

ESP Campus Deploy

Validated Solution Guide

Aruba Solution TME

May 28, 2025

Table of Contents

ESP Campus Deploy	4
Document Conventions	4
Introduction	5
Purpose of This Guide	5
Deploying the Campus Network	7
Planning for Deployment	8
HPE GreenLake	12
Aruba Central	12
Campus Wired Connectivity 2	27
Preparing Campus Switches 2	28
Switch Installation	28
Physical Cabling	30
Switch Profiles and Interface Groups	31
DHCP	31
Switch Group Configuration	31
Wired Core Configuration 4	13
Configure the Core Switch Group 4	13
Access and Services Aggregation Configuration 5	;4
Configure the Aggregation Switch Groups	54
Wired Access Configuration	57
Configure the Access Switch Groups	57
Campus Wireless Connectivity 8	37
Wireless Group Configuration 8	88
Configure a Central Group for Wireless Management	38
Configure AP Settings for Group	39
Configure Gateway Settings for Group	91
Gateway Devices Configuration 9	6
Configure Gateway VLANs)6
Enable Physical Interfaces)8
Configure Port Channels)9
Configure the Default Gateway)3
Configure the Gateway Base Features)3
Configure Layer 2 Gateway Clustering)8
Wireless Access Configuration 11	2
User Experience Insight Deploy 12	27
Prepare for UXI Deployment	27
Deploy UXI on GLP	<u>29</u>

Campus Services	153
Al Insights Configuration	154
AirMatch Configuration	155
ClientMatch Configuration	156
Aruba Central NetConductor	157
Underlay Orchestration Plan the Underlay	158 158 159
Overlay Fabric Orchestration Network Review Device Onboarding Considerations Configure Role Policy Deploy the Fabric Configure Wireless Integration Configure External Connectivity ClearPass Integration Edge Port Configuration Verification Brownfield Considerations	 167 169 169 172 181 199 200 200 201 207
EdgeConnect SD-WAN Multi-Site Prerequisites Configure MTU Define Roles Adding Segments Configure Templates Configure BGP EVPN on EdgeConnect Configure BGP EVPN on the Border Switches Routing Considerations	208 209 212 215 217 228 233 235
Campus Switch Reference Configuration	236
Appendix A: Visitor WLAN ClearPass Details	237
Validated Hardware and Software	240

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 gu	ide
---	-----

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-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 homepage.



Step 1 Login to GreenLake and select the workspace.

Step 2 Click the Services tab on the top.

HPE GreenLake	Orange TME $$	1	Home	Services	Devices
				2	

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.





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

2000		
DG9-AGG01		
lake this group compatible with New Central	-	
roup will contain:		
Access points		
Gateways		
Switches		5
		•

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.

← Add Group		
Type of switches used in this group:		
AOS-CX switches		6
Make these the preferred group settings	Cancel	Add



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.

Customer: Orange TME			
🗟 Global ┥ 📀	Network structure Platform integration		
Devices	Combine devices with common configuration	n into a single group to apply the same configuration	Q +
⊑ ī Clients			
🚉 Guests			
Applications			V
Security	BDG9-AGG01 (0)	Emer [New Central]	
🗞 Network Services			
- Analyze			
✿ Alerts & Events			
🗹 Audit Trail			
🖏 Tools			
🛍 Reports			
- Launch			
App Catalog			
- Maintain			
Firmware			
🔓 Organization			



Step 4 Provide the password. Click Save.

SET DEVICE PASSWORD	
Please specify an administrator password for devices in this group. Further configuration of the group will be	prohibited until a password is set.
Administrator password	
	9
	CANCEL



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.





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

CREATE NEW SITE	×
CITE MANE	
FXAMPLE SITE	
STREET ADDRESS	
123 Any Street	
СІТҮ	
Santa Clara	
United States	▼
California	▼
ZIP/POSTAL CODE	
95054	
LATITUDE (OPTIONAL)	
LONGITUDE (OPTIONAL)	
Add 🥌	



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.

~	Unprovisioned devices (5)			
	Device Name	Туре	Serial Number	MAC Address
	RSVCP-AG2-AC4-1	Aruba CX	TW3BLZB0V0	4C:D5:87:7A:28:80
				1 item(s) selected Clear
				5 3



Step 6 Select the Destination group, then click Move.

I selected devices will be	moved from 'Unprovisioned devices' group to	
Destination group BDG9-AGG01	~	
Destination group setti	ngs:	
AOS-CX switches		
AOS-CX switchesNew Central Group		
 AOS-CX switches New Central Group The devices will adopt th 	e destination group configuration	
 AOS-CX switches New Central Group The devices will adopt th	e destination group configuration	Ø



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**.

ll Devices		164				-
				RSVCP-AG2-AC4	CP-RSVACC	SWITCH
SP-RS01	8501 foothills blvd	0	+			
New Site			29 Sites	Remove Device(s)	dafault	SWITCH

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.

May 28, 2025

aruba	Support				¢	CONTACT US 🔻	LOGIN
Enterprise company	Portal		Software & D	ocuments	Service	e Management	Resourc
t started now and	log in or register for a HPI	Passport account. You can also email u	s for help or feedback.				
Service Managen	n ent Software & D	ocuments Notifications		R	egistered	Devices & Contra	acts
Case Manage Create and mar () Case Mana	ement Anage your support cases gement			Log ir contra	nto ASP to acts, enabl relevan	register your dev ing you to access t to your network LOGIN	ices and software
License Mana Add and manag → License Ma	agement A ge your Aruba licenses inagement			Learn h	now to reg	ister your contrac	ts on ASP!
Online RMA Submit your rec Online RM/	aquest to process your Aru	ba product returns online					
Related Inform	mation						
Airheads		Innovation Zo	ne	Solutio	n Exch	ange	
Discuss product-s base, or jump into	specific topics, visit our kn o our learning portal	owledge Have an idea for a produ request? Submit it here.	ict or a product document	Generate de cases.	vice configu	iration for a variety (of use
				🕘 Aruba So	olution Exch	ange (ASE)	
lirheads Com	nmunity	() Innovation Zone					
Airheads Com Resources	nmunity	Innovation Zone			Judon Exch		
Airheads Com Airheads Com Com	hmunity best to access and port services	Access network designs to rapidly deplo	y Verify Aruba product complia country	nce by	Understar warranty o	nd more about your	product

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

Service Management Software & Docum	ents Notifications	Registered Devices & Contracts
earch for product documentation, software upd	ates, and release notes for your Aruba products	Log into ASP to register your devices and
Mobility Controllers (AOS)	⊖ Central	relevant to your network
➔ Switches	O NetInsight	LOGIN
ClearPass Policy Manager (CPPM)	⊖ Virtual Intranet Access (VIA)	
➔ AirWave	→ Analytics and Location Engine (ALE)	
Access Points	HPE DataCenter Switches	Learn how to register your contracts on ASF
➔ SD-WAN	HPE FlexNetwork Switches	Video Tutorial
ClearPass Device Insight (CPDI)	HPE Intelligent Management Center (IMC)	

Step 4 Select the filter options on the left.

• File Type: Document

• Product: Aruba Switches

FILTERS
File Type
Document (2161)
Product
Aruba Switches (2161)

• 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.

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.

🕺 Global	C
요 Global	
▼ Filter lists	
ជGroups	
BR-TMESDB	
BR-WDSM02	
BR-WHE01	
BR-WHE02	
BR-WHE06e	
BR-YRKME01	
BRWHE-BackTo8	
CP-RSVACC	
CP-RSVAGG	
CP-RSVCORE	
CP-RSVWLAN	
default	
EXAMPLE-GROUP	
FW_Upgrade_Test	3
GW-CONVERT	
IAP-CONVERT	

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.

System

Properties Contact, location, time zone and VRF

HTTP Proxy HTTP proxy server integration

SNMPv2 communities, SNMPv3 users and trap destinations

Logging Log server and event severity classification

Administrator Local device administration

Source Interface Service communication interfaces

Stacking Switch stacks and chassis

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**

Network operations	VRF	administrator username admin
.ocation Santa Clara, CA	Management DNS servers 10.2.120.08	Administrator password
fimezone .os Angeles (UTC−08:00) ∨	10.2.120.99 10.2.120.99 +	
	NTP servers 10.2.120.98	
	10.2.120.99 +	

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.

← Server Groups (2)			
Name	Servers		
RADIUS	0		
TACACS	0		
	Edit		

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)

FQDN or IP address 10.2.120.94	Shared secret
Authentication Port	Timeout (secs)
49	5
VRF	
Management 🗸	

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.

twor	ို့ k Structure					
÷	Groups (31) Combine devices with common co	onfiguration into a single	e group to apply the same con	figuration		۹ +
	▼ Group Name All connected devices (96)					
>						
	Unprovisioned devices (0)	Unprovisioned devices (0)				
~	🖌 default (6) 🛨					
	Device Name	Туре		Serial Number	MAC Address	
	8360-1	Aruba CX			00:FD:45:	
	8360-2	Aruba CX			00:FD:45:	
	Aruba9004_E	Gateway			20:4C:03:	
	Aruba9004_E	Gateway			20:4C:03:	



~	default (6) ★	<u> </u>	<u>A</u> ==		
	Device Name	Туре	Serial Number	MAC Address	
				00:FD:45:	
				00:FD:45:	
	Aruba9004_	Gateway		20:4C:03:E	

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

2 item(s) selected	
5 3	
	_

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

င်း Network Structure		
← Move De	evices	
2 selected de	evices will be moved from 'default' group to	
Destination grou BD9-AGG01	p 🗸	
Destination	group settings:	
• AOS-CX	witches	
• Ul Group	1	
The devices	vill adopt the destination group configuration	
		Cancel 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.

ss to AOS-CX search and custom config	uration (editor & express configuration).	
E cut Properties		
Name	VRF	Administrator
8360-1		admin
	VRF	
	Default	Administrato
Contact		
	DNS servers	
	+	
Location		
Location	NTP servers	
_	+	
Timezone		

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.

FirmwareCrganization	-	Ma	intain ———	
<mark>ង្</mark> ធ Organization		0	Firmware	
		ß	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

CREATE NEW GROUP	×	
group name CORE1-Template		
Use the group as Template group by selecting the device $oldsymbol{ extsf{i}}$		
AP AND GATEWAY		
(i) The group password is still required as AP and Gateway are part of a UI group.		
Group password settings (i) PASSWORD		
CONFIRM PASSWORD		
Cancel Add	Group	

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.

∀ Group Name	Devices	\\\\> Name
ALL CONNECTED DEVICES	56	8320-S2-2
UNASSIGNED DEVICES	0	8325-AG3-1
TG Access-Template	2	8325-AG3-2
TG CORE1-Template	0	8400-C1-1
TG CORE2-Template	0	€ 8400-C1-2

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

요 Global				
∀ Filter lists				
ជGroups				
CORE1-Template	TG			
CORE2-Template	TG			

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

🛱 ाल CORE1-Template 🔿	G End Access Points Switches	<u>条</u> Gateways
- Manage	SWITCHES • ON 1 1	ILINE • OFFLINE 0
Devices	SWITCHES	
🗖 Clients	Z Device Name	Туре
😩 Guests	• 8400-C1-1	AOS-CX

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

(교) 유민	:≡	اا،	<mark>ුරු</mark>
	List	Summary	Config

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

Templates			Q			\odot
Template Name	Device Type	Model	Version	Last Modified		

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

and format.	iguration should i	nateri tile running	comparation cerorae
MPLATE NAME			
DEVICE TYPE			
Aruba CX			
MODEL			
8400			
RT NAME			
LL)			
A			
Select Part Name	as (ALL) to apply th	his template for sta	icked switches.
A CONTRACTOR OF			
RSION			

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

TEMPLATE	IMPORT CONFIGURATION AS TEMPLATE Show	v Variables List
1	i Importing configuration from a switch will replace the existing template content	
	SEARCH DEVICES	
[8400-C1-1	

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

SWITCHES 1	• ONLINE 1	• OFFLINE 0	E			
SWITCHES						
SWITCHES						
Y Device Name		Туре	Clients	Alerts	Y Model	Config Status
• 8400-C1-1		AOS-CX	0	1	8400 Base Chassis/3xFT/18xFan	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.

switches									II. ∷≣ Summary List Config
MultiEdit Access to AC	t 💶	nd custom configuration (editor & expre	ss configuration).						Configuration Status
Device- Search and	Level Con	figuration s and choose either of the methods belo	w to change configuration for the selec	ted devices.					
Contextual S Enter Sea	iearch Engine rch Query (e.		s) SEAF	CH & FILTER Ch	eck Search Documentatior	1			
Device	s (2)								
Name	15.	Firmware Version	Config Modified	Status	Config Status	NAE Status	MAC Address	IP Address	Serial
RSVCP-CR									
RSVCP-CR	1-2	10.10.1010	Jun 28, 2023, 19:21:45	 Online 	Sync	Normal	ec0273-b72400	172.16.107.25	SG1ZKZ4057
								2 item(s) s	elected Clear

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



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 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 uni	cast
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**.

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

양 교 안 아 아 아 아 아 아 아 아 아 아 아 아 아 아 아 아 아 아	ট Console		
Remote Console Session New Session Saved Sessions			
Device Type Switch	Switch RSVCP-CR1-1	Username ➤ admin	Password
Create New Session			

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**.

switches								II. Summary	List	Config
MultiEdit Access to AO	IultiEdit IultiEdit Configuration (editor & express configuration). Configuration Status									
Device-I Search and Contextual S Enter Sear	Level I select o earch Eng rch Que	Configuration levices and choose either of the ine ry (e.g. nae-status:Critical AND	methods below to change conf	iguration for the sele	FILTER Check Search	Documentation				
Device	s (2)									\odot
Name	1≞.	Firmware Version	Config Modified	Status	Config Status	NAE Status	MAC Address	IF	P Address	
8360-1		10.08.0001	Oct 01, 2021, 15:15:19		Not in sync (Configura	Normal	00fd45-67dd40		0.1.1.224	
8360-2										
							2 VIEW CONFIG	item(s) sele EDIT CONFIG	ected	DNFIG

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.

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 1 Switches

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

Remote Console Sessi	on				
New Session Saved Se	essions				
Device Type Switch	~	Switch 8360-1	~	Username admin	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.

:= Console session	for the devi	e: 8320-AG1-1			𝔥 No Session Found ▾ O	()	0.02
admin@8320-AG1-1 [12::	25:28 PM] 🥒	× +					
820-AG1-1# 8320-A	p ospf nei 1 VRF defs 	ghbors ult ===== 2					
Neighbor ID	Priority	State	Nbr Address	Interface			
10.0.6.2	n/a	FULL	172.18.101.26	1/1/47			
10.0.6.1	n/a	FULL	172.18.101.22	1/1/48			
8320-AG1-1#							
[2021 Nov 11 12:25:31 PM							

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.

E Console session for the devi	ce: 8320-AG1-1	🔊 No Session Found 👻	Q	()	11
admin@8320-AG1-1 [12:25:28 PM] 🧪	× +				
8320-AG1-1# sh ip pim neig	ghbor vrf default				
PIM Neighbor					
VRF Total number of neighbors	: default : 10				
IP Address Interface Up Time (HH:MM:SS) Expire Time (HH:MM:SS) DR Priority Hold Time (HH:MM:SS)	: 10.1.1.3 : vlan1 : 78 days 01:09:23 : 00:01:31 : 1 : 00:01:45				
IP Address Interface Up Time (HH:MM:SS) Expire Time (HH:MM:SS) DR Priority Hold Time (HH:MM:SS)	: 10.1.2.3 : vlan2 : 78 days 01:09:19 : 00:01:39 : 1 : 00:01:45				
IP Address Interface Up Time (HH:MM:SS) Expire Time (HH:MM:SS) DR Priority Hold Time (HH:MM:SS)	: 10.1.3.3 : vlan3 : 78 days 01:09:22 : 00:01:31 : 1 : 00:01:45				
IP Address Interface (2021 Nov 11 12:25:31 PMI Ssh session st	: 10.1.4.3 : vlan4			/	

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-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.

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

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

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	A2:02:00:00:01
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 0.0.00
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.

SAVE

Example: Access Aggregation

		Reserved	Reserved Active	
VLAN VLA	N Access Access	Active	gateway MAC	IP helper
Name ID	Agg 1 Agg 2	Network gates w ay IP	address	address
ZTP_NA1 2	10.2.2.2 10.2.2.3	3 10.2.2.0 10.2.2.1	A2:01:00:00:00:01	10.2.120.9810.2.120.99
EMPLOYEB	10.2.3.2 10.2.3.3	3 10.2.3.0/ 29 .2.3.1	A2:01:00:00:00:01	10.2.120.9810.2.120.99
VISITOR 12	10.2.12.: 10.2.12	. 10.2.12. 10.2.12.1	A2:01:00:00:00:01	10.2.120.9810.2.1 <mark>20.99</mark>
REJECT_A 13 TH	10.2.13.2 10.2.13	.310.2.13.0/12042.13.1	A2:01:00:00:00:01	10.2.120.9810.2.120.99
CRITICAI 14 AUTH	10.2.14. 10.2.14	. 10.2.14. 10.2.14.1	A2:01:00:00:00:01	10.2.120.9810.2.120.99
MGMT 15	10.2.15.2 10.2.15	.3 10.2.15.0/12242.15.1	A2:01:00:00:00:01	10.2.120.9810.2.120.99

Example: Service Aggregation 1

VLAN Name	VLAN ID	Service Agg 1	Service Agg 2	Network/	Reserved Active Mgatekway 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 10.2.120.99
VISITOR	112	10.6.112.2	10.6.112.3	10.6.112.0	/2246.112.1	A2:04:00:00:00:	010.2.120.98 10.2.120.99
REJECT_/	113	10.6.113.2	10.6.113.3	10.6.113.(10.6.113.1	A2:04:00:00:00:	10.2.120.98 10.2.120.99
CRITICAL_ AUTH	_114	10.6.114.2	10.6.114.3	10.6.114.0) /129 46.114.1	A2:04:00:00:00:0	010.2.120.98 10.2.120.99
MGMT	115	10.6.115.2	10.6.115.3	10.6.115.(10.6.115.1	A2:04:00:00:00:	10.2.120.98 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.

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**.

← Move Devices		
1 selected devices will be moved from 'default' group to		
CP-RSVACC Y		
Destination group settings:		
AOS-CX and AOS-S switchesUI Group		
The devices will adopt the destination group configuration		
Alternatively, CX-Switches can keep their existing configuration.		
Retain CX-Switch configuration		
	Cancel	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**.

Edit Properties		
Name RSVCP-AG3-AC2	VRF VRF Management	Administrator username admin Administrator password
Location Roseville, CA	10.2.120.98 10.2.120.99 +	
Timezone Los Angeles (UTC−08:00) ∨	NTP servers 10.2.120.98 10.2.120.99	

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

← 📼 6300

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

nd configure the conductor switch the Series Conductor 10 Conductor RSVCP-AG3-AC2 Link 2 Port(s) 26	ies Conductor ies Conductor Y RSVCP-AG3-AC2 X(s) Link 2 Port(s) 26
Series Conductor IO × IO × IS 1 Port(s) Link 2 Port(s) 26	ies Conductor × RSVCP-AG3-AC2 × Link 2 Port(s) 26
Link 2 Port(s) 26	t(s) Link 2 Port(s) 26
Link 2 Port(s) 26	Link 2 Port(s) 26
26	26
Culit Mada datast	Mada data t

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.

Swi	 tche	5						II. Summary	Elst Config
M Acc	ultil ess t	AOS-CX search and custom config	turation (editor & express configurat	ion).				Configu	ration Status
<	- Crea	VSF Stacking (1) te and manage VSF stacks						(ર + ⊙
	1	lame			Series		Members		
	KSVCP-AG3-AC2 6			6300	6300 1			+ 🗇	
		Member	Device	Role	Link 1 Ports	Link 2 Ports			
		1 •	6300M 24SR CL6 PoE 2p50G	Conductor	25	26			

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.

