aruba
a Hewlett Packard Enterprise company

Validated Solution Guide

Aruba Solution TME

May 28, 2025

Table of Contents

ESP SD-WAN & Branch Deploy

This guide provides IT professionals with the prescriptive steps to deploy both SD-WAN & Branch network outlined in the Design document using the following products:

- Aruba Central
- Aruba ClearPass Policy Manager
- EdgeConnect Orchestrator
- EdgeConnect EC-US, EC-XS, EC-S-P, EC-M-H, EC-L-H
- Aruba Access Point 300, 600 and 500 Series
- Aruba Gateway 7000, 7200, and 9000 Series
- Aruba CX Switching 6100, 6200, and 6300

Document Conventions

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

Examples:

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

Italic text indicates the definition of important terminology, user interface input, or table heading.

Examples:

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

Code blocks indicates a variable for which you should 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 to SD-Branch

Software-defined branch (SD-Branch) is a technology shift toward solutions that are agile, open, and cloud-integrated. SD-Branch includes SD-WAN components that deliver a secure, service-provider-independent network with enterprise-level performance over disparate wide-area network (WAN) technologies. However, although SD-WAN solves a real IT problem, it addresses only part of the issue organizations face when dealing with distributed locations.

Organizations often roll out and operate distributed, heterogeneous networks with centralized teams. These distributed networks offer many services in addition to WAN connectivity. Branch networks require wired and wireless LANs, security and policy enforcement, and, of course, WAN interconnects. SD-Branch extends the concepts beyond SD-WAN to all elements in the branch, delivering a full-stack solution that includes SD-LAN and security that address all network connectivity needs.

When formulating the strategy for an SD-Branch rollout, Aruba recommends:

- Purchase as much WAN bandwidth as possible to alleviate potential bottlenecks during the busiest times of the day.
- Increase Internet bandwidth, instead of buying additional private bandwidth.
- Use cloud-based tools to simplify the configuration, operation, and management of the WAN.

Purpose of This Guide

This deployment guide covers the Aruba SD-Branch in the Edge Services Platform (ESP) architecture. It contains an explanation of the requirements that shaped the design and the benefits it can provide to your organization. The guide describes a single unified infrastructure that integrates access points (APs), switches, gateways, and network management with access-control and traffic-control policies. Refer to volume one of this VSG for design guidance:

Aruba VSG: SD-Branch Design

This guide assumes the reader has an equivalent knowledge of an Aruba Certified Mobility Associate or Aruba Certified Switching Associate.

Design Goals

The overall goal is to create a simple, scalable design that is easy to replicate across all sites in your network. The solution components are limited to a specific set of products to help with operations and maintenance. The key features addressed by Aruba SD-Branch include:

- **Simplicity with Zero Touch Provisioning (ZTP):** SD-Branch devices can be factory-shipped directly to a remote site. By automatically matching orders to an Aruba customer account, the mobile Installer app is available for third-party systems integrators to quickly install equipment. Standardized group- and device-level configurations for APs, switches, and gateways enable fast network deploymnet.

- **Unified policy management:** For Aruba and third-party network infrastructure, Aruba ClearPass delivers a common policy framework for multivendor wired and wireless networks. This software-defined approach makes it easy for the network administrator to distribute changes quickly based on corporate risk and compliance requirements. ClearPass Device Insight (CPDI) adds AI-powered device profiling to help automate discovery of the latest mobile and IoT endpoints.
- **Predictive analytics and assurance:** Aruba Central's artificial intelligence (AI), machine learning (ML), and automation capabilities identify issues and notify IT of problems with recommended changes. When shifting to a cloud-hosted model, data can be collected and crowdsourced from Aruba's installed base to take advantage of Aruba's extensive data science expertise.
- **Secure WAN connectivity:** Enable SD-WAN technology to support the use of the Internet to replace or augment private WAN services. Elements of the solution include: path quality monitoring (PQM) to track the available paths, stateful firewall with application fingerprinting to identify traffic flows, dynamic path selection (DPS) to use the optimal path, and centralized routing to free branch gateways (BGWs) from participating in the routing decisions. End-user identity information refines the selection of available WAN paths.
- **LAN automation with dynamic segmentation:** Most branch networks are needlessly complex because designs are based on a proliferation of VLANs, complex IP addressing schemes, access control lists (ACLs), and architectures tailored to the needs of automation software. The SD-Branch architecture flattens the branch into fewer subnets or even a single subnet, eliminating the dependence on static IP addressing schemes and hardwired ACLs across multiple devices. This is achieved by consolidating all policy enforcement into a single device in the branch.

Use this guide to design new networks or to optimize and upgrade existing networks. It is not intended as an exhaustive discussion of all options; it presents commonly recommended designs, features, and hardware.

Audience

This guide is written for IT professionals who need to design an Aruba SD-Branch network. These IT professionals serve in a variety of roles:

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

Customer Use Cases

Branch networks are changing rapidly. The most pressing challenges include an increasing number of mobile and IoT devices, growing bandwidth requirements of the business, and modern users who expect connectivity for work and personal use from anywhere at any time. The teams that run these distributed networks are often shrinking while demands increase.

Organizations expect new network rollouts within shorter timeframes, and IT organizations are asked to improve service levels, reduce costs, and shift spending from capital expense to operating expense.

This guide discusses the following use cases:

- Secure WAN communications using IPsec tunnels over an independent transport
- ZTP for all networking components in the branch
- Switch stacking for simplified management, high availability, and scalability
- Link aggregation for high bandwidth, redundancy, and resiliency between switches and gateways
- Wireless as the primary access method for branch employees
- Wireless and wired guest access for customers, partners, and vendors
- Consistent security for wired and wireless devices based on roles.

Aruba SD-Branch Network Deployment Overview

This section provides details for the SD-Branch deployment used in subsequent sections.

It is best practice to standardize the branch design for all sites to reap the full benefits of Aruba Central configuration. OWL Corp., however, has a requirement for two branch designs.

A pair of VPNCs (VPN concentrators) is configured to facilitate connectivity between the campus network and branch sites using IPsec tunnels and route sharing. VPNCs summarize the campus subnets to a single route of 10.0.X.X/13 and prevent advertising point-to-point links to the branches.

Each remote site has redundant branch gateways, and each gateway is connected to a single WAN transport. Switches at branch provide L2 connectivity for the APs and other client devices. Each branch site is assigned a /21 subnet from the superset address space of 10.14.X.X/16. Within the 10.14.X.X/16 address space, the 10.14.254.X/24 is reserved for Microbranch system IPs.

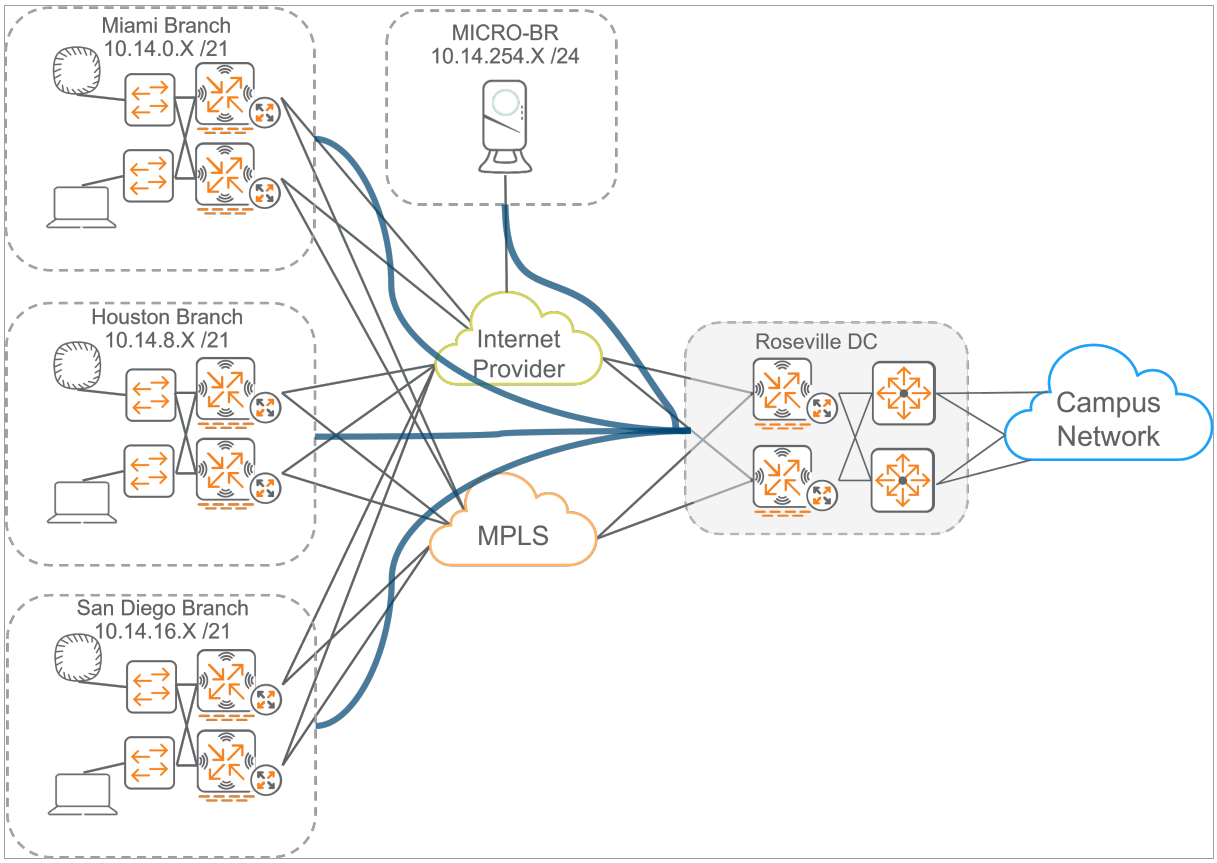


Figure 1: Network_Overview

Hub Site Configuration

- Gateways will be connected to the services aggregation block in the OWL campus network.
- Gateways will use OSPF to peer with the campus service aggregation.

- Gateways will have redundant connections to each aggregation block.
- Gateways will have redundant Internet and MPLS connections.
- Gateways will use eBGP for MPLS connectivity.
- The standby EdgeConnect appliance will have a lower metric than the primary to ensure route symmetry.
- EdgeConnect SD-WAN appliances will summarize campus routes before redistribution into the SD-WAN Fabric.
- Gateways will use the summary address 10.0.X.X/13 to advertise the Campus network to branch sites
- Gateways will summarize all branch sites to 10.14.X.X/16 to advertise to the Campus network.

RSVDC-VPNC1-1	VLAN	Local IP address	Port	Peer IP address	Peer Device
OSPF Uplink 1	4001	172.18.106.22/30	GE0/0/0	172.18.106.21/30	RSVCP-CR1-SS2-1
OSPF Uplink 2	4002	172.18.106.30/30	GE0/0/1	172.18.106.29/30	RSVCP-CR1-SS2-2
MPLS Uplink	2086	100.100.7.6	GE0/0/2	100.100.7.1	——-
Internet Uplink	2084	Static IP	GE0/0/3	——-	——-
Microbranch (CL2)	101	10.8.0.2 - VRRP (10.8.0.1)	——-	——-	——-
Gateway System IP	2085	10.0.6.111/32	——-	——-	——-

RSVDC-VPNC1-2	VLAN	Local IP address	Port	Peer IP address	Peer Device
OSPF Uplink 1	4001	172.18.106.18/30	GE0/0/0	172.18.106.17/30	RSVCP-CR1-SS2-1
OSPF Uplink 2	4002	172.18.106.26/30	GE0/0/1	172.18.106.25/30	RSVCP-CR1-SS2-2
MPLS Uplink	2086	100.100.7.5	GE0/0/2	100.100.7.1	——-
Internet Uplink	2084	Static IP	GE0/0/3	——-	——-
Microbranch (CL2)	101	10.8.0.2 - VRRP (10.8.0.1)	——-	——-	——-
Gateway System IP	2085	10.0.6.111/32	——-	——-	——-

Quantity	SKU	Description
2	9012	RJ45 console port 12 x 10/100/1000BASE-T ports 6 x PoE+ portsUSB Type A Host port 1xRJ45 console port Micro USB console port

NOTE:

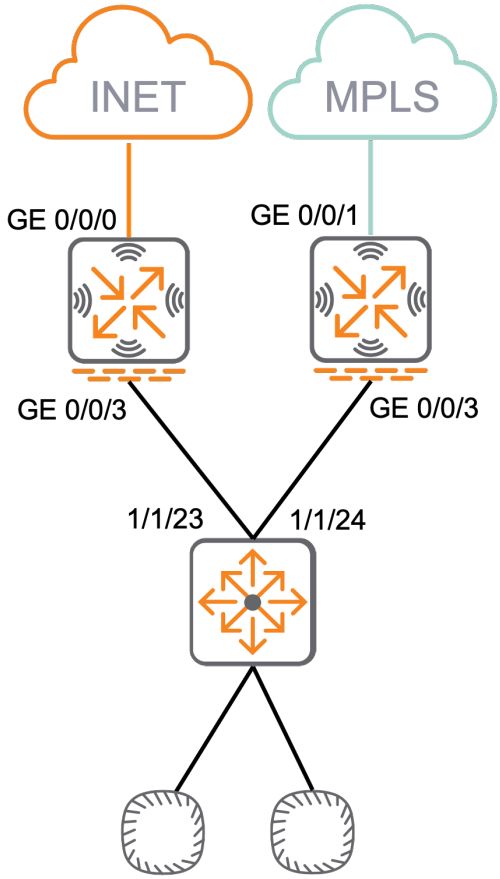
The equipment listed may not be the same equipment used in the guide; however, the configuration steps are alike.

Branch Site Requirements

- Wi-Fi should be the main connection used by employees. Ethernet connections should be available for use as needed. Ensure that switchport count is available for all users
- Access points should be mounted to the ceiling, not above the ceiling tile in plenum space or behind any barrier that may cause signal reflection or attenuation.
- Wireless coverage is required.
- Employees use Office 365 and Microsoft Teams for communications, along with other business productivity apps (Salesforce, SAP, etc.).
- Sites use IoT devices such as smart thermostats, smart access control, and meeting room kiosk.
- Sites must be able to upgrade with hitless failover.
- Sites have a single MPLS 10 Mbps download 5Mbps upload and Internet connection 100 Mbps download 25Mbps upload. Both are RJ-45 drops.
- Employee and guest SSIDs must be provided.

Low Traffic Site Requirements

OWL's low traffic site have the logical topology shown below.



Low Traffic Site Characteristics

- 3750 square feet, closed office space

- Low-traffic sites to support up to 30 employees, each with a docking station and a laptop.
- 10 large workspace
- 12 small workspace
- 18 open workspaces
- 4 conference rooms
- 1 IDFs
- 1 MDF/Computer Room

Low Traffic Branch Site Configuration

- Gateway 1 will use GE0/0/0 Port for INET connectivity.
- Gateway 2 will use GE0/0/1 eBGP for MPLS connectivity.
- Gateway will use GE0/0/2 to trunk listed VLANs down to the access switches' highest ethernet port.
- Gateway will be the default gateway for the site.
- Gateway will enable RADIUS snooping.
- Gateway should be version 10.4 or higher.
- Gateway will use DHCP relay for addressing devices.
- Access switches will use the standard feature template (MOTD, RADIUS, TACACS, User-Roles, STP, etc.).
- The first 12 Ports on access switching will be reserved for the access points.
- All IOT devices will be reserved for the next 24 ports.
- Workstations will be revered for the last 12 ports (special case ports).
- Access points should have two SSIDs for Guest and Corporate access

Required Equipment

Quantity	SKU	Description
2	9004	4 x 100/1000BASE-T ports1 x USB 3.0 portRJ45 console port Micro USB console port
2	6300F (JL663A)	48x ports 10/100/1000 BaseT ports 4x 1G/10G/25G/50G1 SFP ports 1x USB-C Console Port 1x OOBM port 1x USB Type A Host port 1x Bluetooth dongle to be used with CX Mobile App
6	Aruba 505 (R2H29A)	1.49 Gbps maximum real-world speed (HE80/HE20) WPA3 and Enhanced Open security Built-in technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devices OFDMA for enhanced multi-user efficiency IoT-ready Bluetooth 5 and Zigbee support

NOTE:

The equipment listed may not be the same equipment used in the guide; however, the configuration steps are alike.

