UBT_CLIENT |
|---|---|---|---|---|---|---|---|---|
| **VLAN ID** | 2 | 3 | 5 | 6 | 13 | 14 | 15 | 4000 |

Enable DHCP snooping and create VLANs at the Group level.

**Step 1** Enable DHCP snooping globally.

```
dhcpv4-snooping
```

**Step 2** Enable DHCP snooping, ARP inspection, and IGMP snooping on each VLAN.

```
vlan 2
  name ZTP_NATIVE
  dhcpv4-snooping
  arp inspection
  ip igmp snooping enable
...
vlan 4000
  name UBT_CLIENT
  dhcpv4-snooping
  arp inspection
  ip igmp snooping enable
```

**CAUTION:**

The access switch VLANs must match the aggregation switch VLANs to enable the access devices to reach their default gateway.

**Step 3** Create a Layer 3 interface on each VLAN except the UBT_CLIENT VLAN and configure the same MTU size used in the aggregation layer.

```
interface vlan 2
  description ZTP_Native
  ip mtu 9198
  ip address 10.2.15.5/24
  ...
interface vlan 15
   description MGMT
   ip mtu 9198
   ip address 10.15.15.5/24
```

**NOTE:**

When using MultiEdit at the group level, right-click device-specific values to set values for individual devices in the group.

**Step 4** Configure the default route in the management VLAN. Add the static route for the active gateway IP address in VLAN 15.

```
ip route 0.0.0.0/0 10.2.15.1
```

**NOTE:**

The access switch must have a default route in the management VLAN to enable connectivity to network services such as Central, TACACS, RADIUS, and NTP servers.

## Configure Spanning Tree

Spanning tree is enabled by default on 6xxx family CX switches. The following procedure illustrates how to enable it when needed. Supplemental features such as admin-edge, root guard, BPDU guard, and TCN guard are enabled on appropriate interfaces to ensure that spanning tree runs effectively.

At the group level, add the following configuration:

**Step 1** Configure spanning tree globally. Multiple Spanning Tree Protocol (MSTP) is enabled by default.

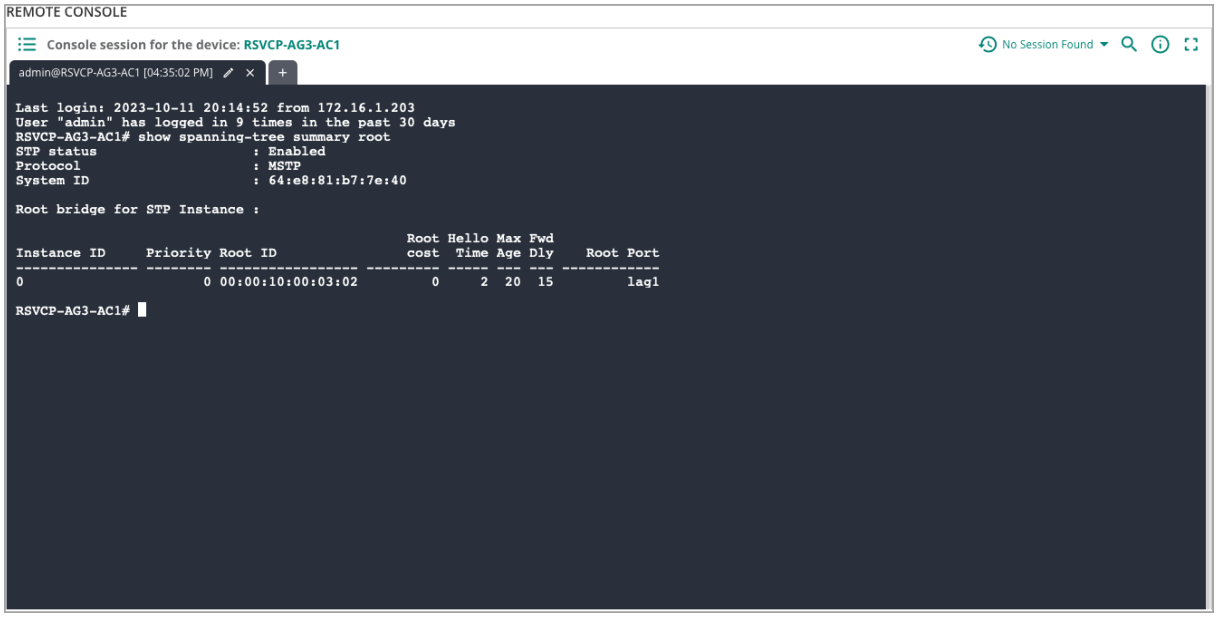
```
spanning-tree
```

**Step 2** Configure the port level spanning tree features and loop-protect on each access interface.

```
interface 1/1/1
  description ACCESS_PORT
  no shutdown
  no routing
  vlan access 1
  spanning-tree bpdu-guard
  spanning-tree port-type admin-edge
  spanning-tree root-guard
  spanning-tree tcn-guard
  loop-protect
  loop-protect action tx-disable
```

## Verify Spanning Tree

**Step 3** Open a Remote Console window, type the command *show spanning-tree summary root*, and press ENTER. The output shown below indicates a healthy MSTP configuration state.




## Configure RADIUS

Use this procedure to configure the RADIUS servers and UBT for the access switch.

Access switches authenticate devices attempting to connect to the network. The two most common methods to authenticate users include an 802.1X supplicant or MAC-based authentication. This design supports both, as well as dynamic authorization, which allows the AAA server to change the authorization level of the device connected to the switch.

RADIUS tracking is enabled to verify the status of the client and server. The configuration also employs user roles for rejected clients and RADIUS failures.

**Step 1** Configure the RADIUS servers. Enable RADIUS dynamic authorization and track client IP addresses with probes.

```
radius-server host 10.2.120.94 key plaintext <Password>
radius-server host 10.2.120.95 key plaintext <Password>
radius dyn-authorization enable
client track ip update-method probe
```

**Step 2** Configure AAA for 802.1X and MAC authentication.

```
aaa authentication port-access dot1x authenticator
    enable
aaa authentication port-access mac-auth
    enable
```

**Step 3** Configure AAA authentication on access ports by defining the client limit, enabling 802.1X and MAC authentication, and specifying the authentication order. Assign the critical and rejection roles to system-defined user roles that use local VLANs. Adjust EAPOL timeout and maximum requests, and retry limits as needed.

```
interface 1/1/1
  description ACCESS_PORT
  no shutdown
  no routing
  vlan access 1
  aaa authentication port-access client-limit 5
  aaa authentication port-access auth-precedence dot1x mac-auth
  aaa authentication port-access critical-role CRITICAL_AUTH
  aaa authentication port-access reject-role REJECT_AUTH
  aaa authentication port-access dot1x authenticator
    eapol-timeout 30
    max-eapol-requests 1
    max-retries 1
    reauth-peroid 300
    enable
  aaa authentication port-access mac-auth
   enable
```

## Configure Local User Roles

Use this procedure to configure the local user roles for the access switch.

The critical role is applied to devices when the RADIUS server is unreachable during the first authentication process or during reauthentication. This role helps ensure that the devices have limited access to the network even though the authentication is not completed. When the RADIUS server is available for authentication, the devices are authenticated and the ultimate role is applied.

The “reject” role is applied when the RADIUS server rejects a device during authentication. The reject role gives restricted access to the device, unlike a full access role.

```
port-access role CRITICAL_AUTH
  reauth-period 120
  auth-mode client-mode
  vlan access 14
port-access role REJECT_AUTH
  reauth-period 120
  auth-mode client-mode
  vlan access 13
```

## Configure Device Profiles

Create a device profile that detects HPE Aruba Networking APs dynamically, places them into the management VLAN, and allows locally bridged VLANs.

**NOTE:**

This procedure is unnecessary if ClearPass is used to authenticate APs.

**Step 1** Configure the *ARUBA-AP* role. Create the role, set the authentication mode, set the native VLAN, and define the allowed VLANs.

```
port-access role ARUBA-AP
  auth-mode device-mode
  vlan trunk native 15
  vlan trunk allowed 1-3,5-6,13-15
```

**NOTE:**

The *ARUBA-AP* role identifies the AP's VLAN and identifies which VLANs are bridged locally.

**Step 2** Configure the LLDP group. Create the group and identify the AP OUIs.

```
port-access lldp-group AP-LLDP-GROUP
  seq 10 match vendor-oui 000b86
  seq 20 match vendor-oui D8C7C8
  seq 30 match vendor-oui 6CF37F
  seq 40 match vendor-oui 186472
  seq 50 match sys-desc ArubaOS
```

**NOTE:**

The LLDP group identifies the APs and sets the system-description at the end as a catchall for future APs.

**Step 3** Configure the device profile. Create the profile, enable it, then associate it with the role and LLDP group created previously.

```
port-access device-profile ARUBA_AP
  enable
  associate role ARUBA-AP
  associate lldp-group AP-LLDP-GROUP
```

Devices in the group automatically synchronize the new configuration. Synchronization status is updated on the **Configuration Status** page. Click **Audit Trail** in the left menu to observe step execution.

## Configure User Based Tunneling

User-Based Tunneling (UBT) enables selective traffic tunneling to an AOS-10 gateway cluster for centralized policy enforcement. Design considerations for UBT are detailed in the UBT Design Chapter. Many campus environments that deploy UBT selectively tunnel certain clients to the gateway for application of centralized policy. This procedure illustrates tunneling wired IOT devices with the role of IOT-LIMITED to the gateway using reserved VLAN mode. Additional roles can be tunneled following this procedure.

**Step 1** Create the UBT client VLAN and UBT zone. The UBT client VLAN serves as a local placeholder for clients on the edge switch. The UBT zone provides detail on the gateway cluster and enables UBT. The *primary-controller* is the system IP of a gateway cluster member. The switch reaches out to the primary-controller, which provides details to the switch for establishing tunnels to necessary gateways.

- **UBT Client VLAN:** *4000*
- **UBT Zone:** *Aruba*

```
ubt-client-vlan 4000

ubt zone OWL vrf default
  primary-controller ip 10.6.15.11
  enable
```

**NOTE:**

Do not use the `backup-controller` command unless a separate cluster is designated for backup. The `primary-controller` establishes connectivity between the switch and all gateways within the cluster.

**Step 2** Set the source IP address for all services to the management VLAN IP address.

```
ip source-interface all interface vlan15
```

**Step 3** Define the required local user roles along with their associated parameters. For tunneled VLANs, specify the gateway zone and corresponding gateway role. Matching role names between the switch and the gateway is recommended for consistency. The following example illustrates the IOT-LIMITED role. Add additional roles as needed.

```
port-access role IOT-LIMITED
    auth-mode client-mode
    gateway-zone zone OWL gateway-role IOT-LIMITED
```

### *Modify Gateway Configuration*

When user traffic is tunneled from a UBT-enabled switch to a gateway, the gateway assigns a user role that defines policy enforcement. Each role must be mapped to a VLAN to ensure that clients are placed in the appropriate network segment.

Multiple roles can be mapped to a single VLAN. In this model, the VLAN provides macro-level segmentation, while gateway-enforced policies deliver micro-level segmentation based on the assigned role. This design supports centralized, role-based policy enforcement while maintaining IP subnet-based filtering capabilities at other points in the network.

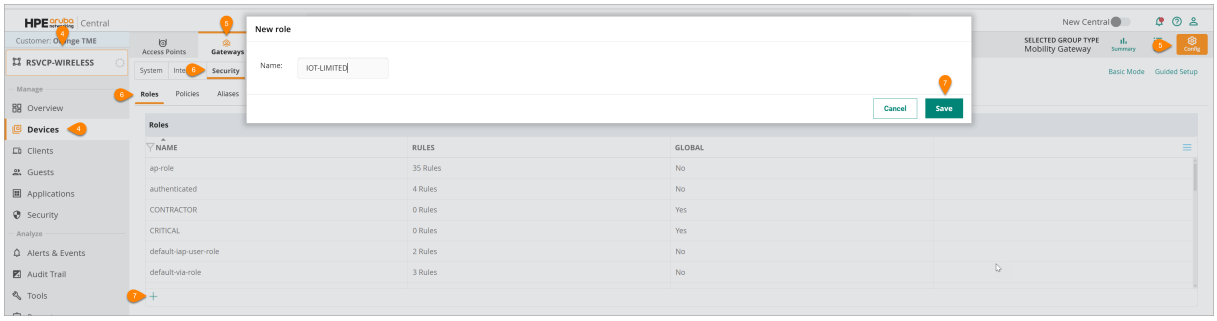
This procedure extends the existing tunneled WLAN configuration defined in the WLAN deployment guide. The WLAN does not use roles. A new role, **IOT-LIMITED**, is created on the gateway. A corresponding policy is applied, and the role is mapped to the same VLAN (VLAN 103) used by the WLAN profile. Alternatively, a dedicated VLAN can be configured for wired UBT traffic to maintain separation from the wireless WLAN segment, if required by the design.

**Step 4** In Aruba Central, navigate to the group containing the UBT-enabled gateways (in this example, **RSVCP-WIRELESS**), then click **Devices**.

**Step 5** Select the **Gateways** tab, then click **Config**. Ensure that advanced mode is selected.

**Step 6** Under **Security**, select **Roles**.

**Step 7** Click the **+** icon, enter **IOT-LIMITED** as the role name, then click **Save**.



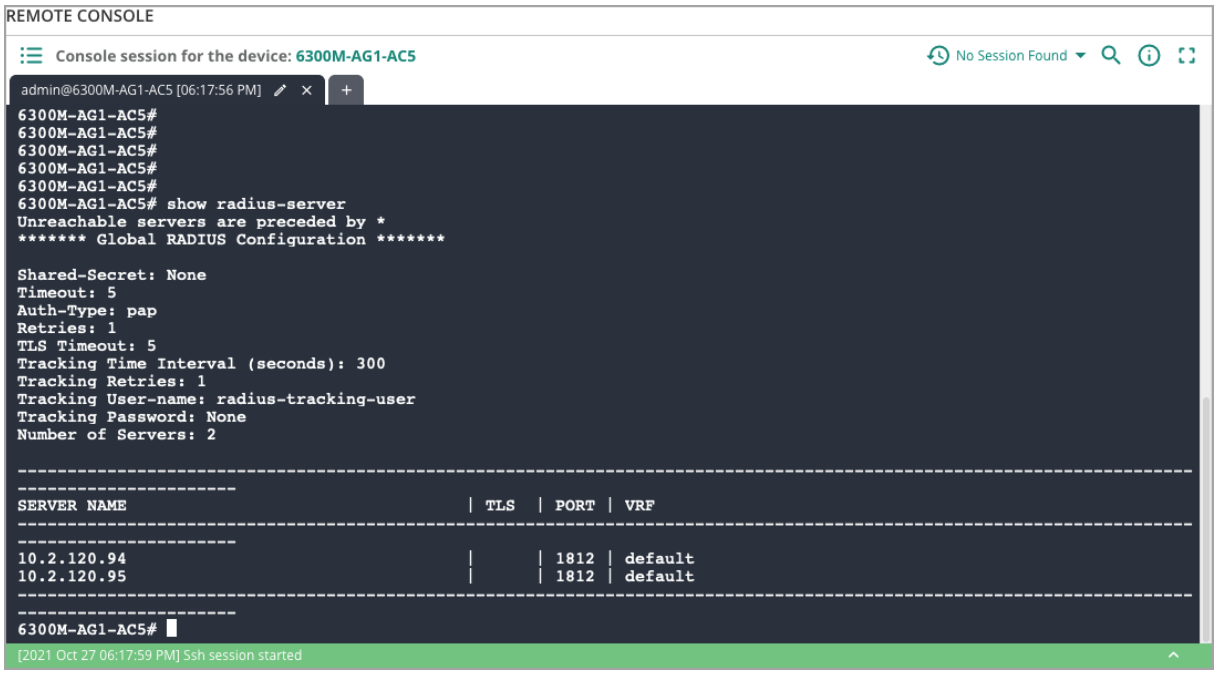

**Step 8** Create and assign policies to the **IOT-LIMITED** role. Refer to the section on Configuring Network Policy with User Roles.

**Step 9** Map VLAN 103 to the **IOT-LIMITED** role. Refer to the section on Associating VLANs to User Roles.

**Step 10** Repeat these steps for each additional role as needed.

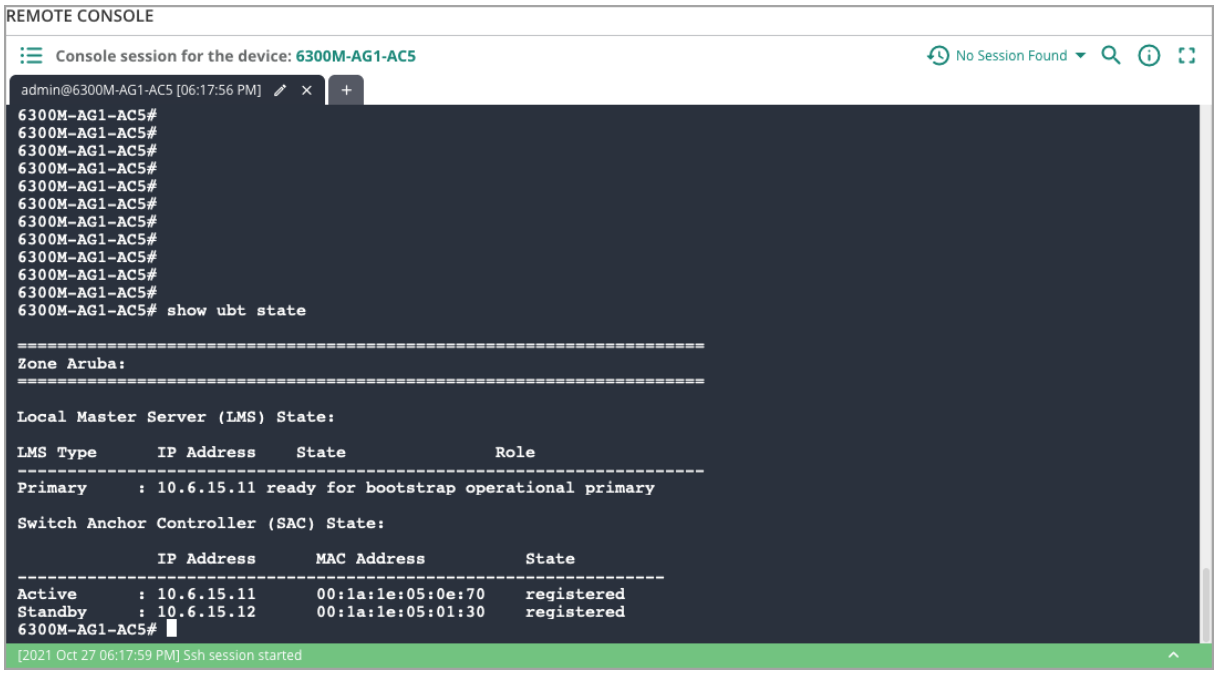
## Verify RADIUS

**Step 11** Open a Remote Console window, type the command `show radius-server`, then press ENTER. The output shown below indicates a healthy RADIUS server configuration.




## Verify UBT

**Step 12** Open a Remote Console window, type the command *`show ubt status`*, then press ENTER. The output shown below indicates a healthy UBT configuration state.



## Configure Interfaces Using a Port Profile

As an alternative to the preceding MultiEdit examples, interface configuration can be completed using the Port Profiles feature. This feature of Central applies the same port level configurations to multiple switches, or switch stacks, at the same time. Create a port profile using the interface level configuration from the previous spanning-tree and RADIUS/UBT sections.

Before proceeding, ensure that spanning tree is enabled, RADIUS authentication is configured, and that local user roles are created. Refer to the preceding procedures for configuration examples.

**Step 1** On the left menu, select **Devices**.

**Step 2** At the upper left of the **Switches** page, de-select **MultiEdit** (if enabled).

**Step 3** Select **Port Profiles** on the **Interfaces** tile.

**Step 4** To clone the **Sample Access Port** profile, click the **Clone** icon visible when the row is highlighted.

**Step 5** Name the new port profile and click the **Clone** button.

**Step 6** In the **Edit Profile** window, enter the following access port configuration, then click **Save**.

- **Name:** *Access ports*
- **Description:** *Port profile for access switch ports*
- **CLI**:

```
interface 1/1/1-1/1/12
  description ACCESS_PORT
  no shutdown
  no routing
  vlan access 1
  spanning-tree bpdu-guard
  spanning-tree port-type admin-edge
  spanning-tree root-guard
  spanning-tree tcn-guard
  loop-protect
  loop-protect action tx-disable
  port-access onboarding-method concurrent enable
  aaa authentication port-access allow-cdp-bpdu
  aaa authentication port-access allow-lldp-bpdu
  aaa authentication port-access client-limit 5
  aaa authentication port-access auth-precedence dot1x mac-auth
  aaa authentication port-access critical-role CRITICAL_AUTH
  aaa authentication port-access reject-role REJECT_AUTH
  aaa authentication port-access dot1x authenticator
    eapol-timeout 30
    max-eapol-requests 1
    max-retries 1
    enable
  aaa authentication port-access mac-auth
    enable
```

**CAUTION:**

Ensure that indent levels copy accurately into the Port Profiles editor.

**Step 7** To apply the profile, highlight the profile row and click the **Apply** icon.

**Step 8** In the **Apply** screen, select the switches for access configuration, and click **Save**.

# Campus Wireless Connectivity

Aruba access points deliver seamless connectivity for Wi-Fi 6, interoperability with previous generations of Wi-Fi, and support for today's rapidly proliferating IoT devices. Aruba Gateways offer high-performance network access, dynamic security, and resiliency for the campus and branch. The Aruba ESP solution for wireless connectivity in the campus is designed for reliability and performance using AI-powered RF optimization, WPA3 for secure connectivity, and role-based access control with deep packet inspection for classification and segmentation of traffic.

Aruba APs can enforce policy and bridge traffic locally or they can tunnel traffic to a gateway device. Tunneling to a gateway centralizes policy enforcement with advanced segmentation rules, and leverages the capabilities of an application-aware stateful firewall.

# Wireless Group Configuration

HPE Aruba Networking Central uses a two-level hierarchy for configuration tasks. A device's final configuration is the result of common configuration applied at the group level, along with individual configuration applied at the device level. Parameters added at the device level override the configuration assigned at the group level. Best practice is to perform the bulk of the configuration at the group level and use device-level configurations only when specific overrides are needed.

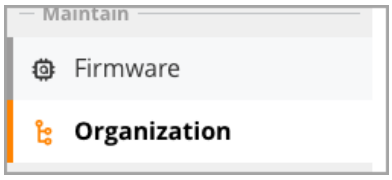
## Configure a Central Group for Wireless Management

Use this procedure to create a group for configuring and managing the wireless environment. This group consists of APs and gateways deployed with the AOS10 architecture. The APs are deployed as campus devices along with gateways, since an AP-only deployment does not offer advanced features such as UBT. The WLAN profiles can be configured to forward traffic in Bridged mode, Tunnel mode, or mixed mode.

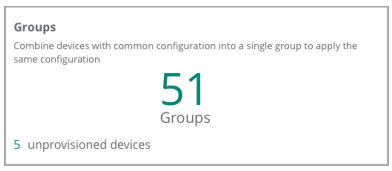
The gateways serve as Mobility gateways to support WLAN and LAN functions in the campus network. They do not support WAN capabilities in this mode. For more guidance on AP and gateway deployment, refer to the Access Point Deployment and Gateway Deployment page of the AOS 10 Fundamentals Guide. This section assumes that the AP's and Gateways are placed in the same group to streamline navigation between the two settings tabs during network deployment.

**Step 1** Login to **HPE Greenlake** and go to **HPE Aruba Networking Central**.

**Step 2** In the left navigation pane, in the **Maintain** section, select **Organization**.

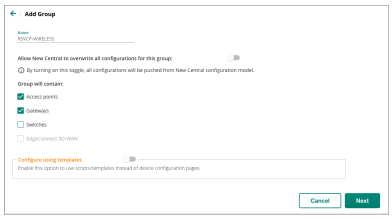



**Step 3** Select the **Groups** tab.



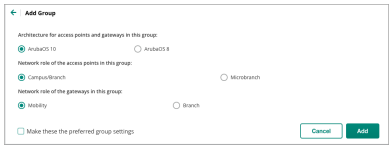

**Step 4** Click the **+** (plus sign) at the top right to create a new group.

**Step 5** Type a name for the group and select the two checkboxes for **Gateways** and **Access points**. Click **Next**.




**Step 6** On the **Add Group** page, assign the following settings, and click **Add**.

- **Architecture for access points and gateways in this group:** *ArubaOS 10*
- **Network role of the access points in this group:** *Campus/Branch*
- **Network role of the gateways in this group:** *Mobility*

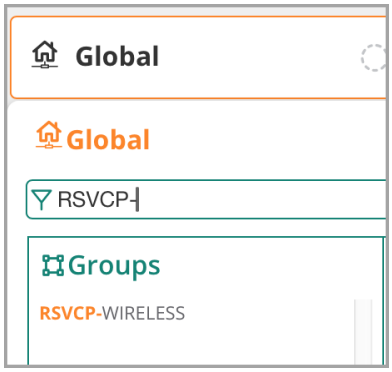



## Configure AP Settings for Group

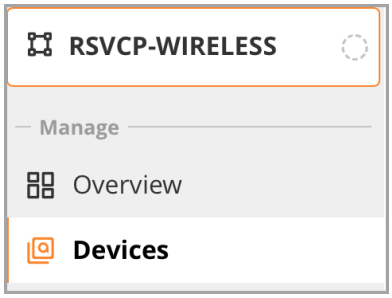
Use this procedure to configure AP settings in the group. This procedure assumes that the APs are deployed with the AOS 10 operating system.

**Step 1** Login to **HPE Greenlake** and go to **HPE Aruba Networking Central**.

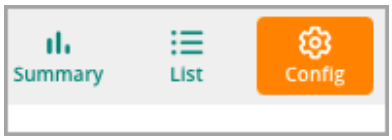
**Step 2** In the filter dropdown, select the wireless group. In this example, the group is **RSVCP-WIRELESS**.




**Step 3** On the left menu, select **Devices**.




**Step 4** In the upper right corner of the **Access Points** page, click **Config**.

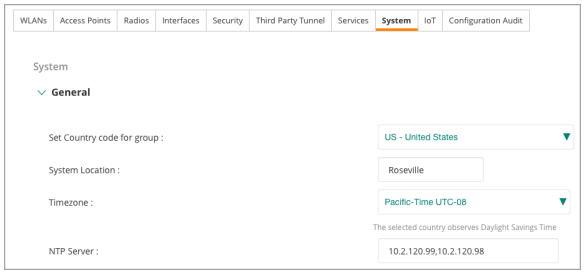



**Step 5** Enter and confirm a password for the group. Click **Set Password**.

**Step 6** On the **Access Points** page, select the **System** tab.


**Step 7** Expand the **General** section on the **System** tab, assign the following settings, then click **Save Settings**.

- **Set Country code for group:** *US - United States*
- **System Location:** Roseville
- **Timezone:** *Pacific-Time UTC-08*
- **NTP Server:** *10.2.120.99, 10.2.120.98*




**CAUTION:**

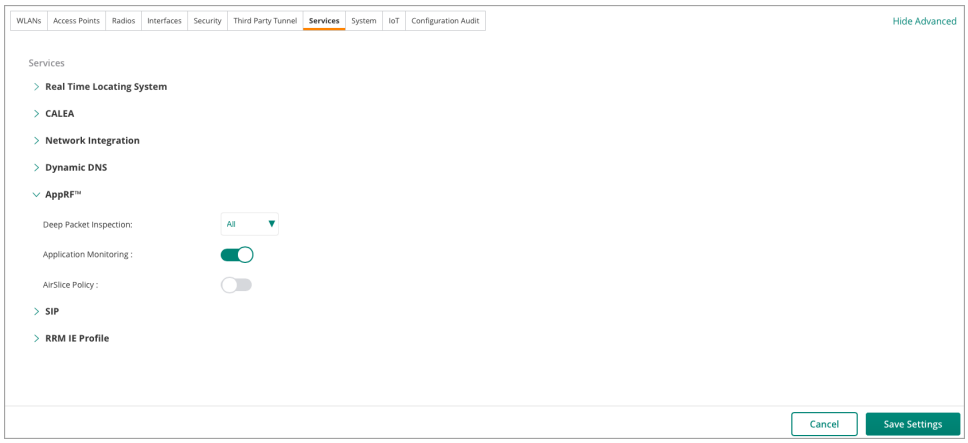
Incorrect time synchronization within the network can lead to authentication errors. An NTP server defined in the Group configuration takes precedence over an NTP configured with DHCP. Ensure that time synchronization is consistent across the network.

**NOTE:**

All APs in the group must have the same country code. Create a group for each country code in the network. The country code must be set before a configuration is pushed to an AP.

**Step 8** Click the **Services** tab and expand the **AppRF** section. Assign the following settings, then click **Save Settings**.

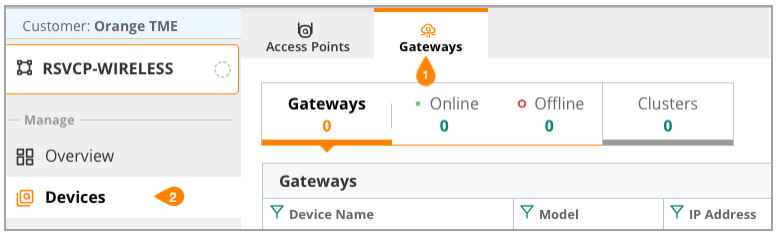
- **Deep Packet Inspection:** *All*
- **Application Monitoring:** *Slide to the right*



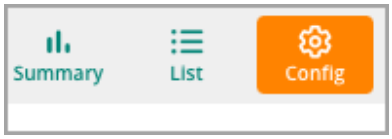

## Configure Gateway Settings for Group

An AOS-10 Mobility Gateway group or an AOS-10 Mobility Gateway can be configured using Guided Setup, Basic mode, or Advanced mode. This section outlines the procedure for configuring group settings for Mobility Gateways using Advanced mode, which offers more options for customizing gateway deployment.

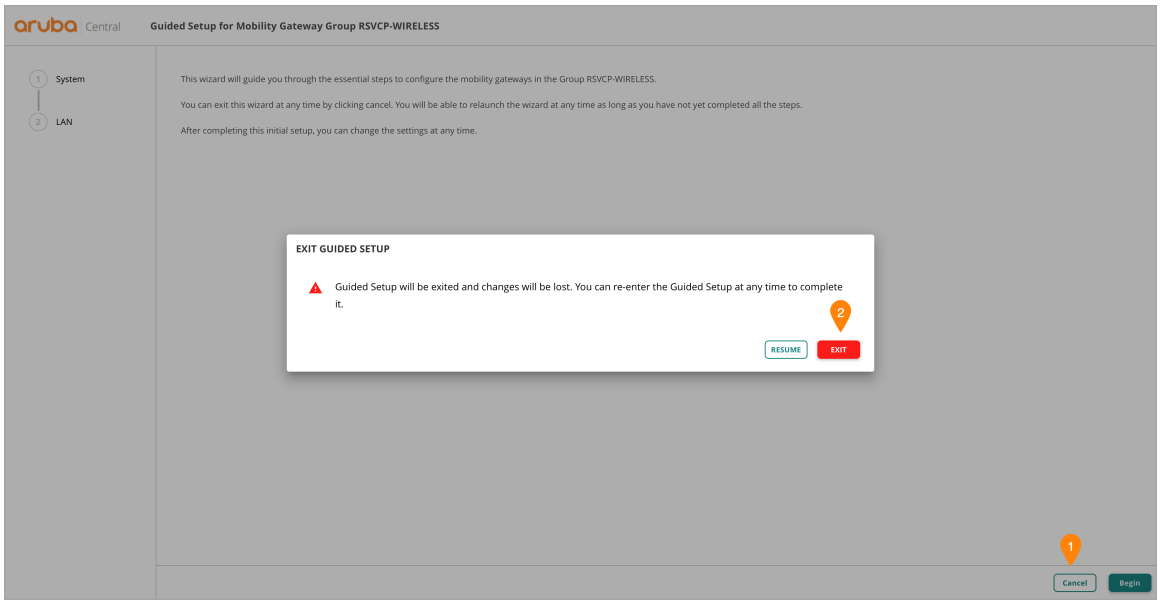
**Step 1** Select the **Gateways** tab. On the left menu, select **Devices**.



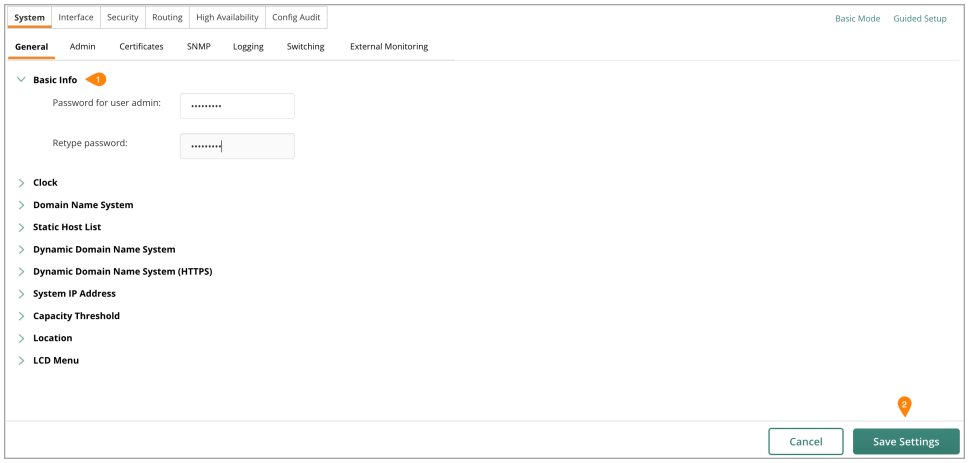

**Step 2** In the upper right of the **Gateways** page, click **Config**.




**Step 3** Click **Cancel** to exit the Guided Setup wizard and switch to Advanced setup. Then click **Exit** at the **EXIT GUIDED SETUP** prompt.

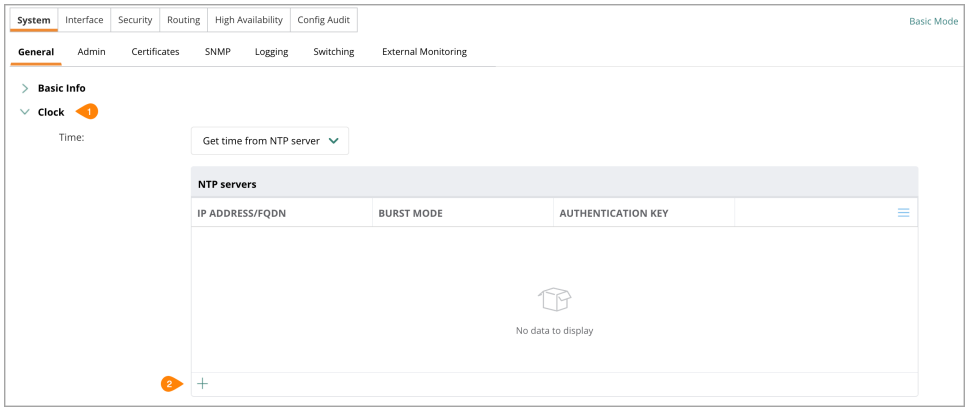



**Step 4** Expand the **Basic Info** section on the **General** tab and update the password. Click **Save Settings**.



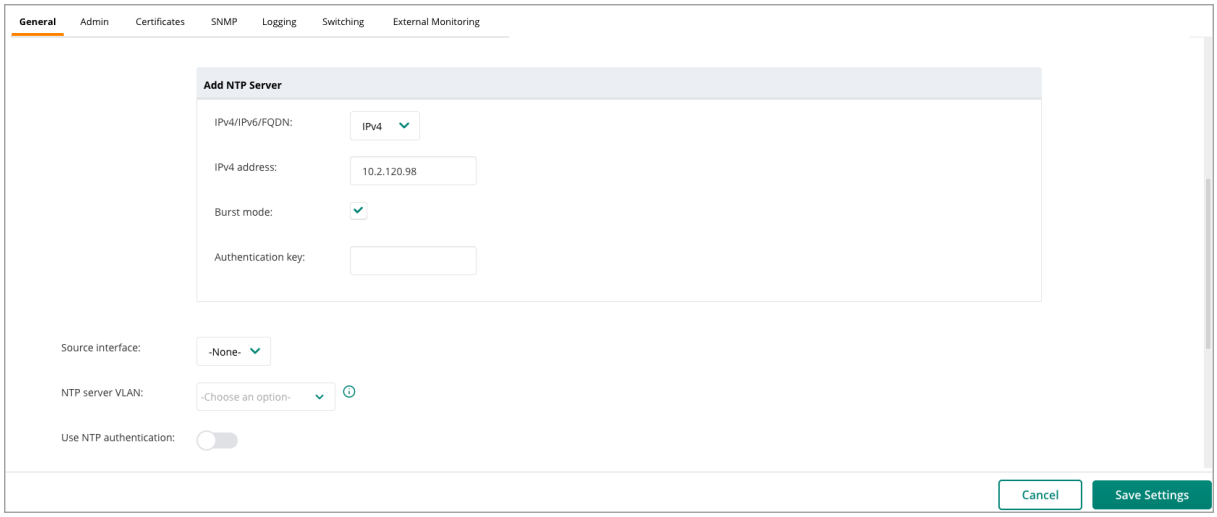

## Configure NTP and Time Zone Settings

**Step 1** Select the **General** tab and expand the **Clock** section. Click the **+ (plus sign)** to add a reachable NTP server.



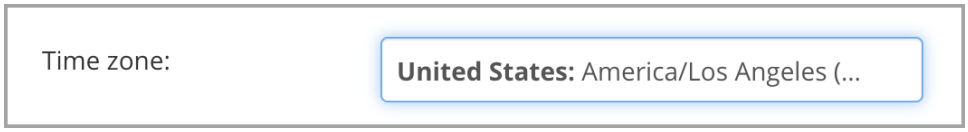
**Step 2** Assign the following settings. Click **Save Settings**.

- **IPv4/IPv6/FQDN:** *IPv4*
- **IPV4 ADDRESS:** *10.2.120.98*
- **Burst Mode:** *Enabled*




**Step 3** Repeat the previous step to enter additional NTP servers.

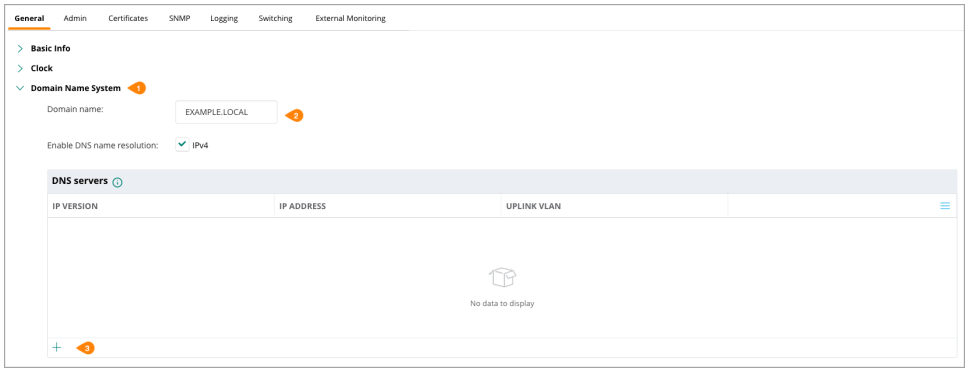
**Step 4** Select the **Timezone**, then click **Save Settings**.




## Configure Domain and DNS Settings

**Step 1** Expand the **Domain Name System** section on the **General** tab and assign the domain name. Click on the **+ (plus sign)** to add a reachable DNS server.

- **Domain name:** *EXAMPLE.LOCAL*




**Step 2** Assign the following settings. Click **Save**.

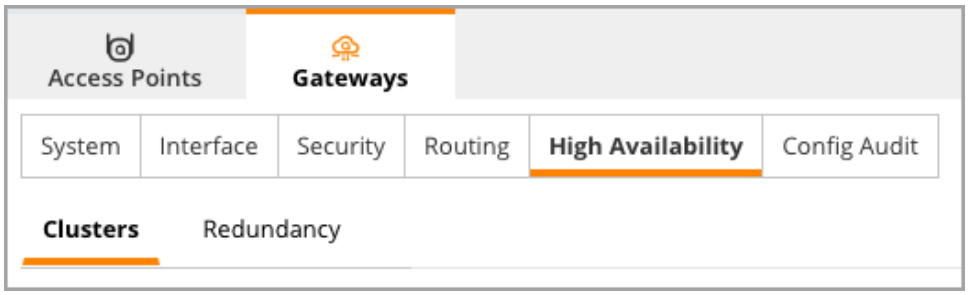
- **IP version:** *IPv4*
- **IPV4 ADDRESS:** *10.2.120.98*


**Step 3** Repeat the previous step to enter additional DNS servers. Finally click **Save Settings**.

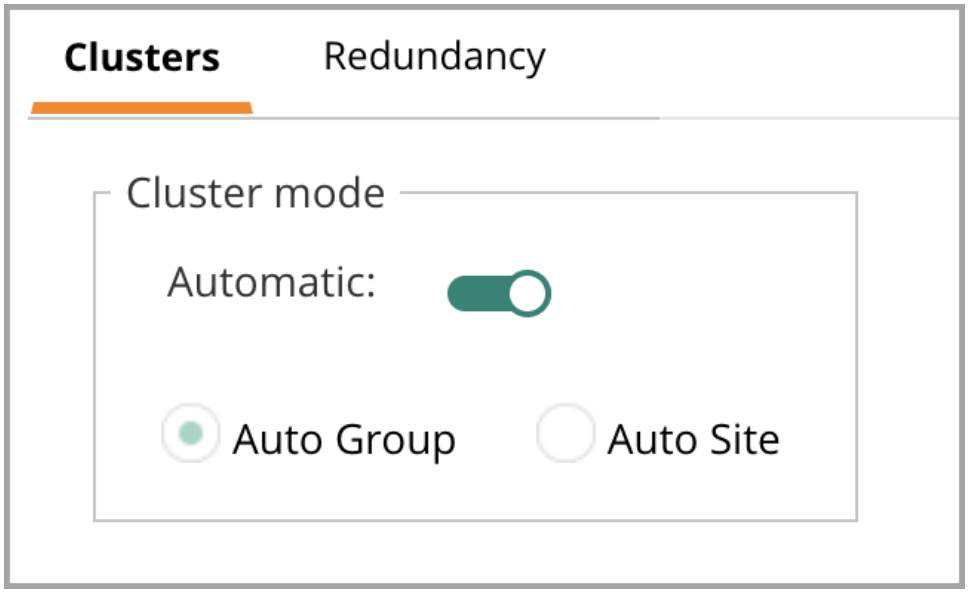
## Configure Gateway Cluster Settings

AOS 10 supports automatic and manual clustering modes to support gateways that are deployed for wireless access, User Based Tunneling (UBT), or VPN Concentrators (VPNCs). This section details the process to set up a gateway cluster using Auto Group mode, which gives the flexibility of forming clusters of gateways belonging to different sites. With auto group clusters, APs can reside in the same configuration group as the gateways or in a separate group and can be assigned to WLAN profiles configured for tunnel and mixed forwarding mode. For more guidance, refer to the **Auto Group Clustering** section of the AOS 10 Fundamentals Guide.

**Step 1** On the **Gateways** tab, click the **High Availability** tab.




**Step 2** Select the **Clusters** tab and click the toggle to turn on **Automatic** cluster mode. Click the radio button next to **Auto Group**, then click **Save Settings**.



**NOTE:**

Only one auto group cluster is permitted for each configuration group. Campus deployments with multiple clusters will implement one configuration group for each cluster.

## Configure Jumbo Frame Processing

Enable jumbo frame processing to accommodate frames exceeding 1500 bytes. This ensures that encapsulated frames, such as within VXLAN packets, are able to transit the network unfragmented.

**Step 1** Go to the Central UI group with the gateways and select **Devices**.

**Step 2** Select the **Gateways** tab.

**Step 3** Click **Config** to enter configuration mode.

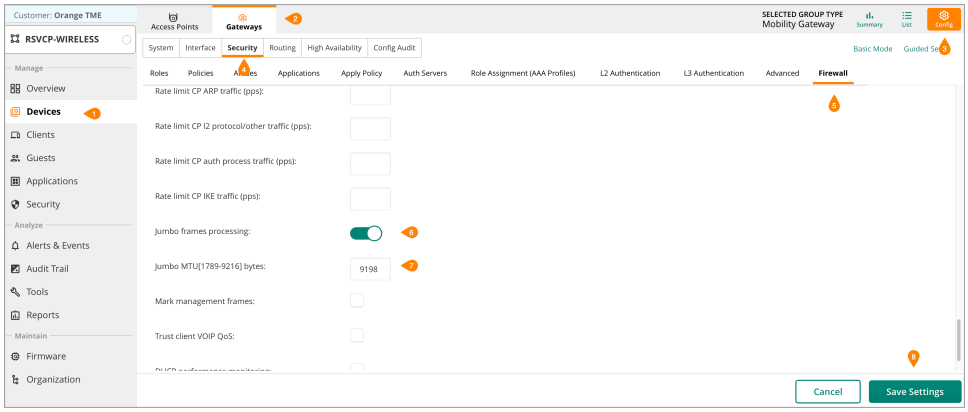
**Step 4** Select the **Security** tab.

**Step 5** On the **Security** tab, select the **Firewall** page.

**Step 6** Move the slider right to enable **Jumbo frame processing**.

**Step 7** Set the **Jumbo MTU** to the following value: - **Jumbo MTU[1789-9216] bytes:** *9198*.

**Step 8** Click **Save Settings**.



# Gateway Devices Configuration

In large-scale campus networks, gateway clusters are deployed within the services aggregation layer. Wireless LANs (WLANs) are tunneled to these gateways to take advantage of advanced policy enforcement and firewall capabilities available on the platform. Gateway clustering is implemented to ensure high availability and throughput.

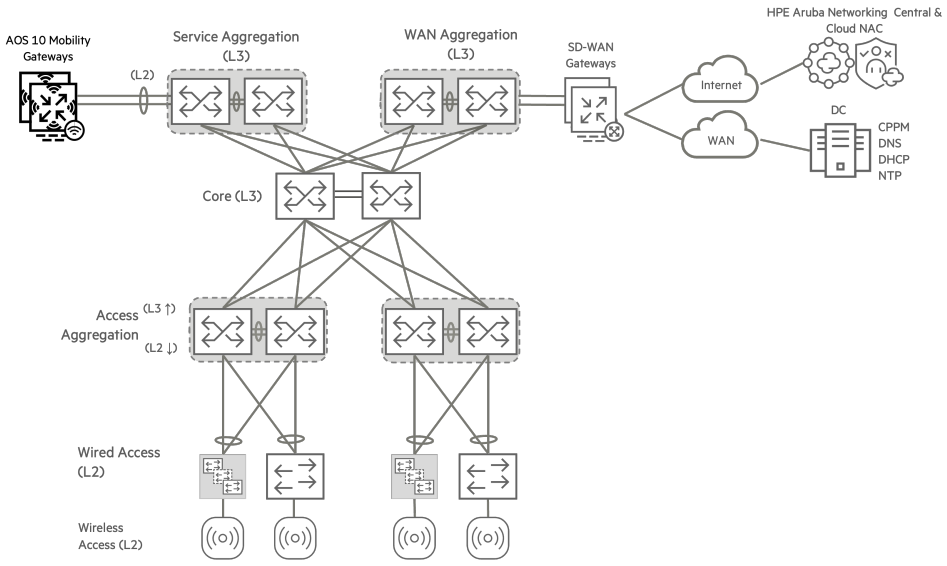



**Figure 21:** Option 1

This section outlines the steps to deploy a gateway in Central using the Zero Touch Provisioning (ZTP) process. The table below provides details on the VLANs and IP addresses used in the procedures.

**Example: IP Addresses and VLAN ID**

| Name | IP address | Default gateway | VLAN ID | VLAN name | Gateway VRRP Address |
|---|---|---|---|---|---|
| RSVCP-SS3-CL1-1 | 10.6.15.11/24 | 10.6.15.1 | 15 | MGMT | 10.6.15.13 |
| RSVCP-SS3-CL1-2 | 10.6.15.12/24 | 10.6.15.1 | 15 | MGMT | 10.6.15.14 |

## Configure Gateway VLANs

Use the following procedure to configure Gateway VLANs.

**Example: VLANs for Gateways**

| VLAN Name | VLAN ID |
|---|---|
| MGMT | 15 |
| EMPLOYEE | 103 |

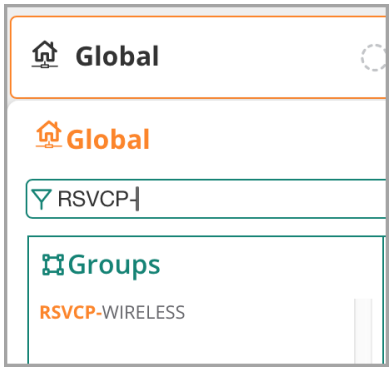
| VLAN Name | VLAN ID |
|---|---|
| BLDG-MGMT | 104 |
| CAMERA | 105 |
| PRINTER | 106 |
| VISITOR | 112 |
| REJECT_AUTH | 113 |
| CRITICAL_AUTH | 114 |
| ZTP | 4094 |

**CAUTION:**

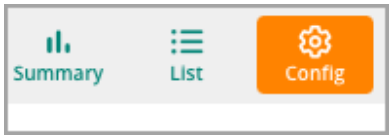
The Gateway VLANs must be created before adding the port channels, so the Native VLAN and Allowed VLANs can be selected from the dropdown lists.

**Step 1** Login to **HPE Greenlake** and go to **HPE Aruba Networking Central**.

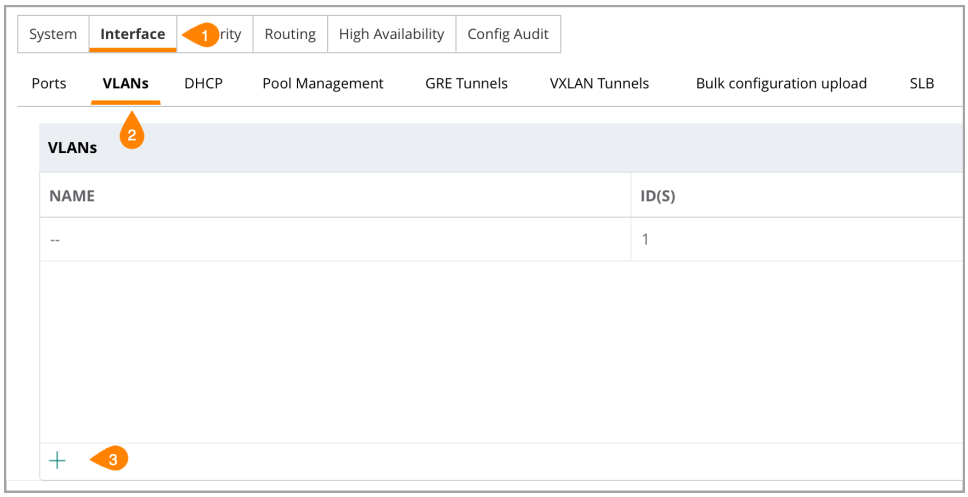
**Step 2** In **Global > Groups**, locate the group. In this example, the group is *RSVCP-WIRELESS*.




**Step 3** In the upper right of the **Gateways** page, click **Config**.

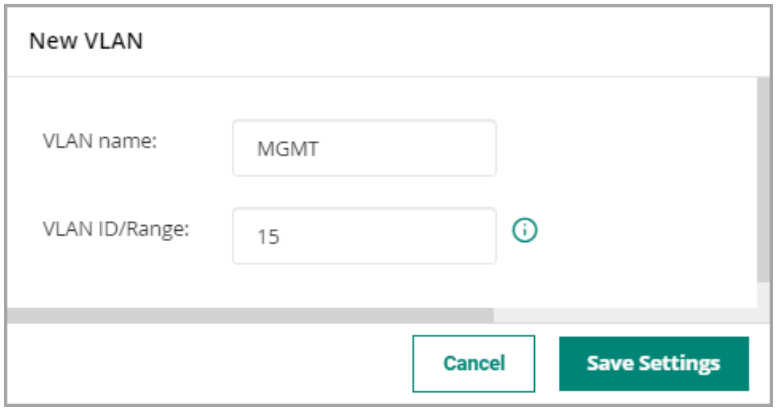



**Step 4** Select the **Interface** tab, and click **VLANs**. Click the **+** (plus sign) in the lower left to add a new VLAN.




**Step 5** In the **New VLAN** window, assign the following settings, then click **Save Settings**.

- **VLAN name:** *MGMT*
- **VLAN ID/Range:** *15*




**Step 6** Repeat this procedure for each Gateway VLAN in the environment.

## Enable Physical Interfaces

Use this procedure to enable gateway physical interfaces in a group for configuration.

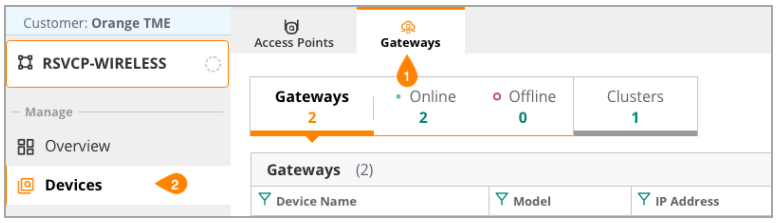
The ESP Campus supports Zero Touch provisioning (ZTP) of gateway devices. ZTP requires that physical interface configuration must be performed for Gateways at the group level. To simplify this configuration, best practice is to standardize a single gateway model within each group.

**CAUTION:**

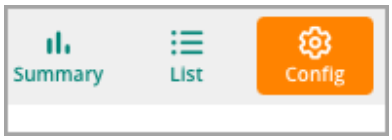
If a group-level interface configuration is applied to a gateway that does not have the specified physical interface, the gateway is not added to the group. The unsupported interface must be removed from the group configuration to add the gateway.

**Step 1** In **Groups**, locate the wireless group. In this example, the group is *RSVCP-WIRELESS*.

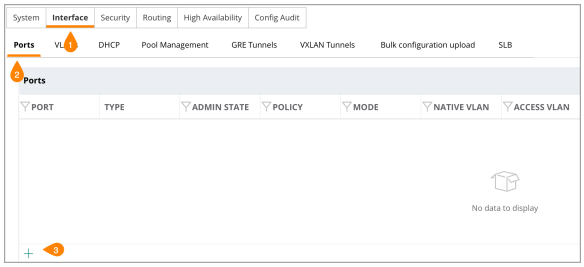
**Step 2** Select the **Gateways** tab. On the left menu, select **Devices**.



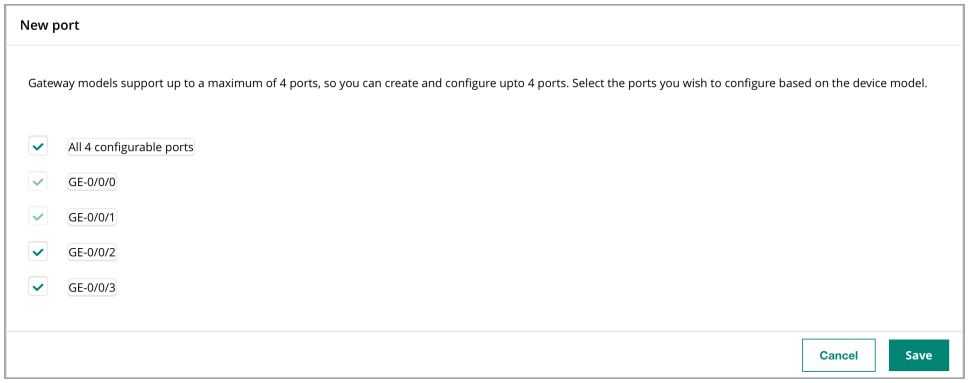

**Step 3** Click **Config** in the upper right.




**Step 4** Select the **Interface** tab, then the **Ports** tab. Click the **+** (plus sign) at the bottom left of the Ports table to add a port.




**Step 5** On the **New port** window, click the checkbox next to the interface name, then click **Save**.




## Configure Port Channels

Use the following procedure to configure Gateway port channels.

In deployments for which uptime and performance are priorities, best practice for gateway connectivity is to use LACP on a multi-chassis LAG (MC-LAG) connected to a pair of switches that support the VSX feature. LACP is enabled on the gateway as part of the Port Channel configuration.

When a Gateway is deployed using ZTP, it does not have an LACP configuration initially. To accommodate this during the provisioning process, LACP Fallback is enabled on the uplink switch. An example configuration for the implementation of the LACP Fallback command in a MC-LAG is shown below:

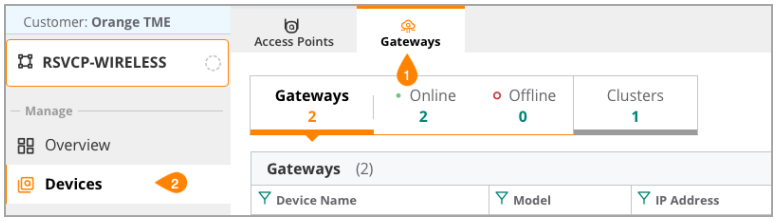
```
interface lag 11 multi-chassis
    description RSVCP-SS3-CL1-1
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
    lacp fallback
```

**NOTE:**

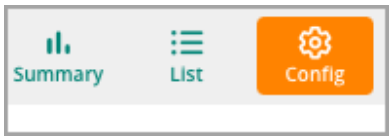
When LACP negotiation fails, LACP Fallback allows switch ports to function as standard access/trunk ports until LACP functions.The above configuration snippet illustrates the implementation of the LACP Fallback command in context. Refer to earlier sections of this guide for complete switch configuration.

**Step 1** In **Groups**, locate the wireless group. In this example, the group is *RSVCP-WIRELESS*.

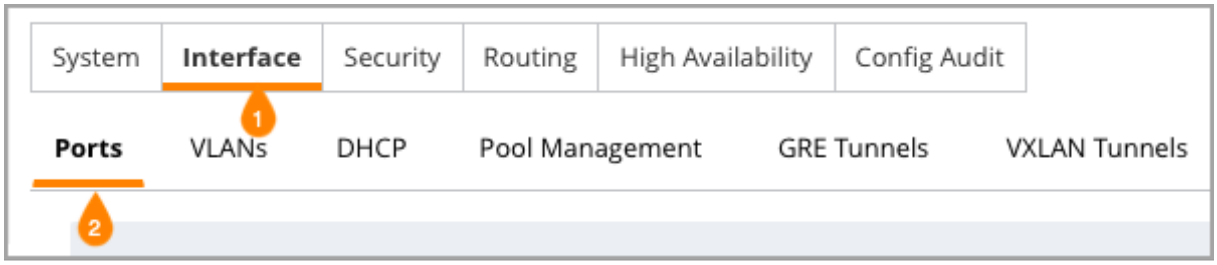
**Step 2** Select the **Gateways** tab. On the left menu, select the **Devices** tab.



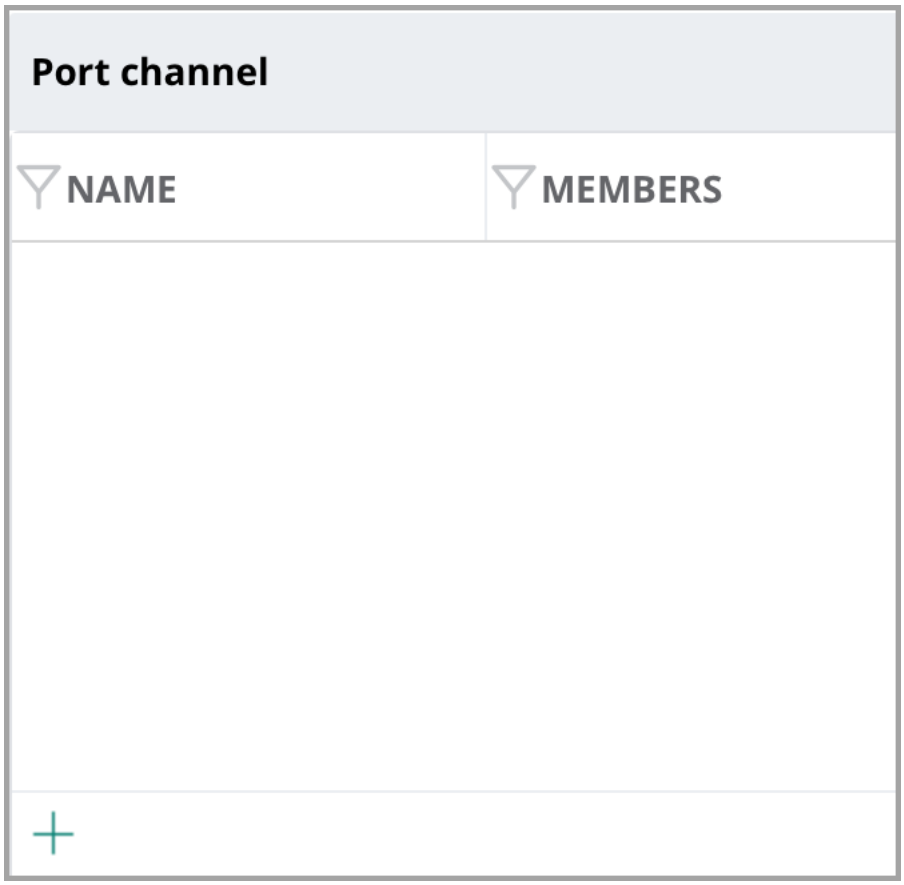

**Step 3** Select **Config** in the upper right.



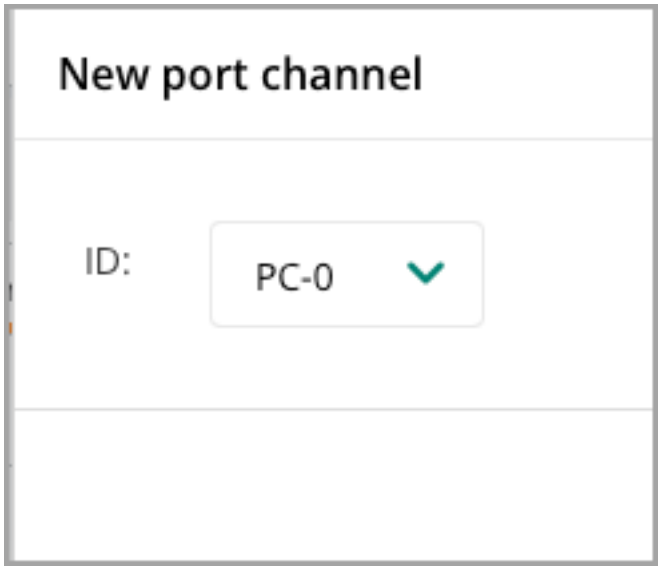

**Step 4** Select the **Interface** tab, then the **Ports** tab.




**Step 5** In the **Port channel** section, click the **+** (plus sign) to add a port channel.



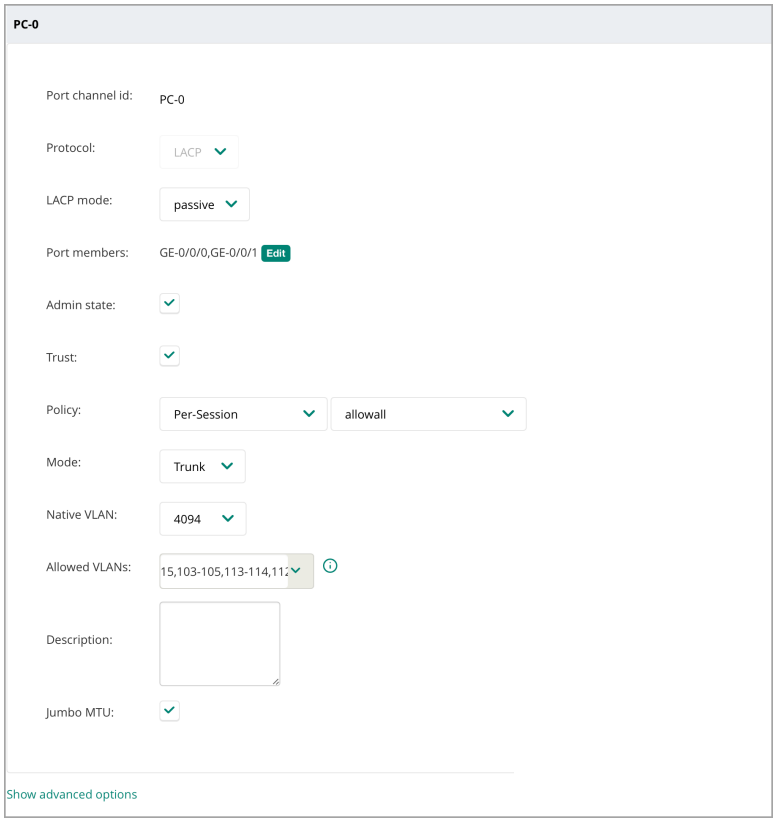

**Step 6** In the **New port channel** window, select the next available PC-*n* ID; in this example *PC-0*. Click **Save**.