Swit	tiEdit						li, ∷≣ Summary List	ැටි Config	
Acces	s to AOS-CX search and	custom configuration (editor & express configuration).				Configuratio	n Status	
← Cri	VSF Stacking eate and manage VSF	(1) stacks					Q -	+ ⊙	
	Name		Series			Members			
	RSVCP-AG3-AC2		6300	6300			3 +		
	Member	Member Device		Role	Li	nk 1 Ports	Link 2 Ports		
	1 •	6300M 24SR CL6 PoE 2p50G 2p25G s	witch(R8S89A)	Conductor	25		26		
	2 •	6300M 24SR CL6 PoE 2p50G 2p25G s	switch(R8589A) Memb	Member	25	26			
	3 •	6300M 24SR CL6 PoE 2p50G 2p25G s	witch(R8S89A)	Member	25		26		
	3	6300M 24SR CL6 PoE 2p50G 2p25G s	witch(R8589A)	Member	25		26		

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

Sw	itches		il. Summary	List Config
Mu Acce	ItiEdit	Con	figuration Status	
(VSF Stacking (1) Greate and manage VSF stacks			৭ + ত
	Name	Series	Members	
>	RSVCP-AG3-AC2	6300	3	+ 🗇
	*			

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.
Interfaces

Ports & Link Aggregations

Specific ports, LAGs and VLAN assignments

Port Profiles

Manage Port Profiles

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

L	ינ					
switch	nes		II. Summary	i List	ADS-S	ADS-CX
Mult	RIEdit: 🜑			Config	uration	Status
+	Port Profiles (2)				Q +	- ⊙
Na	ime	Description				
Sam	nple Access Port	This is a sample Access port config				
Sarr	nple Uplink	This is a sample uplink port lag config for Access Switches		Ō	l 🗗 /	10

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

🚥 Switches	
MultiEdit	•
Access to AOS	-CX search and custom configuration (editor & express configuration).
Name Access	s Uplink LAG
Сору	'Sample Uplink' settings into this new profile.
	CANCEL

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

Switches	si	II. ummary	i List	<mark>ලි</mark> AOS-S	AOS-CX
MultiEdit			Cont	iguratio	n Status
← Port Profiles (3)				Q -	+ 😳
Name	Description				
Access uplink LAG	This is a sample uplink port lag config for Access Switches			∂ ₽,	/ Ō
Sample Access Port	This is a sample Access port config				
Sample Uplink	This is a sample uplink port lag config for Access Switches				