Miami Branch Details

VLAN ID	Description	Network	Default Gateway (VRRP)	MIABR-ECB1-1 IP Address	MIABR-ECB1-2 IP Address
100	MGMT (Gateway System IP)	10.14.0.0	10.14.0.1	10.14.0.2	10.14.0.3
101	Employee	10.14.1.0/24	10.14.1.1	10.14.1.2	10.14.1.3
102	PRINTER	10.14.2.0	10.14.2.1	10.14.2.2	10.14.2.3
103	IoT (smart thermostats, smart access control, and meeting room kiosk.)	10.14.3.0/24	10.14.3.1	10.14.3.2	10.14.3.3
104	Guest	10.14.4.0	10.14.4.1	10.14.4.2	10.14.4.3
105	Reject	10.14.5.0/24	10.14.5.1	10.14.5.2	10.14.5.3
106	Critical	10.14.6.0	10.14.6.1	10.14.6.2	10.14.6.3
107	Quarantine	10.14.7.0/24	10.14.7.1	10.14.7.2	10.14.7.3
Sumr		10.14.0.0	——–	——–	——–

MIABR-ECB1-1	Local IP address	Port	Peer IP address	Peer Device
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0,	——–	MIABR-ECB1-CR1(STK)
MPLS Uplink	——–	GE0/0/1	——–	——–
Internet Uplink	DHCP (VLAN 4085)	GE0/0,	——–	——–

MIABR-ECB1-2	Local IP address	Port	Peer IP address	Peer Device
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0,	——–	MIABR-ECB1-CR1(STK)

MIABR-ECB1-2	Local IP address	Port	Peer IP address	Peer Device
MPLS Uplink	MPLS (VLAN 4085)	GE0/0/1	——–	——–
Internet Uplink	——–	GE0/0,	——–	——–

MIABR-ECB1-CR1	Local IP address	Port	Peer port	Peer Device
MGMT VLAN	DHCP	——–	——–	——–
Gateway Uplink 1	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	1/1/23	GE0/0/3	MIABR-ECB1-1
Gateway Uplink 2	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	1/1/24	GE0/0/3	MIABR-ECB1-2

Huston Branch Details

VLAN ID	Description	Network	Default Gateway (VRRP)	HOUBR-ECB1-1 IP Address	HOUBR-ECB1-2 IP Address
100	MGMT (Gateway System IP)	10.14.8.0	10.14.8.1	10.14.8.2	10.14.8.3
101	Employee	10.14.9.0/24	10.14.9.1	10.14.9.2	10.14.9.3
102	Printer	10.14.10.(	10.14.10.1	10.14.10.2	10.14.10.3
103	IoT (smart thermostats, smart access control, and meeting room kiosk.)	10.14.11.0/24	10.14.11.1	10.14.11.2	10.14.11.3
104	Guest	10.14.12.(	10.14.12.1	10.14.12.2	10.14.12.3
105	Reject	10.14.13.0/24	10.14.13.1	10.14.13.2	10.14.13.3
106	Critical	10.14.14.(	10.14.14.1	10.14.14.2	10.14.14.3
107	Quarantine	10.14.15.0/24	10.14.15.1	10.14.15.2	10.14.15.3
Sumr		10.14.8.0	——–	——–	——–

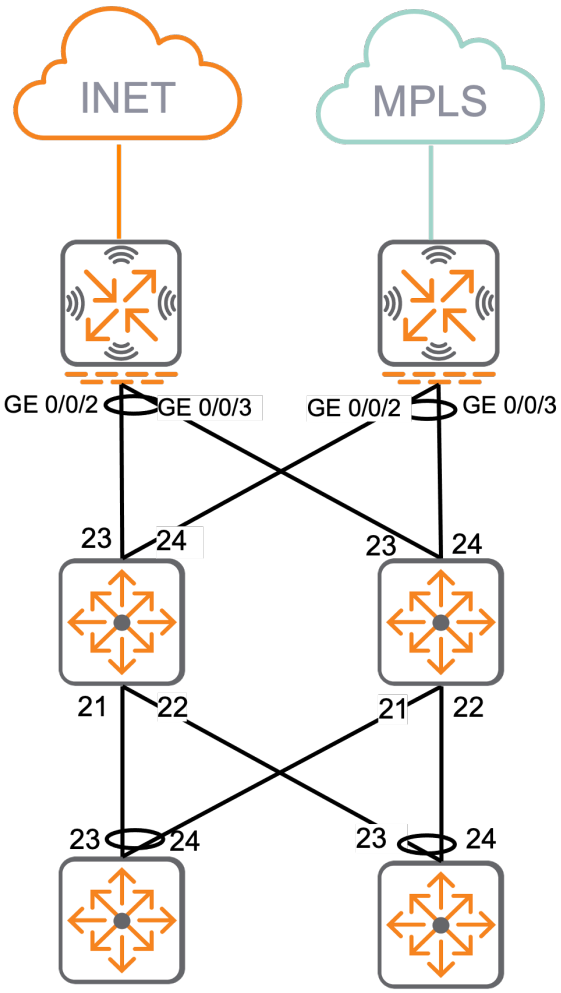
HOUBR-ECB1-1	Local IP address	Port	Peer IP address	Peer Device
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0,	1/1/23	HOUBR-ECB1-CR1(STK)
MPLS Uplink	——–	GE0/0/1	——–	——–
Internet Uplink	DHCP (VLAN 4085)	GE0/0,	——–	——–

HOUBR-ECB1-2	Local IP address	Port	Peer IP address	Peer Device
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0,	1/1/24	HOUBR-ECB1-CR1(STK)
MPLS Uplink	MPLS (VLAN 4085)	GE0/0/1	——–	——–
Internet Uplink	——–	GE0/0,	——–	——–

HOUBR-ECB1-CR1	Local IP address	Port	Peer port	Peer Device
MGMT VLAN	DHCP	——–	——–	——–
Gateway Uplink 1	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	1/1/23	GE0/0/2	HOUBR-ECB1-1
Gateway Uplink 2	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	1/1/24	GE0/0/2	HOUBR-ECB1-2

High Traffic Site Requirements

OWL's High traffic site have the logical topology shown below.



HIGH TRAFFIC BRANCH SITE CONFIGURATION

- All network infrastructure should use ZTP for provisioning.
- Gateway 1 will use WAN0 Port for INET connectivity.
- Gateway 2 will use WAN1 eBGP for MPLS connectivity.
- Gateways will be connected using LAN0 to enable WAN HA.
- Gateways will use LAN 1 to trunk listed VLANs down to the access switches' highest ethernet port.
- Gateways will use VRRP and be the default gateway for the site.
- Gateways will enable RADIUS snooping.
- Gateways should be version 9.2 or higher.
- Gateways will use DHCP relay for addressing devices.
- Access switches will use the standard feature template (MOTD, RADIUS, TACACS, User-Roles, STP, etc.).
- The first 12 ports on access switching will be reserved for the access points.
- All IoT devices will be reserved for the next 24 ports.
- Workstations will be reserved for the last 12 ports (special case ports).
- Access points should have two SSIDs for Guest and Corporate access

Quantity	SKU	Description
2	9004	4 x 100/1000BASE-T ports1 x USB 3.0 portRJ45 console port Micro USB console port
2	6300F (JL663A)	48x ports 10/100/1000 BaseT ports 4x 1G/10G/25G/50G1 SFP ports 1x USB-C Console Port 1x OOBM port 1x USB Type A Host port 1x Bluetooth dongle to be used with CX Mobile App
4	6200F (JL725A)	48x ports 10/100/1000 BaseT ports 4x 1G/10G SFP ports 1x USB-C Console Port 1x OOBM port 1x USB Type A Host port 1x Bluetooth dongle to be used with CX Mobile App
11	Aruba 505 (R2H29A)	1.49 Gbps maximum real-world speed (HE80/HE20) WPA3 and Enhanced Open security Built-in technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devicesOFDMA for enhanced multi-user efficiencyIoT-ready Bluetooth 5 and Zigbee support

NOTE:

The equipment listed may not be the same equipment used in the guide; however, the configuration steps are alike.

San Diego Branch Details

VLAN ID	Description	Network	Default Gateway (VRRP)	SANBR-ECB1-1 IP Address	SANBR-ECB1-2 IP Address
100	MGMT (Gateway System IP)	10.14.16.(	10.14.16.1	10.14.16.2	10.14.16.3
101	Employee	10.14.17.0/24	10.14.17.1	10.14.17.2	10.14.17.3
102	PRINTER	10.14.18.(	10.14.18.1	10.14.18.2	10.14.18.3
103	IoT (smart thermostats, smart access control, and meeting room kiosk.)	10.14.19.0/24	10.14.19.1	10.14.19.2	10.14.19.3
104	Guest	10.14.20.	10.14.20.1	10.14.20.2	10.14.20.3
105	Reject	10.14.21.0/24	10.14.21.1	10.14.21.2	10.14.21.3
106	Critical	10.14.22.	10.14.22.1	10.14.22.2	10.14.22.3
107	Quarantine	10.14.23.0/24	10.14.23.1	10.14.23.2	10.14.23.3
Sumr		10.14.16.(	——–	——–	——–

SANBR-ECB1-1	Local IP address	Port	Peer IP address	Peer Device
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0,	1/1/23	SANBR-ECB1-CR1(STK)
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0/3	1/1/24	SANBR-ECB1-CR1(STK)
MPLS Uplink	——–	WAN1	——–	——–
Internet Uplink	DHCP (VLAN 4085)	WAN0	——–	——–

SANBR-ECB1-2	Local IP address	Port	Peer IP address	Peer Device
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0,	2/1/23	SANBR-ECB1-CR1(STK)
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0/3	2/1/24	SANBR-ECB1-CR1(STK)
MPLS Uplink	MPLS (VLAN 4085)	WAN1	——–	——–
Internet Uplink	——–	WAN0	——–	—-

San Francisco Branch Details

VLAN ID	Description	Network	Default Gateway (VRRP)	SFOBR-ECB1-1 IP Address	SFOBR-ECB1-2 IP Address
100	MGMT (Gateway System IP)	10.14.24.	10.14.24.1	10.14.24.2	10.14.24.3
101	Employee	10.14.25.0/24	10.14.25.1	10.14.25.2	10.14.25.3
102	PRINTER	10.14.26.	10.14.26.1	10.14.26.2	10.14.26.3
103	IoT (smart thermostats, smart access control, and meeting room kiosk.)	10.14.27.0/24	10.14.27.1	10.14.27.2	10.14.27.3
104	Guest	10.14.28.	10.14.28.1	10.14.28.2	10.14.28.3
105	Reject	10.14.29.0/24	10.14.29.1	10.14.29.2	10.14.29.3
106	Critical	10.14.30.	10.14.30.1	10.14.30.2	10.14.30.3

VLAN ID	Description	Network	Default Gateway (VRRP)	SFOBR-ECB1-1 IP Address	SFOBR-ECB1-2 IP Address
107	Quarantine	10.14.31.0/24	10.14.31.1	10.14.31.2	10.14.31.3
Sumr		10.14.24.	——–	——–	——–

SFOBR-ECB1-1	Local IP address	Port	Peer IP address	Peer Device
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0,	1/1/23	SFOBR-ECB1-CR1(STK)
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0/3	1/1/24	SFOBR-ECB1-CR1(STK)
MPLS Uplink	——–	WAN1	——–	——–
Internet Uplink	DHCP (VLAN 4085)	WAN0	——–	——–

SFOBR-ECB1-2	Local IP address	Port	Peer IP address	Peer Device
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0,	2/1/23	SFOBR-ECB1-CR1(STK)
Access Downlink	Native VLAN: 100, Trunked VLAN: 101,102,103,104,105,106,107	GE0/0/3	2/1/24	SFOBR-ECB1-CR1(STK)
MPLS Uplink	MPLS (VLAN 4085)	WAN1	——–	——–
Internet Uplink	——–	WAN0	——–	—-

Preparing to Deploy Aruba SD-Branch Network

This section provides details for configuring Aruba Central to prepare for an SD-Branch deployment, including establishing interaction with HPE GreenLake.

Four requirements include: importing devices, licensing devices, creating groups, and creating site configuration.

This section also describes the fundamental differences between group and device configuration levels.

Device Management with HPE GreenLake

This section demonstrates how to applications to you HPE GreenLake account, add Aruba Central subscription keys, and add a new network device to the HPE GreenLake portal for management from Aruba Central.

The HPE GreenLake platform delivers a unified experience that enables customers to use a single dashboard to view, manage, and orchestrate the system's network, compute, storage infrastructure and related services.

Import and License Devices

To use Aruba Central, devices must be licensed and maintained in HPE GreenLake's inventory. Follow this procedure to import devices and apply the correct licenses. This article assumes that an account has been set up with HPE GreenLake and the Aruba Central application has been installed. If the prerequisite have not been complete, follow the documented process here.

Add a Subscription Key

Devices within Aruba Central require a subscription key to function. These keys grant access to various licenses, depending on the device type.

Step 1 On the HPE GreenLake top menu bar, select **Manage**.

Step 2 Click the **Subscriptions** tile.

Step 3 Click **Add Device Subscription**.

Step 4 In the **Add Device Subscription** window, enter the subscription key sent with the device or emailed after purchase. Click **Submit**.

Step 5 Repeat the process to continue adding subscription keys for additional devices as needed.

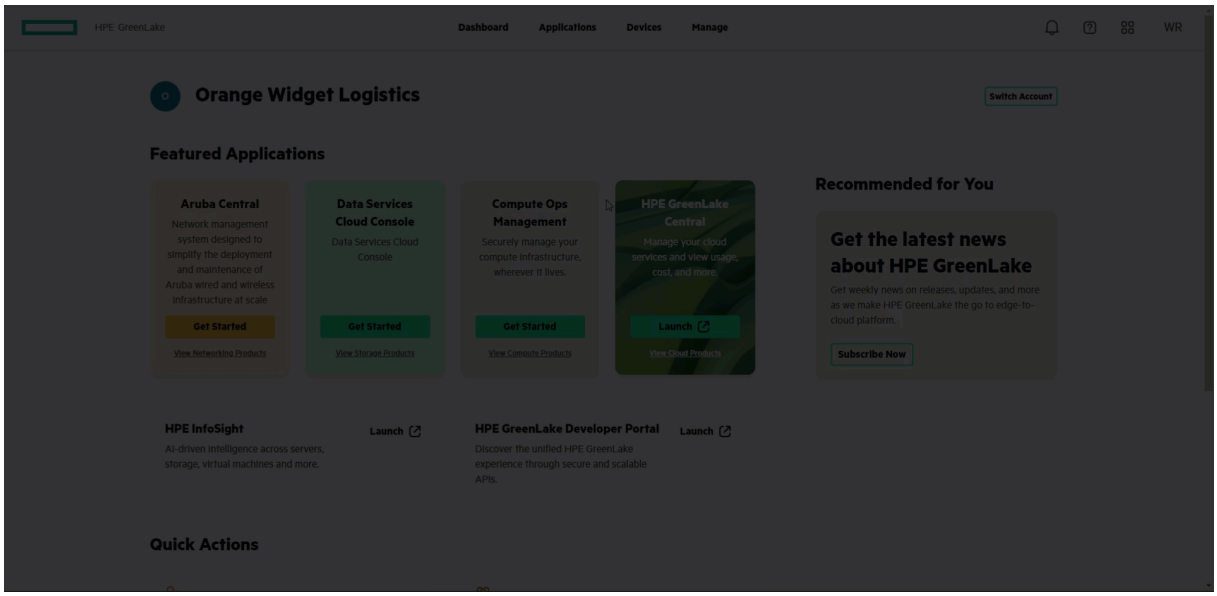


Figure 2: Add_Subscription_Key

Add a Device to GreenLake

Add network devices to HPE GreenLake using a .CSV file or by entering the Serial Number and MAC Address. Use the procedure below to enter the Serial Number and MAC Address. When complete, the device is assigned to Central automatically.

Step 1 On the HPE GreenLake top menu bar, select **Devices**.

Step 2 Click **Add Devices**.

Step 3 Select *Network Devices* as the **Device Type**, then click **Next**.

Step 4 On the **Ownership Type** list, click **Serial Number & MAC Address**.

Step 5 Type or paste the **Serial Number** and **MAC Address** values, then click **Enter**.

Step 6 Continue adding devices as needed. When finished, click **Next**.

Step 7 Tags are not entered in this example. Click **Next**.

Step 8 Review the list of devices and click **Finish**.

Step 9 Click **Close**.

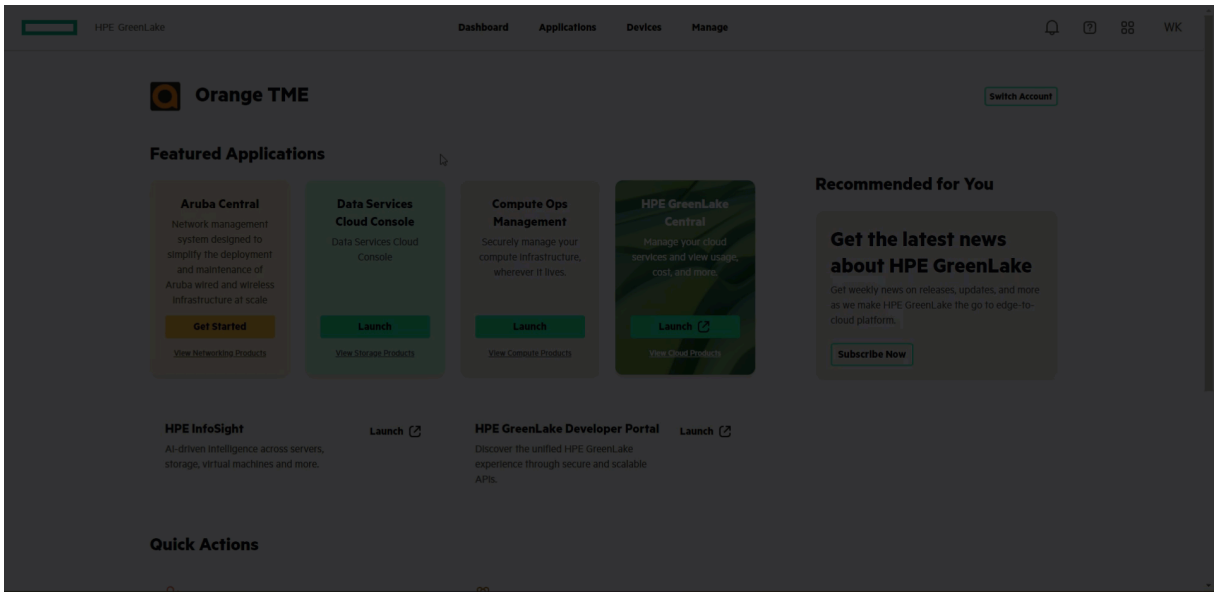


Figure 3: Add_Device

Assign Subscriptions to the Devices

The following procedure assigns the subscription key to the device. This procedure demonstrates manual subscription key assignment, but the process can be automated for some device types. Instructions for the automated process can be found here.

Step 1 On the HPE GreenLake top menu bar, select **Devices**.

Step 2 Click the **Require Subscriptions** tile.

Step 3 Click the checkbox for each device to be assigned a subscription.

Step 4 Click the **Actions** menu.

Step 5 Click **Apply Subscriptions**.

Step 6 Select the **Subscription Tier**, then select the **Subscription Key** to apply.

Step 7 Click **Apply Subscriptions**.

Step 8 Click **Finish**, then click **Close**.

Step 9 Repeat steps 2 to 8 for additional device types that require licensing.

NOTE:

This process supports multi-select in step 3 to license multiple devices, when applying the same license.