**Step 7** In the **PC-*n*** section, assign the following settings.

- **Protocol**: *LACP*
- **LACP Mode:** *Passive*
- **Port Members:** Click **Edit**, select port channel ports under **Available**, use the right arrow to move them to **Selected**, then click **OK**.
- **Admin State:** *checkmark*

- **Trust:** *checkmark*
- **Policy:** *Per-Session* and *allowall*
- **Mode:** *Trunk*
- **Native VLAN:** *4094*
- **Allowed VLANS:** *15, 102-106,112-114,4094*
- **Jumbo MTU:** *checkmark*

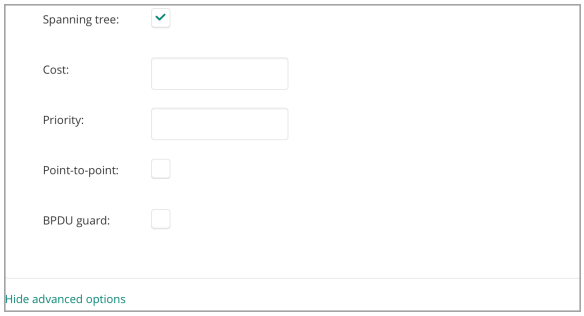



**NOTE:**

The **Allowed VLANs** dropdown is populated from the Gateway VLANs created in the “Configure VLAN Interfaces” procedure.

**Step 8** At the bottom of the page, expand **Show advanced options**, assign the following settings, then click **Save Settings**.

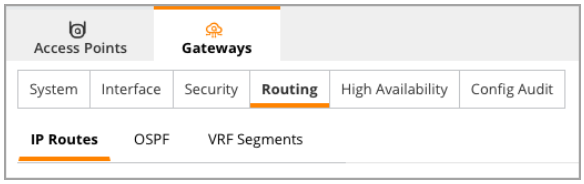
- **Spanning tree:** *checkmark*



# Configure the Default Gateway

Use the following procedure to configure a default gateway on the gateway device.

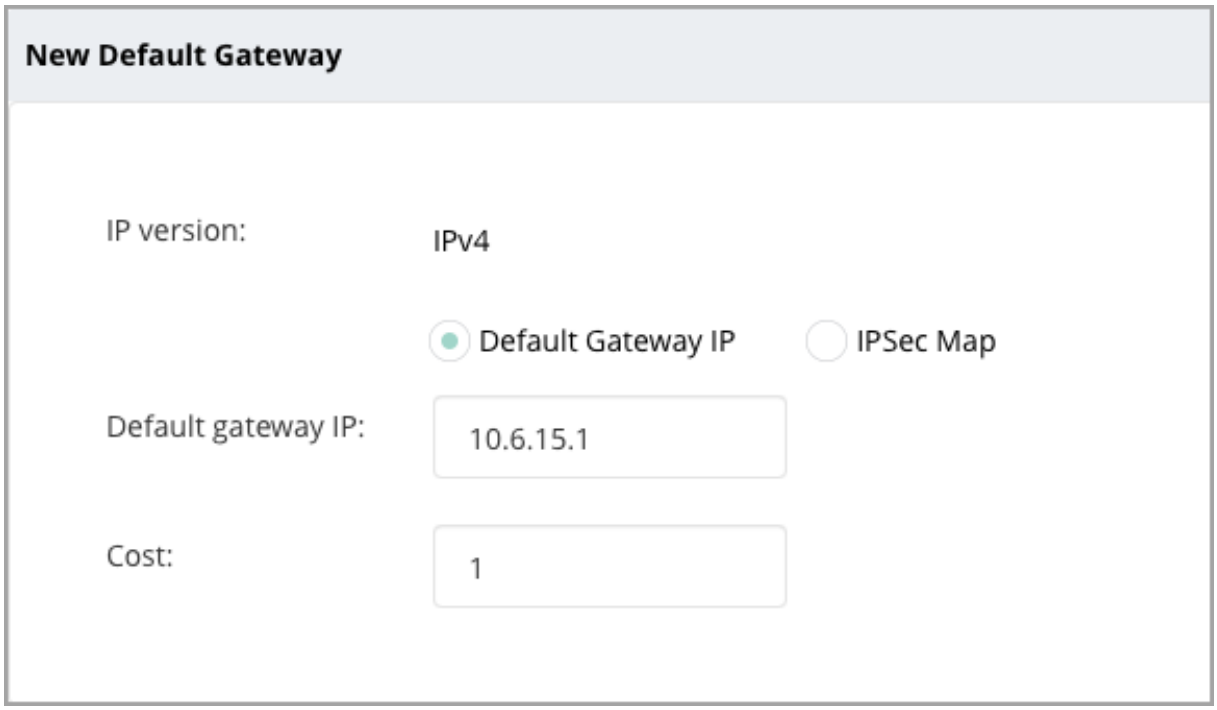
**Step 1** On the **Gateways** tab, select the **Routing** tab, then the **IP Routes** tab.




**Step 2** Expand the **Static Default Gateway** section. At the bottom of the table, click the **+** (plus sign).


**Step 3** On the **New Default Gateway** page, enter the IP address, then click **Save Settings**.

- **Default Gateway IP:** *10.6.15.1*

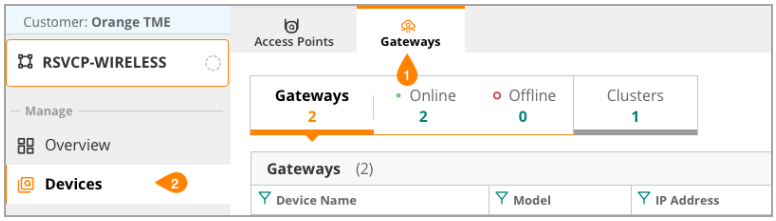



# Configure the Gateway Base Features

Use this procedure to configure the base features of the gateway. The base features include the hostname, VLAN IP addresses, and the System IP address.

**Step 1** Select the wireless group. In this example, the group is **RSVCP-WIRELESS**.

**Step 2** Select the **Gateways** tab. On the left menu, select the **Devices** tab.

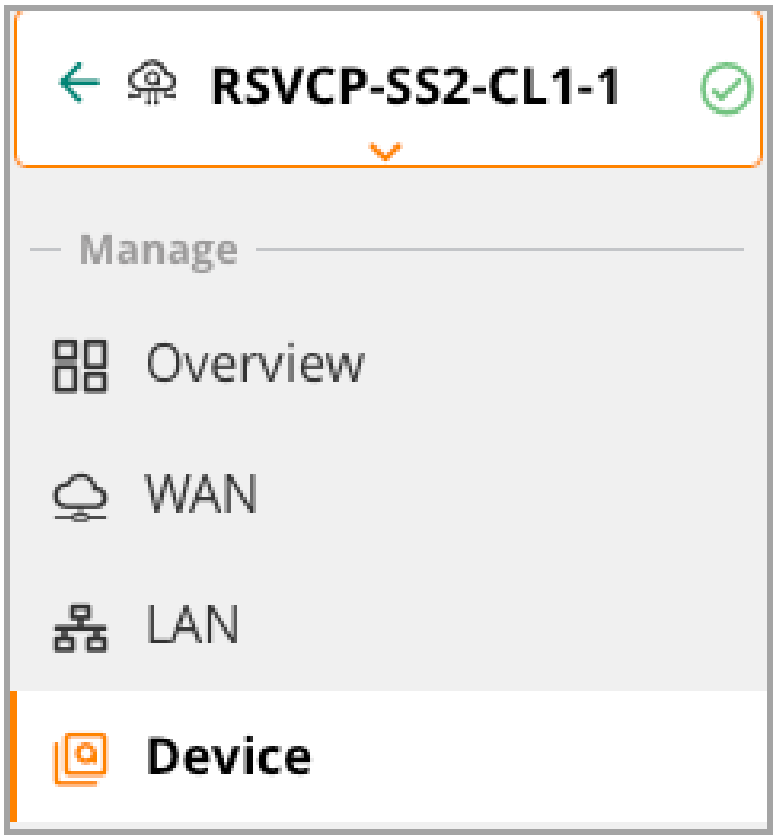



**Step 3** Select a new gateway from the list.

**NOTE:**

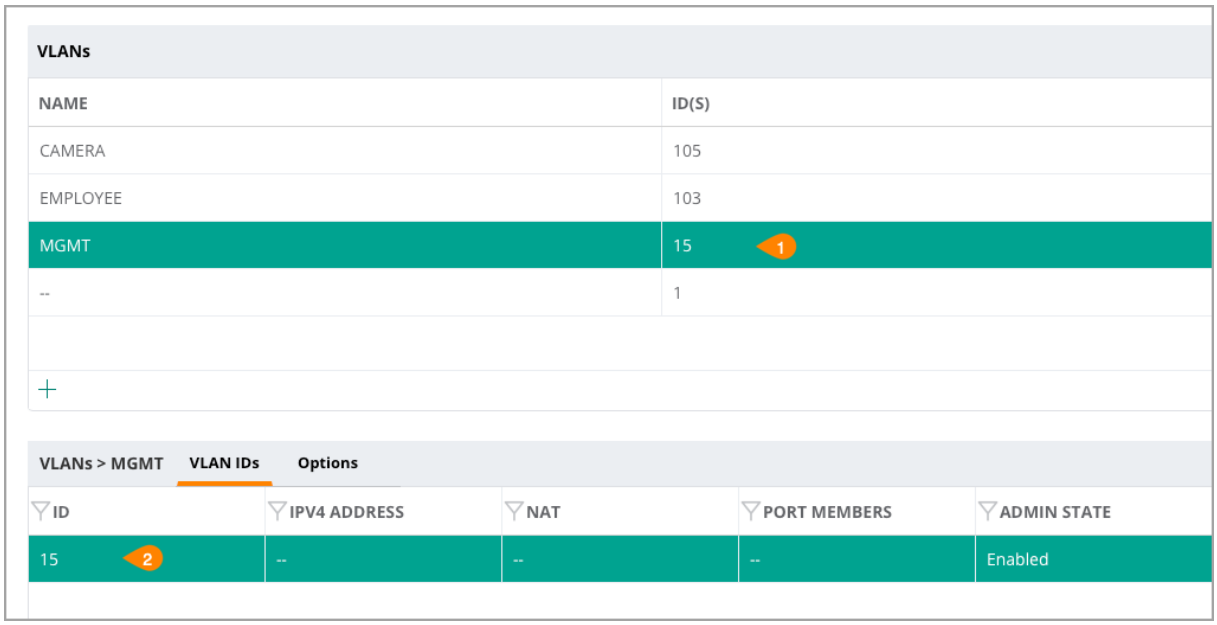
An unnamed gateway is listed with the system MAC address.

**Step 4** On the left menu, select **Device**.



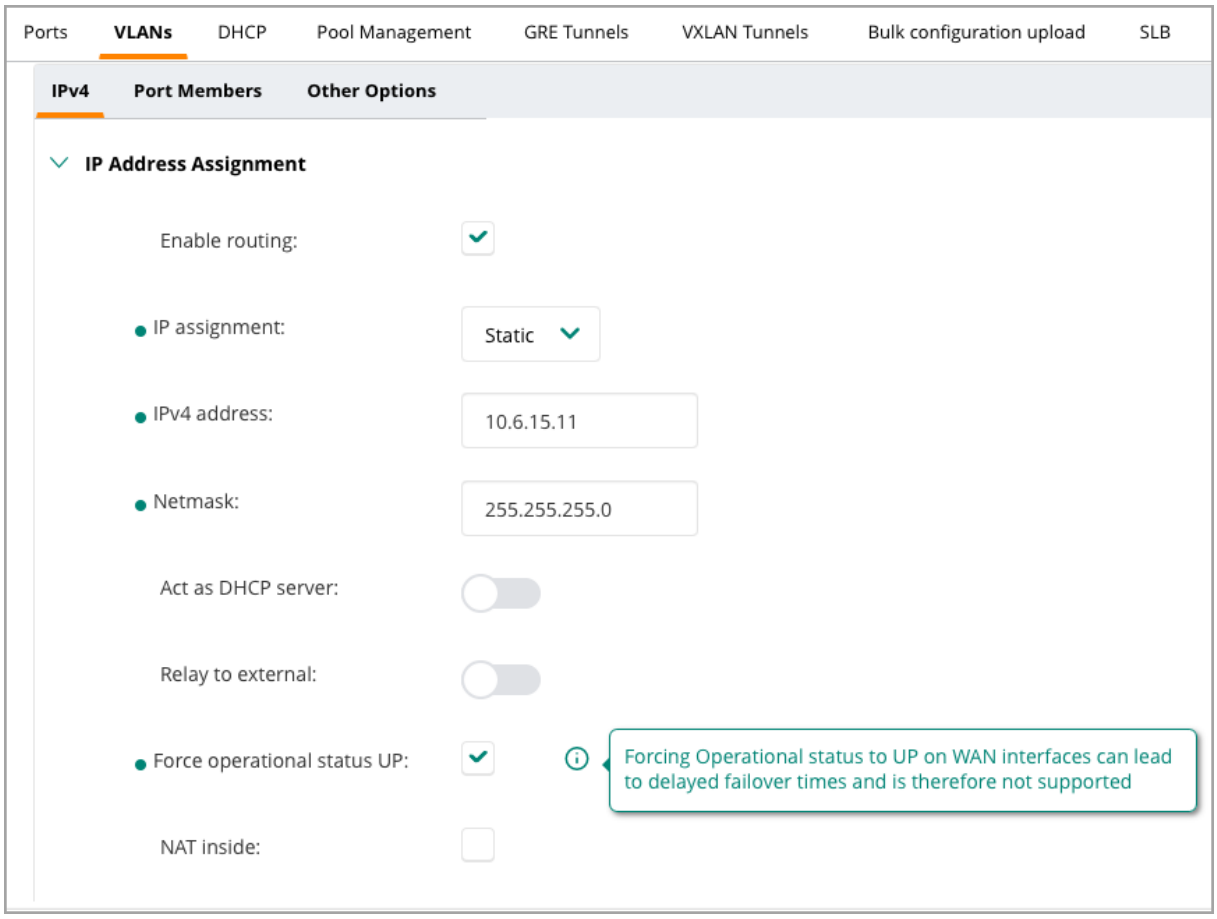

**Step 5** Select the **Interface** tab, then the **VLANs** tab.


**Step 6** In the **VLANs** table, select the **MGMT** VLAN. In the lower VLAN IDs section, click the **VLAN** row.




**Step 7** Scroll down to the **IP Address Assignment** section, assign the following settings, then click **Save Settings**:

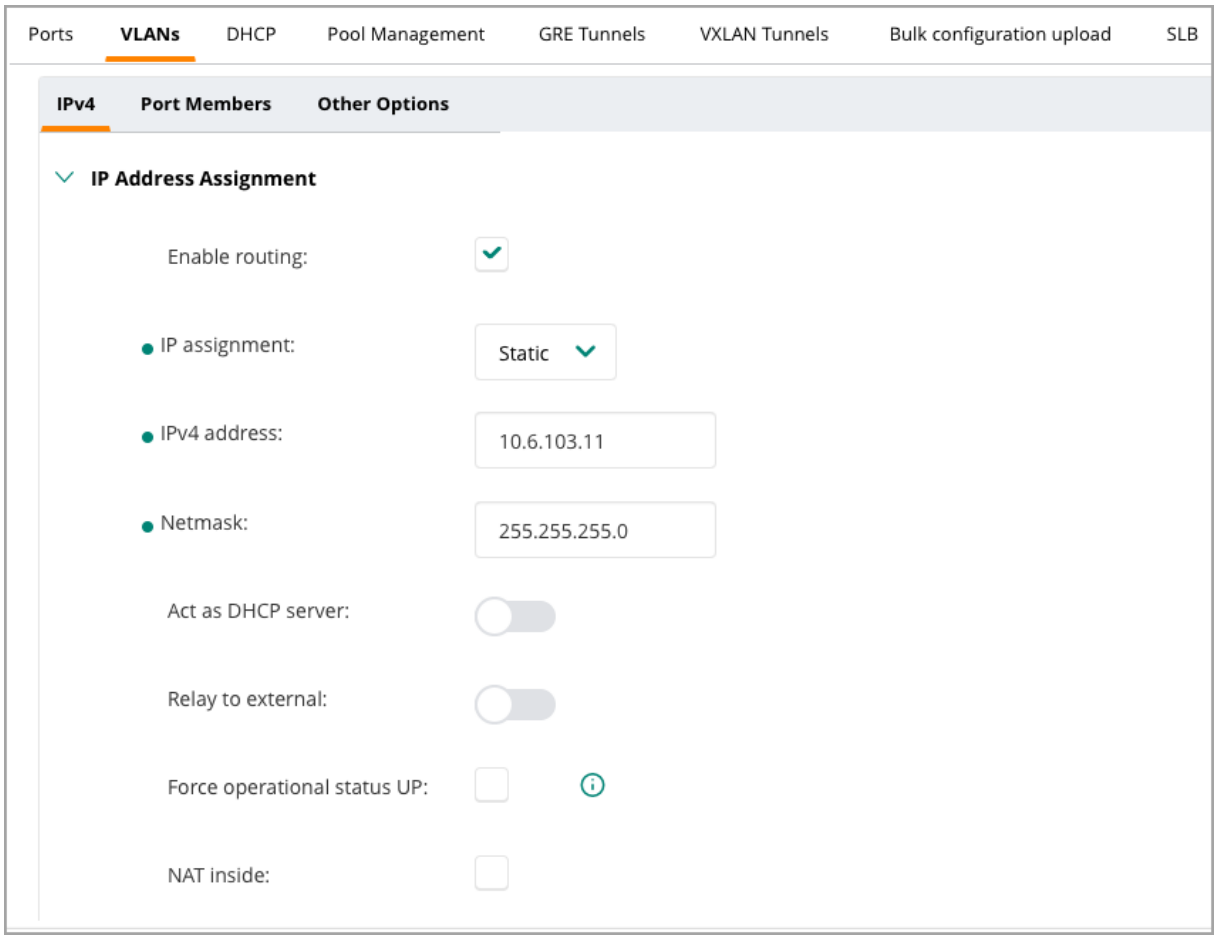
- **IP Assignment:** *Static*
- **IPv4 Address:** *10.6.15.11*
- **Netmask:** *255.255.255.0*
- **Force operational status UP:** *checkmark*




**Step 8** In the **VLANs** table, select a different VLAN. In this example, VLAN 103 is selected. In the lower **VLAN IDs** section, click the **VLAN** row.

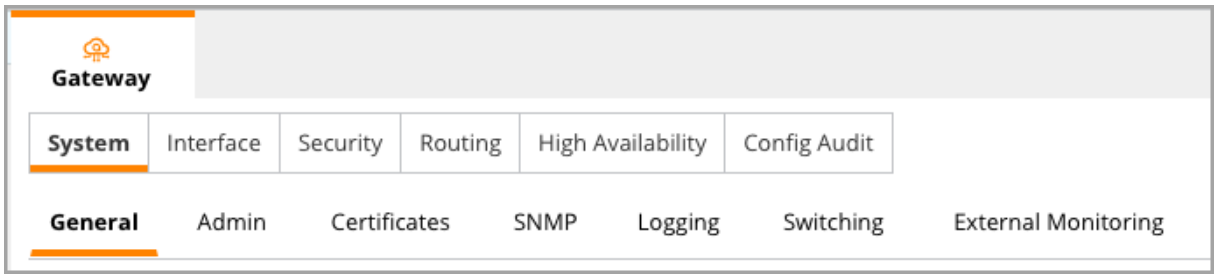
**Step 9** Scroll down to the IP Address Assignment section, and assign the following settings. Click **Save**.

- **IP Assignment:** *Static*
- **IPv4 Address:** *10.6.103.11*
- **Netmask:** *255.255.255.0*
- **Force operational status UP:** *un-checked*

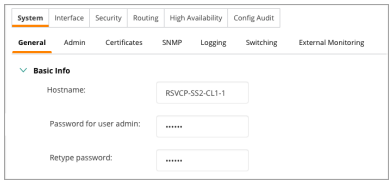



**Step 10** Repeat the previous two steps for each additional VLAN in the environment.

**Step 11** On the **Gateway** page, select the **System** tab, then the **General** tab.




**Step 12** On the **System** tab, expand the **Basic Info** section and change the **Hostname** as required. Click **Save Settings**.

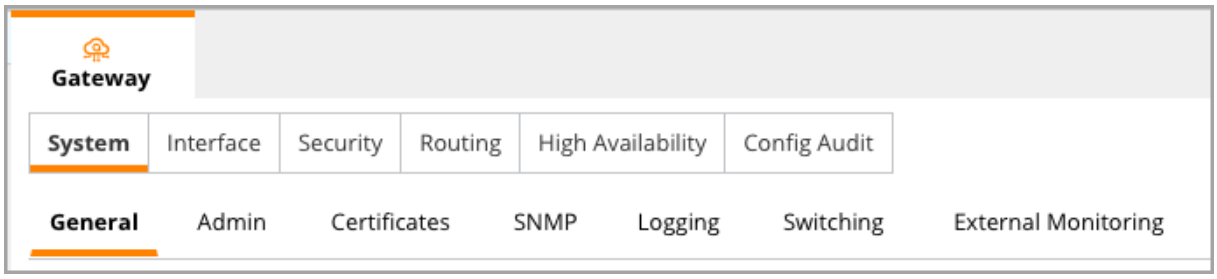


**Step 13** Repeat step 2 to rename the other gateways in the group.

**CAUTION:**

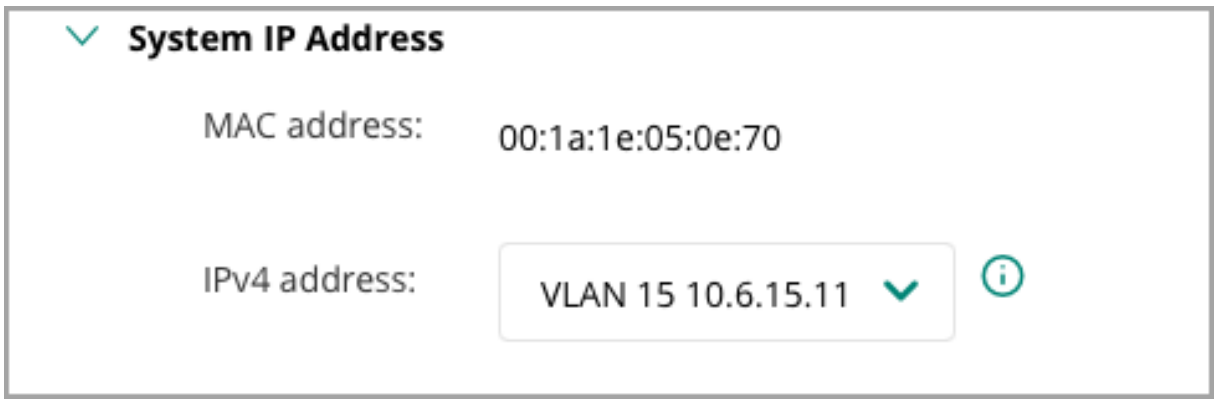
The admin password is inherited from the group settings. Do not change it at the device level.

**Step 14** On the **Gateway** page, select the **System** tab, then the **General** tab.




**Step 15** Expand the **System IP Address** section, use the **IPv4 address** dropdown to select the VLAN with the Force operational UP setting, then click **Save**.

- **IPv4 address:** *VLAN 15 10.6.15.11*




**Step 16** Repeat step 2 to assign a system IP address to the other gateways in the group.

## Configure Layer 2 Gateway Clustering

Use this procedure to configure Layer 2 Gateway clustering.

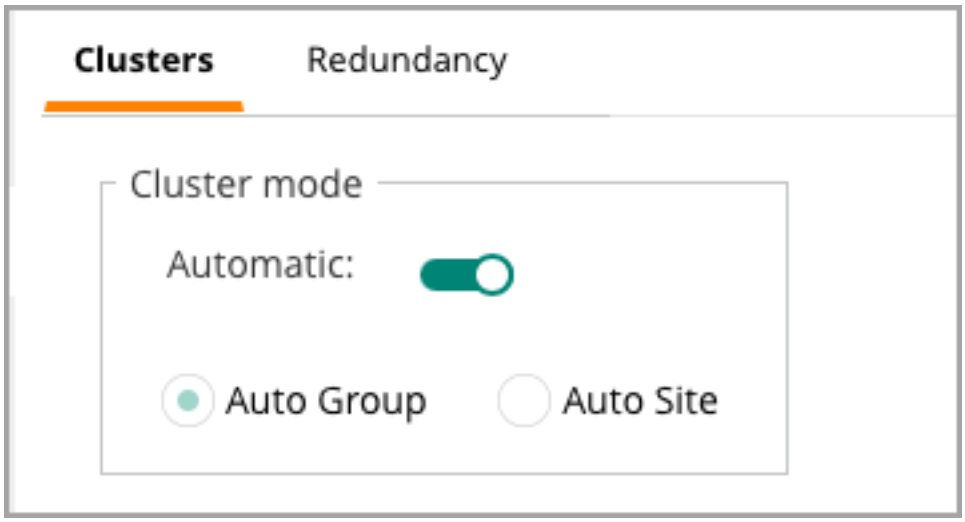
Gateway clustering provides load-balancing across two or more devices, resulting in increased availability and throughput for users and endpoints. The Gateway VRRP IP addresses allow authorization servers such as ClearPass to make a Change of Authorization (CoA) request for a user anchored to a specific gateway.

**Example: Gateway VRRP IP Addresses and VLANs**

| Gateway | IP address | Multicast VLAN | VRRP IP address | VRRP VLAN |
|---|---|---|---|---|
| RSVCP-SS2-CL1-1 | 10.6.15.11 | 15 | 10.6.15.13 | 15 |
| RSVCP-SS2-CL1-2 | 10.6.15.12 | 15 | 10.6.15.14 | 15 |

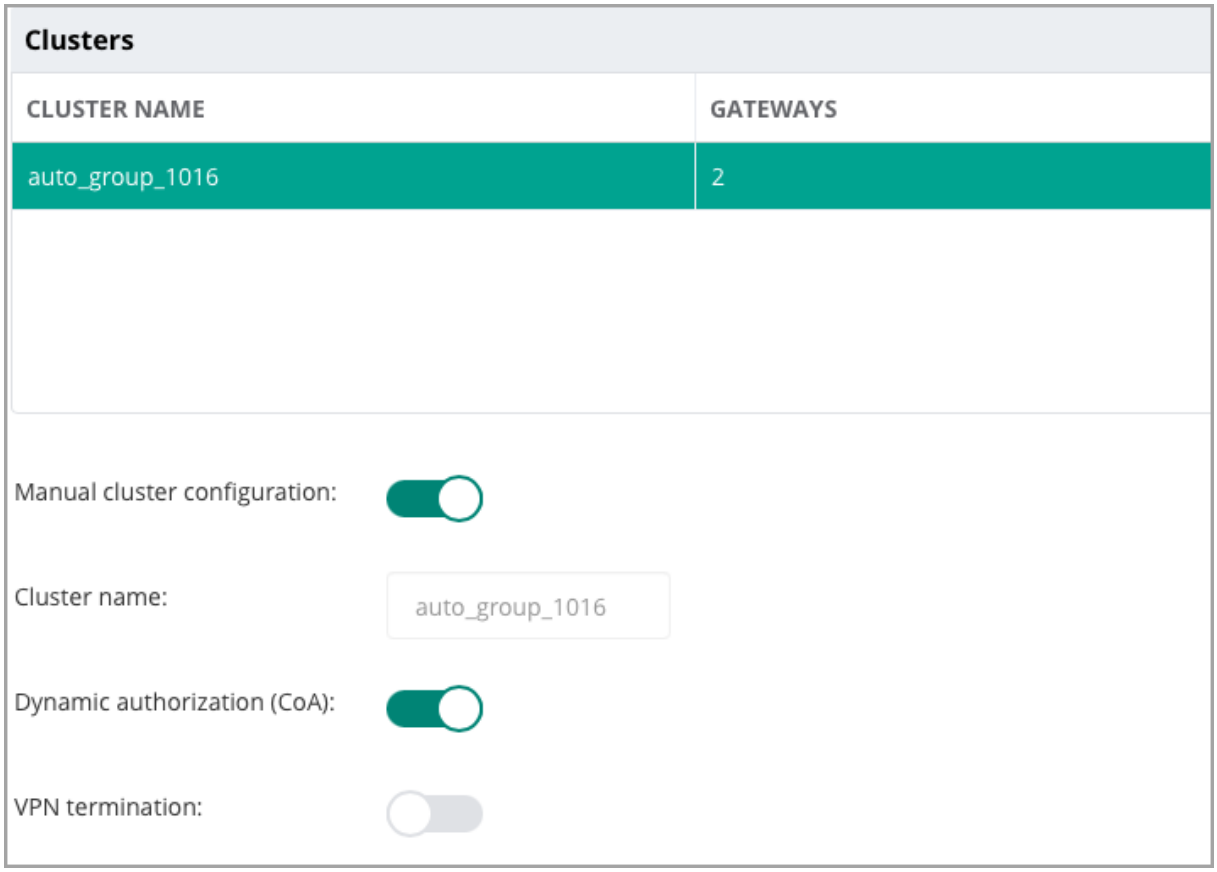
**Step 1** On the **Gateway** page, select the **High Availability** tab.


**Step 2** Confirm the **Cluster mode: Auto Group**.




**Step 3** On the Clusters table, click the cluster name and assign the following settings.

- **Manual cluster configuration:** *Slide to right*
- **Dynamic Authorization (CoA):** *Slide to right*

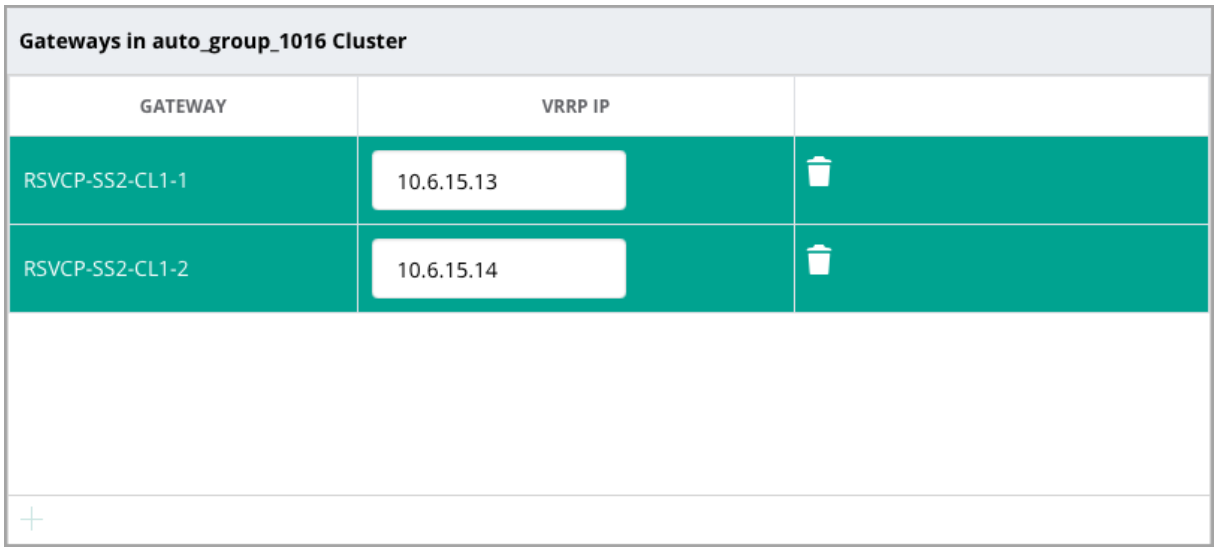


**NOTE:**

The cluster name is populated by default and cannot be changed in an auto group cluster.

**Step 4** Select the box next to the gateway name in **Gateways in Cluster** table and assign the following settings.

- **RSVCP-SS2-CL1-1:** *10.6.15.13*
- **RSVCP-SS2-CL1-2:** *10.6.15.14*




**Step 5** Scroll down, assign the following settings, then click **Save Settings**.

- **Multicast VLAN:** *15*
- **VRRP VLAN:** *15*
- **VRRP ID:** *15*
- **VRRP Passphrase:** *passphrase*

**NOTE:**

AOS-10 reserves VRRP instance IDs in the 220-255 range.


**NOTE:**

Cluster changes disrupt client traffic and should be made during a maintenance window.

# Wireless Access Configuration

The primary function of the wireless access layer is to provide network connectivity anywhere on the campus for wireless devices. Wireless access must be secure, available, fault tolerant, and reliable to meet the demands of today's users.

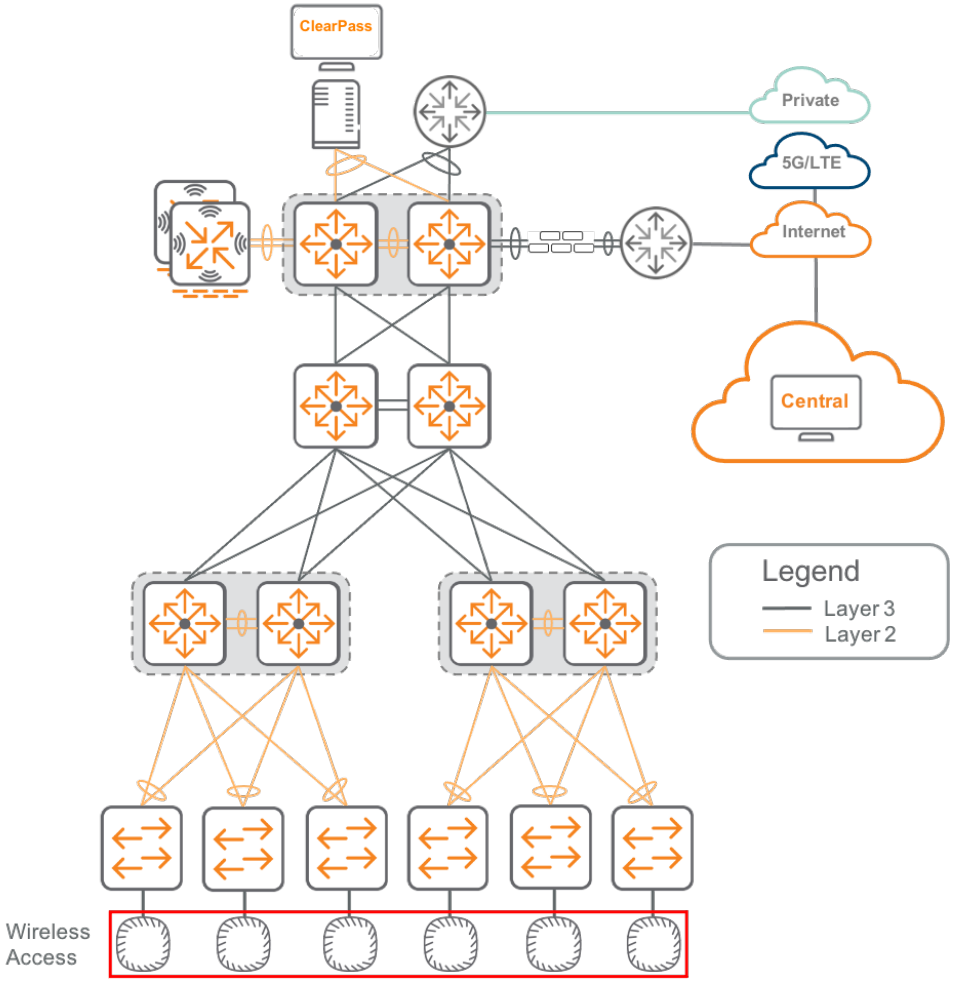
To satisfy the requirements for wireless access in a variety of network designs, the Aruba ESP Campus supports two modes of switching traffic between wireless and wired networks.

- In bridged mode, the AP converts the 802.11 frame to an 802.3 Ethernet frame.
- In tunneled mode, the AP encapsulates the 802.11 frame in a GRE packet and tunnels the traffic to a gateway device for decapsulation, additional inspection, and, if permitted, switching onto the correct VLAN.

An SSID is used to segment traffic between WLANs. A typical reason for using multiple SSIDs is to separate employee traffic from visitor traffic. Another reason is to separate IoT devices from other types of endpoints.

The Aruba ESP Campus for large campus topology uses bridged mode for a Visitor SSID and for an SSID using pre-shared key authentication as might be required for devices in a warehouse or healthcare setting. The same topology implements tunneled mode for an 802.1X authenticated SSID.

The figure below shows the wireless APs in the ESP Campus.




The following table shows the access VLANs for bridge-mode SSIDs.

**Example: AP Access VLANs**

| VLAN Name | VLAN ID |
|---|---|
| EMPLOYEE | 3 |
| BLDG_MGMT | 4 |
| CAMERA | 5 |
| PRINTER | 6 |
| VISITOR | 12 |
| REJECT_AUTH | 13 |
| CRITICAL_AUTH | 14 |
| MGMT | 15 |

The following table shows the ClearPass Policy Managers for the RADIUS server configuration.

**Example: RADIUS Servers**

| Hostname | IP Address | Role |
|---|---|---|
| CPPM-1.EXAMPLE.LOCAL | 10.2.120.94 | Publisher |
| CPPM-2.EXAMPLE.LOCAL | 10.2.120.95 | Subscriber |

## Configure the WPA3-Enterprise Wireless LAN

Use this procedure to configure a WPA3-Enterprise SSID.

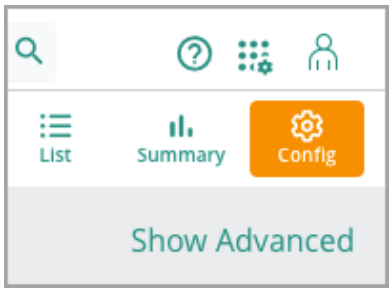
WPA3-Enterprise enables authentication using passwords or certificates to identify users and devices before they are granted access to the network. The wireless client authenticates against a RADIUS server using an EAP-TLS exchange, and the AP acts as a relay. Both the client and the RADIUS server use certificates to verify their identities.

**Step 1** Navigate to **Central** and login using administrator credentials.

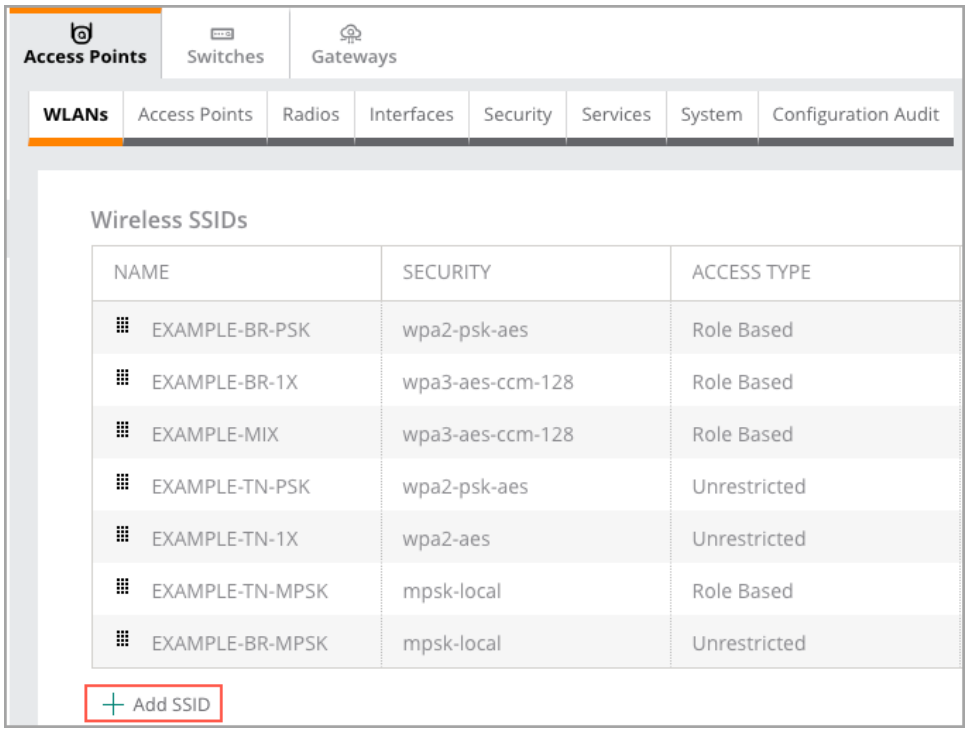
**Step 2** On the Central Account Home page, launch the **Network Operations** app.

**Step 3** In the dropdown, select an AOS10 **Group** name. On the left menu, select **Devices**.

**Step 4** In the upper right of the **Access Points** page, select **Config**.



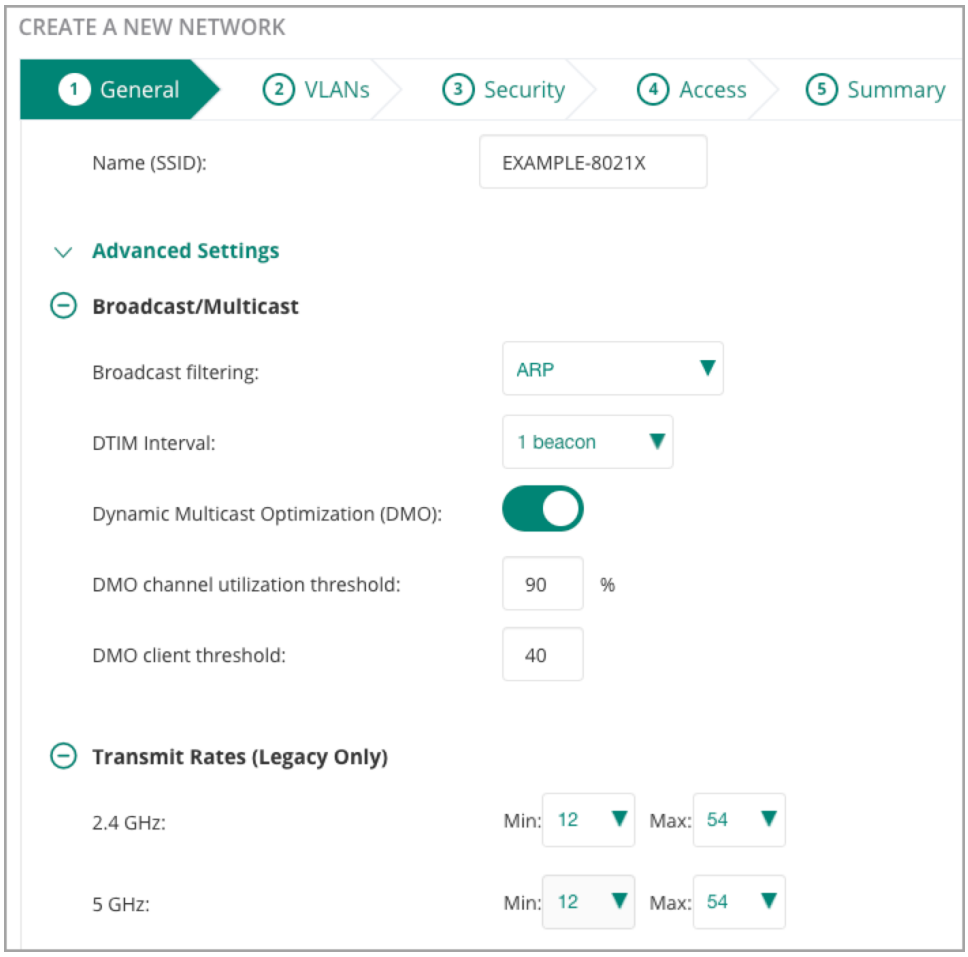

**Step 5** On the **Access Points** page, select the **WLANs** tab. On the bottom left of the **Wireless SSIDs** table, click **+ Add SSID**.




**Step 6** In the **Create a New Network** page on the **General** tab, expand **Advance Settings**, then click the **+** (plus sign) to expand **Broadcast/Multicast**.

**Step 7** Click the **+** (plus sign) to expand **Transmit Rates (Legacy Only)**, assign the following settings, then click **Next**.

- **Name (SSID)**: *EXAMPLE-8021X*
- **Broadcast filtering:** *ARP*
- **Dynamic Multicast Optimization (DMO):** *Slide to the right*
- **DMO Client Threshold:** *40*
- **2.4 GHz: Min:** *12*
- **5 GHz: Min:** *12*

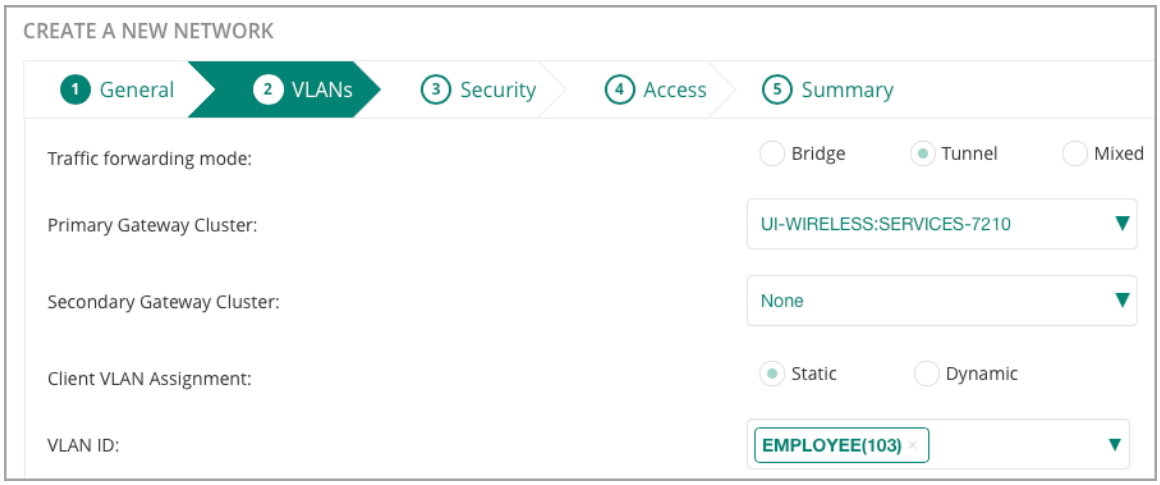



**NOTE:**

The SSID name should not include spaces or special characters for compatibility with all client devices.A **DMO Client Threshold** of 40 is the recommended initial value and should be adjusted based on actual performance results.

**Step 8** On the **VLANs** tab, assign the following settings, then click **Next**.

- **Traffic Forwarding Mode:** *Tunnel*
- **Primary Gateway Cluster:** *UI-WIRELESS:SERVICES-7210*
- **Secondary Gateway Cluster:** *None (default)*
- **Client VLAN Assignment:** *Static (default)*
- **VLAN ID:** *EMPLOYEE (103)*




**NOTE:**

The Primary Gateway Cluster and VLAN ID were created in the Configuring Gateway Devices section.If they have not been configured, create the named VLANs for the SSID in this section.

**Step 9** On the **Security** tab, assign the following settings.

- **Security Level:** *Slide to Enterprise*
- **Key Management**: *WPA3 Enterprise(CMM 128)*

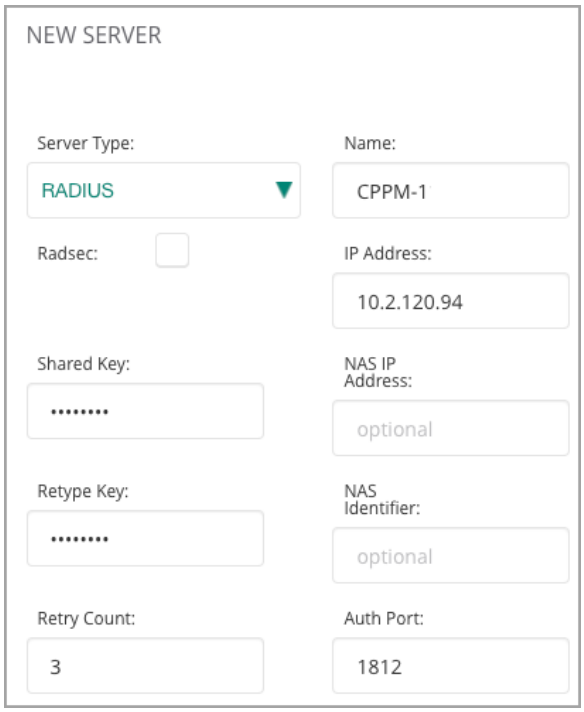
**NOTE:**

WPA3 provides significant security improvements over WPA2 and should be used when possible. Consult endpoint documentation to confirm support.

**Step 10** On the **Security** tab, click the **+** (plus sign) next to **Primary Server**.

**Step 11** In the **NEW SERVER** window, assign the following settings, then click **OK**.

- **Server Type:** *RADIUS*
- **Name:** *CPPM-1*
- **IP Address:** *10.2.120.94*
- **Shared Key:** *shared key*
- **Retype Key:** *shared key*



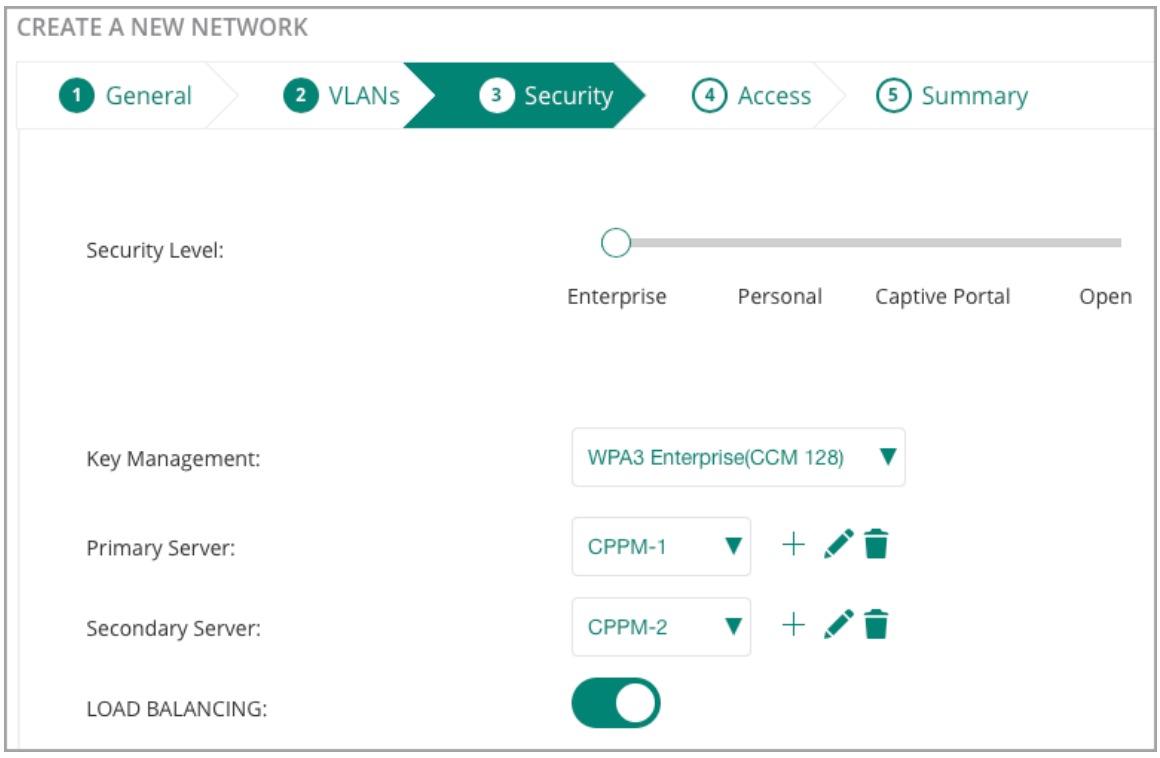

**NOTE:**

It is important to record the **Shared Key** created above for use when configuring ClearPass Policy Manager in the procedure below.

**Step 12** Repeat the two previous steps for the second CPPM server using the appropriate values.

**Step 13** On the **Security** tab, assign the following setting.

- **Load Balancing:** *Slide to the right*

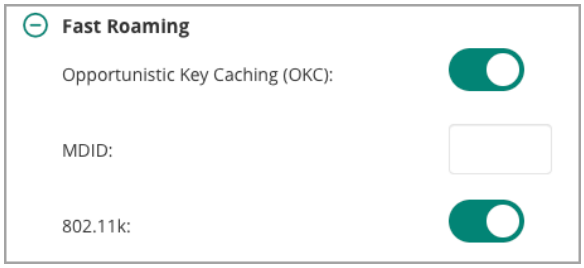


**NOTE:**

Best practice is to deploy 2 RADIUS servers and enable load balancing.

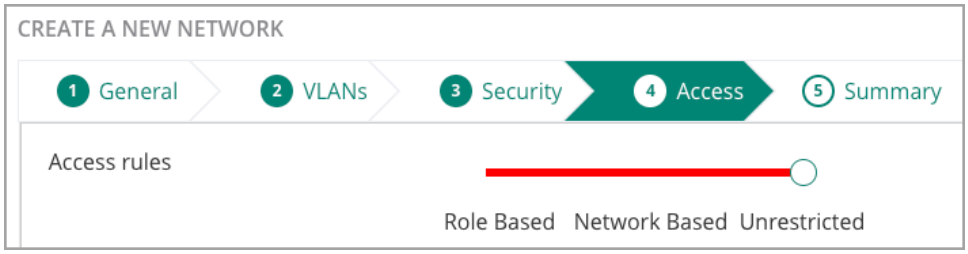
**Step 14** On the **Security** tab, expand **Advanced Settings**, scroll down and click the **+** (plus sign) to expand **Fast Roaming**. Assign the following settings, then click **Next**.

- **Opportunistic Key Caching:** *Slide to the right*
- **802.11K:** *Slide to the right*




**Step 15** On the **Access** tab, assign the following setting, then click **Next**.

- **Access Rules:** *Slide to Unrestricted*




**NOTE:**

The restrictions for this type of SSID are assigned in the gateway.

**Step 16** On the **Summary** tab, review the settings and click **Finish**.

## Configure ClearPass for the WPA3-Enterprise Wireless LAN

To support the WPA3-Enterprise WLAN created in the previous steps, ClearPass Policy Manager must be configured to receive, process, and respond to RADIUS authentication requests from this solution. For detailed guidance on configuring a ClearPass service to support WPA3-Enterprise authentication, refer to the Wireless 802.1X Authentication section of the Policy Deploy chapter in the VSG.

## Configure the Pre-Shared Key Wireless LAN

Use this procedure to configure a WPA3-Personal SSID with a pre-shared key.

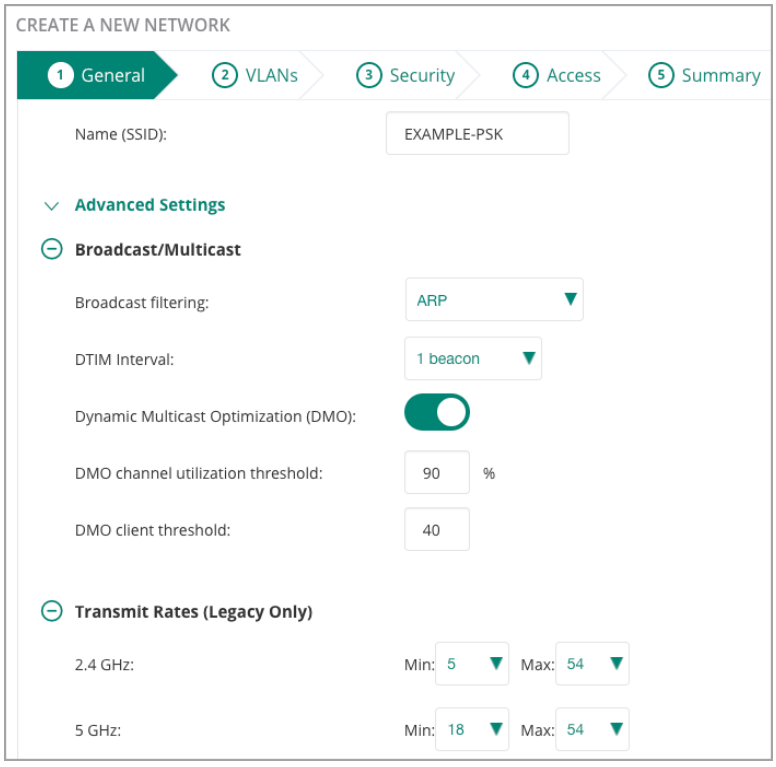
WPA3-Personal allows for authentication using a pre-shared key on a device that does not support 802.1X authentication.

**Step 1** On the **Access Points** page, select the **WLANs** tab. On the bottom left of the **Wireless SSIDs** table, click **+ Add SSID**.

**Step 2** In the **Create a New Network** page on the **General** tab, expand **Advance Settings**, then click the **+** (plus sign) to expand **Broadcast/Multicast**.

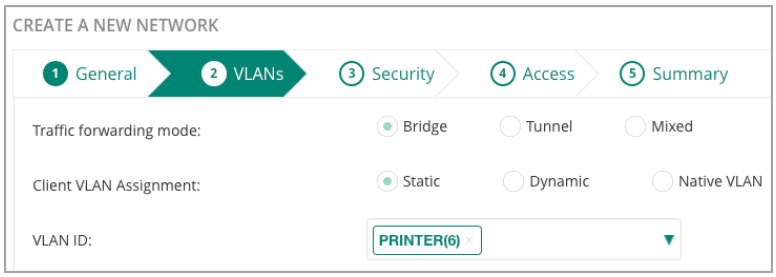
**Step 3** Click the **+** (plus sign) to expand **Transmit Rates (Legacy Only)**, assign the following settings, then click **Next**.

- **Name (SSID)**: *EXAMPLE-PSK*
- **Broadcast filtering:** *ARP*
- **Dynamic Multicast Optimization (DMO):** *Slide to the right*
- **DMO Client Threshold:** *40*
- **2.4 GHz: Min:** *5*
- **5 GHz: Min:** *18*



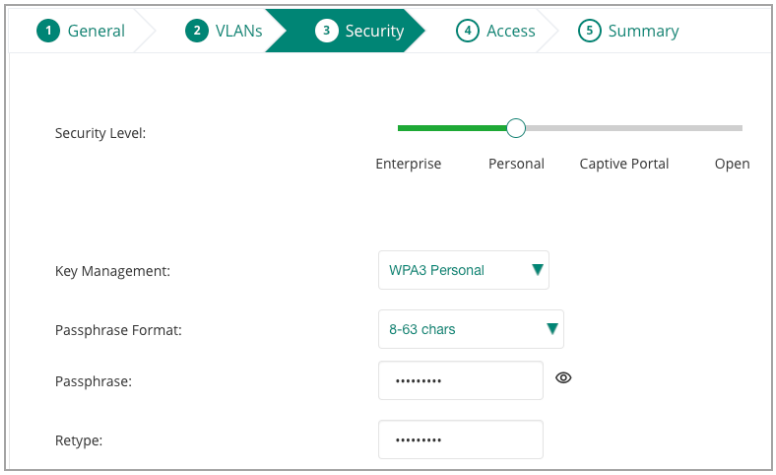

**Step 4** On the **VLANs** tab, assign the following settings, then click **Next**:

- **Traffic Forwarding Mode:** *Bridge*
- **Client VLAN Assignment:** *Static*
- **VLAN ID:** *PRINTER(6)*



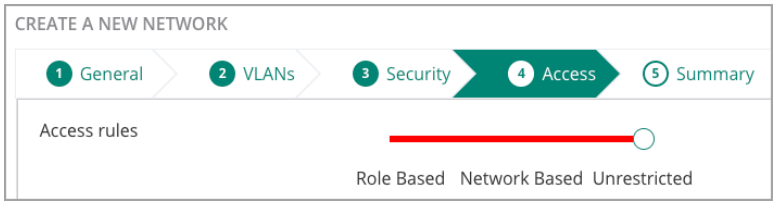
**Step 5** On the **Security** tab, assign the following settings, then click **Next**:

- **Security Level:** *Slide to Personal*
- **Key Management:** *WPA3 Personal*
- **Passphrase:** *passphrase*
- **Retype:** *passphrase*




**Step 6** On the **Access** tab, assign the following setting, then click **Next**.

- **Access Rules:** *Slide to Unrestricted*




**NOTE:**

The restrictions for this type of SSID are made in the switch network.

**Step 7** On the **Summary** tab, review the settings and click **Finish**.

## Configure the Visitor Wireless LAN

Use this procedure to configure a visitor SSID.

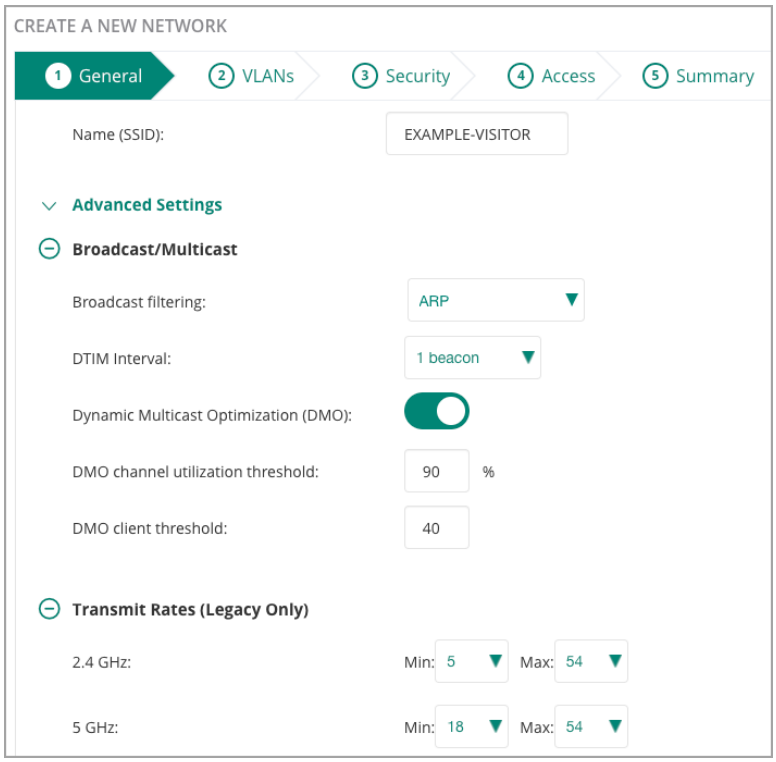
**Step 1** On the **Access Points** page, select the **WLANs** tab. On the bottom left of the **Wireless SSIDs** table, click **+ Add SSID**.

**Step 2** On the **Create a New Network** page on the **General** tab, expand **Advance Settings**, then click the **+** (plus sign) to expand **Broadcast/Multicast**.

**Step 3** Click the **+** (plus sign) to expand **Transmit Rates (Legacy Only)**, then assign the following settings.

- **Name (SSID)**: *EXAMPLE-VISITOR*

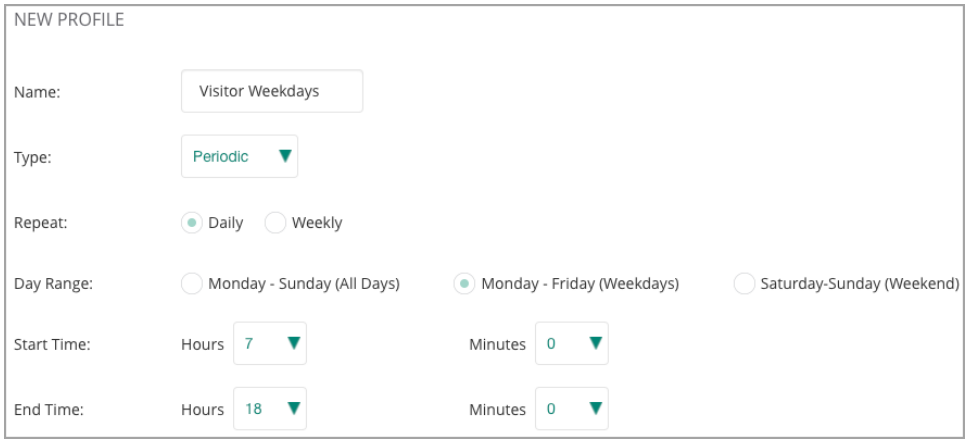
- **Broadcast filtering:** *ARP*
- **Dynamic Multicast Optimization (DMO):** *Slide to the right*
- **DMO Client Threshold:** *40*
- **2.4 GHz: Min:** *5*
- **5 GHz: Min:** *18*




**Step 4** On the **General** tab, scroll down and click the **+** (plus sign) to expand **Time Range Profiles**. In the middle of the section, click **+ New Time Range Profile**.