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
```

switches		
Access to AOS-CX search and custom configuration	on (editor & express configuration).	
Edit Profile		
Name	1 interface lag 1	
Access-Uplink-LAG	2 no shutdown	
	3 description Uplink LAG	
Description	4 no routing	
Port profile for access switch	5 vlan trunk native 2	
uplink LAGS	6 vlan trunk allowed all	
	7 lacp mode active	
	8 dhcpv4-snooping trust	
	9 arp inspection trust	
	10 Interrace 1/1/2/	
	12 mtu 1108	
	13 lag l	
	14 interface 2/1/27	
	15 no shutdown	
	16 mtu 9198	
	17 lag 1	
	CANCEL SAVE	
		_

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**.

			ସ ⊡	2 no shutdown		
Vame	Status	Address	Serial	3 description U		
SVCP-AG1-AC1	Online			5 vlan trunk nat		
SVCP-AG1-AC2	Online			6 vlan trunk al. 7 lacp mode act:	lowed all ive	
SVCP-AG1-AC5	Online			8 dhcpv4-snoopin		
WCP-AG1-AC6	Online			9 arp inspection 10 interface 1/1/27	1 trust	
	Online			11 no shutdown		
SVCP-AG2-ACT	Online			12 mtu 9198 13 lag 1		
SVCP-AG2-AC2	Online			14 interface 2/1/27		
SVCP-AG2-AC4	Online			15 no shutdown		
				17 lag 1		

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	EMPLOYE	ECAMERA	PRINTER	REJECT_AU	Teritical_aut	ſ₩IGMT	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.

HPE Central	New role			New Central	ے 💿
Customer: Ounge TME	a			SELECTED GROUP TYPE II. Mobility Gateway Service	D San
II RSVCP-WIRELESS	Access Points Gateways				
Manage	System mile Swearney			7	Guided Setup
PD over days	Roles Policies Aliases				
08 Overview	Balar		Cancel	Save	
🙆 Devices 🤜	A A				
🖽 Clients	∀ NAME	RULES	GLOBAL		
🚨 Guests	ap-role	35 Rules	No		i i
Applications	authenticated	4 Rules	No		
Security	CONTRACTOR	0 Rules	Yes		
- Analyze	CRITICAL	0 Rules	Yes		
	default-lap-user-role	2 Rules	No		
Audit Trail	default-via-role	3 Rules	No	6	
🗞 Tools 🧧	+				

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.

REMOTE	CONSOLE
ILL IN O I L	CONDOLL

Console session for the device: 6300M-AG1-AC5 admin@6300M-AG1-AC5 [06:17:56 PM] 🖉 × +				O No Session Found ▼	۹	()	0
6300M-AG1-AC5# 6300M-AG1-AC5# 6300M-AG1-AC5# 6300M-AG1-AC5# 6300M-AG1-AC5# 6300M-AG1-AC5# show radius-server Unreachable servers are preceded by * ******* Global RADIUS Configuration ******							
Shared-Secret: None Timeout: 5 Auth-Type: pap Retries: 1							
TLS Timeout: 5 Tracking Time Interval (seconds): 300 Tracking Retries: 1 Tracking User-name: radius-tracking-user							
Tracking Password: None Number of Servers: 2				 			_
SERVER NAME	TLS	PORT	VRF				
10.2.120.94 10.2.120.95		1812 1812	default default				
6300M-AG1-AC5#							

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 high-lighted.



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 highperformance 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**.

ISVCF-WIRELESS		
Now New Central to overwrite all configurations for this group:		
D By turning on this toggle, all configurations will be pushed from New Cem	tral configuration model.	
Group will contain:		
Access points		
Gateways		
Switches		
EdgeConnect SD-WWN		
Configure using templates		
triable this option to use scripts/templates instead of device configuration page		

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

🗧 Add Group		
Architecture for access points a	d gateways in this group:	
Anuba0510	ArabaDS 8	
Network role of the access point	s in this group:	
Compus/Branch	O Micro	branch
Network rale of the gateways in	this group:	
Mobility	O Branch	
Make these the preferred	group settings	Cancel

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**.

🕸 Global	0
요 Global	
RSVCP-	
ជGroups	
RSVCP-WIRELESS	

Step 3 On the left menu, select Devices.

ជ RSVCP-WIRELESS	0
— Manage —	
B Overview	
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.

:	SET DEVICE PASSWORD		
1	Mease set a password for a	ccess points in the group RSVCP-WIRELESS	
	Pacovord		
ŀ	Confirm Password		t:

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

Gateways									
WLANs Access	LANs Access Points Radio		Interfaces	Security	Third Party Tunnel	Services	System	IoT	Configuration Audit

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

WLANs	Access Points	Radios	Interfaces	Security	Third Party Tunnel	Services	System	IoT	Configuration Audit
Syst	em								
~	General								
S	Set Country code	for group		US - Uni	ted St	ates			
5	System Location			Rosevil	le				
1	limezone :						Pacific-T	îme U	TC-08
							The selected	countr	y observes Daylight Saving
1	NTP Server :						10.2.12	0.99,1	0.2.120.98

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

WLANS	Access Points	Radios	Interfaces	Security	Third Party Tunnel	Services	System	IoT	Configuration Audit		Hide Advanced
Sei	vices										
>	Real Time Lo	cating S	/stem								
>	CALEA										
>	Network Inte	gration									
>	Dynamic DNS	5									
~	AppRF™										
	Deep Packet Insp	pection:			All 🔻						
	Application Moni	itoring :									
	AirSlice Policy :										
>	SIP										
>	RRM IE Profil	e									
										Cancel	Save Settings

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.

Customer: Orange TME	ල් Access Points	<u>چ</u> Gateways			
ជា RSVCP-WIRELESS 🛛 🔿		1			
- Manage	Gateways <mark>0</mark>	• Online 0	 Offline 0 	Clusters 0	
🗄 Overview					_
🗵 Devices 🥠	Gateways				
E Devices	V Device Name		▼ Model	Y IP Add	lress

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.

Central	suided Setup for Mobility Gateway Group RSVCP-WIRELESS
1 System	This weard will guide you through the essential steps to configure the mobility gateways in the Group RSVCP-WIRELESS. You can exit this wizard at any time by clicking cancel. You will be able to relaunch the weard at any time as long as you have not yet completed all the steps. After completing this initial setup, you can change the settings at any time.
	EXIT GUIDED SETUP Guided Setup will be exited and changes will be lost. You can re-enter the Guided Setup at any time to complete it. RELINE TO TO TO TO TO TO TO TO TO T
	9
	Cancel Brgin

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

System	Interface	Security	Routing	High Availabilit	y Config Audit		Basic Mode	Guided Setup
General	Admin	Certific	ates	SNMP Loggi	ng Switching	External Monitoring		
∨ Bas	ic Info 🤫							
	Password f	or user adr	nin:					
	Retype pas	sword:						
> Clo	ck							
> Dor	nain Name	System						
> Sta	tic Host Lis							
> Dyr	amic Doma	in Name S	System					
> Dyr	amic Doma	in Name S	System (H	TTPS)				
> Sys	cem IP Addi	ess bold						
	ation	liolu						
> LC	Menu							
								?
						Cancel	Sa	ve 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.

System	Interface	Security	Routing	High Availabilit	y Config Audit					Basic Mode			
General	Admin	Certifi	ates	SNMP Loggi	ng Switching	External Monitoring							
> Basi	c Info												
✓ Cloc	k ┥												
	Time:			Get time from N	TP server 🗸								
	NTP servers												
	IP ADDRESS/FQDN BURST MODE AUTHENTICATION KEY												
				Ê									
				No data to display									
			2 +	-									

Step 2 Assign the following settings. Click Save Settings.

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

General Admin Certificates	SNMP Logging Swit	itching External Monitoring
	Add NTP Server	
	IPv4/IPv6/FQDN:	IPv4 🗸
	IPv4 address:	10.2.120.98
	Burst mode:	✓
	Authentication key:	
Source interface:	-None- 💙	
NTP server VLAN:	-Choose an option-	0
Use NTP authentication:		

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

Step 4 Select the Timezone, then click Save Settings.

Time zone:	United States: America/Los Angeles (

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

General	Admin Certificates S	SNMP Logging Swit	tching External Monitoring					
> Bas	sic Info							
> Clo	ck							
V Dor	main Name System < 1							
	Domain name:	EXAMPLE.LOCAL	•					
	Sector DMS and a sectorization							
	Enable Divis name resolution:	IPV4						
	DNS servers 🕕							
	IP VERSION		IP ADDRESS	UPLINK VLAN	=			
	18							
	No data to display							
	+ 🔞							

Step 2 Assign the following settings. Click Save.

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

Add DNS serve	r		
IP version:	IPv4		
IPv4 address:	10.2.120.98		
Uplink VLAN:	~		
		Cancel	Save

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.

ල් Access Points		<u>ඉ</u> Gateways	;		
System	Interface	Security	Routing	High Availability	Config Audit
Clusters Redundancy		dancy			

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**.

Clusters	Redundar	псу	
Cluster	mode		
Autor	matic: 🗨	O	
• A	uto Group	Auto Site	

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.



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*.

🖗 Global	0
硷 Global	
RSVCP-	
ជGroups	
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.

System	Interface	-1 rity	Routing	High Availability	/ Config Aud	it			
Ports	VLANs	DHCP	Pool Man	agement GF	RE Tunnels	VXLAN Tunn	els	Bulk configuration upload	SLB
VLA	Ns 2								
NA	ME						ID(S)		
							1		
+	-3								

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

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

New VLAN		
VLAN name:	MGMT	
VLAN ID/Range:	15	0
		Cancel Save Settings

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.

Customer: Orange TME					
ជ RSVCP-WIRELESS 이	Access Points	Gateways			
— Manage ———	Gateways 2	• Online 2	 Offline 0 	Clusters 1	
B Overview					
Devices	Gateways (2)				
Devices	V Device Name		Y Model	▼ IP Address	

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.

Ports Vite DHCP Pool Management GRE Tunnels VXLAN Tunnels Bulk configuration upload SLB Ports Ports <th>System</th> <th>Interface</th> <th>Security</th> <th>Routing</th> <th>High Availability</th> <th>Config Audit</th> <th>1</th> <th></th> <th></th> <th></th>	System	Interface	Security	Routing	High Availability	Config Audit	1			
Port TYPE VADMIN STATE VPOLICY VMODE VNATIVE VLAN VACCESS V	Ports	VL	DHCP	Pool Man	agement GRE	Tunnels V	XLAN Tunnels	Bulk configuration	upload	SLB
Ports Ports <th< th=""><th>۵.</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></th<>	۵.									
PORT TYPE PADMIN STATE PPOLICY PMODE PNATIVE VLAN PACCESS V Image: Comparison of the state	Port	ts								
TP No data to deplay	ΥP	DRT	TYPE		\heartsuit admin state	POLICY	∀мор	e 🖓 NA	FIVE VLAN	\bigtriangledown access vlan
									T. No data	B a to display

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

New p		
Gate	models support up to a maximum of 4 ports, so you can create and configure upto 4 ports. Select the ports you wish to configure b	ased on the device model.
~	I 4 configurable ports	
~	E-0/0/0	
~	E-0/0/1	
~	E-0/0/2	
~	E-0/0/3	
		Cancel 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*.

Customer: Orange TME	G Access Boints	<u>A</u>		
🛱 RSVCP-WIRELESS	Access Points	dateways		
Manage —	Gateways	• Online 2	 Offline 0 	Clusters 1
Overview				
	Gateways	(2)		
Devices 2	V Device Name			Y IP Address

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.

Port channel				
VNAME	MEMBERS			
+				

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

New po	ort chan	nel	
ID:	PC-0	~	

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

1	
Port channel id:	PC-0
Protocol:	LACP 🗸
LACP mode:	passive 💙
Port members:	GE-0/0/0,GE-0/0/1 Edit
Admin state:	\checkmark
Trust:	\checkmark
Policy:	Per-Session V allowall V
Mode:	Trunk 🗸
Native VLAN:	4094 🗸
Allowed VLANs:	15,103-105,113-114,112
Description:	

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*

Spanning tree:	\checkmark		
Cost:			
Priority:			
Point-to-point:			
BPDU guard:			
d			

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.

System Interface Security Routin	g High Availability Config Audit
IP Routes OSPF VRF Segments	

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

Static Default Gateway 🛛 🔥		
Static default gateway		
☆ DEFAULT GATEWAY	COST	
		F
		No data to displa
+ 📀		

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

• Default Gateway IP: 10.6.15.1

New Default Gateway							
IP version:	IPv4						
	Default Gateway IP	IPSec Map					
Default gateway IP:	10.6.15.1						
Cost:	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.

Customer: Orange TME	ල් Access Points	🙊 Gateways			
ជ RSVCP-WIRELESS 〇					
— Manage ————	Gateways 2	• Online 2	• Offline 0	Clusters 1	
B Overview					-
	Gateways (2)			
	V Device Name		▼ Model	Y IP Ad	dress

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**.

← ♀ RSVCP-SS2-CL1-1	\odot
— Manage —	
E Overview	
Q WAN	
윪 LAN	
Device	

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

Γ	System	Interface	Security	Routing	High Availabil	lity	Config Audit	t		
	Ports	VLANs	DHCP	Pool Man	agement	GRE	Tunnels	VXLAN Tunnels	Bulk configuration upload	SLB

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

VLANs					
NAME			ID(S)		
CAMERA			105		
EMPLOYEE			103		
MGMT			15		
			1		
+					
VLANs > MGMT VLAN IDs	Options				
ΥID	$\overline{\gamma}$ IPV4 ADDRESS	\bigtriangledown NAT		PORT MEMBERS	∀ADMIN STATE
15	-				Enabled

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

Ρ	orts	VLANs	DHCP	Pool Management	GRE Tunn	els V)	(LAN Tunnels	Bulk configuration upload	SLB
	IPv4	Port N	Nembers	Other Options					
	∨ IP	9 Address	Assignmer	ıt					
		Ena	able routing	:	-				
		● IP a	ssignment:		Static 💙				
		• IPv4	4 address:		10.6.15.11				
		• Net	mask:		255.255.255.0)			
		Act	t as DHCP se	erver:					
		Rel	lay to exterr	al:					
		 Ford 	ce operatior	al status UP:	• 0	Forcing to delay	Operational statu ed failover times	s to UP on WAN interfaces ca and is therefore not support	in lead ed
		NA	T inside:						

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

Ports	VLANs	DHCP	Pool Managemen	it GRE Tur	inels V.	XLAN Tunnels	Bulk configuration upload	SLB
IPv4	Port M	lembers	Other Options					
V IP	• Address	Assignmer	it					
	Ena	ble routing	:	~				
	 IP as 	signment:		Static 💙				
	• IPv4	address:		10.6.103.11				
	 Netr 	nask:		255.255.255	i.0			
	Act	as DHCP se	erver:					
	Rela	ay to exterr	al:					
	Ford	ce operatio	nal status UP:	0				
	NAT	۲ inside:						

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.

🙊 Gateway	,						
System	Interface	Security	Routing	High	Availability	Config Audit	
General	Admin	Certifi	cates	SNMP	Logging	Switching	External Monitoring

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

System	Interface	Security	Routing	High A	wailability	Config Audit	
General	Admin	Certifi	cates	SNMP	Logging	Switching	External Monitoring
∨ Basi	c Info						
Hostname:			RSVCP-SS2-CL1-1				
Password for user admin:							
	Retype pas	sword:					

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.

<u>으</u> Gateway	,						
System	Interface	Security	Routing	High A	vailability	Config Audit	
General	Admin	Certifi	cates	SNMP	Logging	Switching	External Monitoring

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

✓ System IP Address		
MAC address:	00:1a:1e:05:0e:70	
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.
System Interface Security Routing High Availability C	Jdit
---	------

Step 2 Confirm the Cluster mode: Auto Group.

Clusters Redundancy	
Cluster mode	
Automatic: 🗾	
Auto Group Auto Site	

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

Clusters		
CLUSTER NAME		GATEWAYS
auto_group_1016		2
Manual cluster configuration:		
Cluster name:	auto_group_1016	
Dynamic authorization (CoA):		
VPN termination:		

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

Gateways in auto_group_1016 Cluster			
GATEWAY	VRRP IP		
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.

Multicast VLAN:	15
Heartbeat threshold:	Default Custom
VRRP VLAN:	15
VRRP ID:	15
VRRP passphrase:	•••••

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**.

ි Access Po	oints	switches	্র Gate	2 ways				
WLANs	A	ccess Points	Radios	Interfaces	Security	Services	System	Configuration Audit
W	/irel	ess SSIDs						
	NAM	ИE		SECUR	ΤY		ACCESS	5 TYPE
		EXAMPLE-BR	-PSK	wpa2-p	sk-aes		Role Ba	ased
		EXAMPLE-BR	-1X	wpa3-a	es-ccm-12	8	Role Ba	ased
	EXAMPLE-MIX		wpa3-a	wpa3-aes-ccm-128		Role Ba	ased	
	EXAMPLE-TN-PSK		wpa2-p	sk-aes		Unrest	ricted	
EXAMPLE-TN-1X		wpa2-a	es		Unrest	ricted		
	ш	EXAMPLE-TN	-MPSK	mpsk-l	ocal		Role Ba	ased
	Ш	EXAMPLE-BR	-MPSK	mpsk-l	ocal		Unrest	ricted
+ 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

CREATE A NEW NETWORK	
1 General ② VLANs	3) Security (4) Access (5) Summary
Name (SSID):	EXAMPLE-8021X
✓ Advanced Settings	
⊖ Broadcast/Multicast	
Broadcast filtering:	ARP V
DTIM Interval:	1 beacon
Dynamic Multicast Optimization (DMO):	
DMO channel utilization threshold:	90 %
DMO client threshold:	40
Transmit Rates (Legacy Only)	
2.4 GHz:	Min: 12 🔻 Max: 54 🔻
5 GHz:	Min: 12 V Max: 54 V

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)

CREATE A NEW NETWORK				
	1 General 2 VLANs 3 Security 4 Access	s Summary		
	Traffic forwarding mode:	Bridge • Tunnel Mixed		
	Primary Gateway Cluster:	UI-WIRELESS:SERVICES-7210 ▼		
	Secondary Gateway Cluster:	None		
	Client VLAN Assignment:	Static Dynamic		
	VLAN ID:	EMPLOYEE(103) ×		

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

NEW SERVER	
Server Type:	Name:
RADIUS 🔻	CPPM-1
Radsec:	IP Address:
	10.2.120.94
Shared Key:	NAS IP Address:
	optional
Retype Key:	NAS Identifier:
	optional
Retry Count:	Auth Port:
3	1812

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

CREATE A NEW NETWORK	
1 General 2 VLANs	3 Security 4 Access 5 Summary
Security Level:	Enterprise Personal Captive Portal Open
Key Management:	WPA3 Enterprise(CCM 128)
Primary Server:	СРРМ-1 🔻 + 🖍 👕
Secondary Server:	СРРМ-2 🔻 🕇 🎽
LOAD BALANCING:	

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

⊖ Fast Roaming	
Opportunistic Key Caching (OKC):	
MDID:	
802.11k:	

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

Access Rules: Slide to Unrestricted

REATE A NEW NETWO	DRK			
1 General	2 VLANs	3 Security	4 Access	5 Summary
Access rules				-0
		Role Based Ne	twork Based Unre	estricted
NOTE:				
The restrictions f	or this type of S	SID are assign	ed in the gatew	vay.

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

CREATE A NEW NETWORK	
1 General ② VLANs	③ Security ④ Access ⑤ Summary
Name (SSID):	EXAMPLE-PSK
✓ Advanced Settings	
 Broadcast/Multicast 	
Broadcast filtering:	ARP V
DTIM Interval:	1 beacon
Dynamic Multicast Optimization (DMO):	
DMO channel utilization threshold:	90 %
DMO client threshold:	40
 Transmit Rates (Legacy Only) 	
2.4 GHz:	Min: 5 🔻 Max: 54 🔻
5 GHz:	Min: 18 🔻 Max: 54 🔻

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)

CREATE A NEW NETWORK			
1 General 2 VLANs	3 Security	(4) Access	5 Summary
Traffic forwarding mode:	Bridge	Tunnel	Mixed
Client VLAN Assignment:	• Static	Dynamic	Native VLAN
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

1 General 2 VLANs	3 Security
Security Level:	Enterprise Personal Captive Portal Open
Key Management:	WPA3 Personal
Passphrase Format:	8-63 chars
Passphrase:	©
Retype:	

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

Access Rules: Slide to Unrestricted

CREATE A NEW NETWORK			
1 General 2	VLANs 3 Security	4 Access	5 Summary
Access rules		(C
	Role Based Netw	ork Based Unres	tricted
NOTE:			
The restrictions	for this type of SSID a	re made in t	he switch r

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

CREATE A NEW NETWORK		
1 General 2 VLANs 3	Security 4 Access 5 Summary	
Name (SSID):	EXAMPLE-VISITOR	
✓ Advanced Settings		
Broadcast/Multicast		
Broadcast filtering:	ARP V	
DTIM Interval:	1 beacon	
Dynamic Multicast Optimization (DMO):		
DMO channel utilization threshold:	90 %	
DMO client threshold:	40	
 Transmit Rates (Legacy Only) 		
2.4 GHz:	Min: 5 🔻 Max: 54 🔻	
5 GHz:	Min: 18 V Max: 54 V	

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

NEW PROFILE			
Name:	Visitor Weekdays		
Туре:	Periodic V		
Repeat:	Daily Weekly		
Day Range:	Monday - Sunday (All Days)	 Monday - Friday (Weekdays) 	Saturday-Sunday (Weekend)
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**.

Time Range Profile	Status
Visitor Weekdays (Periodic Weekday 07:00 - 18:00)	Enabled V

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)

CREATE A NEW NETWORK			
1 General 2 VLANs	3 Security	4 Access	5 Summary
Traffic forwarding mode:	Bridge	Tunnel	Mixed
Client VLAN Assignment:	• Static	Dynamic	Native VLAN
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

EXTERNAL CAPTIVE PORTAL-CPPM-PORTAL	
Name:	CPPM-Portal
Authentication Type:	RADIUS Authentication
IP or Hostname:	cppm.example.local
URL:	/guest/example_guest.
Port:	443
Use HTTPS:	
Captive Portal Failure:	Deny Internet
Server offload:	
Prevent Frame Overlay:	

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

NEW SERVER	
Server Type:	Name:
RADIUS 🔻	CPPM-1
Radsec:	IP Address:
	10.2.120.94
Shared Key:	NAS IP Address:
	optional
Retype Key:	NAS Identifier:
•••••	optional
Retry Count:	Auth Port:
3	1812

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

Splash Page	
Captive Portal Type:	External 🔻
Captive Portal Profile:	CPPM-Portal 🔻 + 🖍 👕
Primary Server:	СРРМ-1 🔻 + 🖍 🗎
Secondary Server:	СРРМ-2 🔻 + 🖍 📋
LOAD BALANCING:	
Encryption:	
Key Management:	Enhanced Open

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

ACCESS RULES							×	:
Rule Type: Access Control	Service: Network Application Category Application Web Category Web Reputation	dhop	V	Action: Allow	V	Destinatio To a partic IP:	ular server 10.2.120.98	•
Options:								
802.1p priority		Disable Scanning			Log			
Denylist		DSCP TAG						
NOTE:								
When using they are in	the provided table, the correct order wl	the easiest w hen finished.	ay to	add the rules	s is from th	e bottoi	m up to ensi	ur

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

1 General 2 VLANs 3 Security 4 Access 5 Su	mmary