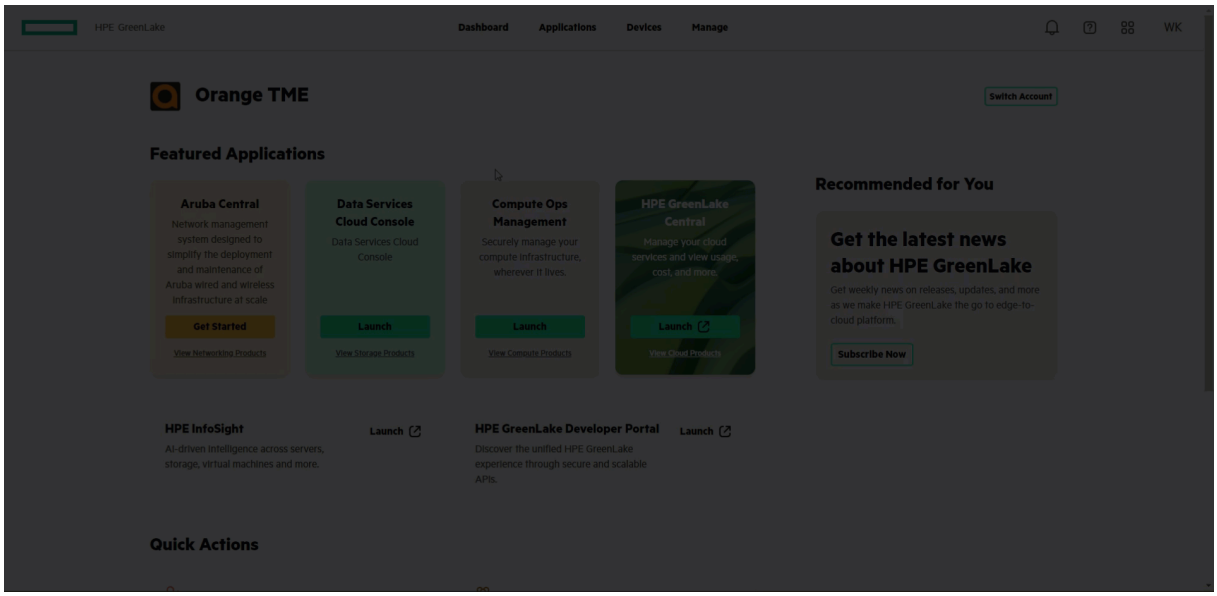


Figure 4: Apply_Subscription

This concludes the steps performed in HPE GreenLake. After completing the above steps, the device(s) are available for use in Aruba Central.

If a device is offline, it does not appear in any Aruba Central groups. In Central, use **Device Preprovisioning** to assign a device to a group and apply appropriate group and device level configuration. After a device is connected, Central downloads the pre-provisioned configuration.

Define Groups in Aruba Central

A device's final configuration settings are defined by its group configuration, and additional device-specific configurations, when applicable.

When creating device groups, the devices should have similar network functions so that common configurations such as VLANs, NTP, and DNS can be applied at the group level. Device-specific configurations, such as IP addresses, should be applied at the device level.

Central uses two group types: template groups and UI groups.

- Template groups are CLI-based configuration files pushed down to a device. Device-specific information can be defined using variables.
- With UI groups, all configuration is performed from the Central user interface. Device-specific configuration can be applied by selecting a particular device and configuring it individually in the user interface.

Template groups are an excellent choice when devices have overlapping configurations or when configurations do not change often. UI groups are a better choice for workflow-driven configurations and provide the flexibility to change single device configurations.

In both cases, devices in the same group must have similar configurations. If port layouts must change or the topology of the branch differs from other sites, create a unique group and configuration for that different site.

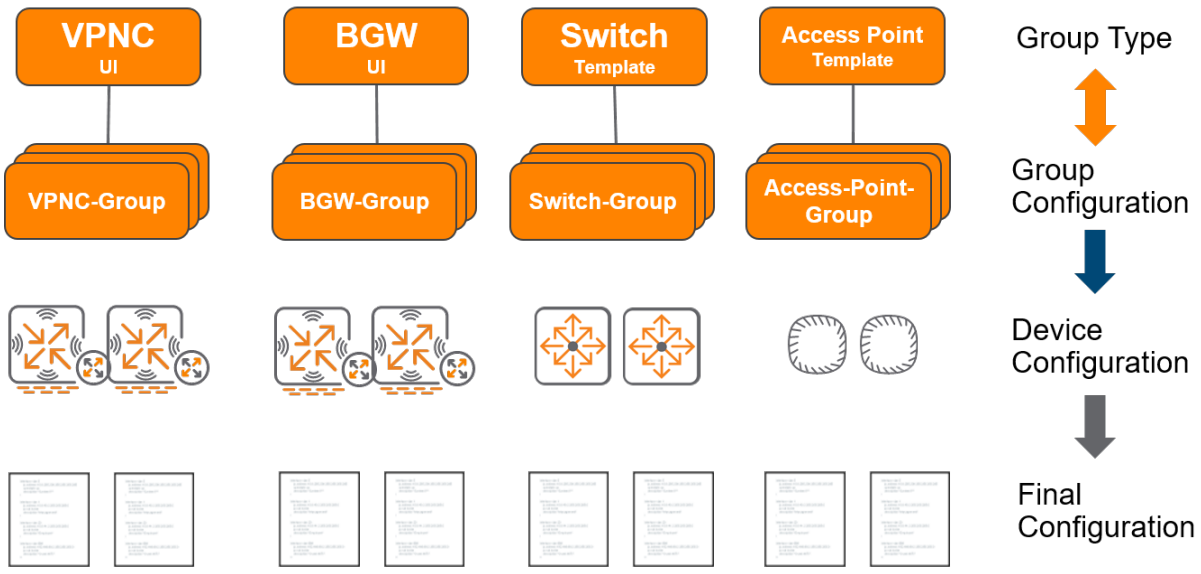


Figure 5: Configuration hierarchy

NOTE:

This graphic does not reflect the exact naming and type used in the guide. It is for reference purposes only.

Configure Device Groups

The following procedure creates a group. This guide uses the following groups and group types.

Device Type	Group Name	Group Type
VPNC	VPNC-RSVDC	UI Group
BGW, AOS-CX Switch, Access Point	BR-EC-SDB	UI Group
Micro Branch	BR-EC-MB	UI Group

Step 1 On the left navigation pane, in the **Maintain** section, select **Organization**.

Step 2 Click the **Groups** tab.

Step 3 Click the **+** (plus sign) to create a new group

Step 4 Enter a **Name** for the group, and select the appropriate checkbox in the **Group will contain** list. Follow the table above.

Step 5 Select the device **Architecture** and **Network Role**.

Step 6 Repeat Steps 3 through 5 for each group.

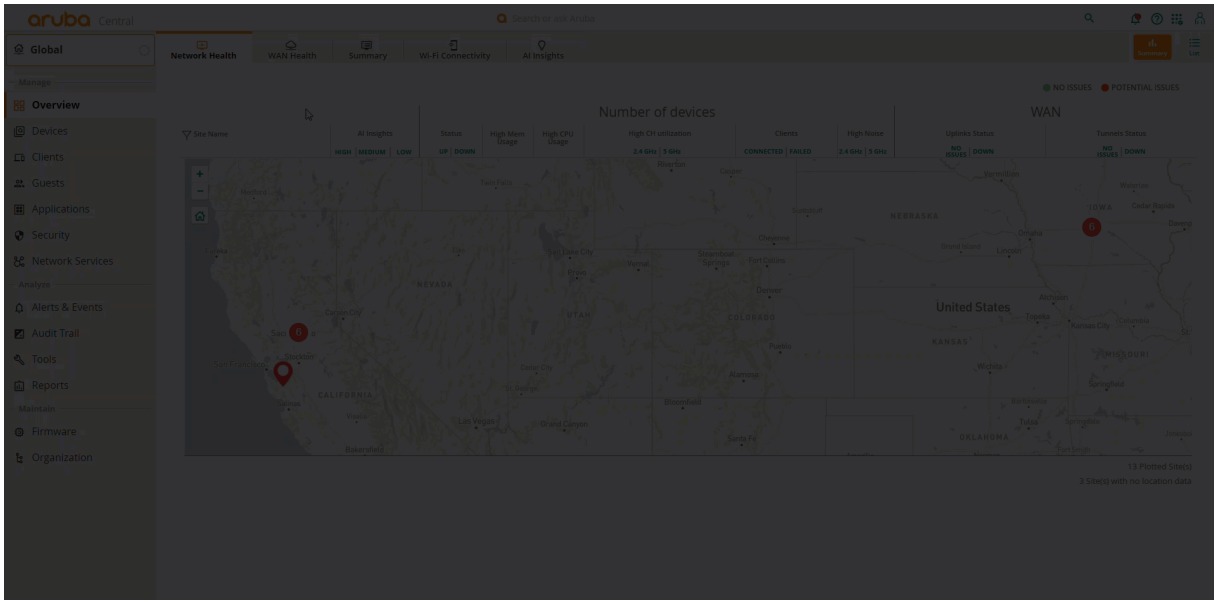


Figure 6: Create_Group

Create Sites

Central uses sites to group devices at the same geographical location. Sites also identify the gateways to be clustered together, and the APs and switches at the same location. This procedure creates sites, used later in this guide. This guide uses RSVDC, which is the hub location in Roseville CA. Chicago, Miami, and San Francisco are the example branch locations.

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

Step 2 In the dropdown, select **All Devices**.

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

Step 4 Click the **Sites** tile, then click **New Site** on the bottom left.

Step 5 In the **Create New Site** window, assign the following settings, then click **Add**.

- **Site Name**: *RSVDC*
- **Street Address**: *8000 foothills Blvd*
- **City**: *Roseville*
- **Country**: *United States*
- **State or Province**: *California*
- **Zip/Postal Code** : *95747*

Step 6 Repeat steps 4 and 5 for all remote sites. This guide uses the following sites:

Site Name
HOURBR
SANBR
MIABR
SFOBR

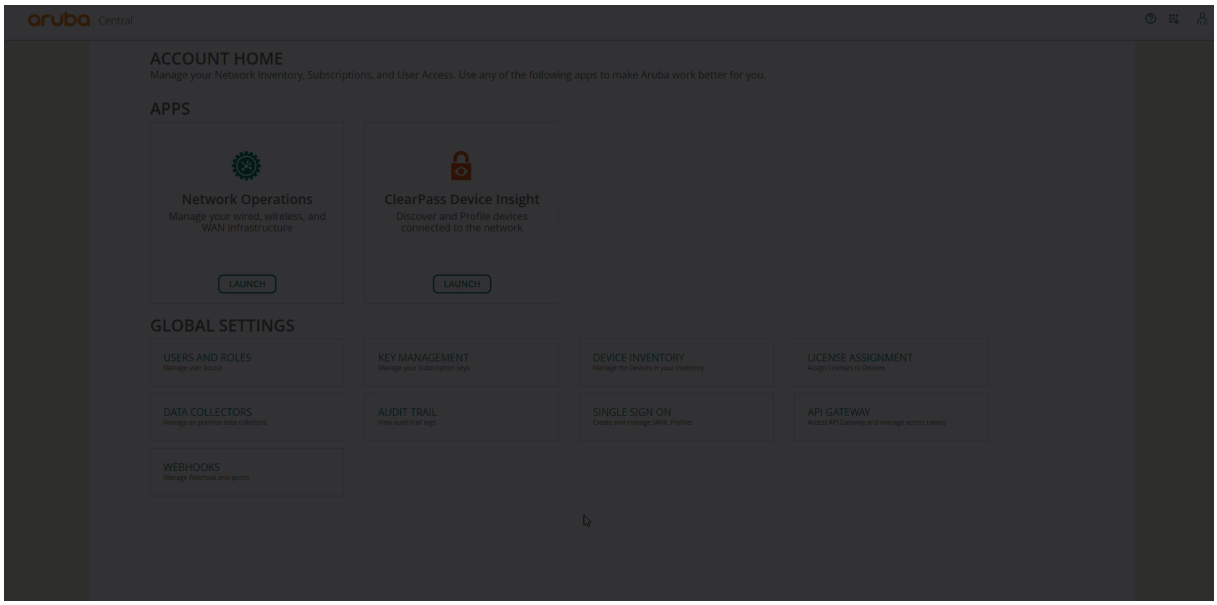


Figure 7: Adding Site

Preprovision Device in Central > Groups

Move the VPNC devices to the hub group (**VPNC-RSVDC**) and the branch gateways to the branch group (**BR-ECSDB**)

Step 1 In the **Aruba Central** app, set the filter to **Global**.

Step 2 Under **Maintain**, click **Organization**.

Step 3 Click the **Device Preprovisioning** tile.

Step 4 Select the device(s) to move to a selected group.

Step 5 Click the **Move** devices icon.

Step 6 Select the **Destination Group** from the dropdown.

Step 7 Click **Move**.

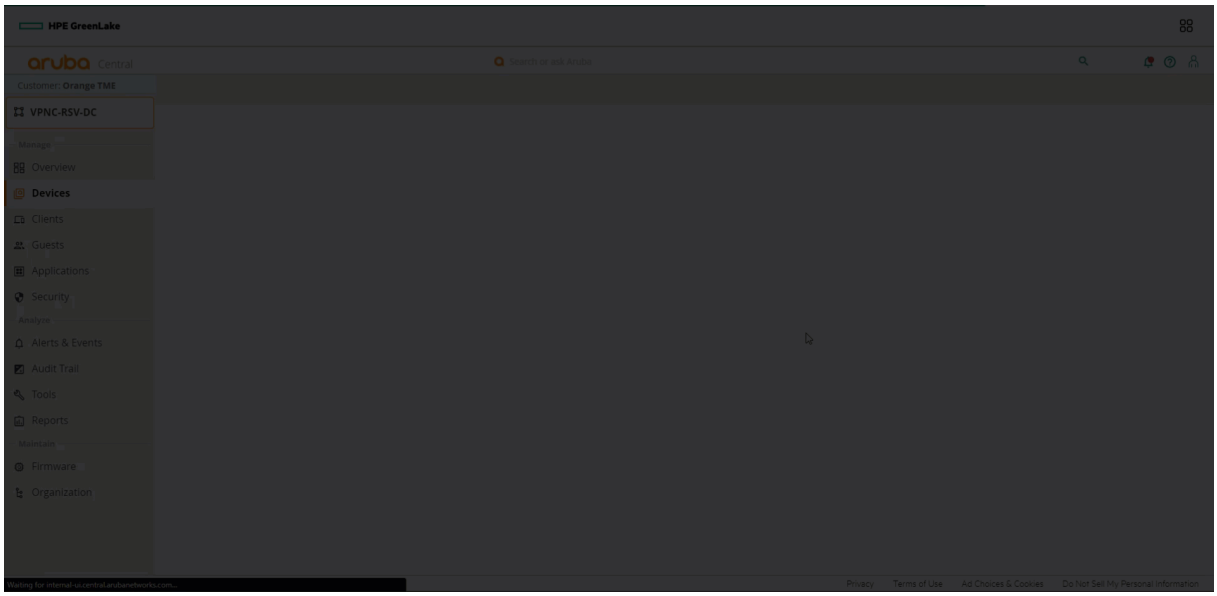


Figure 8: Verify_Preprovisioning

Preprovision Device in Central > Sites

Move the VPNC devices to the hub site (**RSVDC**) and the branch gateways, switches, and access points to the branch sites (**MIABR**, **HOUBR**, **SANBR**)

Step 1 In the **Aruba Central** app, set the filter to **Global**.

Step 2 Under **Maintain**, click **Organization**.

Step 3 Click the **Sites** tile.

Step 4 Select the device(s) to move to a selected site.

Step 5 Drag the devices to the corresponding site.

Step 6 Click **Yes** to confirm the move.

NOTE:

This step requires the system MAC address of the devices to determine the site to which they are moved. If that is not plausible, devices can be moved to the correct group after a hostname has been established later in the deployment process.

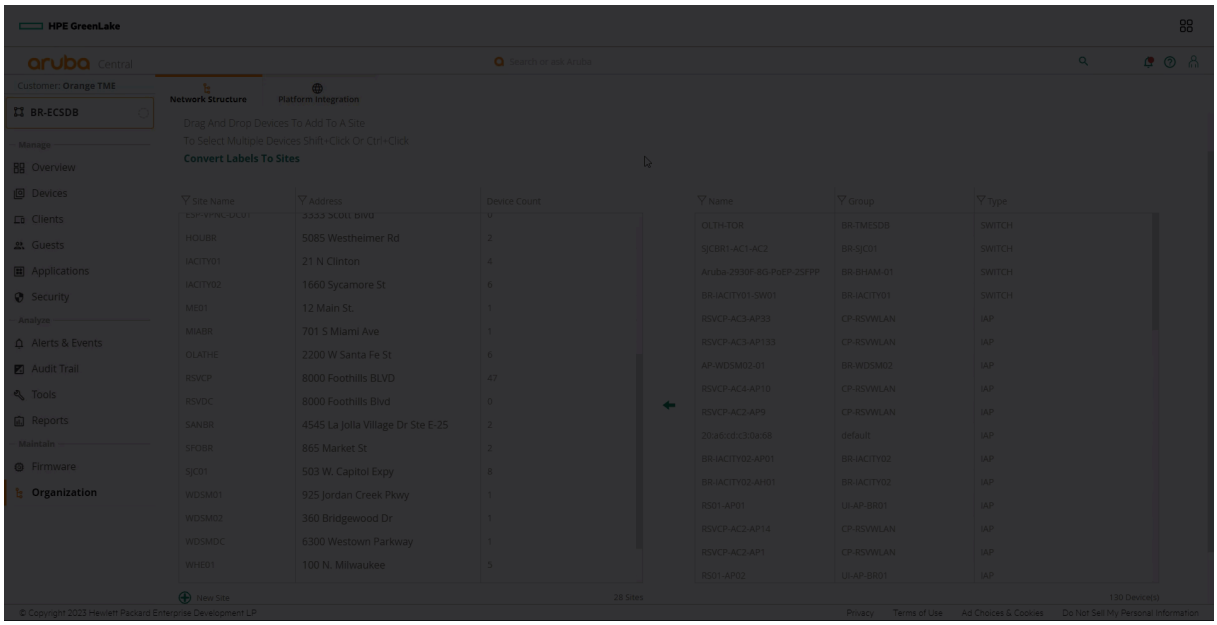


Figure 9: PreProvision Sites

Aruba VPNC Group Configuration

The VPNC is configured in two steps. First, the group level configuration includes all the common configurations such as NTP, DNS, and OSPF area. A majority of the configuration is performed at the group level. After the group is configured, device level configuration can be applied. Device level configuration includes entering device-specific information such as IP addresses, hostnames, etc.