**Step 5** In the **New Profile** window, assign the following settings, then click **Save**.

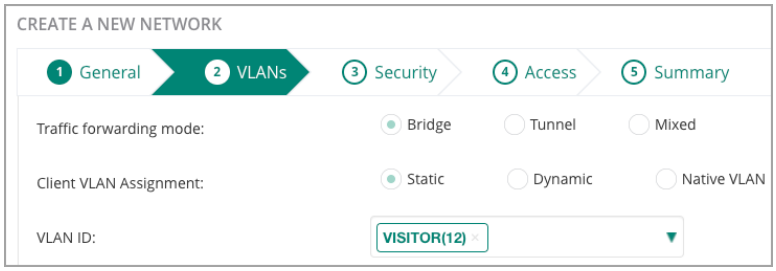
- **Name:** *Visitor Weekdays*
- **Type:** *Periodic*
- **Repeat:** *Daily*
- **Day Range:** *Monday - Friday (Weekdays)*
- **Start Time Hours:** *7* **Minutes:** *0*
- **End Time Hours:** *18* **Minutes:** *0*



**Step 6** In the **Time Range Profiles** section in the **Status** dropdown, find the newly created profile, and select **Enabled**. At the bottom of the page, click **Next**.


**Step 7** On the **VLANs** tab, assign the following settings, then click **Next**.

- **Traffic Forwarding Mode:** *Bridge*
- **Client VLAN Assignment:** *Static*
- **VLAN ID:** *VISITOR(12)*



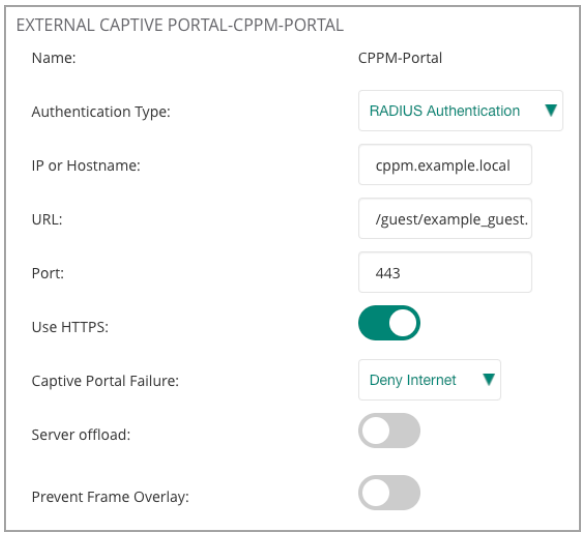

**Step 8** On the **Security** tab, assign the following settings.

- **Security Level:** *Slider to Captive Portal*
- **Captive Portal Type:** *External*

**Step 9** In the **Splash Page** section, click the **+** (plus sign) next to **Captive Portal Profile**.

**Step 10** In the **External Captive Portal-New** window, assign the following settings, then click **OK**.

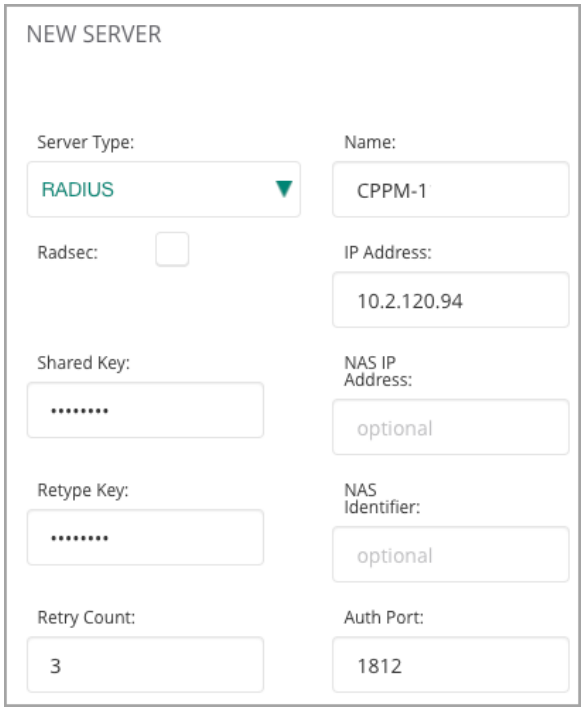
- **Name:** *CPPM-Portal*
- **Authentication Type:** *RADIUS Authentication*
- **IP or Hostname:** *cppm.example.local*
- **URL:** */guest/example_guest.php*
- **Port:** *443*
- **Redirect URL:** *http://arubanetworking.hpe.com*



**Step 11** On the **Security** tab in the **Splash Page** section, click the **+** (plus sign) next to **Primary Server**.

**Step 12** In the **New Server** window, assign the following settings, then click **OK**.

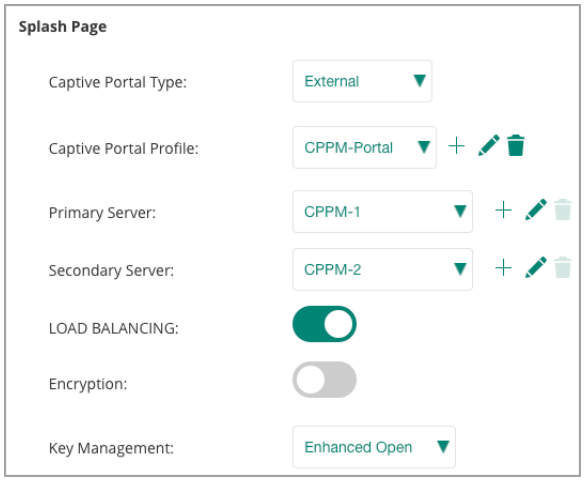
- **Server Type:** *RADIUS*
- **Name:** *CPPM-1*
- **IP Address:** *10.2.120.94*
- **Shared Key:** *shared key*
- **Retype Key:** *shared key*




**Step 13** Repeat the two previous steps for the second CPPM server using the appropriate values.

**Step 14** On the **Security** tab in the **Splash Page** section, assign the following settings, then click **Next**.

- **LOAD BALANCING:** *slide to the right*
- **Encryption:** *slide to the left*
- **Key Management:** *Enhanced Open*



**NOTE:**

The Captive Portal Profile requires information from the CPPM server on the network. For detailed steps, see *Appendix 1: How to Find ClearPass Details for the Visitor WLAN*.

**Step 15** On the **Access** tab, move the slider to **Network Based**, select the **Allow any to all destinations** rule, then click the **edit** (pencil) icon.


**Step 16** In the **Access Rules** window, assign the following settings, then click **OK**.

- **Action:** *Deny*

**CAUTION:**

This step changes the default *allow any to all destinations* rule to a *deny any to all destinations* rule for visitor traffic. This line always must be the last entry in the Access Rules to prevent unauthorized access to internal network resources.

**Step 17** On the **Access** tab, select **+ Add Rule**.

In most cases, the visitor needs access only to DHCP and DNS services, and HTTP/HTTPS access to all destinations on the Internet. Allow access to DHCP servers on the internal network and allow DNS to two well-known DNS servers. To prevent access to internal resources, add an exception network and mask covering the internal IP addresses to the HTTP and HTTPS allow rules.

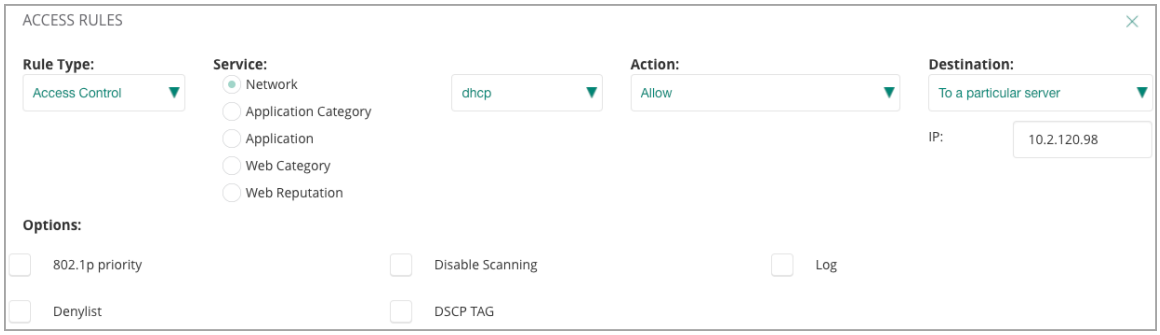
**Example: Access Rules for Visitors**

| Rule Type | Service type | Service name | Action | Destination |
|---|---|---|---|---|
| Access control | Network | DHCP | Allow | 10.2.120.98 (internal DHCP server) |
| Access control | Network | DHCP | Allow | 10.2.120.99 (internal DHCP server) |
| Access control | Network | DNS | Allow | 8.8.4.4 (well-known DNS server) |
| Access control | Network | DNS | Allow | 8.8.8.8 (well-known DNS server) |
| Access control | Network | HTTP | Allow | To all destinations, except internal |
| Access control | Network | HTTPS | Allow | To all destinations, except internal |
| Access control | Network | Any | Deny | To all destinations |

**Step 18** In the **Access Rules** window, assign the following settings, then click **OK**.

- **Rule Type:** *Access Control*
- **Service:** *Network*
- **Service: Dropdown:** *dhcp*
- **Action:** *Allow*

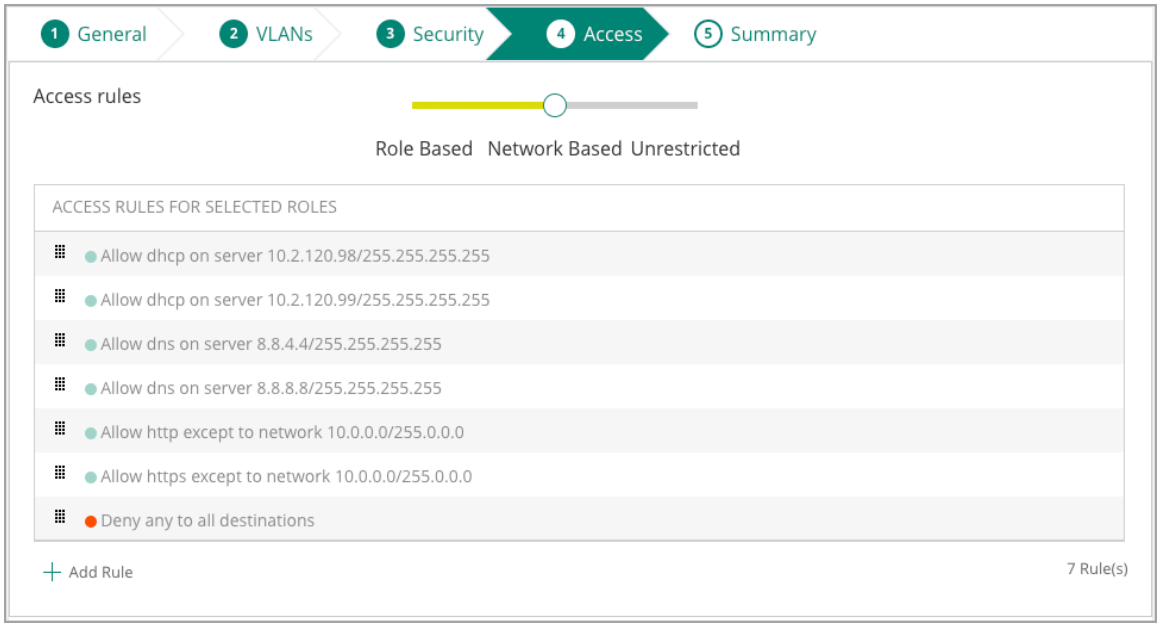
- **Destination:** *To a particular server*
- **IP:** *10.2.120.98*
- **Options:** *none selected*




**NOTE:**

When using the provided table, the easiest way to add the rules is from the bottom up to ensure they are in the correct order when finished.

**Step 19** Repeat the previous two steps to add all the rules in the table.




**Step 20** On the **Access** tab, click **Next**.

**Step 21** On the **Summary** tab, review the settings, and select **Finish**.

# User Experience Insight Deploy

This section details the steps to deploy UXI for Orange Widget Logistics (OWL) described on the Reference Customer page. The IT department has a centralized helpdesk call center in the Roseville, CA, headquarters, with no IT presence in other branch and office locations. UXI will be deployed and configured to monitor network and application performance at the Seattle campus. The deployment process in this guide can be repeated for the rest of the locations. The deployed solution uses the following products:

- Aruba UXI Cloud Dashboard
- Aruba UXI Sensor UX-G5 and UX-G6 Series

## Prepare for UXI Deployment

Completing the preparatory tasks below is crucial before installing and configuring the UXI sensors. This ensures a smooth and successful deployment of the UXI sensors for network and application performance monitoring.

### URL Access

UXI sensors communicate with multiple systems to download configuration and upload test results. The URLs below must be accessible for the sensors to function correctly. Additional services used for testing should also be allow-listed to enable proper testing.

#### *Backend Systems*

The URL https://device-gateway.capenetworks.io is essential for all communication between Aruba UXI sensors and their backend systems. The sensors must be able to access it.

**CAUTION:**

Do not use SSL decryption for the URL above.

#### *Date and Time*

The sensor uses one of the following methods to obtain the correct time:

- NTP servers provided in DHCP option 42.
- The publicly accessible 0.pool.ntp.org NTP server(s).
- If NTP is unavailable, the sensor syncs time via HTTP from http://device-gateway.capenetworks.io/ on port 80.
- If the URL http://device-gateway.capenetworks.io/ is not accessible on port 80, the sensor attempts to sync via HTTPS from https://device-gateway.capenetworks.io/ on port 443.

### *Captive Portal and Proxy Detection*

Reachability to http://cdn.capenetworks.io/auth on port 80 is a critical test for detecting the presence of a captive portal and identifying potential proxy-related issues during the UXI sensor's test cycle. Depending on the test results, the sensor takes appropriate actions, such as continuing the regular test cycle, running the captive portal test, or reporting errors related to the captive portal and proxy configurations. More details can be found in the UXI Troubleshooting Guide.

### *External Connectivity Detection*

The sensor uses the following URLs to test for external connectivity. If the URLs cannot be accessed, the sensor reports a **No connectivity** issue on the dashboard.

http://cdn.capenetworks.io/auth

http://cdn.capenetworks.io/connectivity-check

http://35.241.22.134/auth.html

http://35.241.22.134/connectivity-check

http://captive.apple.com/hotspot-detect.html

http://connectivitycheck.gstatic.com/generate_204

**CAUTION:**

If a network has a captive portal in place, it is advisable not to allow-list the above URLs, which may prevent the proper redirection of the sensor to the Captive Portal. Instead, these URLs should be accessible, but unauthenticated clients should receive a captive portal redirect response.

More information can be found in this UXI URL help article.

## Activate UXI Account on GreenLake Cloud Platform (GLP)

The HPE Greenlake Cloud Platform (GLP) provides a common interface to access and manage all HPE cloud applications in one place. HPE Aruba Networking User Experience Insight (UXI) is taking steps to be an application on GLP.

The following functions are now performed through GLP:

- Adding and removing sensors from the UXI dashboard
- Adding UXI subscriptions
- Assigning users to the UXI dashboard

### *Create a GLP Account*

To access the GLP UXI onboarding page, a valid Greenlake account is necessary. To create one, follow the steps in the **Create an HPE GreenLake Account** section of the GreenLake Platform chapter in the VSG, then return to this page to deploy UXI. If you already have an active GLP account, proceed to the next steps.

**NOTE:**

When users first provision UXI, they will automatically see eval subscriptions added to their workspace. If they have purchased a subscription, they can also add the subscription key to their workspace. Purchased subscription keys are emailed to the end user identified in the purchase order.

## Deploy UXI on GLP

Once logged into GLP, follow the steps below to begin the UXI deployment process.

## Provision UXI in your GLP Workspace

**Step 1** From your GLP Workspace home screen, click on **Services**, then **Catalog**, and lastly, **User Experience Insight**

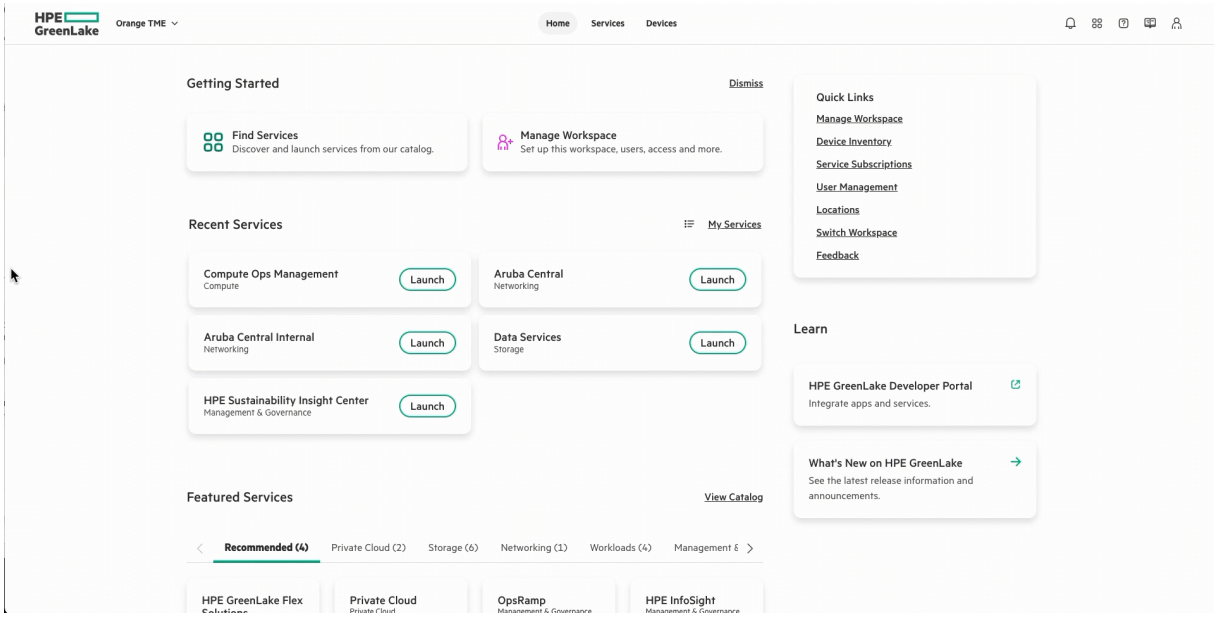



**Figure 22:** UXI-ProvisionUXIInGLP

**Step 2** On the next page, click the **Provision** button on the upper right of the browser window.

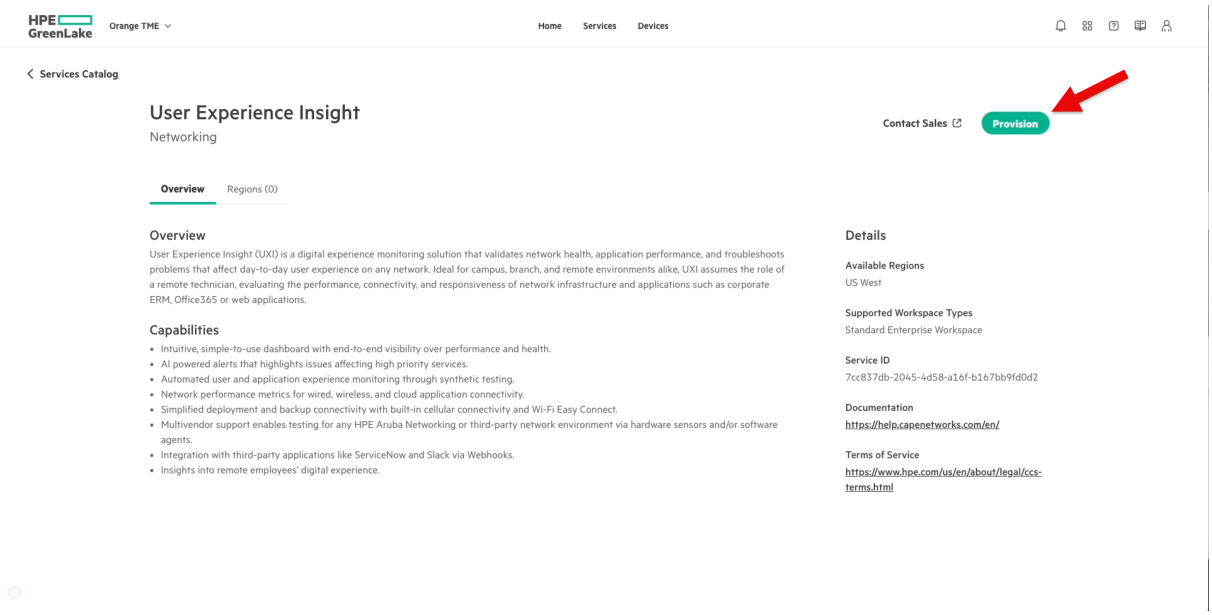



**Figure 23:** UXI Provision

**Step 3** In the **Provision Service Manager** window, perform the following:

- Select region **US West**
- Check the box to agree to the **Terms of Service**
- Click **Deploy**

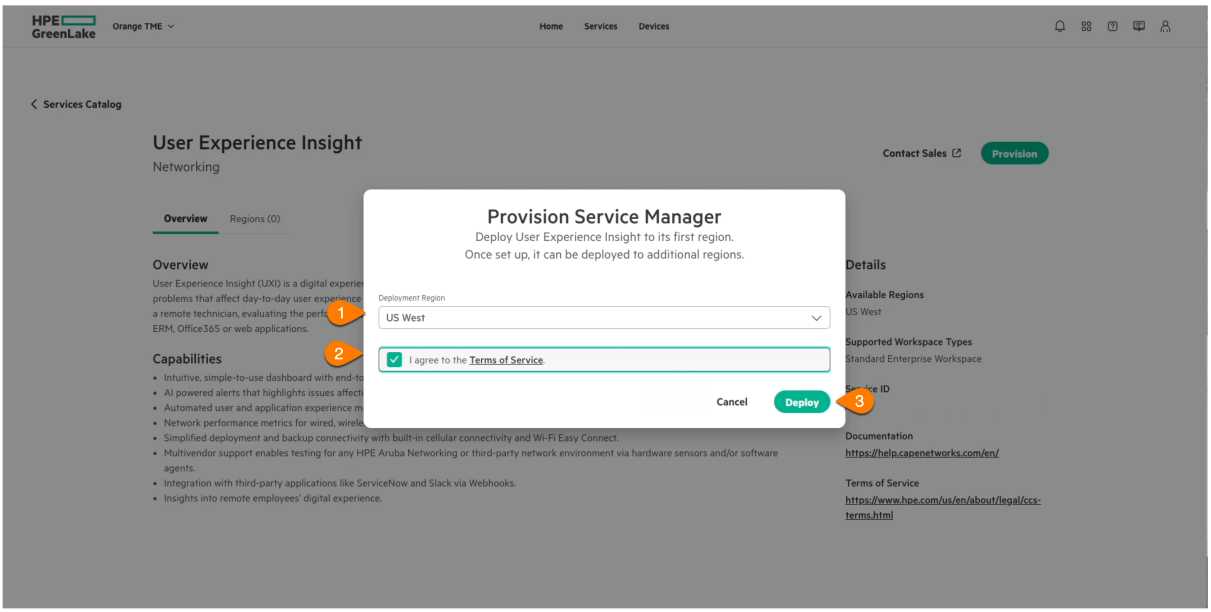



**Figure 24:** UXI Provision Service Manager

## Add Devices to GLP Inventory

**Step 1** When provisioning is complete, click **Devices** at the top center of the browser.

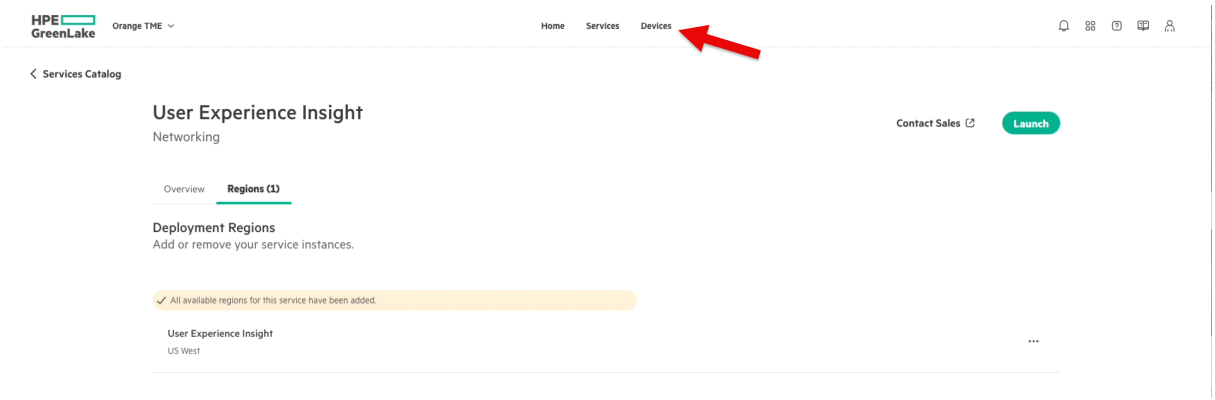



**Figure 25:** UXI Devices Link

**Step 2** On the **Devices** page, click the **Add Devices** button on the right.

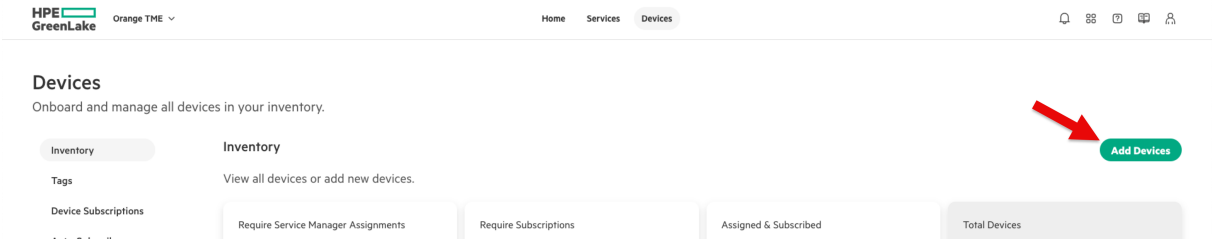



**Figure 26:** UXI Add Devices

**Step 3** On the **Select Device Type** page:

- Select *Networking Devices* from the Device Type dropdown list
- Click the **Next** button.

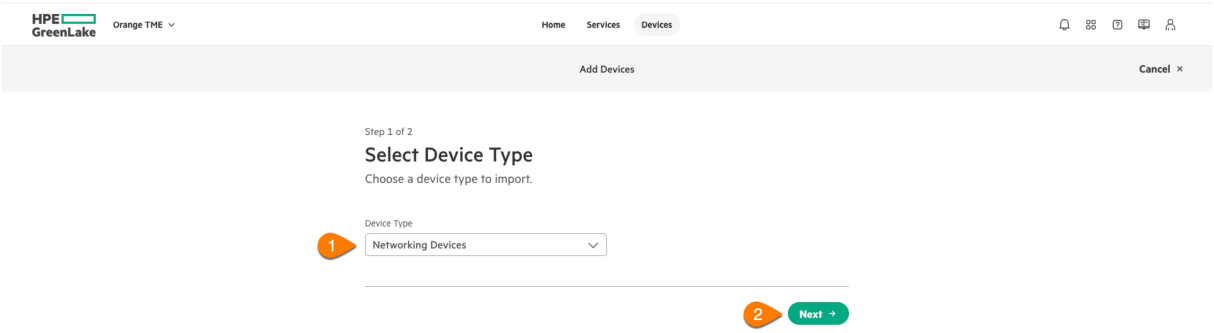



**Figure 27:** UXI Select Device Type

**Step 4** On the next page:

- Select the **Serial Number & MAC Address** radio button
- Add the **Serial Number**
- Ethernet **MAC Address** of the new sensor
- Click **Enter**

- Verify the device appears on the list, as shown in the example below
- Click **Next** at the bottom of the page.

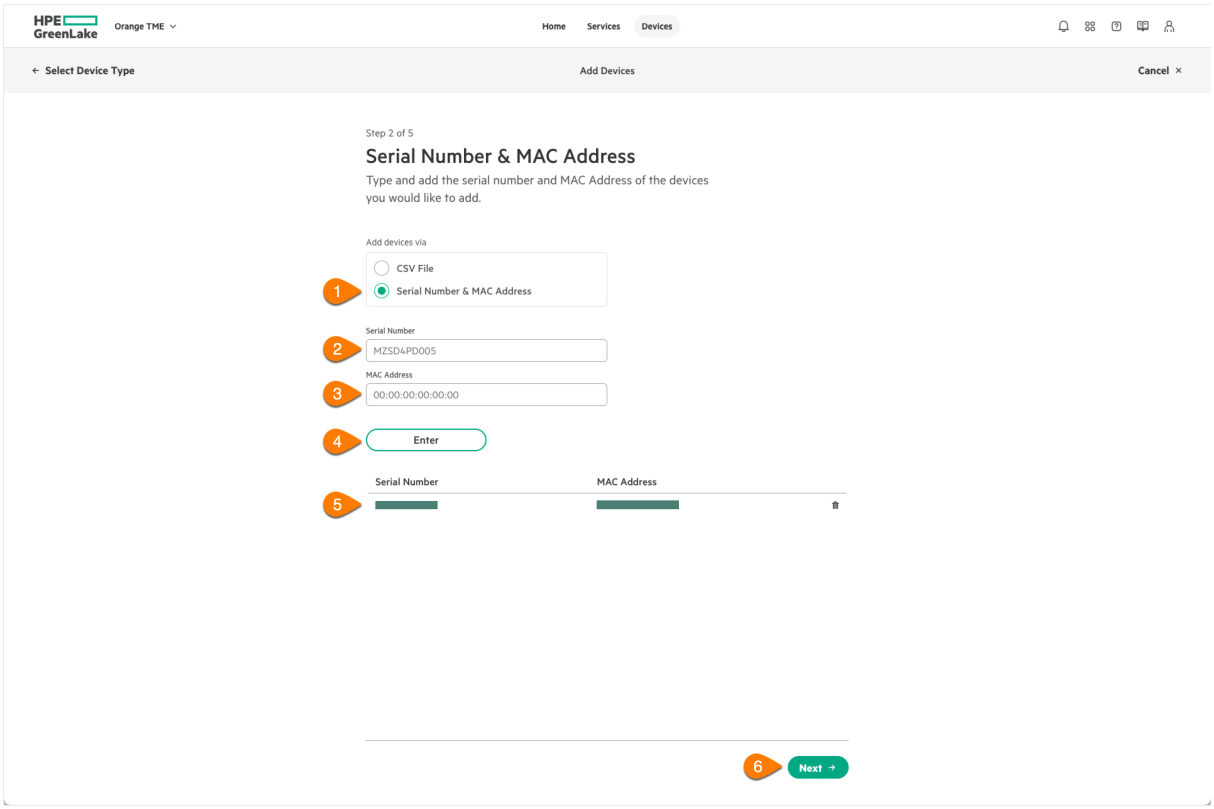



**Figure 28:** UXI Add SN & MAC Address

**NOTE:**

Enter the Ethernet (not the Wi-Fi) MAC address for each device.

**NOTE:**

When onboarding a large number of sensors, the **CSV File** option allows you to use a CSV file.

**Step 8** Click **Next** twice to skip the **Assign Tags** and **Location and Service Delivery Contact** page.

**Step 9** On the **Review Add Devices** page:

- Verify the expected devices are listed
- Click **Finish**

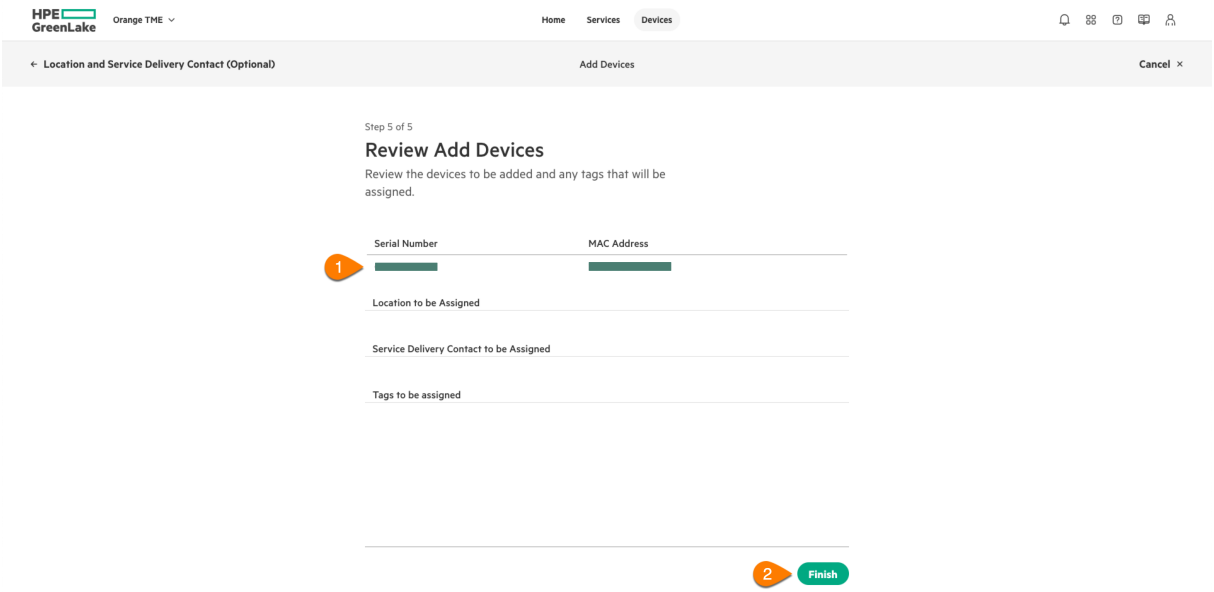



**Figure 29:** UXI Review Devices

## Assign Devices to the UXI Application

**Step 1** After devices have been added to GLP inventory, verify **Service Manager** and **Service Region** categories are assigned to your new devices by doing the following:

- Go to **Devices**
- Filter for the new sensors by using serial number, Ethernet MAC, or model number
- If **Service Manager** and **Service Region** categories are assigned as shown, skip the next two steps and move on to the **Add UXI Device Subscription** section. If they are not, continue to step **2**.

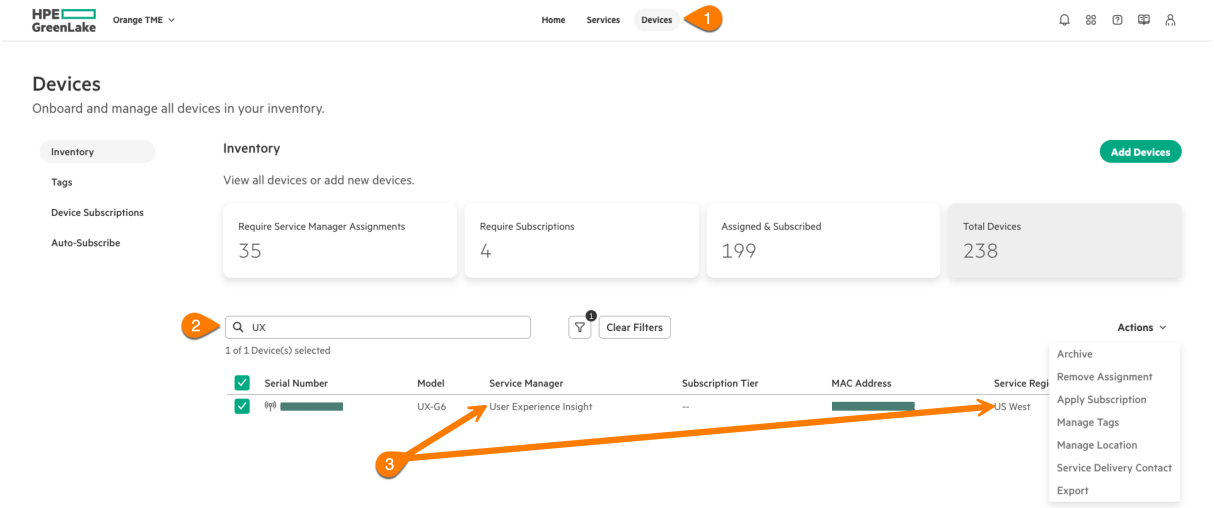



**Figure 30:** UXI Assign Devices

**Step 2** While still filtering per the previous step, if **Service Manager** and **Service Region** categories are not assigned, take the following steps as shown in the image below:

- Check the box next to the sensor
- Click on **Actions**
- Click on **Assign to Service Manager** from the dropdown list

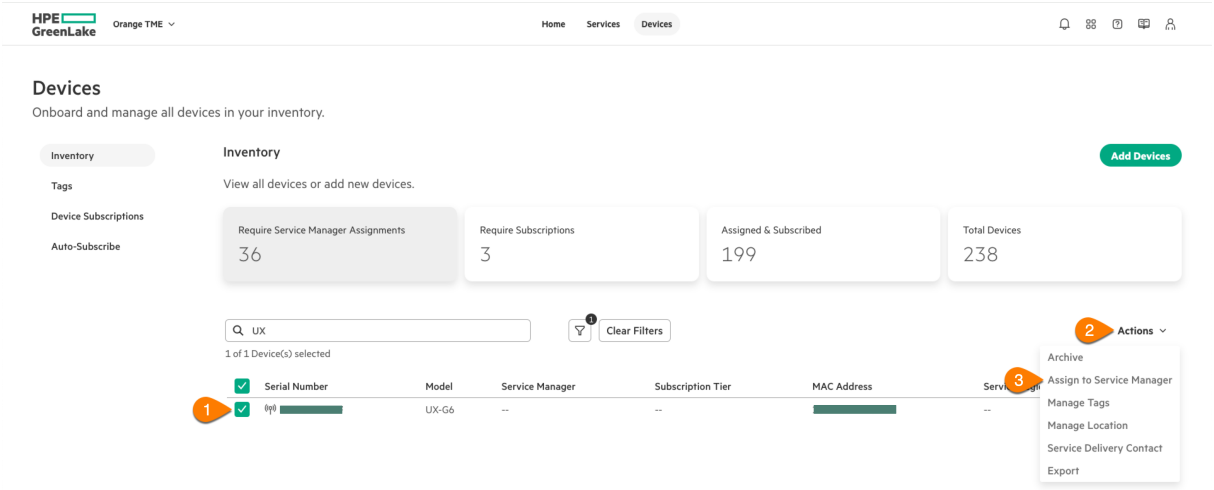



**Figure 31:** UXI Assign to Service Manager

**Step 3** In the **Assign (*x*) Devices to Service Manager** Instance page:

- Select *User Experience Insight* from the **Service Manager** dropdown list
- Select *US West* from the **Region** dropdown list
- Click **Finish**

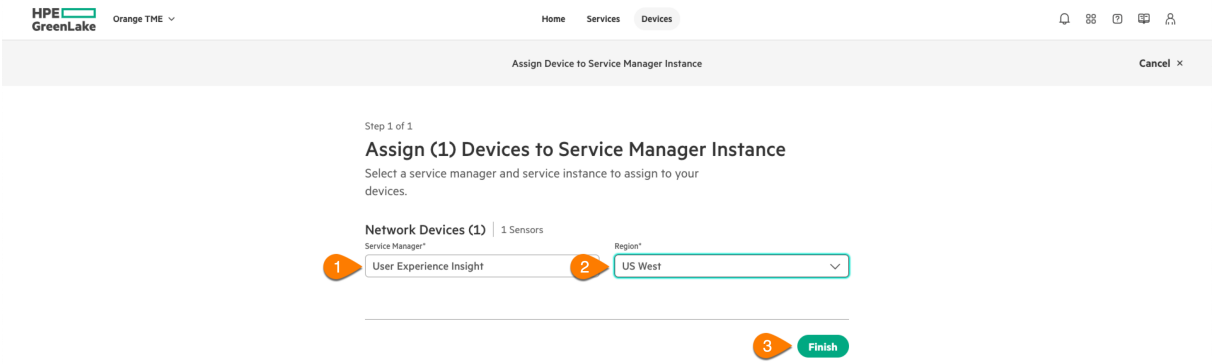



**Figure 32:** UXI Assign Devices to Service Manager

## Add UXI Device Subscriptions

**Step 1** To add UXI Device Subscriptions, perform the following steps:Go to **Devices**, filter for the new sensors by using serial number, Ethernet MAC, or model number. When sensor appears, check the box next to the sensor, click on **Actions**, then select **Apply Subscription** from the dropdown list as shown below.

- Go to **Devices**
- Filter for the new sensors by using serial number, Ethernet MAC, or model number
- When it appears, check the box next to the sensor
- Click on **Actions**
- Select **Apply Subscription** from the dropdown list

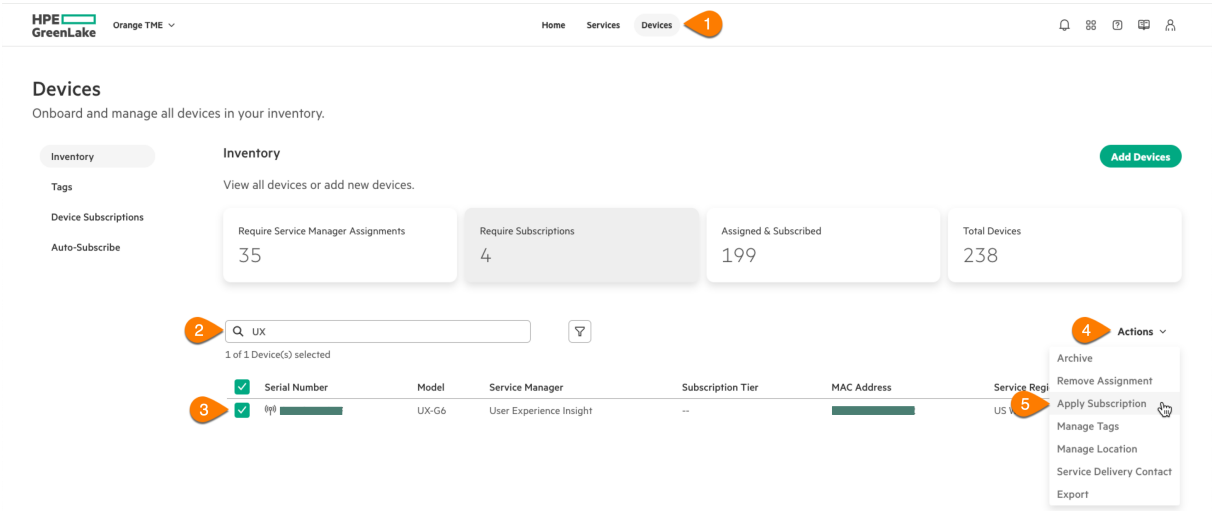



**Figure 33:** UXI Apply Subscription

**Step 2** In the **Apply Subscriptions** page, click on the **Apply Subscriptions** button as shown below.

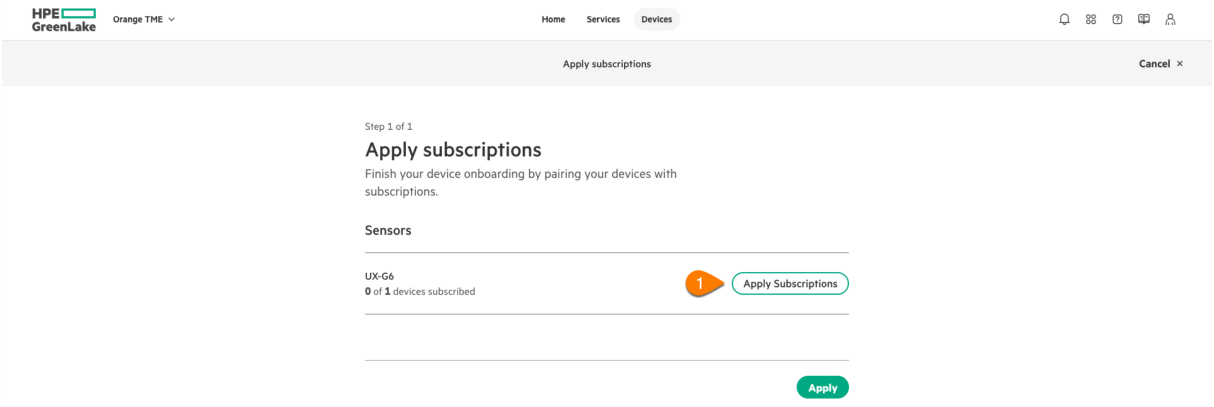



**Figure 34:** UXI Apply Subscription Button

**Step 3** In the **Apply Subscriptions** popup window:

- Select *UXI-Foundation-Sensor-Cloud* from the **Select Subscription Tier** dropdown list

- Check the box next to the subscription key
- Click the **Apply Subscriptions** button

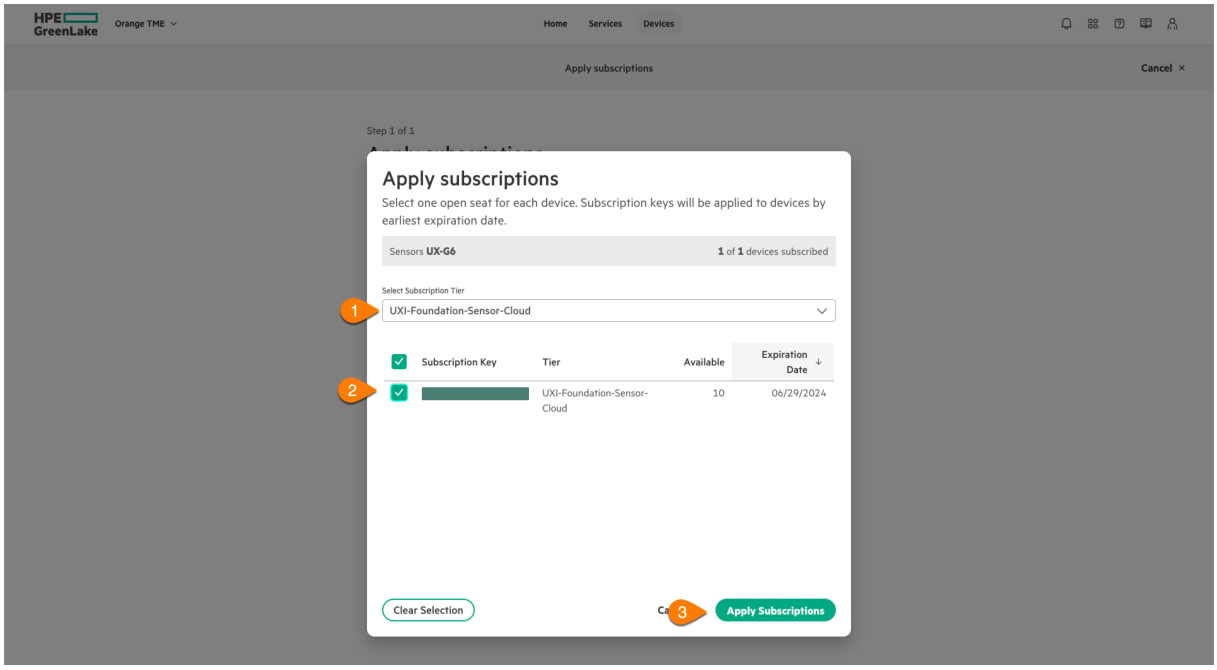



**Figure 35:** UXI Apply Subscription Tier

**Step 4** Ensure you see the expected number of devices subscribed, then click the **Apply** button.

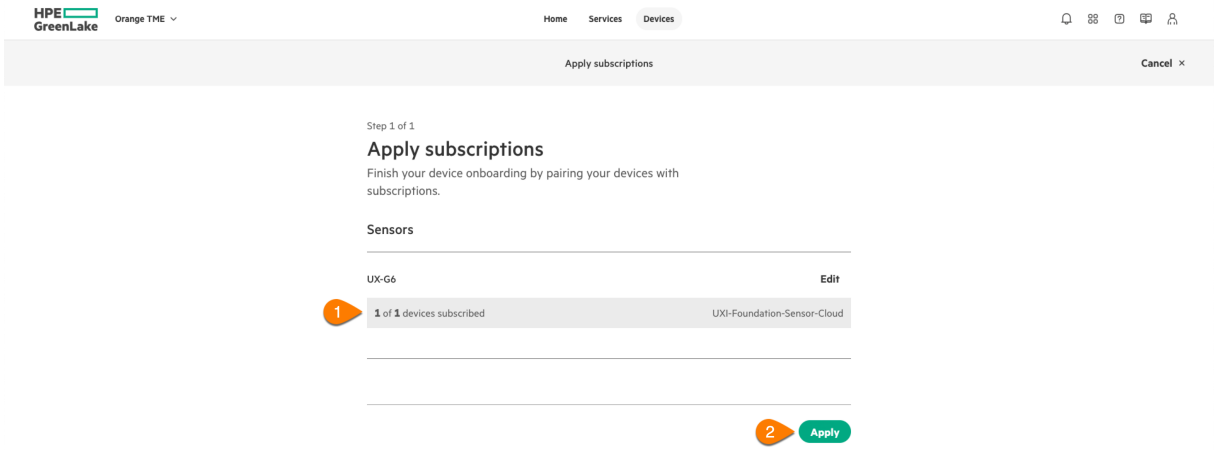



**Figure 36:** UXI Apply UXI Foundation Sensor Cloud 2

**Step 5** When Service Manager, Service Region, and Subscription Tier are successfully assigned, they should look similar to the circled information in the image below.

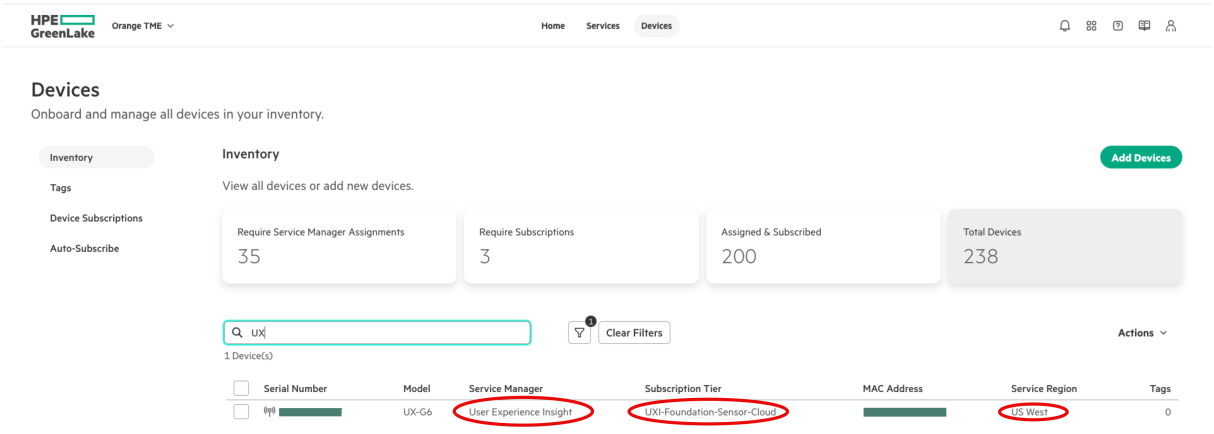



**Figure 37:** UXI - Verify Inventory

**Step 6** At this stage, you have completed the following tasks: - The UXI application is provisioned in your GLP workspace - Your UXI sensors are added as devices in GLP - Your UXI sensors are assigned to the UXI application in GLP - Your subscriptions have been added to GLP and assigned to sensors

If all is complete, move on to the next section.

## Launch UXI Application from GLP

**Step 1** To launch the UXI Application from GLP, log into https://common.cloud.hpe.com/home do the following: - Click the **Services** link at the top of the page - Click the **Launch** button next to the **User Experience Insight** service.

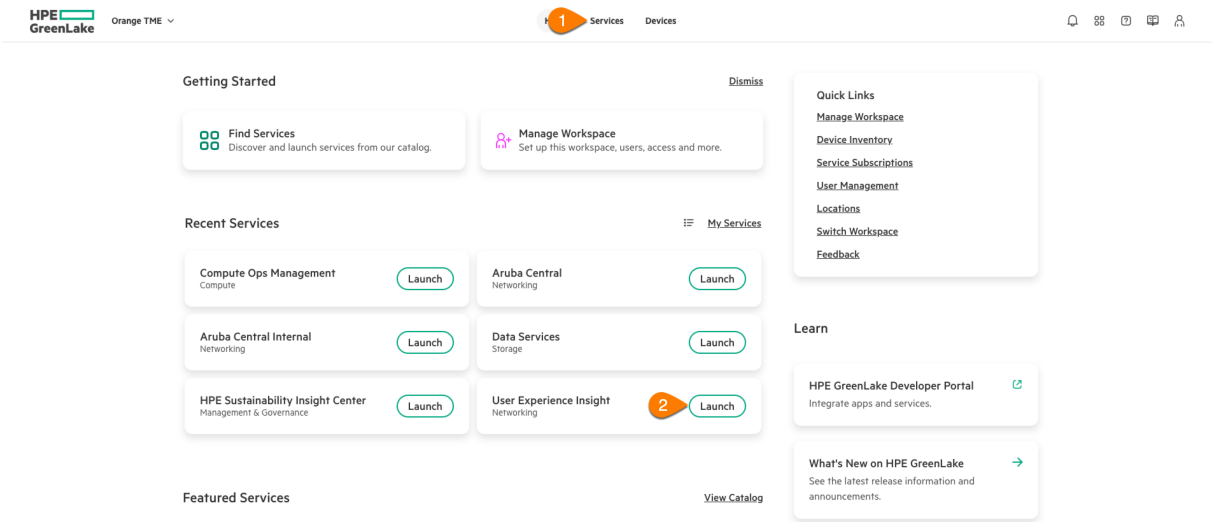



**Figure 38:** UXI Launch GLP UXI

**Step 2** When opening the UXI dashboard for the first time, a message will be displayed indicating no sensors have been configured. Click the **Configure a Sensor** button to go to the sensors page.

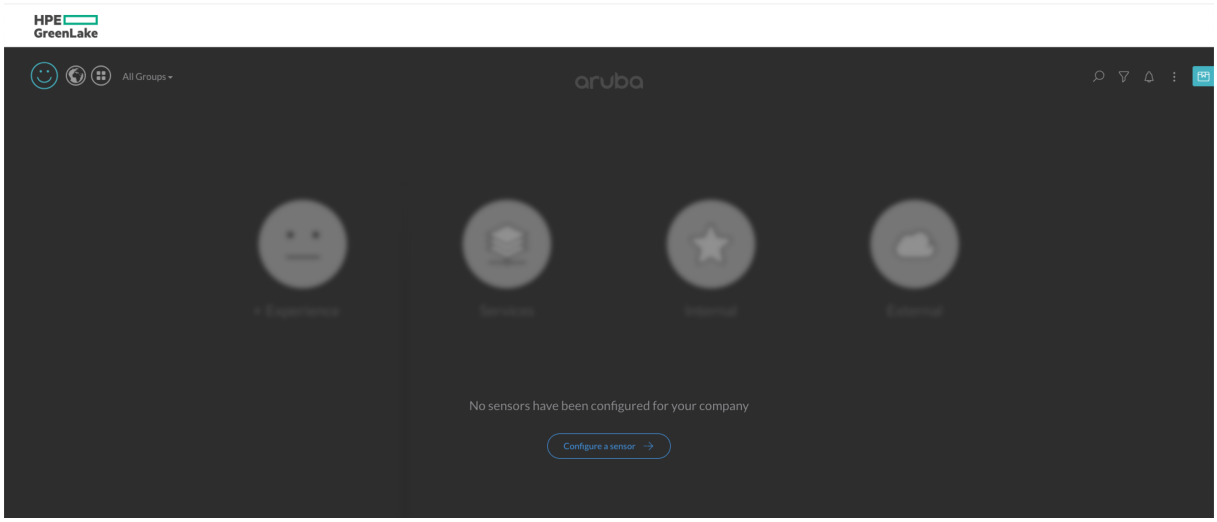



**Figure 39:** UXI Configure a Sensor

**Step 3** In the Sensors & Agents page, verify that the newly added sensor appears in the **Unconfigured** section of the **Sensors & Agents** page with a status of **Waiting for sensor config**.

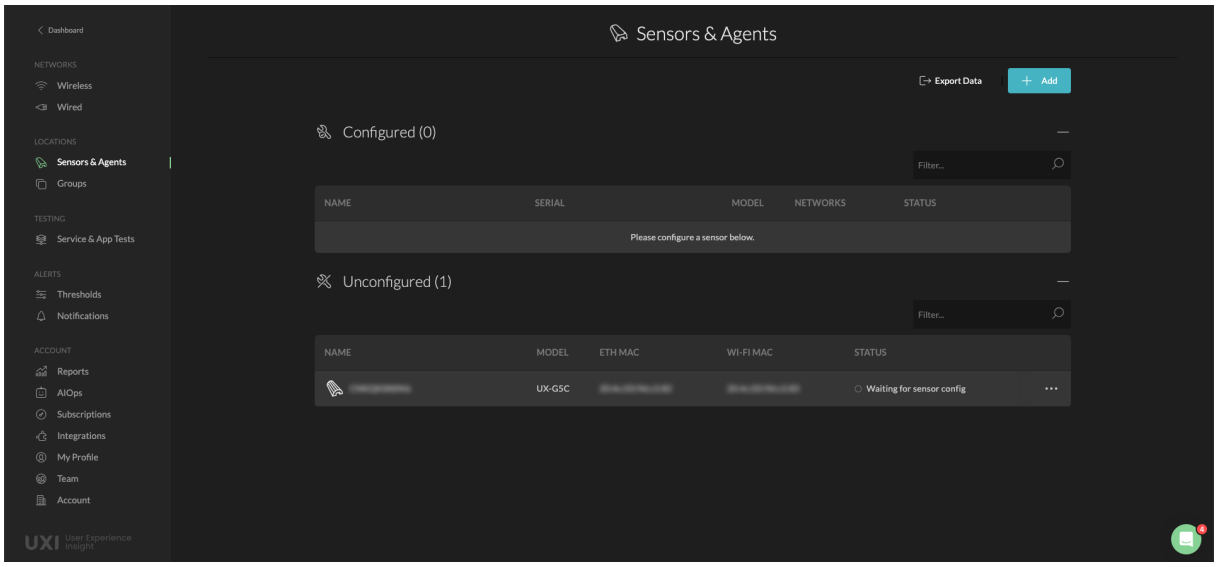



**Figure 40:** Sensor Onboarded

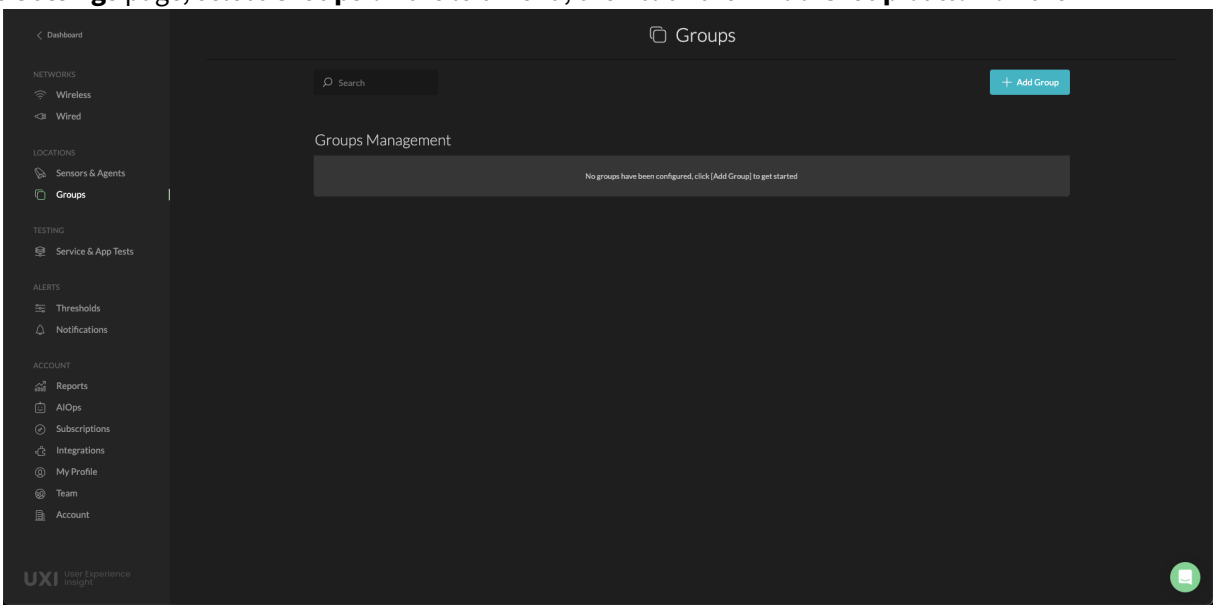
With new sensors ready for configuration, proceed to configure the dashboard.

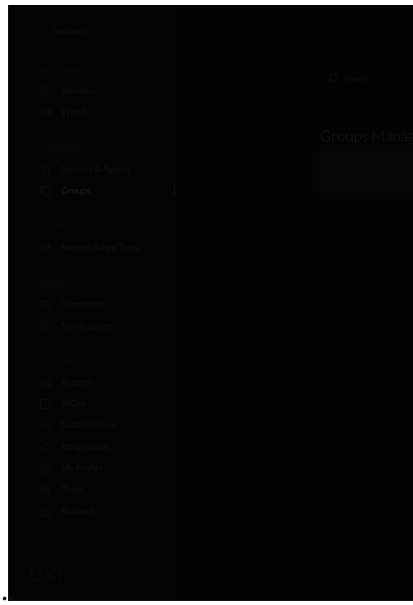
## Configure Dashboard

### *Create Groups*

With sensors onboarded, the next step is to create the Roseville campus group.

**Step 1** In the **Settings** page, select **Groups** on the left menu, then click the **+ Add Group** button on the upper right.



**Step 2** When prompted, enter the name and alias of the Roseville group and click **Add**.

**Step 3** Repeat steps 1 and 2 to create additional groups.

**NOTE:**

Group hierarchy is now available to customers upon request. See the UXI Groups help page for features and instructions.

### *Configure Network Monitoring*

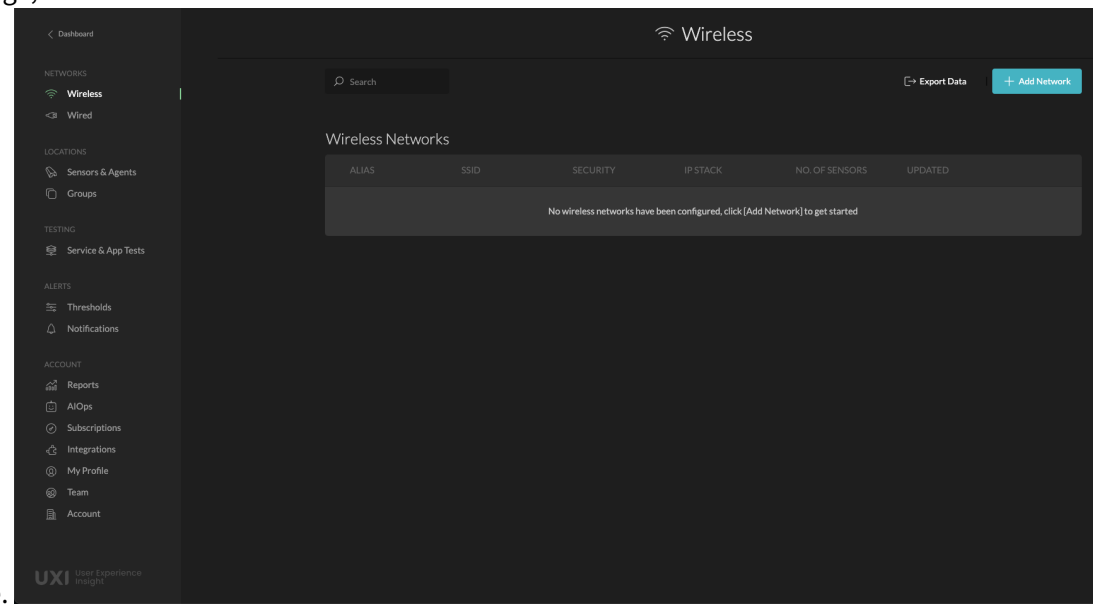
With the new Roseville Campus group created, the next step is to configure the network and service tests. This guide uses the following network settings.

| Network Type | SSID/Alias | Security | Username | Password/Passphrase | Advanced |
|---|---|---|---|---|---|
| Wireless | OWLCorp | PEAP/MSCHAPv2 | uxiservice | Ux153rv1c3! | Band = 5 GHz |
| Wireless | OWLIoT | PSK | N/A | Ux153rv1c3! | None |
| Wired | Guest | None | N/A | N/A | VLAN = 2 |
| Wired | Management | None | N/A | N/A | None |

**NOTE:**

While there is no limit to the number of networks that can be created on the UXI dashboard, each sensor supports up to four networks in any combination of wired and wireless. For more information, visit the Testing Multiple Networks page.

**Step 1** On the **Settings** page, select **Wireless** on the left menu and click the **+ Add Network** button on the upper right of the page.