Access rules	
Role Based Network Based Unrestricted	
ACCESS RULES FOR SELECTED ROLES	
Allow dhcp on server 10.2.120.98/255.255.255.255	
Allow dhcp on server 10.2.120.99/255.255.255.255	
Allow dns on server 8.8.4.4/255.255.255.255	
Allow dns on server 8.8.8.8/255.255.255.255	
Allow http except to network 10.0.0/255.0.0.0	
Allow https except to network 10.0.0/255.0.0.0	
Deny any to all destinations	
+ Add Rule	7 Rule(s

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**

GreenLake Orange TME	,	Home Services Devices		Q # 0 # A
	Getting Started Find Services Discover and launch services from our catalog.	Dismiss Manage Workspace Set up this workspace, users, access and more.	Quick Links Manage Workspace Device Inventory Service Subscriptions	
h	Recent Services Compute Ops Management Compute	I≣ My.Services	User Management Locations Switch Workspace Feedback	
	Aruba Central Internal Launch	Data Services Launch	Learn	
	HPE Sustainability Insight Center Launch		HPE GreenLake Developer Portal	
	Featured Services	View Catalog	What's New on HPE GreenLake See the latest release information and announcements.	
	< Recommended (4) Private Cloud (2) Storage (6)	Networking (1) Workloads (4) Management & >		
	HPE GreenLake Flex Private Cloud	OpsRamp Mananement & Governance Mananement & Governance		

Figure 22: UXI-ProvisionUXIInGLP

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

HPE Orange	TME ~ Home Services Devices	L ::: 0 # 8
< Services Catalog		
	User Experience Insight Networking	Contact Sales 🕑 Provision
	Overview Regions (0)	
	Overview	Details
	User Experience Insight (UXD) is a digital experience monitoring solution that validates network health, application performance, and troubleshoots problems that affect day-to-day user experience on any network. Ideal for campus, branch, and remote environments alike, UXI assumes the role of a remote technician, evaluating the performance, connectivity, and responsiveness of network infrastructure and applications such as corporate	Available Regions US West
	ERM, Office365 or web applications. Capabilities	Supported Workspace Types Standard Enterprise Workspace
	Intuitive, simple-to-use dashboard with end-to-end visibility over performance and health. A powered later shar highlighting issues affecting high priority services. Automated user and application experience monitoring through synthetic testing.	Service ID 7cc837db-2045-4d58-a16f-b167bb9fd0d2
	Network performance metrics for wired, wireless, and cloud application connectivity. Simplified deployment and backgo connectivity and Wi-Fi Easy Connect. Multivendor support enables testing for any HPE Aruba Networking or third-party network environment via hardware sensors and/or software	Documentation https://help.capenetworks.com/en/
	agenis. Integration with third-party applications like ServiceNow and Slack via Webhooks. Insights into remote employees' digital experience.	Terms of Service https://www.hpe.com/us/en/about/legal/ccs- terms.html

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**

HPE GreenLake	range TME 🗸	Home Services Devices	
HPE a GreenLake a < Services Catalog	Arrange TME	Home Services Provision Service Manager Deploy User Experience Insight to its first region. Once set up, it can be deployed to additional regions.	Contact Sales (? Provision Details Available Regions US West Supported Workspace Types
	Capabilities Introduce simple-to-suce dashboard with end-te A powered alerts that highlights issues aftert Automated user and application experience in Simplified deployment and backup connectivity Multivendor support enables testing for a nyi Magents. Integration with third-party applications like Se Insights into remote employees' digital experience	Cancel Deploy With bullt-in cellular connectivity and Wi-Fi Easy Connect. E Aruba Networking or third-party network environment via hardware sensors and/or software viceNow and Slack via Webhooks. ce.	Standard Enterprise Workspace

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.

HPE Orange TM	1E ¥	Home	Services	Devices				Q	80	0	:	ል
Services Catalog												
1	User Experience Insight Networking					Contact Sales 🖉	Launch					
	Overview Regions (1) Deployment Regions Add or remove your service instances.											
	 All available regions for this service have been added. 											
	User Experience Insight US West											

Figure 25: UXI Devices Link

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

GreenLake Orange TME ~		Home Services Devices		Q 88 Ø 🛱 🖁
Devices Onboard and manage all device Inventory Tags	s in your inventory. Inventory View all devices or add new devices.			Add Devices
Device Subscriptions	Require Service Manager Assignments	Require Subscriptions	Assigned & Subscribed	Total Devices

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.

GreenLake Orange TME V	Home Services Devices	0 # A
	Add Devices	Cancel ×
₽	Step 1 of 2 Select Device Type Choose a device type to import. Device Type Networking Devices	

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.

	Home Services Devices	0 # A
← Select Device Type	Add Devices	Cancel ×
	Step 2 of 5	
	Serial Number & MAC Address	
	Type and add the serial number and MAC Address of the devices you would like to add.	
	Add devices via	
	CSV File	
1	Serial Number & MAC Address	
	Serial Number	
2	MZSD4PD005	
	MAC Address	
3	00:00:00:00:00	
4	Enter	
	Serial Number MAC Address	
5	i	
	6 Next →	

Figure 28: UXI Add SN & MAC Address

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

HPE Orange TME ~ GreenLake	Home Services Devices	0 # A
← Location and Service Delivery Contact (Optional)	Add Devices	Cancel ×
	Sten 5 of 5	
	Review Add Devices	
	Review the devices to be added and any tags that will be assigned.	
	Serial Number MAC Address	
	Location to be Assigned	
	Service Delivery Contact to be Assigned	
	Tags to be assigned	
	2 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.

reenLake		Home Services	Devices 1	¢ % Ø 🛱
Devices nboard and manage all dev	vices in your inventory.			
Inventory	Inventory			Add Device
Tags	View all devices or add new devices.			
Device Subscriptions Auto-Subscribe	Require Service Manager Assignments	Require Subscriptions 4	Assigned & Subscribed	Total Devices 238
•	Q UX	Clear F	ilters	Actions ~
	1 of 1 Device(s) selected Serial Number Mod	del Service Manager	Subscription Tier MAC Address	Archive Service Regi Remove Assignment
	v وه الم	G6 User Experience Insight		US West Apply Subscription Manage Tags

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

HPE Orange TME ~ GreenLake		Home Services Devices		ር ፡፡ ወ ፡፡ ሲ
Devices Onboard and manage all dev	vices in your inventory.			
Inventory	Inventory			Add Devices
Tags	View all devices or add new devices.			
Device Subscriptions Auto-Subscribe	Require Service Manager Assignments	Require Subscriptions	Assigned & Subscribed	Total Devices 238
	Q UX 1 of 1 Device(s) selected	Clear Filters		Actions ~
	Serial Number Mode	l Service Manager Subscrip	tion Tier MAC Address	Servi Assign to Service Manager
	1 🤨 🚧 💶 ux-g	6	_	Manage Tags Manage Location Service Delivery Contact Export

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





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

GreenLake Orange TME V			Home Services	Devices	1			ၞ ። º ፡፡ ႙
Devices Onboard and manage all devic	es in your inventory.							
Inventory	Inventory							Add Devices
Tags	View all devices or add new devic	ces.						
Device Subscriptions Auto-Subscribe	Require Service Manager Assignment	ts	Require Subscriptions 4		Assigned & Subs 199	cribed	Total Devices	
2	Q UX		Y					4 Actions ~
	1 of 1 Device(s) selected	Model	Service Manager	Sub	scription Tier	MAC Address	Service Regi	Archive Remove Assignment
3	0q0	UX-G6	User Experience Insight				us 5	Apply Subscription Manage Tags Manage Location

Figure 33: UXI Apply Subscription

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

GreenLake Orange TME ~	Home Services Devices	0 # A
	Apply subscriptions	Cancel ×
	Step 1 of 1 Apply subscriptions Final wave device onboarding by pairing your devices with subscriptions. Sensors Or 1 devices subscribed Or 1 devices subscribed Apply Subscriptions Apply Subscriptions	

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

HPE Orange TME ~	Home Services Devices	Q # @ # &
	Apply subscriptions	Cancel ×
	Subscription Key Ter Cersterion Uni-Foundation-Sensor- 10 Cersterion 10 10 10	

Figure 35: UXI Apply Subscription Tier

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

Apply subscriptions Cancel > Step 1 of 1 Apply subscriptions Apply subscriptions. Finish your device onboarding by pairing your devices with subscriptions. Sensors	GreenLake Orange TME ~	Home Services Devices		Q	# Ø 🛱 🖁
Step1of1 Apply subscriptions Finish your device onboarding by pairing your devices with subscriptions. Sensors		Apply subscriptions			Cancel ×
UX-66 Edit 1 of 1 devices subscribed UXI-Foundation-Sensor-Cloud 2 Apply	3	Step 1 of 1 Apply subscriptions Finish your device onboarding by pairing your devices with subscriptions. Sensors UX-G6 1 of 1 devices subscribed	Edit UXI-Foundation-Sensor-Cloud 2 Apply		

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.

GreenLake Orange TME ~		Home Services Devices		Q # 0 # A
Devices Onboard and manage all device Inventory Tags	es in your inventory. Inventory View all devices or add new devices.			Add Devices
Device Subscriptions Auto-Subscribe	Require Service Manager Assignments	Require Subscriptions 3	Assigned & Subscribed	Total Devices 238
	Q ux 1 Device(s)	Y Clear Filters		Actions ~
	Serial Number Model	Service Manager Subscription User Experience Insight UXI-Foundat	Tier MAC Address	Service Region Tags

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.

HPE Orange TME	~	F Services Devices		0 # A
	Getting Started	Manage Workspace	Dismiss Quick Links Manage.Workspace Device.Inventory	
	Recent Services	i≡ MySi	Service Subscriptions User Management Locations Switch Workspace Feedback	
	Compute Ops Management Launch Compute Aruba Central Internal Networking Launch	Aruba Central Launch Networking Data Services Launch	h Learn	
	HPE Sustainability Insight Center Launch	User Experience Insight 2 Launch	h HPE GreenLake Developer Portal (2 Integrate apps and services.	
	Featured Services	View 6	What's New on HPE GreenLake → See the latest release information and announcements.	

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**.

		🖗 Sensors &	Agents			
					[→ Export Data	+ Add
	🗞 Configured (0)					
🖗 Sensors & Agents						
		Please configure a sen	sor below.			
ALERTS	X Unconfigured (1)					
iii AlOps	Ø			 Waiting f 	or 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

				🗇 Grou	ips		
						+ Add Group	
		Groups Manageme	nt				
				No groups have been configured, click [/	Add Group] to get started		
	Groups						
	Subscriptions						
upper right.	UXI User Experience Insight						C



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

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

				Wireless			
		Ø Search				[→ Export Data	+ Add Network
	Wireless						
		Wireless Networks					
	Sensors & Agents						
	Groups						
			No wireless networks have beer	n configured, click [Add Netw	ork] to get started		
	in Inresholds						
ູ່ບ	User Experience Insight						

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!

		Add SSID: Wireless
,O Search		C+ Export Data
	SSID	OWLCorp
Wireless Netwo		Please note, SSID name is case sensitive
ALIAS	Alias	OWLCorp Collection Collection
	Hidden	
		b get started
	Security	Open Passphrase Enterprise
	Auth Method	d Password Certificate
	EAP.Type	PEAP LEAP TTLS
	Phase 2 Auth	h MS-CHAPv2 -
	Username	
	Osername	axisel with
	Password	
		Show Password
		Advanced *
	WI-FI	
	Band Locking	IS Auto 2.4 GHz 5 GHz
	Specify	
	Server.CA	Upload file Choose a file

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 +

< D				🗠 Wired		
NETW 	VORKS Wireless Wired					[→ E
		Wired Networks				
LOCA B						
Ō				conconfigured state [A	ld Mohumul) to not storted	
TESTI			NO WIRED NETWORKS have b	ieen conngurea, ciick (Ad	id Network] to get started	
ê						
ALERI						
4						
ACCO						
66 0						
Ċ	AlOps					
(e) A	Subscriptions					
e Ø	My Profile					
8						
Ē						
UX						

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

		Add Wired Network
🛜 Wireless		L→ Export Data + Add Network
<3 Wired		
	Wired Network	Alias 💦 Guest
🖗 Sensors & Agents	ALIAS	Security None Enterprise
Groups		Advanced x
		Purvaixeu ·
Service & App Tests		IP STACK
ALERTS		Version IPv6
🚝 Thresholds		
		DNS
ACCOUNT		Lookun Domain Auto Custom
武] Reports		
🖾 AlOps		Disable EDNS
 Subscriptions 		
Integrations		VLAN
(g) My Profile		
- Team		Specify.XLAN
El Account		
		XLANIR / 2
UXERSE		соннеститу

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					
Туре	Template	Title	Target	Tests	Frequency
Internal	Custom/Webserver	Webserv	172.16.23.36	HTTP, ICMP Ping	Fastest
External	Predefined/Salesfo	r txl∉ /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 Selec-

			父 Service & App	Tests
		Networks & Groi The enabled tests below appl	UPS v to all sensors across 12 groups and 11 networks.	
	LOCATIONS Sensors & Agents G Groups			
₊│				

tion 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

< Dashboard	ତ Service & App Tests						
NETWORKS रू Wireless <ा Wired	Networks & Groups The enabled tests below apply to 1 sensor across 1 group and		Close Selection				
LOCATIONS	Selected Groups	Selected Networks					
😥 Sensors & Agents	ALL GROUPS						
Groups	Roseville Campus (RSV)	1 🕑 OWLCorp					
TESTING		OWLI6T					
후 Service & App Tests		C ALL WIRED					
Thresholds		Guest					
لِ Notifications		Management					
ACCOUNT							
nil Reports							
🖆 AlOps							
right. ^{© Subscriptions}							

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.





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
| | Add Test | | |
|----------------------------|---------------------------------------|-------|--|
| National a C.C. | | | |
| NCDWORKS CAL | Internal External | | |
| bernee earcearry | | | |
| Template Type | Predefined Custom | | |
| Test Template | Webserver + | | |
| Serection Statements Title | Webserver | TESTS | |
| | | | |
| Jarget | 172.16.23.36 | | |
| Tests | | | |
| | | | |
| | — HTTPS | | |
| | ICMP ping | | |
| | HTTP status codes | | |
| | Validate SSL Certificate | | |
| | | | |
| Frequency | Sensor/Agent test frequency Fastest 👻 | | |
| | | | |
| RateLimit | Apply a rate limit to this test | | |
| | Discard Add | | |

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.





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

Networks & Groups Networks & Groups <th></th> <th>© Service Add Test</th> <th></th> <th></th> <th></th>		© Service Add Test			
Service Category Service Category Internal Template Type Predefined Custom Test Template Service Category HTTP Put 4a3 Sensor/Agent test frequency Solvin Test Elimit Apply a rate limit to this test		Add Test			
Service Category Internal Template Type Template Type Template Type Test Template Saledorce Test Template Saledorce Test Template Saledorce Test Template Saledorce Test Template Saledorce Test Template Saledorce Test Template Saledorce Test Template Saledorce Test Template Saledorce Test Template Saledorce Test Test Template Saledorce Test Test Test Test Test Test Test Test	The enabled tests below				
Second Secon	Service Catego	ory Internal	External		
Interplate Custom Custom <td>O starte</td> <td></td> <td></td> <td></td> <td></td>	O starte				
Instruction Test Template Solution Tartest Www.salesforce.com Tests HTTP Purt HTTPS UCMP ping Fressuency: Solution Fressuency: Solution Solution Solution Test Template Discont	lemplate lype	Predefined	Custom		
Schwick & Appe Intest Target Tests Tests HTTP Purt HTTPS KCMP ping Exequency Sensor/Agent test frequency Solution Exequency Solution Exequency Solution Solution <th>Test Template</th> <th>Salesforce</th> <th>•</th> <th>TESTS</th> <th></th>	Test Template	Salesforce	•	TESTS	
Tests HTTP HTTPS Put HTTPS Put HTTPS Fut HTTPS<	I Webserver	www.salesforce.com		Port 80, Ping	
 HTTPS Part 443 ○ ICMP ping C Bate limit Apply a rate limit to this test Discard Add 	Tests	HTTP	Port 80		
C HTTPS Image: C Fort Image: C Image: C Image: C Image: C </td <td>EXTERNAL SERVICES</td> <td>0</td> <td></td> <td>TESTS</td> <td></td>	EXTERNAL SERVICES	0		TESTS	
ICMP ping ICMP ping Eresuency Sensor/Agent test frequency 30 Min Rate_Limit Apply a rate limit to this test Implement Discard Add		HTTPS	Port 443		
Etsauency Sensor/Agent test frequency 30 Min Rate Limit Apply a rate limit to this test Discard Add		ICMP ping			
Bate Limit Apply a rate limit to this test					
Rate Limit Apply a rate limit to this test Discard Add	Erequency	Sensor/Agent test frequency	30 Min 👻		
Discard Add	Pate Limit	Apply a rate limit to this test			
Discard Add	Batter Little	Apply a face limit to this test			
Discard Add					
		Discard	Add		

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

C Dashboard		Service Add Test			
😴 Wireless					
<a>I Wired	The enabled tests below				
LOCATIONS	Service Category	Internal	External		
😥 - Sensors & Agents	Template Type	Predefined	Custom		
Groups	rempire type	Treatment			
TESTING	Test Template	Telnet Server	*		
👳 Service & App Tests	🔛 Webserver 🛛 Title	A5400			
ALERTS	Jarget	as400.corp.owllogistics.com			
🚋 Thresholds	EXTERNAL SERVICES				
A Notifications	Tests	Search string Check for this text on server (Optional)			
ACCOUNT	Salesforce	Port	23		
्री Reports					
📋 AlOps	Frequency	Sensor/Agent test frequency	30 Min 👻		
 Subscriptions 	Deter Livelé	A			
C Integrations	Ratectont	Apply a rate limit to this test			
(i) My Profile		Discard	Add		
The Account		Discard	200		
UXI instruction					



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.



to the right of each line to enable or disable monitoring for the

Step 3 Click the pencil icon

Step 2 Click the slider

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

related issue.

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 **Subscribe to Alerts** section, click the slider **Subscribe** 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**

< Dashboard		A	Sensors & Agents		
NETWORKS				[→ Export Data	+ Add
<2 Wired LOCKTIONS ⊗ Sensors & Agents	Configured (0)				
C Groups					
TESTING 문 Service & App Tests			Please configure a sensor below.		
ALERTS Thresholds O Notifications	🕺 Unconfigured (1)			Filter	
ACCOUNT					
යුදී Reports (ධා AlOns				 Waiting for sensor config 	\$
 Subscriptions 	CN	UX-G5C 20:4c:	20:4c:/	 Waiting for sensor config 	
-(?: Integrations ② My Profile	🕅 си	UX-G5C 20:4c:	20:4c:	 Waiting for sensor config 	
i⊚ Team <u>∏</u> Account					
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

		A	dd Config	Sensors & A uration				
🗇 Wireless								
<s th="" wired<=""><th>& Configured</th><th>Genera</th><th>al +</th><th>Advanced</th><th></th><th></th><th></th><th></th></s>	& Configured	Genera	al +	Advanced				
LOCATIONS								
🛞 Sensors & Agents 🛛		Name	RSVCP-UXI1					
Groups	NAME	Group	Roseville Campus		•	ETWORKS S		
TESTING 👳 – Service & App Tests		Wireless	OWLCorp	Configure	• 🗎			
ALCRIS	🕺 Unconfigure		OWLIoT	Configure	•			
Thresholds								
ίζι Notifications	NAME	Wired	Guest	Configure	•	STATUS		
account क्वे Reports			Management	Configure	•	 Waiting for 		
AlOps								
Subscriptions				Discard Ad	1			
Integrations My Profile								
(a) Tram								
The Account								
UXI								

Figure 49: Add Configuration

< Dashboard			🖗 Sensors & .
NETWORKS		& Configured (1)	
LOCATIONS	ents		
Groups			
TESTING	Taska	🐘 RSVCP-UXI1	CNKQKSN0N6

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

Blue	Booting without factory reset button
Magenta	Booting with factory reset button
Magenta blinking	Running factory reset
 White blinking 	Software starting
White	Sensor testing your network
Green blinking	Waiting for configuration
Yellow	Power outage detected
Yellow blinking	Power outage shutting down
Orange	No connectivity
Cyan blinking	Waiting for configuration via Bluetooth / Bluetooth mode ON
Rainbow	Identifying sensor

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

Al 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

Manage B Overview Image Clients Clients Object Automatically deploy optimization at OS:00 VIRELESS COVERAGE TUNING Image Applications Security Security Security Security Autwork Services - Analyze Alerts & Events	ନ୍ତି Global 🔿	ල් Access Points	Switches	으 Gateways			List	il. Summary	Config	i
□ Clients 05:00 ▼	- Manage	Radios RF manag ACTIVATE	ement configur OPTIMIZATION	ation to optimiz	e the wireless coverage for	network.				
Security I<	다 Clients 와 Guests 폐 Applications	05:00 WIRELESS	COVERAGE TU	NING						
	Security Security Ketwork Services Analyze Alerts & Events	l Co	l l l	1 1 1	Balanced (Recommended)	Aggressive				

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



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.

硷 Global	
요 Global	
Y HERCP	
ជ្ជGroups	
HERCP-FAB	

Step 2 On the left menu, select Devices.

법 HERCP-FAB ✓	\bigcirc
— Manage —	
B Overview	
Devices	

Step 3 Select Switches, then select Config.

Customer: Orange TME		0		Ģ	II. Summary	i List	Config
		Access Points	Switches	Gateways	Summary	List	com
ដ HERCP-FAB	\odot						

Step 4 Under Routing, select Underlay Networks.



Step 5 In the **Networks** table, click the **+** (plus sign) at the top right.

Access Points Switches	<u>ଭ</u> Gateways			
MultiEdit Access to AOS-CX search and custom core	nfiguration (editor & express o	configuration).		5
← Networks				Q + ⊕
Name	Туре		Devices	
		No data to display		