Configure the VPNC Group

This procedure configures groups for VPNCs.

Step 1 In the **Global** filter dropdown, search or select the **VPNC-RSVDC** group.

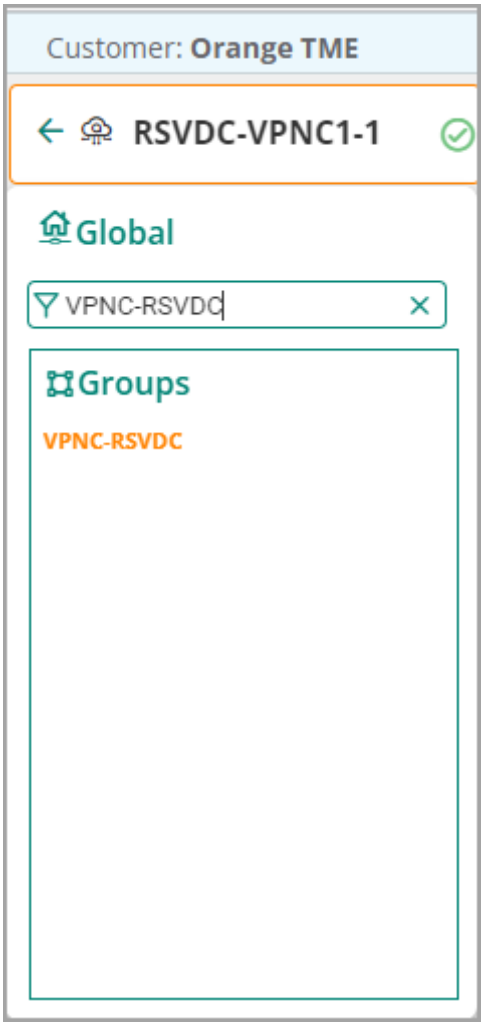


Figure 10: Select Group

Step 2 On the left navigation pane, in the **Manage** section, select **Devices**.

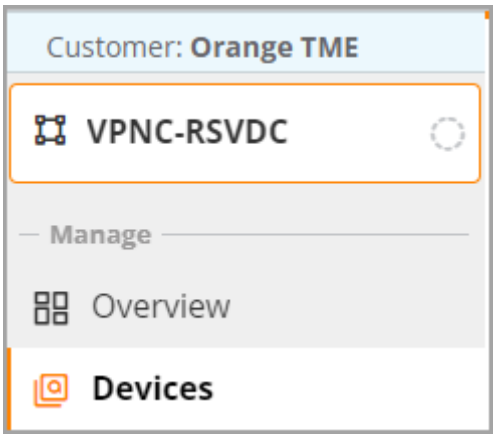


Figure 11: Select Devices

Step 3 Select the **Gateways** tab, then click the **Config** (gear) icon in the upper right corner.

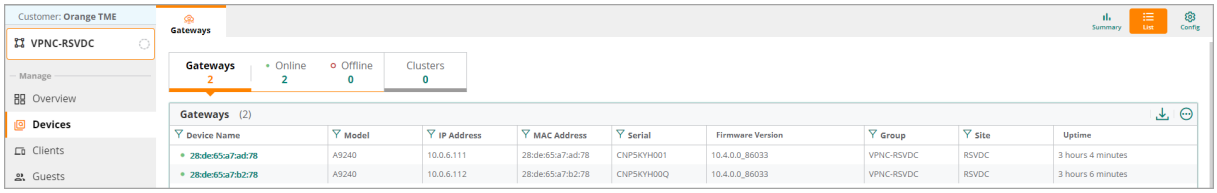


Figure 12: Select Gateway

Step 4 Click **Cancel**, then click **Exit**.

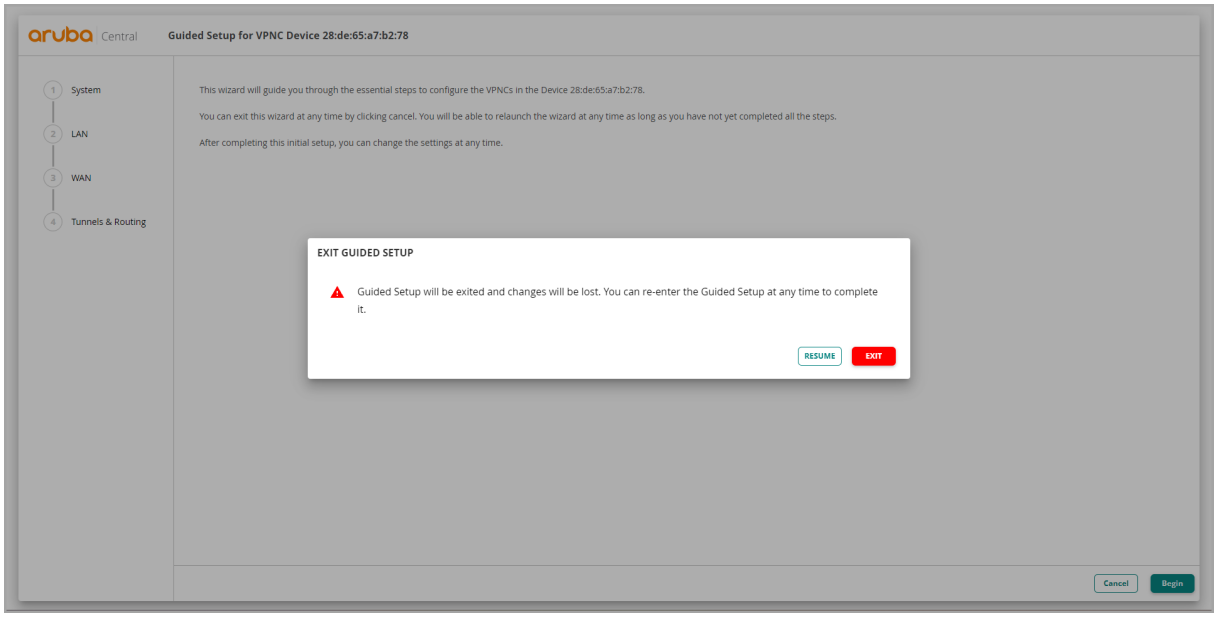


Figure 13: Guided_Setup

Select the Hardware Model for the VPNC Group

Only one VPNC gateway model can be assigned for each group.

Step 1 On the **Gateways** tab, in the **System** section, select **Model**.

Step 2 In the **VPNC Model** dropdown, select the hardware model for the VPNC gateway group; for example: *A9240*.

Step 3 Use the toggle to disable **Automatic Group Clustering**, since clustering assigned at the site level.

NOTE:

Clustering is required for MicroBranch and can be left enabled if needed. Exercise caution since other devices brought into the group are clustered.

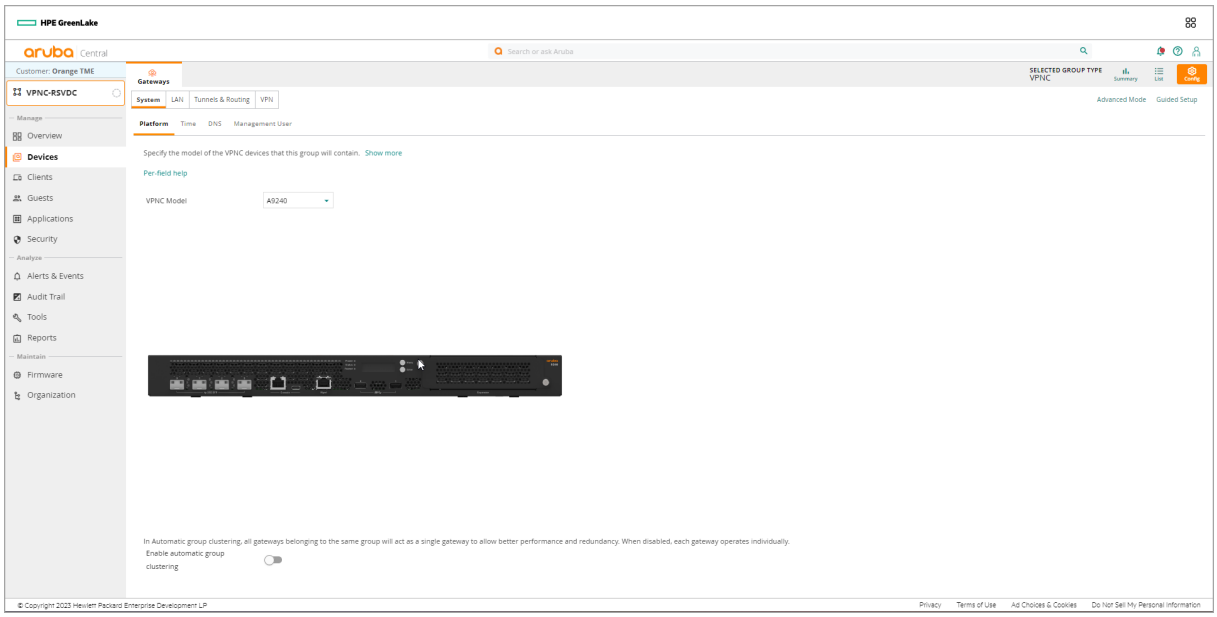


Figure 14: hardware_selection

Step 4 Click **Save Settings** in the bottom right corner.

Set the VPNC Group System Time Parameters

Use this procedure to set the network time protocol (NTP) parameters and time zone to keep the VPNC clocks synchronized.

Step 1 On the **Gateways** tab, in the **System** section, select **Time**.

Step 2 In the **Public NTP Servers** table, click the **+** (plus sign) to add a public NTP server.

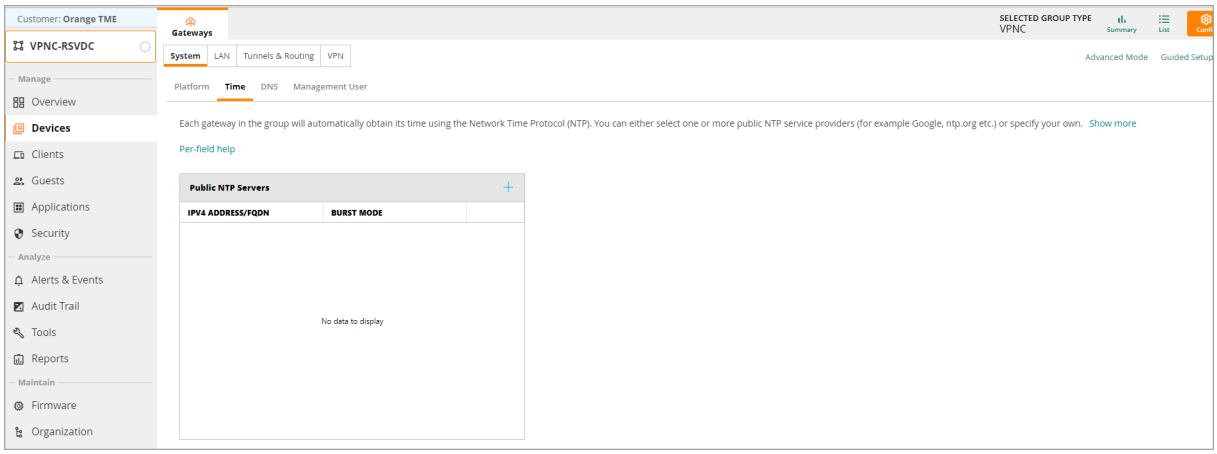


Figure 15: Setting_NTP

Step 3 In the **IPv4 Address/FQDN** column, enter *pool.ntp.org* or other NTP server address.

Step 4 Check **Burst Mode** if this feature is supported by the NTP server. Burst mode provides faster time synchronization.

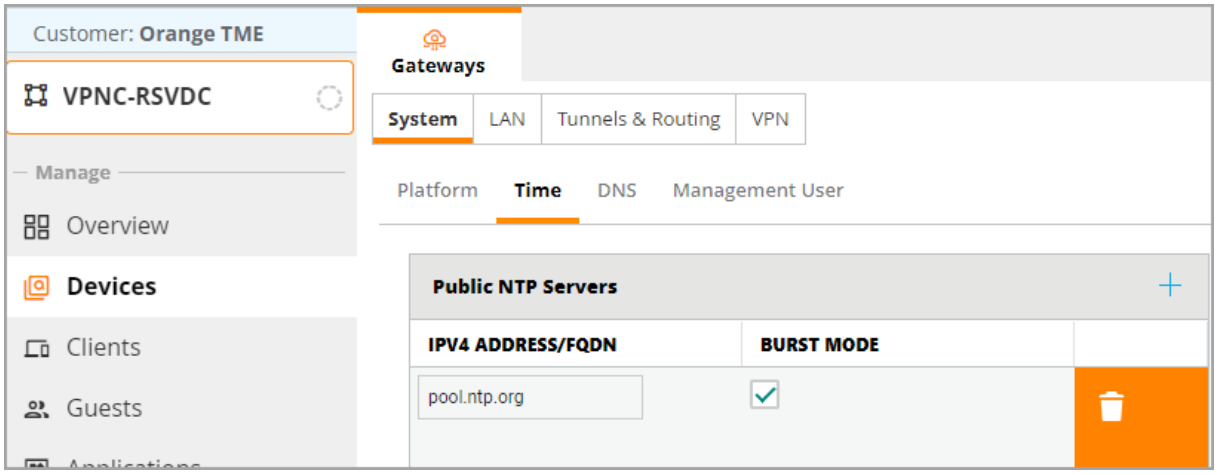


Figure 16: configuring_NTP

Step 5 In the **Timezone** dropdown, choose the appropriate time zone, then click **Save Settings**.

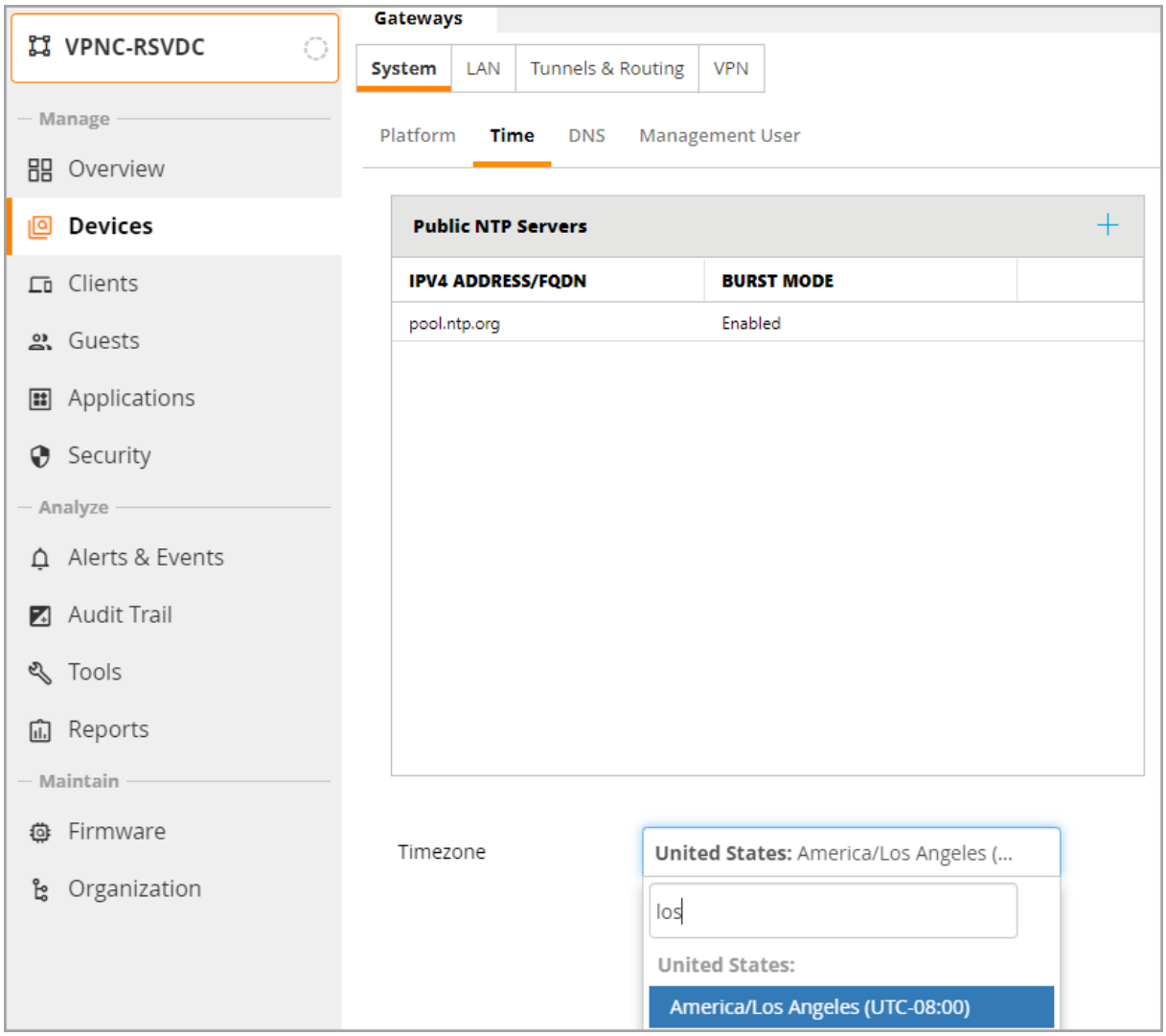


Figure 17: Timezone

Select a DNS Server for the VPNC Gateway

Specify the DNS server(s) the VPNC gateway uses to communicate with Central.

Step 1 On the **Gateways** tab, in the **System** section, select **DNS**.

Step 2 Select **Specify DNS servers**.

Step 3 In the **Domain name** text box, enter a domain name; for example: *example.local*.

Step 4 In the **Public DNS Servers** table, click the **+** (plus sign) to assign a public DNS server. For a virtual gateway VPNC, leave the default DNS provided by the cloud provider and go to step 6.