**Step 2** In the **Add SSID** window, enter the following information for OWLCorp SSID:

- **SSID:** *OWLCorp*
- **Alias:** *OWLCorp*
- **Security:** *Enterprise*
- **Auth Method:** *Password*
- **EAP Type:** *PEAP*
- **Phase 2 Auth:** *MS-CHAPv2*
- **Username:** *uxiservice*
- **Password:** *Ux153rv1c3!*

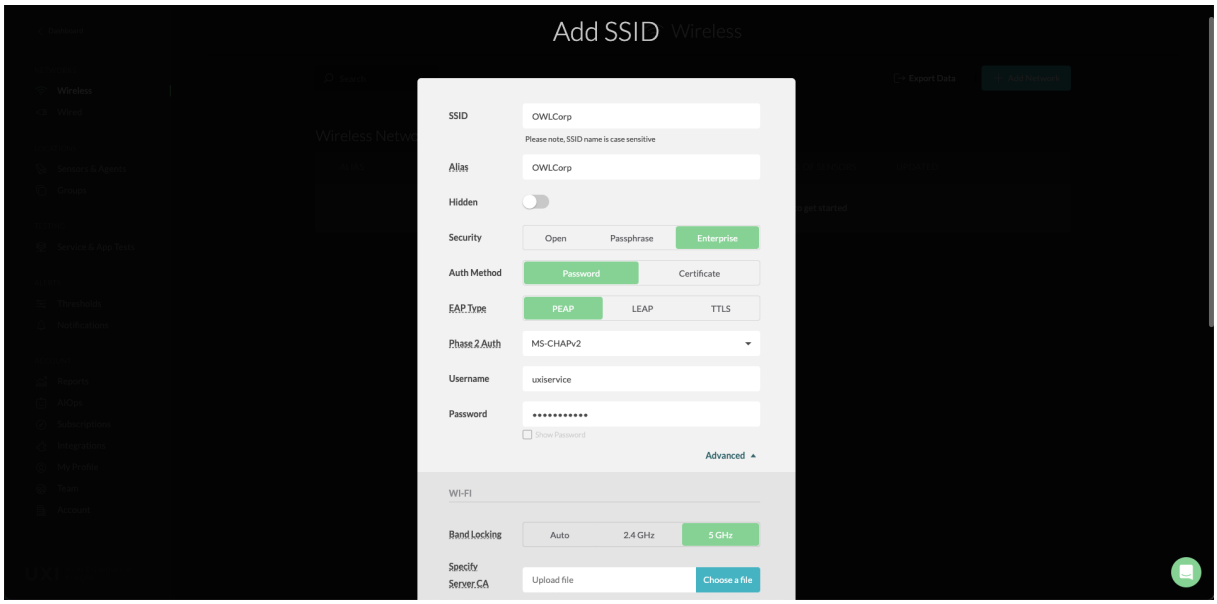
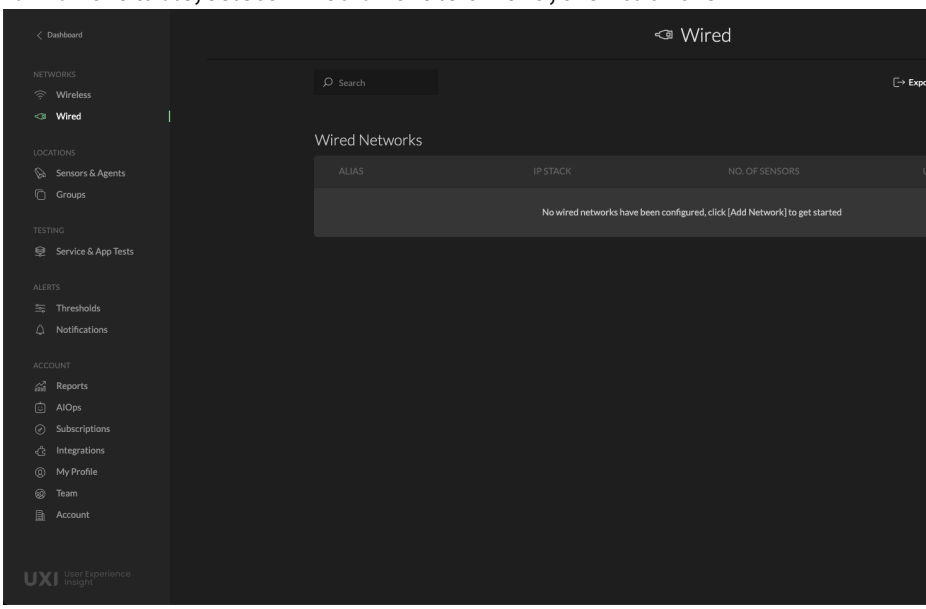



**Figure 41:** Add SSID

**Step 3** Repeat steps **1** and **2** above to add the next wireless network in the table at the beginning of this section.

**Step 4** To configure the wired **Guest** network on the table, select **Wired** on the left menu, then click the **+ Add Network** button on the upper right.




**Step 5** In the **Add Wired Network** window, assign the following settings, then scroll to the bottom and click the **Add** button.

- **Alias**: *Guest*
- **Specify VLAN**: *Enable*
- **VLAN ID**: *2*

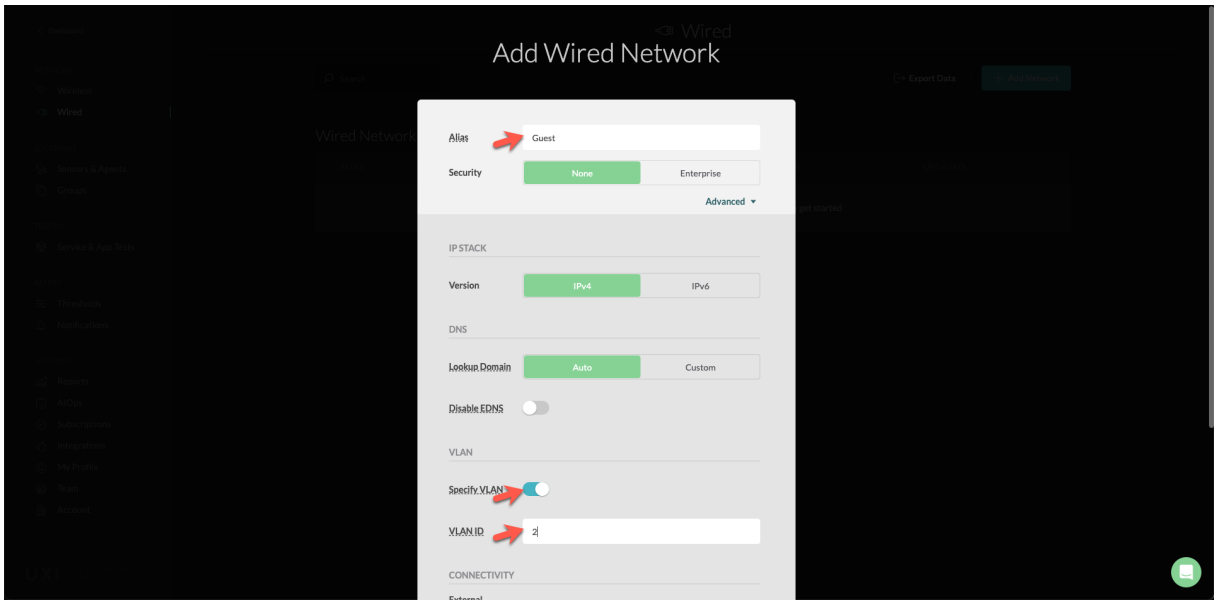



**Figure 42:** Add Wired Network

**Step 6** Repeat steps 4 and 5 to add the last wired network in the table

**NOTE:**

For guest networks with captive portals, follow the steps on the Aruba UXI Captive Portal Setup page.

### *Configure Services and App Tests*

OWL hosts multiple large customers every week. Fast, reliable, and stable connectivity to both internal and external resources is crucial. To provide reliable connectivity, the following services are monitored:

| Service Type | Template | Title | Target | Tests | Frequency |
|---|---|---|---|---|---|
| Internal | Custom/Webserver | Webserv | 172.16.23.36 | HTTP, ICMP Ping | Fastest |
| External | Predefined/Salesforce | N/A | www.salesforce.com | HTTP, HTTPS, ICPM Ping | 30 Min |
| Internal | Custom/Telnet Server | AS400 | as400.corp.owllogistics. | Port 23 | 10 Min |

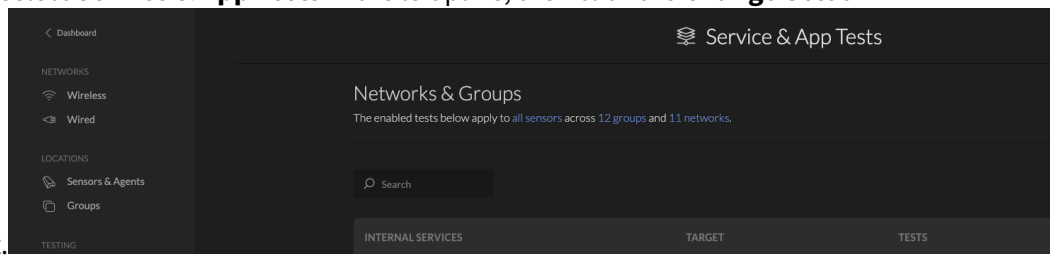
#### *Select Groups*

To add a new test to sensors in a specific group or network, follow the steps below.

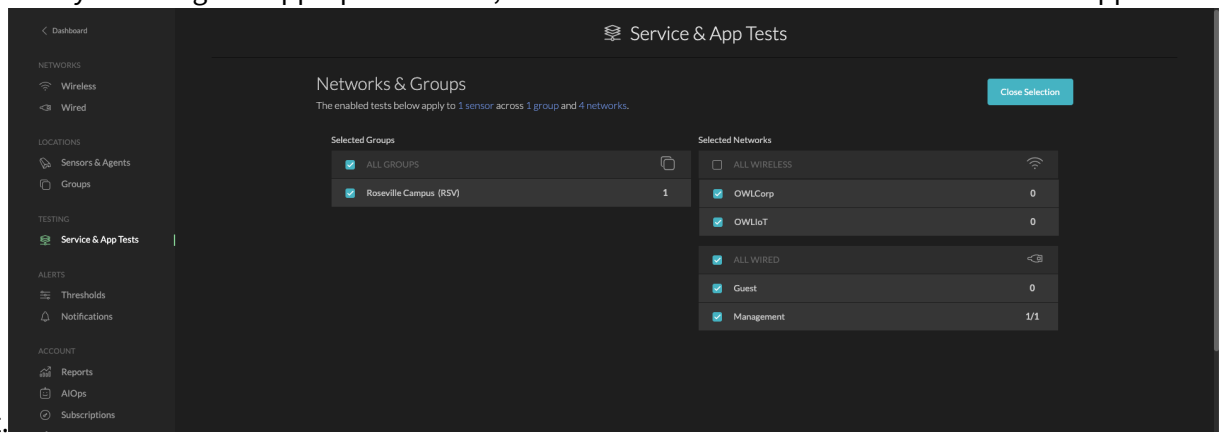
**CAUTION:**

When creating a new test, the default selection includes all groups, sensors, and networks, leading to global application. Ensure that the correct groups, SSIDs, and ethernet networks are chosen in advance to avoid unintended application across all of them.

**Step 1** On the **Settings** page, select **Service & App Tests** in the left pane, then click the **Change Selection** button on the upper right.




**Step 2** Ensure that the **Roseville Campus** group and the required wired and wireless networks are selected by checking the appropriate boxes, then click the **Close Selection** button on the upper right.




**NOTE:**

For more detail about network and group selection, go to the Selecting Groups and Networks While Configuring Tests page.

### *Add Internal Web Server Test*

The first test added is for the internal web server. Aruba UXI tests a web server by checking the following:

- Port availability
- HTTP status codes

Follow the steps below to configure the first test in the service table above.

**Step 1** On the **Settings** page, select **Service & App Tests** in the left pane and click the **Add Test** button on the upper right.

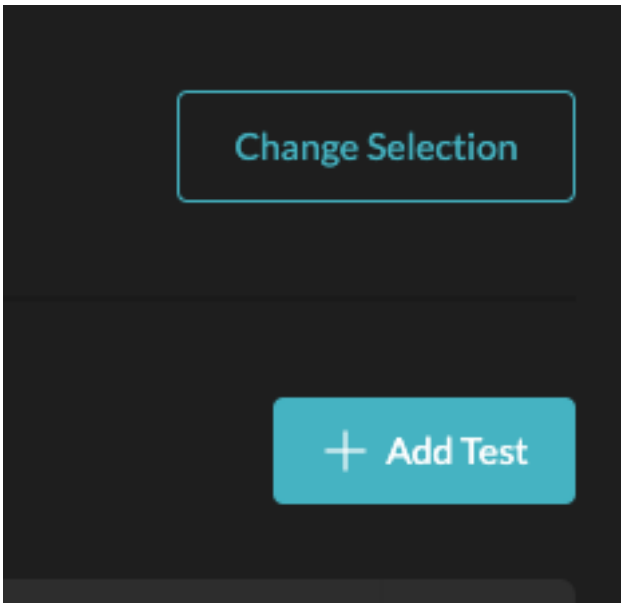



**Figure 43:** Add Test

**Step 2** In the **Add Test** window, enter the following information and click the **Add** button.

- **Service Category:** *Internal*
- **Template Type:** *Custom*
- **Test Template:** *Webserver*
- **Title:** *Webserver*
- **Target:** *172.16.23.36*
- **Tests:**
  - **HTTP:** *enabled*
  - **HTTPS:** *disabled*
  - **ICMP ping:** *enabled*
  - **HTTP status codes:** *disabled*
  - **Validate SSL** Certificate: *disabled*
- **Frequency:** *Fastest*
- **Rate Limit:** *disabled*

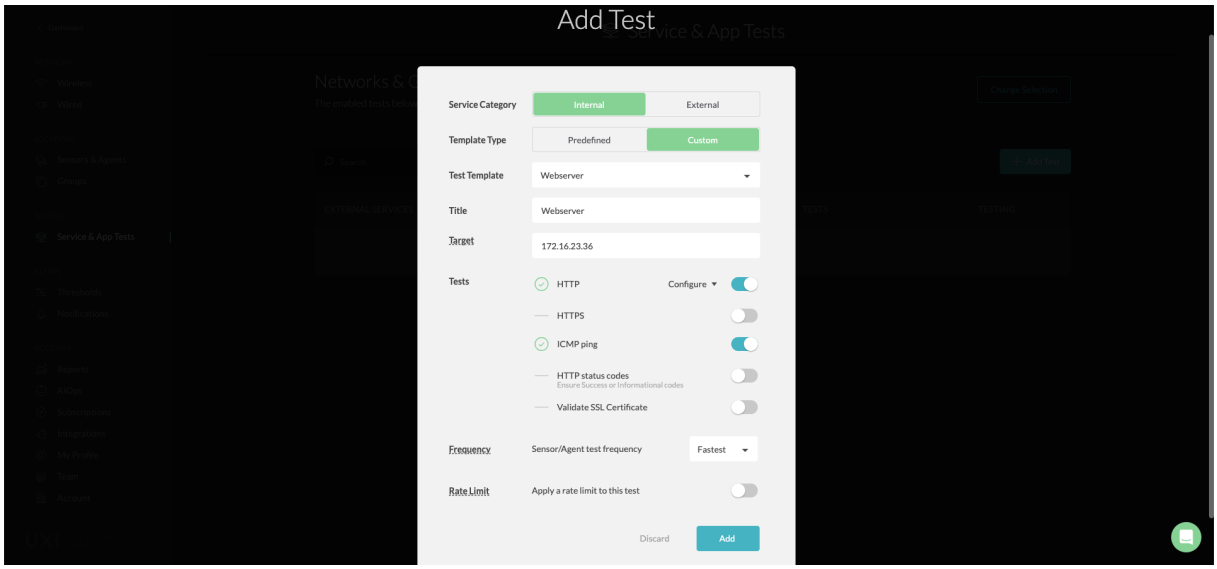



**Figure 44:** Add Tests

**NOTE:**

User Experience Insight now provides customers with a deeper understanding of web application performance from the end-user perspective with the Web Application Testing (WAT) framework. For more details, visit the UXI Web Application Testing page.

### *Add External Predefined Test*

With the proper groups selected as instructed in the **Select Groups** section above, proceed to configure the second test.

**Step 1** On the **Settings** page, select **Service & App Tests** in the left pane and click the **Add Test** button on the upper right.

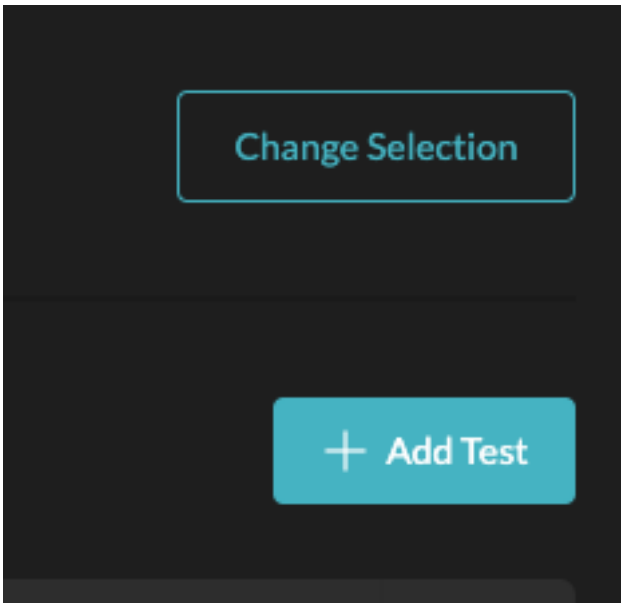



**Figure 45:** Add Test

**Step 2** In the next **Add Test** window, enter the following information and click the **Add** button.

- **Service Category:** *External*
- **Template Type:** *Predefined*
- **Test Template:** *Salesforce*
- **Target:** *172.16.23.36*
- **Tests:**
  - **HTTP:** *Port 80*
  - **HTTPS:** *Port 443*
  - **ICMP ping:** *enabled*
- **Frequency:** *30 Min*
- **Rate Limit:** *disabled*

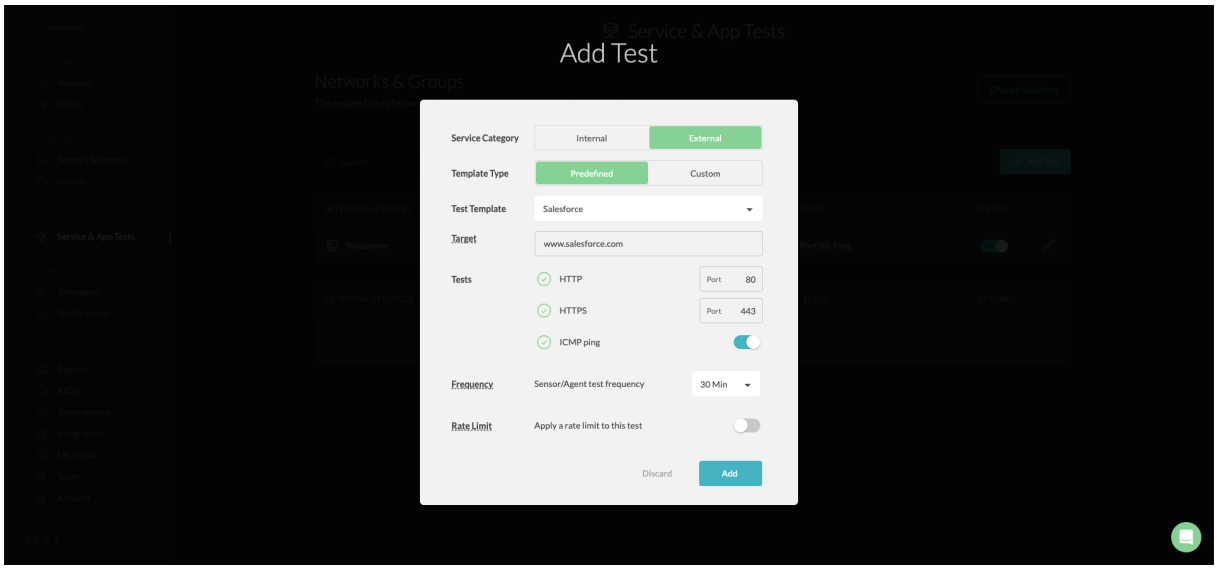



**Figure 46:** Add Salesforce Test

### *Add Custom Test Template*

Aruba UXI includes customizable tests that provide useful end-user experience data and analytics for applications and services. Use the following procedure to configure the custom test template listed as the last test in the **Tests** table above.

**Step 1** With the proper groups selected as instructed in the **Select Groups** section above, proceed to configure the custom test(s).

**Step 2** On the **Settings** page, select **Service & App Tests** in the left pane and click the **Add Test** button on the upper right

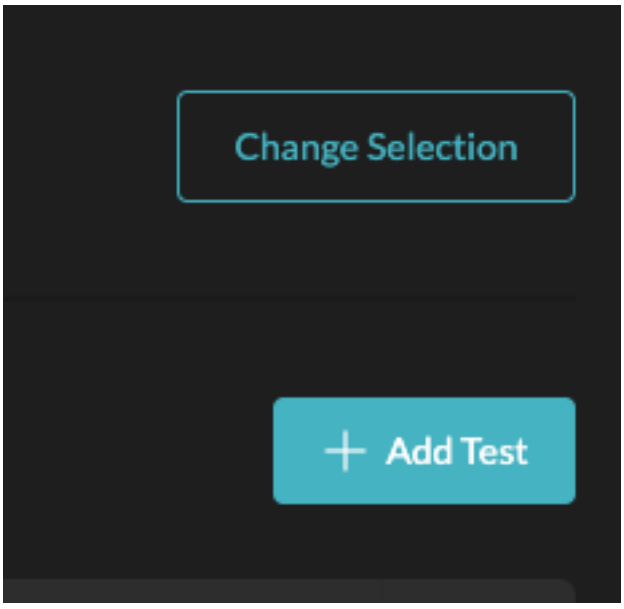



**Figure 47:** Add Test

**Step 3** In the next **Add Test** window, enter the following information and click the **Add** button. - **Service Category:** *Internal* - **Template Type:** *Custom* - **Test Template:** *Telnet Server* - **Target:** *as400.corp.owllogistics.com* - **Tests:** - **Search String:** (leave blank) - **Port:** *23* - **Frequency:** *30 Min* - **Rate Limit:** *disabled*

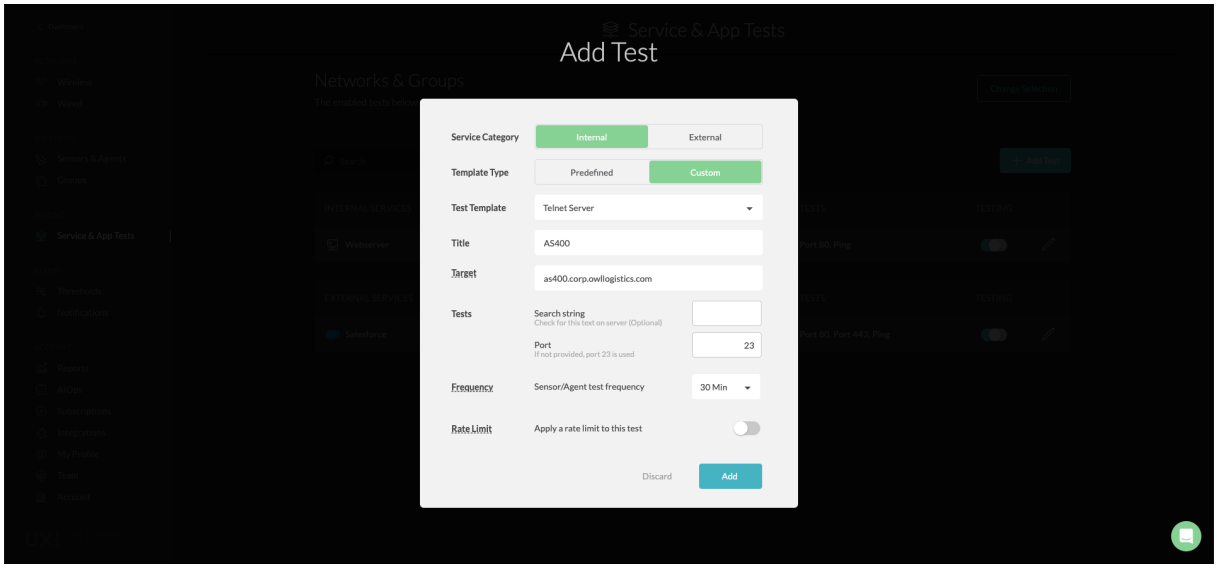



**Figure 48:** Add Telnet Test

## *Configure Alerts*

Aruba UXI alerts include dashboard notifications and emails. Follow the steps below to review and edit as needed.

### *Thresholds*

Thresholds are calculated by taking a rolling mean over the last three measurements. Threshold breaches must last for a specified duration before they are reported.

Use the default settings for the initial deployment, then monitor for a few weeks to establish a baseline for the sites. If threshold changes are needed, modify and review them using the steps below.

**Step 1** On the **Settings** page, select **Thresholds** under **Alerts** and review the **Wi-Fi** thresholds.

**Step 2** Click the slider  to the right of each line to enable or disable monitoring for the related issue.

**Step 3** Click the pencil icon  on the right of the enable/disable slider to modify the thresholds.

**Step 4** Repeat steps 1 to 3 for **Network**, **Internal**, and **External** thresholds.

### *Notifications*

To subscribe to notifications, follow the steps below.

**Step 1** In the same **Alerts** section of the left pane, click **Notifications** and review or modify the configuration.

**Step 2** Under the **Subscribe to Alerts** section, click the slider  on the right of the notifications to be enabled.

**Step 3** Click the pencil icon  on the right of the alert email address to modify the email, notification hours, and/or time zone.

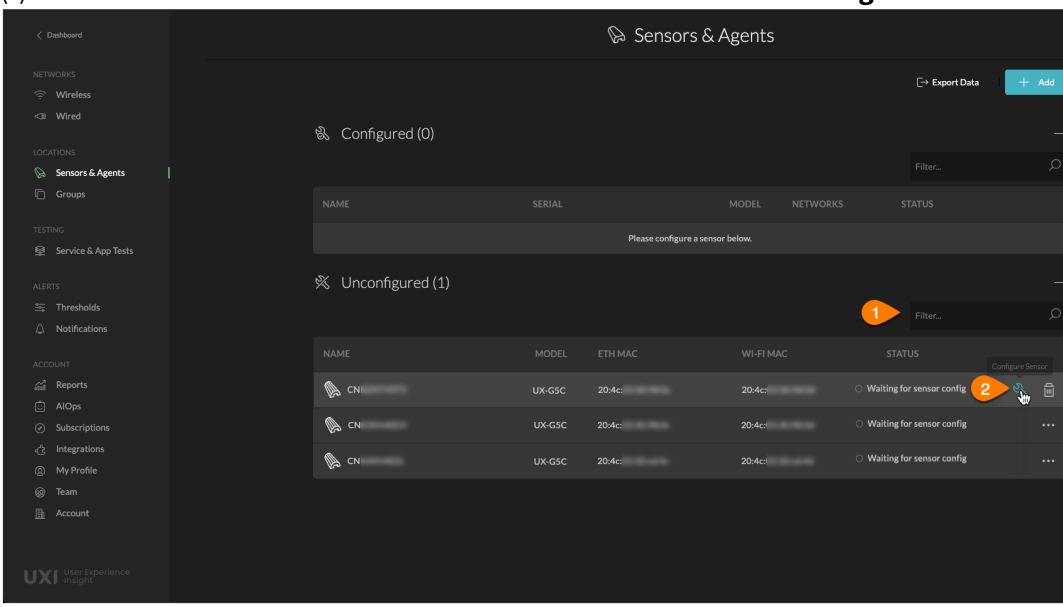
## Configure Sensors

After configuring network testing, groups, and alerting, the sensors can be renamed and added to their designated groups. The steps below install the sensors according to OWL's requirements.

### *Organize and Rename*

Follow the steps below to rename sensors and assign them to their designated groups.

**Step 1** On the **Settings** page, click **Sensors & Agents** in the left menu and type the serial number of the first sensor in the **Filter** box (1). Hover the mouse cursor over the sensor line item and click the **Config Sensor** icon (2) that appears.




**Step 2** On the **Add Configuration** page, configure the sensor using the following settings and click the **Add** button:

- **Name:** *RSVCP-UXI1*
- **Group:** *Roseville Campus*
- **Wireless:**
  - *OWLCorp*
  - *OWLIoT*

- **Wired:**
  - *Guest*
  - *Management*

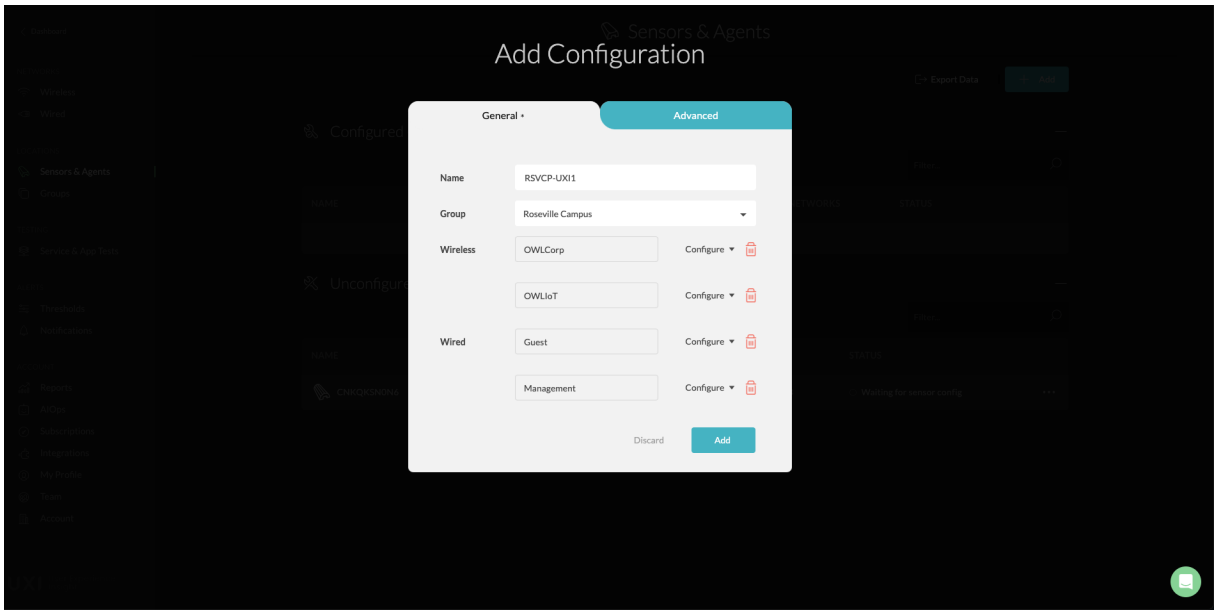
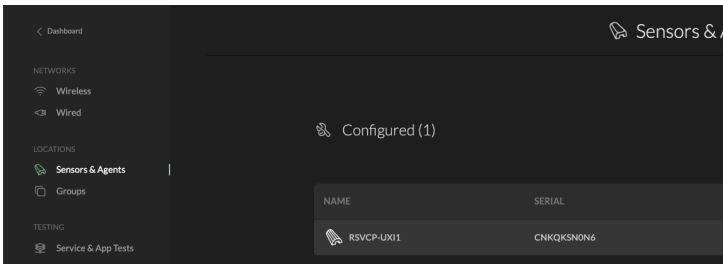



**Figure 49:** Add Configuration




**Step 3** Verify that the sensor moves to the **Configured** list.

**Step 4** Repeat steps 1 and 2 for the remaining sensors.

### *Mount and Connect*

Because Aruba UXI sensors are intended to test user experience, they should be placed where users connect. They can be permanently fixed in certain areas or temporarily relocated for events that may require extra monitoring, such as company meetings or press conferences.

OWL's requirements call for the permanent installation of three UXI Sensors.

Detailed installation steps and options can be found in the Aruba User Experience Insight (UXI) - Sensors tech brief.

### *Monitor*

The time a sensor takes to be detected on the dashboard can vary depending on what process it needs to go through.

When the sensor is first powered, startup software is activated to facilitate faster onboarding: this is designated by a solid **white** LED. The software uploads an AP scan while the main software is still starting up. On Ethernet, the sensor should be detected on the dashboard within **30 seconds** or about **40 seconds** when using mobile only.

If the software onboarding does not succeed, wait for the main software to run (designated by the **flashing white LED**) before the sensor is detected. This will happen about **2 minutes** after powering up the sensor.

The time for the sensor to start testing an SSID varies from this point onward. If the sensor must update to the latest release, testing starts approximately **5 minutes** after powering up (if configured on the dashboard). On a bad mobile connection or if the software requires multiple updates, the time can be extended to 10-15 minutes.

**NOTE:**

If the LED color is **orange,** the sensor has no external connectivity.

See the legend below for the meaning of the sensor LED status lights:

**STATUS LIGHT**


**Figure 50:** Status LEDs

When all three sensors are connected and mounted, log into the UXI dashboard to verify they are collecting performance data as designed.

This concludes the UXI deployment for example customer, OWL Corporation.

# Campus Services

The Services Layer is where the operations team interacts with the Connectivity and Policy layers. It provides significant capabilities using AI, ML, and location-based services for network visibility and insights into how the network is performing. Aruba ESP correlates cross-domain events using a unified data lake in the cloud. It also displays multiple dimensions of information in context, unlocking powerful capabilities for automated root-cause analysis and providing robust analytics. The primary homes for Services Layer functionality are Central and ClearPass Policy Manager.

# AI Insights Configuration

AI Insights quickly identifies, categorizes, and resolves issues that impact client onboarding, connectivity, and network optimization. These insights provide clear descriptions of the detected issue, visualizations of the data, recommended fixes, and contextual data to determine the overall impact.

In this release, the insights are classified in four categories:

- Connectivity — Issues related to the wireless connectivity in the network.
- Wireless Quality — Issues related to the RF Info or RF Health in the network.
- Availability — Issues related to the health of the network infrastructure and the devices in the network such as APs, switches, and gateways.
- Class and Company Baselines — Established to determine what is normal, unusual, and how to improve each network

**NOTE:**

There are no specific knobs for AI Insights. As long as the devices are licensed and connected in Central, AI insights continues to work and provide meaningful, usable insights.

# AirMatch Configuration

AirMatch is a Radio Resource Management service. AirMatch provides automated RF optimization by adapting dynamically to the ever-changing RF environment at the network facility. The AirMatch service receives telemetry data from APs for radio measurements, channel range, transmit power range, operational conditions, and local RF events such as radar detection or high noise. Aruba Central supports the AirMatch service on APs to enable networks to adapt quickly to changing RF conditions, such as co-channel interference (CCI), coverage gaps, and roaming.

Use this procedure to enable AirMatch for automated RF planning.

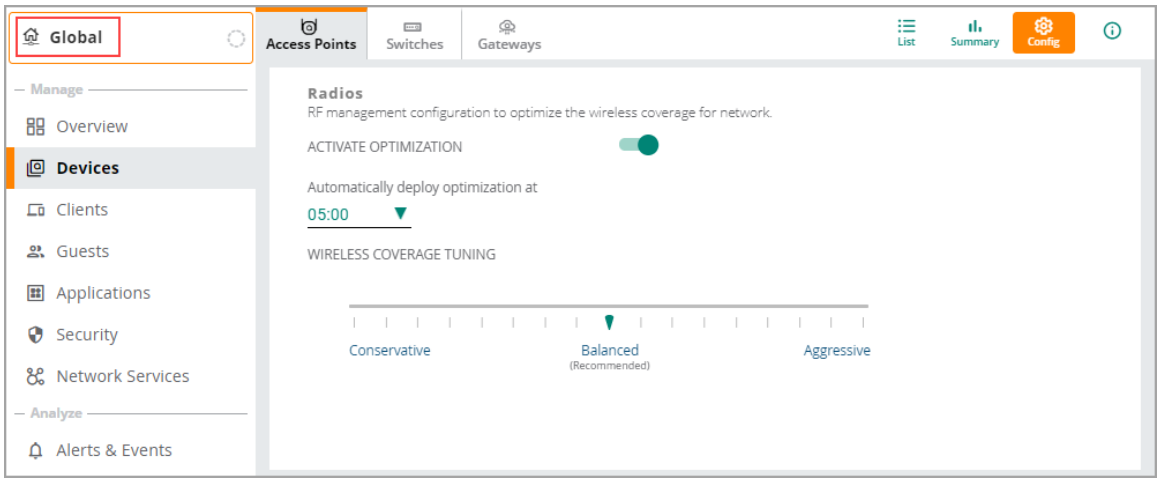
**Step 1** On the Aruba Central Account Home page, launch the **Network Operations** app.

**Step 2** In the dropdown, select the **Global** filter.

**Step 3** On the left menu, select **Devices**, select **Access Points**. At the top right, select **Config**.

**Step 4** On the **Access Points** page, assign the following settings, then click **Save Settings**.

- **Activate Optimization**: *Move slider right*
- **Automatically deploy optimization at**: *05:00*
- **Wireless coverage tuning**: *Balanced*




**NOTE:**

AirMatch is configured at the Global filter level. However, all sites, groups, and devices have a unique channel and power plan based on the AirMatch configuration and local RF environment.

# ClientMatch Configuration

The ClientMatch service helps to improve the experience of wireless clients. ClientMatch identifies wireless clients that are not getting the required level of service at the AP to which they are currently associated and intelligently steers them to an AP radio that can provide better service and improve user experience. No software changes are required in the clients to use the functionality.

**NOTE:**

ClientMatch is enabled by default and does not have configuration options when deployed using AOS 10.

# Aruba Central NetConductor

The Aruba ESP campus can be built using the Aruba Central NetConductor solution of edge-to-cloud networking and security services.

Aruba Central NetConductor is an edge-to-cloud network and security framework designed to meet the challenge of creating dynamic and consistent security policy across the modern enterprise network. Intelligent overlays built on highly available underlays are tied to a full policy-based micro-segmentation model, based on global roles, across the customer's entire network infrastructure.

Role-based policies abstract policy from the underlying network to enable flexible and simplified policy definition and enforcement. Policy definition is enhanced by full automation of the underlay, orchestration of the overlay, a single-pane-of-glass view management and monitoring, and a rich array of complementary services.

The Underlay Orchestration builds an OSPF-based underlay network.

The Overlay Orchestration builds an EVPN-VXLAN overlay network.

# Underlay Orchestration

This section describes how to deploy an OSPF campus underlay network using the HPE Aruba Networking Central NetConductor underlay orchestration workflow. Review requirements listed in the NetConductor Architecture Guide before proceeding with this procedure, especially if using in-band management for switches.

A three-tier network identified as **Herndon** is used to illustrate this process.

## Plan the Underlay

**NOTE:**

Underlay Orchestration requires a minimum AOS-CX firmware version 10.12.

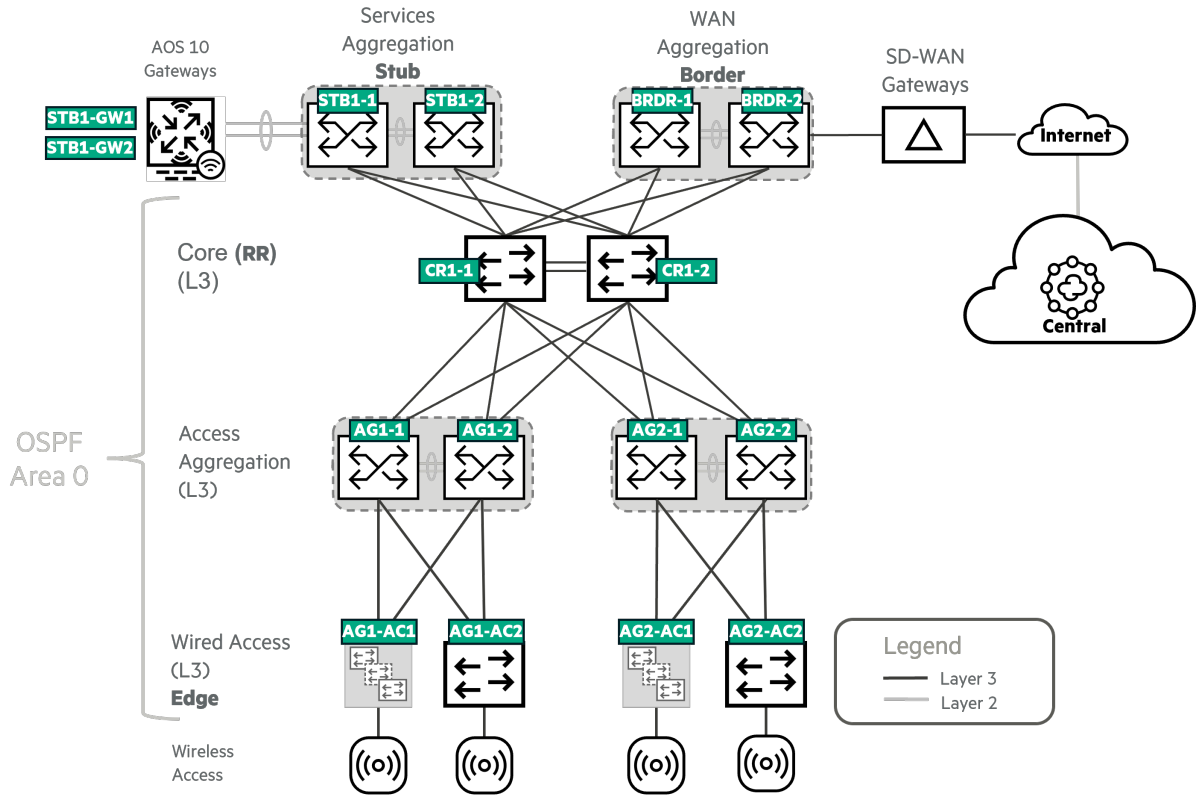
All switches must be online and added to the appropriate Central group to starting the workflow. Connectivity to Central can be established using either in-band management or out-of-band management interface.

For 8000, 9000, and 10000 series CX switches, all ports are configured as Layer 3 and are administratively shut by default. A one-touch provisioning process is required to bring these switches online. In addition, these platforms may require manual configuration of interface speed when connecting to devices using non-default speeds, as well as split-port configurations when breakout cables are in use.

Before running the Underlay Orchestration workflow, all physical links between switches must be connected. This includes the VSX inter-switch link and the VSX keepalive connection. The orchestration process uses these physical connections to determine the network topology and automatically configure OSPF and VSX. Establishing these links during switch deployment allows the workflow to detect redundant switch pairs and apply the appropriate VSX configuration.

The Underlay Orchestration workflow requires two IP address pools. The pools are used to configure point-to-point OSPF links between switches in the fabric and to create two loopback interfaces on each switch. The *loopback0* interface is used as the OSPF router ID and in-band management interface. The *loopback1* interface is used as the VTEP source interface if an EVPN-VXLAN fabric is deployed next.

| Pool Name | Address Range |
|---|---|
| Routed Interface IP Pool | 10.10.0.0/24 |
| Loopback IP Pool | 10.10.1.0/24 |




**NOTE:**

Hostnames shown above have been abbreviated for readability.

## Create a Central Group

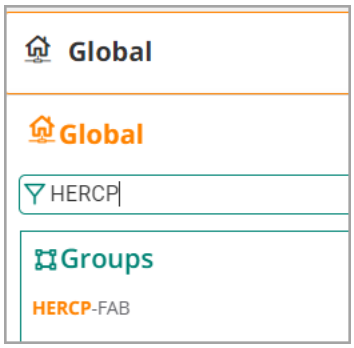
All switches must be online and in the same group. Wireless gateways and APs may be in a different group; however, consider including them in the same group for ease of network management in a greenfield deployment.

For step-by-step instructions on creating a new group and adding devices to it, consult the Central section found earlier in this guide.

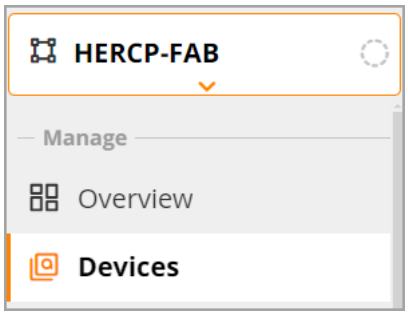
# Configure the Underlay

Use this procedure to configure an OSPF campus using the **Underlay Orchestration** workflow in Central.

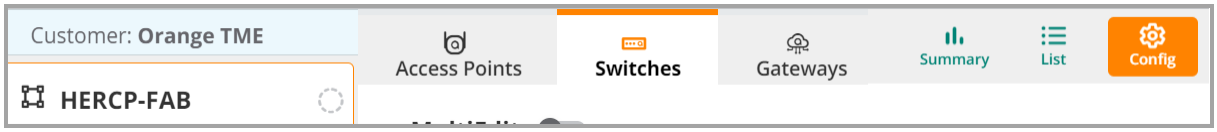
**Step 1** In the **Global** dropdown, select the switch group. In this example, the group is **HERCP-FAB.**




**Step 2** On the left menu, select **Devices**.

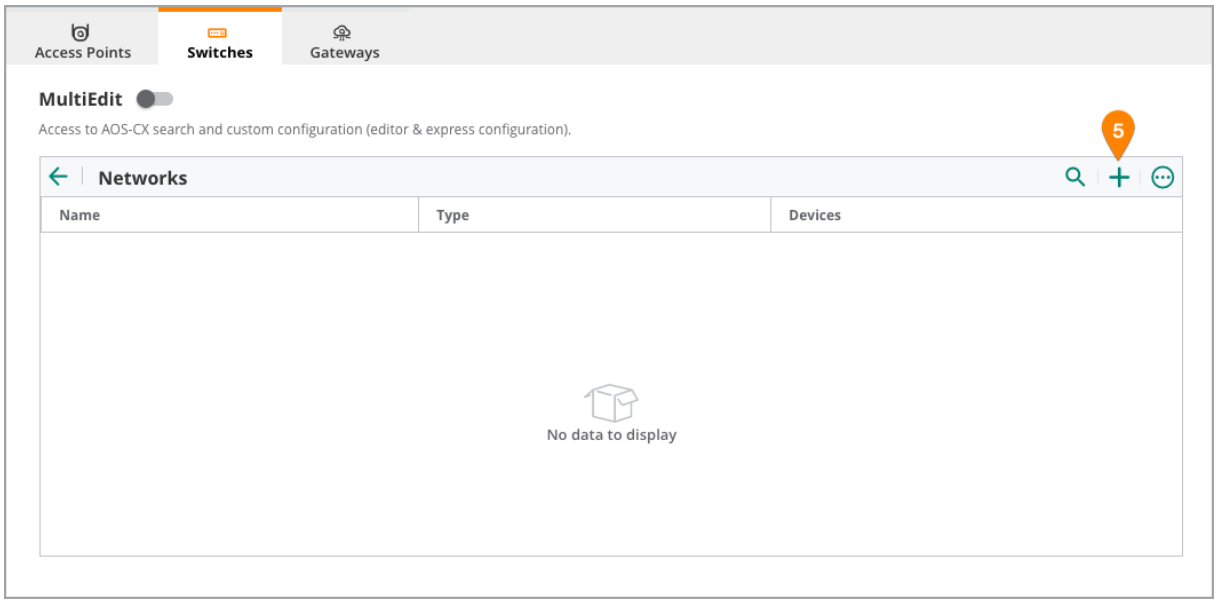



**Step 3** Select **Switches**, then select **Config**.

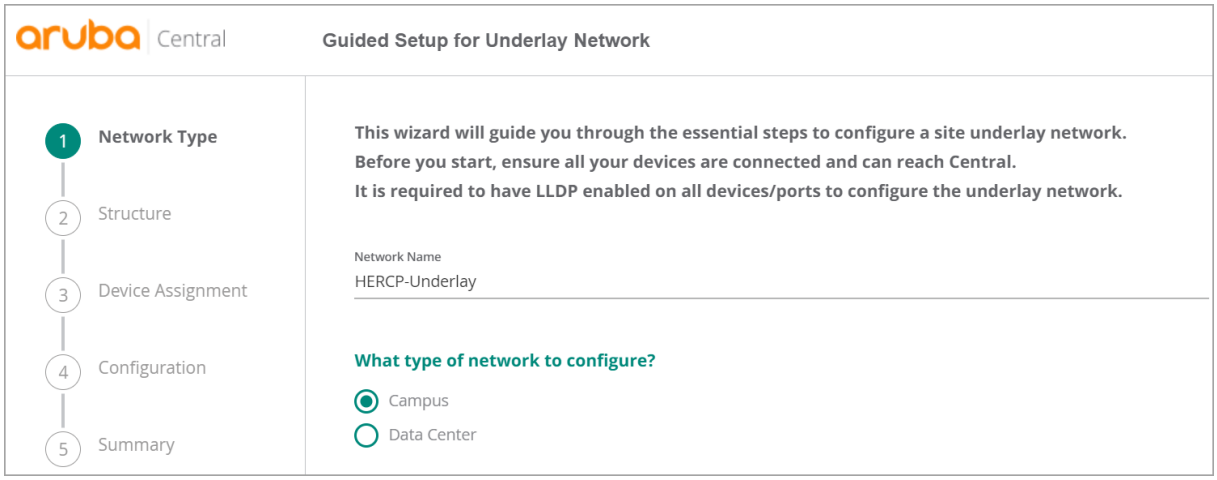



**Step 4** Under **Routing**, select **Underlay Networks.**

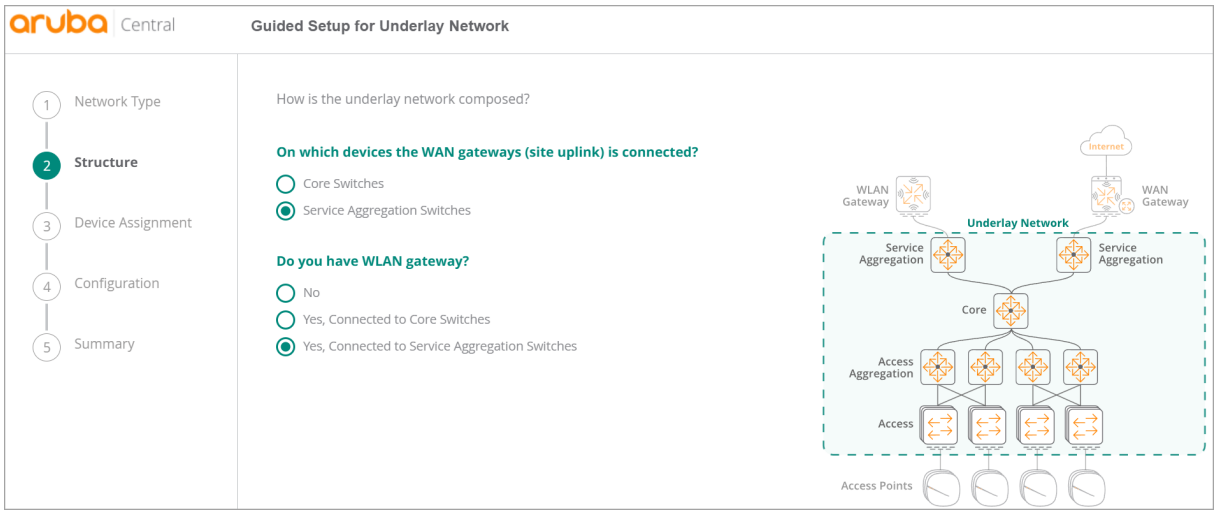

**Step 5** In the **Networks** table, click the **+** (plus sign) at the top right.



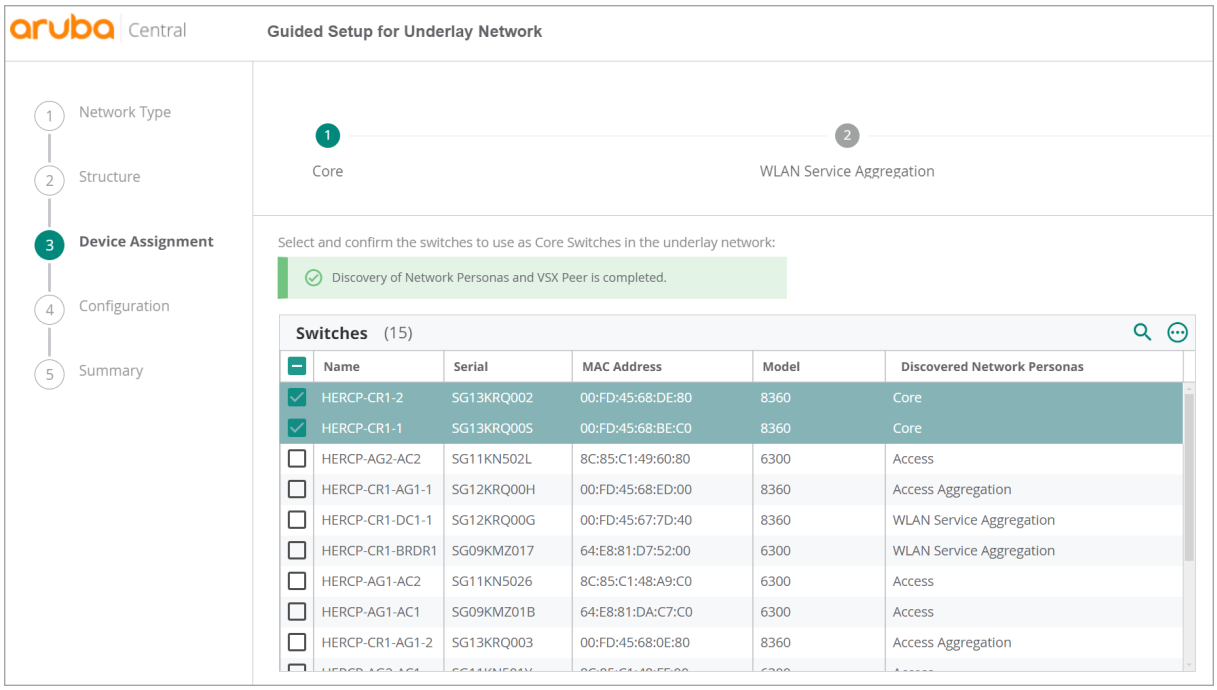

**Step 6** The **Guided Setup for Underlay Network** workflow appears. In the **Network Type** window, assign the following settings, and click **Next**. - **Network Name:** *HERCP-Underlay* - **What type of network to configure?:** *Campus(3 tier L3 access)*



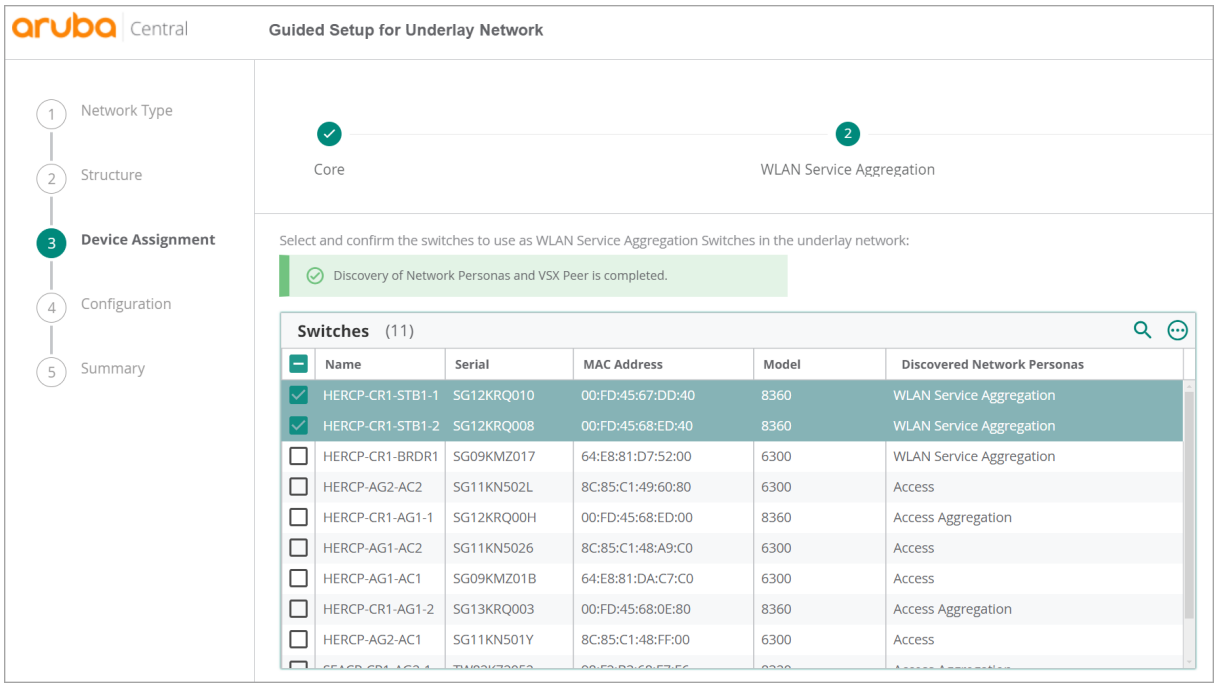

**Step 7** In the **Structure** window, assign the following settings and click **Next**. - **On which devices the WAN gateways (site uplink) is connected?:** *Service Aggregation Switches* - **Do you have WLAN gateway?:** *Yes, Connected to Service Aggregation Switches*



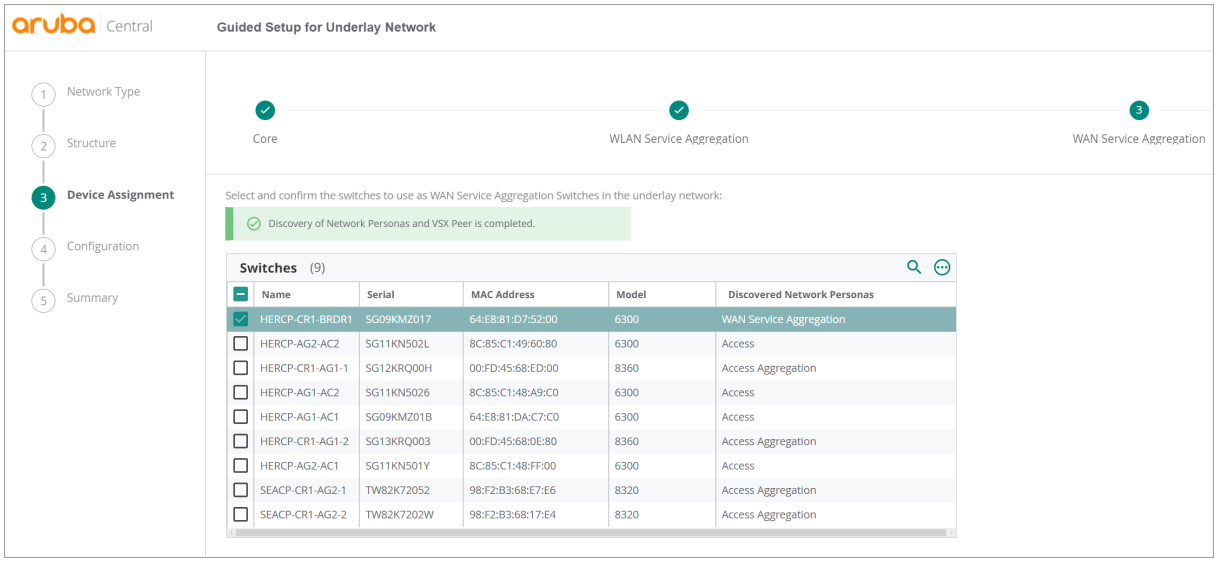

**Step 8** In the **Device Assignment** window, select the **Core Switches** of the network and click **Next**.




**Step 9** In the **Device Assignment** window, select the **WLAN Service Aggregation Switches** for the network and click **Next**.



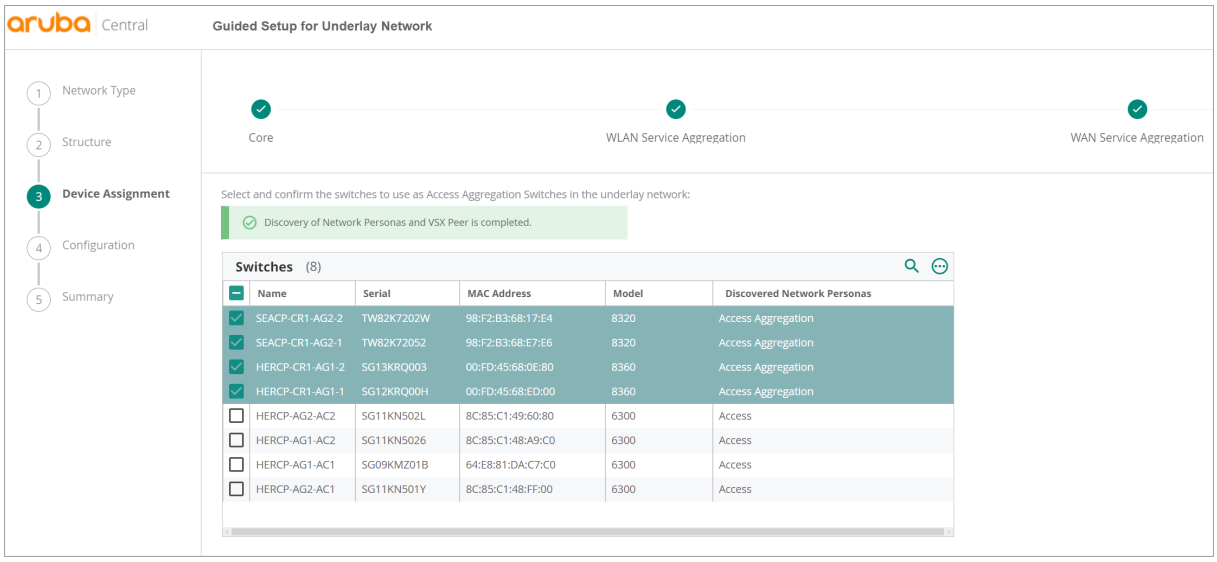

**Step 10** In the **Device Assignment** window, select the **WAN Service Aggregation Switches** for the network and click **Next**.



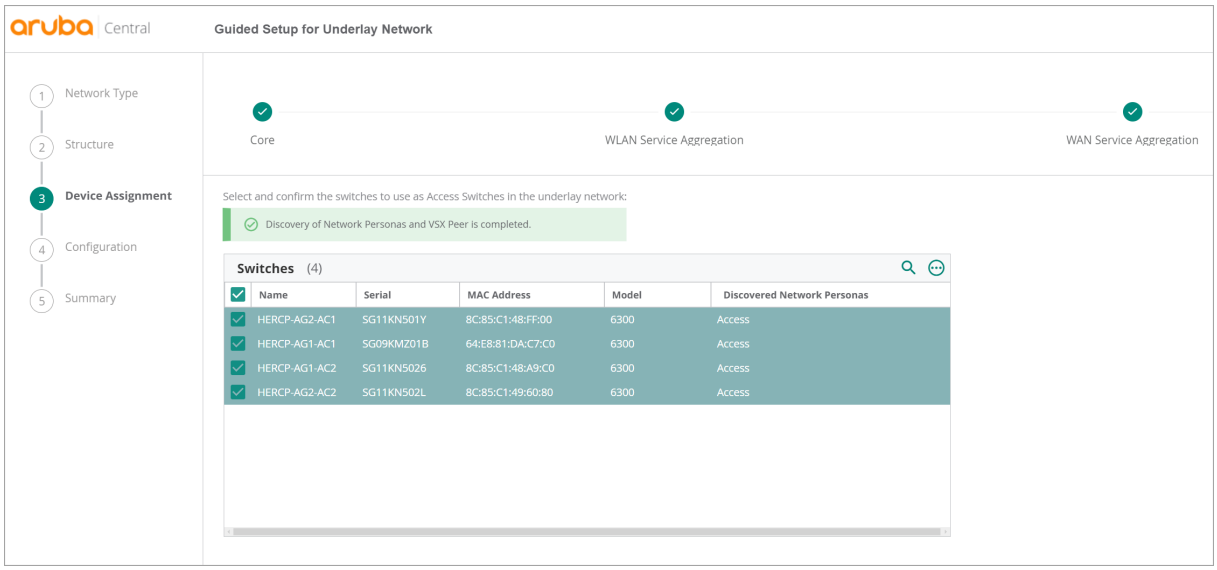

**NOTE:**

In the topology above, the **WAN Service Aggregation** switches are a VSF stack and only one logical switch is selected.