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)*

Central	Guided Setup for Underlay Network
1 Network Type	This wizard will guide you through the essential steps to configure a site underlay network. Before you start, ensure all your devices are connected and can reach Central.
2 Structure	It is required to have LLDP enabled on all devices/ports to configure the underlay network.
3 Device Assignment	Network Name HERCP-Underlay
4 Configuration	What type of network to configure? Campus
5 Summary	O Data Center

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*

aruba Central	Guided Setup for Underlay Network		
1 Network Type	How is the underlay network composed?		
2 Structure	On which devices the WAN gateways (site uplink) is connected?		Internet
	O Core Switches		WAN
Bevice Assignment	Service Aggregation Switches	Underlay	Network
	Do you have WLAN gateway?	Aggregation	Service Aggregation
4 Configuration	O No		
	O Yes, Connected to Core Switches	I Core	
5 Summary	Yes, Connected to Service Aggregation Switches	Access Aggregation	
		Access	
		Access Points	66

Step 8 In the Device Assignment window, select the Core Switches of the network and click Next.

aruba	Central	Guided Setup for Underlay Network								
1 Networ 2 Structu	rk Type re		1 Core			2 WLAN Service Aggr	egation			
3 Device	Assignment	Select and confirm the switches to use as Core Switches in the underlay network: O Discovery of Network Personas and VSX Peer is completed.								
	Iration	Sv	vitches (15)					Q 💬		
5 Summa	ary		Name	Serial	MAC Address	Model	Discovered Network Personas			
			HERCP-CR1-2 HERCP-CR1-1	SG13KRQ002 SG13KRQ00S	00:FD:45:68:DE:80 00:FD:45:68:BE:C0			-		
			HERCP-AG2-AC2	SG11KN502L	8C:85:C1:49:60:80	6300	Access			
			HERCP-CR1-AG1-1	SG12KRQ00H	00:FD:45:68:ED:00	8360	Access Aggregation			
			HERCP-CR1-DC1-1	SG12KRQ00G	00:FD:45:67:7D:40	8360	WLAN Service Aggregation			
			HERCP-CR1-BRDR1	SG09KMZ017	64:E8:81:D7:52:00	6300	WLAN Service Aggregation			
			HERCP-AG1-AC2	SG11KN5026	8C:85:C1:48:A9:C0	6300	Access			
			HERCP-AG1-AC1	SG09KMZ01B	64:E8:81:DA:C7:C0	6300	Access			
			HERCP-CR1-AG1-2	SG13KRQ003	00:FD:45:68:0E:80	8360	Access Aggregation			
				CCANNEDAN	00.05.01.40.55.00	6200	A	Y		

Step 9 In the **Device Assignment** window, select the **WLAN Service Aggregation Switches** for the network and click **Next**.

Central	Guided	Setup for Unde	rlay Network						
Network Type Structure	Co	ore			2 WLAN Service Aggr	egation			
3 Device Assignment	Assignment Select and confirm the switches to use as WLAN Service Aggregation Switches in the underlay network:								
4	Swit	tches (11)					Q 😳		
5 Summary		Name	Serial	MAC Address	Model	Discovered Network Personas			
\bigcirc	- H	HERCP-CR1-STB1-1	SG12KRQ010				<u>^</u>		
	- F	HERCP-CR1-STB1-2	SG12KRQ008	00:FD:45:68:ED:40	8360	WLAN Service Aggregation			
		HERCP-CR1-BRDR1	SG09KMZ017	64:E8:81:D7:52:00	6300	WLAN Service Aggregation			
		HERCP-AG2-AC2	SG11KN502L	8C:85:C1:49:60:80	6300	Access			
		HERCP-CR1-AG1-1	SG12KRQ00H	00:FD:45:68:ED:00	8360	Access Aggregation			
		HERCP-AG1-AC2	SG11KN5026	8C:85:C1:48:A9:C0	6300	Access			
		HERCP-AG1-AC1	SG09KMZ01B	64:E8:81:DA:C7:C0	6300	Access			
		HERCP-CR1-AG1-2	SG13KRQ003	00:FD:45:68:0E:80	8360	Access Aggregation			
		HERCP-AG2-AC1	SG11KN501Y	8C:85:C1:48:FF:00	6300	Access			
			TM02//72052	00.53.03.60.57.56	0000	A	v		

Step 10 In the **Device Assignment** window, select the **WAN Service Aggregation Switches** for the network and click **Next**.

Central	Guided Setup for Und	erlay Network				
1 Network Type						3
2 Structure	Core		regation	WAN Service Aggregation		
3 Device Assignment	Select and confirm the sw	itches to use as WAN	I Service Aggregation Switch	nes in the underlay netwo	ork:	
4 Configuration	 Discovery of Netw 	ork Personas and VSX	Peer is completed.			
	Switches (9)	Serial	MAC Address	Model	Q 💮	
5 Summary	HERCP-CR1-BRDR1	SG09KMZ017	64:E8:81:D7:52:00	6300	WAN Service Aggregation	
	HERCP-AG2-AC2	SG11KN502L	8C:85:C1:49:60:80	6300	Access	
	HERCP-CR1-AG1-1	SG12KRQ00H	00:FD:45:68:ED:00	8360	Access Aggregation	
	HERCP-AG1-AC2	SG11KN5026	8C:85:C1:48:A9:C0	6300	Access	
	HERCP-AG1-AC1	SG09KMZ01B	64:E8:81:DA:C7:C0	6300	Access	
	HERCP-CR1-AG1-2	SG13KRQ003	00:FD:45:68:0E:80	8360	Access Aggregation	
	HERCP-AG2-AC1	SG11KN501Y	8C:85:C1:48:FF:00	6300	Access	
	SEACP-CR1-AG2-1	TW82K72052	98:F2:B3:68:E7:E6	8320	Access Aggregation	
	SEACP-CR1-AG2-2	TW82K7202W	98:F2:B3:68:17:E4	8320	Access Aggregation	

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**.

Q Central	Guided Setup for U	nderlay Network				
etwork Type ructure	O re			WLAN Service	Aggregation	
e Assignment	Select and confirm the	switches to use as Acc	ess Aggregation Switches in	the underlay netwo	rk:	
figuration	Switches (8)	etwork Personas and VS	<pre>{ Peer is completed.</pre>			۹ 💬
mmary	E Name	Serial	MAC Address	Model	Discovered Network Personas	
	SEACP-CR1-AG2	-2 TW82K7202W	98:F2:B3:68:17:E4	8320	Access Aggregation	
	SEACP-CR1-AG					
	HERCP-CR1-AG					
	HERCP-CR1-AG	I-1 SG12KRQ00H			Access Aggregation	
	HERCP-AG2-AC	2 SG11KN502L	8C:85:C1:49:60:80	6300	Access	
	HERCP-AG1-AC	2 SG11KN5026	8C:85:C1:48:A9:C0	6300	Access	
	HERCP-AG1-AC	2 SG11KN5026 SG09KMZ01B	8C:85:C1:48:A9:C0 64:E8:81:DA:C7:C0	6300	Access	

Step 11 In the **Device Assignment** window, select the **Access Switches** for the network and click **Next**.

Central	Guided Setup for Un	derlay Network					
1 Network Type	Core			WI AN Service Age	reation		WAN Service Aggregation
3 Device Assignment	Select and confirm the s	witches to use as Acco	ess Switches in the underlay Peer is completed.	network:			
Configuration	Switches (4)					Q ()	
5 Summary	Name	Serial	MAC Address	Model	Discovered Network Personas		
	HERCP-AG2-AC1	SG11KN501Y	8C:85:C1:48:FF:00	6300	Access		
	HERCP-AG1-AC1						
	HERCP-AG1-AC2						
	HERCP-AG2-AC2	SG11KN502L	8C:85:C1:49:60:80	6300	Access		
						3	

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

orubo Central	Guided Setup for Underlay Network
1 Network Type	Configure your underlay network.
2 Structure	Interface IPv4 subnet pool 10.10.0.1/24
3 Device Assignment	Loopback IPv4 subnet pool 10.10.1.1/24
4 Configuration	MTU size (bytes) 9198
5 Summary	VSX-Pair Transit VLAN 4000
	Use out-of-band management port for VSX keepalive A dedicated point-to-point physical interface is being used for VSX Keepalive.
	Use NTP servers
	Use DNS servers
	(i) The servers will be configured on the default vrf.

Step 13 In the **Summary** window, review the configuration details, then click **Finish**. Central immediately begins to configure the network.

1 Network Type		Device Assignment	t (13)	0
1 Network Type			()	\odot
Name HERCP-		Name	Network Persona	
	Underlay	HERCP-CR1-1	Core	
2 Structure Networ	k type	HERCP-CR1-2	Core	
Campus		HERCP-CR1-STB1-1	WLAN Service Aggregation	
3 Device Assignment Interface 10.10.0.	ce IPv4 subnet pool 1/24	HERCP-CR1-STB1-2	WLAN Service Aggregation	
Loopba	ck IPv4 subnet pool	HERCP-CR1-BRDR1	WAN Service Aggregation	
4 Configuration 10.10.1.	1/24	SEACP-CR1-AG2-2	Access Aggregation	
MTU siz 9198	ze (bytes)	SEACP-CR1-AG2-1	Access Aggregation	
5 Summary VSX-Pai	ir Transit VLAN	HERCP-CR1-AG1-2	Access Aggregation	
Use ou t Disable	c-of-band management port for VSX keepalive d - A dedicated point-to-point physical interface is being used for VSX Keepalive.			
NTP set 10.2.120 10.2.120	rvers 0.98 0.99			
DNS se 10.2.12 10.2.12	rvers 1.98 1.99			

Step 14 On the left menu, select **Audit Log**. Confirm the successful deployment of the underlay configuration by observing the log messages highlighted below.

Z Audit Trail						3 hours		
Audit Trail (36)	Audit Trail (36)							
Y Occurred On ↓ ↓ F	▼ IP Address	▼ Username	▼ Target		▼ Description			
Dec 14, 2023, 18:16				Configuration	Config push successful			
Dec 14, 2023, 18:16				Configuration	Config push successful			
Dec 14, 2023, 18:16				Configuration	Config push successful			
Dec 14, 2023, 18:14				Configuration	Configuration difference before pushing config to device			
Dec 14, 2023, 18:14				Configuration	Configuration difference before pushing config to device			
Dec 14, 2023, 18:14				Configuration	Configuration difference before pushing config to device			
Dec 14, 2023, 18:14				Configuration	Configuration difference before pushing config to device			
Dec 14, 2023, 18:14	74.65.136.183			Configuration	Created Underlay : SEACP-Underlay			
Dec 14, 2023, 18:14	74.65.136.183			Configuration	Created Underlay : SEACP-Underlay			
Dec 14, 2023, 18:14	74.65.136.183			Configuration	Created Underlay: SEACP-Underlay			
Dec 14, 2023, 18:14	74.65.136.183			Configuration	Created Underlay : SEACP-Underlay			

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**.

	orubo Central
র্টু	Global
— Ma	anage
88	Overview
٥	Devices
ſ	Clients
2	Guests
**	Applications
•	Security
රී	Network Services
— An	alyze

Step 2 Click the Client Roles tab.

(S) RAPIDS	Authentication & Policy	Gateway IDS/IPS) Firewall	Client Roles

Step 3 Create a new role by clicking the + (plus sign) in the upper right corner of the table.

Role-to-Role Policy Enforcement 💶					
ROLES (0)			+		
	Description	Policy Identifier	Permissions		

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.

←	← Create new role					
		PERMISSIONS (0)	PERMISSIONS (0)			1
	Name	Y Name	Description			
	EMPLOYEE					
	Description					
	This is an internal employee role.					
	Policy Identifier					
	100					
			TR			
	Allow default role to source role permissions for wired clients		No da	ata to display		
	-					
					Cancel	Save

Step 5 Repeat steps 3 and 4 to create the CONTRACTOR role and enter an optional description.

ole-to-Role Policy Enforcement						
ROLES (2)						
⊽ Name	Description	Policy Identifier	Permissions			
CONTRACTOR		200	0 permitted			
EMPLOYEE 100 0 permitted						

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.

Role-to-Role Policy Enforcement	ole-to-Role Policy Enforcement 💶							
Roles (2)								
V Name Description Policy Identifier Permissions								
CONTRACTOR 200 0 permitted				/ 0				
EMPLOYEE		100	0 permitted					

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.

PERMISSIONS (0)		1
∧ Name ∧	Description	

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

Assign Permissions Assign permissions for source role CONTRACTOR					
DESTINATION ROLES (1)	DESTINATION ROLES (1)				
▽ Name	Allow Source to Destination	Allow Destination to Source			
CONTRACTOR (self)	~	~			
EMPLOYEE					

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

Assign Permissions					
Assign permissions for source role EMPLOYEE					
DESTINATION ROLES (1)					
▼ Name	Allow Source to Destination	Allow Destination to Source			
CONTRACTOR					
EMPLOYEE (self)	\checkmark	✓			

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.

ដ HERCP-FAB	0
— Manage ————	
B Overview	
Devices	

Step 3 Select Switches, then select Config.

Customer: Orange TME		0		<u>@</u>	II. Summary	:= List	Config
		Access Points	Switches	Gateways	Summary	LISU	Coming
법 HERCP-FAB 🤇	0						
		MultiEdit					

Step 4 Under Routing, select Fabrics.

Routing	
Static Routing Custom network destination routing table	
Fabrics Overlay network topology	

Step 5 On the **Fabrics** table, click the + (plus sign) at the top right.

(C) Access Points	Switches	糜 Gateways			llı Summary	List	Config
MultiEdit en						uration	n Status
← Fabrics	s					Q +	F 😳
Fabric Na	ime		BGP AS Number	Devices			

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

← Create a New F	abric			
1 Name Fabric	2 Add Devices	3 Add Overlay Network	4 Stub Tunnels to Gateway	5 Summary
Fabric Name Herndon-Fabric				
BGP AS Number 65001				
VLAN Client Presence Detec	t 💶			
FIB Optimization				
Cancel				Next

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**.

Name Fabric	,	Add Devices	Add	③ Overlay Network	4 Stub Tunnels to Gateway	Summa
Devices (13)			م 💬	AOS Gateway	xternal Network
ame ↓ <u>=</u>	Firmware Version	MAC Address	Serial N	4 item(s) selected		
			SG09KM			(A) (A)
			SG11KN	Border	Stub Border	
			SG11KN	Stub		
RCP-AG2-AC2	10.14.1000	8c85c1-496080	SG11KN	RR	R	र ।
RCP-CR1-1	10.14.1000	00fd45-68bec0	SG13KR(Cancel Apply		
RCP-CR1-2	10.14.1000	00fd45-68de80	SG13KR		Edge 😂 🛛	Edge 🔛 🏑

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**.

÷	Edit Fabric						
Ν	ame Fabric	Add Devices	3 Add Overlay Network	Stub Tunnel	4) s to Gateway		5 Summary
	Overlay Networks (3)		+ 😔				
ſ	Name	1=	VNI				
	Corporate		20000				
	Guest		30000				
	Infrastructure		10000				
	Cancel				Back	Skip	Next

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

Name Fabric	Add Devices	Add Overlay Network	4 Stub Tunnels to Gateway	5 Summary
Tunnels (1)			+ 💬	
Switch	t a	Gateway IP List		
HERCP-CR1-STB1-1		10.10.9.4, 10.10.9.5		
NOTE:				
Gateway IPs ured later in	must match the V this procedure.	(LAN Tunnel Source config	gured on the AOS-10 Ga	teways, config-

Step 14 Repeat steps 10 and 11 for additional stub switches. Click Next.

← Edit Fabric				
Name Fabric	Add Devices	Add Overlay Network	4 Stub Tunnels to Gateway	5 Summary
Tunnels (2)				
Switch	1=	Gateway IP List		
HERCP-CR1-STB1-1		10.10.9.4, 10.10.9.5		
HERCP-CR1-STB1-2		10.10.9.4, 10.10.9.5		
Cancel			Back	Skip Next

Step 15 Review the **Summary** page for accuracy. Return to previous pages and make corrections, if needed. Click **Save**.

ame Fabric	BGP A	Add De	vices	Add Overlay Network	Stub Tunnels	to Gateway	5 Summar
erndon-Fabric	65001 etwork	Enabled (3)	Disable	d Fabrics (10)			\odot
Name 🚛	VNI	Route	Route Disti	Devices	Network Personas	Operation	
Corporate	20000	65001:20000	20000	HERCP-CR1-1	RR		A
Guest	30000	65001:30000	30000	HERCP-CR1-2	RR		
Infrastructu	10000	65001:10000	10000 🗸	HERCP-CR1-BRDR-2	BORDER		
				HERCP-CR1-BRDR-1	BORDER		
Tunnels (2)			HERCP-CR1-STB1-1	STUB		
Switch	↓≞.	Gateway IP List		HERCP-CR1-STB1-2	STUB		
HERCP-CR1-STE	31-1	10.10.9.4, 10.10.9.5					
HERCP-CR1-STE	31-2	10.10.9.4, 10.10.9.5					

Create the Fabric Segments

Follow these steps to create segments within the fabric.

step i Expand the memory i done, then each the memory segment form
--

←	Fabrics (1)				Q	+ 💬
	Fabric Name	BGP AS Number	Devices	Config Status	- 1)
\sim	Herndon-Fabric	65001	10	Sync	े प्	3 / Ō

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

ay Network & VLAN 2 Segment y Network rrate VLAN ay Fabric Wired 100 ion Defau 10.10.	N ID ult Gateway IP 0.5.1	Roles Subnet Bits	Devices	Summ
2 Segment vertication vertica	N ID ult Gateway IP 0.5,1	Subnet Bits		
v Network vrate VLAN Name VLAN ay Fabric Wired 100 ion Defau VLAN 10.10.	N ID ult Gateway IP 0.5.1	Subnet Bits		
Name VLAN ay Fabric Wired 100 ion Defau 20.10.	N ID ult Gateway IP 0.5.1	Subnet Bits		
ay Fabric Wired 100 ion Defau 10.10.	ult Gateway IP 0.5.1	Subnet Bits		
ion Defau 2010	ult Gateway IP 0.5.1	Subnet Bits		
<u> </u>	0.5.1			
		24		
HCP Relays (2)		+		
CP Server VRF	erver			
ult 10.2.120.	0.99			
ult 10.2.120.	0.98			

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.

← Edit Segment				
Overlay Network & VLAN		2 Roles	3 Devices	(4) Summary
CONTRACTOR	CRITICAL	EMPLOYEE IOT-NO-INET PRINTER SECURITY		
Cancel				Back Next

Step 4 On the Devices page, select the Edge devices, then click Next.

stub VTEP (2) Name HERCP-CR1-STB1-1 SG12KRQ010 HERCP-CR1-STB1-2 SG12KRQ008 HERCP-AG1-AC1 SG09KMZ018 HERCP-AG1-SG12KRQ008 HERCP-AG1-AC2 HERCP-AG1-AC2 SG11KN5026 HERCP-AG2-AC2 HERCP-AG2-AC2	N	ew Segment									
Image: Serial Number Image: Serial Number Image: HercP-Cr1-STB1-1 SG12KRQ010 Image: HercP-Cr1-STB1-2 SG12KRQ008 Image: HercP-AG1-AC1 SG09KMZ01B Image: HercP-AG1-AC1 SG09KMZ01B Image: HercP-AG1-AC1 SG11KN5026 Image: HercP-AG2-AC1 SG11KN501Y Image: HercP-AG2-AC2 SG11KN502L	verla	ay Network & VLAN				Roles			3 Devices		Su
Name Serial Number HERCP-CR1-STB1-1 SG12KRQ010 HERCP-CR1-STB1-2 SG12KRQ008 HERCP-AG1-AC1 SG09KMZ01B HERCP-AG1-AC2 SG11KN5026 HERCP-AG2-AC1 SG11KN501Y HERCP-AG2-AC2 SG11KN502L	Sti	ub VTEP (2)			E	dge VTEP (4)					
□ HERCP-CR1-STB1-1 SG12KRQ010 ✓ HERCP-AG1-AC1 SG09KMZ01B □ HERCP-CR1-STB1-2 SG12KRQ008 ✓ HERCP-AG1-AC2 SG11KN5026 ✓ HERCP-AG2-AC1 SG11KN501Y ✓ HERCP-AG2-AC2 SG11KN502L		Name	ι=	Serial Number		Name	1=	Serial Number			
HERCP-CR1-STB1-2 SG12KRQ008 HERCP-AG1-AC2 SG11KN5026 HERCP-AG2-AC1 SG11KN501Y HERCP-AG2-AC2 SG11KN501Y	כ	HERCP-CR1-STB1-1		SG12KRQ010		HERCP-AG1-AC1		SG09KMZ01B			
✓ HERCP-AG2-AC1 SG11KNS01Y ✓ HERCP-AG2-AC2 SG11KNS02L		HERCP-CR1-STB1-2		SG12KRQ008		HERCP-AG1-AC2					
✓ HERCP-AG2-AC2 SG11KN502L						HERCP-AG2-AC1					
						HERCP-AG2-AC2					
	Canc	el								Back	

Step 5 Review the **Summary** page for accuracy, then click **Save**.

New Segment								
Overlay Network & Vi	.AN			Roles		O evices		4 Summar
Overlay Network					Roles	(0)	Devices (4)	
Corporate							HERCP-AG2-AC2 HERCP-AG2-AC1	
VLAN							HERCP-AG1-AC2	
Segment Type Layer 3								
VLAN Name Overlay Fabric W	red		VLAN ID 100					
IP Version ipv4			Default Gatewa 10.10.5.1/24	y IP				
Route Target auto			Route Distinguis auto	sher				
DHCP Relays	(2)							
DHCP Server VRF	1=	DHCP Server						
default		10.2.120.99						
default		10.2.120.98						
τ.			F					

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

←	Fabrics (1)								Q -	+ ⊙		
	Fabric Name	Fabric Name 6 Herndon-Fabric 6		BGP AS Number			Devices		Config S	Config Status			
~	Herndon-Fabric			65001			10	10		Sync			
	Segment	Overlay Ne	VLAN Nam	e	VLAN ID	Default Gat	Subnet Bits	Default Gate	IPv6 Subn	DHCP Ser	Roles	C	
	Layer 3	Corporate	Overlay Fab	ric Wired	100	10.10.5.1	24			2	0	4	
	Layer 3	Corporate	Overlay Fab	ric Wireless	102	10.10.6.1	24			2	0	2	
	Layer 3	Guest	Overlay Fab	ric Wired - Guest	200	10.10.7.1	24			2	0	4	
	Layer 3	Guest	Overlay Fab	ric Wireless -Gu	201	10.10.8.1	24			2	0	2	
	Layer 3	Infrastructure	Gateway Ma	inagement	301	10.10.2.1	24			2	0	2	
	Layer 3	Infrastructure	UXI Sensor M	Vanagement	302	10.10.3.1	24			2	0	4	
	Layer 3	Infrastructure	AP Manager	nent	303	10.10.4.1	24			2	0	4	
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.

ជ HERCP-FAB	ं
— Manage ————	
B Overview	
Devices	

Step 2 On the left menu, select Devices.

♯ HERCP-FAB	୍
— Manage ————	
B Overview	
Devices	

Step 3 Select Switches, then select Config.

Customer: Orange TME		6		<u>@</u>	l Sum	l. mary	:= List	<mark>ලි</mark> Config
		Access Points	Switches	Gateways	Sum		2.50	comb
🛱 HERCP-FAB	\bigcirc							
		MultiEdit 🔵						

Step 4 Enable the MultiEdit toggle.

Step 5 Select the two stub switches.

Step 6 Click Edit Config.

Devices el constiguration el monte al constiguration de la conste la constiguration de la consteguration de la constegura	O
Description StatCLA FLICT Check Starch Terr South Outry (e.g. engles testsback Trees testsback Tr	Θ
Devices (14) Name If Immer Version Carly Modified Status Carly Status NAL Status MAC Advers P Advers HBICP-AG1/AC1 10.14.1010 COTA, 2024, 1702.081 -0101e Synch Normal 64815407.01 72.15.101.37 HBICP-AG1/AC2 10.14.1010 COTA, 2024, 1702.081 -0101e Synch Normal 648154800 172.16.103.7 HBICP-AG1/AC2 10.14.1010 COTA, 2024, 1702.081 -0101e Synch Normal 8261-48800 172.16.10.37	
Name Improvement Compared	
HGR>AGACH Indian OdA;Y0200 Ome Spread Normal 648dar20 C/2x/03.73 HGR>AGACH Indian Oda;Y0200 Online Spread Normal 648dar20 72x/03.73 HGR>AGACH Indian Oda;Y0200 Online Spread Normal 65dar400 72x/03.74 HGR>AGACH Indian Oda;Y0200 Online Spread Normal 65d-M000 72x/03.74	
HERCPAGH/GZ 10.14.1010 Oct.24.2024,170.028 ofteine Spr.c Normal 8.856-148860 172.16.101.57 HERCPAGH/AC1 10.14.1010 Oct.24.2024,170.028 ofteine Spr.c Normal 8.856-148860 172.16.101.57	
HERCP-MG2/AC1 10.14.1010 Oct 24, 2024, 17:02:08 • Online Sync Normal 8:d85c1-d8fB00 172.16.101.24	
HERCP-AG2-AG2 10.14.1010 0x124,2024,17:02:09 • Online Sync Normal 8x85c1-466080 122.16.101.74	
HER0P-Gr.1-1 014.1010 0c18,2024,172659 • online 50rd 50rd 121.61.0128	
HERCP-CR1-2 10,14,101 0c18, 3224,172,859 • Online 9mc Normal 00645.684680 122.16.10.73	
HERCP-CR1-AGL-1 0c18,2024,155338 • Online Sync Nermal 00/4568ed00 122.16.101.85	
HER0P-QR1-A61-2 10.14.1010 0x18,2024,155338 • Online Sync Normal 00645680e80 122.16.10.30	
HEROP-CRI-1462-1 0.018, 2024, 155339 • Online Sync Normal 902b368676 121.16.10.23	
HERCP-CR14.62.2 10.14.100 0c.18, 2024, 15:53:38 • Online 9nc Normal 98/26.368/74 172.16.101.32	
HERCP-CR1-BRDR-1 10.14.1010 0c124_2024_222:12:1 • Online 9mc Normal ec6794.48780 172.16.10.11	
HER0P-GR1-BBDR2 0x14,0204,222-121 • Online 9mc Normal ec6794-44500 12.16.10.12	
HERCP-CRI-STB1-2 10.14.1010 Oct 25, 2024, 20:23:06 Online Sync Normal 00/645-68ed40 172.16.101.26	

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.

🖗 Global	
요 Global	
Y HERCP	
ជ្ជGroups	
HERCP-FAB	

Step 2 On the left menu, select Devices.

법 HERCP-FAB ✓	0
— Manage ————	
B Overview	
Devices	

Step 3 Select Gateways, then select Config.

Customer: Orange TME		0			9	<u>92</u>		SELECTED GROUP TYPE Mobility Gateway	II. Summary	:= List	Config
P-9		Access F	oints	Switches	Gat	eways		mobility dateway	,		
HERCP-FAB	0	System	Interface	Security	Routing	High Availabilit	ty Config Audit		Basic Mode	Guide	d Setup

Step 4 Select the Interface tab and select VLANs. In the lower left, click the + (plus sign).

S	ystem	Interface	Security	Routing	High Avail	ability	Config Au	dit				
Ρ	orts	VLANs	DHCP	Pool Man	agement	GRE	Tunnels	V	XLAN Tunnels	Bulk config	guration upload	SLB
	VLAN	S										
	NAME					ID(S)						
						1,15,3	801					
	+ •	4										

Step 5 In the **New VLAN** window, assign the following settings, then click **Save Settings**. * **VLAN name:** *Overlay-MGMT* * **VLAN ID/Range:** *301*

New VLAN		
VI AN		
vLAN name:	Overlay-MGMT	
VLAN ID/Range:	301	0
		Ca

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.