Step 5 In the **Provider** dropdown, select one of the listed providers, or select **Alternate DNS** if the desired server is not in the list.

Step 6 Click **Save Settings**.

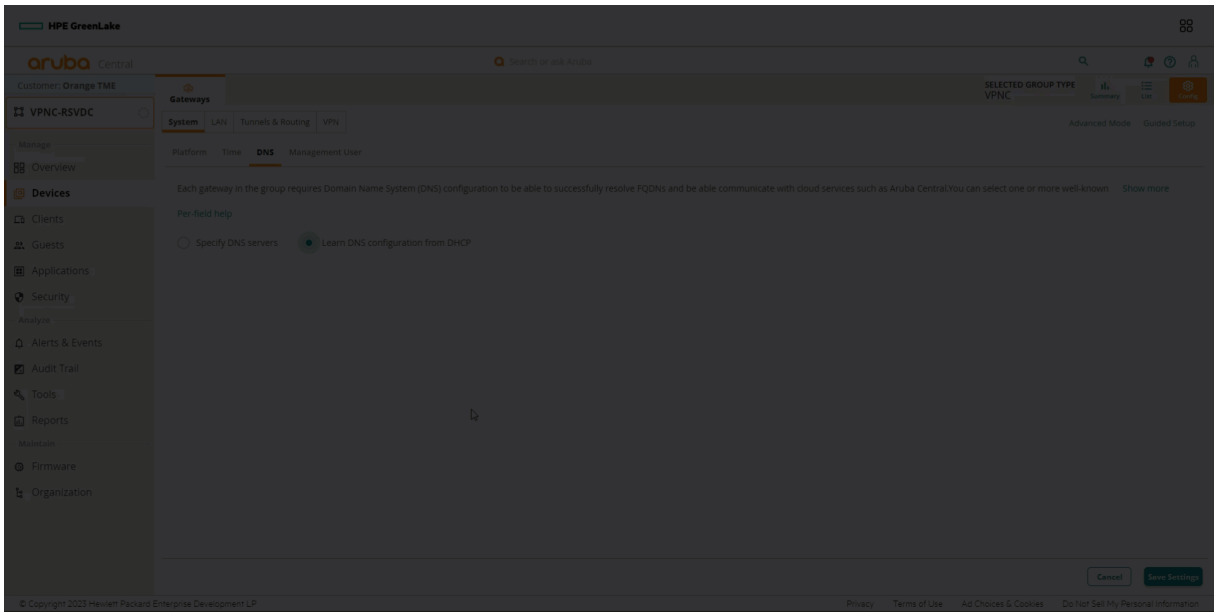


Figure 18: Configuring_DNS

NOTE:

The gateway uses this DNS server for DNS lookups. Clients do not use this DNS server.

Create a Management User Account

Create a management user account for CLI to access the gateways.

Step 1 On the **Gateways** tab, in the **System** section, select **Management User**.

Step 2 In the **Local management users** table, click the **+** (plus sign).

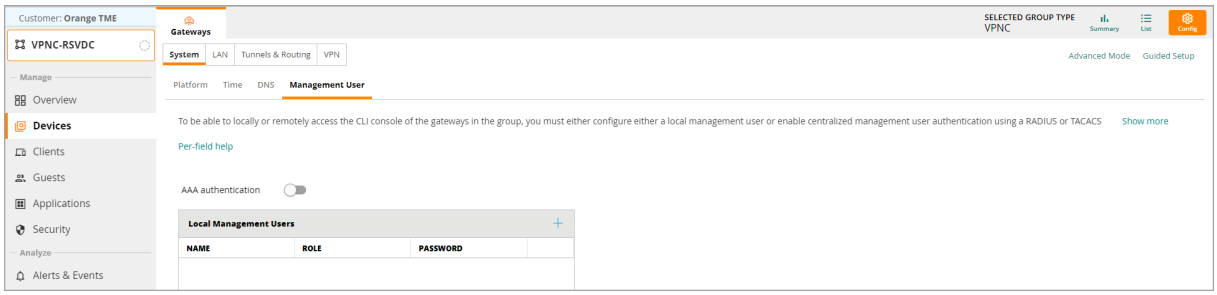


Figure 19: Add_MGMT_User

Step 3 In the **Add Management User** table, assign the following settings, then click **Save**.

- **Name**: *admin*
- **Password**: *password*
- **Retype Password**: *password*
- **Role**: *Super user role*

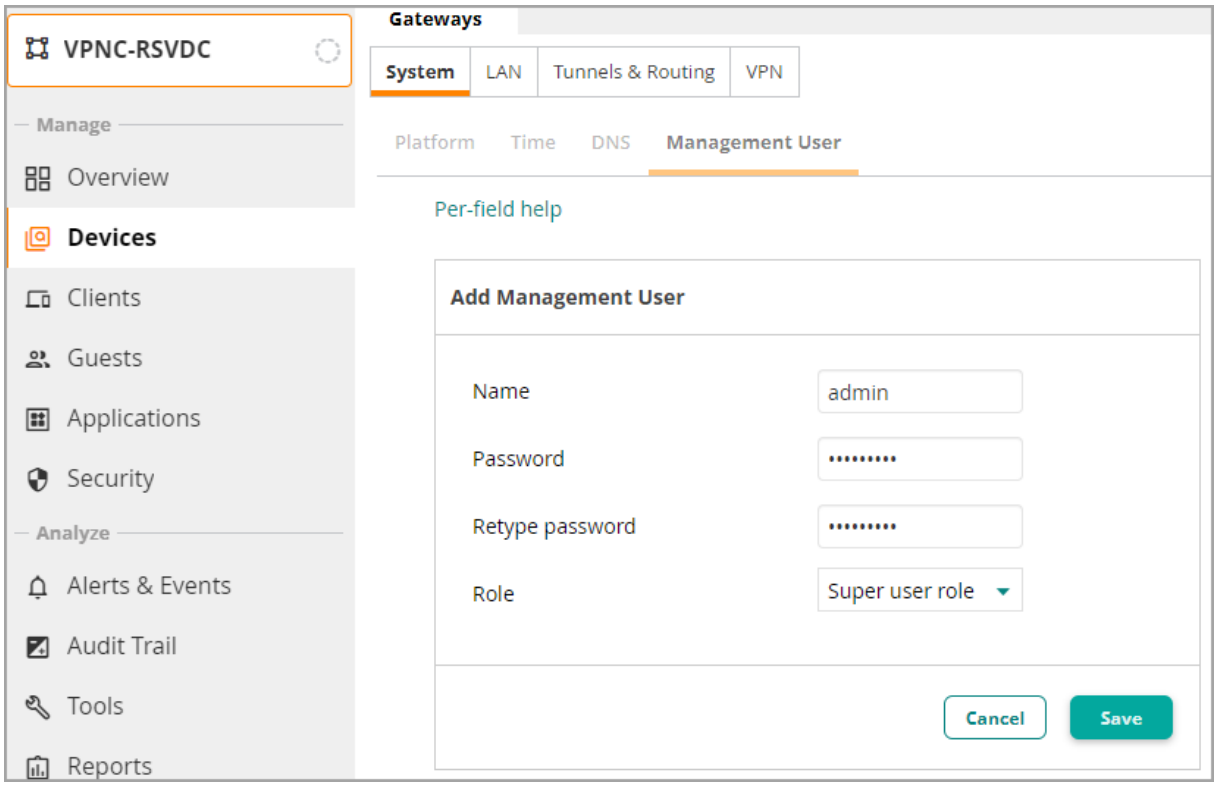


Figure 20: MGMT_Name_PW

NOTE:

You can add additional users with other roles as needed.

Step 4 Click **Save Settings** in the bottom right corner.

Create VLANs for Each Ethernet Port

Create five VLANs on the VPNCs including one each for WAN type of MPLS and Internet, and two for the LAN connections and OSPF peering to the campus infrastructure. The Gateway Pool VLAN is for the gateway's System IP address, configured for auto assignment.

Step 1 On the right side, click **Advanced mode**.

Step 2 Go to **Interface**, then select **VLANs**.

Step 3 In the **VLANs** table, click the **+** (plus sign).

Step 4 In the **New VLAN** window, configure the following VLANs, and click **Save Settings**.

VLAN Name	VLAN ID
MPLS	2086
INET	2084
GATEWAY_POOL	2085

VLAN Name	VLAN ID
OSPF_LAN_UPLINK_1	2001
OSPF_LAN_UPLINK_2	2002

NOTE:

VLANs 4080 and above are reserved. If these VLANs must be used, contact Aruba support.

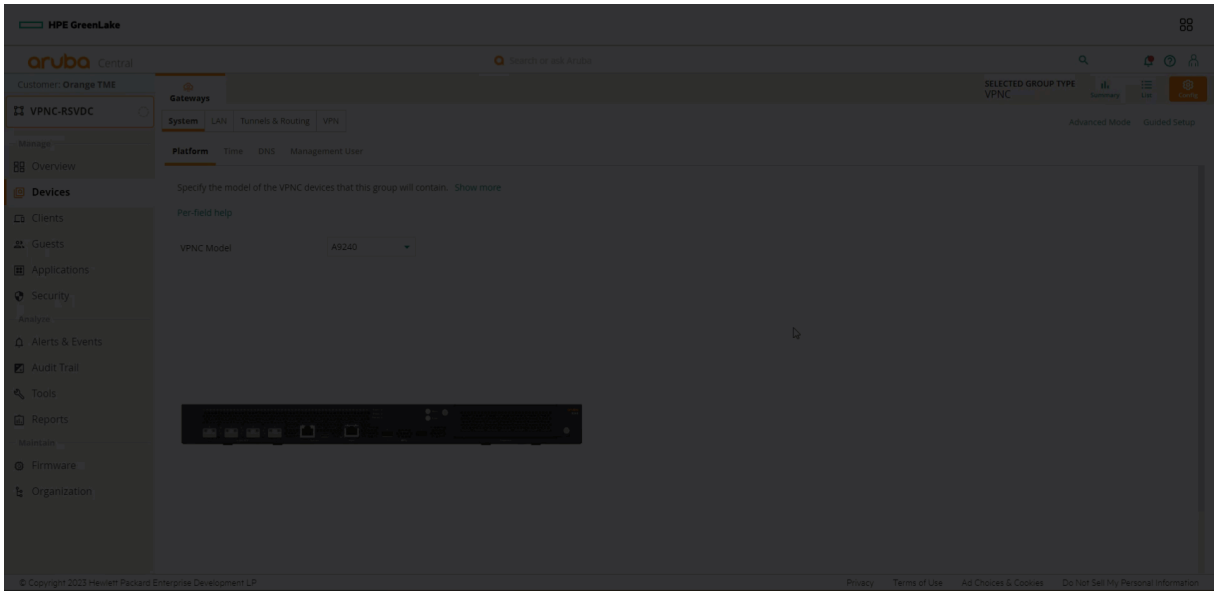


Figure 21: Creating_VLAN

Step 5 Verify the VLAN information in the summary table, then click **Save Settings** in the bottom right corner.

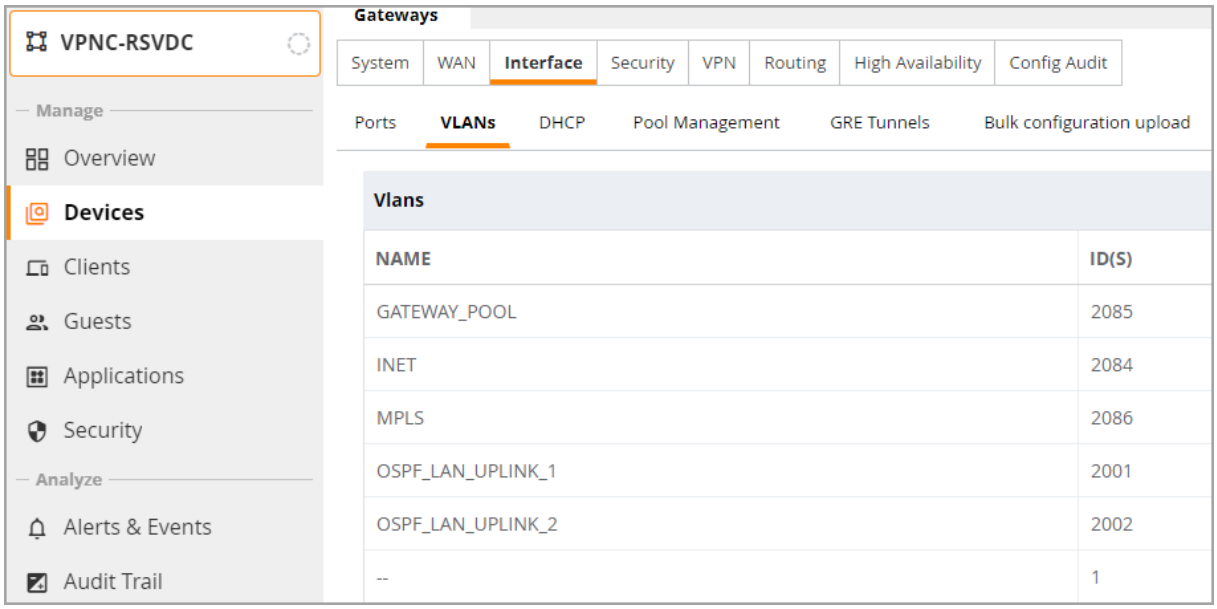


Figure 22: Complete_VLAN_List

Step 6 Configure the following settings on each VLAN in the **IP Address Assignment** section.

Interface	Enable Routing	IP Assignment	NAT Outside
MPLS	Checked	Static	
INET	Checked	Static	Checked
GATEWAY_POOL	Checked	Gateway Pool	
OSPF_LAN_UPLINK_1	Checked	Static	
OSPF_LAN_UPLINK_2	Checked	Static	

CAUTION:

DO NOT enable NAT on the ***OSPF_LAN_UPLINK***, **MPLS**, or ***Gateway Pool*** VLANs.

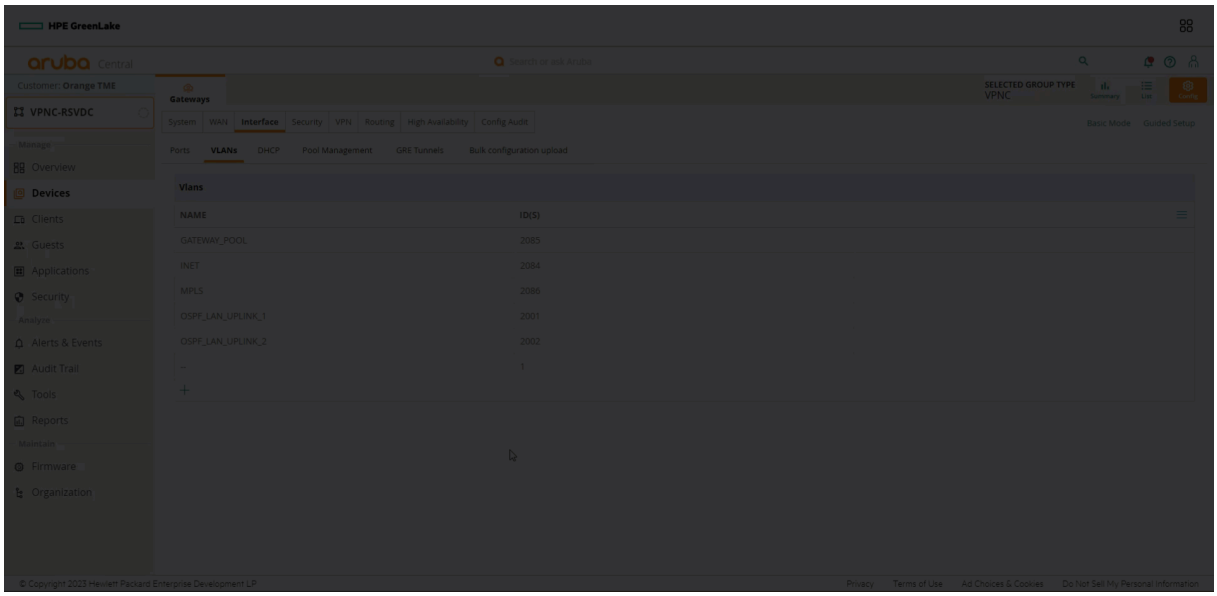


Figure 23: Enable_Routing

Step 8 Enable **OSPF** for the ***Gateway Pool***, ***OSPF_LAN_Uplink_1***, and ***OSPF_LAN_Uplink_2*** VLANs.

- Select the ***OSPF_LAN_UPLINK_1***.
- Enable **OSPF**.
- Enter the **OSPF area**: *0.0.0.0*.
- Click **Save Settings**.
- Repeat these steps for the ***OSPF_LAN_Uplink_2*** and ***Gateway Pool*** VLANs.

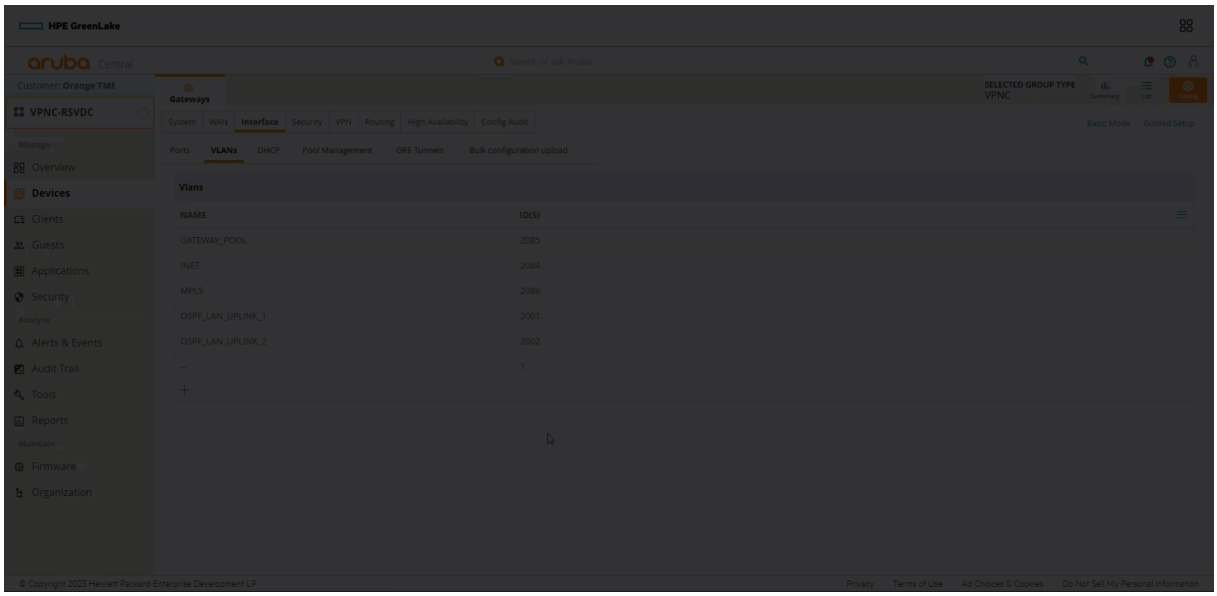


Figure 24: Enable_OSPF

Enable OSPF Globally

Although OSPF has been enabled for the VLAN, it is not enabled globally. The following procedure enables OSPF globally so the interfaces can participate in OSPF.