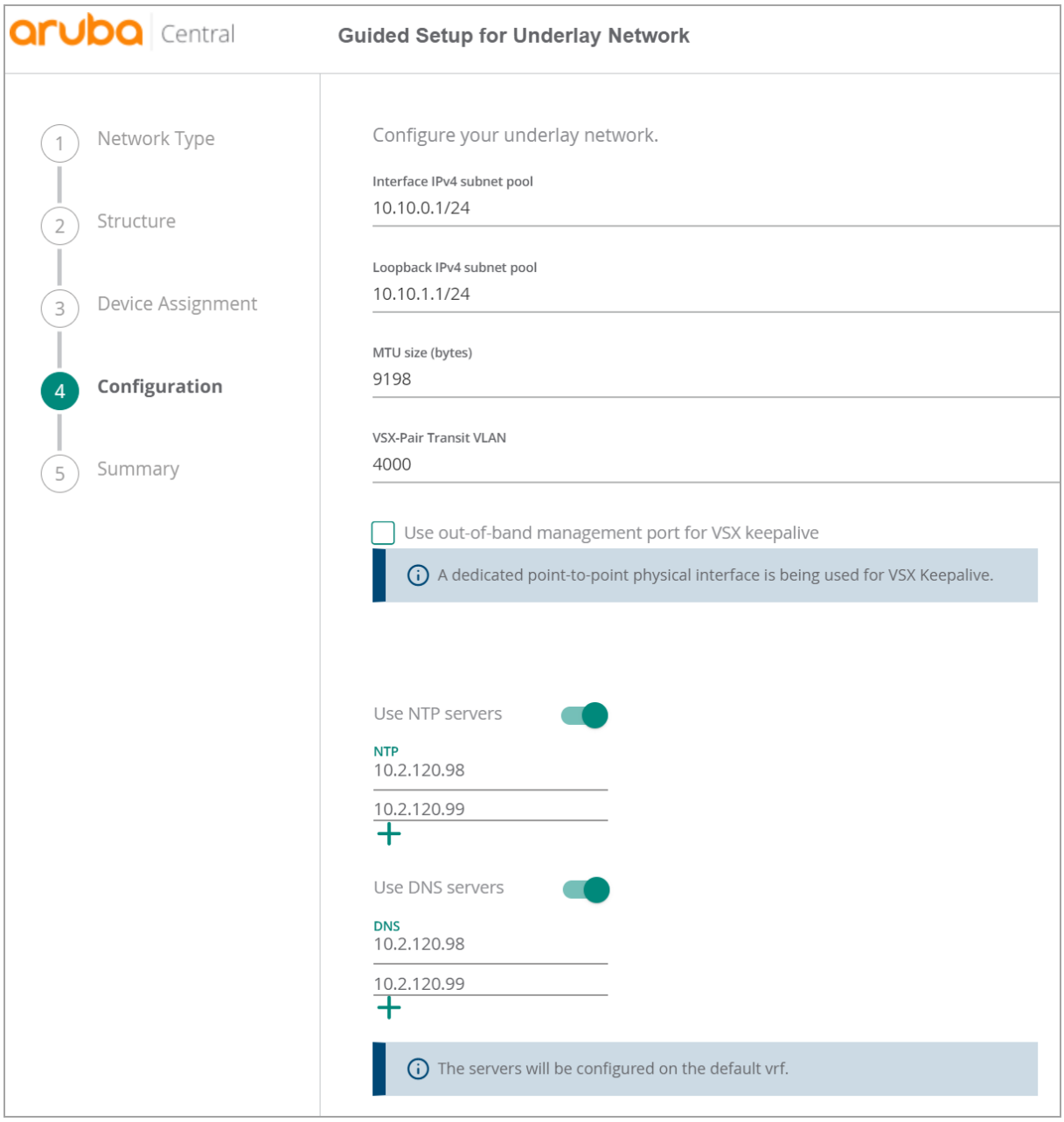
**Step 10** In the **Device Assignment** window, select the **Access Aggregation Switches** for the network and click **Next**.



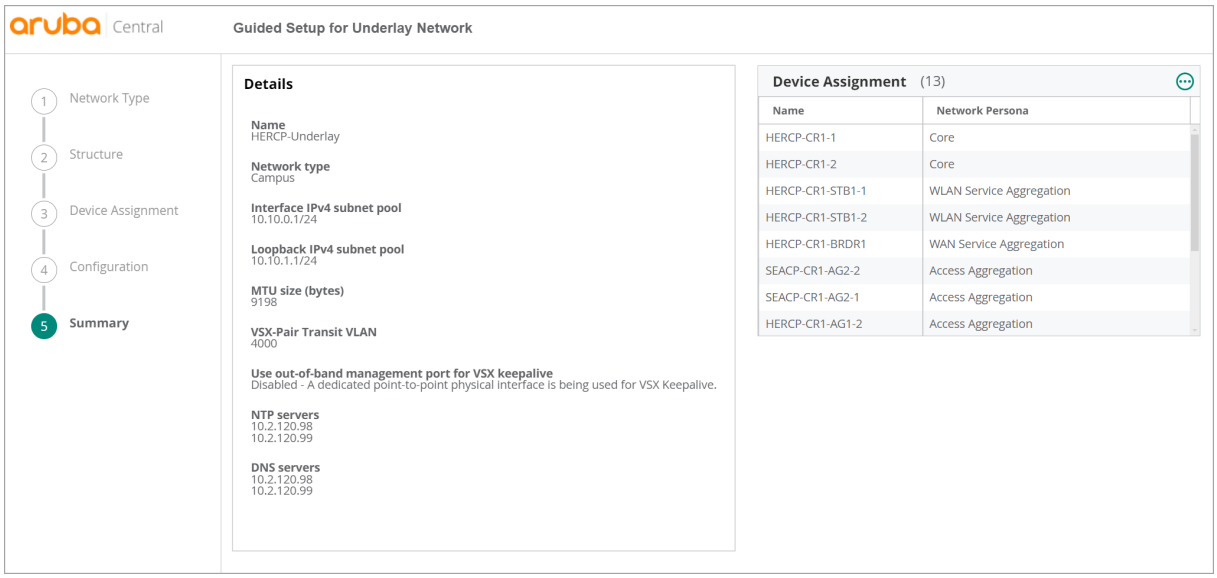

**Step 11** In the **Device Assignment** window, select the **Access Switches** for the network and click **Next**.



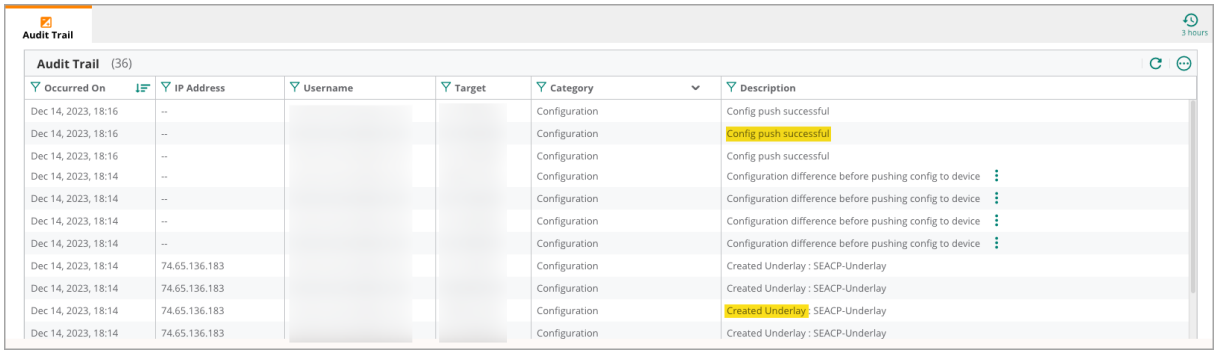

**Step 12** In the **Configuration** window, enter the following values or leave the default, then click **Next**: - **Interface IPv4 subnet pool:** *10.10.0.1/24* - **Loopback IPv4 subnet pool:** *10.10.1.1/24* - **MTU size (bytes):** *Leave default* - **VSX-Pair Transit VLAN:** *Leave default* - **Use out-of-band management port for VSX keepalive:** *Leave unchecked* - **Use NTP servers:** *Slide to the right* - Inherited from group - **Use DNS servers:** *Slide to the right* - Inherited from group




**Step 13** In the **Summary** window, review the configuration details, then click **Finish**. Central immediately begins to configure the network.




**Step 14** On the left menu, select **Audit Log**. Confirm the successful deployment of the underlay configuration by observing the log messages highlighted below.



# Overlay Fabric Orchestration

This section describes how to deploy a NetConductor EVPN-VXLAN overlay on a deployed underlay using the Underlay Wizard.

A three-tier network identified as **Herndon** is used to illustrate the process.

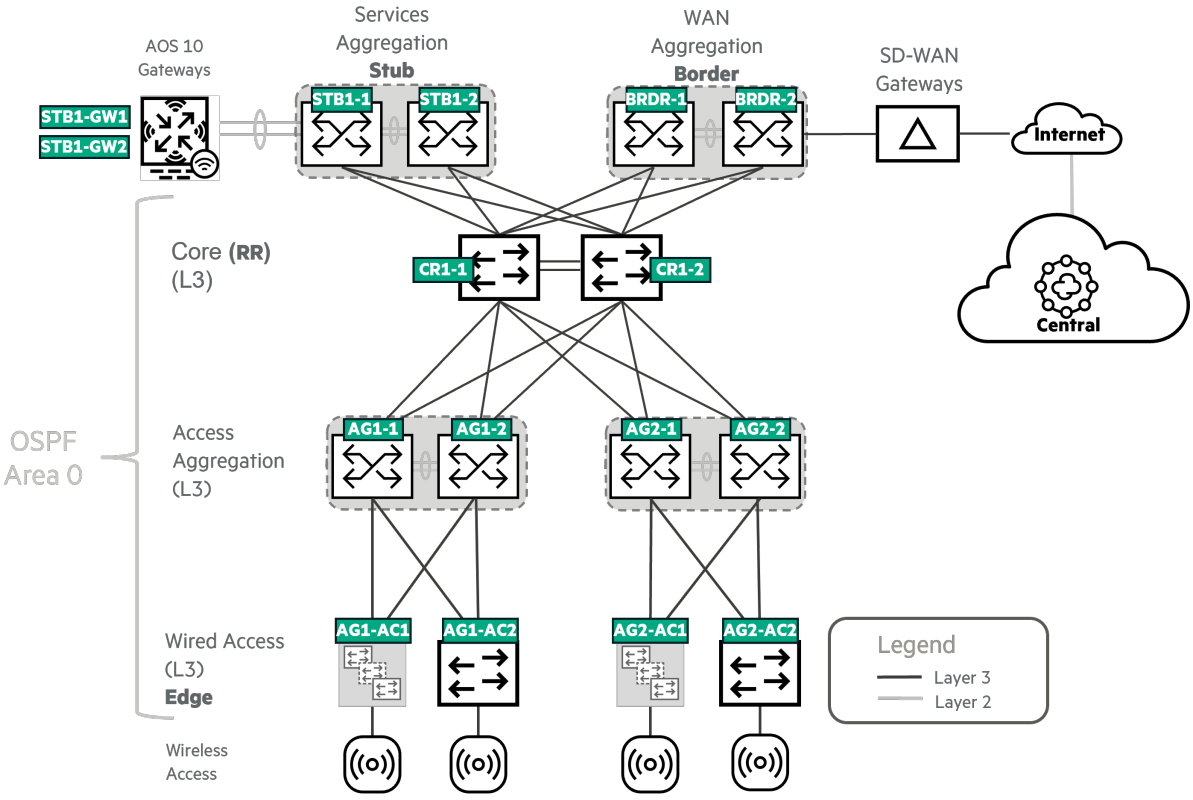
Some steps require manual CLI configuration of switches. Complete these steps using the MultiEdit feature of Central UI groups.

## Network Review

Best practice uses the NetConductor Underlay Orchestration workflow to create an OSPF underlay. After all requirements for the Fabric workflow are met, the EVPN-VXLAN overlay can be built.

Fabric deployment procedures assume that a large campus underlay was created using the Underlay Orchestration workflow. If the campus was deployed using the VSG Campus Wired Connectivity procedures, review the brownfield migration considerations.

The following illustration shows a Layer 3 access configuration along with the fabric personas used during the EVPN configuration. Device fabric personas to be assigned are shown in **bold**. Access aggregation switches perform only underlay functions and do not have fabric personas.




The Herndon site is summarized as 10.10.0.0/20.

The following table lists the IP subnets of the underlay networks.

| Description | IP Subnet |
|---|---|
| Routed Interface IP Pool | 10.10.0.0/24 |
| Loopback IP Pool | 10.10.1.0/24 |
| Gateway Underlay IP Space | 10.10.9.0/28 |

The following table lists the IP subnets used to deploy the distributed overlay. Best practice is to segment wired and wireless traffic into separate networks and segment the gateways and APs to isolate AP broadcast traffic.

| Description | VRF | VLAN | IP Subnet |
|---|---|---|---|
| Gateway Management | Infrastructure | 301 | 10.10.2.0/24 |
| UXI Sensor Management | Infrastructure | 302 | 10.10.3.0/24 |
| AP Management | Infrastructure | 303 | 10.10.4.0/24 |
| Overlay Fabric Wired | Corporate | 100 | 10.10.5.0/24 |
| Overlay Fabric Wireless | Corporate | 102 | 10.10.6.0/24 |
| Overlay Fabric Wired - Guest | Guest | 200 | 10.10.7.0/24 |
| Overlay Fabric Wireless - Guest | Guest | 201 | 10.10.8.0/24 |

**NOTE:**

Limit each AP management segment to a maximum of 500 APs. Deploy additional segments as necessary to accommodate larger AP deployments.

## DHCP Considerations

Ensure that DHCP scopes exist for the above subnets. A scope must be created for VTEP loopbacks and excluded from DHCP allocation. This is required for most DHCP servers to accept the DHCP Discovery. The DHCP must be configured to accept option 82. If the DHCP server is not configured to accept option 82, when it receives requests containing option 82 information, it cannot use the information to set parameters and it cannot echo the information in its response message. Older servers, such as Windows 2008, may not support option 82.

**NOTE:**

In the fabric wizard, changing the **DHCP Server VRF** to any VRF other than default results in the creation of additional loopbacks with the same IP address as loopback 1 in a selected VRF.

## Device Onboarding Considerations

An out-of-band management network for infrastructure devices is recommended when possible, but not required. In this procedure, the switches are managed out-of-band, but the APs, Gateways, and UXI sensors are managed in-band.

Gateways use an underlay interface for initial communication with Central, and are then migrated to an overlay interface for communication and tunneling with the access points. Access points and UXI sensors are managed in the overlay.

When devices are managed in-band, various levels of infrastructure must be configured so the device is reachable. For the access points and UXI sensors, the fabric must be fully provisioned and the border handoff must be configured to extend reachability for the overlay networks. Because the gateways are initially managed in the underlay, they are reachable as long as the underlay is fully configured and extended via the border handoff.

## Configure Role Policy

**NOTE:**

Customers must contact their Aruba Account Manager for addition to the allow-list for the Global Policy Manager feature.

Roles and role policies are provisioned at a global level and apply to all fabrics. This procedure uses two sample roles:

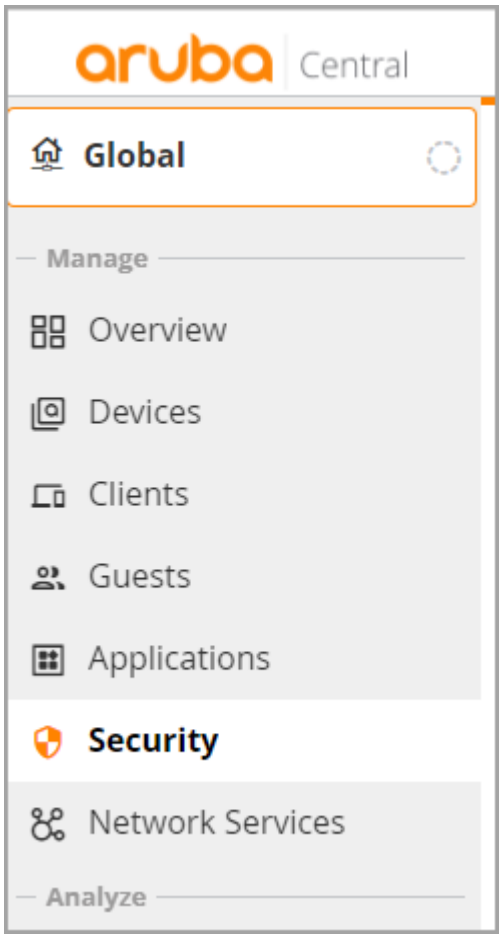
- EMPLOYEE
- CONTRACTOR

The following example role-to-role policy prevents employees and contractors from communicating.

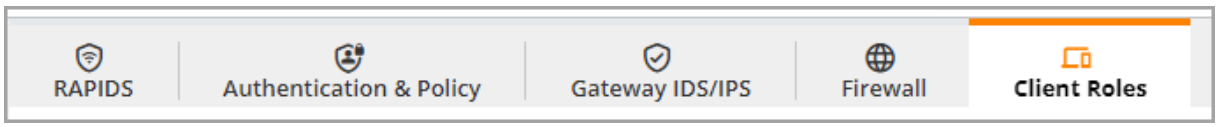
### Create Roles

Use this procedure to create the EMPLOYEE and CONTRACTOR roles:

**Step 1** In the filter dropdown, select **Global**, if it is not already selected. On the left menu, select **Security**.




**Step 2** Click the **Client Roles** tab.



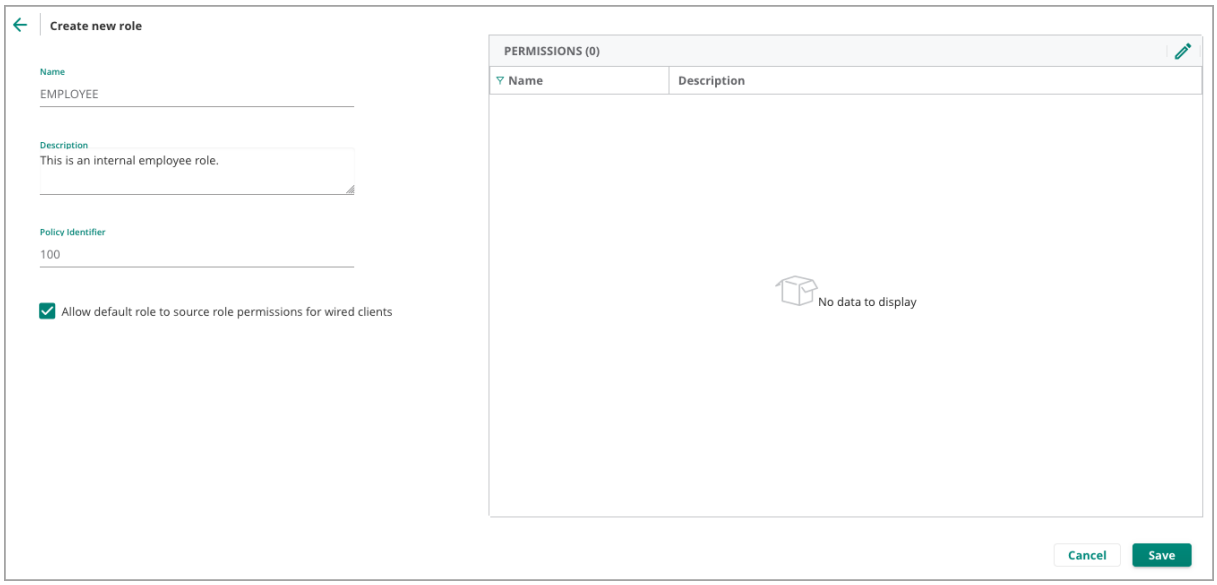

**Step 3** Create a new role by clicking the **+** (plus sign) in the upper right corner of the table.


**Step 4** In the **Create new role** window, assign the following settings, then click **Save**.

- **Name** : *EMPLOYEE*
- **Description**: *<insert optional role description>*
- **Policy Identifier**: *<use default value>*
- **Allow default role to source role permissions for wired clients:** *<selected>*

**NOTE:**

The **Allow default role to source role permissions for wired clients** option creates policy rules that allow clients assigned the role to send and receive ARP packets and traffic from outside the fabric.

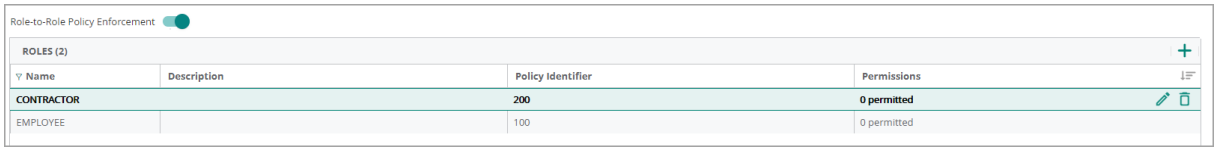



**Step 5** Repeat steps 3 and 4 to create the **CONTRACTOR** role and enter an optional description.


## Define Role-to-Role Policy

Use this procedure to create a policy to prevent the EMPLOYEE and CONTRACTOR roles from communicating.

**Step 1** Mouse-over the CONTRACTOR row and click the **edit** icon (pencil) on the right.

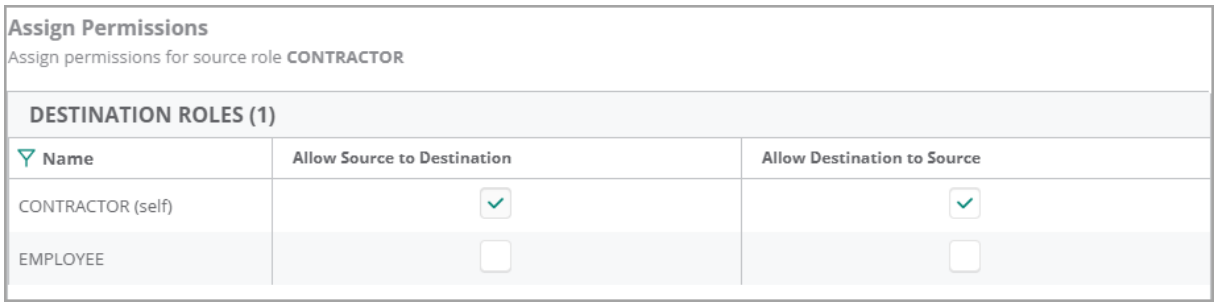



**Step 2** In the **PERMISSIONS** edit window for the CONTRACTOR role, click the **edit** icon (pencil) at the top right. The **Assign Permissions** window appears.


**Step 3** In the **Assign Permissions** window, assign the following settings and click **Save**.

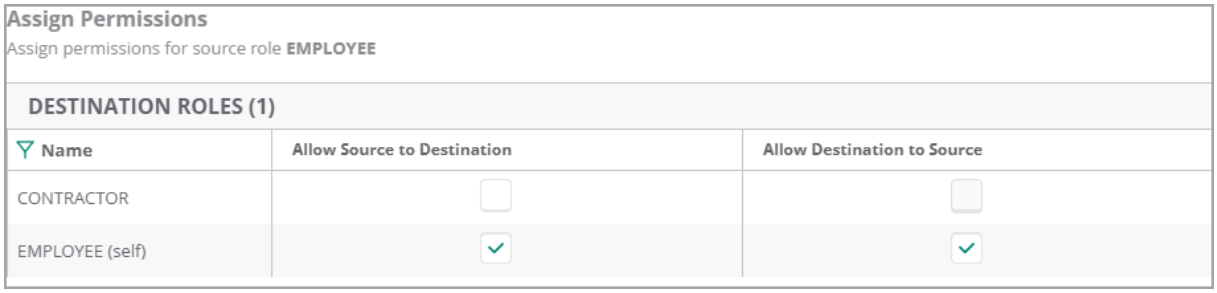
- CONTRACTOR (self):
  - **Allow Source to Destination:** *checked*
  - **Allow Destination to Source:** *checked*
- EMPLOYEE:
  - **Allow Source to Destination:** *unchecked*

- **Allow Destination to Source:** *unchecked*




**Step 4** Repeat steps 1 to 3 for the EMPLOYEE role using the following settings.

- CONTRACTOR
  - **Allow Source to Destination:** *unchecked*
  - **Allow Destination to Source:** *unchecked*
- EMPLOYEE (self):
  - **Allow Source to Destination:** *checked*
  - **Allow Destination to Source:** *checked*




# Deploy the Fabric

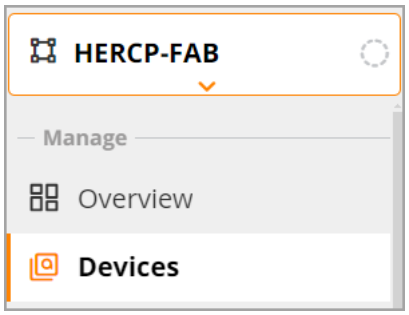
Use the fabric wizard to deploy an overlay fabric. Follow the procedures below to provision the VXLAN interfaces, EVPN control plane, VRFs, fabric VLANs, and Anycast Gateways.

**NOTE:**

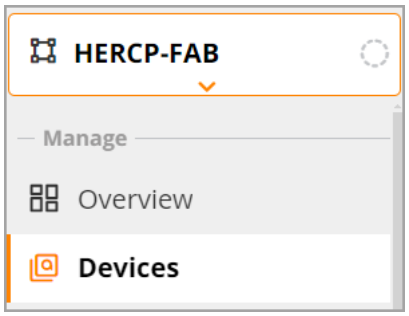
All Aruba CX switches included in the fabric must be in the same Central UI group and have advanced licenses.

## Create The Fabric

**Step 1** In the **Global** dropdown, select the switch group. In this example, the group is **HERCP-FAB.**

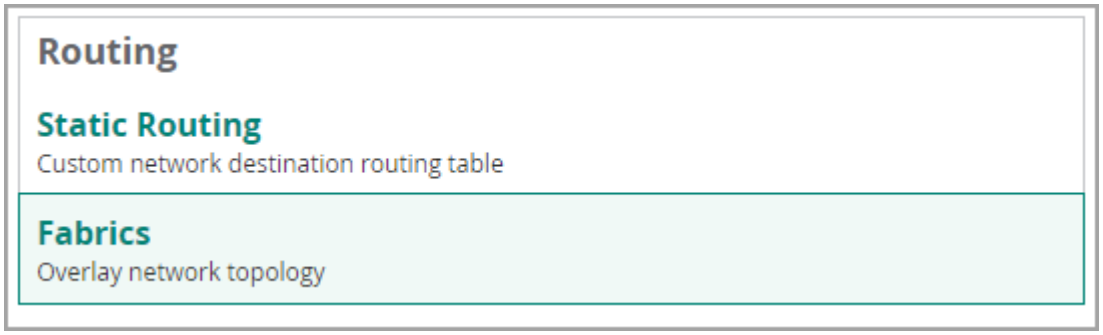



**Step 2** On the left menu, select **Devices**.




**Step 3** Select **Switches**, then select **Config**.


**Step 4** Under **Routing**, select **Fabrics.**

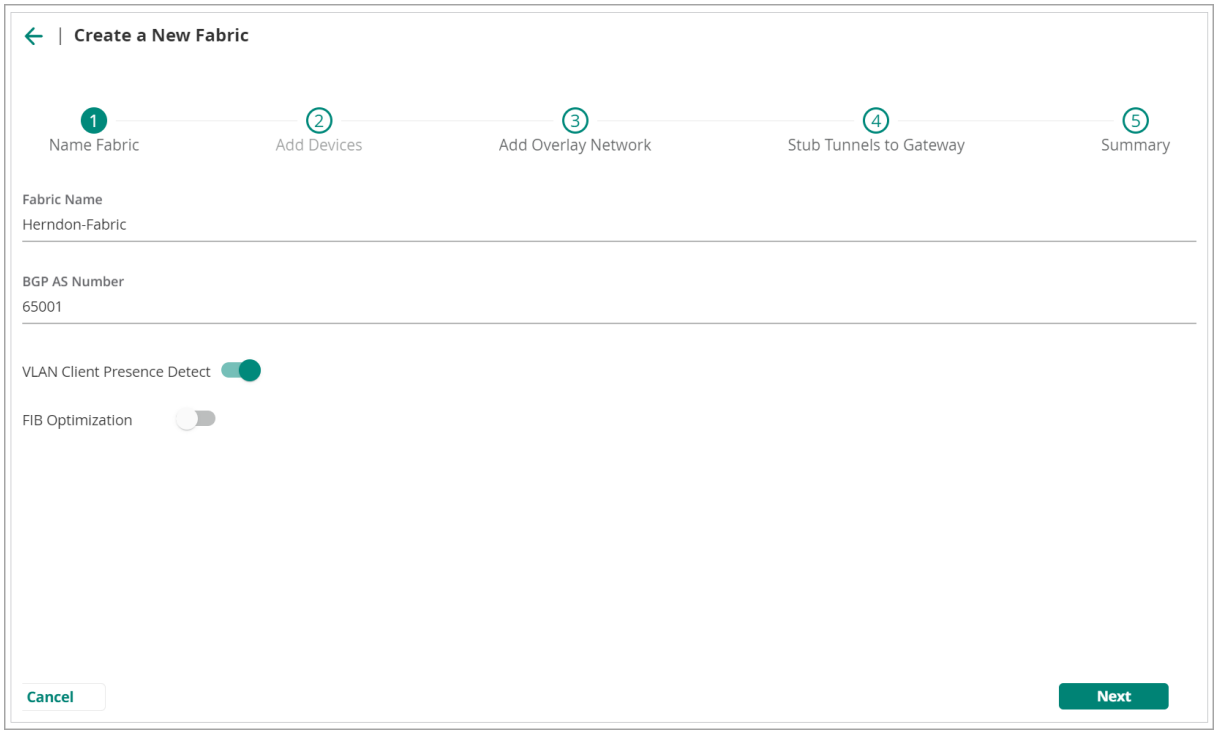



**Step 5** On the **Fabrics** table, click the **+** (plus sign) at the top right.


**Step 6** In the **Create a New Fabric** workflow, click **Name Fabric**, assign the following settings, and click **Next**.

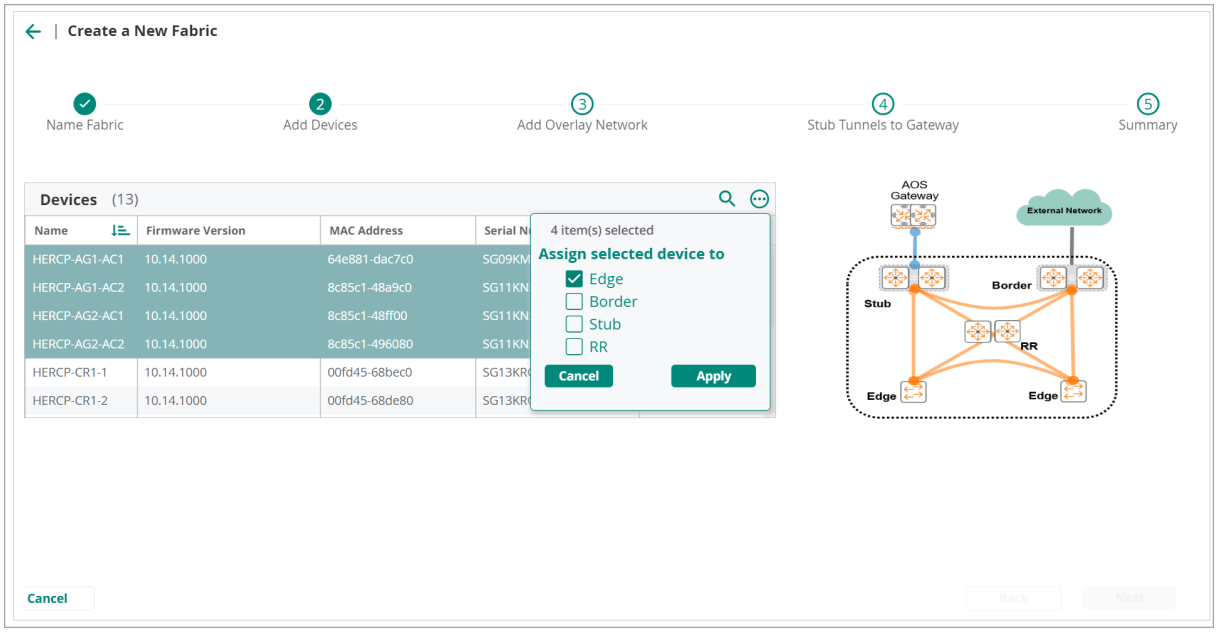
- **Fabric Name:** *Herndon-Fabric*
- **BGP AS Number:** *Use default*
- **VLAN Client Presence Detect:** *Enabled*

- **FIB Optimization:** *Disabled*




Enabling **VLAN Client Presence Detect** is recommended to provide increased scalability by avoiding flooding BUM traffic to VTEPs when a client is not detected for a given VLAN. Disabling **FIB Optimization** is recommended because it can affect the control plane based on traffic patterns.

**Step 7** On the **Add Devices** page, select each access switch and use the **Assign selected devices to** window to assign the **Edge** persona. Click **Apply**.




**Step 8** Repeat steps 6 and 7 for the **RR**, **Border**, and **Stub** device personas, then click **Next**.

| Device | Persona |
|---|---|
| HERCP-CR1-1 | RR |
| HERCP-CR1-2 | RR |
| HERCP-CR1-STB1-1 | Stub |
| HERCP-CR1-STB1-2 | Stub |
| HERCP-CR1-BRDR1-1 | Border |
| HERCP-CR1-BRDR1-2 | Border |
| HERCP-AG1-AC1 | Edge |
| HERCP-AG1-AC2 | Edge |
| HERCP-AG2-AC1 | Edge |
| HERCP-AG2-AC2 | Edge |

**NOTE:**

You must click **Apply** after each persona selection to save the assignment.

**NOTE:**

Because aggregation switches are underlay devices, they are not assigned personas.

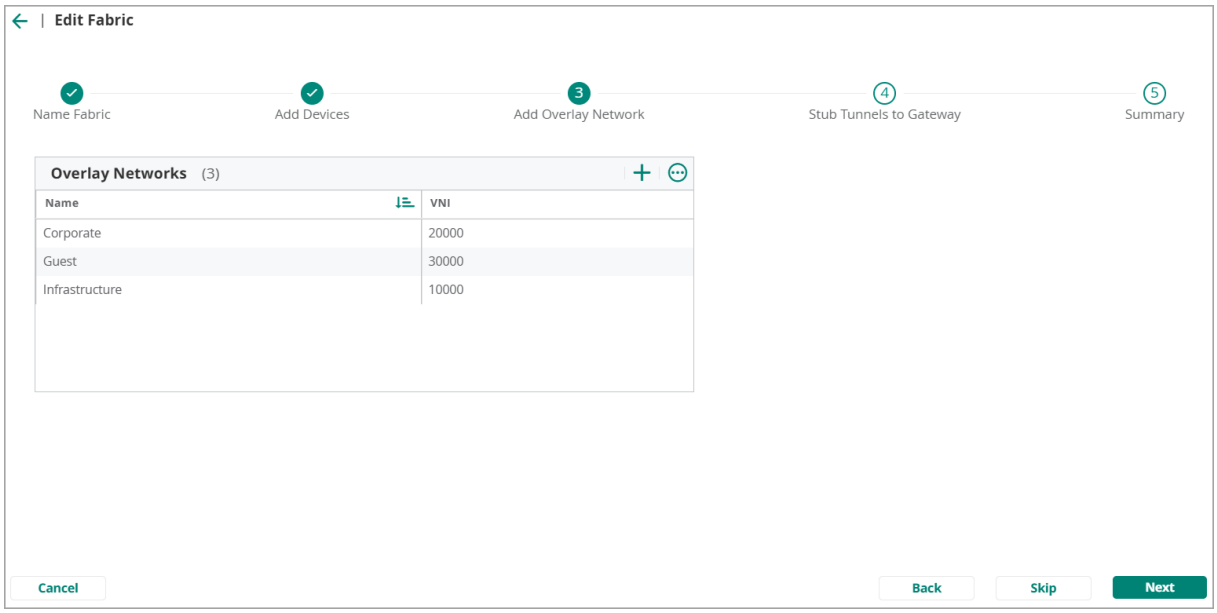
**Step 9** On the **Add Overlay Network** click the **+** (plus sign) at the top right.

**Step 10** Assign the following **Overlay Network** settings: * **Name:** *Infrastructure* * **VNI:** *10000*

**Step 11** Repeat step 9 and 10 for the **Guest** and **Infrastructure** networks.

**NOTE:**

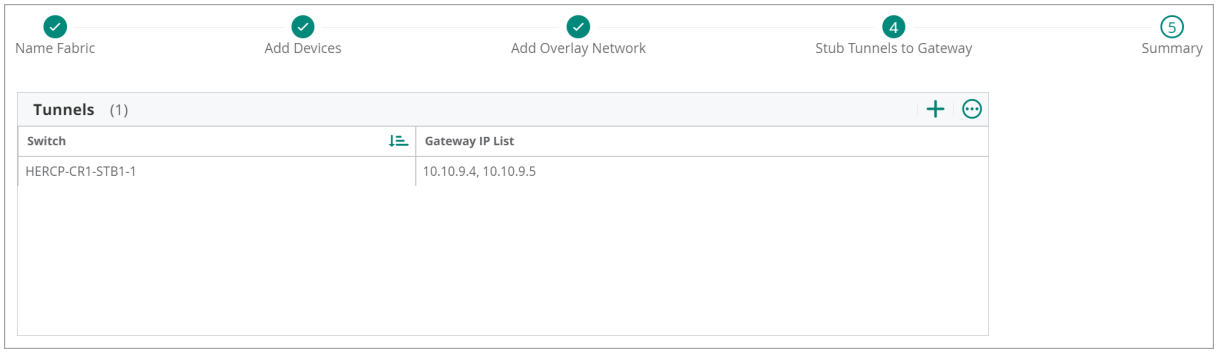
Rename or delete the default **overlay_network**.




**Step 12** On the **Stub Tunnels to Gateway** page, click the **+** (plus sign) at the top right of the table.

**Step 13** In the **Tunnels** table, assign the following settings. Click outside the new row to continue.

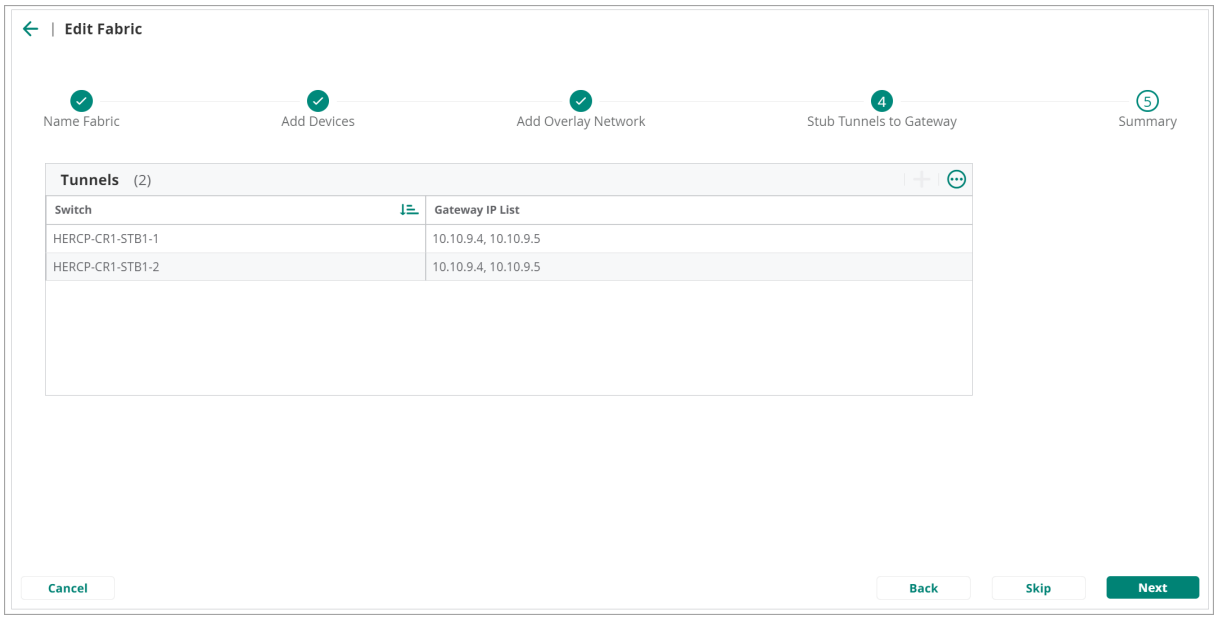
- **Switch:** *HERCP-CR1-STB-1*
- **Gateway List IP:** *10.10.9.4, 10.10.9.5*



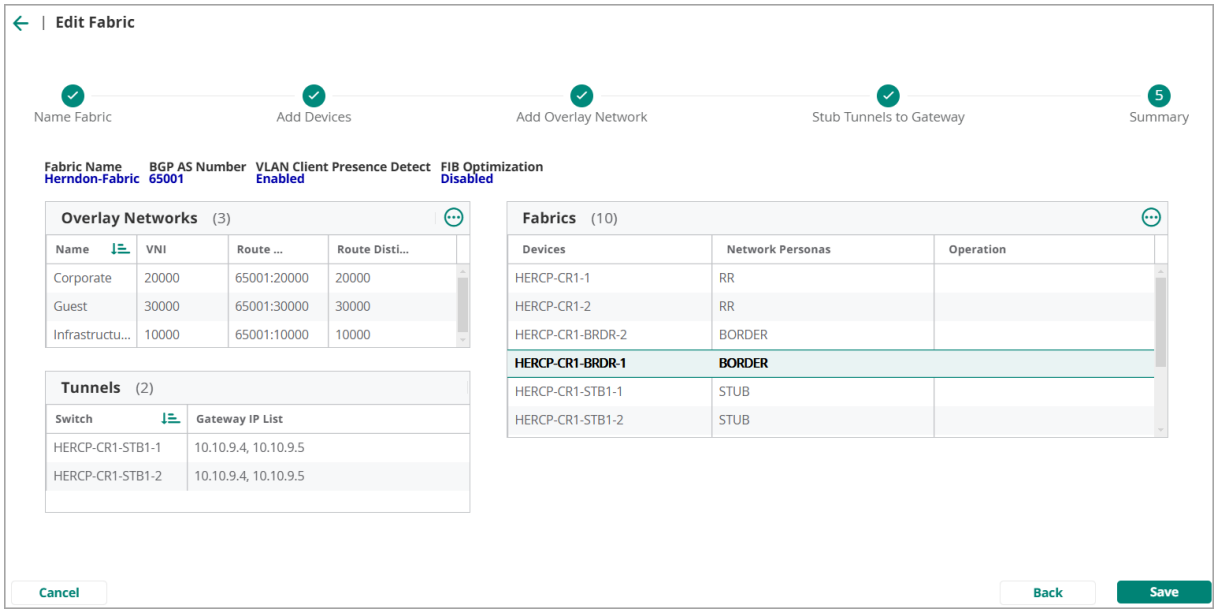

**NOTE:**

Gateway IPs must match the VXLAN Tunnel Source configured on the AOS-10 Gateways, configured later in this procedure.

**Step 14** Repeat steps 10 and 11 for additional stub switches. Click **Next**.




**Step 15** Review the **Summary** page for accuracy. Return to previous pages and make corrections, if needed. Click **Save**.



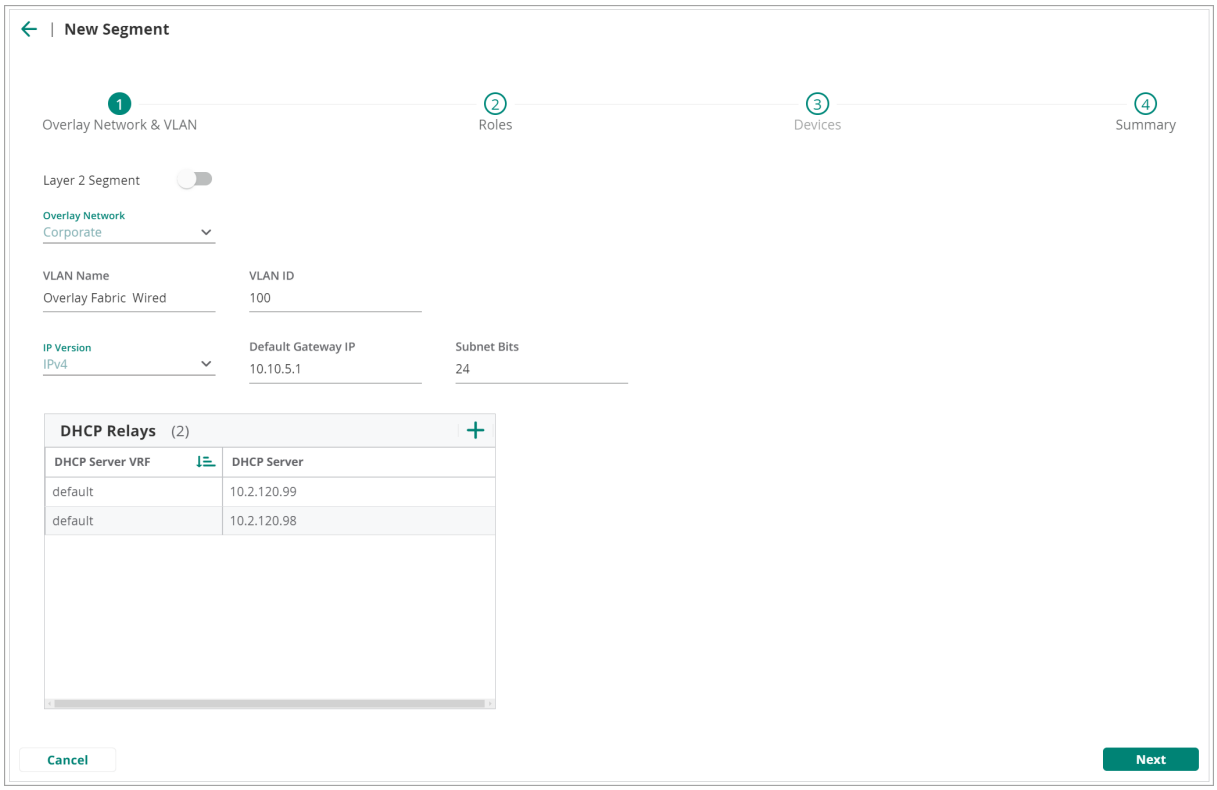

## Create the Fabric Segments

Follow these steps to create segments within the fabric.

**Step 1** Expand the **Herndon-Fabric**, then click the **New Segment** icon. 


**Step 1** On the **Overlay Network & VLAN** page of the **New Segment** workflow, assign the following settings using the **+** (plus sign) to add DHCP servers, and click **Next**.

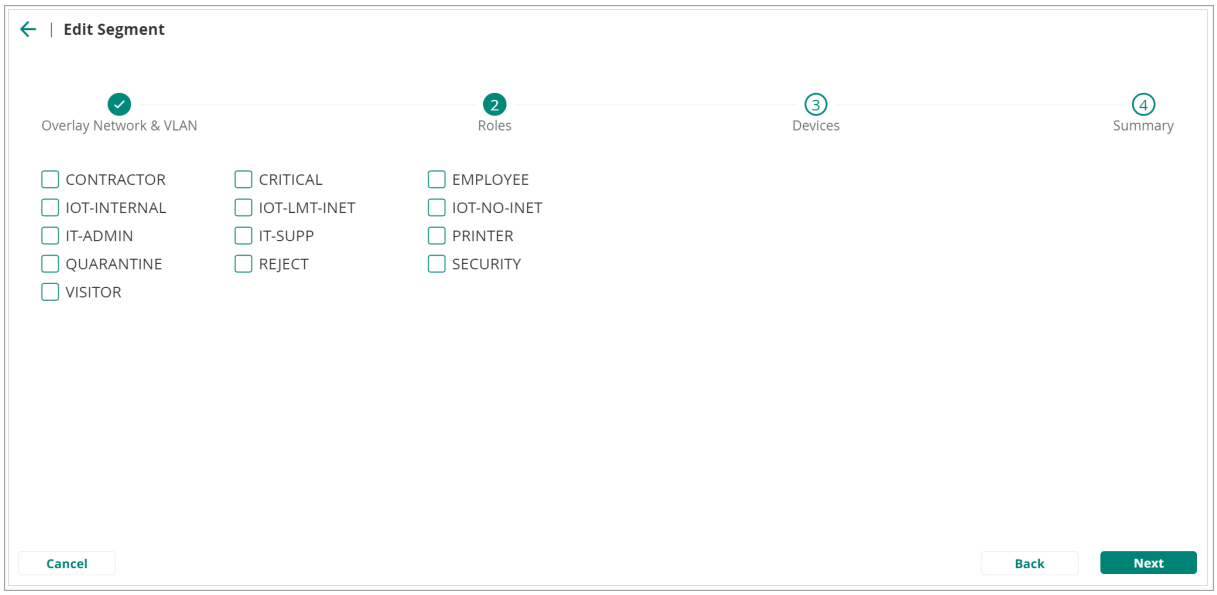
- **Overlay Network**: *Corporate*
- **VLAN Name**: *Overlay Fabric Wired*
- **VLAN ID**: *100*
- **Default Gateway IP**: *10.10.5.1*
- **IPv4 Version**: *IPv4*
- **Subnet Mask**: *24*
- **DHCP Server**: *10.2.120.98, 10.2.120.99*
- **DHCP Server VRF:** *default*



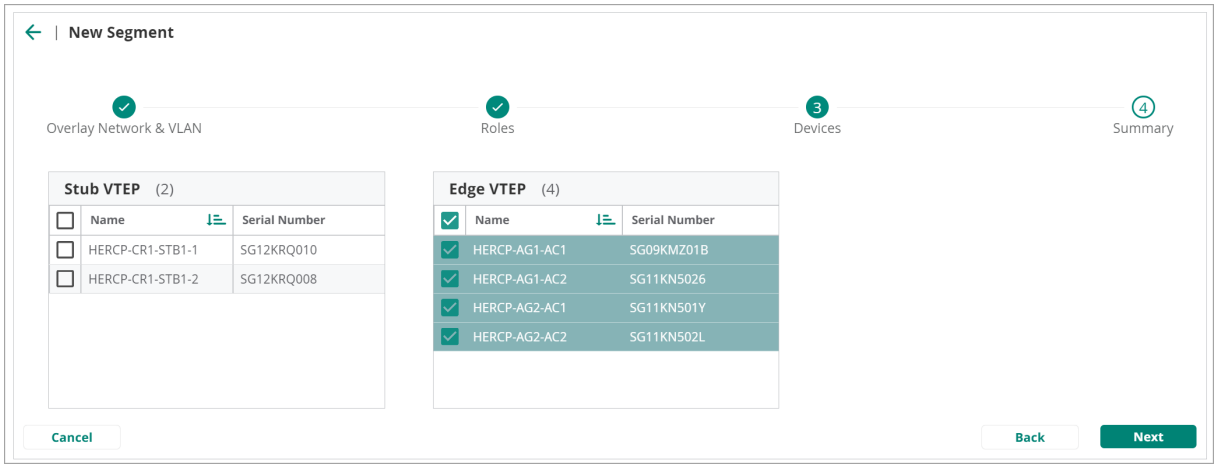

**Step 3** Skip the role mapping page by clicking **Next**.

**NOTE:**

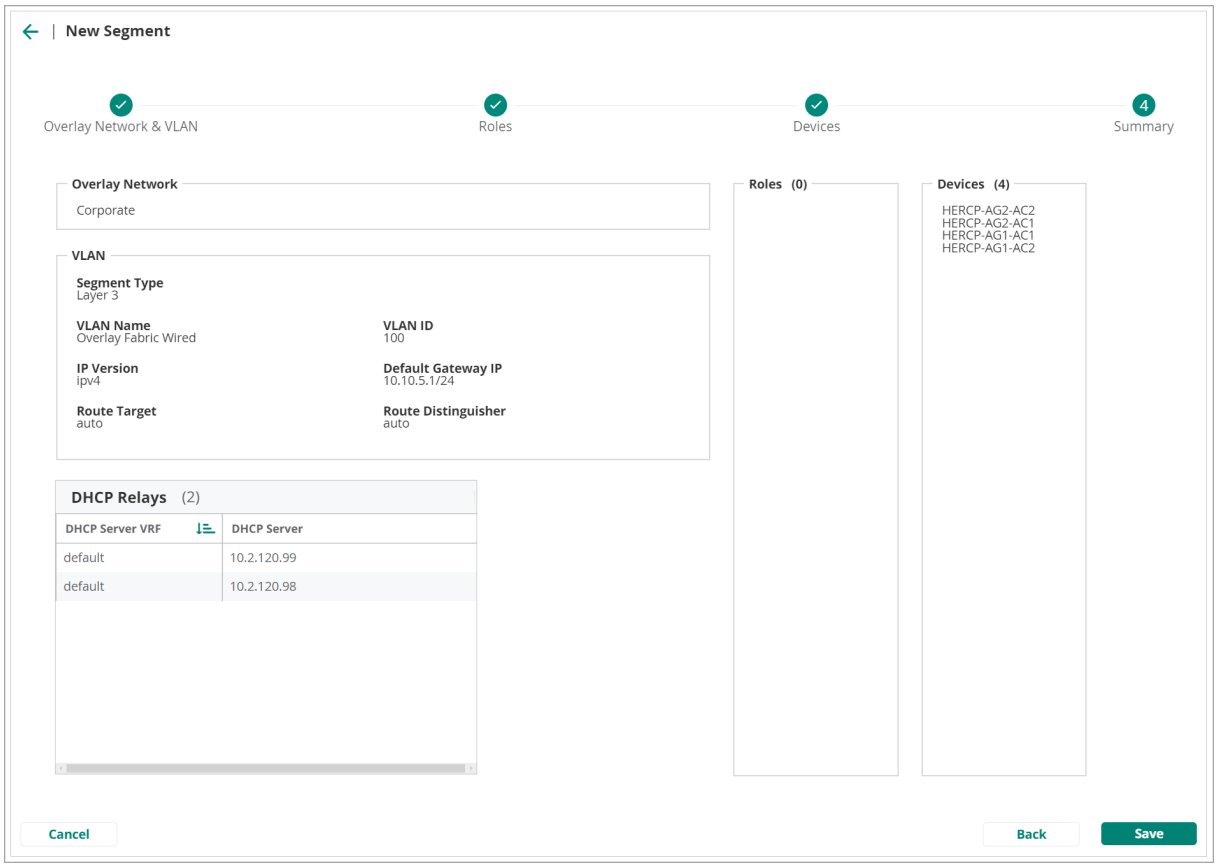
It is recommended **not** to map roles to segments at this stage. Instead, use the NAC server to assign both the VLAN and Role, which is specified in the RADIUS response during device authentication.




**Step 4** On the **Devices** page, select the **Edge** devices, then click **Next**.

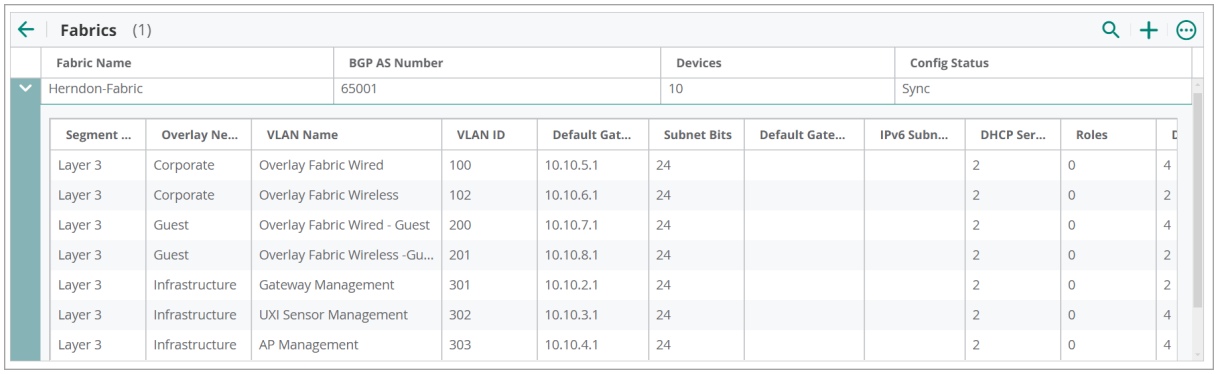



**Step 5** Review the **Summary** page for accuracy, then click **Save**.




**Step 6** Repeat the step above until all segments are created.

| **VLAN Name** | Overlay Network | VLAN ID | **IP Subnet** | Apply to Devices |
|---|---|---|---|---|
| UXI Sensor Management | Infrastructure | 302 | 10.10.3.0/24 | Edge VTEPs |
| AP Management | Infrastructure | 303 | 10.10.4.0/24 | Edge VTEPs |
| Overlay Fabric Wireless | Corporate | 102 | 10.10.6.0/24 | Stub VTEPs |
| Overlay Fabric Wired - Guest | Guest | 200 | 10.10.7.0/24 | Edge VTEPs |
| Overlay Fabric Wireless -Guest | Guest | 201 | 10.10.8.0/24 | Stub VTEPs |



# Configure Wireless Integration

This procedure assumes that the AOS-10 Gateway has been configured according to the **Campus Gateway Deploy Guide**. The following VLANs are required:

- **VLAN 15**: Underlay VLAN
- **VLAN 301**: Gateway Management
- **VLAN 102**: Overlay Fabric Wireless
- **VLAN 201**: Overlay Fabric Wireless Guest

**VLAN 15** serves as both the underlay VLAN and the source for the static VXLAN tunnel. **VLAN 301** is dedicated to managing the gateway. **VLAN 15** and **VLAN 301** are trunked to the stub switches. **VLAN 102** and **VLAN 201** are SSID VLANs used for client access, and they extend over the static VXLAN tunnel.

Wireless gateways establish static VXLAN tunnels with the stub switch. This enables connectivity within the fabric and maps VLANs to VNIs. This procedure enables jumbo frames on gateway interfaces and configures the static VXLAN tunnels.

Additionally, the **System IP,** used for establishing GRE tunnels with access points, will be migrated from the underlay **VLAN 15** to the overlay **VLAN 301**.

Before proceeding, ensure that the following are configured on the stub switch.

- The IP MTU is set on the VLAN interface.
- The MTU is configured on the LAG members of the stub switch.

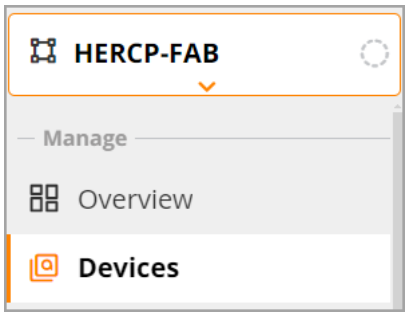
The configuration shown below represents the initial setup on the stub switches at the start of this procedure.

```
interface vlan 15
    description UNDERLAY BETWEEN GATEWAY AND STUB
    ip mtu 9198
    ip address 10.10.0.66/28
    active-gateway ip mac a2:01:00:a2:a2:a2
    active-gateway ip 10.10.0.65
interface lag 11 multi-chassis
    description Stub-GW-1
    no shutdown
    no routing
    vlan trunk native 15
    vlan trunk allowed 1,15
    lacp mode active
    lacp fallback
    exit
interface lag 12 multi-chassis
    description Stub-GW-2
    no shutdown
    no routing
    vlan trunk native 15
    vlan trunk allowed 1,15
    lacp mode active
    lacp fallback
    exit
interface 1/1/5
    description HERCP-GW
    mtu 9198
    no shutdown
    lag 11
interface 1/1/6
    description HERCP-GW
    mtu 9198
    no shutdown
    lag 12
```

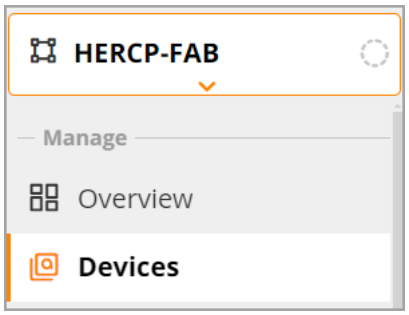
## Configure Gateway Overlay

In this procedure, VLAN 301, designated as the gateway management VLAN, is manually created to prevent the unintended configuration changes that would be applied by the Fabric Wizard. The Fabric Wizard is not used for this segment, as it pushes configurations that are not required for gateway management. Additionally, VLAN 301 is added to the LAG interfaces connecting the gateways to the border to ensure proper network segmentation and communication.

**Step 1** In the **Global** dropdown, select the switch group. In this procedure, the group is **HERCP-FAB.**




**Step 2** On the left menu, select **Devices**.

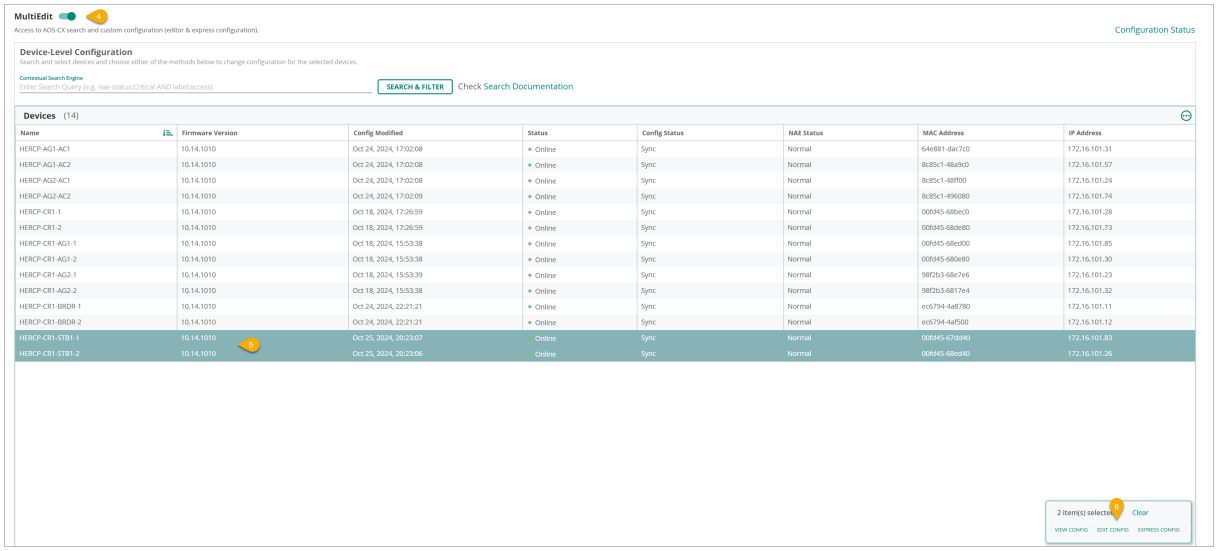



**Step 3** Select **Switches**, then select **Config**.


**Step 4** Enable the **MultiEdit** toggle.

**Step 5** Select the two stub switches.

**Step 6** Click **Edit Config**.




**Step 7** Enter the following configuration and click **Save**.

```
vlan 301
    name Gateway Management
interface lag 11 multi-chassis
    description Stub-GW-1
    vlan trunk allowed 1,15,301
    exit
interface lag 12 multi-chassis
    description Stub-GW-2
    vlan trunk allowed 1,15,301
    exit
interface vlan 301
    vrf attach Infrastructure
    ip mtu 9198
    ip address 10.10.2.1/24
    active-gateway ip mac 00:00:00:00:00:01
    active-gateway ip 10.10.2.1
```

**NOTE:**

Ensure that the fabric wireless VLANs (101,201) are **not** trunked in the underlay. Fabric wireless VLANs must be enabled only in the Static VXLAN tunnel to avoid loops in the network.

## Verify Jumbo Frames on the Gateway

This procedure details how to enable jumbo frames on the AOS-10 Gateways.

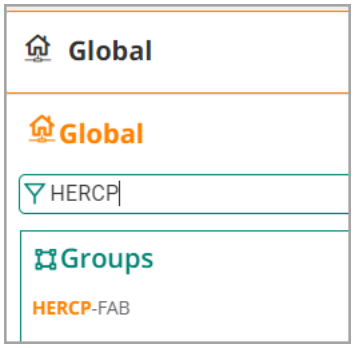
Refer to Configuring Wireless Group Settings to assist with enabling jumbo frame processing.

Refer to Configure Gateway VLANs to assist with verifying jumbo frames on the port channel.

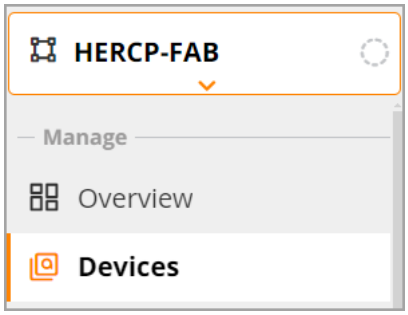
## Configure VLANs on Gateways

This step configures additional required VLANs for the NetConductor deployment.

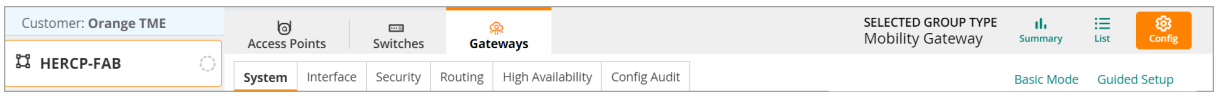
**Step 1** In the **Global** dropdown, select the switch group. In this example, the group is **HERCP-FAB**.