Syste	m Interface	Security Routing	High Availability	Config Audit								Basic Mode	Guided Setup
Port	s VLANs	DHCP Pool Mana	agement GRE Ti	unnels VXLAN Tur	nels Bulk config	uration upload	SLB						
1	1) ts												
Y	PORT	TYPE	\heartsuit admin state	POLICY	∀ MODE	VNATIVE VLAN	∀ACCESS VLAN	$\overline{\gamma}$ trunk vlans	TRUSTED VLANS	SPANNING TREE	DESCRIPTION		=
G	E-0/0/0		Enabled	Not-defined	PC-0				1-4094	v	GE0/0/0		
G	E-0/0/1		Enabled	Not-defined	access		1			v			
G	E-0/0/2		Enabled	Not-defined	PC-0				1-4094	~	GE0/0/2		
G	E-0/0/3		Enabled	Not-defined	access		1		-	~			
G	E-0/0/4		Enabled	Not-defined	access		1			~			
G	E-0/0/5		Enabled	Not-defined	access		1			V			
+													
P	ort channel												
Y	NAME	MEMBERS	s $ abla PI$	ROTOCOL	POLICY	ΎMODE	\bigtriangledown	ACCESS VLAN	\bigtriangledown NATIVE VLAN	TRUNK	/LANS		=
Р	c·o 🔁	GE-0/0/0,GE	E-0/0/2 LAC	Ρ	Not-defined	trunk			15	1,15,301	ĺ.]	

Step 3 Scroll to the port-channel configuration.

Step 4 From the dropdown, select VLAN 301 to add it.

Step 5 Click Save Settings.

System	Interface Securi	ty Rouding Hegh Availability Config Audit	Basic Mode	Guided Setup
Ports	VLANS DHCP	Pool Management GRE Tunnets VXLAN Tunnets Bulk configuration upload SLB		
PC-0				
	Port channel id:	PC0		
	Protocol:	LLCP V		
	LACP mode:	passive V		
	Port members:	GE-000,GE-0022 848		
	Admin state:			
	Trust:			
	Policy:	Not defined 🗸		
	Mode:	Trunk 🗸		
	Native VLAN:	15 🗸		
	Allowed VLANs:	1,15,301 🗸 O 🔫		
	Description:			
	Jumbo MTU:			5
		Cancel	Sav	re 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).

Access	j 📮 🐥 Points Switches Gateways		SELECTED GROUP TYPE Mobility Gateway	th Sunnary	iiii 🛞							
System	Interface Security Routing High Availability Config Audit			Basic Mode	Guided Setup							
IP Routes CSFF VIFF Segme												
> IP	> IP Routes											
∨ Sta	atic Default Gateway											
	Static default gateway											
		COST			=							
	10.10.9.1	1										
	+ 🥝											
> Dy	namic Default Gateway											

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

• Default Gateway IP: 10.10.2.1

G Access P	oints Switches	ateways		SELECTED GROUP TYPE Mobility Gateway	ili Summary	iiii 🛞
System	Interface Security Routin	g High Availability Config Audit			Basic Mode	Guided Setup
IP Routes	OSPF VRF Segments					
> IP R	outes					
∨ Stat	ic Default Gateway					
	Static default gateway					
	DEFAULT GATEWAY		COST			=
	10.10.9.1		1			
	+					
	New Default Gateway					
	Duarrian					
	IP version:	IPv4				
		Default Gateway IP IPSec Map				
	Default gateway IP:	10.10.2.1				
	Cost:	1				
> Dyn	amic Default Gateway					
						•
						•
				Cancel	Sa	ve Settings

Step 4 Select the original static default gateway and set the **Cost** to *50*, making this a backup route. Then click **Save Settings**.

Image: Selected GROU S									
System interface Security Neuring High-Availability Config-Availt									
IP Routes OSPF Wei Segments									
> IP Routes									
∨ Sta	tic Default Gateway								
	Static default gateway								
	TDEFAULT GATEWAY		COST			=			
	10.10.2.1		1						
	10.10.9.1		50						
	+								
	IP Default > 10.10.9.1								
	IP version: IPv4								
	Default gateway IP: 10.10.9.1								
	Cost: 50	-							
> Dy	namic Default Gateway								
						•			
				Cancel	Sa	ve Settings			
	NATE								

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).

Access) 💷 🔗 Points Switches Gateways						SELECTED GROUP TYPE Mobility Gateway	th Summary	iiii 🛞 List Config	
System	Interface Security Routing High	Availability Config Audit						Basic Mode	Guided Setup	
V IP	Routes									
	IP routes	DESTINATION MASK	NEXT HOP (FORWARDING ROUTER AL COST	DISTANCE	VIPSEC MAP NAME	NULL INTERFACE			=	
				63						
				No data to display						
	+ 🔴									
> St	> Strife Default Gateway									
> D;	mamic Default Gateway									

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

Image: Second										
System Interface Security Routing High Auditability Config.Audit									Guided Setup	
IP Reviews OXFF VID Segments										
✓ IP I	Routes									
	IP routes									
	Y DESTINATION IP ADDRESS	DESTINATION MASK	Y NEXT HOP (FORWARDING ROUTER AL COST	DISTANCE	Y IPSEC MAP NAME	NULL INTERFACE				
				1P						
				No data to display						
	+									
	New IP Route									
	IP version:	IPv4								
	Destination IP address:	10.10.1.0								
	Destination network mask:	255.255.255.0								
	Forwarding settings:	Using Forwarding Router Address 💙								
	Next hop IP address:	10.10.9.1								
	Cost:									
	Distance:								•	
							Cancel	Sa	ve Settings	

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**.

HPE or ubo networking Central			٩	Search fo	or failed c	ilients, ne	twork de
Customer: Orange TME	<u>@</u>						
← 🙊 HERCP-STB1-GW2 ⊘	System	Interface	Security	Routing	High A	vailability	Config
— Manage —	General	Admin	Certifi	cates	SNMP	Loggin	g Sv
🗄 Overview							
Q WAN	> Basi	c Info k					
ය 옵	> Dom	nain Name	System				
Device	> Dyna	amic Doma	ain Name S	System			
🗔 Clients	> Dyna	amic Doma	ain Name S	System (H	HTTPS)		
Applications	∨ Syst	em IP Addr	ress				
Security		MAC addre	ss: 20:4	4c:03:b1:a	19:da		
— Analyze ————		IPv4 addres	s:	// 4.NI 201	10 10 2 5		i)
🗘 Alerts & Events				LAN 301	10.10.2.5		
🔀 Audit Trail	> Loop	back Inter	face				
🖏 Tools	> Capa	acity Thres	hold				
ட் Reports	> Loca	tion					

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**.

🖗 Global	
요 Global	
[▼ HERCP]	
ជGroups	
HERCP-FAB	

Step 2 On the left menu, select Devices.

篇 HERCP-FAB ✓	$^{\circ}$
— Manage —	
B Overview	
Devices	

Step 3 Select Gateways, then select Config.

	Customer: Orange TME		0			S	<u>9</u> 2		SELECTED GROUP TYPE	th Summary	:= List	Config
IAM HERE!!!!	ដ HERCP-FAB	2	Access P	oints Interface	Switches	Routing	High Availability	Config Audit	woonity Succivity	Basic Mode	Guide	d Setup

Step 4 Click the Interface tab and click VXLAN Tunnels. Click the + (plus sign) at the lower left.

Access Points Switches	œ Gateways					SELECTED GROUP TYPE Mobility Gateway	ll. Summary	iii 👸 List Config	
System Interface Security R	outing High Availability Config Au	lit					Basic Mode	Guided Setup	
Ports VLANs DHCP Poo	l Management GRE Tunnels	XLAN Tunnels Bulk configuration	upload SLB						
Virtual extensible LAN (vxlan	Virtual extensible LAN (vxlan) tunnels								
IP VERSION	VXLAN SOURCE IP	VTEP PEER IP	VNI COUNT	TUNNEL ADMIN STATE	GPID TAG			≡	
			No data to display						
+									

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*

Edit VXLAN Tunnel	
IP version:	IPv4 💟
VXLAN tunnel source:	VLAN 🗸
VLAN interface:	15 🗸
Virtual tunnel end point (vtep) peer IP:	10.10.1.14
Maximum transmission unit (mtu):	9198
Enable tunnel admin state:	
Enable global policy identifier (gpid) tag:	

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*

. Ac	id VNI		
s r V	/LAN ID:	102 🗸	
и _V	/irtual network identifier:	102	
			Ca

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.

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.

The below table summarizes the policies applied to each role.

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 <i>r2r</i> 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.

♯ HERCP-FAB ✓	0
— Manage —	^
B Overview	
Devices	

Step 2 On the left menu, select Devices.

ជ HERCP-FAB	0
— Manage ————	
B Overview	
Devices	

Step 3 Select Gateways, then select Config.

Customer: Orange TME		6			9	<u>چ</u>		SELECTED GROUP TYPE Mobility Gateway	th. Summary	:= List	Config
PT USDCD FAD		Access P	oints	Switches	Gat	eways		mobility dutemay	,		
MERCP-FAB	\circ	System	Interface	Security	Routing	High Availability	Config Audit		Basic Mode	Guide	d Setup

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.

Customer: Orange TME	O Access F	Points	switches.	<u>@</u> Gateways							
ជ HERCP-FAB 이	System	Interface	Security	Routing High Av	ailability Con	fig Audit					
- Manage	Roles	Policies	Aliases	cations	Apply Policy	Auth Servers	Role Assignment (AAA Profiles)	L2 Authentication	L3 Authentication	Advanced	Firewall
B Overview	∨ Net	work Alias	es								
Devices		Network	aliases								
Clients		NAME				ITEMS		DESCRIPTION			IP VERSION
🕰 Guests		any				1					IPv4
Applications		auth-fac	ebook			3					IPv4
Security		auth-go	ogle			2					IPv4
Analyze		controlle	er			1					IPv4
Alerts & Events		localip				1					IPv4
Audit Trail		mswitch	ı			1					IPv4
🖏 Tools		+ 🧹									

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.

Destination client-	networks			
Name: Description: Invert:	client networks subnets with identity att			
Items				
TYPE		IP ADDRESS	NETMASK/RANGE/OFFSET	≡

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

Add new user rule				
Rule type:	Network 💙			
IP address:	10.10.5.0			
Netmask/wildcard:	255.255.255.0	i		
				Cancel

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.

Customer: Orange TME				*									SELECTED GROUP TYPE Mobility Gateway	th Surreary	
더 HERCP-FAB 〇	System	Interface	Security	Routing High Av	ailability Con	ing Audit								Basic Mode	Guided Setup
Manage	Roles	Policies	Aliases	Applications	Apply Policy	Auth Servers	Role Assignment (AAA Profiles)	L2 Authentication	L3 Authentication	Advanced	Firewall				_
Devices		dient-n	etworks			4		subnets with iden	ntity attached		IPv4	-			
D Clients		controll	ler			1					IPv4				
🚨 Guests		localip				1					1944				
Applications		+													
Security		Destinat	tion client-n	etworks											
Analyze															
Alerts & Events		Desi	cription:	subnets with ide	entity att										
😰 Audit Trail		Inve	at												
🗞 Taols															
Reports		Ite	ems												
Maintain		TY	PE				IP ADDRESS				NETMASK/RANGE/OFFSET				
Firmware		ne	itwork				10.10.7.0				255.255.255.0				
b Organization		ne	twork				10.10.8.0				255.255.255.0				
		ne	EWORK				10.10.5.0				255,255,255,0				
		ne	INVOLK				10.10.6.0				255,255,255,0				
		Ŧ													
	. Se	den Allarr													
	> serv	nce allase													
															Q
													Cancel	Sa	we Settings

Create Policies

Step 1 Navigate to the Security tab and select Policies.

HPE GreenLake				88
HPE orubo Central		Q Search for failed clients, network devices, connectivity issues, documentation and more	New Central	¢ 🤉 2
Customer: Orange TME	6		SELECTED GROUP TYPE	
🛱 HERCP-FAB 🕓	Access Points Switches System Interface Security	Cuateways Routing High Availability Config Audit	Basic Mode	Guided Setup
- Manage	Roles Policies	Applications Apply Policy Auth Servers Role Assignment (AAA Profiles) L2 Authentication L3 Authentication Advanced Firewall		

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

HPE aruba Central	Add policy			
Customer: Orange TME	Access Points Switches 6			
다 HERCP-FAB 이	System Interface Security Routin Policy type:	Session 🗸		
Manage	Roles Policies Allases App Policy name:	allowed-network-service		
B Overview				•
Devices	Policies			
Et Clients	∑ NAME			Cancel Save
요. Guests	allow-stuff	0	session	
# Applications	allow-stuff2	1	session	
Security	ap-acl	7	session	
Analyze	apprf-authenticated-sacl	0	session	
↓ Alerts & Events	apprf-contractor-sacl	0	session	
🗷 Audit Trail	apprf-default-via-role-sacl	0	session	
🖏 Tools	+ 🕙			

Step 3 Select the allowed-network-services policy and click the + (plus sign).

0			
Access Points Switches Gateways			
System interace security Routing High Availability Coning Au			
Roles Policies Aliases Applications Apply Policy A	uth Servers Role Assignment (AAA Profiles) L2 Authentication	L3 Authentication Advanced Firewall	
Policies			
∀ NAME	RULES COUNT	∀туре	$\overline{\forall}$ POLICY USAGE
validuserethacl	1	eth	
allowall	2	session	
allow-diskservices	4	session	
allowed-network-services	0	session	
allow-printservices	3	session	
allow-stuff	0	session	-
+			
Policy > allowed-network-services Rules			
PRIORITY IP VERSION	∀source	∀ destination ∀ serv	/ICE/APPLICATION ACTION
		B	
		No data to display	
+ 🜏			

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

Q Search for failed	lients, network devices, connectivity issues, documentation and more	New Central 🌒 🔅	1 @ &
Access Points Switches Gateways		SELECTED GROUP TYPE II. III Mobility Gateway Summary List	Config
System Interface Security Routing High-Availability Config Audit		Basic Mode Gu	Jided Setup
Roles Policies Aliases Applications Apply Policy Auth Servers	Role Assignment (AAA Profiles) L2 Authentication L3 Authentication Advanced Firewall		
allowed-network-services > New forwarding Rule			
IP version:	IPv4 🗸		
Source:	Any 🗸		
Destination:	Any 🗸		
Service/app:	Service 🗸		
Services alias:	svc-dns 🗸		
Action:	Permit 🗸 O		
DSCP:			
Time range:	- None - V Reset		
802.1p priority:	×		
Options:	Log Mirror		
Queue:	~		
Position:		•	
			7
		Cancel Save S	ettings

Step 5 Repeat Step 4 to create a rule for *svc-dhcp*.

Below is the complete policy.

Policies											
VNAME BIOWPOISAGELVICES	RULE	ES COUNT		∀түре зеззюп			POLICY USAGE				=
allowed-network-services									Î		
allow-printservices	3			session							
allow-stuff	0			session							
allow-stuff2	1			session							
ap-acl	7			session							
apprf-authenticated-sacl	0			session							
+											
										-	
Policy > allowed-network-services Rules										0	Drag rows to re-order
PRIORITY	IP VERSION		SOURCE		Testination	<i>∀</i> SERVICE	E/APPLICATION	ACTION			=
1	IPv4		any		any	svc-dns		permit			
2	IPv4		any		any	svc-dhcp		permit			
+											

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.

Access F	oints	E Switches	<u>¢</u> Gate	ک ways											
System	Interface	Security	Routing	High Ava	ailability	Config Au	ıdit								
Roles	Policies	Aliases	Applica	itions	Apply P	olicy A	Auth Servers	Role Assignm	ient (AAA Profil	les) L2 A	uthentication	L3 /	Authentication	Advanced	l Firewall
	ME				RULES	OUNT								GE	
cplog	out				1				session						
deny-	inbound-cli	ents			1				session				-		
dhcp	acl				1				session						
dns-a	cl				1				session						
faceti	me-acl				4				session						
globa	l-sacl				0				session						
+															
Policy	/ > deny-inl	bound-clier	nts Rules												
PRIO	RITY		IP V	ERSION			SOURCE		YDE	STINATION		YSER	VICE/APPLICATI	ON	ACTION
1			IPv2	1			client-netv	vorks	user			any			deny

Below is the complete policy.

Apply Policies to Role

Step 1 Navigate to the Security tab. In the Roles section, select the EMPLOYEE role.

HPE GreenLake										88
HPE arving Central	٩	Search for failed clients, no	etwork devices, connectivity issues, doci	umentation and more				New Centr	al 🌑	2 © ف
Customer: Orange TME	Access Points Switcher	WF						SELECTED GROUP TYPE Mobility Gateway	il. Summary	
업 HERCP-FAB 이	System Interface Security Routing I	igh Availability Config Auc	dit						Basic Mode	Guided Setup
Manage	Roles Policies Aliases Applicatio	ns Apply Policy Au	uth Servers Role Assignment (AAA Pr	ofiles) L2 Authentication	L3 Authentication	Advanced Firew				
B Overview	Roles		5							
Devices	∑ NÂME	R	RULES	GL	DBAL					=
La Clients	CONTRACTOR	1	Rules	No						
2. Guests	CRITICAL	0) Rules	Yes						
Applications	default-lap-user-role	2	2 Rules	No						
Security	default-via-role	3	Rules	No						
Analyze	default-vpn-role	4	l Rules	No						
	EMPLOYEE	a) Rules	No						
🛛 Audit Trail	+	i.		i i			i			
🖏 Tools										
🛍 Reports	EMPLOYEE Policies Bandwidth	More								
Maintain	∑NAME	RULES COUNT	r	Ттуре	7	POLICY USAGE				=
Firmware	global-sacl	0	-	session		ap-role, authenticated, G	ONTRACTOR, default-via-ro			
torganization	apprf-employee-sacl	0	:	session		EMPLOYEE				
	EMPLOYEE_r2r_policy	0	:	session		EMPLOYEE				
	+									

Step 2 Click the + (plus sign).

EMPLOYEE Policies Bandwidth More				
∀NAME	RULES COUNT	∀туре	∀ POLICY USAGE	=
global-sacl	0	session	ap-role, authenticated, CONTRACTOR, default-via-ro	
apprf-employee-sacl	0	session	EMPLOYEE	
EMPLOYEE_r2r_policy	0	session	EMPLOYEE	
+ 📀				

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.

	Add policy						_	New Cent	ral 🌑	2 © گ
G D	ridd policy							SELECTED GROUP TYPE Mobility Gateway	ili Sunnary	
System Interface Security Routin	Add an existing policy:	۲							Basic Mode	Guided Setup
Roles Policies Aliases App	Create a new policy:									
_										
Roles	Policy type:	Session 🗸								
√NAME	Policy name:	allowed-networ	k services							=
CRITICAL										
default-lap-user-role	Position:									
default-via-role							V			
default-vpn-role							Cancel Save			
EMPLOYEE			o nanz				_			
guest			11 Rules		No					
+			27 Dular		Mo					
EMPLOYEE Policies Bandwidt	h More									
∀ NAME		RULES COUNT		∀туре		POLICY USAGE				
global-sacl		0		session		ap-role, authenticated, CONTRACTOR,	default-via-role, default-vpn-r			
apprf-employee-sacl		0		session		EMPLOYEE				
EMPLOYEE_r2r_policy		0		session		EMPLOYEE				
+										

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.

Q Sean	ch for failed clients, network devices, connectivity issues, documentati	on and more	
Access Points Switches Gateways			
System Interface Security Routing High Availability Config Au	udit		
Roles Policies Aliases Applications Apply Policy	Auth Servers Role Assignment (AAA Profiles) L2 Authentication	L3 Authentication Advanced Firewall	
Roles			
	RULES	GLOBAL	
CONTRACTOR	i Rules	140	
CRITICAL	0 Rules	Yes	
default-iap-user-role	2 Rules	No	
default-via-role	3 Rules	No	
default-vpn-role	4 Rules	No	
EMPLOYEE			
guest	11 Rules	No	
+			
EMPLOYEE Policies Bandwidth More			
<i></i> ∀NAME	RULES COUNT	Ύтүре	▽ POLICY USAGE
global-sacl	0	session	ap-role, authenticated, CONTRACTOR, default-via-role, default-vpn-r
apprf-employee-sacl	0	session	EMPLOYEE
EMPLOYEE_r2r_policy	0	session	EMPLOYEE
allowed-network-services	2	session	EMPLOYEE
deny-inbound-clients	1	session	EMPLOYEE
allowall	2	session	authenticated, default-iap-user-role, default-via-role, default-vpn-rol
+			

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.

Request Details						
Summary Input	utput Accounting					
Enforcement Profiles:	erndon Wired OWL EMP	LOYEE				
System Posture Status:	NKNOWN (100)					
Audit Posture Status:	Audit Posture Status: UNKNOWN (100)					
RADIUS Response						
Radius:Aruba:Aruba-Us	r-Role EMPLOYEE					
Radius:IETF:Egress-VLA	IID 100					

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.

E Console session for the device: HERCP-AG1-AC1	<pre>Console session for the device: HERCP-AGI-AC1 admin@HERCP-AGI-AC1[02:43:29 PM] / x + Last login: 2025-01-23 21:49:25 from the console User "admin" has logged in 3 times in the past 30 days HERCP-AGI-AC1# HERCP-AGI-AC1# HERCP-AGI-AC1# Total Number of Neighbors : 2 Neighbor ID Priority State Nbr Address Interface 10.10.1.9 n/a FULL 10.10.0.64 1/1/28 10.10.1.6 n/a FULL 10.10.0.40 2/1/28 HERCP-AGI-AC1#</pre>	REMOTE CONSOLE				
admin@HERCP-AG1-AC1[02:43:29 PM] / Last login: 2025-01-23 21:49:25 from the console User "admin" has logged in 3 times in the past 30 days HERCP-AG1-AC1# HERCP-AG1-AC1# show ip ospf nei VXR: default Process : 1 Total Number of Neighbors : 2 Neighbor ID Priority State Nbr Address Interface 10.10.1.9 n/a FULL 10.10.0.64 1/1/28 10.10.1.6 n/a FULL 10.10.0.40 2/1/28	admin@HERCP-AG1-AG1 [02:43:29 PM] / x + Last login: 2025-01-23 21:49:25 from the console User "admin" has logged in 3 times in the past 30 days HERCP-AG1-AC1# HERCP-AG1-AC1# HERCP-AG1-AC1# Total Number of Neighbors : 2 Neighbor ID Priority State Nbr Address Interface 10.10.1.9 n/a FULL 10.10.0.64 1/1/28 10.10.1.6 n/a FULL 10.10.0.40 2/1/28 HERCP-AG1-AC1#	\Xi Console sessi	on for the devi	e: HERCP-AG1-	AC1	
Total Number of Neighbors : 2 Neighbor ID Priority State Nbr Address Interface 10.10.1.9 n/a FULL 10.10.0.64 1/1/28 10.10.1.6 n/a FULL 10.10.0.40 2/1/28 HERCP-AG1-AC1#	Total Number of Neighbors : 2 Neighbor ID Priority State Nbr Address Interface 10.10.1.9 n/a FULL 10.10.0.64 1/1/28 10.10.1.6 n/a FULL 10.10.0.40 2/1/28 HERCP-AG1-AC1#	admin@HERCP.AG1-AI Last login: 20 User "admin" h HERCP-AG1-AC1# HERCP-AG1-AC1# VRF : default	1 [02:43:29 PM] 25-01-23 21: as logged in show ip osp	/ × + 49:25 from - 3 times in of nei	the console the past 30 days Process : 1	
Neighbor ID Priority State Nbr Address Interface 10.10.1.9 n/a FULL 10.10.0.64 1/1/28 10.10.1.6 n/a FULL 10.10.0.40 2/1/28 HERCP-AG1-AC1#	Neighbor ID Priority State Nbr Address Interface 10.10.1.9 n/a FULL 10.10.0.64 1/1/28 10.10.1.6 n/a FULL 10.10.0.40 2/1/28 HERCP-AG1-AC1#	Total Number o	f Neighbors	: 2		
10.10.1.9 n/a FULL 10.10.0.64 1/1/28 10.10.1.6 n/a FULL 10.10.0.40 2/1/28 HERCP-AG1-AC1# ■	10.10.1.9 n/a FULL 10.10.0.64 1/1/28 10.10.1.6 n/a FULL 10.10.0.40 2/1/28 HERCP-AG1-AC1#	Neighbor ID	Priority	State	Nbr Address	Interface
10.10.1.6 n/a FULL 10.10.0.40 2/1/28 HERCP-AG1-AC1#	10.10.1.6 n/a FULL 10.10.0.40 2/1/28 HERCD-AG1-AC1#	10.10.1.9	n/a	FULL	10.10.0.64	1/1/28
HERCP-AG1-AC1#	HERCD-AG1-AC1#	10.10.1.6	n/a	FULL	10.10.0.40	2/1/28
		HERCP-AG1-AC1#	•			

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	n for the device: HERCP-AG1-AC1					🕓 Current Sessio	n ▼ Q () []
admin@HERCP-AG1-AC1	103:08:35 PM1 🥒 🗙 🕇 +						
User "admin" has	s logged in 4 times in the past	30 days					
HERCP-AG1-AC1# s	show ip route						
Displaying ipv4	routes selected for forwarding						
Origin Codes: C	- connected, S - static, L - lo	ocal					
R	- RIP, B $-$ BGP, O $-$ OSPF, D $-$ D	DHCP					
Type Codes: E	- External BGP, I - Internal BG A - OSPF internal area, E1 - OSF	SP, V - VPN, EV - EVPN SF external type 1					
E	2 - OSPF external type 2						
Flags: F	- FIB-optimized route						
VRF: default							
Prefix	Nexthop	Interface	VRF(egress)	Origin/	Distance/	Age	
Prefix	Nexthop	Interface	VRF(egress)	Origin/ Type	Distance/ Metric	Age	
Prefix 0.0.0.0/0	Nexthop 10.10.0.64	Interface 1/1/28	VRF(egress) 	Origin/ Type O/E2	Distance/ Metric [110/50]	Age 02m:01w:06d	