Step 1 On the **Gateway** tab in **Advanced Mode**, go to **Routing > OSPF**.

Step 2 Enable the **OSPF** toggle.

Step 3 Enter the **Area ID**: *0.0.0.0*.

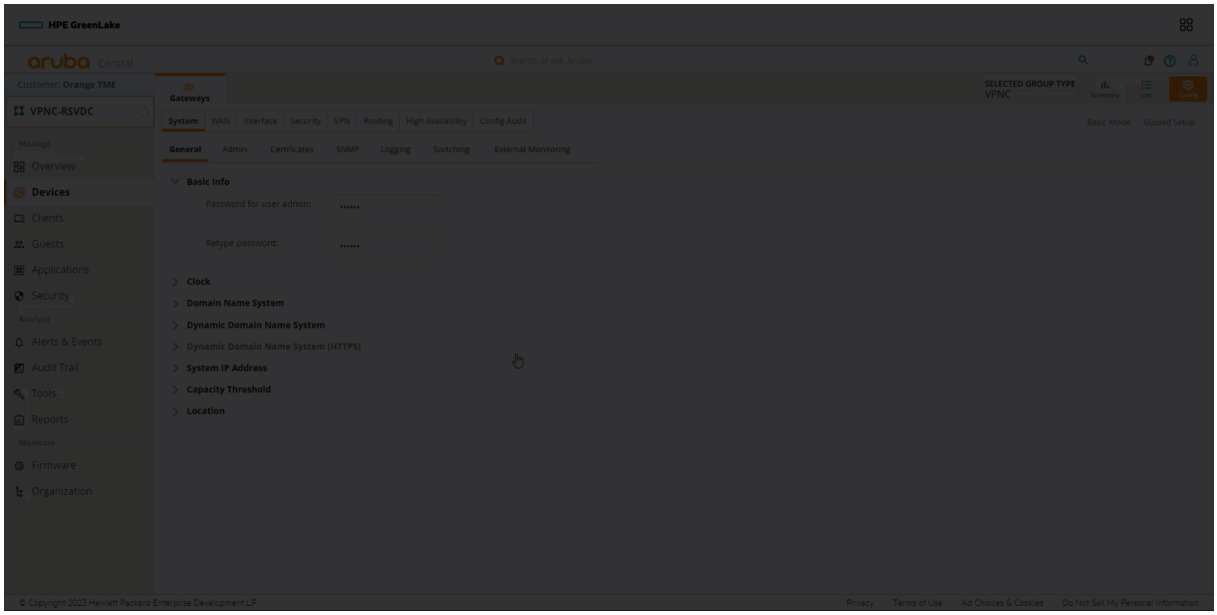


Figure 25: Enabling OSPF

Define the Gateway Pool

In the previous sections, the Gateway Pool VLAN was defined. However, it was not configured as a Gateway Pool. This procedure completes the Gateway Pool configuration, which automatically assigns Gateway IP Addresses.

Step 1 In **Advanced Mode**, go to **Interface** and select **Pool Management**. Expand the **Gateway Pool** option.

Step 1 Select the **+** (plus sign) to create a **Gateway Pool**.

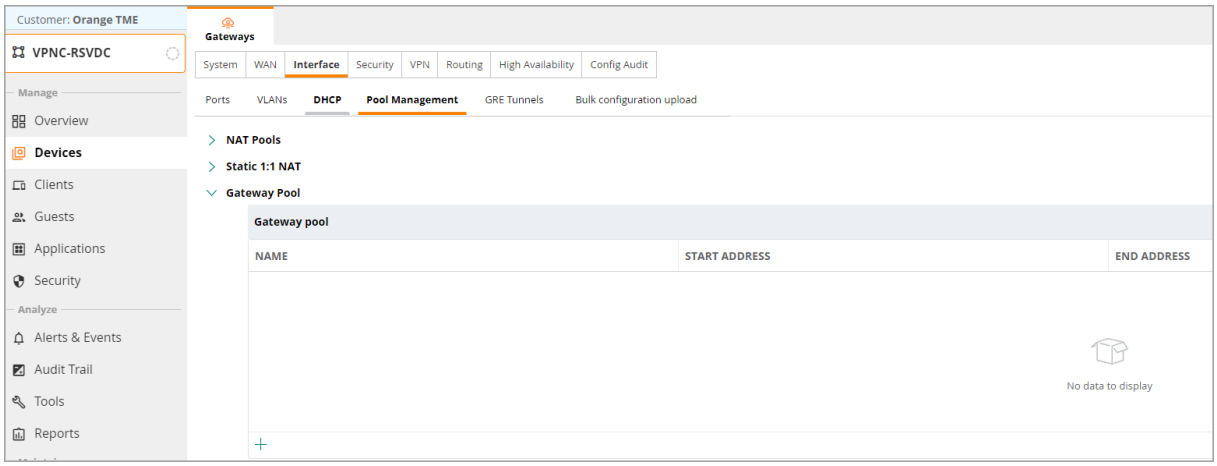


Figure 26: Nav_Gateway_Pool

Step 3 Enter the pool of IP Addresses for the Gateway Pool.

1. Enter the **Start IP address**: *10.0.6.111*.
2. Enter the **End IP address**: *10.0.6.120*.
3. Click **Save Settings**.

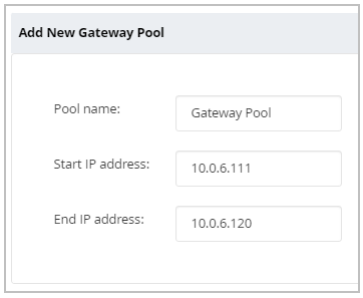


Figure 27: Gateway_Pool_Config

I AM HERE!!!!

Step 4 Go to **Interface > VLANs**.

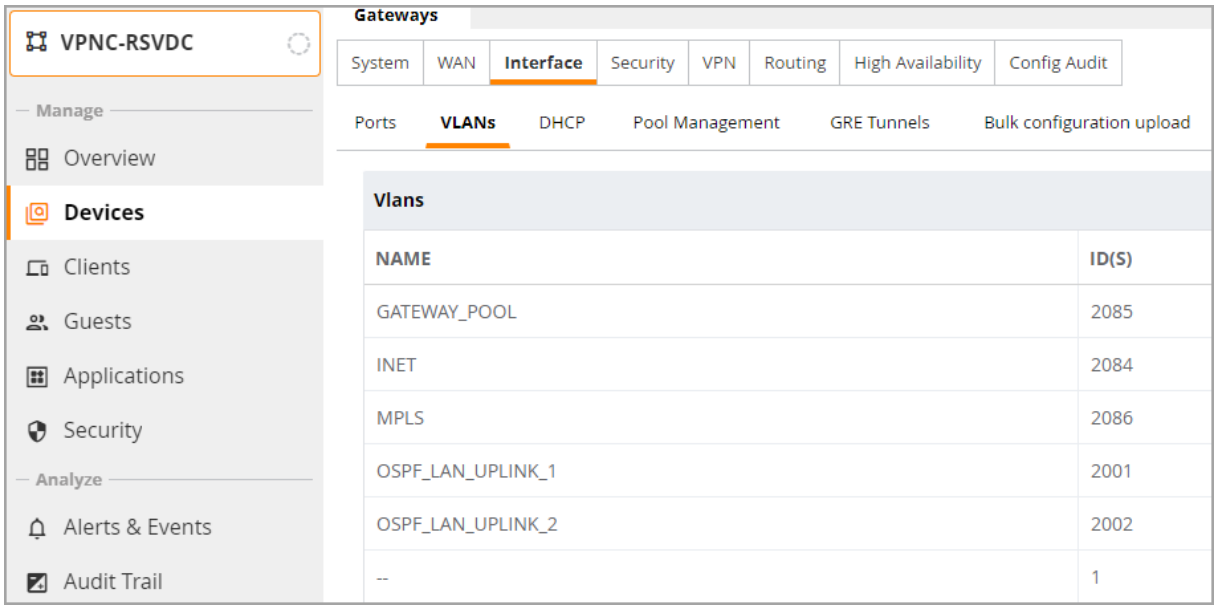


Figure 28: Nav_VLAN_List

Step 5 Select the **Gateway Pool VLAN**.

- Set the **IP Assignment** to *Gateway Pool*.
- Set the **VLAN Pool** to *Gateway Pool*.
- Click **Save Settings**

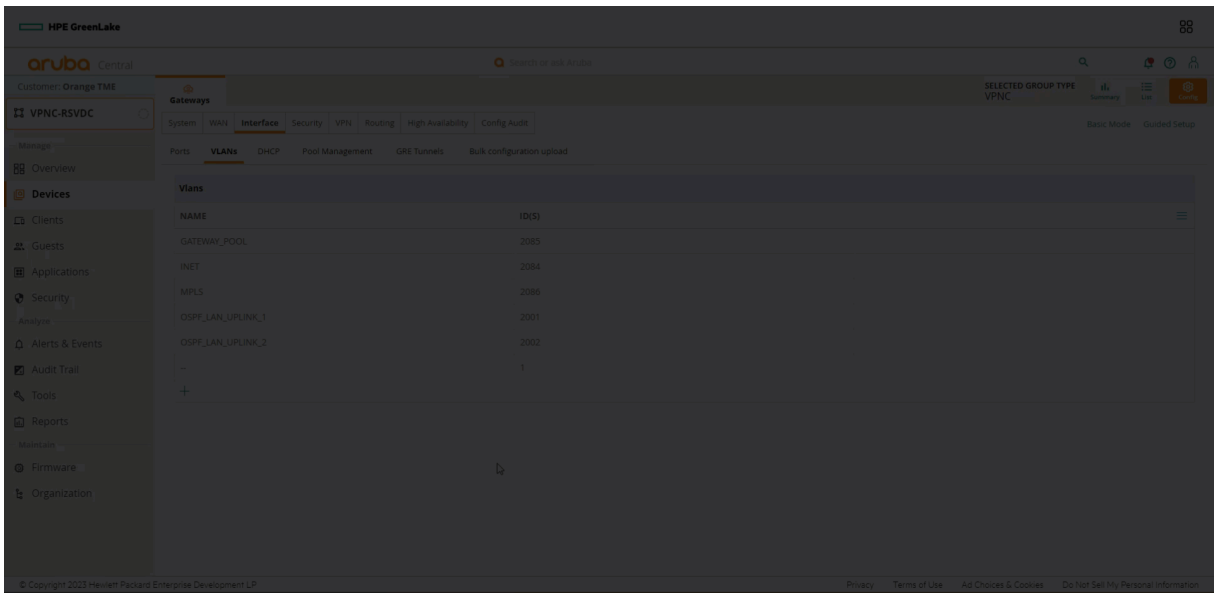


Figure 29: Applying Gateway Pool

Step 6 Go to **System > General**.

Step 7 Expand the **System IP Address** and select ***VLAN 2085*** (the Gateway Pool VLAN).

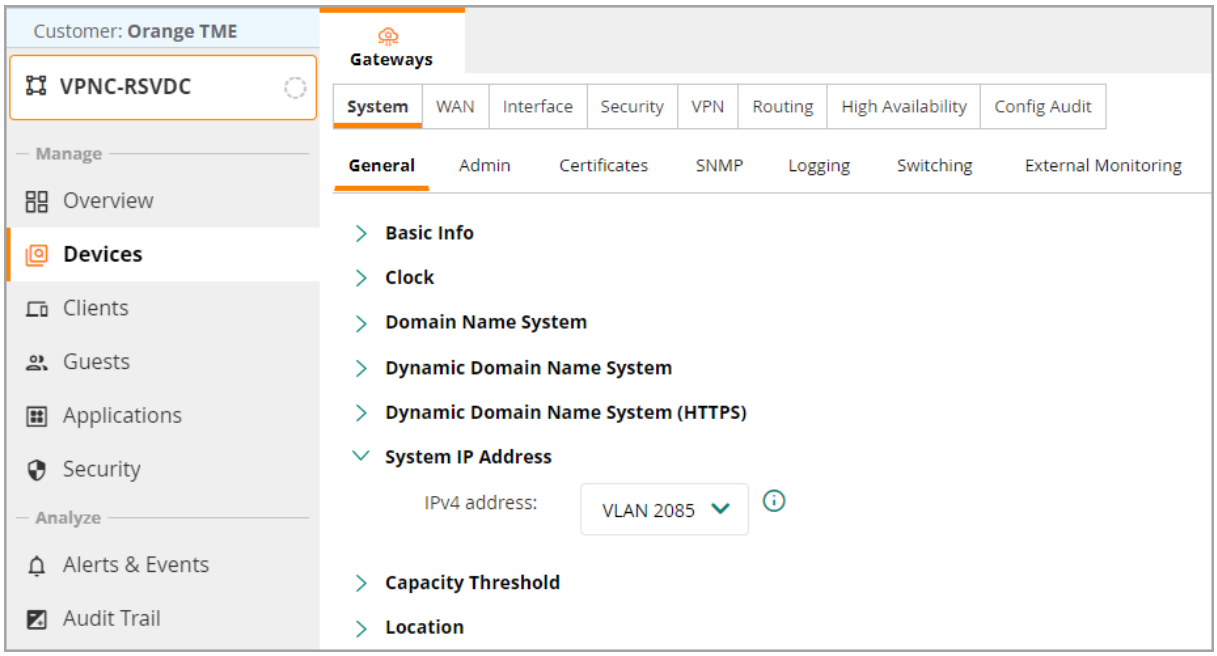


Figure 30: Set System IP

Step 8 Click **Save Settings**

Assign the VLANs to the LAN Ports

After each VLAN is configured appropriately, the VLANs must be assigned to the correct ports.

Later in this guide, the VPNC is set up for One Touch Provisioning, so it is important to assign the correct port layout.

Step 1 Go to **Gateways > Config**. On the right side, click **Advanced mode**.

Step 2 Go to **Interface > Ports**.

Step 3 In the **LAN ports/port channel** table, click the **+** (plus sign).

Step 4 Select all the ports to be used. This example uses **Ports Ge 0/0/0 - Ge 0/0/3**.

Figure 31: Selecting Ports

Step 5 Configure the Interface Type, VLAN ID and Description, and LLDP on each port, as shown below.

Port ID	Interface Type	VLAN ID	Description
Ge 0/0/0	LAN	2001	OSPF_LAN_UPLINK_1
Ge 0/0/1	LAN	2002	OSPF_LAN_UPLINK_2
Ge 0/0/2	WAN	2086	MPLS
Ge 0/0/3	WAN	2084	INET

NOTE:

Before registering an appliance with Central, interface Ge 0/0/1 can be reserved for One Touch Provisioning. Do not use this interface as a WAN port if DHCP addressing is required (such as an Internet circuit).

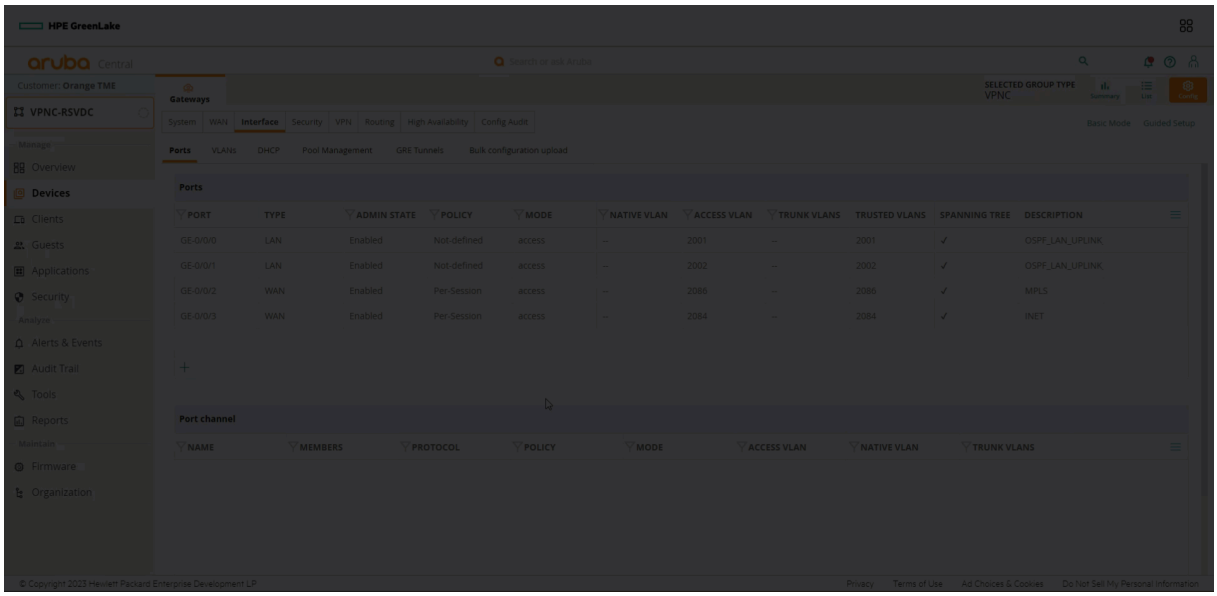


Figure 32: Configuring Interfaces

Step 6 Verify the port information in the summary table.