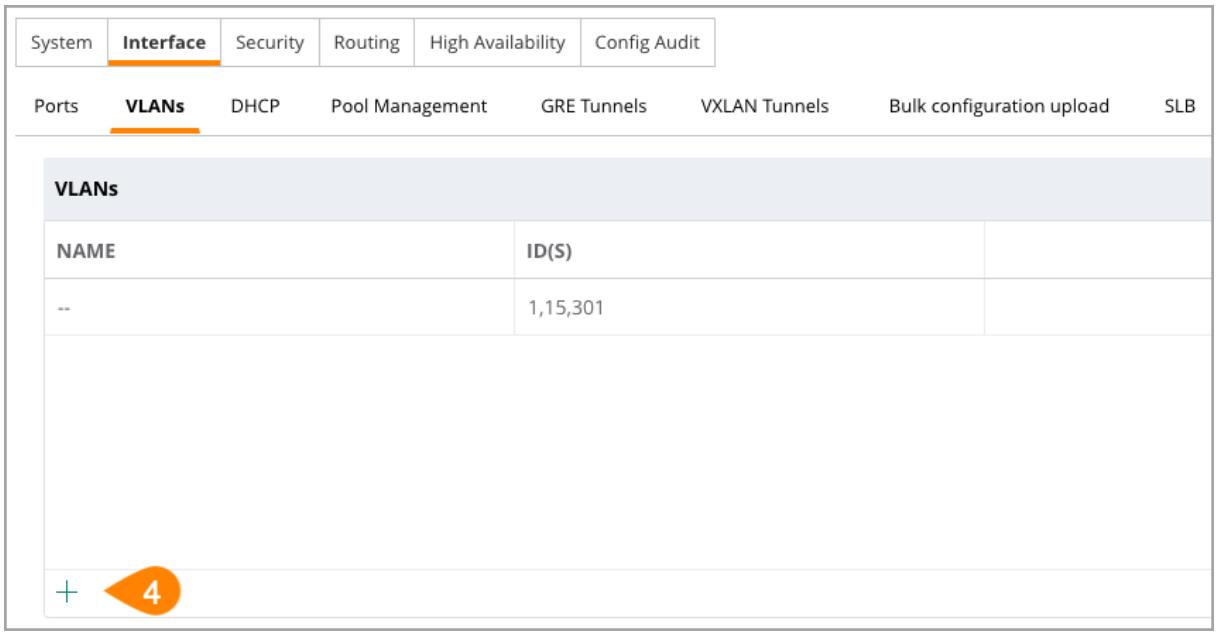

**Step 2** On the left menu, select **Devices**.



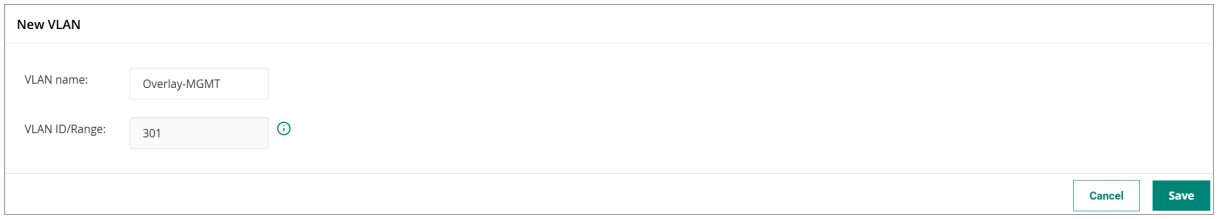

**Step 3** Select **Gateways**, then select **Config**.




**Step 4** Select the **Interface** tab and select **VLANs**. In the lower left, click the **+** (plus sign).




**Step 5** In the **New VLAN** window, assign the following settings, then click **Save Settings**. * **VLAN name:** *Overlay-MGMT* * **VLAN ID/Range:** *301*

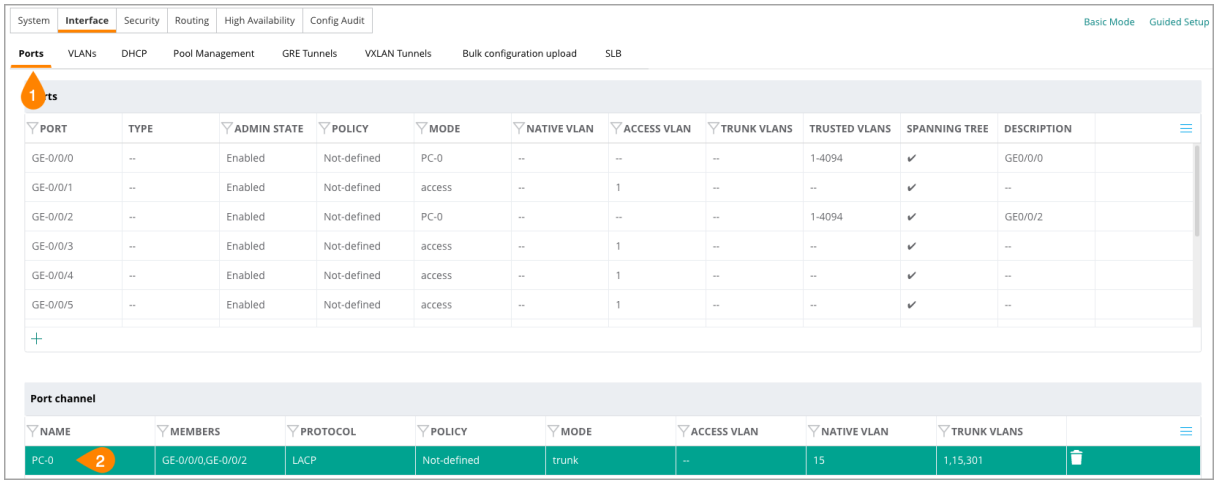



**Step 6** Repeat this procedure for **VLAN 102** (Overlay-Fabric-Wireless) and **VLAN 201** (Overlay-Fabric-Wireless-Guest).

## Modify Port Channel on Gateways

**Step 1** On the **Gateways** page, select the **Interface** tab, then the **Ports** tab.

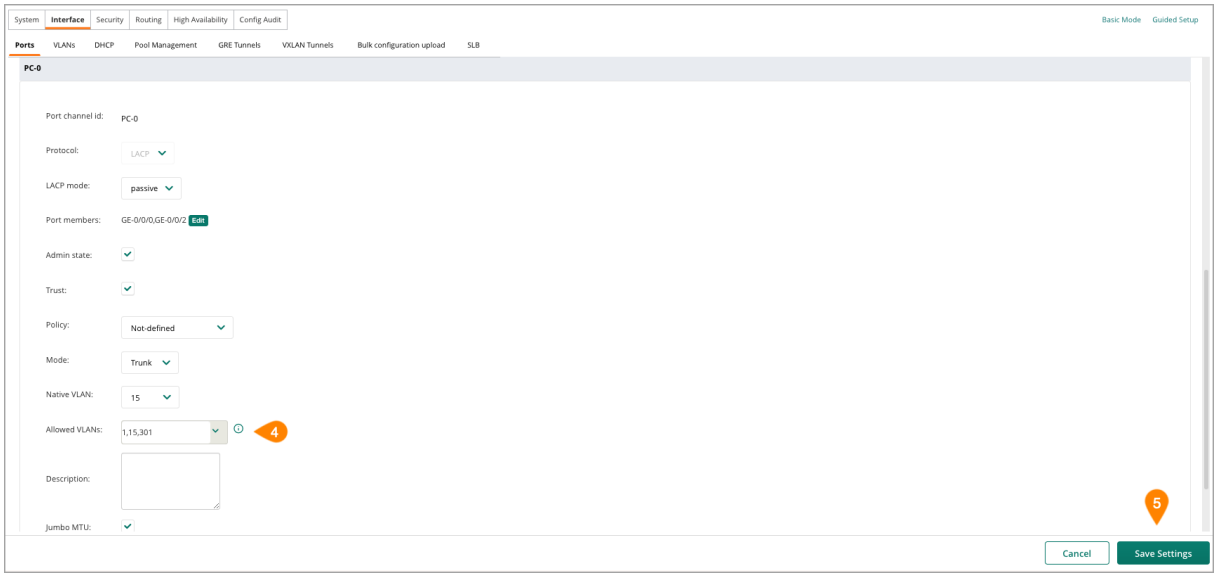
**Step 2** Select **PC-0**.




**Step 3** Scroll to the port-channel configuration.

**Step 4** From the dropdown, select **VLAN 301** to add it.

**Step 5** Click **Save Settings**.

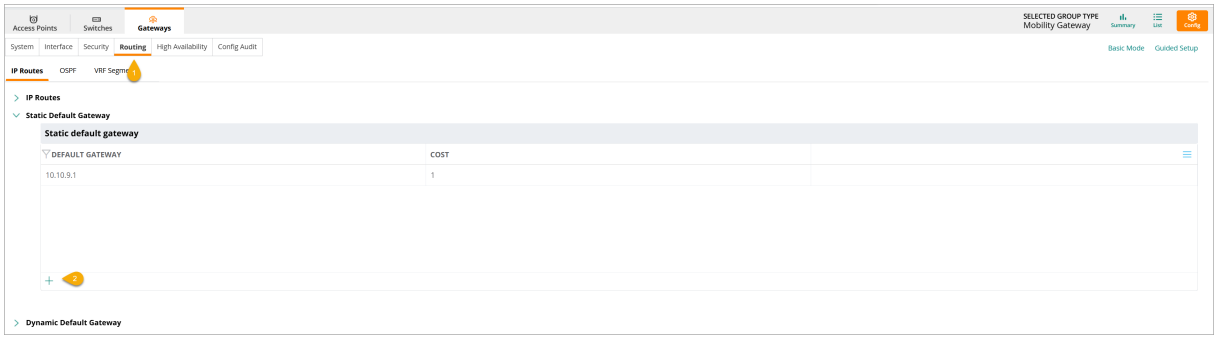



### Configure Static Routes

Use the following procedure to configure required routing on the gateway. A default route points to VLAN 301, which is in the fabric. A static route for the loopback IP space points to VLAN 15 and is used to establish the static VXLAN tunnel.

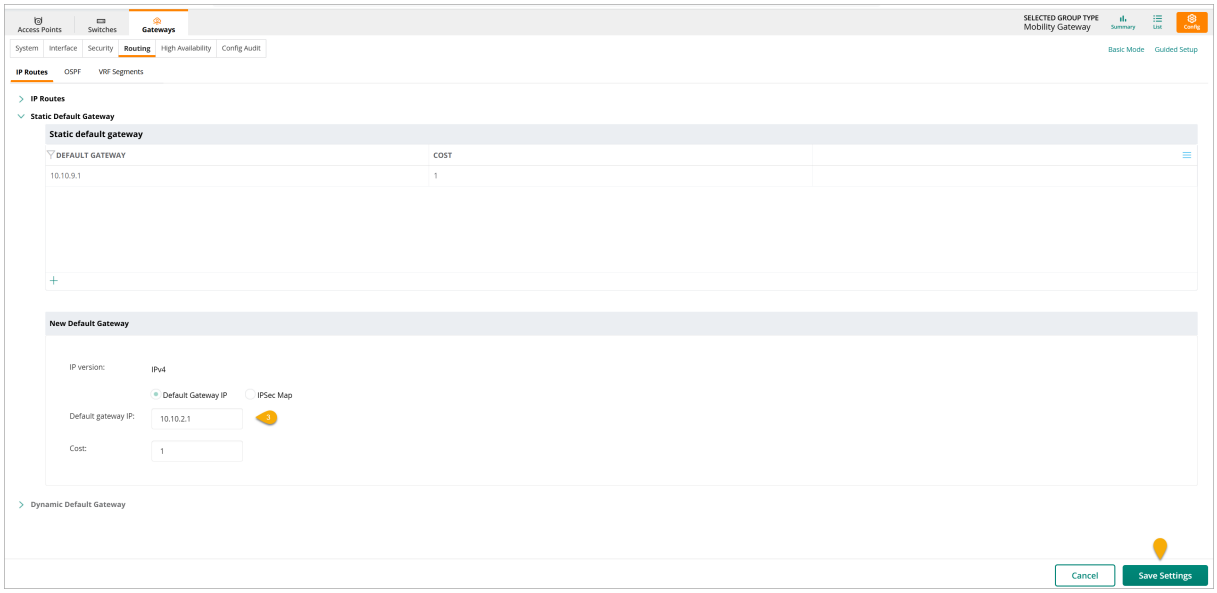
**Step 1** On the **Gateways** tab, select the **Routing** tab, then the **IP Routes** tab.

**Step 2** Expand the **Static Default Gateway** section. At the bottom of the table, click the **+** (plus sign).

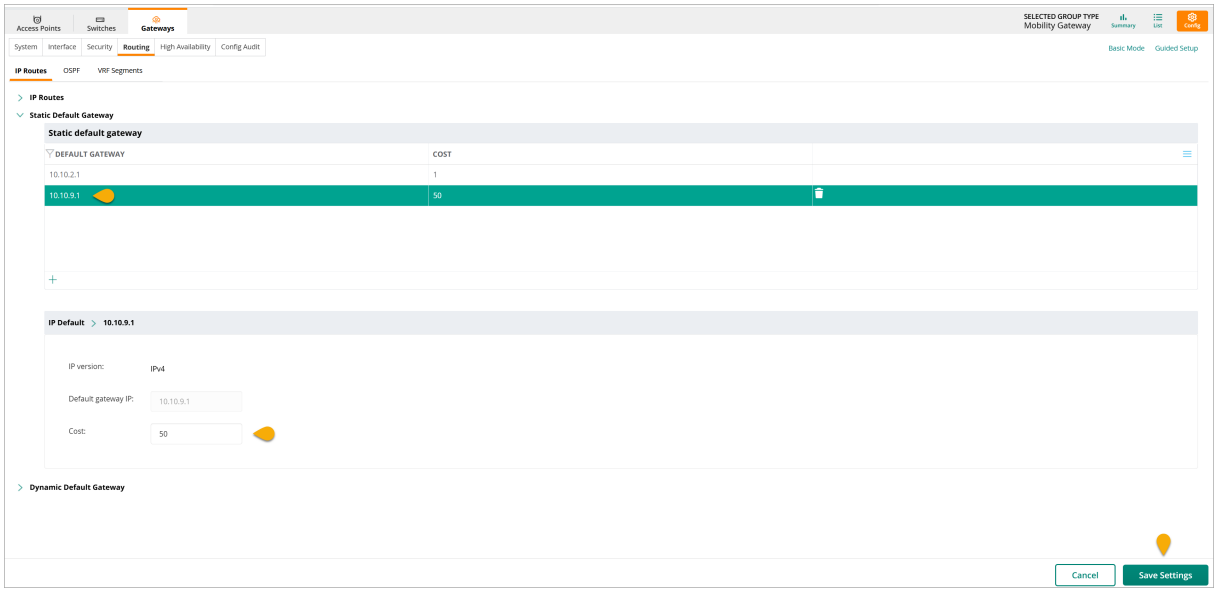



**Step 3** On the **New Default Gateway** page, enter the IP address, then click **Save Settings**.

- **Default Gateway IP**: *10.10.2.1*



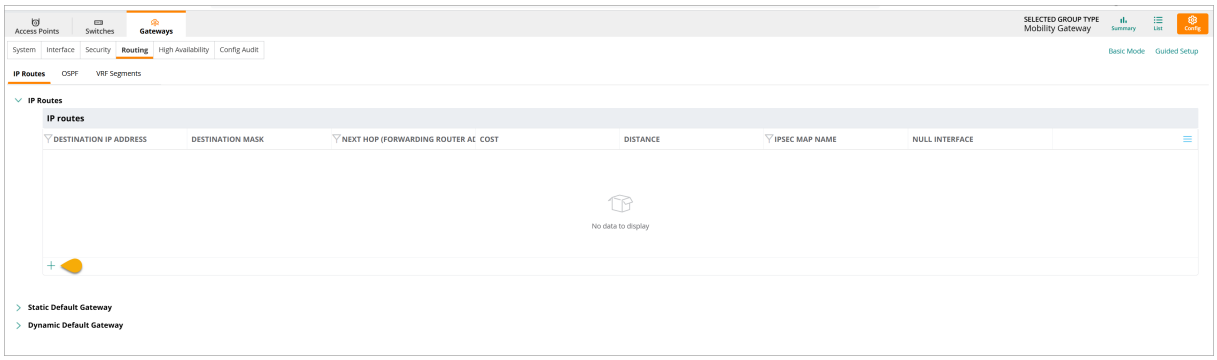

**Step 4** Select the original static default gateway and set the **Cost** to *50*, making this a backup route. Then click **Save Settings**.




**NOTE:**

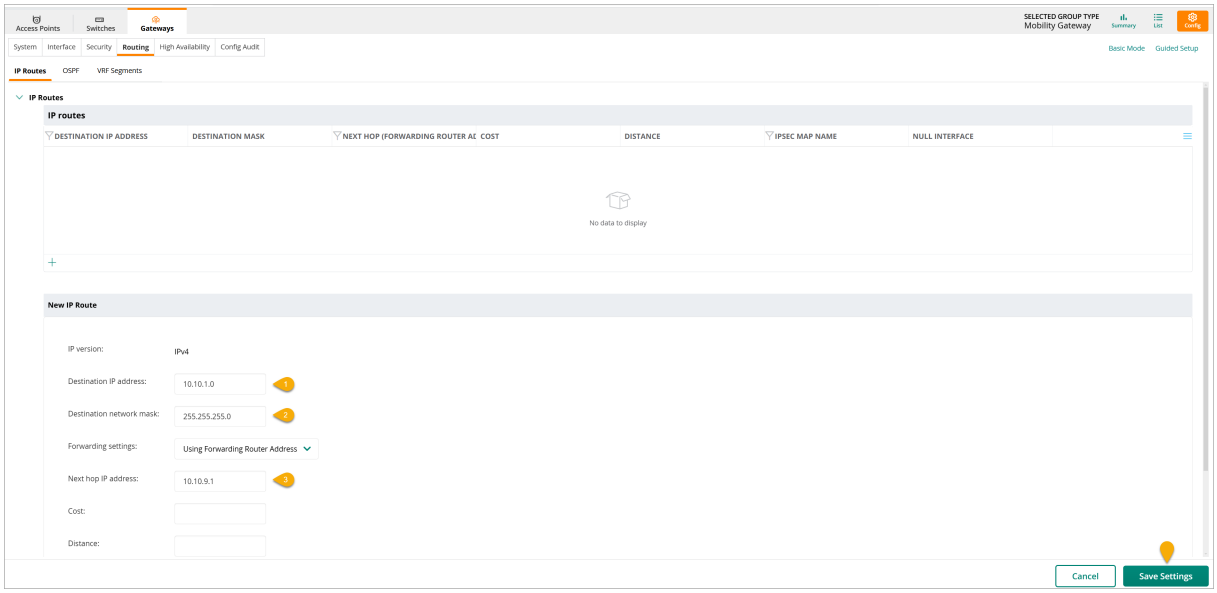
Verify there is no local override in any of the gateway device static default configurations. The local overrides may have been set during onboarding. Remove all static default gateway local overrides.

**Step 5** Expand the **IP Routes** section. At the bottom of the table, click the **+** (plus sign).




**Step 6** On the **New Default Gateway** page, assign the following settings, then click **Save Settings**. * **Destination IP Address:** *10.10.1.0*

- **Destination Network Mask:** *255.255.255.0*
- **Next hop IP Address:** *10.10.9.1*




## Modify System IP address

Use the following procedure to change the System IP address from VLAN 15 to VLAN 301 on each gateway at the device level. This is done to ensure the APs build their control and data plane connections in the overlay (VLAN 301) vs. the underlay (VLAN 15).

**NOTE:**

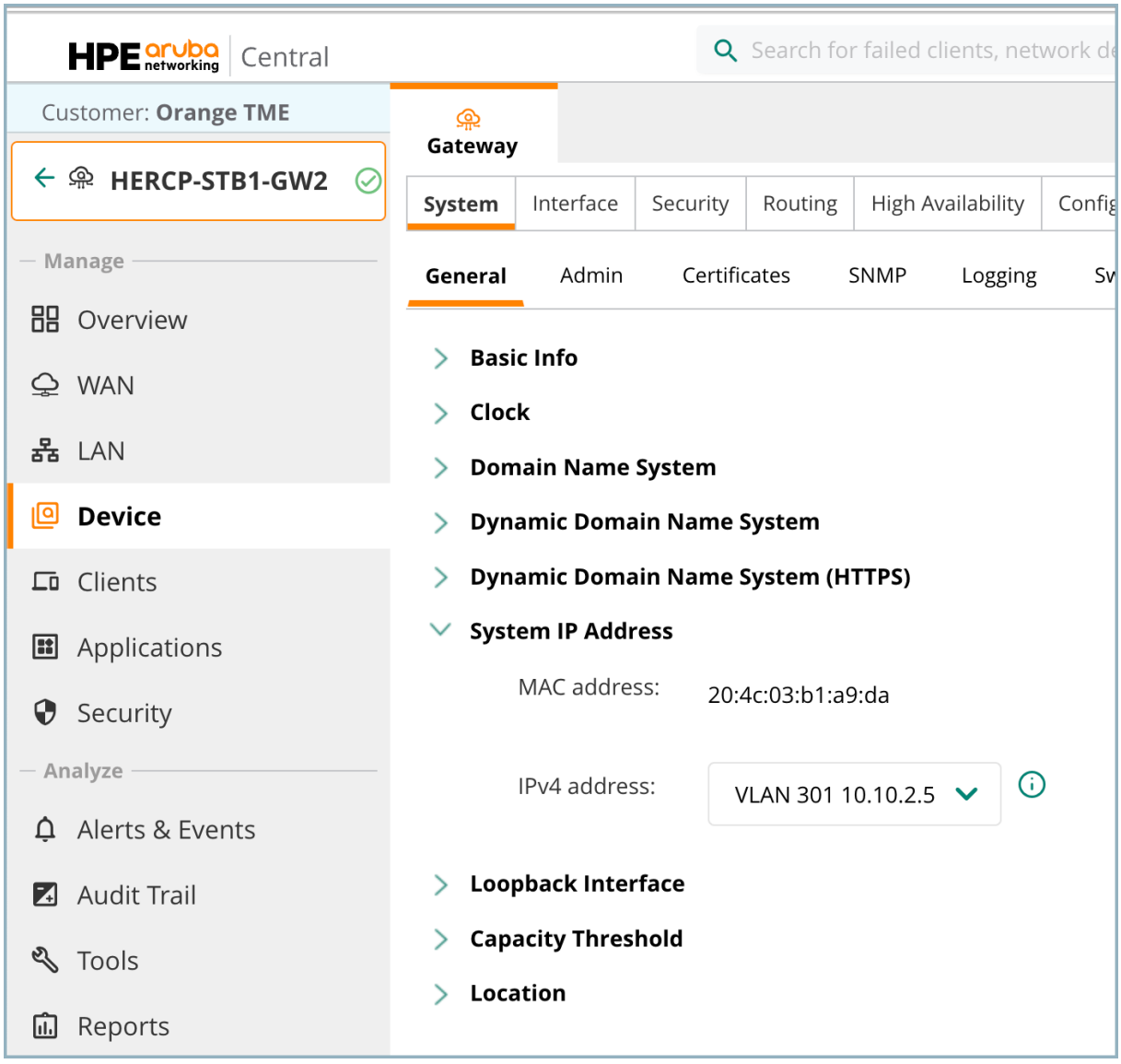
If the APs are being deployed in the underlay this step is not needed and the system IP should be kept to VLAN 15.

**Step 1** On the left menu, select Devices on menu bar, then select Gateways.

**Step 2** Select a gateway from the list.

**Step 3** On the **Gateway** page, select the **System** tab, then the **General** tab.

**Step 4** Expand the **System IP Address** section, use the **IPv4 address** dropdown to select VLAN 301, then click **Save**.

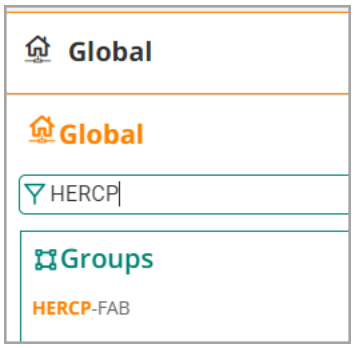



**Step 5** Repeat steps 1-4 on the other gateways.

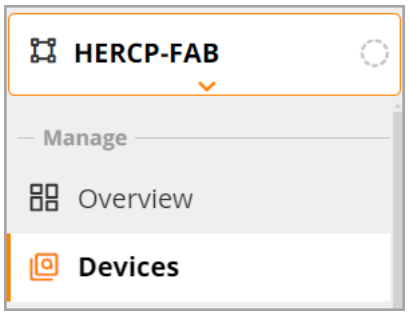
## Configure Static VXLAN Tunnel

Use the following procedure to configure static VXLAN tunnels between the gateways and stub switches:

**Step 1** In the **Global** dropdown, select the switch group. In this example, the group is **HERCP-FAB**.

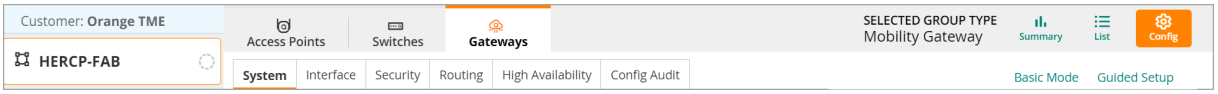



**Step 2** On the left menu, select **Devices**.

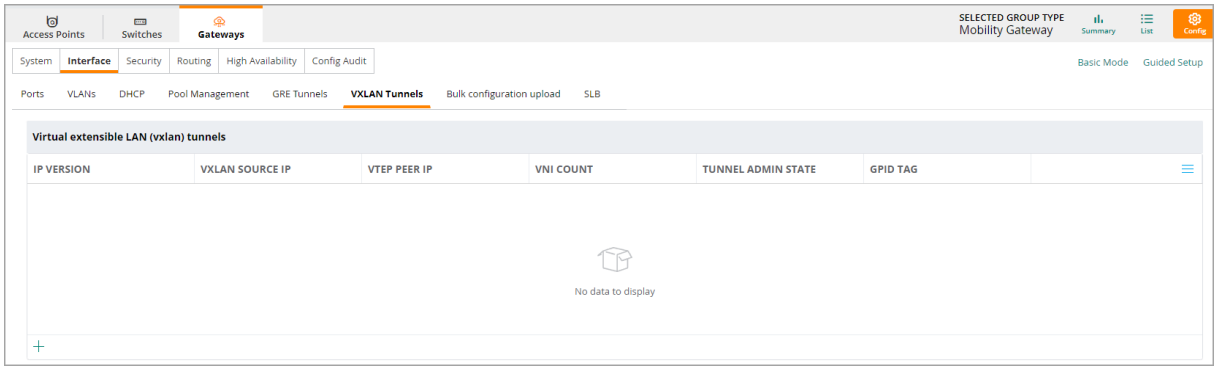



**Step 3** Select **Gateways**, then select **Config**.

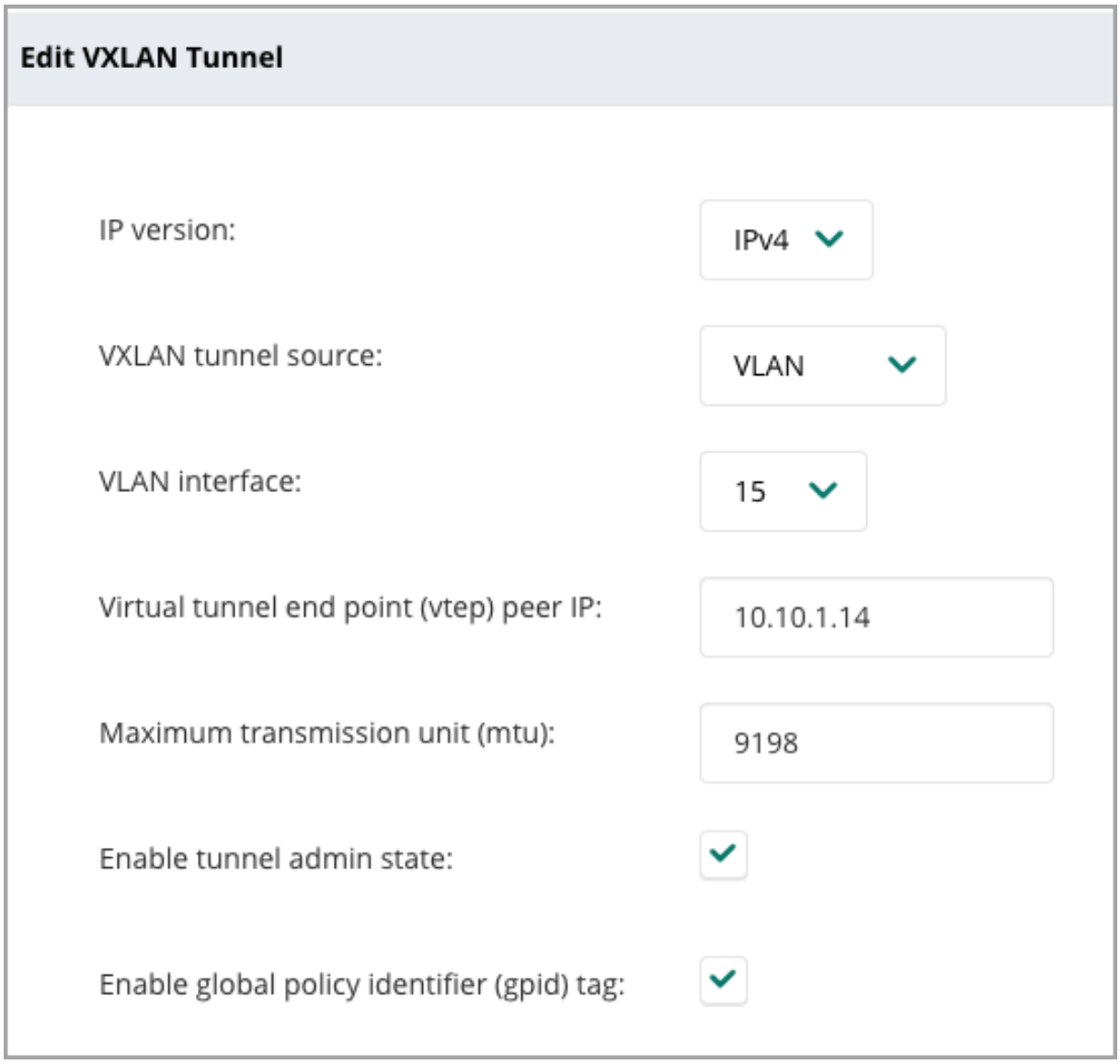
I AM HERE!!!!




**Step 4** Click the **Interface** tab and click **VXLAN** Tunnels. Click the **+** (plus sign) at the lower left.




**Step 5** On the **Add VXLAN Tunnel** page, assign the following settings: * **IP Version:** *IPv4* * **VXLAN Tunnel Source:** *VLAN* * **VLAN Interface:** *15* * **Virtual tunnel end point (vtep) peer IP:** *10.10.1.14* * **MTU**: *9198* * **Enable tunnel admin state:** *checked* * ***Enable global policy identifier (gpid):*** checked*




**NOTE:**

The 10.10.10.14 IP address above is the loopback1 IP address shared among the VSX pair devices acting as stub VTEPs. Use NetEdit to obtain the IP address from one of the border switches.

**Step 6** Click the **+** (plus sign) in VLAN/VNI mapping, assign the following settings and click **OK**. * **VLAN ID:** *102* * **Virtual network identifier:** *102*


**Step 7** Repeat the VLAN-to-VNI mapping for all SSID VLANs.

| Name | VLAN | VNI |
|---|---|---|
| Overlay Fabric Wireless | 102 | 102 |
| Overlay Fabric Wireless - Guest | 201 | 201 |

## Modify Role Policy on the gateway

AOS-10 gateways direct all traffic through the AOS-Firewall, enforcing policies based on the user's role. Each role is governed by a *role-to-role (r2r)* policy, which incorporates rules from the Global Client Roles. Although the user interface may display this policy as empty, it actually contains the rules from the Global Client Roles.

To achieve the desired functionality, additional policies must be created and applied to each role. The following policies are applied to ensure proper traffic flow:

- **allowed-network-services**: This policy enables DNS, DHCP, and other required network services.
- **deny-inbound-clients**: This policy prevents users with an assigned role from communicating to clients with other roles not explicitly allowed in the *r2r* policy and clients that should have roles assigned that do not.
- **allowall**: This policy permits all other traffic. The reference architecture assumes a firewall outside the fabric is used to enforce policy between VRFs and non-fabric resources. If more granular filtering is needed, custom policies can be applied to specific roles, replacing the *allowall* policy.

**NOTE:**

Each role has an implicit deny policy that applies after all system and user-defined policies. Ensure this behavior is accounted for when designing role policies.

Within the **deny-inbound-clients** policy, a network alias called *client-networks* is referenced. This alias should include all subnets where traffic is expected to have identity attached. In a single fabric environment, these would include all wired and wireless subnets local to the site. However, in multi-fabric or SD-WAN extensions, which preserve identity information in the packet, these subnets would also be included.

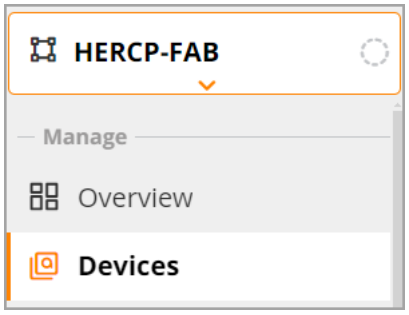
The below table summarizes the policies applied to each role.

| Position | Policy | Notes |
|---|---|---|
| 1 | global-sacl | Default system policy applied to all roles. |
| 2 | apprf-sacl | Default system policy applied to all roles. |
| 3 | r2r_policy | Managed by Global Client Roles to control role-to-role traffic. |

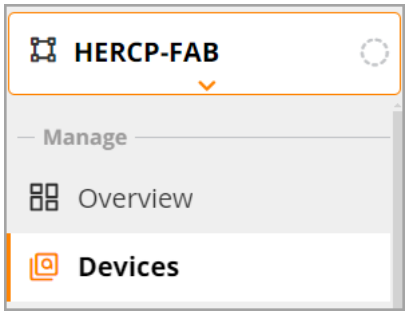
| Position | Policy | Notes |
|---|---|---|
| 4 | allowed-network-services | Allows essential services (e.g., DNS, DHCP) while preventing clients from serving addresses. |
| 5 | deny-inbound-clients | Prevents communication between assigned roles unless explicitly allowed in *r2r* or for unassigned clients. |
| 6 | allowall | Permits all remaining traffic. |

The *role-to-role (r2r)* policy applies when both the source and destination clients are connected to the same gateway or when the gateway is the egress VTEP for the destination client. The *allowall* policy enables *r2r* enforcement when the local gateway is the ingress VTEP, ensuring policy is applied on the remote device connected to the destination client, such as an egress VTEP or a remote gateway.

**Step 1** Select the **HERCP-FAB** group.




**Step 2** On the left menu, select **Devices**.

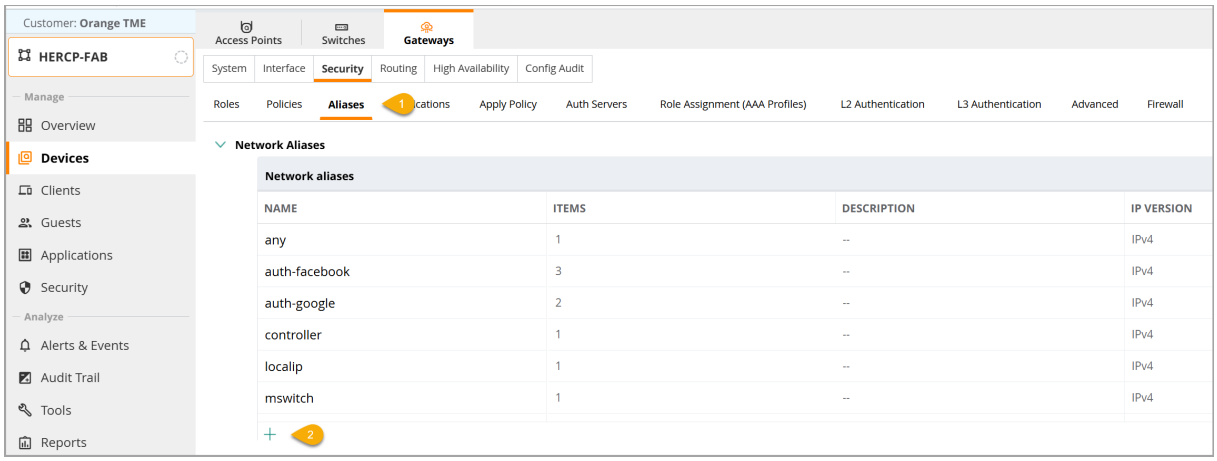



**Step 3** Select **Gateways**, then select **Config**.


### *Create Alias*

**Step 1** Navigate to the **Security** tab and select **Aliases**.

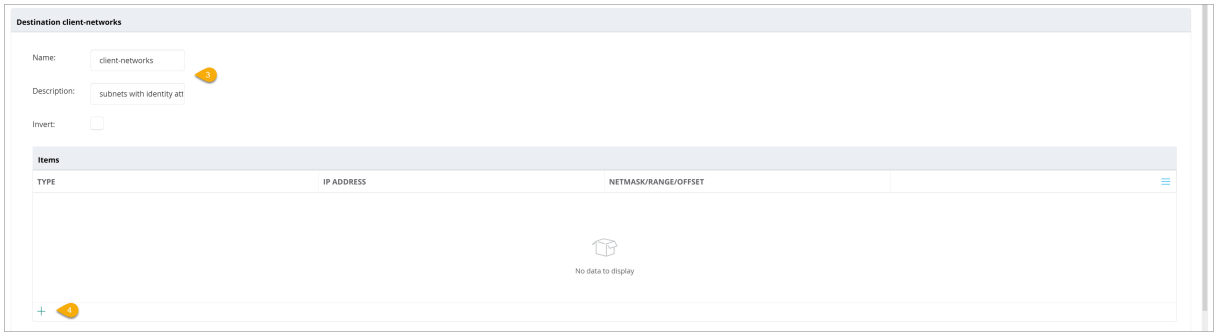
**Step 2** Click the **+** (plus sign) under **Network Aliases** to create a new alias.




**Step 3** In the **Destination client-networks** section, configure the following settings:

- **Name**: *client-networks*
- **Description**: *subnets with identity attached*

**Step 4** Click the **Plus** in the **Items** section.

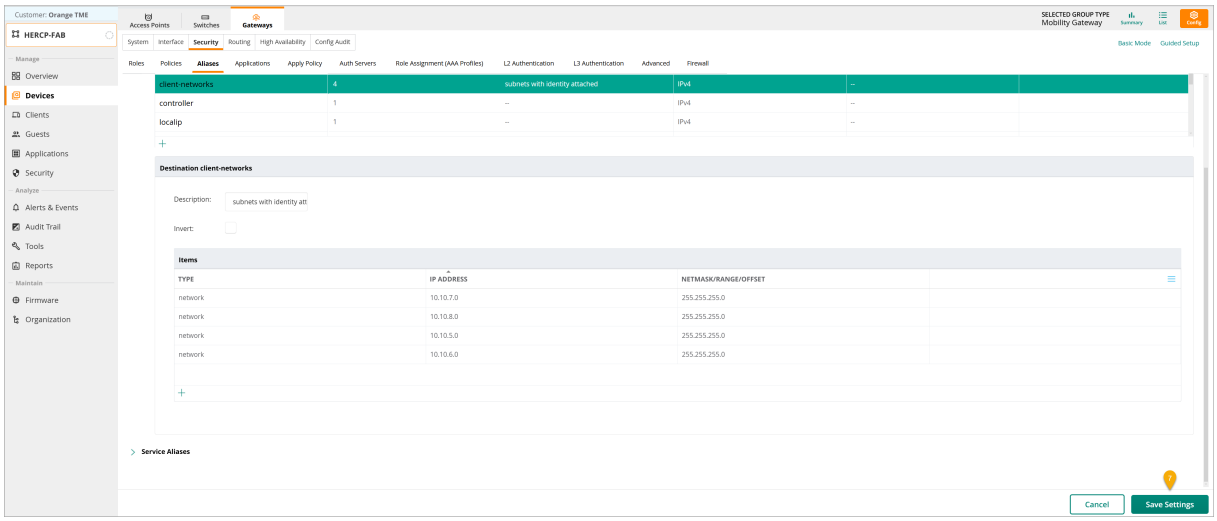



**Step 5** In the **Add New User Rule** window, configure the following settings:

- **Rule Type**: *network*
- **IP Address**: *10.10.5.0*
- **Netmask/Wildcard**: *255.255.255.0*

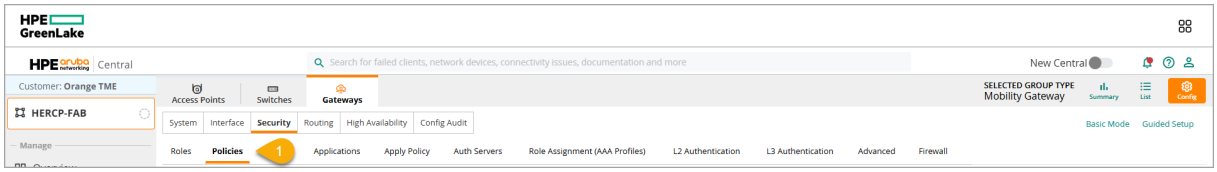

**Step 6** Repeat these steps for all remaining client subnets. For Herndon, configure the following subnets: 10.10.6.0/24, 10.10.7.0/24, and 10.10.8.0/24.

**Step 7** Click **Save Settings** to apply changes.




## *Create Policies*

**Step 1** Navigate to the **Security** tab and select **Policies**.

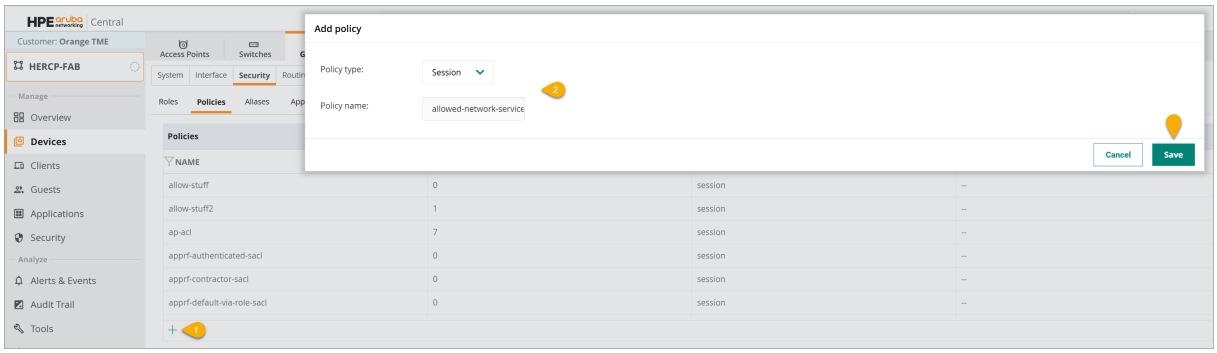



## *Create Allowed-Network-Service Policy*

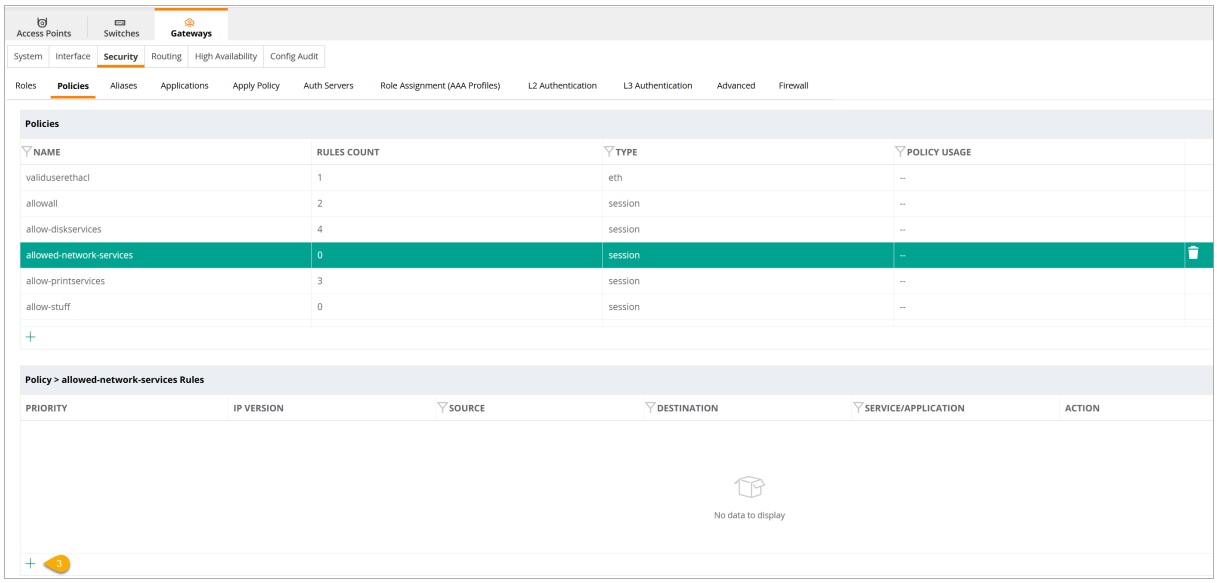
**Step 1** Click the **+** (plus sign) under **Policies** to create a new policy.

**Step 2** In the Add Policy section, configure the following settings and click **Save**.

- **Policy Type**: *session*
- **Policy Name**: *allowed-network-services*

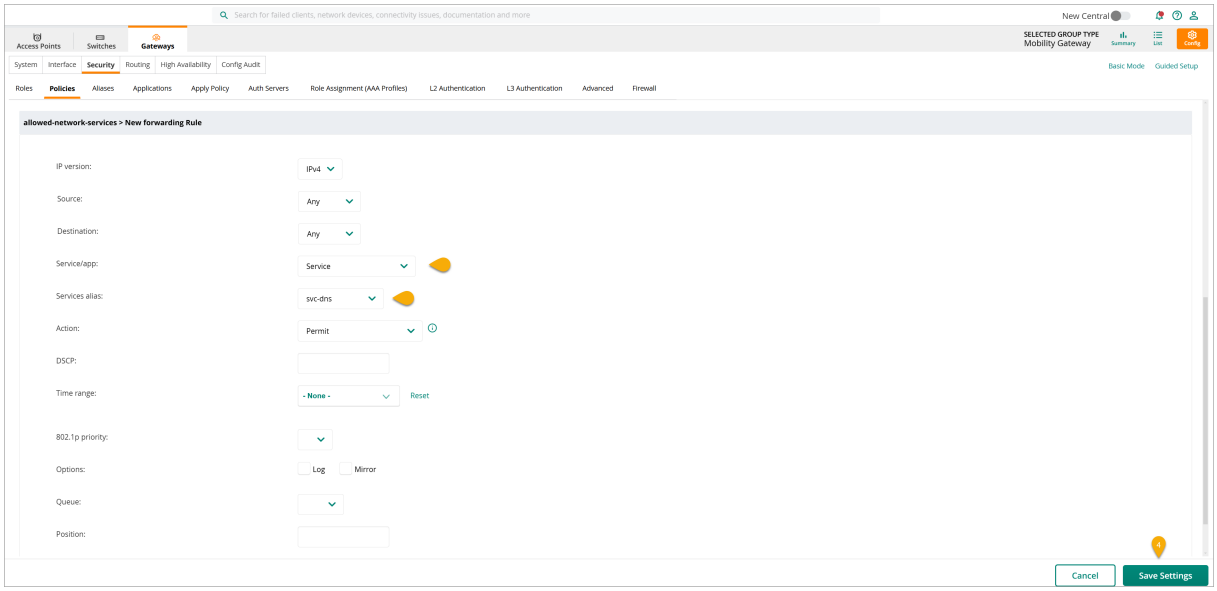



**Step 3** Select the **allowed-network-services** policy and click the **+** (plus sign).



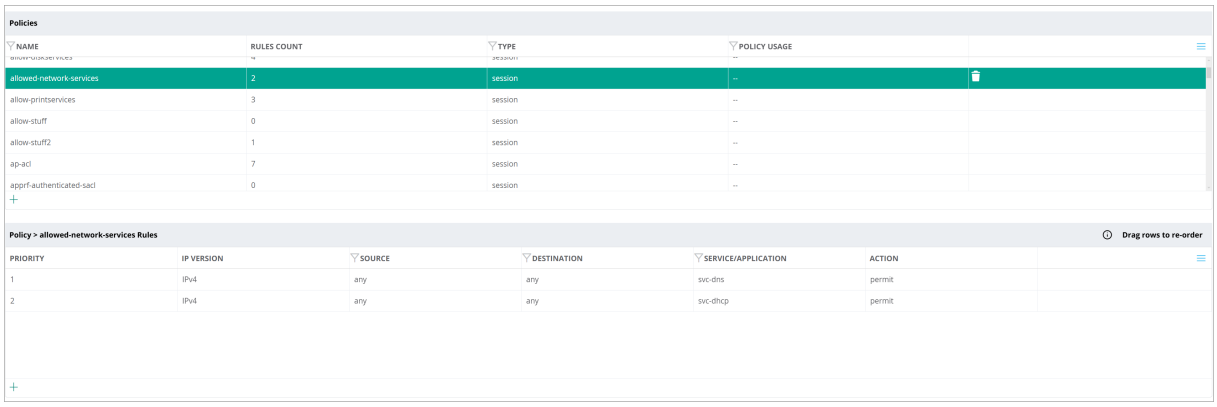

**Step 4** In the Policy > allowed-network-services Rules section and configure the following settings, leaving all other settings as default and Click **Save Settings**.

- **Service/App**: *service*
- **Services Alias**: *svc-dns*




**Step 5** Repeat Step 4 to create a rule for *svc-dhcp*.

Below is the complete policy.




## *Create Deny-Inbound-Clients Policy*

Use the same steps detailed in Allowed-Network-Service Policy to create the Deny-Inbound-Client Policy.

**Step 1** Click the **+** (plus sign) under **Policies** to create a new policy.

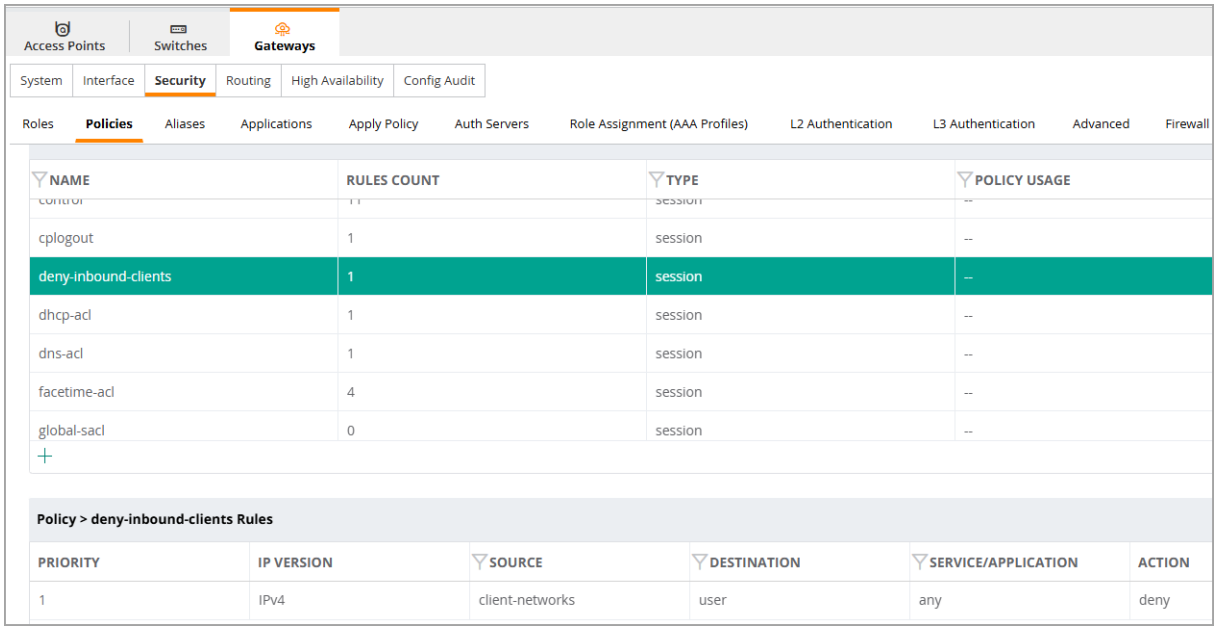
**Step 2** In the Add Policy section, configure the following settings: - **Policy Type**: *session* - **Policy Name**: *deny-inbound-clients*

**Step 3** Select the deny-inbound-clients policy.

**Step 4** Click the **+** (plus sign) in the Policy > deny-inbound-client-policy Rules section and configure the following settings, leaving all other settings as default: - **Source**: *Alias* - **Source alias**: *client-networks* - **Destination**: *User* - **Action**: *Deny*

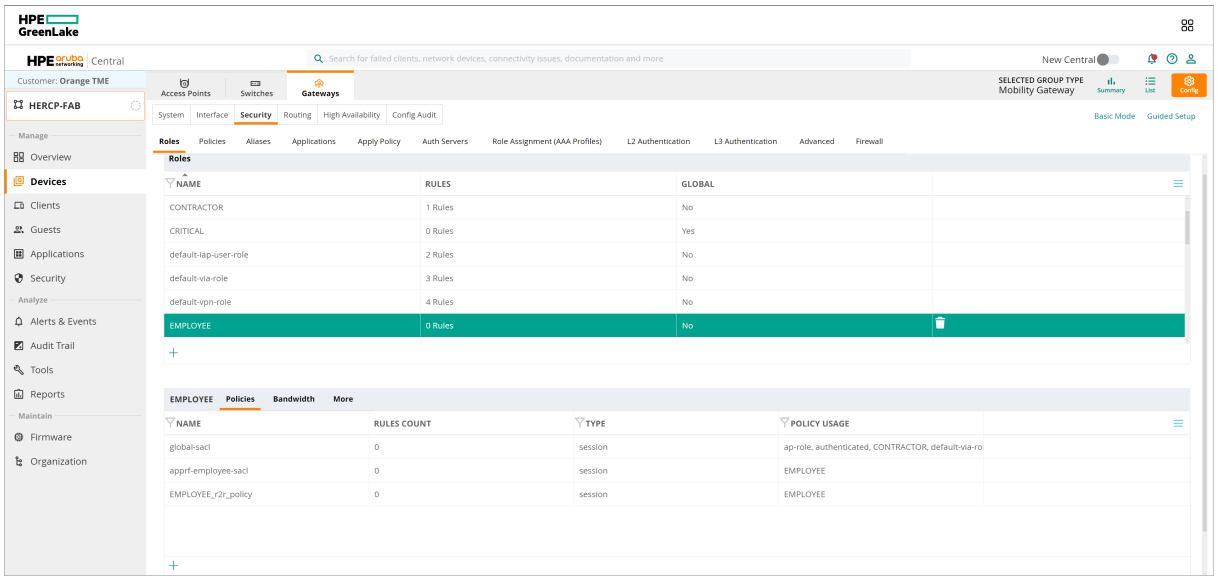
**Step 5** Click **Save Settings** to apply changes.

Below is the complete policy.

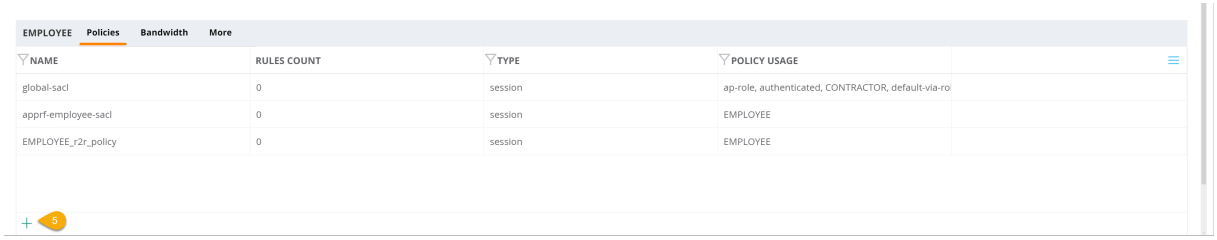



## *Apply Policies to Role*

**Step 1** Navigate to the **Security** tab. In the **Roles** section, select the **EMPLOYEE** role.

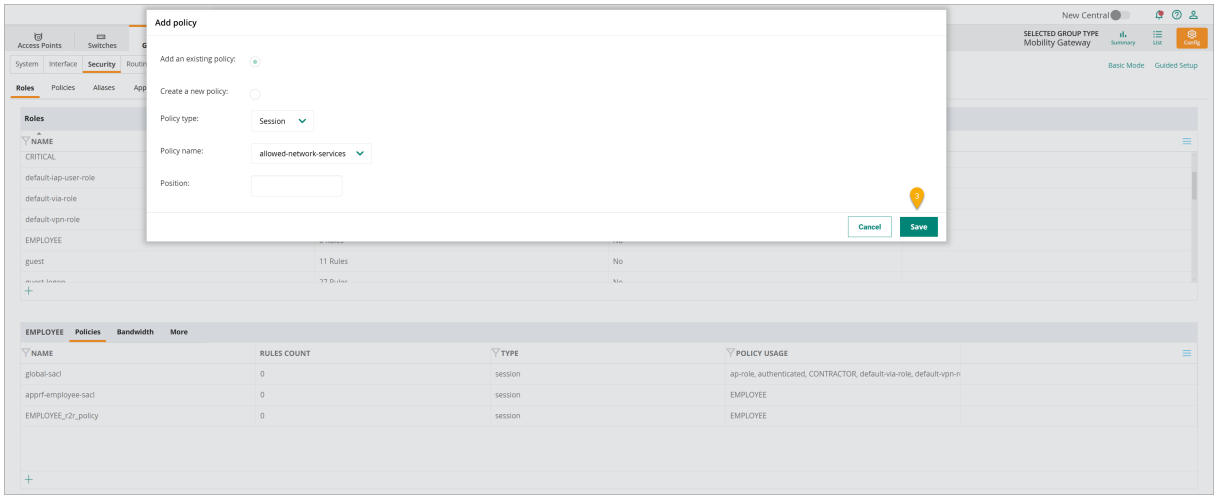



**Step 2** Click the **+** (plus sign).




**Step 3** In the Add Policy Window select the following items and **click Save**.

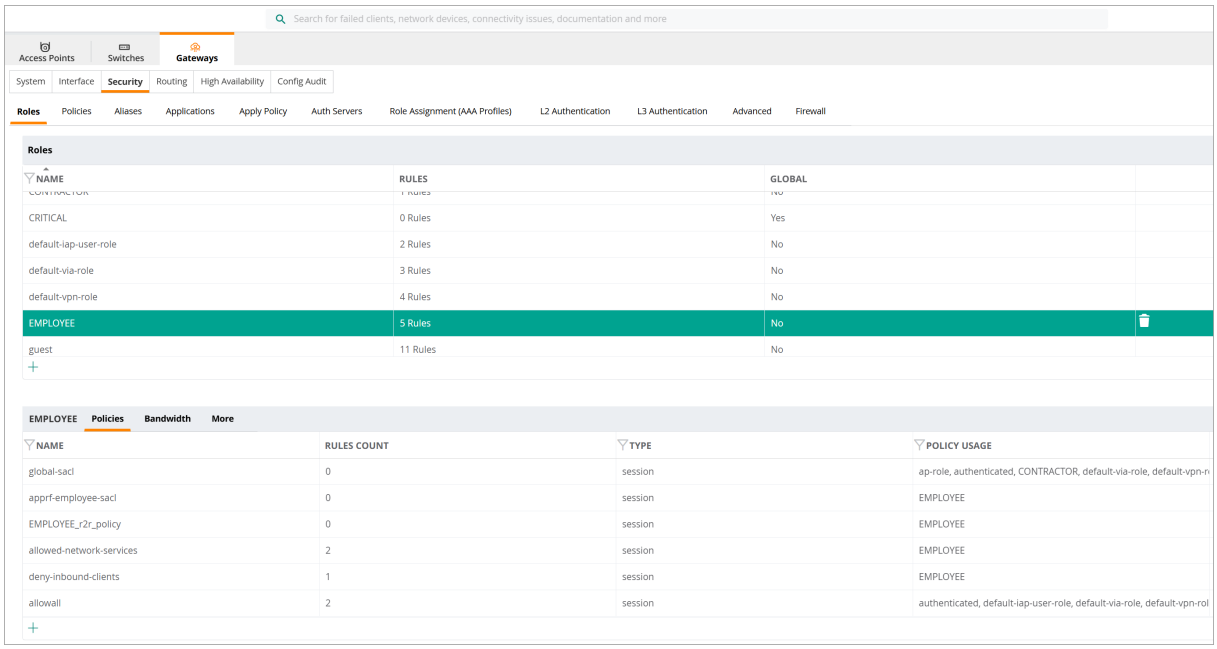
1. Select the **Add an Existing Policy** button.
2. Choose the **allowed-network-services** policy.




**Step 4** Repeat Steps 3 to add the **deny-inbound-client** and **allowall** policies.

**Step 5** Repeat the **Apply Policies to Role** steps for each role in use.

Below is the resulting policies applied to the EMPLOYEE role.




**NOTE:**

Policy order is critical to correct policy enforcement. Out of order positioning will result in a failure to apply the policy as intended. Ensure the rule order illustrated above is implemented exactly as shown.

**NOTE:**

After adding the *allowall* policy, additional *global* and *apprf* policies appear. These system policies are applied to all roles by default. When using the default policies, evaluate their impact on traffic forwarding within assigned roles.

## Create Fabric SSID

Refer to Configuring Wireless Access to assist with creating an SSID named **SSID-HERCP-01** that authenticates to ClearPass. Configure this SSID to place users into VLAN 301.

# Configure External Connectivity

External connectivity can be configured in two distinct ways.

VRF Lite handoff allows each fabric VRF to connect to devices such as firewalls with multiple zones, upstream routing devices with extended VRFs, or the global routing table. Although this guide does not illustrate VRF Lite handoff, an example is available in the Data Center Deployment Guide. This option is suitable when connecting to devices that do not support EVPN-VXLAN.

Configuring an EVPN-VXLAN handoff enables the extension of both VRF and role information. When integrating with an HPE Aruba Networking SD-WAN solution, the role and VRF are maintained throughout the SD-WAN fabric. Detailed instructions for this configuration are available in the EdgeConnect SD-WAN Multi-Site chapter.

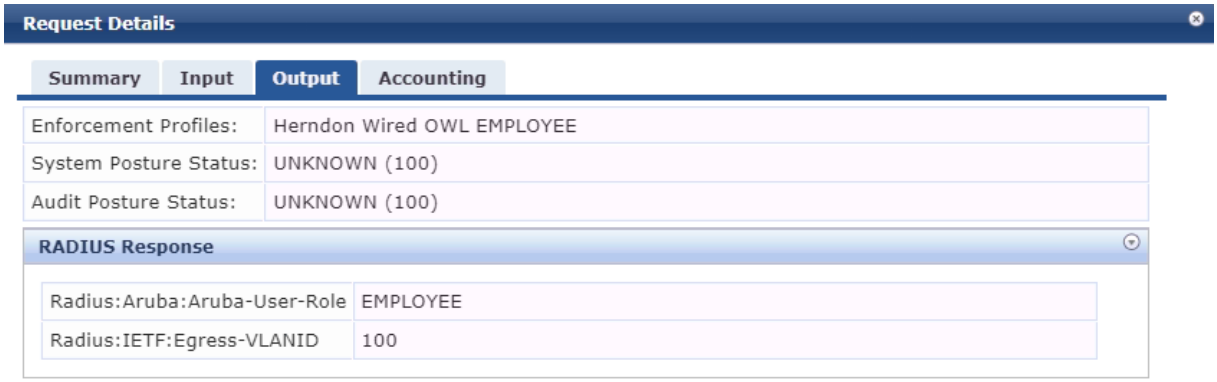
## ClearPass Integration

RADIUS-based authentication is required on all edge ports participating in the fabric. ClearPass is the recommended solution.

Ensure that edge switches and edge ports are configured to support 802.1x. Refer to the Configure RADIUS and UBT section for guidance.

Modify the ClearPass services as needed to ensure that ClearPass returns a role and VLAN.

The below screenshot shows the RADIUS response returned by ClearPass after successful authentication.




## Edge Port Configuration

Edge ports should be configured as colorless ports using Port Profiles. Use Device Profiles to detect APs and UXI sensors dynamically and place them in the correct VLAN.

The configuration shown below is an example of an edge port. Refer to the Example Configuration section for guidance to configure edge ports and Device Profiles.