Prefix 0.0.0.0/0	Nexthop 10.10.0.64 10.10.0.40	Interface 1/1/28 2/1/28	VRF(egress) 	Origin/ Type O/E2	Distance/ Metric [110/50] [110/50]	Аде 02m:01w:06d 02m:01w:06d	
Prefix 0.0.0.0/0 10.0.0.0/13	Nexthop 10.10.0.64 10.10.0.40 10.10.0.64	Interface 1/1/28 2/1/28 1/1/28	VRF (egress) - - -	Origin/ Type O/E2 O/E2	Distance/ Metric [110/50] [110/50] [110/50]	Age 02m:01w:06d 02m:01w:06d 02m:01w:06d	
Prefix 	Nexthop 10.10.0.64 10.10.0.40 10.10.0.64 10.10.0.40	Interface 1/1/28 2/1/28 1/1/28 2/1/28	VRF (egress) - - - - - -	Origin/ Type O/E2 O/E2	Distance/ Metric [110/50] [110/50] [110/50] [110/50]	Age 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d	
Prefix 	Nexthop 10.10.0.64 10.10.0.40 10.10.0.64 10.10.0.64 10.10.0.64	Interface 1/1/28 2/1/28 1/1/28 2/1/28 1/1/28	VRF (egress) 	Origin/ Type 0/E2 0/E2 0/E2	Distance/ Metric [110/50] [110/50] [110/50] [110/50] [110/50]	Age 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d	
Prefix 0.0.0.0/0 10.0.0.0/13 10.2.120.0/24	Nexthop 10.10.0.64 10.10.0.40 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.40	Interface 1/1/28 2/1/28 1/1/28 2/1/28 1/1/28 2/1/28 2/1/28	VRF(egress) - - - - - - - -	Origin/ Type O/E2 O/E2 O/E2	Distance/ Metric [110/50] [110/50] [110/50] [110/50] [110/50] [110/50]	Aga 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d	
Prefix 	Nexthop 10.10.0.64 10.10.0.40 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64	Interface 1/1/28 2/1/28 1/1/28 1/1/28 1/1/28 2/1/28 1/1/28	VRF (egress) - - - - - - - - - - - - - -	Origin/ Type O/E2 O/E2 O/E2 O/E2	Distance/ Metric [110/50] [110/50] [110/50] [110/50] [110/50] [110/50]	Age 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d	
Prefix 0.0.0.0/0 10.0.0.0/13 10.2.120.0/24 10.10.0.0/20	Nexthop 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.40	Interface 1/1/28 2/1/28 1/1/28 2/1/28 1/1/28 2/1/28 1/1/28 2/1/28	VRF(egress) - - - - - - - - - - - - - -	Origin/ Type O/E2 O/E2 O/E2 O/E2	Distance/ Metric [110/50] [110/50] [110/50] [110/50] [110/50] [110/50] [110/50]	Age 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d	
Prefix 0.0.0.0/0 10.0.0/13 10.2.120.0/24 10.10.0.0/20 10.10.0.4/31	Nexthop 10.10.0.64 10.10.0.40 10.0.0.40 10.10.0.40 10.10.0.40 10.10.0.64 10.10.0.40 10.10.0.64 10.10.0.64	Interface 1/1/28 2/1/28 1/1/28 1/1/28 2/1/28 1/1/28 2/1/28 1/1/28 1/1/28	VRF(egress) 	Origin/ Type O/E2 O/E2 O/E2 O/E2 O/E2	Distance/ Metric [110/50] [110/50] [110/50] [110/50] [110/50] [110/50] [110/50] [110/50] [110/18]	Age 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d	
Prefix 0.0.0.0/0 10.0.0/13 10.2.120.0/24 10.10.0.0/20 10.10.0.4/31	Nexthop 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.40	Interface 1/1/28 2/1/28 1/1/28 2/1/28 1/1/28 2/1/28 1/1/28 2/1/28 1/1/28 2/1/28 2/1/28	VRF(egress) 	Origin/ Type O/E2 O/E2 O/E2 O/E2 O	Distance/ Metric [110/50] [110/50] [110/50] [110/50] [110/50] [110/50] [110/50] [110/18] [110/18] [110/18]	Age 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d	
Prefix 0.0.0.0/0 10.0.0/13 10.2.120.0/24 10.10.0.0/20 10.10.0.4/31 10.10.0.6/31	Nexthop 10.10.0.64 10.10.0.40 10.0.0.40 10.10.0.40 10.10.0.40 10.10.0.44 10.10.0.40 10.10.0.40 10.10.0.40 10.10.0.40 10.10.0.64 10.10.0.64	Interface 1/1/28 2/1/28 1/1/28 1/1/28 2/1/28 2/1/28 1/1/28 2/1/28 2/1/28 1/1/28 2/1/28 1/1/28	VRF (egress) 	Origin/ Type 0/E2 0/E2 0/E2 0/E2 0 0 0	Distance/ Metric [110/50] [110/50] [110/50] [110/50] [110/50] [110/50] [110/18] [110/18] [110/18]	Age 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d	
Prefix 0.0.0.0/0 10.0.0/13 10.2.120.0/24 10.10.0.0/20 10.10.0.4/31 10.10.0.6/31	Nexthop 10.10.0.64 10.10.0.40 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64 10.10.0.64	Interface 1/1/28 2/1/28 1/1/28 2/1/28 2/1/28 2/1/28 2/1/28 2/1/28 2/1/28 2/1/28 2/1/28 2/1/28 2/1/28	VRF(egress) - - - - - - - - - - - - - - - - -	Origin/ Type 0/E2 0/E2 0/E2 0/E2 0 0 0	Distance/ Metric [110/50] [110/50] [110/50] [110/50] [110/50] [110/50] [110/50] [110/50] [110/18] [110/18] [110/18]	Age 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 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							
E Console session for the device: HERCP-CR1-2							So Session Found ▼ Q (i) []
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 Feers : 8 Cfg. Hold Time : 180 Confederation Id : 0	BGP Router Ide Log Neighbor C Cfg. Keep Aliv	entifier Changes Ve	: 10.10 : No : 60	0.1.0			
Address-family : IPv4 Unicast							
Address-family : IPv6 Unicast							
Address-family : VPNv4 Unicast							
Address-family : L2VPN EVPN							
Neighbor 10.10.1.2 10.10.1.3 10.10.1.4 10.10.1.5 10.10.1.10 10.10.1.11 10.10.1.12	Remote-AS 65001 65001 65001 65001 65001 65001 65001	MsgRcvd M 121298 1 121302 1 121161 1 121245 1 121158 1 121205 1 121176 1	(sgSent 21426 21340 21406 21385 21363 21415 21445	Up/Down Time 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d 02m:01w:06d	State Established Established Established Established Established Established	AdminStatus Up Up Up Up Up Up 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

E Console session for the device:	ERCP-AG1-AC1	🚯 Current Session 🔻 🔍 🚺 🚼
admin@HERCP-AG1-AC1 [03:24:20 PM] 🥒	+	
Last login: 2025-01-23 23:08:	38 from ::1	
User "admin" has logged in 5	times in the past 30 days	
HERCP-AG1-AC1# show evpn evi		
L2VNI : 100		
Route Distinguisher	: 10.10.1.23:100	
VLAN	: 100	
Status	: up	
RT Import	: 65001:100	
RT Export	: 65001:100	
Local MACs	: 0	
Remote MACs	: 0	
Peer VTEPs	: 0	
T.21/NT + 200		
Poute Distinguisher	. 10 10 1 23.200	
VT.AN	. 200	
Status	: up	
BT Import	: 65001:200	
BT Export	: 65001:200	
Local MACs	: 0	
Remote MACs	: 0	
Peer VTEPs	: 0	
L2VNI : 302		
Route Distinguisher	: 10.10.1.23:302	
VLAN	: 302	
Status	: up	
RT Import	: 65001:302	
RT Export	: 65001:302	

Step 3 In a **Remote Console** window, type the command *show bgp l2vpn evpn* and press ENTER. Verify EVPN overlay routes.

REMOTE CONSOLE								
E Console session for the device: HERCP-AG1-AC1				e.	Current Session 🔻 🔍 🛈 🚼			
admin@HERCP-AG1-AC1 [10401:02 PM] 🖊 🗙 🕇 +								
Last login: 2025-01-23 23:24:23 from ::1 Jser "admin" has logged in 6 times in the past 30 days HERCP-AI-AC1# show bgp 12vpn evpn Status codes: s suppressed, d damped, h history, * valid, > best, = multipath, i internal, e external S Stale, R Removed, a additional-paths Origin codes: i - IGP, e - EGP, ? - incomplete								
EVPN Route-Type 1 prefix: [1]:[ESI]:[EthTag] EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP] EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP] EVPN Route-Type 4 prefix: [4]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr] VRF : default Local Router-ID 10.10.1.11								
Network	Nexthop	Metric	LocPrf	Weight	Path			
Route Distinguisher: 10.10.1.15:102 (I.2VNT 102)								
*>i [2]:[0]:[0]:[00:00:00:00:01]:[10.10.6.1]	10.10.1.15	0	100	0	?			
* i [2]:[0]:[0]:[00:00:00:00:01]:[10.10.6.1]	10.10.1.15	0	100	0				
*>i [3]:[0]:[10.10.1.15]	10.10.1.15	0	100	0				
* i [3]:[0]:[10.10.1.15]	10.10.1.15	0	100	0				
Route Distinguisher: 10.10.1.15:201 (L2VNI 201)								
*>i [2]:[0]:[0]:[00:00:00:00:01]:[10.10.8.1]	10.10.1.15	0	100	0				
* i [2]:[0]:[0]:[00:00:00:00:01]:[10.10.8.1]	10.10.1.15	0	100	0				
*>i [3]:[0]:[10.10.1.15]	10.10.1.15	0	100	0				
* i [3]:[0]:[10.10.1.15]	10.10.1.15	0	100					
Route Distinguisher: 10.10.1.15:301 (L2VNI 301)								

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 CO	REMOTE CONSOLE							
i≣ Cons	🗄 Console session for the device: HERCP-AG1-AC2							
admin@HE	RCP-AG1-AC2 [04:13:15 PM]	/ × +						
HERCP-A	G1-AC2# show evpn m	ac-ip						
Flags:	Local(L), Remote(R), Sticky bit(S)						
EVI	MAC	IP	Next-hop	Seq-Num	Flags			
202		10 10 4 1		·				
303	00:00:00:00:00:00:01	10 10 4 1	rr = 1/10 + 10 + 24	2	T'2			
303	00:00:00:00:00:00:01	10.10.4.1	vxlan1(10.10.1.25)	5	R.S			
303	20:a6:cd:c3:09:e4		vxlan1(10.10.1.24)	ō	R			
303	20:a6:cd:c3:09:e4	10.10.4.80	vxlan1(10.10.1.24)	0	R			
303	d0:d3:e0:c0:8d:b1				L			
303	d0:d3:e0:c0:8d:b1	10.10.4.76		0	L			
303	d0:d3:e0:c0:90:ff		vxlan1(10.10.1.24)	0	R			
303	d0:d3:e0:c0:90:ff	10.10.4.75	vxlan1(10.10.1.24)	0	R			
303	fc:7f:fl:c0:ab:bc	10 10 4 77		0	L			
303	IC:/I:II:CU:AD:DC	10.10.4.77		0	L L			
303	fa.7f.fl.a0.b2.fg	10 10 4 92	vx1an1(10.10.1.25)	0	R			
505	10./1.11.00.05.18	10.10.4.02	Vx1an1(10.10.1.25)	v	R			
MACs Remote 1	:6 MACs:3							
HERCP-A	31-AC2#							

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								
\Xi Console session for the device: HERCP-AG1-AC1 😳 Current Session 👻 🔍 🛈 🖸								
admin@HERCP-AG1-AC1 [04:16:45 P	M] 🖉 🗙	+						
Last login: 2025-01-24 User "admin" has logged HERCP-AG1-AC1# HERCP-AG1-AC1# show int	00:12:3 in 8 t erface	9 from ::1 imes in the pa vxlan 1	st 30 days					
Interface vxlanl is up Admin state is up Description: Underlay VRF: default Destination UDP port: 4 VTEP source IPV4 addres	Interface vxlanl is up Admin state is up Description: Underlay VRF: default Destination UDP port: 4789 VTEF source IFv4 address: 10.10.1.23							
inter valan bridging mo	ae: aen	Y.						
replication-mode : ingr	ess							
VNI Routing	VLAN	VRF	VTEP Peers		Origin			
100 disabled	200		 					
302 disabled	302							
303 disabled	303							
10000 enabled		Infrastructur	e 10.10.1.14		evpn			
10000 enabled		Infrastructur	e 10.10.1.15		evpn			
10000 enabled		Infrastructur	e 10.10.1.22		evpn			
10000 enabled		Infrastructur	e 10.10.1.24		evpn			
10000 enabled		Infrastructur	e 10.10.1.25		evpn			
20000 enabled		Corporate	10.10.1.15		evpn			
30000 enabled		Guest	10.10.1.15		evpn			
HERCP-AG1-AC1#								

Step 6 In a **Remote Console** window, type the command *show port-access clients* and press EN-TER. Verify the authentication state of an endpoint and confirm proper role assignment.



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

E Console s	ession for the device: HERCP-AG1-AC1					O Current Session ▼ Q (i)
admin@HERCP-A HERCP-AG1-A HERCP-AG1-A	G1-AC1[04:16:45 PM]					
Port Access	GBP User Configured Policy Detai	ls: =====				
GBP Name GBP Type GBP Status	: CONTRACTOR_r2r_policy : Local : Applied					
SEQUENCE	CLASS	TYPE	ACTION			
10 20 30	CONTRACTOR_ALLOW CONTRACTOR_ALLOW CONTRACTOR_ALLOW	gbp-ipv4 gbp-ipv6 gbp-mac	permit permit permit			
GBP Name GBP Type GBP Status	: CRITICAL_r2r_policy : Local : Applied					
SEQUENCE	CLASS	TYPE	ACTION			
10 20 30	CRITICAL_ALLOW CRITICAL_ALLOW CRITICAL_ALLOW	gbp-ipv4 gbp-ipv6 gbp-mac	permit permit permit			
GBP Name GBP Type GBP Status	: EMPLOYEE_r2r_policy : Local : 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.

ල්		<u>으</u>	
Access Points	Switches	Gateways	
Gateways	• Online	 Offline 0 	Clusters
2	2		1

Step 4 In the Name column, click the name of the fabric connected cluster.

	Gateways 2							
G	Gateway Clusters (1)							
	Name		Group					
>	 auto_group 	_938 (2 👗)	HERCP-FAB					

Step 5 Select the Tunnels page.

😇	<u>ඉ</u>				<u>়</u>					
Summary	mary Gateways				ry Gateways Tunnels					
CLUSTER	CLUSTER INFO									
CLUSTER NA	CLUSTER NAME									
auto_group	auto_group_938									
CURRENT L	CURRENT LEADER VERSION									
10.6.0.3_90	10.6.0.3_90581									

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".

(GATEWAYS HERCP-STB1-GW1 ¥									
	Tunnels (6)									
		Destination Device		∀ VxLAN ×	▼ Status 🗸	SSID	VNI (VxLAN)			
	>	10.10.1.14	10.10.1.14	VxLAN	• Up		102,201			

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.

HPE aruba networking	aruba-solution-tm	e			
Monitoring Configuration	Administration Orchestrator	Support Search Menu			
OVERLAYS & SECURITY	NETWORKING	TEMPLATES & POLICIES	CLOUD SERVICES		
Business Intent Overlays Apply Overlays Interface Labels Hubs Regions Deployment Profiles Internet Traffic Definition <i>Security</i> Firewall Zone Matrix Firewall Zone Matrix Firewall Zone Definition Firewall Zone Security Policies Firewall Protection Profiles IPSec Key Rotation Inbound Port Forwarding Advanced Security Settings	Deployment Interfaces NAT VRRP DNS Proxy WCCP PPPoE USB LTE Loopback Orchestration Loopback Interfaces Virtual Tunnel Interfaces (VTI) DHCP Server Defaults DHCP Leases DHCP Failover State Link Aggregation Cluster Profiles	Templates System, QoS, Opt, Tunnels, UDA, Shaper, Routes Apply Template Groups Policies Route Policies QoS Policies Schedule QoSMap Activation Optimization Policies SaaS NAT Policies ACLs Access Lists Address Groups Service Groups Shaping Shaper	AWS Network Manager HPE SSE Microsoft Azure Virtual WAN Microsoft Office 365 Zscaler Internet Access Netskope Service Orchestration <i>IaaS</i> Deploy Cloud Hubs in AWS Deploy Cloud Hubs in Azure Deploy Cloud Hubs in GCP		
Roles Custom CA Certificate Trust Stor End Entity Certificates Clients Table Network Access Control (NAC)	Clusters re Bridge Groups Routing Routes Regional Routing	Applications & SaaS User Defined Applications SaaS Optimization Application Definitions Application Groups			
SSL Certificates SSL CA Certificates	Routing Segmentation (VRF) Management Services BGP	AppExpress Groups Apply AppExpress Groups <i>TCAs</i>			
SSL for SaaS BGP ASN Global Pool Discovery OSPF Discovered Appliances BFD Preconfiguration Multicast Configuration Wizard Peer Priority Admin Distance Management Routes Licenses VXLAN		IP SLA			
	Tunnels Tunnels Auto MTU Discovery Tunnel Exception				

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.

HPE or uba aruba	HPE networking aruba-solution-tme											
Search tags, appliances 8 Appliances +/- 1 Selected Show Tags AMS 8 / RRANCH 6										nterfaces × Routes		
BOIBR-ECE1 BOIBR-ECE1 C M M CHIBR-ECE-1 C M M CHIBR-ECE-2 A HERCH-EC-1 C M HERCH-EC-2 A HERCH-EC-2	Interfaces 🕜 All Hardware Dynamic 12 Rows, 1 Selected											
A RSVDC-ECE1	A HERCP-EC-1	mgmt0	Interfaces - HE	RCP-EC-1								×
			Interface	s 🕐								
	HEROP-EC-1											
	HEROP-EC-1	wan2	Hardv	All Interfa	ces Assigned Interfac							
<u> </u>	HEROP-EC-1										Search	
	/ HEROP-EC-1	lan1	Name	Admin Status	IP Address/Mask 🔺	Public IP	Segment	Speed (Mbps) /	State	мти мас	SNMP IfIndex	Туре
	/ HEROPEC-I		mgmt0		172.16.101.15/24			auto / auto	1000 / full	1500 00:1B:BC:07:09		
	/ HEROPECT	theo		up down	169.254.0.1/16			auto / auto		1500 00:1B:BC:07:09		
	/ HERCE-EC-1		wan0	up up			Default	auto / auto	1000 / full	1500 00:18:8C:07:09	:CF 3 R	945
	# HERCE-EC-1			up up				auto / auto		1500 00:18:8C:07:09		
			wan2	up down				auto / auto		1500 00:18:8C:07:09		945
								auto / auto	1000 / full 🦲	5 9000 00:18:BC:07:09		
				up up			Default	auto / auto	1000 / full (6 9000 00:1B:BC:07:09		345
								auto / auto		1500 00:18:8C:07:09		
			twan0	up down				10000 / full		1500 00:1B:BC:07:09		FP
				up down				10000 / full		1500 00:18:8C:07:09		
			Dynar 2 Rows	ıic							Search	
				Name	Status	LACP Status	IP Add	ress/Mask 🔺	Segmen		SNMP	IfIndex .
												Save Cancel

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.**

ば HERCP-FAB	0
— Manage ————	
B Overview	
Devices	

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

법 HERCP-FAB	0
— Manage ————	
B Overview	
Devices	

Step 4 Click Switches, then select Config.

Customer: Orange TME	Ø		<u>@</u>	II. Summary	:= List	Config
ដ Hercp-fab	Access Points	Access Points Switches		,		
	MultiEdit					

Step 5 Enable the MultiEdit Toggle.

Step 6 Select the two border switches.

Step 7 Click Edit Config.

ultiEdit	configuration (editor & express configuration).						Configuration Stat
Device-Level Configuration earch and select devices and choos	on e either of the methods below to charge configuration for	r the selected devices.					
ortestual Search Engine Inter Search Query (e.g. nae-statu		SEARCH & FILTER Che	ck Search Documentation				
Devices (14)							6
4ame	15. Firmware Version	Config Modified	Status	Config Status	NAE Status	MAC Address	IP Address
ERCP-AG1-AC1	10.14.1010	Oct 24, 2024, 17:02:08	Online	Sync	Normal	64e881-dac7c0	172.16.101.31
RCP-AG1-AC2	10.14.1010	Oct 24, 2024, 17:02:08	Online	Sync	Normal	8c85c1-48a9c0	172.16.101.57
RCP-AG2-AC1	10.14.1010	Oct 24, 2024, 17:02:08	Online	Sync	Normal	8c85c1-48ff00	172.16.101.24
RCP-AG2-AC2	10.14.1010	Oct 24, 2024, 17:02:09	Online	Symc	Normal	8c85c1-496080	172.16.101.74
RCP-CR1-1	10.14.1010	Oct 18, 2024, 17:26:59	Online	Sync	Normal	00fd45-68bec0	172.16.101.28
:RCP-CR1-2	10.14.1010	Oct 18, 2024, 17:26:59	Online	Sync	Normal	00fd45-68de80	172.16.101.73
RCP-CR1-AG1-1	10.14.1010	Oct 18, 2024, 15:53:38	Online	Sync	Normal	00fd45-68ed00	172.16.101.85
RCP-CR1-AG1-2	10.14.1010	Oct 18, 2024, 15:53:38	Online	Sync	Normal	00fd45-680e80	172.16.101.30
RCP-CR1-AG2-1	10.14.1010	Oct 18, 2024, 15:53:39	Online	Sync	Normal	98f2b3-68e7e6	172.16.101.23
RCP-CR1-AG2-2	10.14.1010	Oct 18, 2024, 15:53:38	Online	Sync	Normal	98f2b3-6817e4	172.16.101.32
	10.14.1010						
RCP-CR1-STB1-1	10.14.1010	Oct 25, 2024, 20:23:07	Online	Sync	Normal	00fd45-67dd40	172.16.101.83
RCP-CR1-STB1-2	10.14.1010	Oct 25, 2024, 20:23:06	Online	Sync	Normal	00fd45-68ed40	172.16.101.26
							2 item(s) selected Clear
							VIEW CONFIG EDIT CONFIG EXPRESS 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.

HPE GreenLake								
		Q Search for failed clients, network dev						
Customer: Orange TME	©							
🕸 Global 🛛 🌖 📄	RAPIDS Authentication & Policy Gateway IDS/IPS Firewall Client Roles							
Manage	Role-to-Role Policy Enforcement							
問 Overview	ROLES (13)							
	∀ Name	Policy Identifier						
	CONTRACTOR	201						
	EMPLOYEE	100						
2. Guests	IOT-INTERNAL	700						
Applications	IOT-LMT-INET	800						
😯 Security	IOT-NO-INET	600						
🗞 Network Services	IT-ADMIN	200						
Analyze	IT-SUPP	300						
Analy20	PRINTER	500						
0 Alerts & Events	QUARANTINE	1000						
🗾 Audit Trail	REJECT	900						
S Tools	SECURITY	1200						
0 10013	VISITOR	400						
료 Reports								

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**.

HPE or ubo networking	aruba-solution-tme			
Monitoring Configuration	Administration Orchestrator			
OVERLAYS & SECURITY	NETWORKING	TEMPLATES & POLICIES	CLOUD SERVICES	
Business Intent OverlaysDeployApply OverlaysInterfaceInterface LabelsNATHubsVRRPRegionsDNS PrDeployment ProfilesWCCPInternet Traffic DefinitionPPPoESecurityUSB LTFirewall Zone MatrixLoopbaFirewall Zone MatrixLoopbaFirewall Zone Security PoliciesVirtualFirewall Zone Security PoliciesDHCP IInbound Port ForwardingDHCP IAdvanced Security SettingsLink AgIDS/IPSClusterCustom CA CertificatesRoutingSSLChrifticatesNetwork Access Control (NAC)RegionSSL CertificatesBGPSSL CortificatesBGPSSL CortificatesBGPSSL for SaaSDSPFDiscovered AppliancesPreconfigurationPreconfiguration WizardAdminLicensingManagLicensesVXLANCloud PortalTunnels	Deployment Interfaces NAT VRRP DNS Proxy WCCP PPPoE USB LTE Loopback Orchestration Loopback Interfaces Virtual Tunnel Interfaces (VTI) DHCP Server Defaults DHCP Leases DHCP Failover State Link Aggregation Cluster Profiles Clusters Brideo Crours	Templates System,QoS,Opt, Tunnels,UDA,Shaper,Routes Apply Template Groups Policies Route Policies QoS Policies Schedule QoSMap Activation Optimization Policies SaaS NAT Policies ACLs Access Lists Address Groups Service Groups Shaping Shaper Applications & SaaS User Defined Applications	AWS Network Manager HPE SSE Microsoft Azure Virtual WAN Microsoft Office 365 Zscaler Internet Access Netskope Service Orchestration <i>IaaS</i> Deploy Cloud Hubs in AWS Deploy Cloud Hubs in Azure Deploy Cloud Hubs in GCP	
	Routing Routes Regional Routing Routing Segmentation (VRF) Management Services BGP BGP ASN Global Pool OSPF BFD Multicast Peer Priority Admin Distance Management Routes VXLAN Tunnels Auto MTU Discovery Tunnel Exception	SaaS Optimization Application Definitions Application Groups AppExpress Groups Apply AppExpress Groups <i>TCAs</i> Threshold Crossing Alerts IP SLA		

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.

Roles ?		×
Add Role Import CSV		
14 ws, 1 Selected	Search	
Role	GPID	
IOT-LMT-INET	800	×
IOT-NO-INET	600	×
IT-SUPP	300	×
PRINTERS	500	×
QUARANTINE	1000	×
REJECT	900	×
SECURITY	1200	×
VISITOR	400	×
CONTRACTOR	200	×
		Cancel

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).

HPE aruba networking	aruba-solution-tme					
Monitoring Configuration	Administration	Orchestrator	Support	segment		
OVERLAYS & SECURITY	NETWORKING		TEMPLATES	5 & POLICIES	CLOUD SERVICES	in
Business Intent Overlays Apply Overlays Interface Labels Hubs Regions Deployment Profiles Internet Traffic Definition <i>Security</i> Firewall Zone Matrix Firewall Zone Matrix Firewall Zone Definition Firewall Zone Definition Firewall Zone Security Policies Firewall Protection Profiles IPSec Key Rotation Inbound Port Forwarding Advanced Security Settings IDS/IPS Roles Custom CA Certificate Trust Store End Entity Certificates Clients Table	Deployment Interfaces NAT VRRP DNS Proxy WCCP PPPoE USB LTE Loopback Orchestration Loopback Interfaces Virtual Tunnel Interfaces (VTI) DHCP Server Defaults DHCP Leases DHCP Failover State Link Aggregation Cluster Profiles Clusters Bridge Groups <i>Routing</i> Routes		Templates System, QoS, Opt, Tunnels, UDA, Shaper, Routes Apply Template Groups Policies Route Policies QoS Policies Schedule QoSMap Activation Optimization Policies SaaS NAT Policies AcLs Access Lists Address Groups Service Groups Shaping Shaper Applications & SaaS User Defined Applications SaaS Optimization Application Definitions Application Groups		AWS Network Manager HPE SSE Microsoft Azure Virtual WAN Microsoft Office 365 Zscaler Internet Access Netskope Service Orchestration <i>JaaS</i> Deploy Cloud Hubs in AWS Deploy Cloud Hubs in Azure Deploy Cloud Hubs in GCP	erit ar
SSL SSL Certificates SSL CA Certificates SSL for SaaS Discovery Discovered Appliances Preconfiguration Configuration Wizard Licensing Licenses Cloud Portal	Routing Segme Management Se BGP BGP ASN Globa OSPF BFD Multicast Peer Priority Admin Distance Management R VXLAN Tunnels Tunnels Auto MTU Disco Tunnel Exception	ntation (VRF) ervices I Pool outes overy on	Apply Appl Apply Appl <i>TCAs</i> Threshold IP SLA	s Groups Express Groups Crossing Alerts		