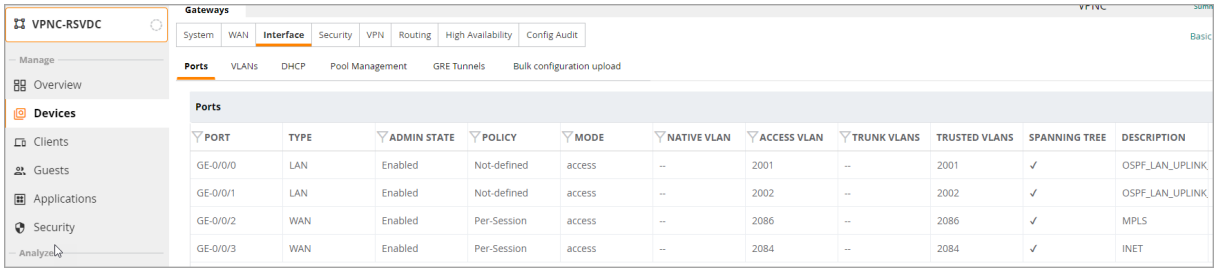


Figure 33: VPNC_Verify_Ports

Enable Tunnel Orchestrator Peering

In this procedure, the SD-WAN overlay orchestrator is enabled to automate establishing tunnels.

Step 1 On the **Gateways** tab in **Basic Mode**, go to **Tunnels & Routing** and select **SD-WAN Overlay**.

NOTE:

In **Advanced Mode**, go to **VPN > SD-WAN Overlay** and switch the overlay mode to orchestrated.

Step 2 Click **Overlay Orchestrator Peering**, then click **Save Settings**.

Figure 34: Enable Overlay Orchestration

Configure Route Filtering

The VPNC filters out all point-to-point routes, 172.18.X.X/16, from the campus. This procedure creates a prefix list and a route map to accomplish the filtering.

Step 1 On the **Gateways** tab in **Basic Mode**, go to **Tunnels & Routing** and select **Route Maps**.

Step 2 Click the **Prefix List** dropdown, then click the **+** (plus sign) to create a new prefix list.

Step 3 Enter the following settings for the **Point-To-Point** prefix list.

- **Name:** *PTP*
- **Sequence:** *10*
- **Action:** *Deny*
- **Address:** *172.18.96.0*
- **Mask:** *255.255.224.0*
- **GE:** 29

Step 4 Click the **+** (plus sign) to create a new prefix list. Enter the following settings for a **Catch all** prefix list.

- **Name:** *ANY*
- **Sequence:** *20*
- **Action:** *Permit*
- **Address:** *0.0.0.0*
- **Mask:** *0.0.0.0*
- **LE:** 32

Step 5 Click **Save Settings**.

NOTE:

The LE and GE configurations are required to enable filtering or allow fewer specific prefixes. In this example, the point-to-point prefix list matches only network 172.18.96.0/19. It would not match the more specific route of 172.18.96.8/30.

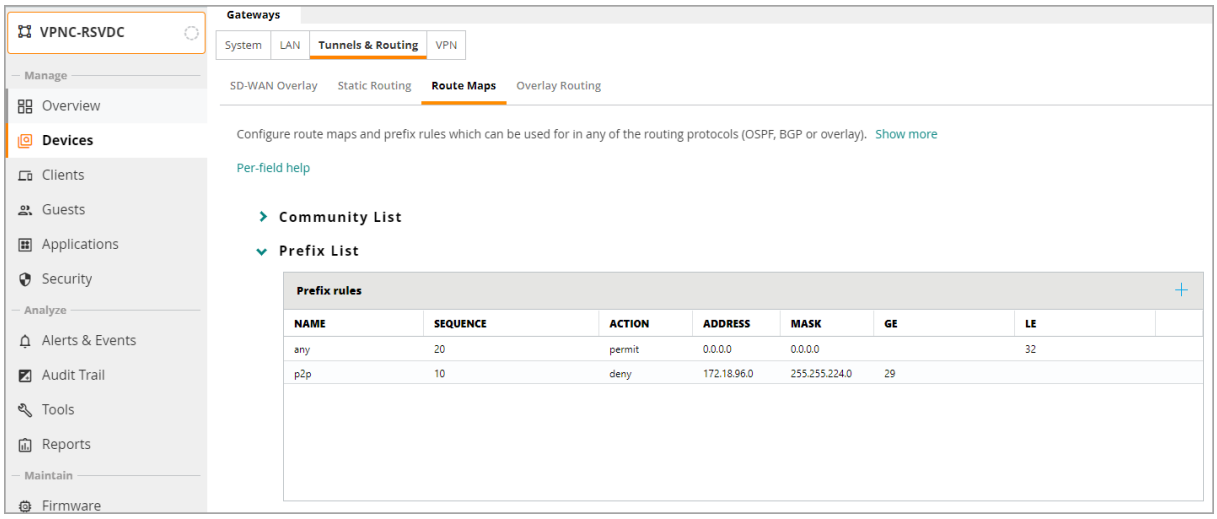


Figure 35: Configure Prefix List

Step 6 Expand the **Route Map** dropdown, and click the **+** (plus sign) to create a new route map.

Step 7 Enter the following settings for the route map.

- **Name:** *Block_PTP*
- **Sequence Number:** *10*
- **Action:** *Permit*

Step 8 In the **Match** box, click the **+** (plus sign) to add a match.

Step 9 Set the type to **IP Address** and set the value to the ***PTP*** Prefix list.

Step 10 Click the **+** (plus sign) to add another match. Set the type to **IP Address** and set the value to the ***ANY*** Prefix list.

Step 11 Click **Save**, then click **Save Settings**.

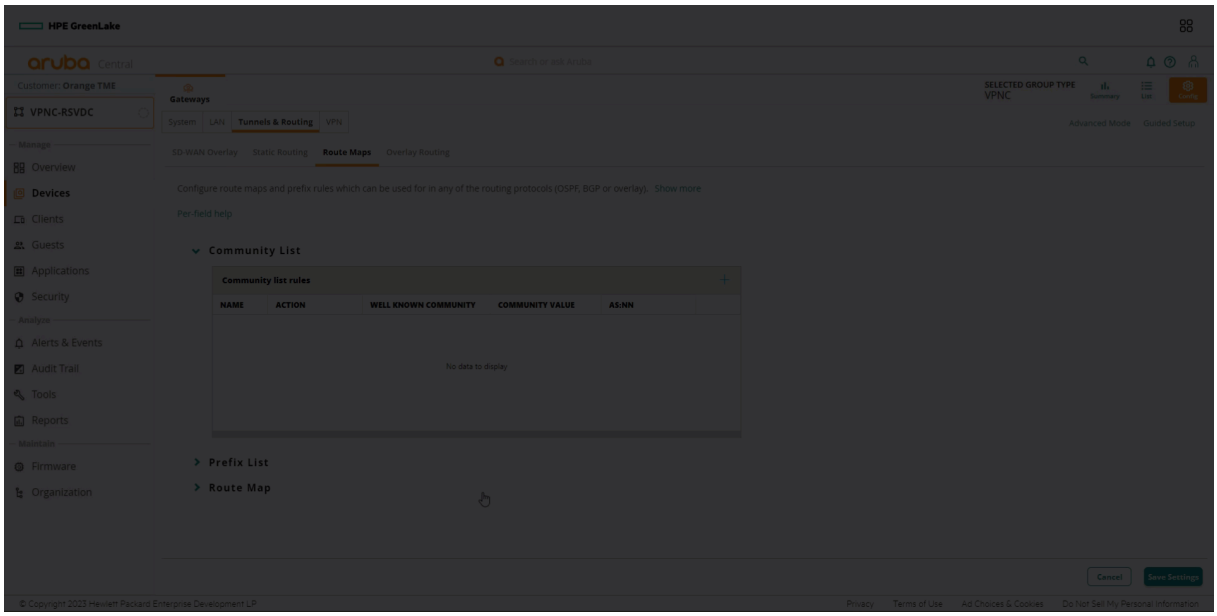


Figure 36: Creating Route Map

Configure the Overlay Routing

Use this procedure to redistribute OSPF routes into the overlay so branches can reach corporate prefixes. Aruba SD-WAN automatically translates route costs between the overlay and data center to ensure symmetry.

Step 1 On the **Gateways** tab, in the **Tunnels & Routing** section, select **Overlay Routing**.

Step 2 On the **Overlay Routing** page, expand **Redistribution** to display the redistribution table.

Step 3 In the **Redistribution** table, click the **+** (plus sign) to create a new redistribution rule.

Step 4 In the **Source Protocol** dropdown, select *OSPF*. Static, connected, and BGP routes also are supported, though not shown in this example.

Step 5 In the **Filter** dropdown, select **Intra Area**, depending on the OSPF routes to be redistributed. Other options can be selected.

Step 6 In the **Route Map** dropdown, select the ***Block_PTP*** route map created in the previous procedure.

Step 7 Click **Save Settings**.

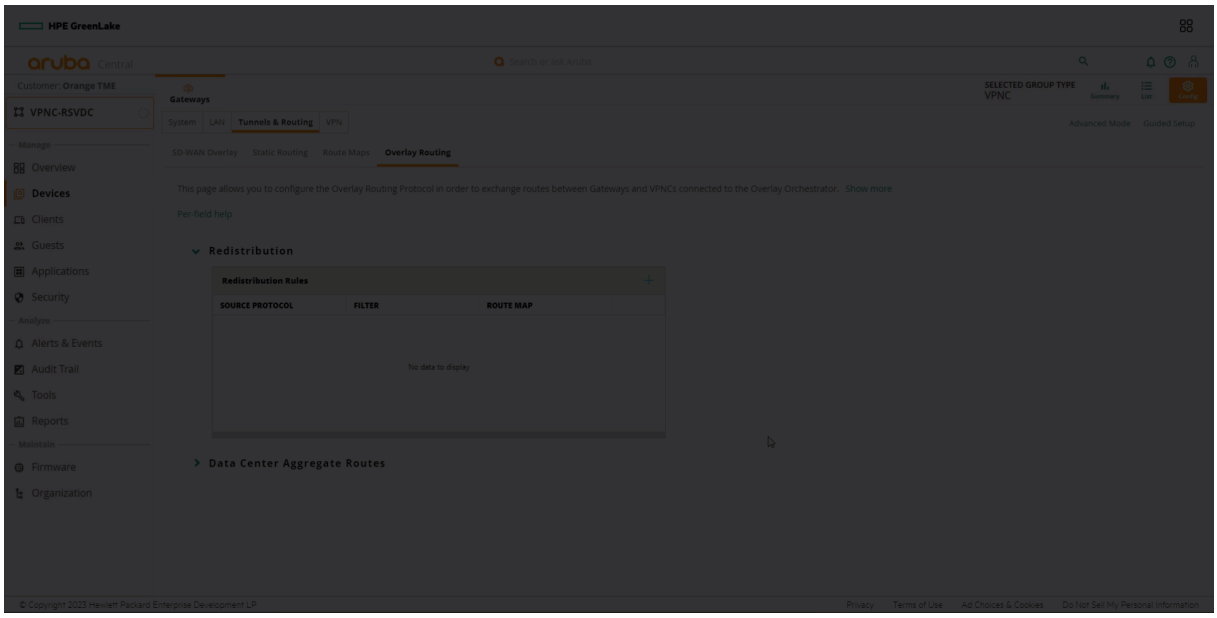


Figure 37: Redistribute Routes

Redistribute SD-WAN Routes

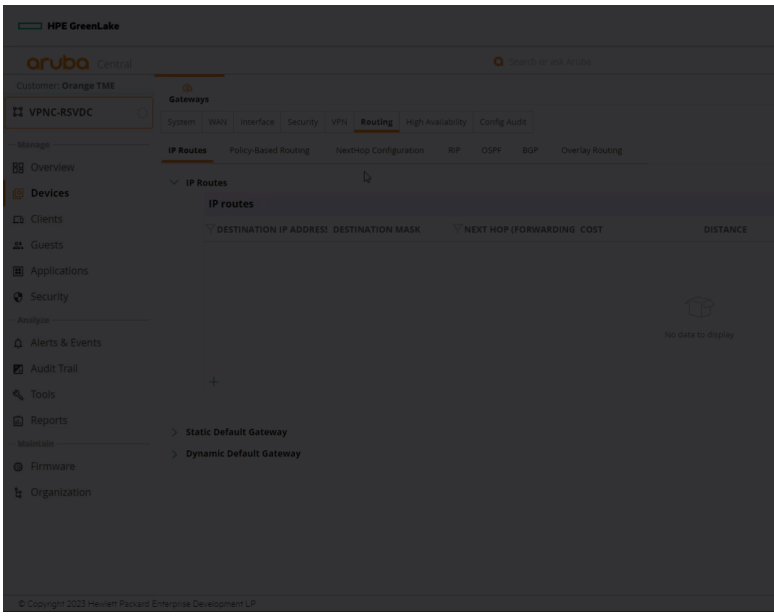
Step 1 In **Advanced Mode**, select the **Routing** tab.

Step 2 Select **OSPF**.

Step 3 Select **Redistribution** and click the **+** (plus sign).

Step 4 Select the source protocol **SDWAN Overlay**. Select the **Route Type** *E1* and set the **Cost**; in this case: *100*.

Step 5 Click **Save Settings** in the bottom right corner.



Configure Aggregation Routes

This procedure uses the DC aggregation routes to summarize the 10.X.X.X addresses in the campus into one summary address. The VPNC advertises the summary route 10.0.0.0/13 to each Branch Gateway. This is optional; however, it is recommended to summarize as much as possible to protect the route table size.

Step 1 On the **Gateways** tab, in the **SDWAN & Routing** section, select **Overlay Routing**.

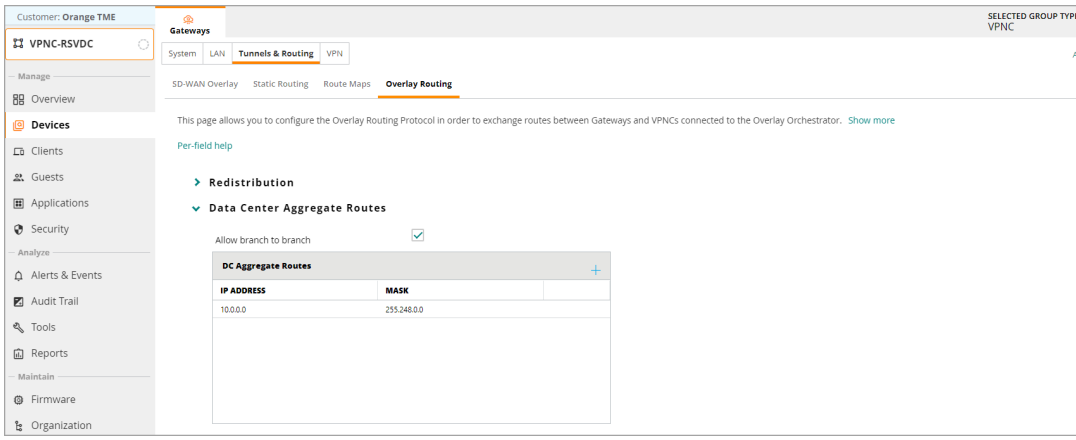
Step 2 On the **Overlay Routing** page, expand **Data Center Aggregate Routes** to display the **DC Aggregate Routes** table.

Step 3 Uncheck **Allow branch to branch**. If selected, the VPNC becomes a transit site allowing branches to communicate through the VPNC. This is typically unwanted if all applications are centralized at the data center.

Step 4 In the **DC Aggregate Routes** table, click the **+** (plus sign) to create a new aggregate route. In this example, the 10.0.0.0/13 summary is used to summarize the corporate address space.

Step 5 In the **IP Address** column, enter *10.0.0.0*, and in the **Mask** column, enter *255.248.0.0*.

Step 6 Click **Save Settings**.



Configure Static Routes

This procedure configures The VPNC gateways with the routes needed to form IPSEC tunnels over the INET and MPLS transports. The INET route is provided via a static default-gateway and the MPLS route is provided via a static route. In this example, the MPLS network can be summarized with the 100.100.7.0/24 prefix. These routes are applied at the group level, since they are the same for all gateways in the group; however, they could be applied at the device level if the next-hops differ. BGP also can be configured on the MPLS circuit to provide these routes, if desired. While the default gateway is configured as part of the OTP process of the gateway, also configure it at the group level.

In the first step illustrated below:

Step 1 In **Advanced Mode** select the **Routing** tab.

Step 2 Select **IP Routes**.

Step 3 Expand **IP Routes**.

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

Step 5 Enter the following information to create the MPLS route. - **Destination IP address:** *100.100.7.0* - **Destination network mask:** *24* - ***Forwarding settings:*** Use Forwarding Router Address - ***Next hop IP address:*** 100.100.7.1 - ***Cost:*** 1* - **Distance:** 1

Step 6 Click **Save Settings**.