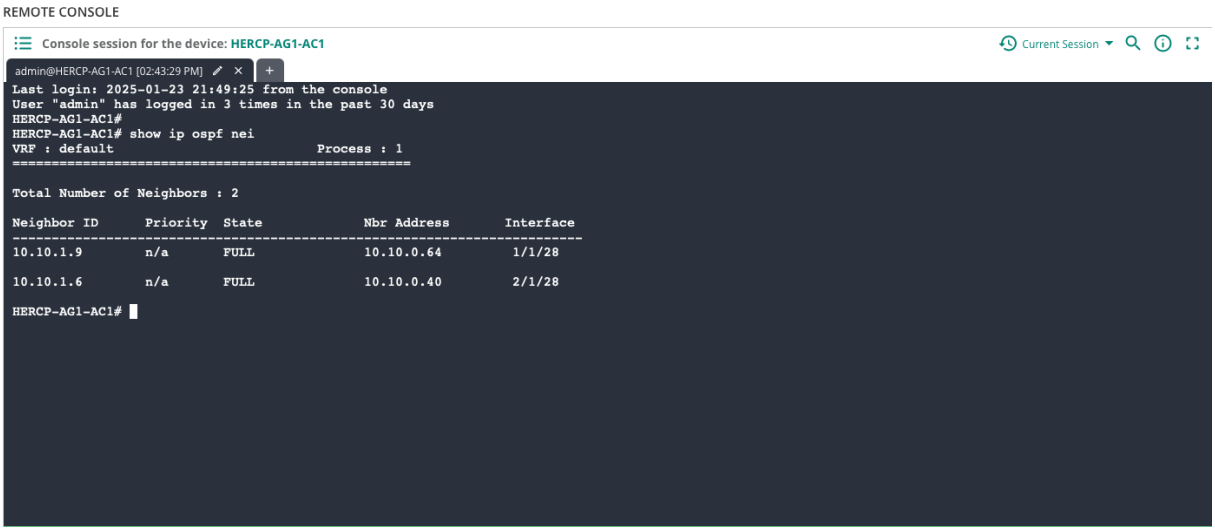
```
interface 1/1/1
    description ACCESS_PORT
    no shutdown
    no routing
    vlan access 1
    spanning-tree bpdu-guard
    spanning-tree root-guard
    spanning-tree tcn-guard
    spanning-tree port-type admin-edge
    aaa authentication port-access client-limit 5
    aaa authentication port-access auth-precedence dot1x mac-auth
    aaa authentication port-access critical-role CRITICAL
    aaa authentication port-access reject-role REJECT
    aaa authentication port-access dot1x authenticator
        eapol-timeout 30
        max-eapol-requests 1
        max-retries 1
        reauth
        enable
    aaa authentication port-access mac-auth
        cached-reauth
        cached-reauth-period 86400
        quiet-period 30
        enable
```

# Verification

The steps below illustrate how to verify functionality for a distributed fabric deployment. Central provides a remote console that enables CLI access on any managed switch. Refer to the Verify OSPF Operation section for a more detailed overview.

## Verify Underlay

**Step 1** In a **Remote Console** window, type the command *show ip ospf neighbors* and press ENTER. Confirm that the state is “FULL” for all appropriate OSPF peers.




**Step 2** In a **Remote Console** window, type the command *show ip route* and press ENTER. Confirm that all loopback0 and 1 /32 routes are listed.

REMOTE CONSOLE

Console session for the device: HERCP-AG1-AC1

Current Session

admin@HERCP-AG1-AC1 [03:08:35 PM]

```
User "admin" has logged in 4 times in the past 30 days
HERCP-AG1-AC1# show ip route

Displaying ipv4 routes selected for forwarding

Origin Codes: C - connected, S - static, L - local
              R - RIP, B - BGP, O - OSPF, D - DHCP
Type Codes:   E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
              IA - OSPF internal area, E1 - OSPF external type 1
              E2 - OSPF external type 2
Flags:        F - FIB-optimized route

VRF: default

Prefix              Nexthop                                 Interface     VRF(egress)       Origin/    Distance/    Age
                                                                                            Type       Metric
-------------------------------------------------------------------------------------------------------------------
0.0.0.0/0           10.10.0.64                              1/1/28        -                 O/E2       [110/50]     02m:01w:06d
                    10.10.0.40                              2/1/28        -                            [110/50]     02m:01w:06d
10.0.0.0/13         10.10.0.64                              1/1/28        -                 O/E2       [110/50]     02m:01w:06d
                    10.10.0.40                              2/1/28        -                            [110/50]     02m:01w:06d
10.2.120.0/24       10.10.0.64                              1/1/28        -                 O/E2       [110/50]     02m:01w:06d
                    10.10.0.40                              2/1/28        -                            [110/50]     02m:01w:06d
10.10.0.0/20        10.10.0.64                              1/1/28        -                 O/E2       [110/50]     02m:01w:06d
                    10.10.0.40                              2/1/28        -                            [110/50]     02m:01w:06d
10.10.0.4/31        10.10.0.64                              1/1/28        -                 O          [110/18]     02m:01w:06d
                    10.10.0.40                              2/1/28        -                            [110/18]     02m:01w:06d
10.10.0.6/31        10.10.0.64                              1/1/28        -                 O          [110/18]     02m:01w:06d
                    10.10.0.40                              2/1/28        -                            [110/18]     02m:01w:06d
```

## Verify Overlay

The EVPN verification below is recommended for all fabric switches. VXLAN verification is recommended for the edge, border, and stub devices. Endpoint verification is recommended for edge switches.

**Step 1** In a **Remote Console** window, type the command *`show bgp all summary`* and press ENTER. Confirm that BGP peering is active between the route reflectors and all fabric devices.

REMOTE CONSOLE

Console session for the device: HERCP-CR1-2

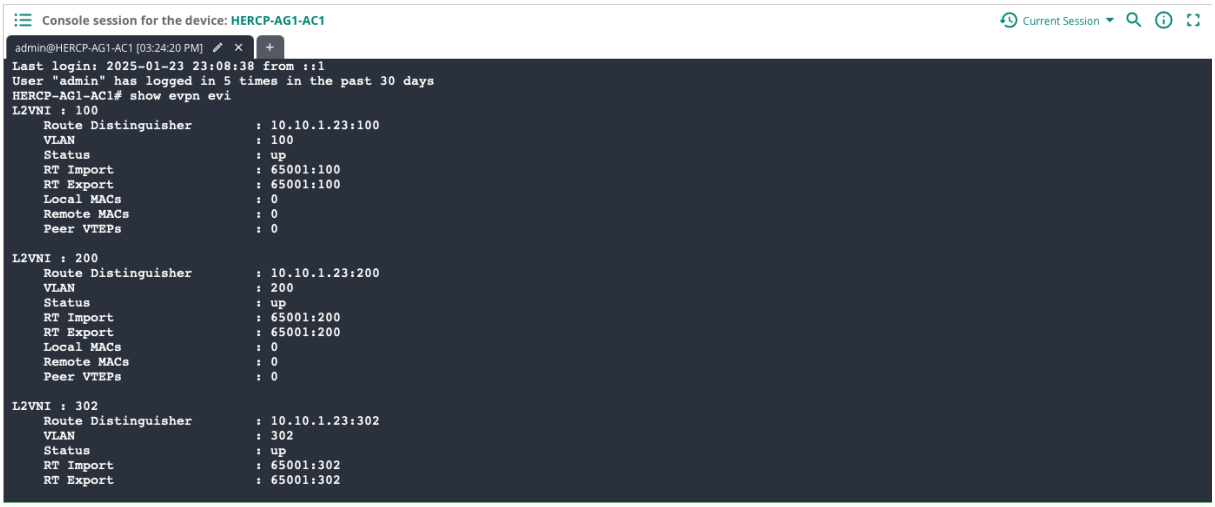
No Session Found

admin@HERCP-CR1-2 [03:21:04 PM]

```
HERCP-CR1-2# show bgp all summary
Codes: * Dynamic Neighbor
VRF : default
BGP Summary
-----------
 Local AS               : 65001        BGP Router Identifier  : 10.10.1.0
 Peers                  : 8            Log Neighbor Changes   : No
 Cfg. Hold Time         : 180          Cfg. Keep Alive        : 60
 Confederation Id       : 0

Address-family : IPv4 Unicast
------------------------------

Address-family : IPv6 Unicast
------------------------------

Address-family : VPNv4 Unicast
------------------------------

Address-family : L2VPN EVPN
------------------------------
 Neighbor                                Remote-AS   MsgRcvd MsgSent Up/Down Time State         AdminStatus
 10.10.1.2                               65001       121298  121426  02m:01w:06d  Established   Up
 10.10.1.3                               65001       121302  121340  02m:01w:06d  Established   Up
 10.10.1.4                               65001       121161  121406  02m:01w:06d  Established   Up
 10.10.1.5                               65001       121245  121385  02m:01w:06d  Established   Up
 10.10.1.10                              65001       121158  121363  02m:01w:06d  Established   Up
 10.10.1.11                              65001       121205  121415  02m:01w:06d  Established   Up
 10.10.1.12                              65001       121176  121445  02m:01w:06d  Established   Up
```

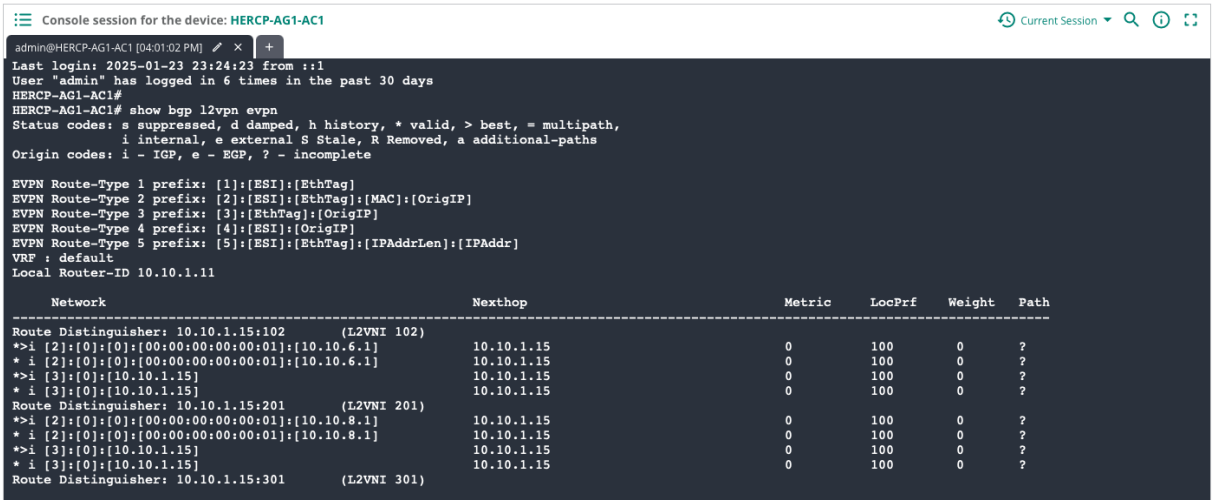
**Step 2** In a **Remote Console** window, type the command*`show evpn evi`* and press ENTER. Verify the EVPN configuration and operational state.

REMOTE CONSOLE



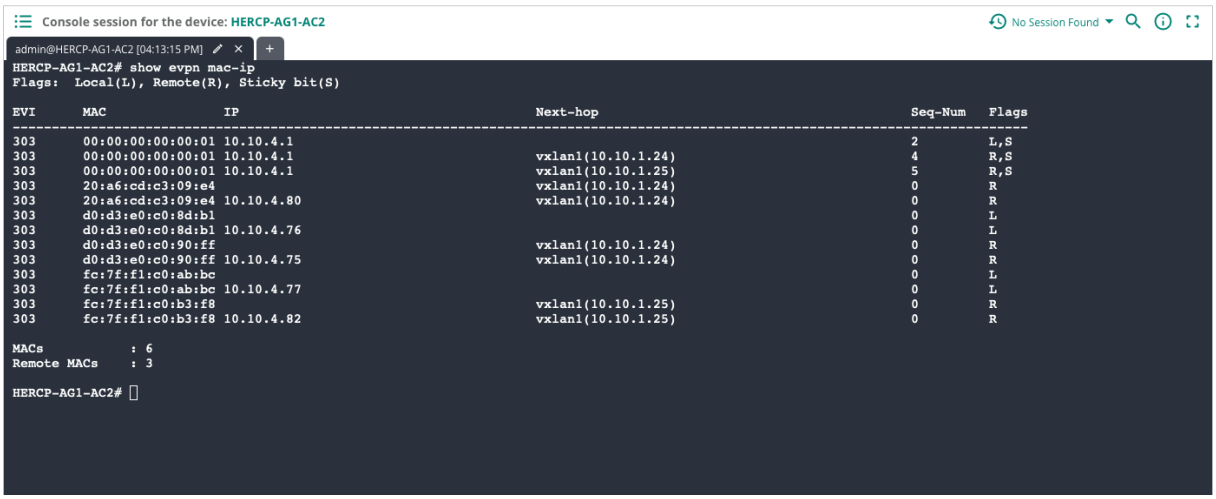

**Step 3** In a **Remote Console** window, type the command *show bgp l2vpn evpn* and press ENTER. Verify EVPN overlay routes.

REMOTE CONSOLE



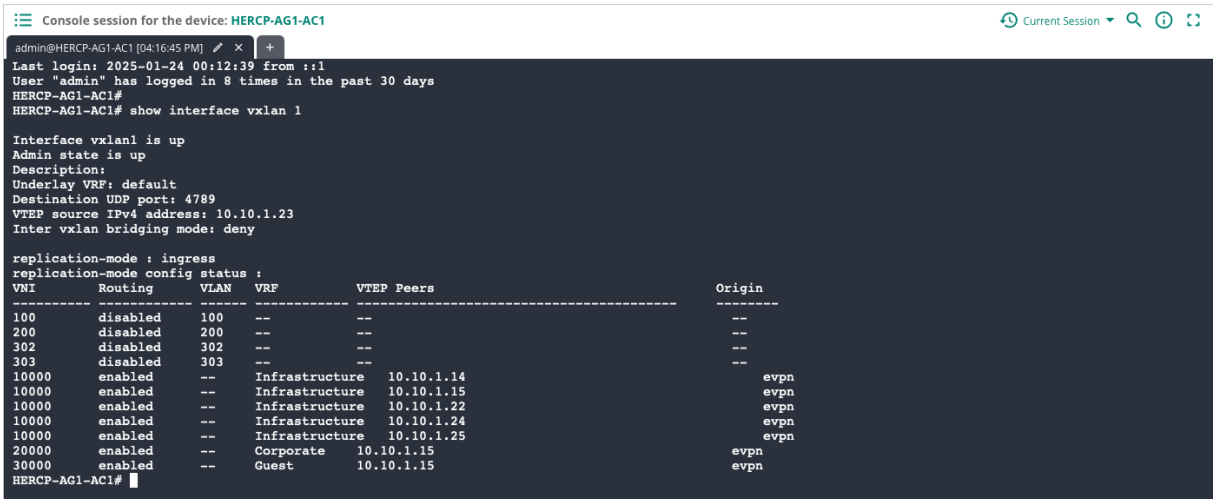

**Step 4** In a **Remote Console** window, type the command *show evpn mac-ip* and press ENTER. Verify that overlay MAC/IP address information is learned from EVPN.

REMOTE CONSOLE



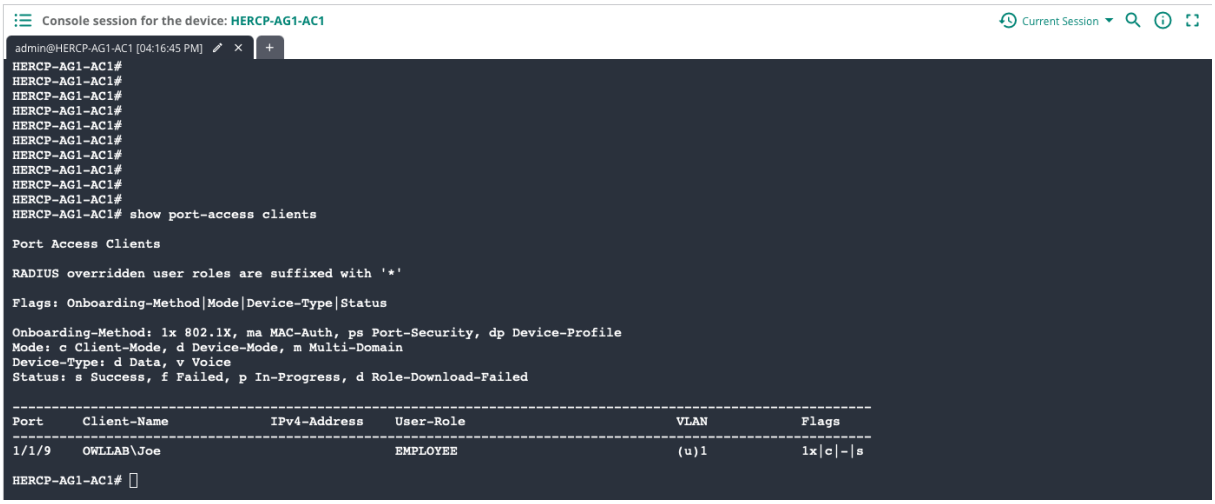
**Step 5** In a **Remote Console** window, type the command *show interface vxlan 1* and press ENTER. Verify that VXLAN tunnels are established.

REMOTE CONSOLE




**Step 6** In a **Remote Console** window, type the command *show port-access clients* and press ENTER. Verify the authentication state of an endpoint and confirm proper role assignment.

REMOTE CONSOLE




**Step 7** In a **Remote Console** window, type the command *show port-access gbp* and press ENTER. Verify that configured GBP policies are applied.

REMOTE CONSOLE

Console session for the device: HERCP-AG1-AC1

Current Session

admin@HERCP-AG1-AC1 [04:16:45 PM]

```
HERCP-AG1-AC1#
HERCP-AG1-AC1# show port-access gbp

Port Access GBP User Configured Policy Details:
===============================================

GBP Name            : CONTRACTOR_r2r_policy
GBP Type            : Local
GBP Status          : Applied

SEQUENCE    CLASS                           TYPE     ACTION
----------- ------------------------------- -------- ----------------------
10          CONTRACTOR_ALLOW                gbp-ipv4 permit
20          CONTRACTOR_ALLOW                gbp-ipv6 permit
30          CONTRACTOR_ALLOW                gbp-mac  permit

GBP Name            : CRITICAL_r2r_policy
GBP Type            : Local
GBP Status          : Applied

SEQUENCE    CLASS                           TYPE     ACTION
----------- ------------------------------- -------- ----------------------
10          CRITICAL_ALLOW                  gbp-ipv4 permit
20          CRITICAL_ALLOW                  gbp-ipv6 permit
30          CRITICAL_ALLOW                  gbp-mac  permit

GBP Name            : EMPLOYEE_r2r_policy
GBP Type            : Local
GBP Status          : Applied
```

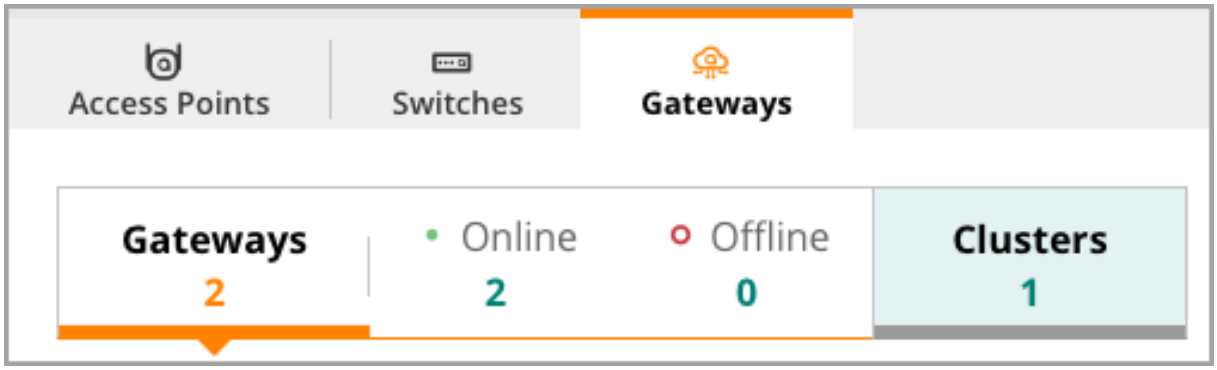
## Verify Gateways

VXLAN verification confirms the operational state of the static VXLAN tunnel. It is recommended for all gateways.

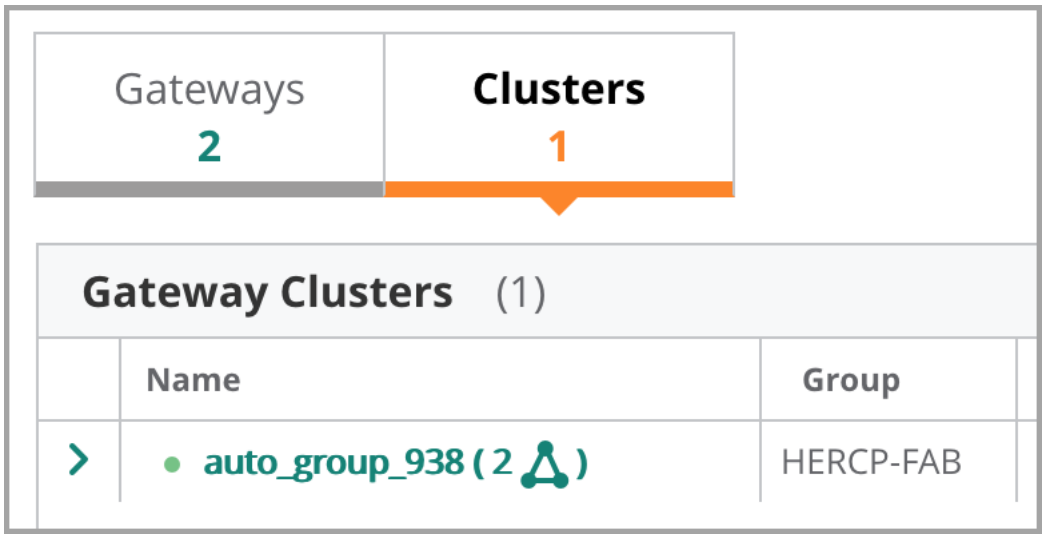
**Step 1** In the **Global** dropdown, select the switch group. In this example, the group is **CP-HER-FAB.**

**Step 2** On the left menu, select **Devices**.

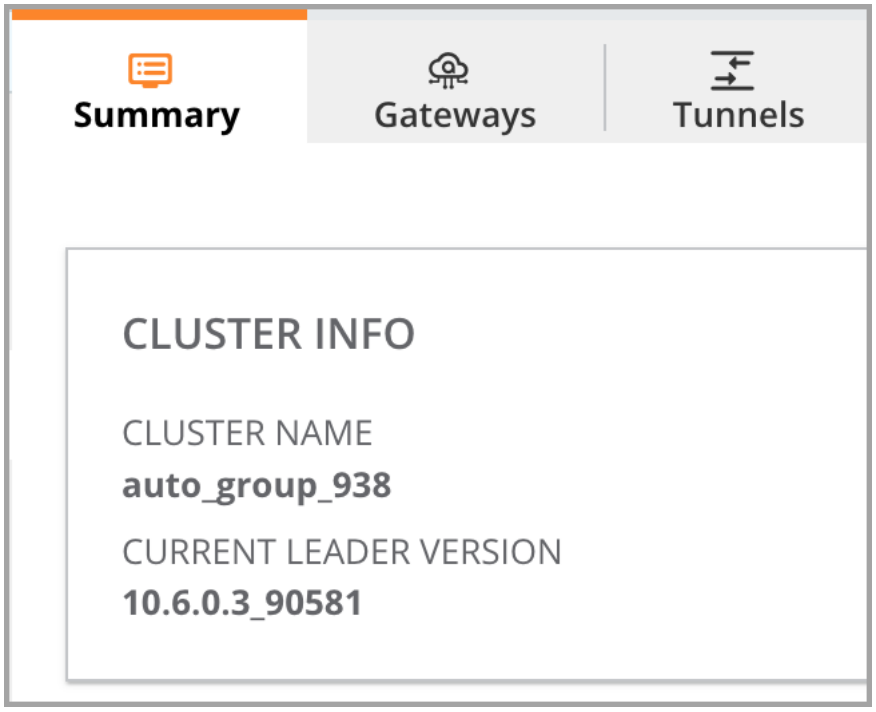
**Step 3** Select **Gateways**, then select **Clusters**.



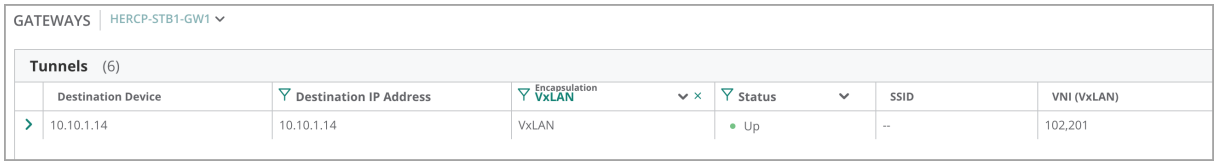

**Step 4** In the **Name** column, click the name of the fabric connected cluster.




**Step 5** Select the **Tunnels** page.




**Step 6** In the **Tunnels** table, find the stub switch VTEP address in the **Destination Device** column, and confirm that the **Status** column indicates “Up”.



# Brownfield Considerations

A NetConductor fabric can be deployed over an existing OSPF underlay using the Fabric workflow. This is supported on underlays with a Layer 2 or a Layer 3 configuration to the access layer. Certain requirements must be met for successful deployment.

**Step 1** All Aruba CX switches to be included in the fabric must be in the same Central UI group. Gateways and access points do not need to be in the same group.

**Step 2** Migrate underlay configured switches to the fabric group in Central using the **Retain CX-switch configuration** option to preserve the existing underlay.

**Step 3** Configure *loopback0* as the interface for OSPF routers. Create *loopback1* for use by the VXLAN configuration of the Fabric workflow.

**Step 4** When deploying the EVPN fabric over an existing Layer 2 access deployment, create a transit VLAN from aggregation to access switches for running OSPF and enabling Layer 3 access to the loopback interfaces of the access layer switches.

**Step 5** Configure all underlay switch interfaces for an MTU of *9198* bytes to ensure unfragmented transport of VXLAN packets through the network.

# EdgeConnect SD-WAN Multi-Site

This procedure describes the process for configuring EVPN-VXLAN between the EdgeConnect SD-WAN gateway and the border using HPE Aruba Networking Central and Orchestrator.

In this design, Aruba EdgeConnect SD-WAN gateways integrate with fabrics deployed at each site to learn the segmentation information (VRFs and/or User Roles) and transport it natively in the SD-WAN (IPSEC) to avoid MTU or fragmentation concerns.

To learn more about this design, consult the Campus Design guide or the NetConductor Architecture Guide.

## Prerequisites

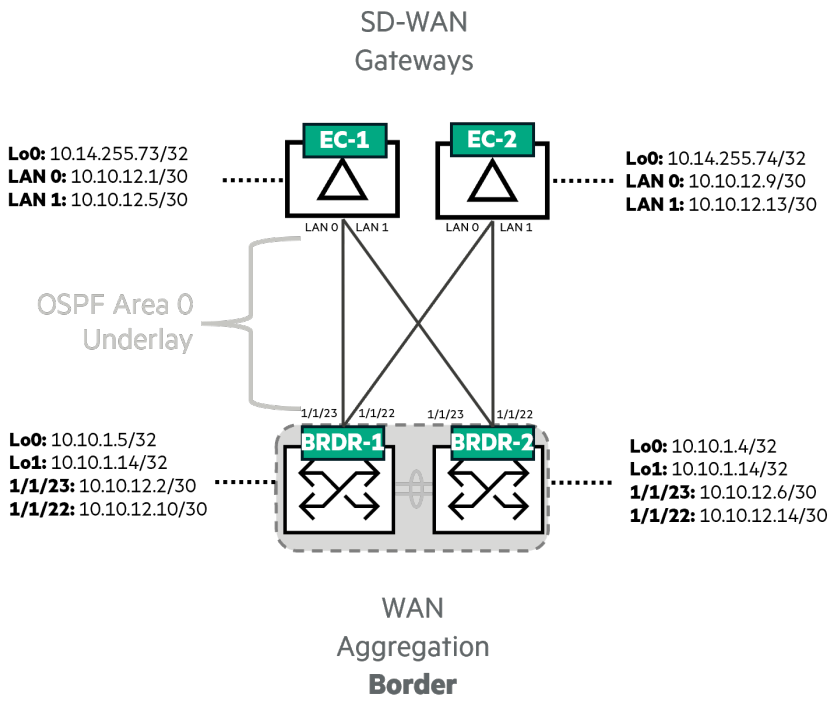
This procedure assumes initial configuration of EdgeConnect following the Branch Deployment Guide:

- EdgeConnect is online and managed by Orchestrator.
- A NetConductor fabric has been deployed according to the instructions on the Underlay and Overlay pages.

Before beginning, ensure that OSPF is operational in the underlay between the border switches and the EdgeConnect SD-WAN gateways. OSPF is essential for exchanging reachability information between loopback interfaces, necessary for forming eBGP adjacencies and establishing VXLAN tunnels.

Additionally, confirm that the EdgeConnect SD-WAN gateway has a loopback interface configured using loopback orchestration, and that loopbacks 0 and 1 set up on border switches. Ensure that jumbo MTU settings are configured on both the EdgeConnect and the border switches.

The below diagram illustrates the starting point for the deployment.



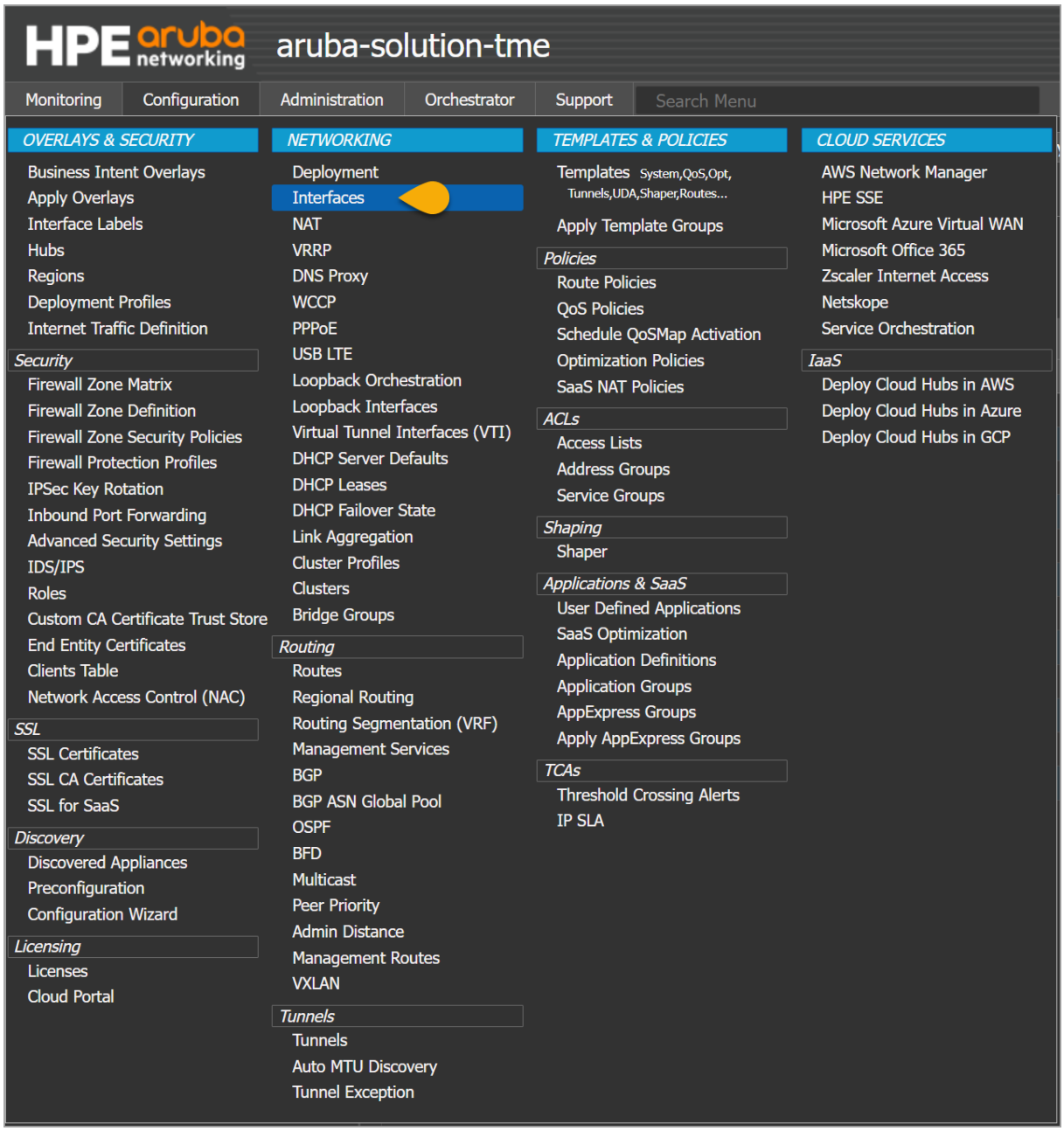

# Configure MTU

Jumbo MTU is necessary for VXLAN tunnels. EdgeConnect SD-WAN gateways support a maximum MTU of 9000. This step will configure the MTU to 9000 on both the EdgeConnect gateways and the border switches. It is essential that adjacent devices have the same MTU setting to establish OSPF neighbor relationships.

### *EdgeConnect SD-WAN Gateways*

**Step 1** Log into **HPE Aruba Networking Orchestrator**.

**Step 2** Hover on **Configuration**. In the **Networking** section and click **Interfaces**.

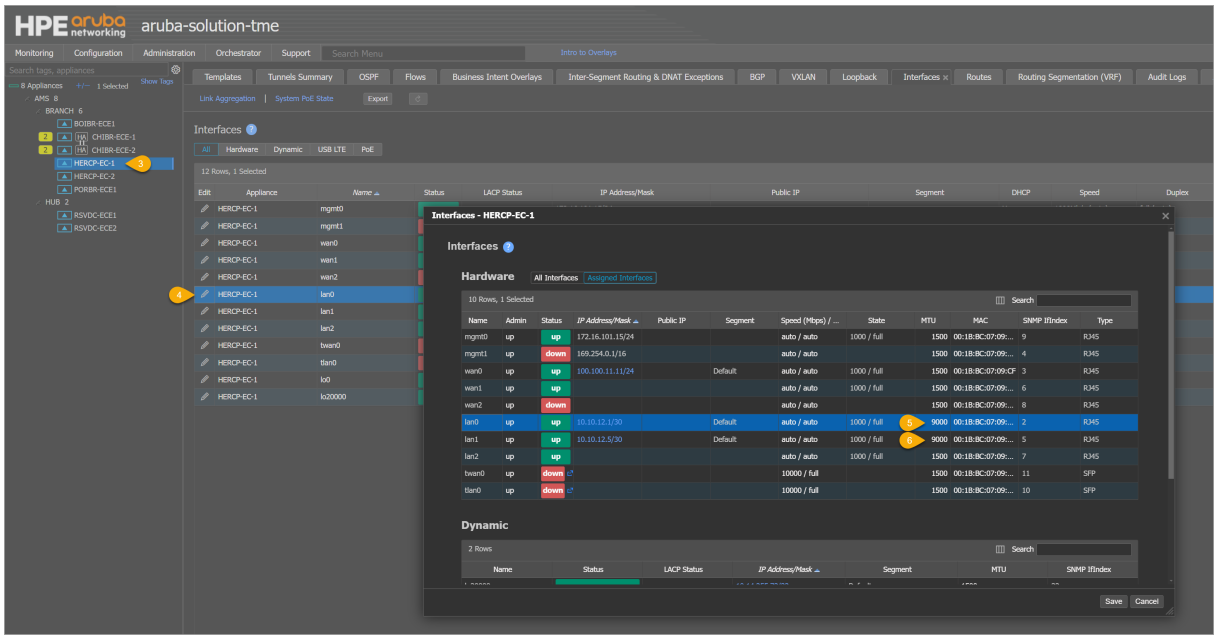



**Step 3** Select **HERCP-EC-1** in the sidebar.

**Step 4** Click the **Edit** icon next to LAN0.

**Step 5** Select the **MTU** in the **lan0** row and change it from 1500 to **9000**.

**Step 6** Repeat step 5 for the **lan1** interface and click **Save**.

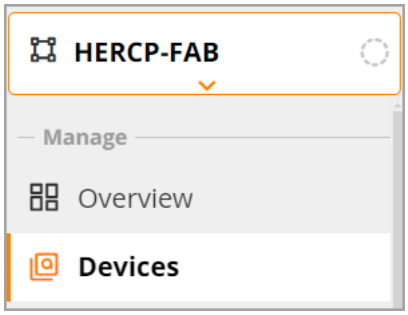



**Step 7** Repeat steps 1 to 6 for **HERCP-EC-2**.

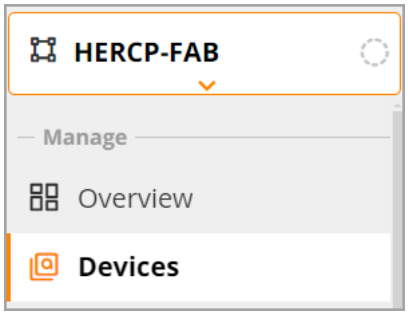
## *Border Switches*

**Step 1** Log into **HPE Aruba Networking Central**.

**Step 2** In the **Global** dropdown, select the switch group. In this sample procedure, the group is **HERCP-FAB.**




**Step 3** On the left menu, select **Devices**.

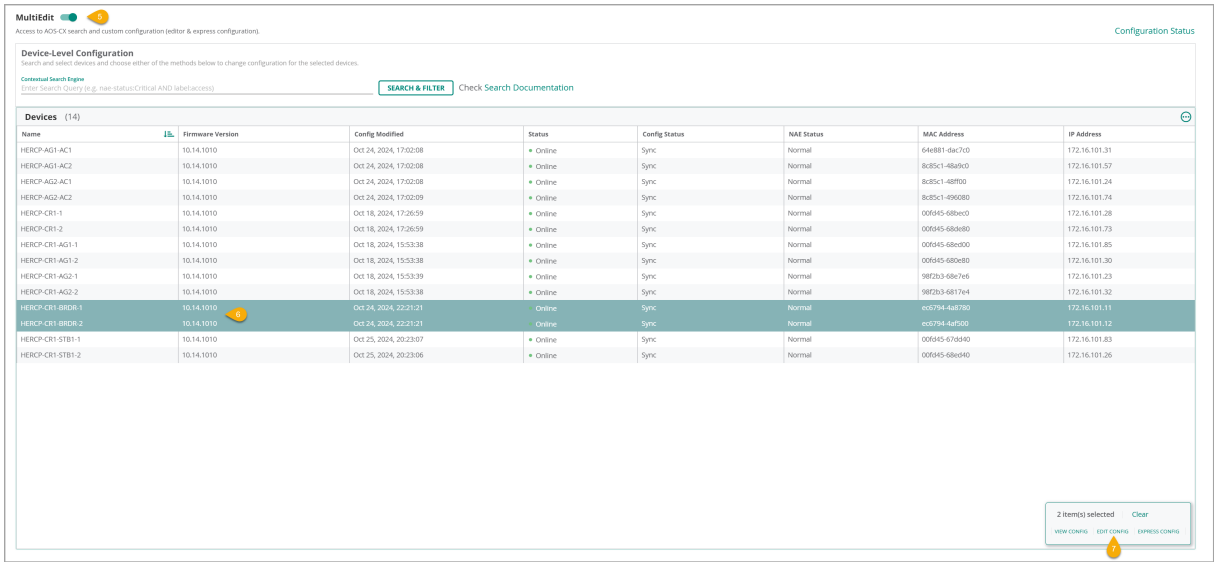



**Step 4** Click **Switches**, then select **Config**.

**Step 5** Enable the **MultiEdit Toggle**.

**Step 6** Select the two border switches.

**Step 7** Click **Edit Config**.




**Step 8** Modify the interfaces connected to EdgeConnect with the following configuration and click **Save**.

```
interface 1/1/22
    description HERCP-EC
    mtu 9000
    ip mtu 9000
interface 1/1/23
    description HERCP-EC
    mtu 9000
    ip mtu 9000
```

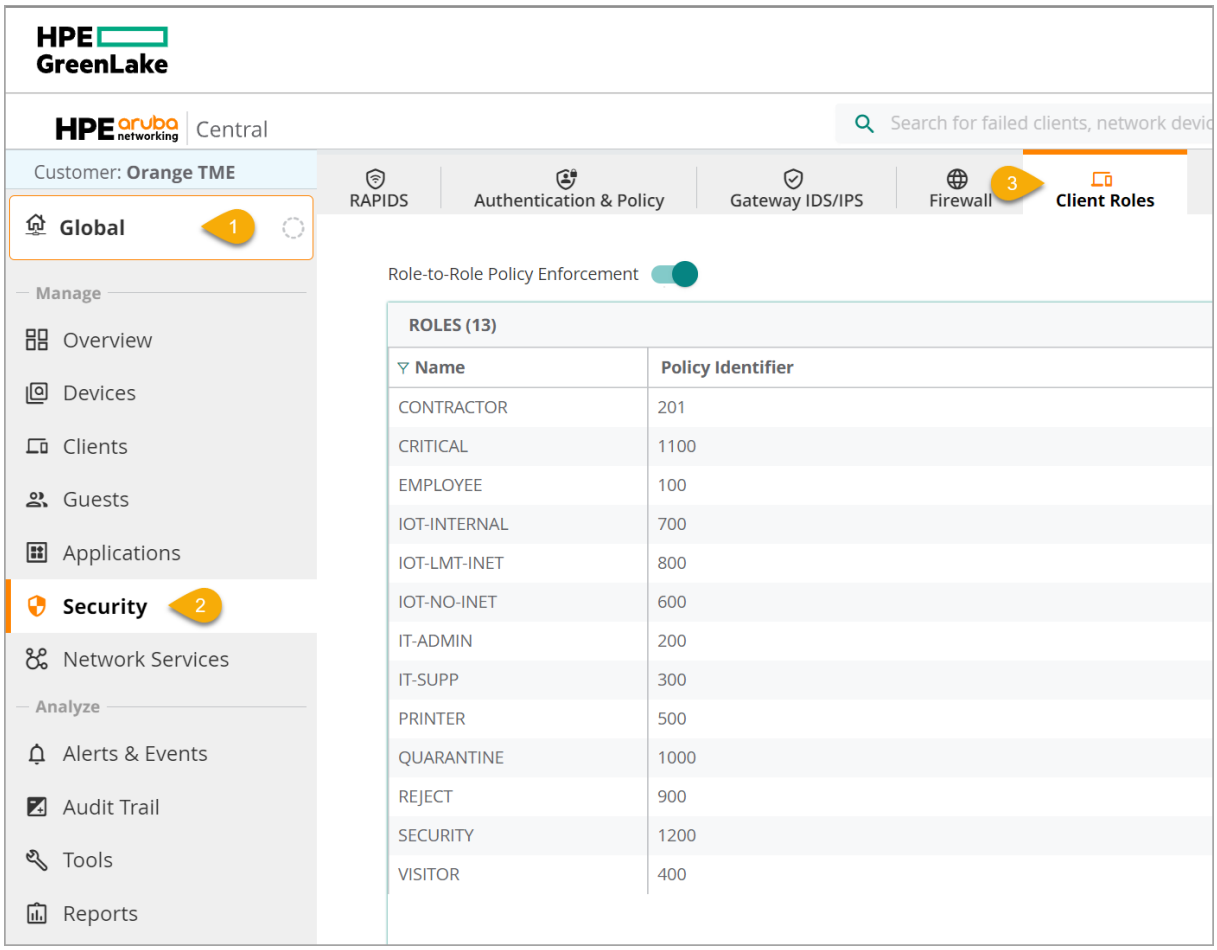
## Define Roles

Roles must be created manually on Orchestrator to match the roles in HPE Aruba Networking Central. Roles are global elements in both HPE Aruba Networking Central and Orchestrator.

**Step 1** Log into **HPE Aruba Networking Central**.

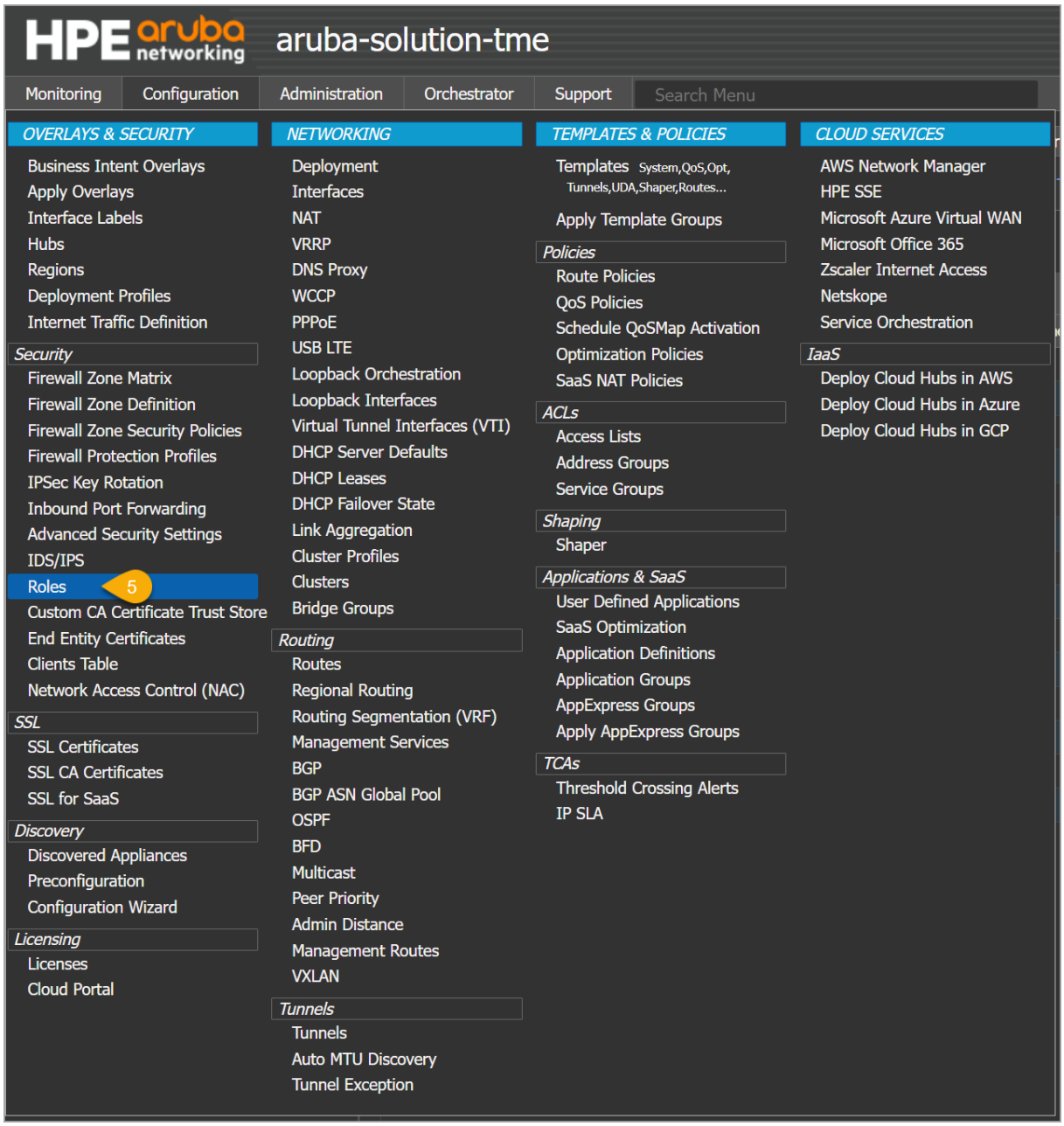
**Step 2** In the filter dropdown, select **Global**, if it is not already selected. On the left menu, select **Security**.

**Step 3** Select the **Client Roles** page.




**Step 4** Make a note of all the roles and their **Policy Identifiers**.

**Step 5** Log into Orchestrator and click **Configuration**. In the **Overlays and Security** section, under the **Security** subsection, click **Roles**.

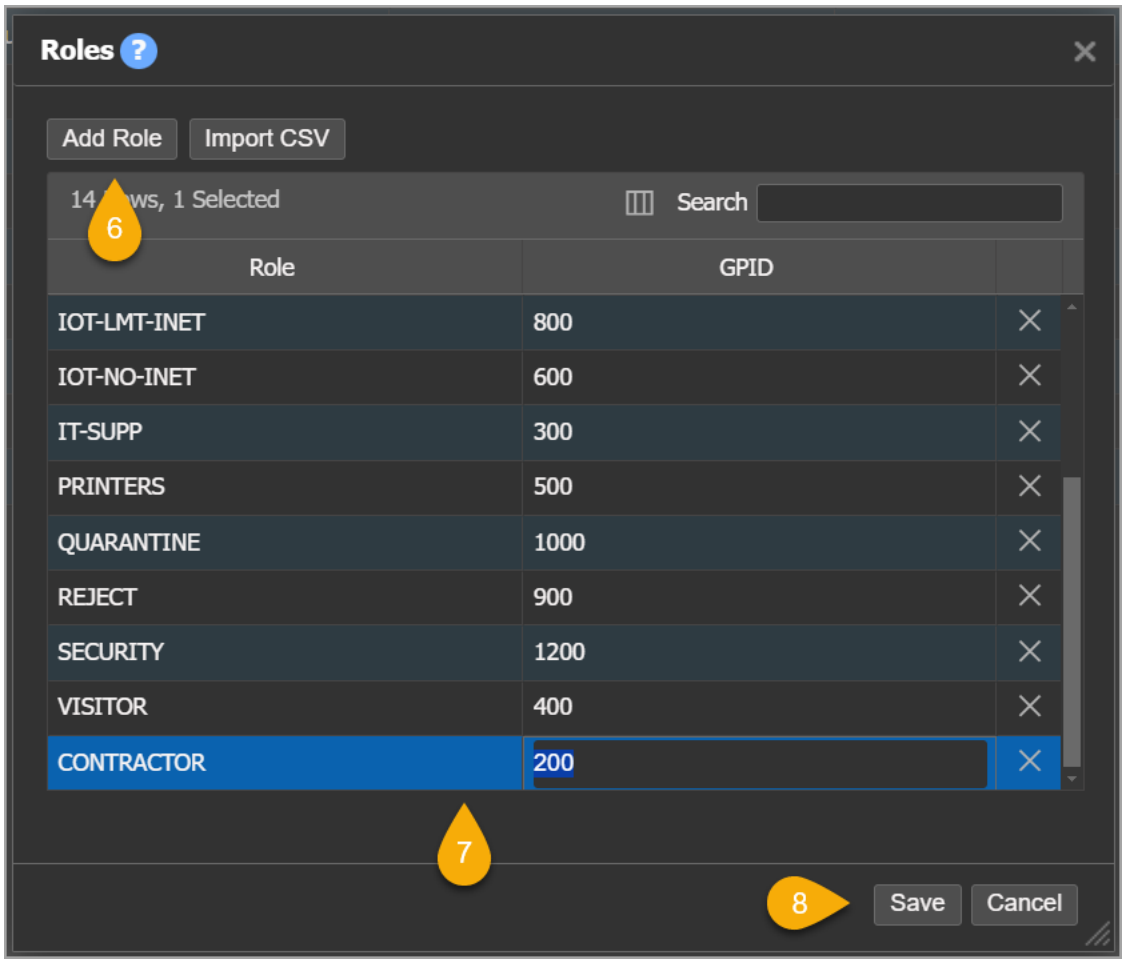



**Step 6** Click **Add Role**.

**Step 7** Enter *CONTRACTOR* in the **Role** field and *200* in the **GPID** field.

**Step 8** Repeat step 6 and 7 for additional roles.

**Step 9** Click **Save**.



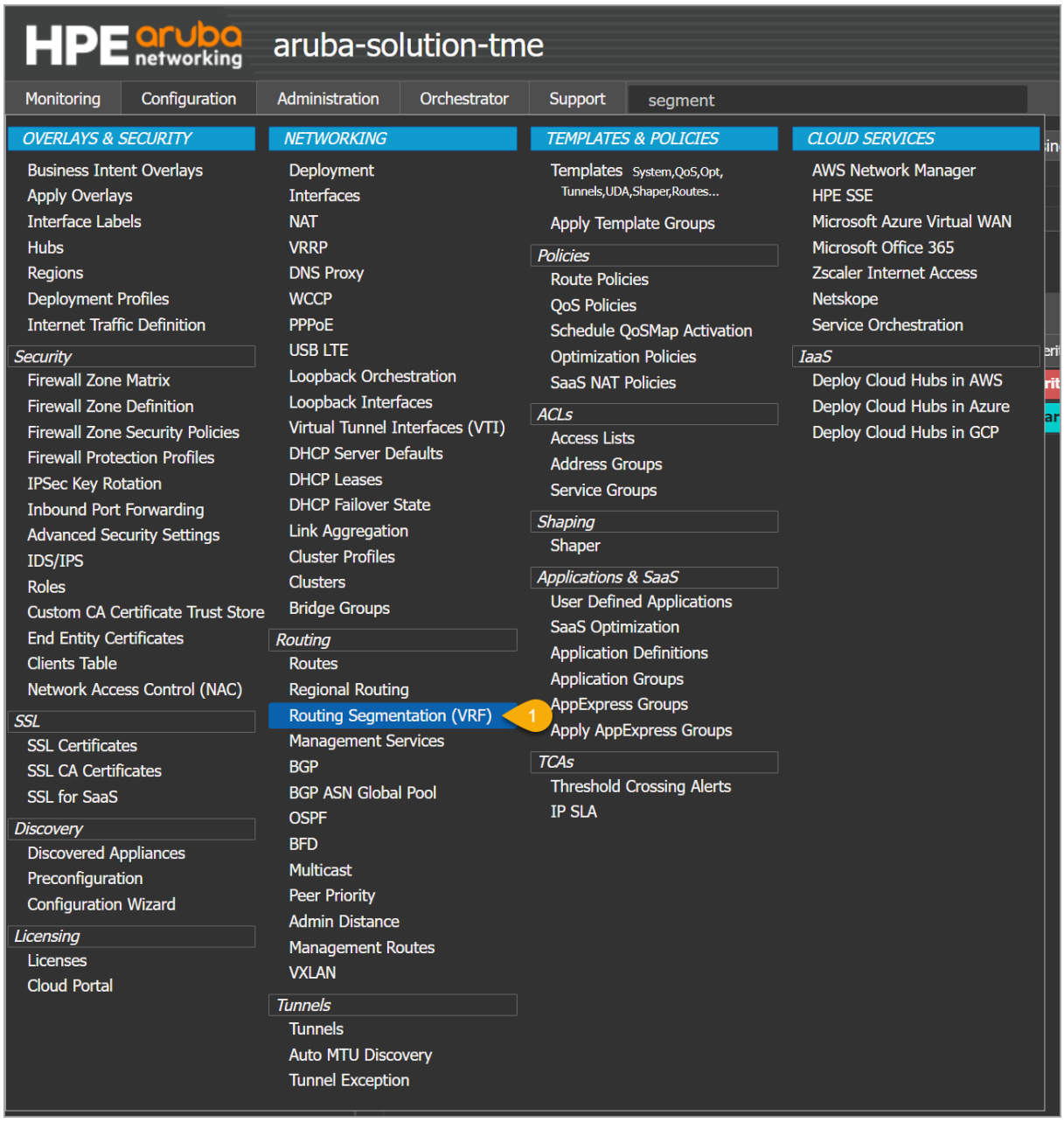

**NOTE:**

Roles are case-sensitive. Ensure that the name and GPID match *exactly* in HPE Aruba Networking Central and Orchestrator

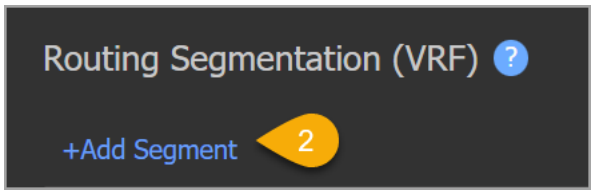
## Adding Segments

EdgeConnect does not interface with the segments, but they must be readable. These steps add the required segments to Orchestrator.

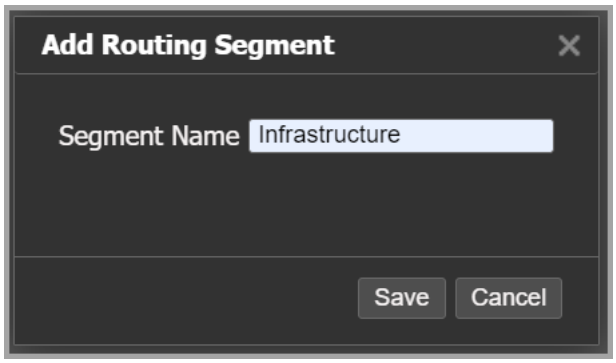
**Step 1** Hover on **Configuration**. In the **Networking** section, **Routing** subsection, and click **Routing Segmentation (VRF)**.




**Step 2** Click **+Add Segment**




**Step 3** Enter *Infrastructure* for Segment Name, then click **Save**.



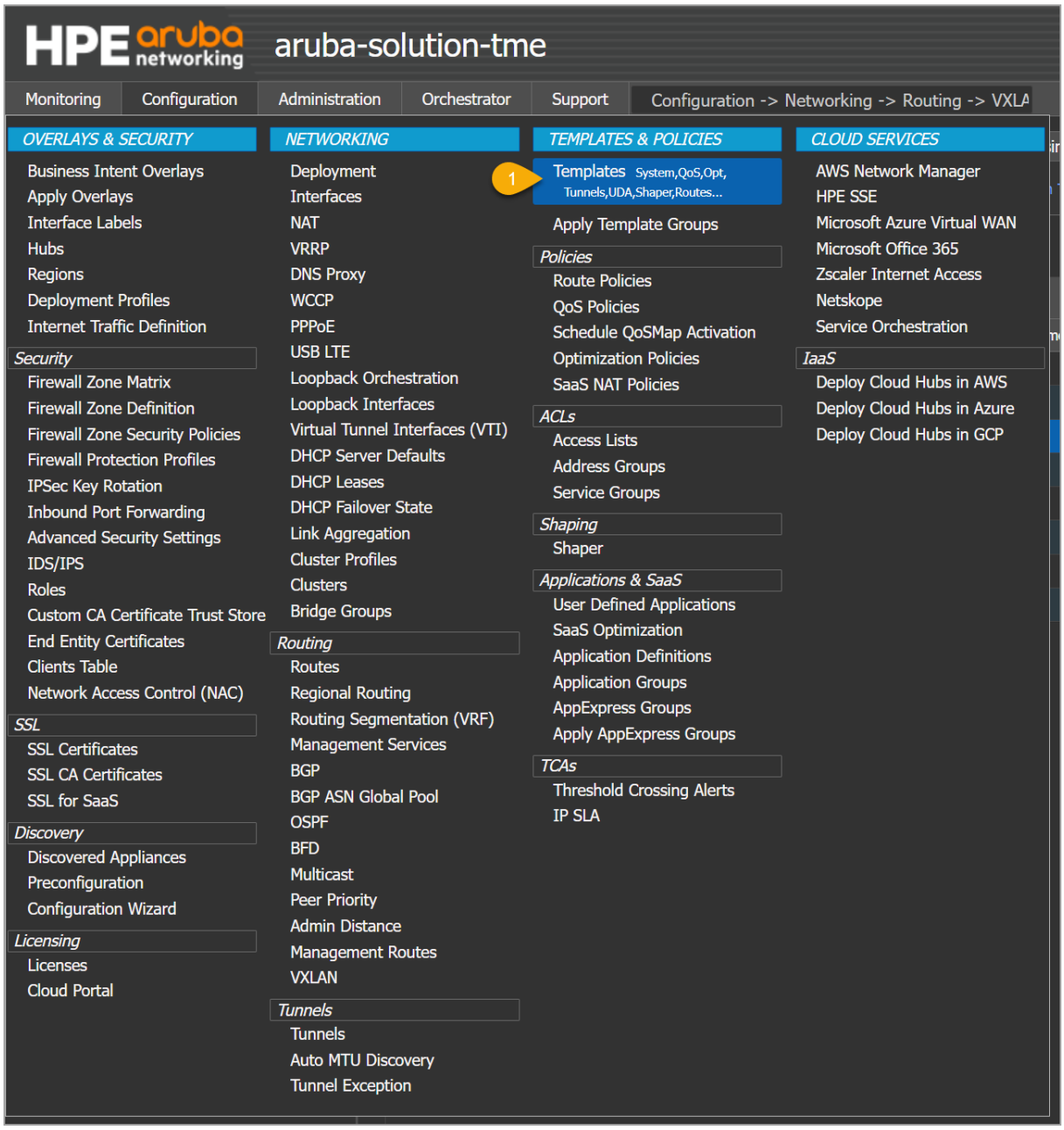

**Step 4** Repeat the steps above to add the **Guest** and **Corporate** segments.

# Configure Templates

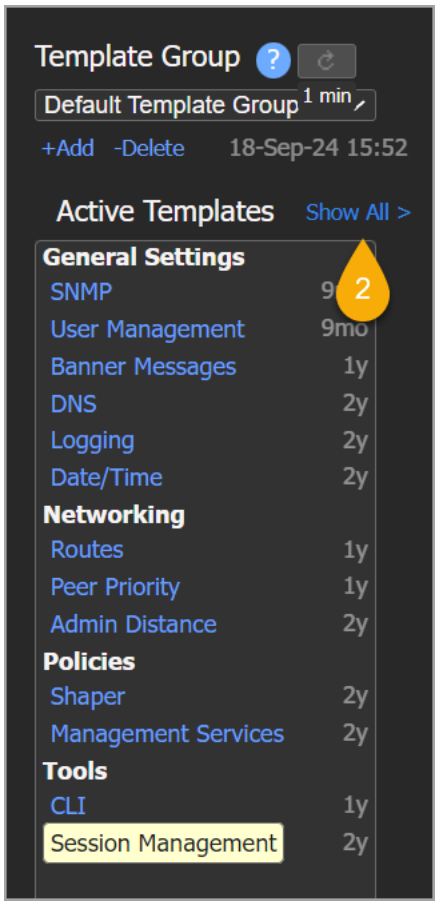
## BGP Route Maps

This template will configure a route-map, used later in this procedure, to set the **BGP Local Preference** to *250*.

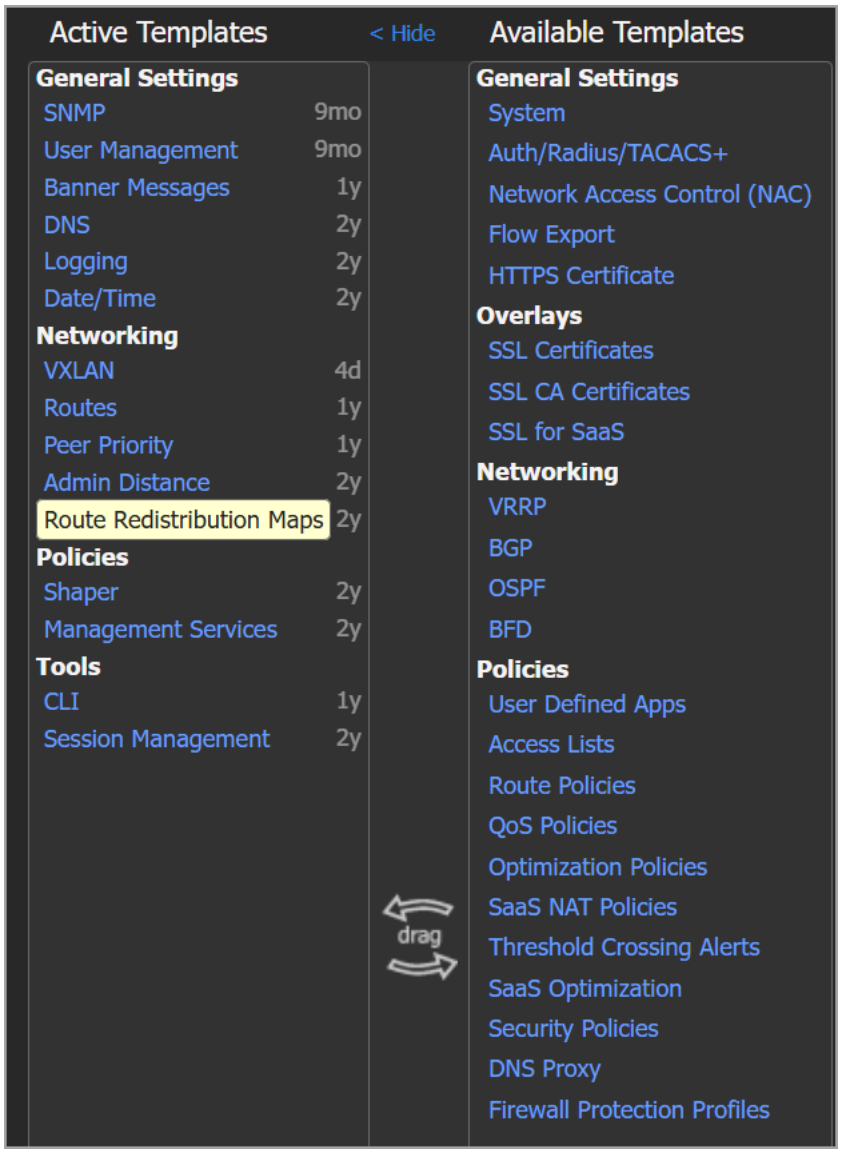
**Step 1** Hover on **Configuration**. In the **Templates & Policies** section, click **Templates**.