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.

HPE aruba networking	aruba-sol	ution-tm	e		
Monitoring Configuration	Administration	Orchestrator	Support	Configuration ->	Networking -> Routing -> VXLA
MonitoringConfigurationOVERLAYS & SECURITYBusiness Intent OverlaysApply OverlaysInterface LabelsHubsRegionsDeployment ProfilesInternet Traffic DefinitionSecurityFirewall Zone MatrixFirewall Zone DefinitionFirewall Zone Security PoliciesFirewall Zone Security PoliciesFirewall Protection ProfilesIDS/IPSRolesCustom CA Certificate Trust StoreEnd Entity CertificatesClients TableNetwork Access Control (NAC)SSLSSL CertificatesSSL CortificatesSSL for SaaSDiscovered AppliancesPreconfigurationConfiguration WizardLicensesCloud Portal	Administration NETWORKING Deployment Interfaces NAT VRRP DNS Proxy WCCP PPPoE USB LTE Loopback Orchest Loopback Orchest Loopback Interfa Virtual Tunnel In DHCP Server Def DHCP Failover St Link Aggregation Cluster Profiles Clusters Bridge Groups Routing Routes Regional Routing Routes Regional Routing Routing Segmen Management Set BGP BGP ASN Global OSPF BFD Multicast Peer Priority Admin Distance Management Rou VXLAN Tunnels Auto MTU Discov Tunnel Exceptior	Orchestrator	Support TEMPLATES Templates Tunnels,UD/ Apply Temp Policies Route Polici QoS Policie Schedule Q Optimization SaaS NAT I ACLS Access List Address Gr Service Gro Shaping Shaper Applications User Definin SaaS Optim Application	Configuration -> System,QoS,Opt, ,,Shaper,Routes plate Groups cies is QoSMap Activation on Policies Policies s roups bups & SaaS ed Applications nization Definitions Groups s Groups Crossing Alerts	Networking -> Routing -> VXLA CLOUD SERVICES AWS Network Manager HPE SSE Microsoft Azure Virtual WAN Microsoft Office 365 Zscaler Internet Access Netskope Service Orchestration IaaS Deploy Cloud Hubs in AWS Deploy Cloud Hubs in GCP

Step 2 In the **Default Template Group** (or the assigned template applied to EdgeConnect), click **Show All**.

Template Group 🕐							
Default Template Group ^{1 min} /							
+Add -Delete 18-Se	p-24 15:52						
Active Templates	Show All >						
General Settings							
SNMP	9 2						
User Management	9mo						
Banner Messages	1y						
DNS	2у						
Logging	2у						
Date/Time	2у						
Networking							
Routes	1y						
Peer Priority	1y						
Admin Distance	2у						
Policies							
Shaper	2у						
Management Services	2у						
Tools							
CLI	1y						
Session Management	2у						

Step 3 Click and drag the **Route Redistribution Maps** from **Available templates** to **Active Templates**.

Active Templates	< Hide	Available Templates
General Settings		General Settings
SNMP 9n	10	System
User Management 9n	10	Auth/Radius/TACACS+
Banner Messages	Ly	Network Access Control (NAC)
DNS	<u>2</u> y	Flow Export
Logging	<u>2</u> y	HTTPS Certificate
Date/Time	2y	Overlavs
Networking		SSL Certificates
VXLAN	ld	SSL CA Certificates
Routes	Ly	SSI for SaaS
Peer Priority	Ly	Networking
Admin Distance	2y	VRRP
Route Redistribution Maps	2y	BGP
Policies Shapor	2.4	OSPE
Management Services	-y),,	BED
	-y	Delicios
	lv	User Defined Apps
Session Management	2v	
		Route Policies
		SaaS NAT Policies
		Threshold Crossing Alerts
		SaaS Optimization
		Security Policies
		DNS Proxy
		Firewall Protection Profiles

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**.

	a-solution-tme								Rolease User	9.5.2.40502 aruba-solution-tme-	licenses@hpe.com	
											2 1	
ANS 8 BRANCH 6 BROBE-ECEI	Template Group () () Default Template Group ^{33 mms} +Add -Delete 24 Oct-24 12:55		Route Redistri	ibution Maps 👔	03-Jun-22 13:12							
	Active Templates <16 General Settings	Available Templates	Mattalariouse Acco	Name	× Add Map	d Default Map Delete Map						
 PORBRECEL HUB 2 												
RSVDC-ECE2												
	Networking VCAN 44	SSL Certificates										
	Admin Distance 2y	Networking VRSP		1010 Source			BGP Local Preference 250					
	magan ba magan ba ka i sa i sa i sa i sa i sa i sa i sa i s	erg erg Herg Herg Annun Lan Annun Lan Annun Lan Annun Lan Annun Lan Ger Anton Ger Anton Ger Anton Ger Anton Ger Anton Ser Anton			Cruste Radio Radio Hadiorettaio Ha Rig Bano: 6100-250-045802	X Ni Guer						
	Bave Bave As Cansol Applies to all templates in group When are Templates Lpdated?											

Step 7 Click Add rule. Complete the following Set Actions fields, then click Add.

- Permit: checked
- BGP Local Preference: checked
- BGP Local Preference: 250

Add Rule		×
Priority 1010	Enable	
Select Match Criteria		
Source Protocol	BGP	
Prefix 🗖		
BGP Communities		
Set Actions		
Permit		
BGP Local Preference 🔽	250]
Metric 🗖		
BGP Communities 🔲		
	🔵 Append 🔵 Override 🔵 Remove 🕧	
Nexthop 🗖		
Comment		
	Add	Close

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.

HPE aruba networking	aruba-solution-tn	ne	
Monitoring Configuration	Administration Orchestrator	Support Configuration ->	Networking -> Routing -> VXLA
MonitoringConfigurationOVERLAYS & SECURITYBusiness Intent OverlaysApply OverlaysInterface LabelsHubsRegionsDeployment ProfilesInternet Traffic DefinitionSecurityFirewall Zone MatrixFirewall Zone DefinitionFirewall Zone Security PoliciesFirewall Zone Security PoliciesFirewall Zone Security PoliciesFirewall Protection ProfilesIDS/IPSRolesCustom CA Certificate Trust StoreEnd Entity CertificatesClients TableNetwork Access Control (NAC)SSLSSL CortificatesSSL for SaaSDiscoveryDiscovered AppliancesPreconfigurationConfiguration WizardLicensing	Administration Orchestrator NETWORKING Deployment Interfaces Interfaces NAT VRRP DNS Proxy WCCP PPPoE USB LTE Loopback Orchestration Loopback Interfaces Virtual Tunnel Interfaces (VTI) DHCP Server Defaults DHCP Failover State Link Aggregation Cluster Profiles Clusters Bridge Groups Routing Routing Routing Segmentation (VRF) Management Services BGP BFD Multicast Peer Priority Admin Distance	Support Configuration -> TEMPLATES & POLICIES Templates System,QoS,Opt, Tunnels,UDA,Shaper,Routes Apply Template Groups Policies Route Policies QoS Policies Schedule QoSMap Activation Optimization Policies SaaS NAT Policies Access Lists Address Groups Shaping Shaper Applications & SaaS User Defined Applications SaaS Optimization Application Definitions Application Groups Application Groups Application Groups Apply AppExpress Groups TCAs Threshold Crossing Alerts IP SLA	Networking -> Routing -> VXLA CLOUD SERVICES AWS Network Manager HPE SSE Microsoft Azure Virtual WAN Microsoft Office 365 Zscaler Internet Access Netskope Service Orchestration JaaS Deploy Cloud Hubs in AWS Deploy Cloud Hubs in GCP
Licenses Cloud Portal	VXLAN <i>Tunnels</i> Auto MTU Discovery Tunnel Exception		

Step 2 In the **Default Template Group**, (or the assigned template applied to EdgeConnect), click **Show All**.

Template Group 🕐	
Default Template Group	$1 \min_{\prime}$
+Add -Delete 18-Se	p-24 15:52
Active Templates	Show All >
General Settings	
SNMP	9 2
User Management	9mo
Banner Messages	1y
DNS	2у
Logging	2у
Date/Time	2у
Networking	
Routes	1y
Peer Priority	1y
Admin Distance	2у
Policies	
Shaper	2у
Management Services	2у
Tools	
CLI	1y
Session Management	2у

Step 3 Click and drag the VXLAN template from Available templates to Active Templates.

Template Group 🕐						
Default Template Group	4 mins					
+Add -Delete 18-Sep-24 15:52						
Active Templates		< Hide	Available Templates			
General Settings			General Settings			
SNMP	9mo		System			
User Management	9mo		Auth/Radius/TACACS+			
Banner Messages	1y		Network Access Control (NAC)			
DNS	2у		Flow Export			
Logging	2у		HTTPS Certificate			
Date/Time	2у		Overlays			
Networking			SSL Certificates			
Routes	1y		SSL CA Certificates			
Peer Priority	1y 2		SSL for SaaS			
	2y 54./		Networking			
	эчу		VRRP			
Shaper	2y		Route Redistribution Maps			
Management Services	2y		BGP			
Tools			OSPF			
CLI	1y		BFD			
Session Management	2у		Policies			
			User Defined Apps			
			Access Lists			
			Route Policies			
			OoS Policies			
			Optimization Policies			
		drag	SaaS NAT Policies			
		S	Threshold Crossing Alerts			
			SaaS Ontimization			
			DNC Drawn			
			Firewall Protection Profiles			



VXLAN 😰		
Common settings for all VNIs		
VXLAN Settings		
Destination UDP port	4789	Leave blank to preserve existing setting on appliances
VTEP source interface	lo20000 🗸	

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

Add VNI Mapping			×
VNI	10000		
Segment	Infrastructure	~	
Firewall zone	LAN	~	
Fallback role	Don't apply	~	
			OK Cancel

Step 7 Repeat the above steps for the following VNIs.

VNI	Segment
20000	Corporate
30000	Guest

VXLAN 📀					
Common settings for all	VNIs				
VXLAN Settings					
Destination UDP po	rt 4789 Leave blank to	preserve existing setting on appliances			
VTEP source interfa	ice 1020000 V				
VNI Mapping					
Add					
3 Rows				III Search	
Edit	Virtual Network Identifier (VNI)	Segment	Firewall Zone	Fallback Role	
		Infrastructure	LAN	Don't apply	
		Corporate		Don't apply	
// 30000		Guest	LAN	Don't apply	

Step 8 In the Template Group window, click Save.

Add Doloto 19-Ser	-24 15:5
+Auu -Delete 10-Set	5-24 15.5
Active Templates	Show All
General Settings	
SNMP	9mo
User Management	9mo
Banner Messages	1y
DNS	2y
Logging	2y
Date/Time	2y
Networking	
Routes	1y
Peer Priority	1y
Admin Distance	2y
VXLAN	54y
Policies	
Shaper	2y
Management Services	2у
Tools	
CLI	1y
Session Management	2у
8	
Save Save As C	ancel
	anoci

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.
--------	---------------------------------	----------------------------	----------------------------------

HPE or uba networking	aruba-solution-tm	ne	
Monitoring Configuration	Administration Orchestrator	Support Search Menu	
OVERLAYS & SECURITY	NETWORKING	TEMPLATES & POLICIES	CLOUD SERVICES
Business Intent Overlays Apply Overlays Interface Labels Hubs Regions Deployment Profiles Internet Traffic Definition <i>Security</i> Firewall Zone Matrix Firewall Zone Matrix Firewall Zone Definition Firewall Zone Security Policies Firewall Protection Profiles IPSec Key Rotation Inbound Port Forwarding Advanced Security Settings IDS/IPS Roles Custom CA Certificate Trust Store End Entity Certificates Clients Table Network Access Control (NAC) <i>SSL</i> <i>SSL</i> Certificates SSL Cartificates SSL Cortificates SSL for SaaS <i>Discovery</i> Discovered Appliances Preconfiguration Configuration Wizard Licenses Cloud Portal	Deployment Interfaces NAT VRRP DNS Proxy WCCP PPPoE USB LTE Loopback Orchestration Loopback Interfaces Virtual Tunnel Interfaces (VTI) DHCP Server Defaults DHCP Leases DHCP Failover State Link Aggregation Cluster Profiles Clusters Bridge Groups <i>Routing</i> Routes Regional Routing Routes Regional Routing Routing Segmentation (VRF) Management Services BGP BGP ASN Global Pool OSPF BFD Multicast Peer Priority Admin Distance Management Routes VXLAN <i>Tunnels</i> Tunnels Auto MTU Discovery Tunnel Exception	Templates System, QoS, Opt, Tunnels, UDA, Shaper, Routes Apply Template Groups Policies Route Policies QoS Policies Schedule QoSMap Activation Optimization Policies SaaS NAT Policies ACLs Access Lists Address Groups Service Groups Shaping Shaper Applications & SaaS User Defined Applications SaaS Optimization Application Definitions Application Groups AppExpress Groups Apply AppExpress Groups TCAs Threshold Crossing Alerts IP SLA	AWS Network Manager HPE SSE Microsoft Azure Virtual WAN Microsoft Office 365 Zscaler Internet Access Netskope Service Orchestration <i>IaaS</i> Deploy Cloud Hubs in AWS Deploy Cloud Hubs in AZURE Deploy Cloud Hubs in GCP

Step 2 Select the first EdgeConnect, HERCP-EC-1, from the sidebar.



Step 3 Click the Edit icon (pencil) beside the default segment.

BGP	BGP 🕜									
5 R	ows, 1 Selected									
Edit	Appliance 🔺	Segment								
Ø	HERCP-EC-1	Default								
Ø	HERCP-EC-1	Infrastructure								
Ø	HERCP-EC-1	Guest								
Ø	HERCP-EC-1	Corporate								

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

BGP - HERCP-EC-1 - Segment : Default							
BGP Information (?)							
Enable BGP							
Autonomous system number	65002	l					
Route target (1)							
	Import:Export						
Router ID	10.14.255.73						
(Router ID is common for BGP and	OSPF; changing it here will	update it for OSPF)					
Graceful restart							
Max restart time	120	(13600) Sec					
Stale path time	150	(13600) Sec					
AS path propagate							
Log BGP update messages	2						

Step 5 Under BGP Peers, click Add.

BGP - HERCP-EC-1 - Segment : Default						
BGP Information ?						
Enable BGP						
Autonomous system number	65002	1				
Route target 🛈]				
	Import:Export					
Router ID	10.14.255.73]				
(Router ID is common for BGP and	OSPF; changing it here will	update it for OSPF)				
Graceful restart						
Max restart time	120	(13600) Sec				
Stale path time	150	(13600) Sec				
AS path propagate						
Log BGP update messages	2					
202.2						
BGP Peers						
Add 5						

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

Update Peer - Segment : De	Update Peer - Segment : Default X					
BGP Peer Information	1 🔮					
Peer IP	10.10.1.4					
Peer Adjacency	Single-Hop Multi-Hop					
EVPN Peer 🛈	✓					
Local Interface	lo20000 V					
Peer ASN	65001					
Override ASN						
Peer Type	Branch ~					
Routes learned from PE-route	er peer will not be advertised to SD-WA	N Fabric.				
Admin Status	UP DOWN					
Soft Reconfiguration						
Next-Hop-Self						
Inbound route map	RTMAP-BGP-HIGHER-LP V					
Outbound route map	default_rtmap_bgp_outbound_br ~	/				
BFD	_					
Keep Alive Timer*	60	(065535) Sec				
Hold Timer*	180	(065535) Sec				
* Timer changes only take ef Admin Down, Up for chang	fect when BGP session is reset. es to take effect immediately.					
Enable MD5 Password 🗌	l i i i i i i i i i i i i i i i i i i i					
Password						
Confirm Password						
		Ok Cancol				
NOTE:						
The peer IP is the Loopbac	ck0 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.

BGP - HERCP-EC-1 - Segment : Default									×								
BGP	Informa	atior	n 🕐														
Ena	ble BGP		Common settings for all segments														
Aut	onomous s	ystem	number [65002					Route ad	vertisement loop	o detection (Rout	e loop detection	n occurs at the s	tart of each de	etection interval)		
Rou	ite target (Max route upo	lates per peer	10					
				Import:Expo	rt					Detection inte	rval	15	∨ m	inutes			
Roi	ter ID			10 14 255 73													
(Ro	uter ID is c	omma	n for BGP and C	SPF: changing i	t here will updat	e it for OSPF)											
Gra	ceful restar	t															
40	noth propo	anto		_													
	paur propa	yate															
Log	BGP updal	te mes	ssages	<													
BGP P	eers																
Ad																	
21														Search			
Edi	t IP.		Remote ASN	Override AS	Туре	EVPN Peer	Local Interfa	Next-Hop-Se	Inbound Ro	Outbound R	Keep Alive Ti	Hold Timer	Soft Reconfi	BFD	Adjacency		
Ø	10.10.1.	4	65001	No	Branch	Yes	lo20000	No	RTMAP-BGP	default_rtm	60	180	No	No	Multi-Hop		
Ø	10.10.1.		65001	No	Branch		lo20000	Yes	RTMAP-BGP	default_rtm		180		No	Multi-Hop		

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

BGP - HERCP-EC-1 - Segment : Infrastructure									
BGP Information 📀									
Enable BGP				Common settings for all segme	nts				
Autonomous system number	65002			Route advertisement loop detection (R	oute loop detection occurs	at the start of each detection	n interval)		
Route target (i)	65001:10000			Max route updates per peer					
	Import:Export			Detection interval	15	✓ minutes			
Router ID	10.14.255.73								
(Router ID is common for BGP ar Graceful restart	d OSPF; changing it here wi	Il update it for OSPF)							
Max restart time									
Stale path time									
AS path propagate	•								
Log BGP update messages	2								
BGP Peers									
Add									
						III Search			
Edit IP 🔺 Remote A	SN Override ASN	Type Local Interfac	Next-Hop-Self Inbound Rout	. Outbound Ro Keep Alive Ti	Hold Timer Soft Recon	ifig BFD Adj	acency		
			No Data Availat	le					
							Save Cancel		

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 routemap. 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 Edge-Connect 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.**

ば HERCP-FAB	0
— Manage ————	
B Overview	
Devices	

Step 2 On the left menu, select Devices.

篇 HERCP-FAB	ं
— Manage —	
B Overview	
Devices	

Step 3 Select Switches, then select Config.

Customer: Orange TME	0		<u>e</u>	ii. Summary	List	Config
	Access Points	Switches	Gateways	,		
🛱 HERCP-FAB 🤇	\geq					
	MultiEdit					

Step 4 Enable the MultiEdit toggle.

Step 5 Select the two border switches.

Step 6 Click Edit Config.

ItiEdit 🐽 🌜	a configuration (editor & express configuration).						Configuration Sta
evice-Level Configurat irch and select devices and cho	ion ose either of the methods below to change configuration for	the selected devices.					
teetual Search Engine ter Search Query (e.g. nae-sta		SEARCH & FILTER Ch	eck Search Documentation				
evices (14)							
me	15. Firmware Version	Config Modified	Status	Config Status	NAE Status	MAC Address	IP Address
RCP-AG1-AC1	10.14.1010	Oct 24, 2024, 17:02:08	Online	Sync	Normal	64e881-dac7c0	172.16.101.31
CP-AG1-AC2	10.14.1010	Oct 24, 2024, 17:02:08	Online	Sync	Normal	8c85c1-48a9c0	172.16.101.57
CP-AG2-AC1	10.14.1010	Oct 24, 2024, 17:02:08	Online	Sync	Normal	8c85c1-48ff00	172.16.101.24
OP-AG2-AC2	10.14.1010	Oct 24, 2024, 17:02:09	Online	Sync	Normal	8c85c1-496080	172.16.101.74
IP-CR1-1	10.14.1010	Oct 18, 2024, 17:26:59	Online	Sync	Normal	00fd45-68bec0	172.16.101.28
IP-CR1-2	10.14.1010	Oct 18, 2024, 17:26:59	Online	Sync	Normal	00fd45-68de80	172.16.101.73
P-CR1-AG1-1	10.14.1010	Oct 18, 2024, 15:53:38	Online	Sync	Normal	00fd45-68ed00	172.16.101.85
-CR1-AG1-2	10.14.1010	Oct 18, 2024, 15:53:38	Online	Sync	Normal	00fd45-680e80	172.16.101.30
P-CR1-AG2-1	10.14.1010	Oct 18, 2024, 15:53:39	Online	Sync	Normal	98f2b3-68e7e6	172.16.101.23
P-CR1-AG2-2	10.14.1010	Oct 18, 2024, 15:53:38	Online	Sync	Normal	98f2b3-6817e4	172.16.101.32
	10.14.1010						
-CR1-STB1-1	10.14.1010	Oct 25, 2024, 20:23:07	Online	Sync	Normal	00fd45-67dd40	172.16.101.83
P-CR1-STB1-2	10.14.1010	Oct 25, 2024, 20:23:06	Online	Sync	Normal	00fd45-68ed40	172.16.101.26
							2 Bentis selected Cover
							Literity selected Creat
							VIEW CONFIG EDIT CONFIG EXPRESS COM

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.

Home » Configuration	» Pages » Web Logins					
Web Login (EXAMPLE Web Login)						
Use this form to make changes to the Web Login EXAMPLE Web Login .						
	Web Login Editor					
* Name:	EXAMPLE Web Login Enter a name for this web login page.					
Page Name:	Example_guest Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".					
Description:	Comments or descriptive text about the web login.					
* Vendor Settings:	Aruba Select a predefined group of settings suitable for standard network configurations.					
Login Method:	Controller-initiated — Guest browser performs HTTP form submit Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.					
* Address:	securelogin.hpe.com Enter the IP address or hostname of the vendor's product here.					
Secure Login:	Use vendor default Select a security option to apply to the web login process.					
Dynamic Address:	The controller will send the IP to submit credentials In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.					

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, sele	ect Virtual IP Settings.
----------------------	---------------	-----------------	-------------	--------------------------

aruba		ClearPass Policy Manager Menu 🚍					
Dashboard 0	Adm	Administration » Server Manager » Server Configuration					
Monitoring • Configuration • Administration •	Sei	rver Configuration				 Image Cl Image Cluster-Wi Clear Macl Manage Point 	uster Password ide Parameters hine Authentication Cache plicy Manager Zones
- DearPass Portal				Targets			
Series and Privileges			Settings				
- Configuration	Pub	lisher Server: CPPM-1 [10	.2.120.94]			* Virtual IF	Settings
- Jog Configuration	#	Server Name 🔺	Management Port	Data Port	Zone	Cluster Sync	Last Sync Time
- Jocal Shared Folders	1.	O CPPM-1	(IPv4) 10.2.120.94	-	default	Enabled	-
- 🥜 Licensing	2.	O CPPM-2	(IPv4) 10.2.120.95	-	default	Enabled	Apr 05, 2021 19:02:32 UTC
→ Device Insight 	Show	wing 1-2 of 2	Collect Logs	Back Up	Restore	Shutdown	Reboot Drop Subscriber

Step 4 On the **Virtual IP** Settings page, observe and record the **Virtual IP** configured for the CPPM cluster.

Virtual IP Settings				8				
Configure Virtual IPs for ClearPass High Availability								
Virtual IP	Primary Node	Secondary Node		Status				
1. 🖲 10.2.120.92	CPPM-1 [MGMT] 🥑	CPPM-2 [MGMT]		Enabled				
indicates current node serving Virt	ual IP							
Virtual IP Details -								
Select IP version:	IPv4 O IPv6							
Virtual IP:	10.2.120.92	10.2.120.92						
Virtual Host ID:	1 (1-255)							
	Node	Interface	Subnet					
Primary Node:	CPPM-1 V	10.2.120.94 [MGMT] 🗸	255.255.255.0					
Secondary Node:	CPPM-2 V	10.2.120.95 [MGMT] 🗸	255.255.255.0					
Enabled:								
		Res	set Delete Save	Close				

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 Versior		
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

© Copyright 2021 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. Aruba Networks and the Aruba logo are registered trademarks of Aruba Networks, Inc. Third-party trademarks mentioned are the property of their respective owners. To view the end-user software agreement, go to: www.arubanetworks.com/assets/legal/EULA.pdf



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