**Step 2** In the **Default Template Group** (or the assigned template applied to EdgeConnect), click **Show All**.



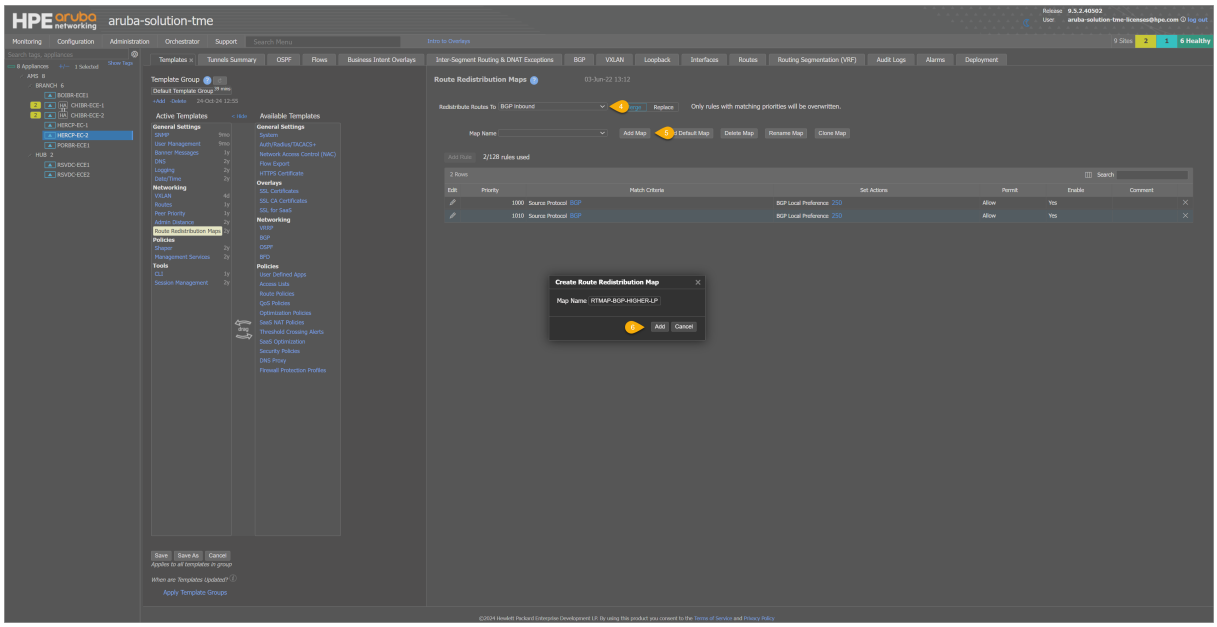

**Step 3** Click and drag the **Route Redistribution Maps** from **Available templates** to **Active Templates**.




**Step 4** For the **Route Redistribution Maps** template, select *BGP Inbound* in the **Redistribute Routes to dropdown, .

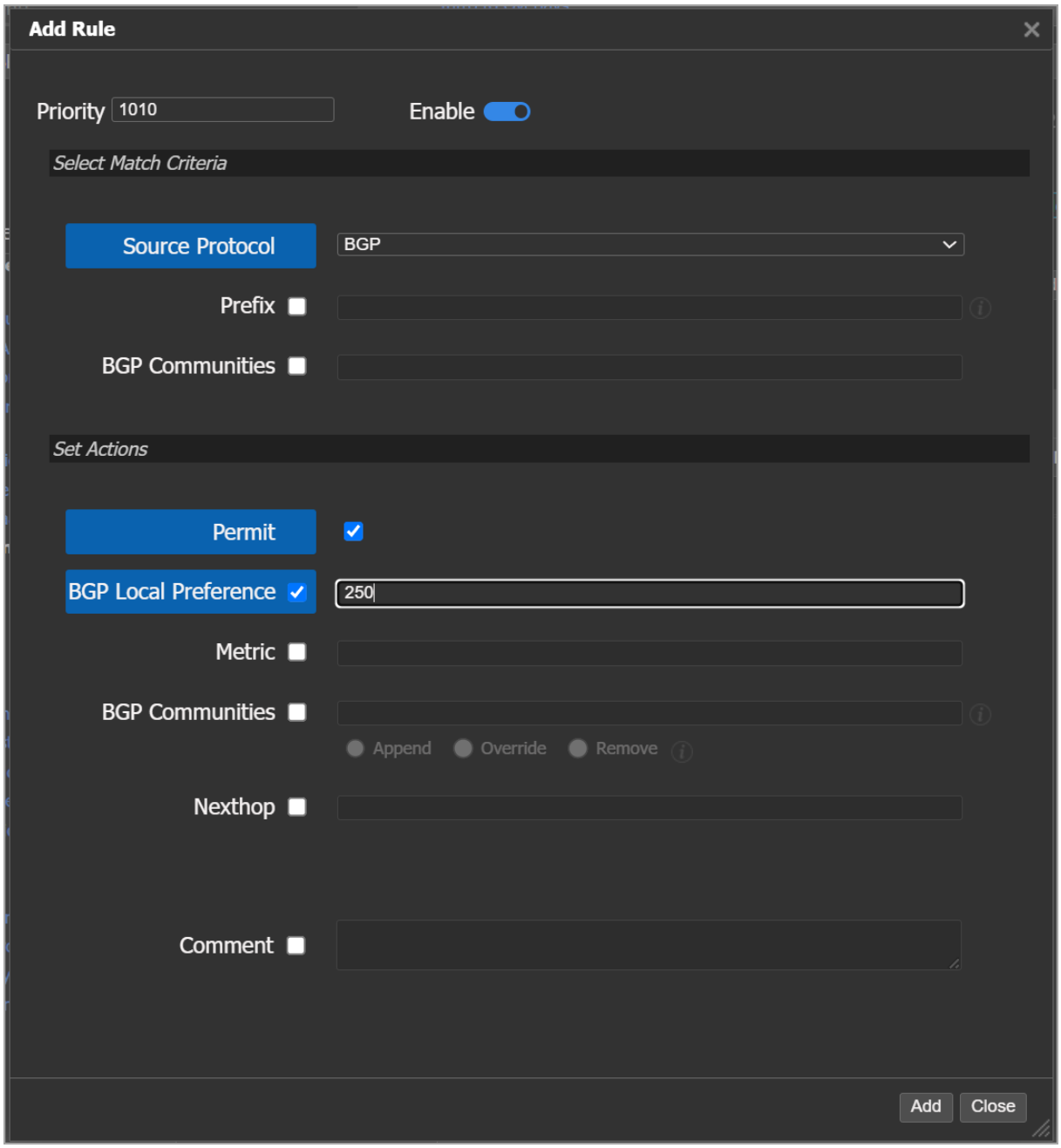
**Step 5** Click **Add Map**.

**Step 6** Enter a **Map Name** of *RTMAP-BGP-HIGHER-LP* and click **Add**.




**Step 7** Click **Add rule**. Complete the following **Set Actions** fields, then click **Add**.

- **Permit**: *checked*
- **BGP Local Preference:** *checked*
- **BGP Local Preference:** *250*

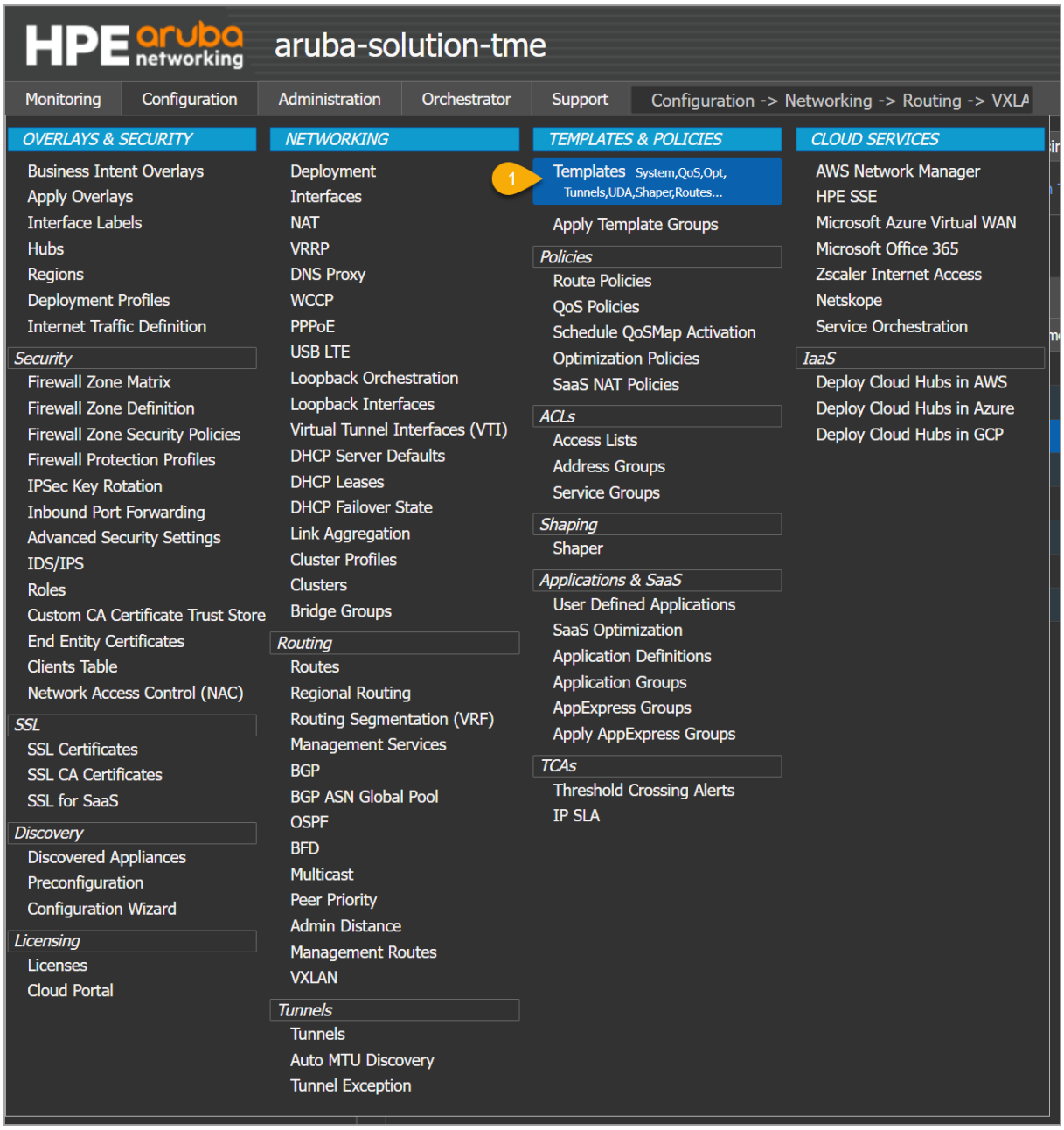



**Step 8** Under the **Template Group**, click **Save**.

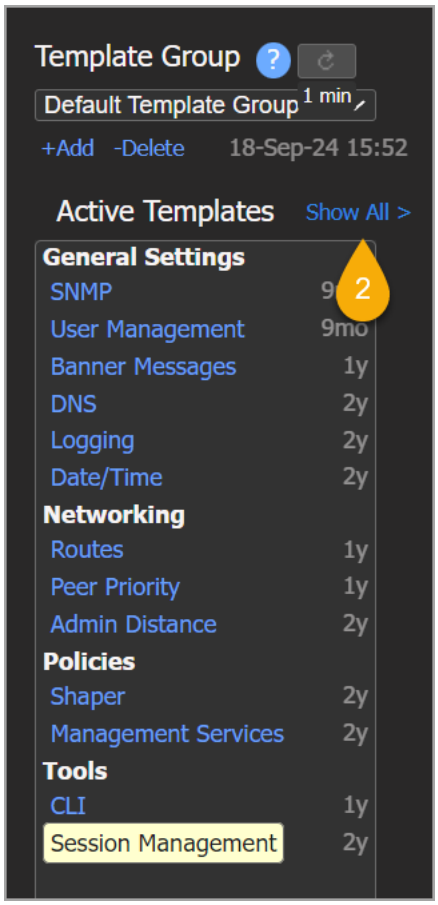
## VNI to Segment Mapping and VTEP Source

VXLAN VNIs are mapped to EdgeConnect segments using a template that applies to all EdgeConnect devices. These VNIs correspond to the same Layer 3 VNIs defined in the NetConductor Fabric Wizard.

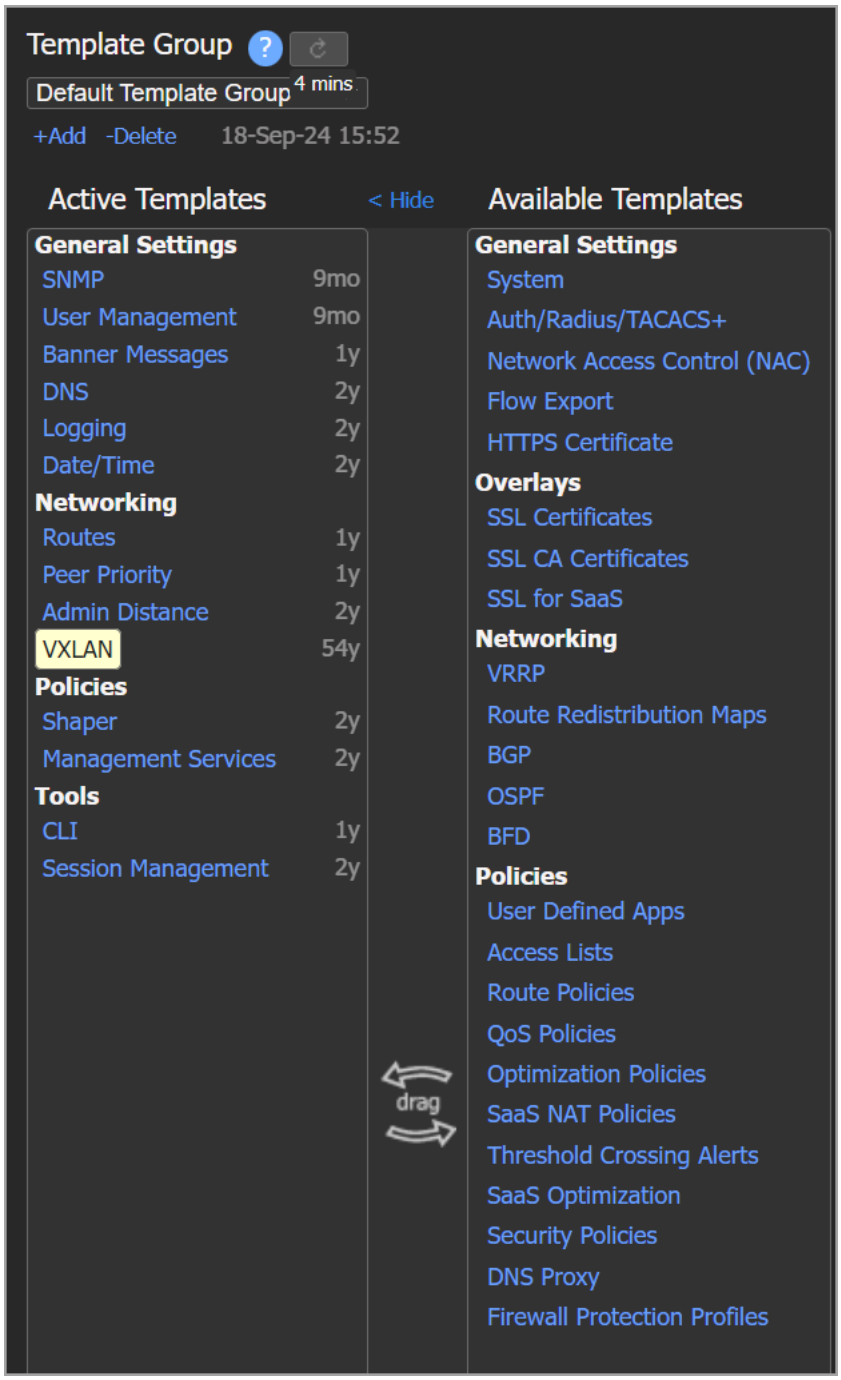
**Step 1** Hover on **Configuration**. In the **Templates & Policies** section, click **Templates**.



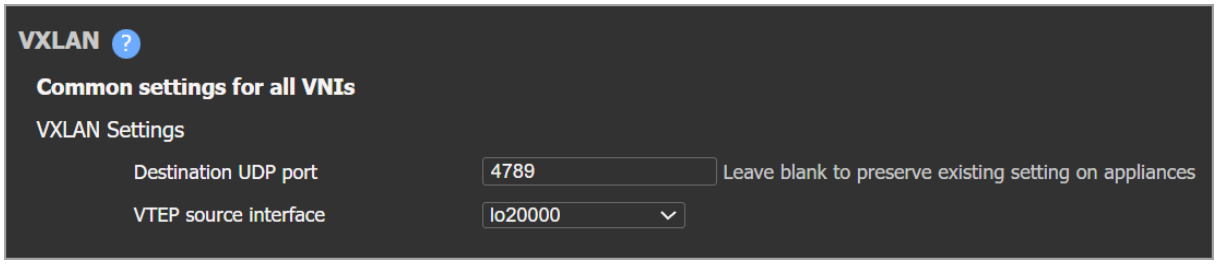

**Step 2** In the **Default Template Group**, (or the assigned template applied to EdgeConnect), click **Show All**.



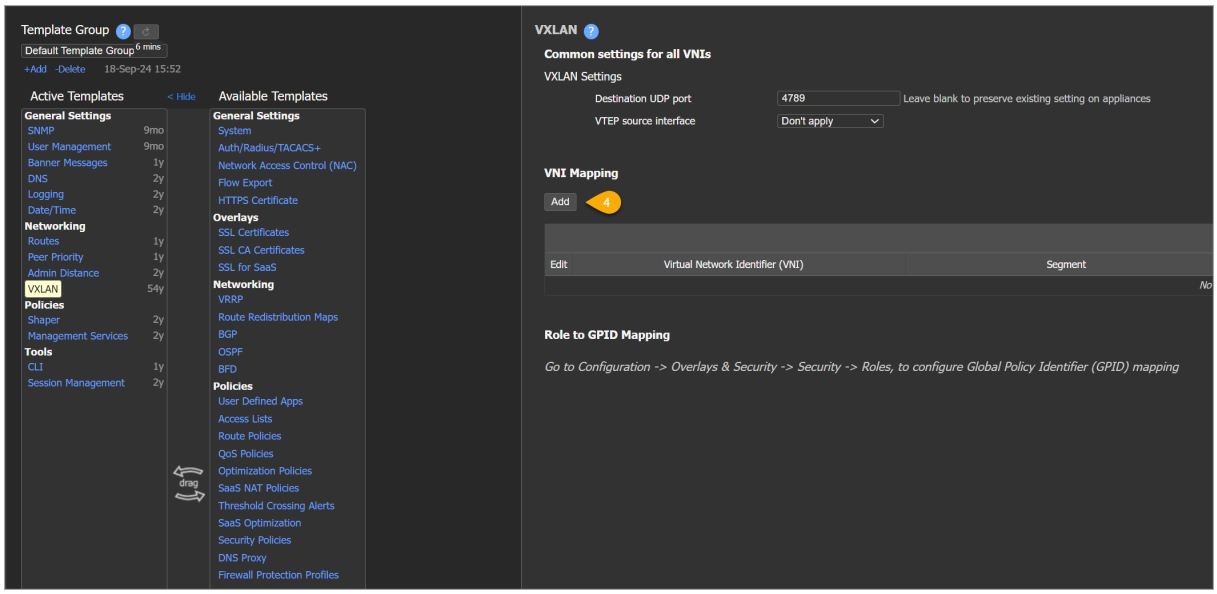

**Step 3** Click and drag the **VXLAN template** from **Available templates** to **Active Templates**.




**Step 4** In the **VXLAN template**, select *lo20000* in the **VTEP source interface** dropdown.

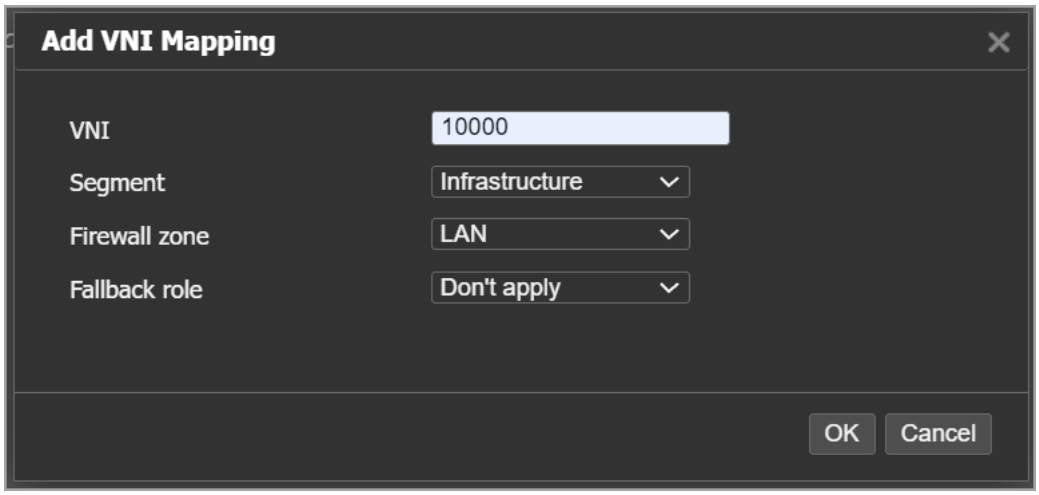



**Step 5** In the **VXLAN Template**, **VNI Mapping** section, click **Add**.



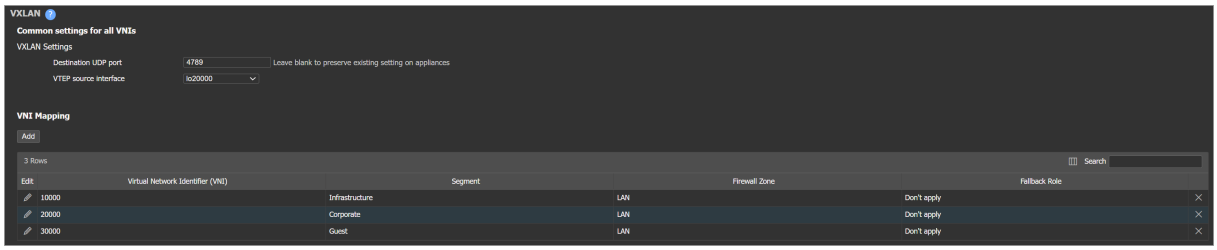

**Step 6** On the **Add VNI Mapping** page, assign the following settings, then click **OK**.

- **VNI**: *10000*
- **Segment**: *Infrastructure*
- **Firewall zone**: *LAN*
- **Fallback role**: *Don't apply*

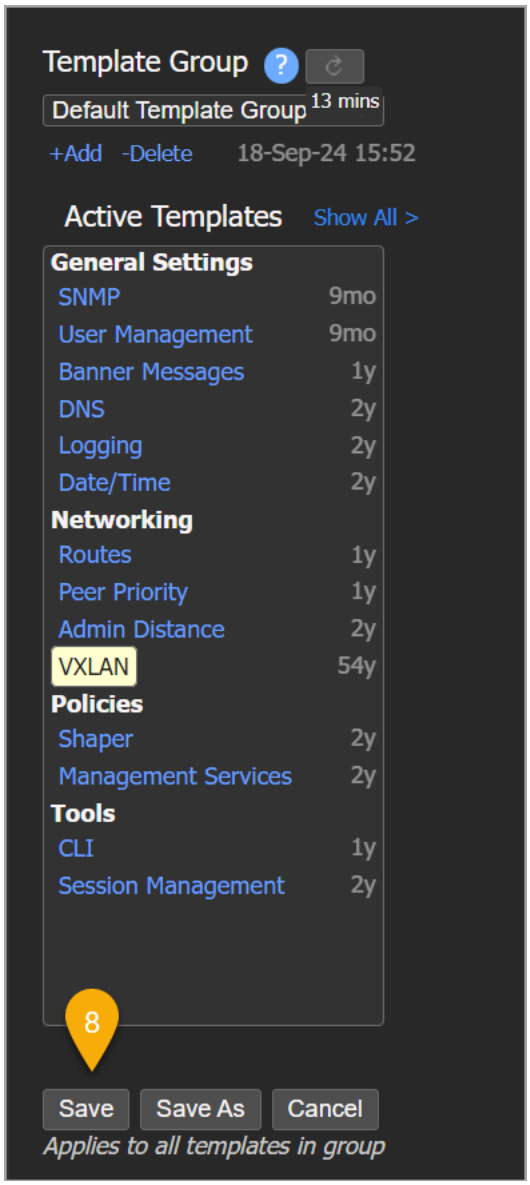



**Step 7** Repeat the above steps for the following VNIs.

| VNI | Segment |
|---|---|
| 20000 | Corporate |
| 30000 | Guest |



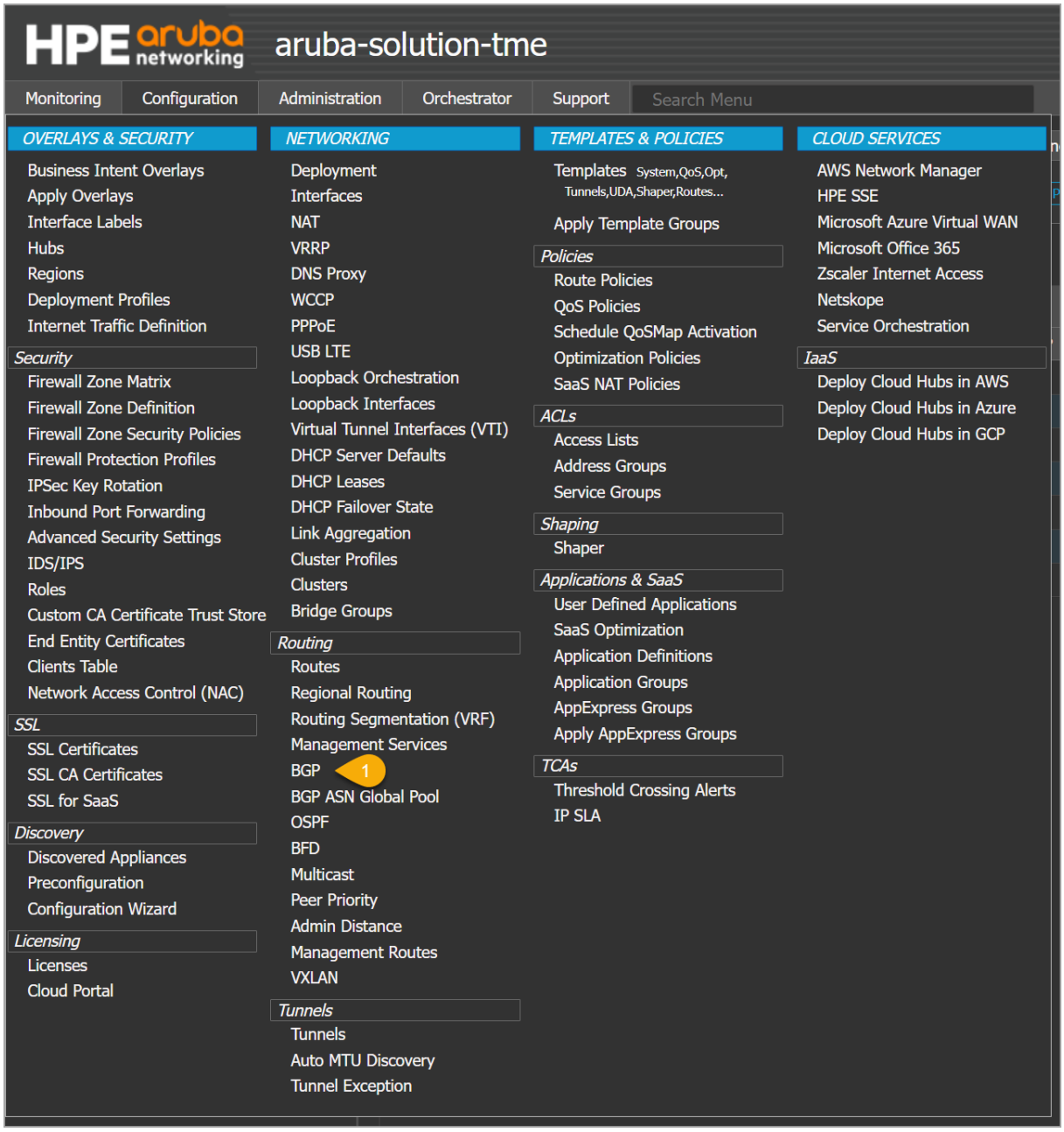

**Step 8** In the **Template Group** window, click **Save**.



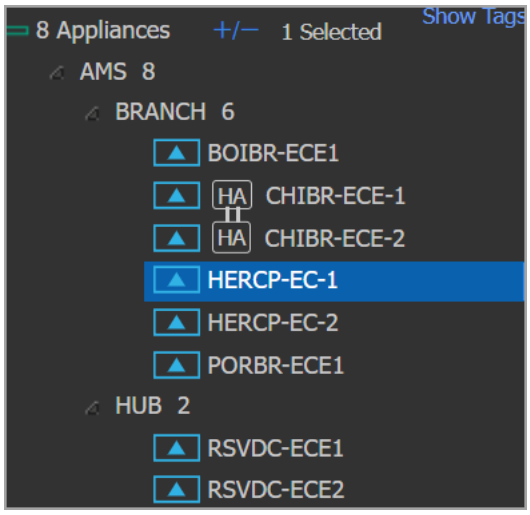
# Configure BGP EVPN on EdgeConnect

This procedure configures the eBGP adjacency between the EdgeConnect gateways and the border switches. EdgeConnect gateways are in BGP ASN 65002 and the NetConductor fabric is in BGP ASN 65001. In order to maintain border symmetry, a route-map is used to set the BGP local preference. After the BGP adjacency is configured, BGP is enabled in each segment to import the routes from EVPN into the routing table.

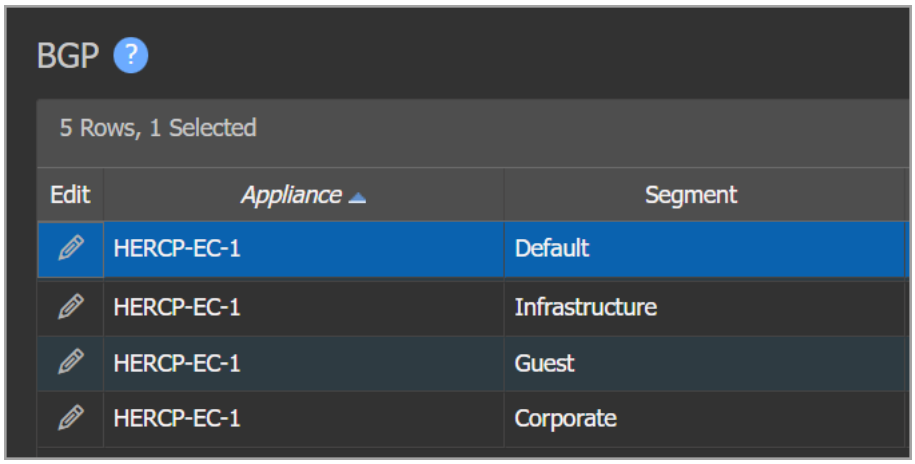
**Step 1** Hover on **Configuration**. In the **Networking** section, **Routing** subsection, click **BGP**.




**Step 2** Select the first EdgeConnect, HERCP-EC-1, from the sidebar.

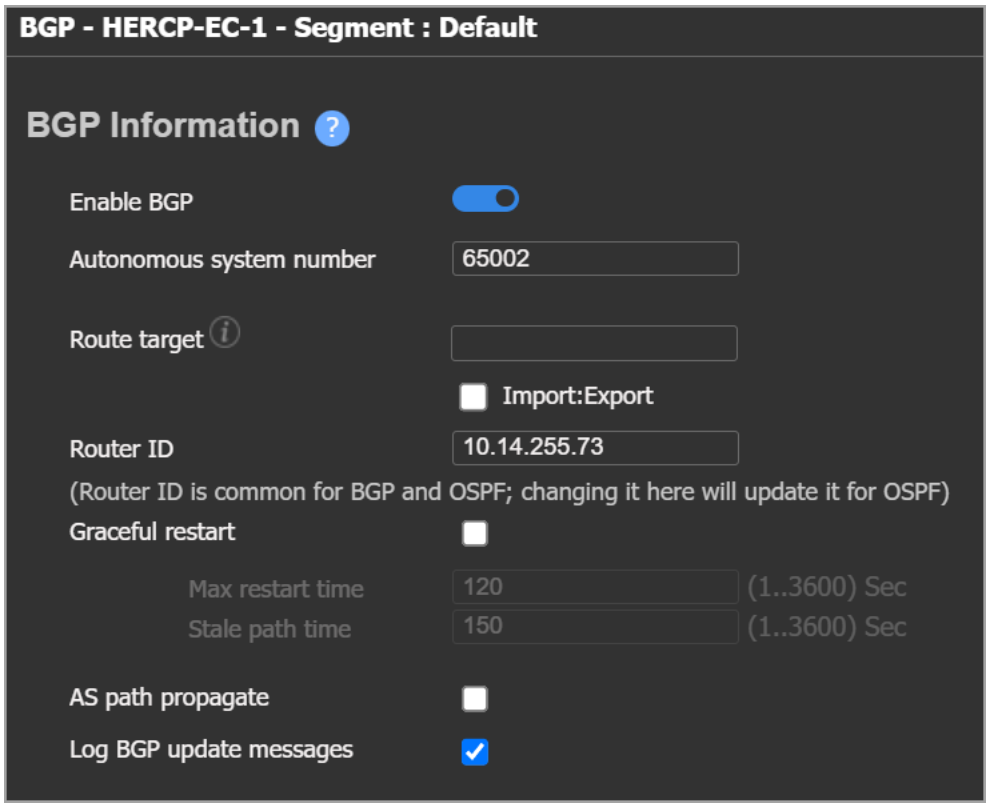



**Step 3** Click the **Edit** icon (pencil) beside the default segment.

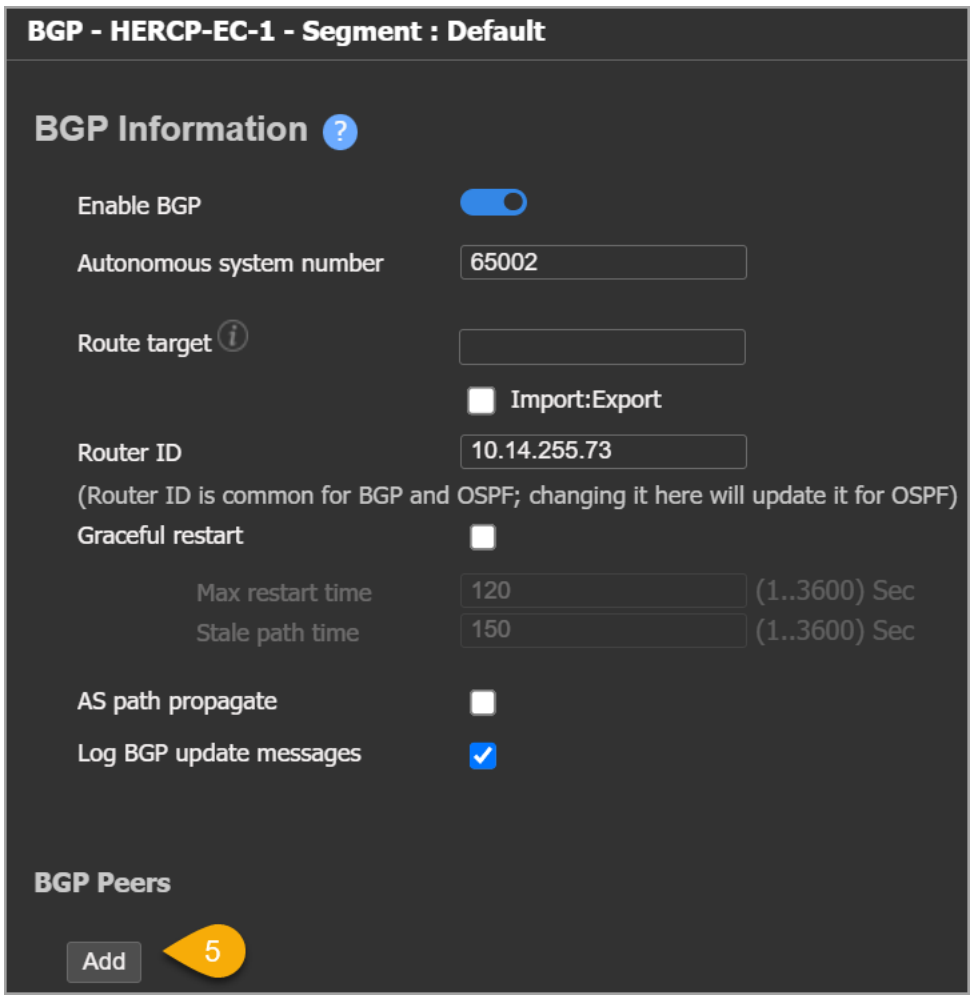



**Step 4** Assign the following setting. The **Router ID** is the loopback IP for the EdgeConnect.

- **Enable BGP Toggle:** *Enabled*
- **Autonomous system number:** *65002*
- **Router ID:** *10.14.255.73*

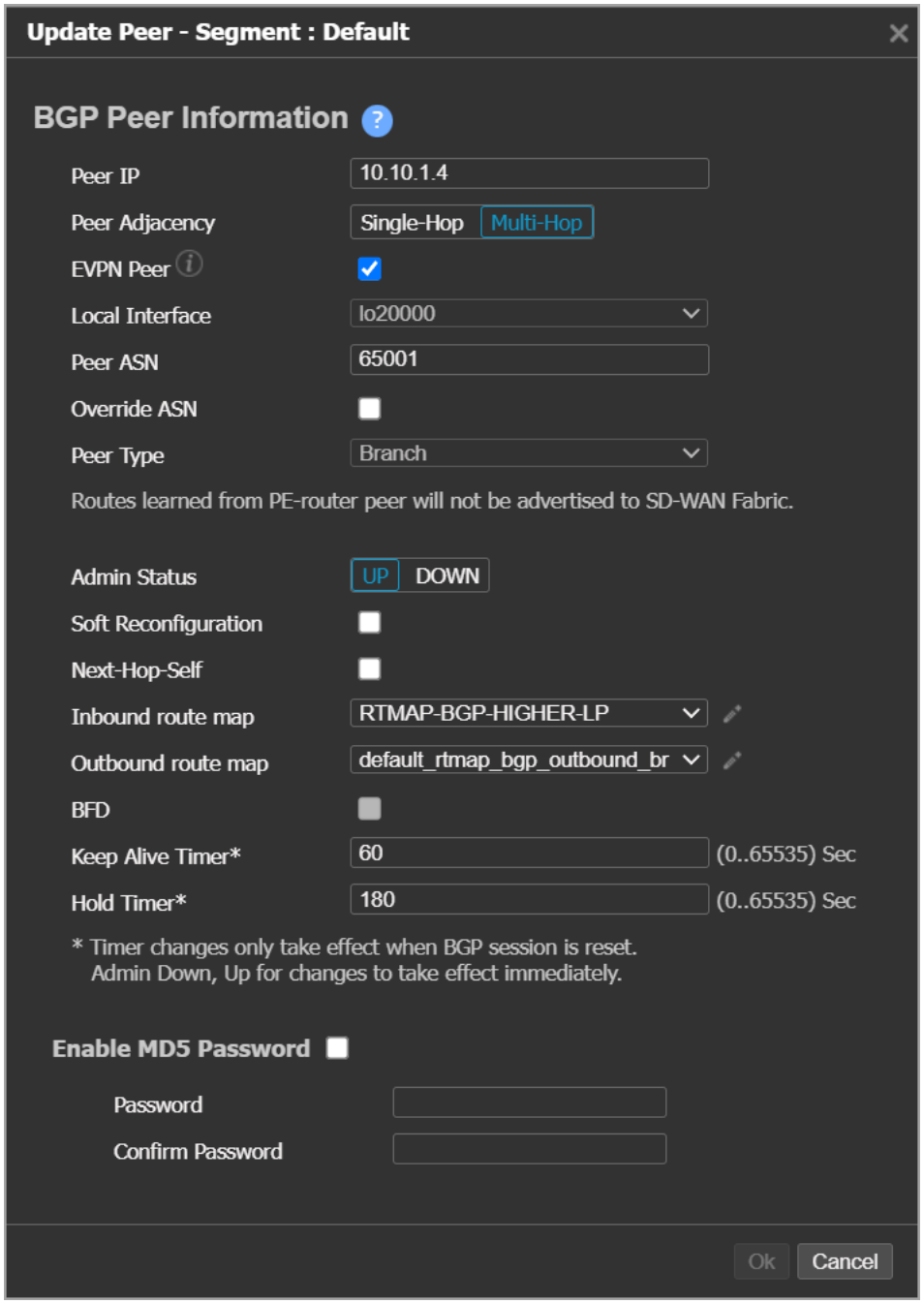



**Step 5** Under **BGP Peers**, click **Add**.



**Step 6** Assign the following settings, then click **Ok**.

- **Peer IP:** *10.10.1.4*
- **Peer Adjacency:** *Multi-Hop*
- **EVPN Peer:** *checked*
- **Peer ASN:** *65001*
- **Inbound route map:** *RTMAP-BGP-HIGHER-LP*
- **Keep Alive Timer**: *60*
- **Hold Timer**: *180*




**NOTE:**

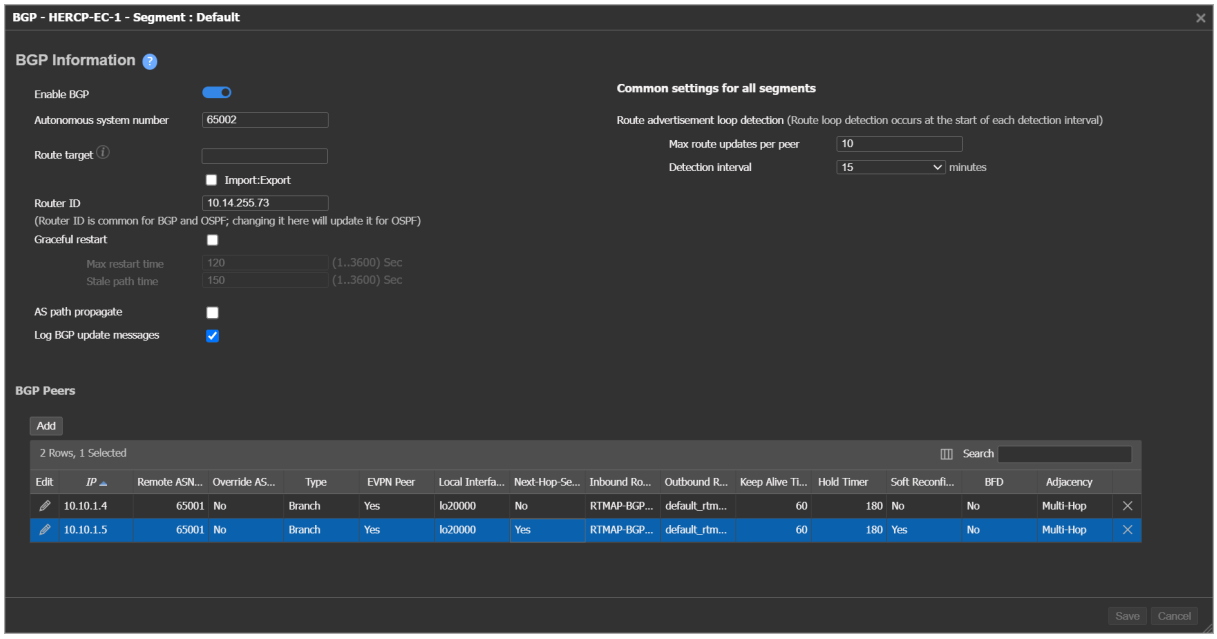
The peer IP is the Loopback0 interface on the border.

**NOTE:**

Keep alive and hold timer are modified to match the default AOS-CX timers.

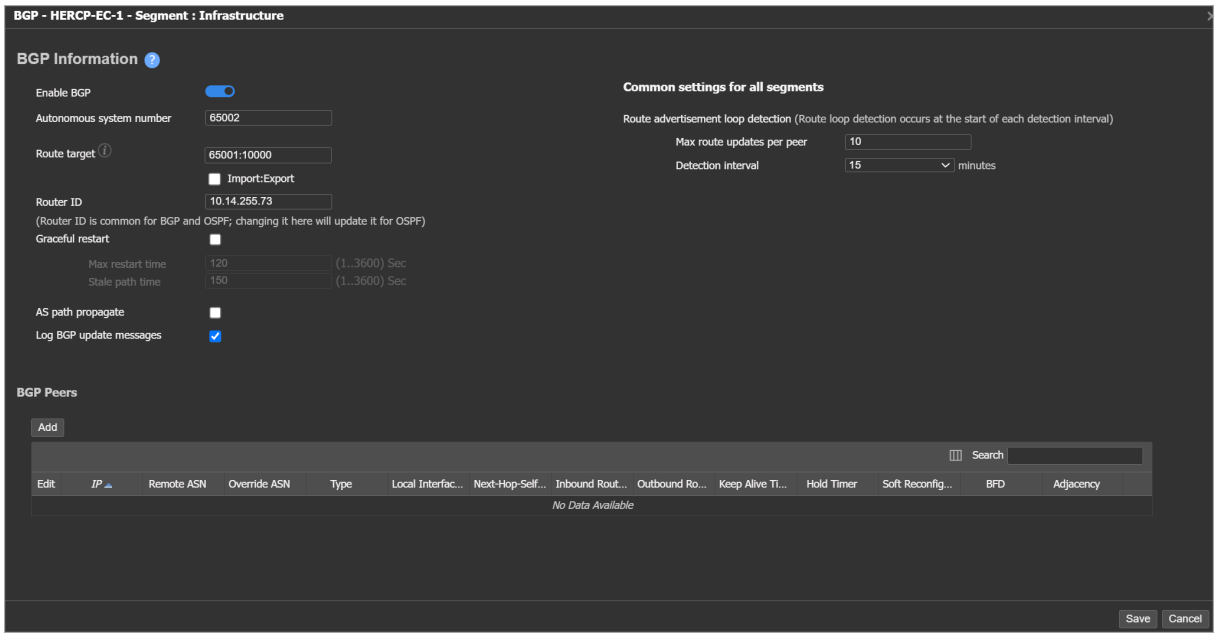
**Step 7** Repeat step 4 to 5 to create a BGP peer for the second border.

**Step 8** Click **Save**.




**Step 9** Click the **Edit** icon (pencil) beside the Infrastructure segment. Assign the following settings, then click **Save**.

- **Enable BGP:** *Enabled*
- **Autonomous system number:** *65002*
- **Route Target:** *65001:10000*
- **Router ID:** *10.14.255.73*



**Step 10** Repeat step 9 for the **Guest** and **Corporate** segments.

**Step 11** Repeat Steps 2 to 8 for the second EdgeConnect **HERCP-EC-2**.

**NOTE:**

When creating the BGP peering for the second EdgeConnect, **do not change** the inbound route-map. The second EdgeConnect should use the default local-preference of 100, while the primary EdgeConnect should have a local-preference of 250.

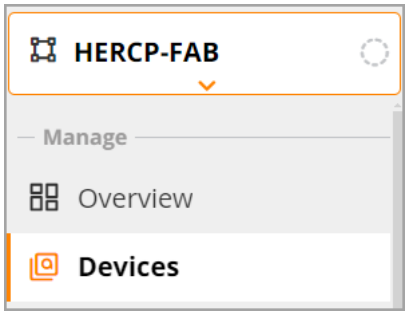
## Configure BGP EVPN on the Border Switches

This procedure configures the border switches and their eBGP adjacency with the EdgeConnect gateways. EdgeConnect gateways are in BGP ASN 65002 and the NetConductor fabric is in BGP ASN 65001. A route-map that sets the BGP local-preference is used to prefer routes from the primary EdgeConnect gateway. An AS path list matches routes originating only from the EdgeConnect gateway's autonomous system and sets the local-preference to 250. This configuration is then applied to the primary EdgeConnect gateway neighbor.

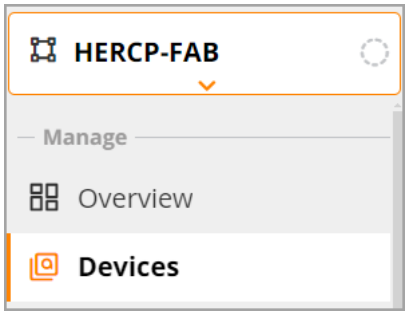
BGP next-hop-self is configured on the BGP adjacencies to the route-reflectors in the fabric. This **required** configuration sets the border as the next-hop for any routes advertised in the fabric from the EdgeConnect gateways.

**Step 1** Log into **HPE Aruba Networking Central**.

**Step 2** In the **Global** dropdown, select the switch group. In this sample procedure, the group is **HERCP-FAB.**




**Step 2** On the left menu, select **Devices**.

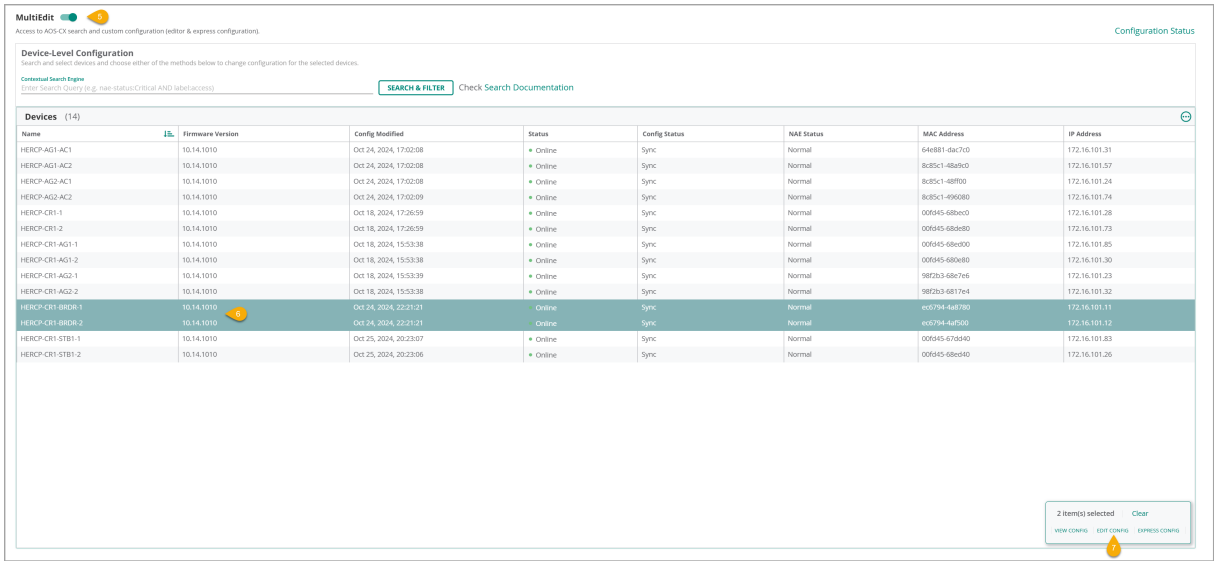



**Step 3** Select **Switches**, then select **Config**.


**Step 4** Enable the **MultiEdit** toggle.

**Step 5** Select the two border switches.

**Step 6** Click **Edit Config**.




**Step 7** Add the following configuration to the MultiEdit Interface and click **Save**.

```
ip aspath-list HERNDON-AS-MATCH seq 10 permit 65002$
route-map INCREASE-LOCAL-PREF permit seq 10
    match aspath-list HERNDON-AS-MATCH
    set local-preference 250
router bgp 65001
    neighbor 10.14.255.73 remote-as 65002
    neighbor 10.14.255.73 ebgp-multihop 5
    neighbor 10.14.255.73 update-source loopback 0
    neighbor 10.14.255.74 remote-as 65002
    neighbor 10.14.255.74 ebgp-multihop 5
    neighbor 10.14.255.74 update-source loopback 0
    address-family l2vpn evpn
        neighbor 10.14.255.73 activate
        neighbor 10.14.255.73 route-map INCREASE-LOCAL-PREF in
        neighbor 10.14.255.73 send-community extended
        neighbor 10.14.255.74 activate
        neighbor 10.14.255.74 send-community extended
```

**Step 8** Use the MultiEdit Interface to add the following configuration, then click **Save**.

```
router bgp 65001
    address-family l2vpn evpn
        neighbor 10.10.1.0 next-hop-self
        neighbor 10.10.1.1 next-hop-self
```


## Routing Considerations

After a NetConductor Fabric is deployed and extended via SD-WAN multi-site, the fabric VRFs may become isolated from the rest of the network. Make sure to plan for and address this. **If one of the following methods is not implemented, the fabric remains unreachable.**

Common methods to prevent VRF isolation include:

- If VRF-based segmentation is already in place, continue extending the VRFs at the hub EdgeConnects using an EVPN handoff (if supported by the LAN-side device) or a VRF-lite handoff.
- If VRF segmentation is not widely used in the environment, consider merging the VRFs through a firewall at the hub. Based on policy, the firewall can then route traffic back into the global routing table.

# Campus Switch Reference Configuration

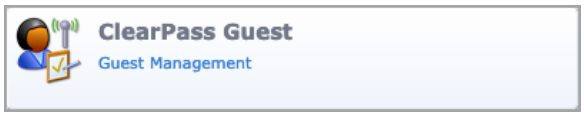
Aruba ESP offers a breadth of services, including onboarding, provisioning, orchestration, analytics, location tracking, and management. The configuration for the complete configuration for the network infrastructure can be found in this section.

# Appendix A: Visitor WLAN ClearPass Details

This section outlines the procedure to collect captive portal information and VRRP VIP information from ClearPass Policy Manager that is needed to configure Visitor WLAN.

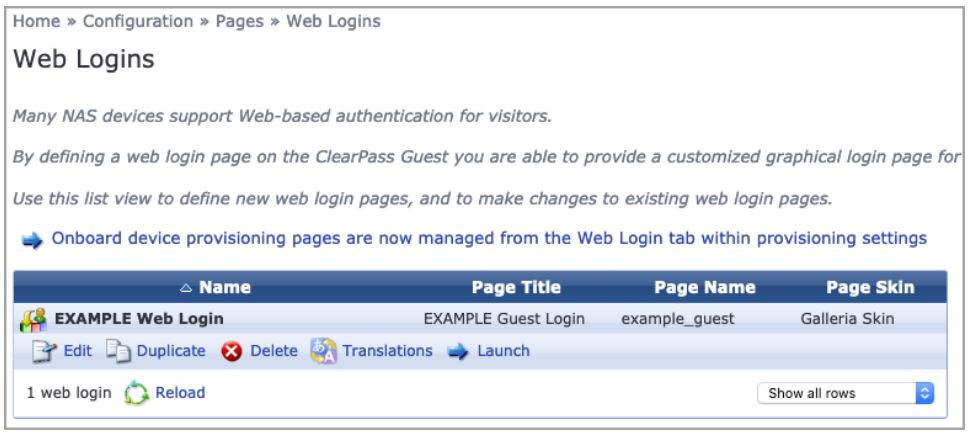
## Find the Captive Portal Information

**Step 1** Open a new browser tab, connect to one of the ClearPass servers, and login to ClearPass Guest with administrator credentials.



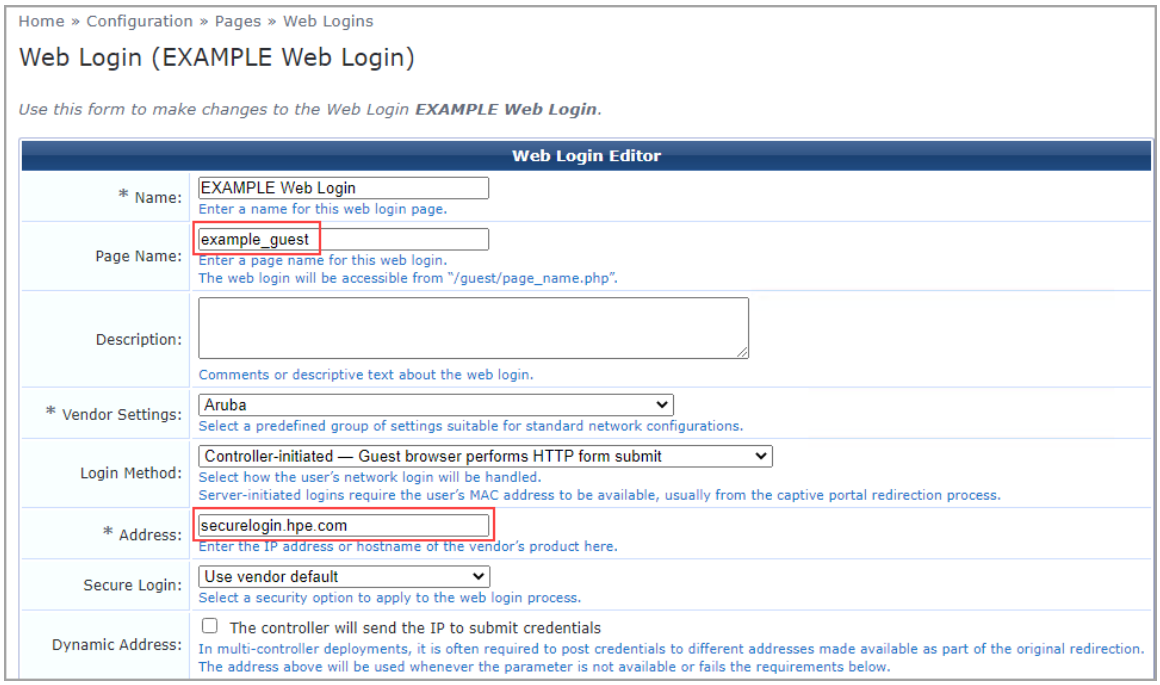

**Step 2** On the left navigation menu, select **Configuration**, click the **+** (plus sign) to expand **Pages**, then select **Web Logins**.

**Step 3** Select the name of the already configured **Web Login**, then click **Edit**.




**Step 4** Copy the values found in **Page Name** and **Address** and store them for later use.

**Step 5** In the top menu, select **Logout**.




**CAUTION:**

Some legacy versions of AOS8 use a certificate with the name of securelogin.arubanetworks.com. All versions of AOS released since 2020 now use a certificate with the name securelogin.hpe.com. If this is a mixed environment where the legacy certificate is still in use, you may need to clone/duplicate the page to use another certificate. It is best practice to replace the certificate with a publicly signed one. If the certificate is replaced, this issue is avoided, but the **Address** in the web login must reflect the Common Name (CN) assigned to the certificate when it was issued.

**NOTE:**

This procedure uses the default certificate. It is best practice to replace the certificate with a publicly signed one. See the caution section above.

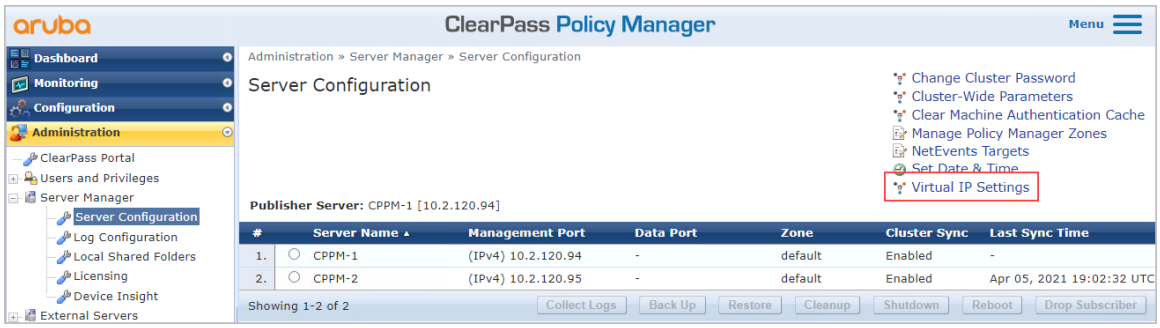
## Find the ClearPass VRRP VIP

When following best practice and using more than one ClearPass Server for network authentication, the captive portal address or hostname in the WLAN **Access Policy** must be the VRRP address of the ClearPass servers. The following procedure shows how to find the VRRP address in ClearPass Policy Manager.

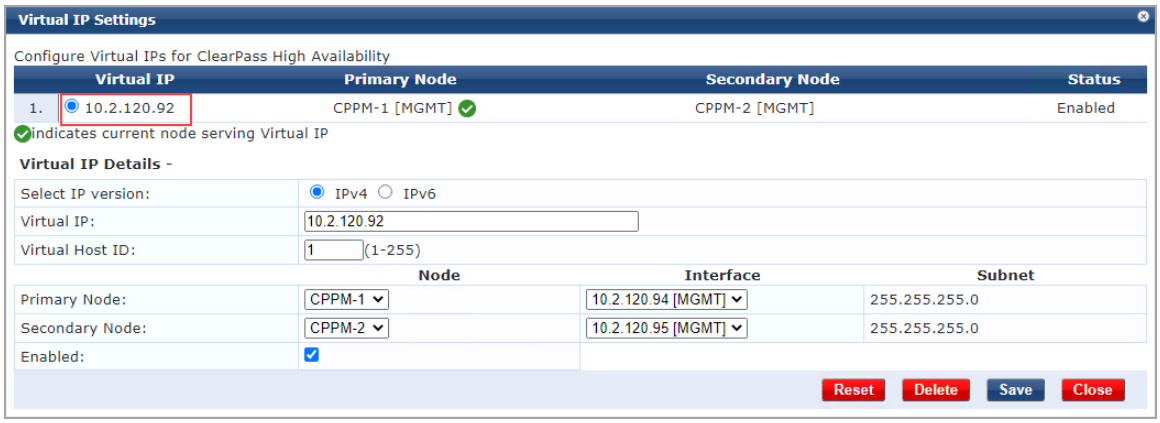
**Step 1** Open a new browser tab, connect to one of the ClearPass servers, and login to ClearPass Policy Manager with administrator credentials.

**Step 2** On the left navigation menu, select **Administration**, click the **+** (plus sign) to expand **Server Manager**, then select **Server Configuration**.

**Step 3** On the **Server Configuration** page in the top right, select **Virtual IP Settings**.




**Step 4** On the **Virtual IP** Settings page, observe and record the **Virtual IP** configured for the CPPM cluster.




**Step 5** Use *nslookup* or other operating system specific mechanism to confirm that the Virtual IP address above has a resolvable host name. Use the host name in the **Captive Portal Profile: IP or Hostname:** field when configuring a WLAN for captive portal authentication.

# Validated Hardware and Software

The following hardware and software versions were validated for this guide. For compatibility, please upgrade to at least the versions listed below.

**Wired Core**

| Product Name | Software Version |
|---|---|
| Aruba CX 8400 | 10.10.0002 |
| Aruba CX 6400v2 | 10.10.1010 |

**Wired Aggregation**

| Product Name | Software Version |
|---|---|
| Aruba CX 8360 | 10.10.0002 |
| Aruba CX 8325 | 10.10.0002 |
| Aruba CX 8320 | 10.10.0002 |
| Aruba CX 6400 | 10.10.0002 |

**Wired Access**

| Product Name | Software Version |
|---|---|
| Aruba CX 6300 | 10.10.0002 |
| Aruba CX 6400 | 10.10.0002 |
| Aruba 3810 | 16.11.0005 |
| Aruba 2930M | 16.11.0005 |

**Wireless Gateways**

| Product Name | Software Version |
|---|---|
| Aruba 7200 | 10.4.0.0 |

**Wireless Access Points**

| Product Name | Software Version |
|---|---|
| Aruba AP 500 Series | 10.4.0.1 |
| Aruba AP 300 Series | 10.4.0.1 |

**Management and Orchestration**

| Product name | Software version |
|---|---|
| Aruba Central | 2.5.6 |
| Aruba ClearPass Policy Manager | 6.9.11 |


**www.arubanetworks.com**

**3333 Scott Blvd. Santa Clara, CA 95054**
1.844.472.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550

ESP-CPDP