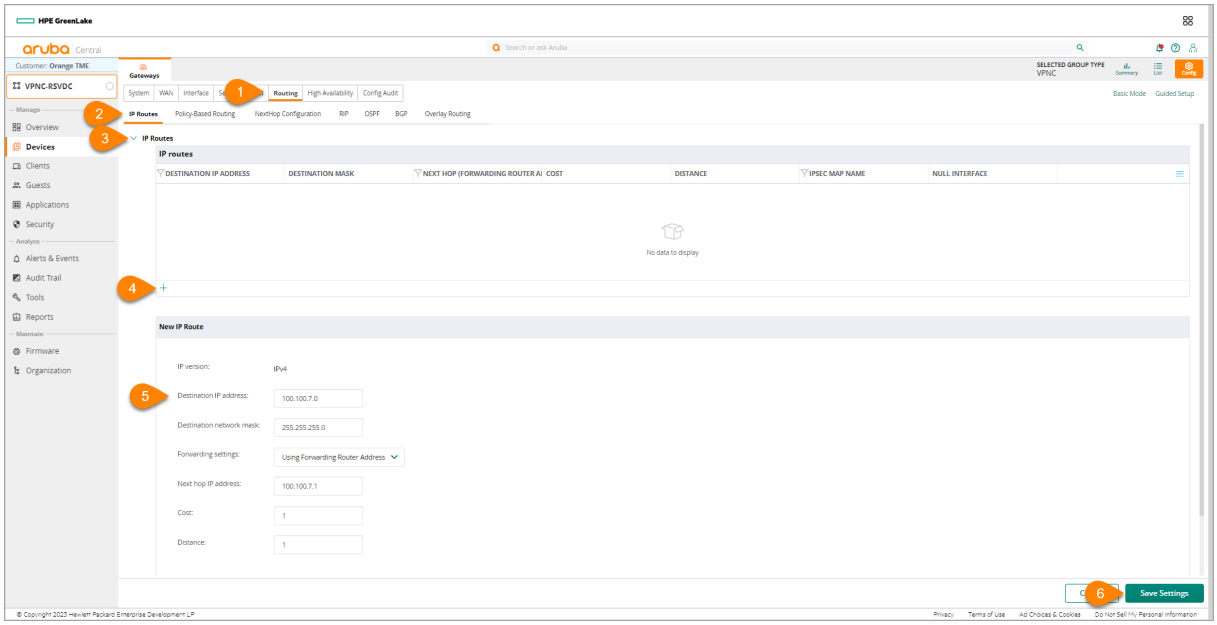


Figure 38: VPNC Static Route

In the second step illustrated below:

Step 1 Expand **Static Default Gateway**.

Step 2 Click the **+** (plus sign) to create a new static default gateway.

Step 3 Enter the following information to create the INET route.

- **Destination IP address:** *Default Gateway IP*
- **Default Gateway IP:** *gateway IP of INET circuit*
- **Cost:** *1*

Step 4 Click **Save Settings**.

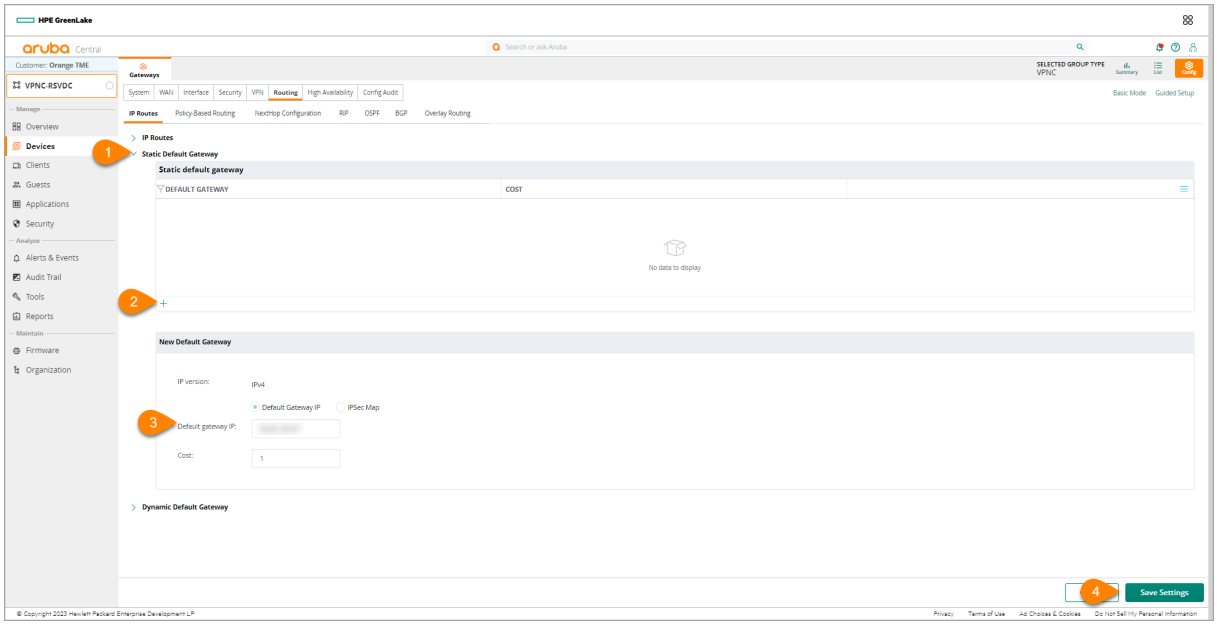


Figure 39: VPNC Default Gateway

Configure VPNC Devices

After the group level configuration is complete, assign device-level configurations. This section walks through the remaining configuration, which is unique to each VPNC. The procedure is provided for one VPNC, but it must be repeated for the second VPNC in the group. Since the devices were moved to the group using preprovisioning, this configuration is completed before the gateways come online.

Assign a VPNC Device to a Group and Site

This step should have been completed in the *Preparing to Deploy Aruba SD-Branch* chapter. If it was not, refer to the procedure here.

Configure VPNC Device

This procedure is illustrated for one VPNC, but must be repeated for the second VPNC in the group. Because the devices were moved to the group using preprovisioning, this configuration can be complete before the device comes online.

Step 1 Go to the ***VPNC-RSVDC*** Group.

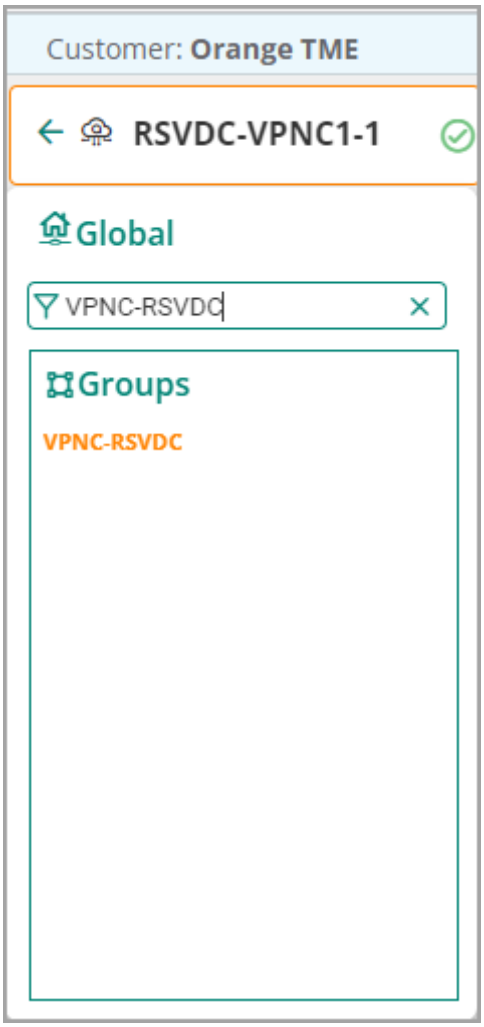


Figure 40: VPNC Select Group

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

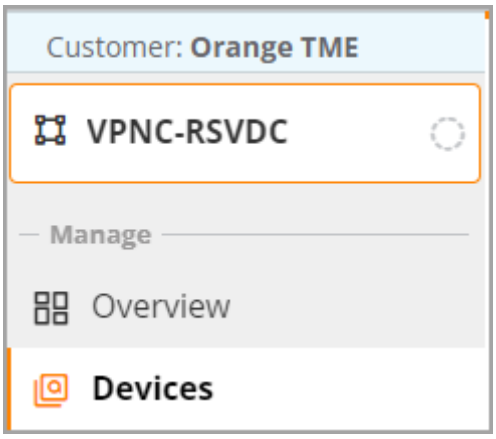


Figure 41: VPNC Select Device

Step 3 In the gateway list, select the first gateway to configure. Correlate the system-mac to the device to select.

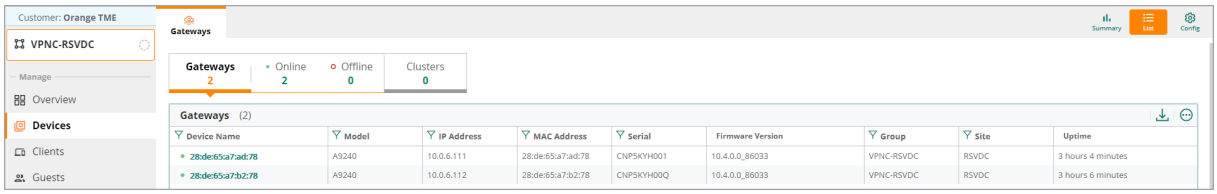


Figure 42: VPNC Select Group

Step 4 In the left navigation pane, select **Device**.

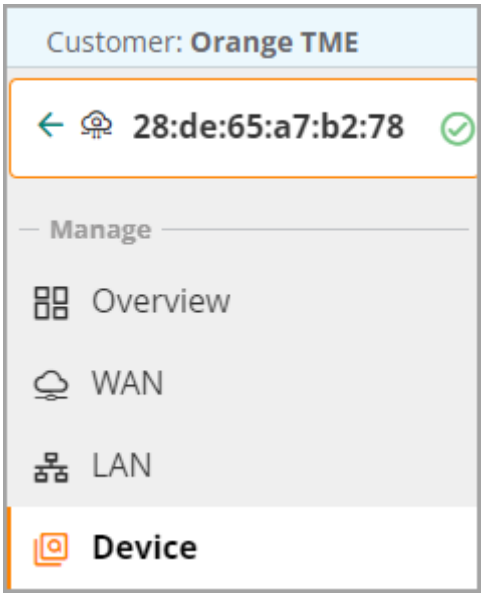


Figure 43: VPNC Select Device 2

Step 5 In the guided setup window, click **Cancel**, then click **EXIT**.

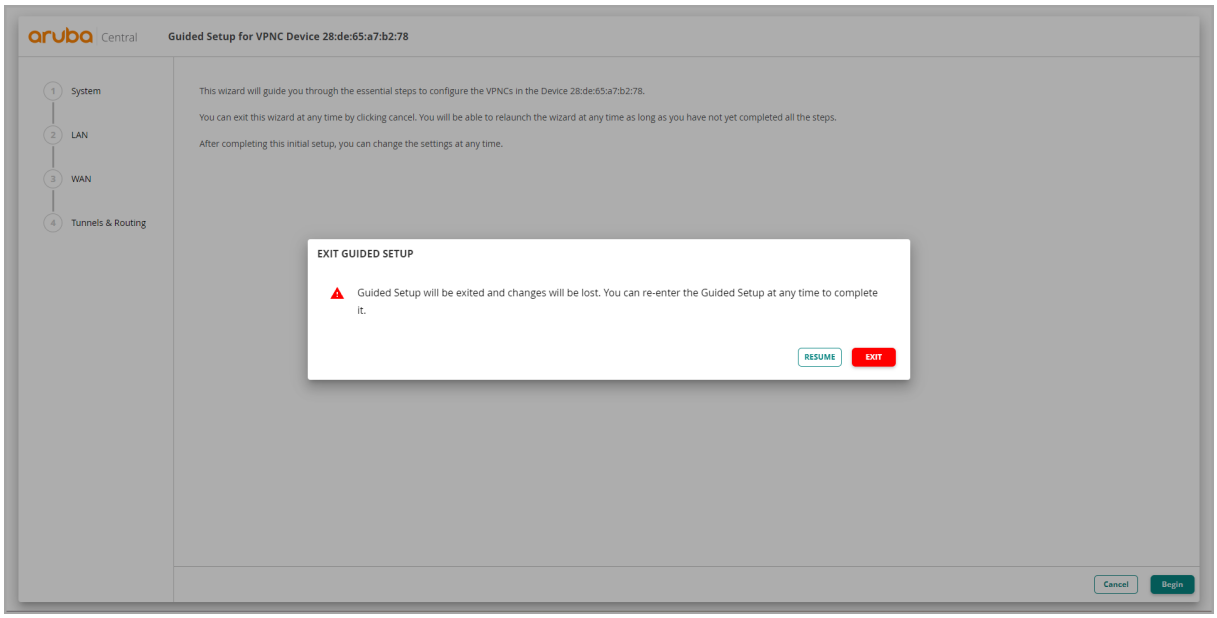


Figure 44: VPNC Cancel Guided Setup

Configure Hostname

Use this procedure to configure the hostname on the gateway.

Step 1 Go to the Gateway configuration and click **Basic Mode**.

Step 2 Select **System > Hostname**.

Step 3 Enter the **Hostname**.

Step 4 Click **Save Settings**.

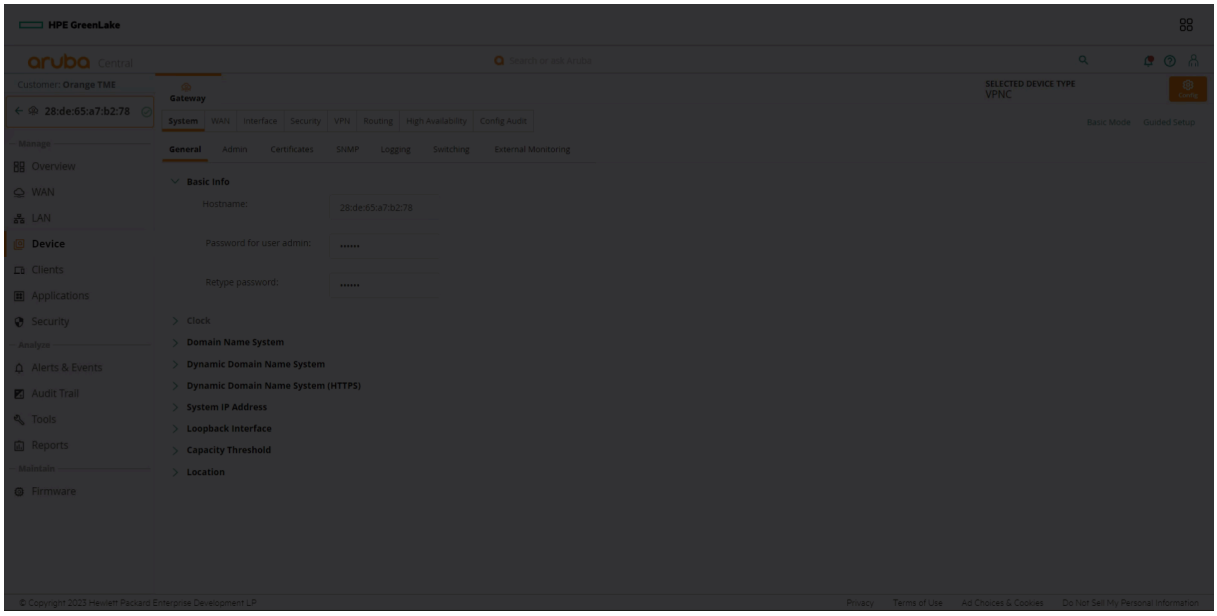


Figure 45: Configure Hostname

Configure the System IP for the VPNC Device

Use this procedure to define the system IP address the gateway will use for network services. Ensure that **Basic Mode** is still selected.

Step 1 Select **System > System IP**.

Step 2 In the **VLAN Interface** box, select the **VLAN 2085**.

Step 3 Click **Save Settings**.

Assign IP Addresses to the VLANs

Step 1 Select the **LAN** tab, and select **VLANs**.

Step 2 In the **VLANs** table, select the VLAN to update, then click the **edit** (pencil) icon.

Step 3 In the **VLAN** window, assign the following settings, then click **Save**. (These settings are for the first VPNC.)

VLAN Name	VLAN ID	IP Address	NetMask
OSPF_LAN_UPLINK_1	2001	172.18.106.18	255.255.255.252
OSPF_LAN_UPLINK_2	2002	172.18.106.26	255.255.255.252
MPLS	2086	100.100.7.5	255.255.255.240
INET	2084	X.X.X.X	X.X.X.X

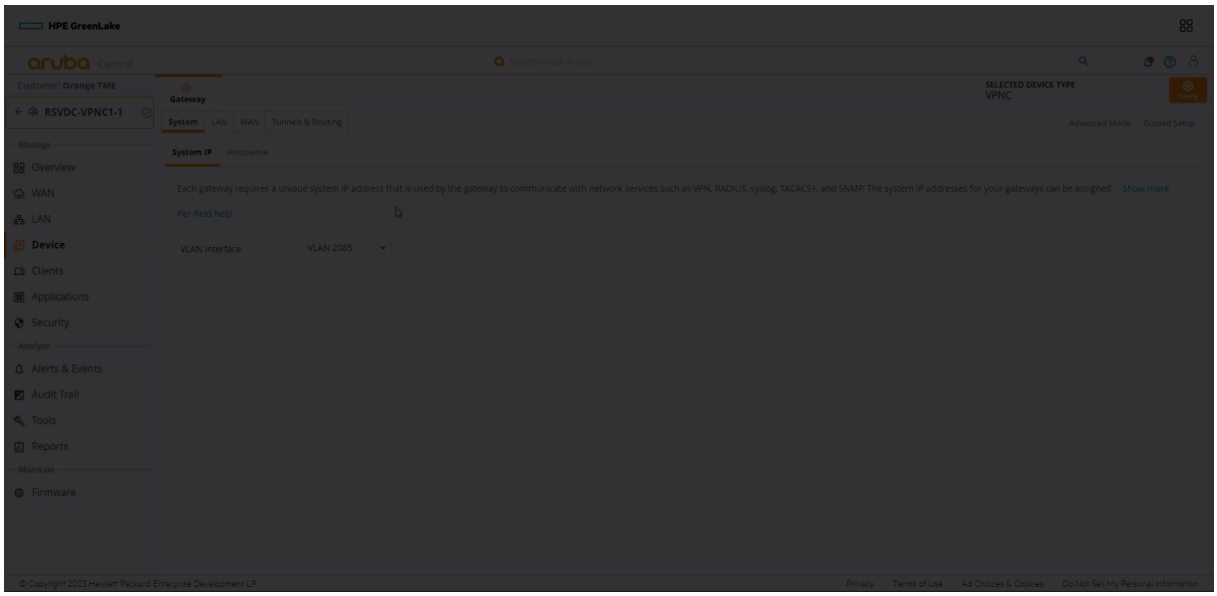


Figure 46: Configuring IP address

Step 4 Repeat steps 3 to 4 for each additional LAN uplink VLANs. The final configuration should look like the image below.

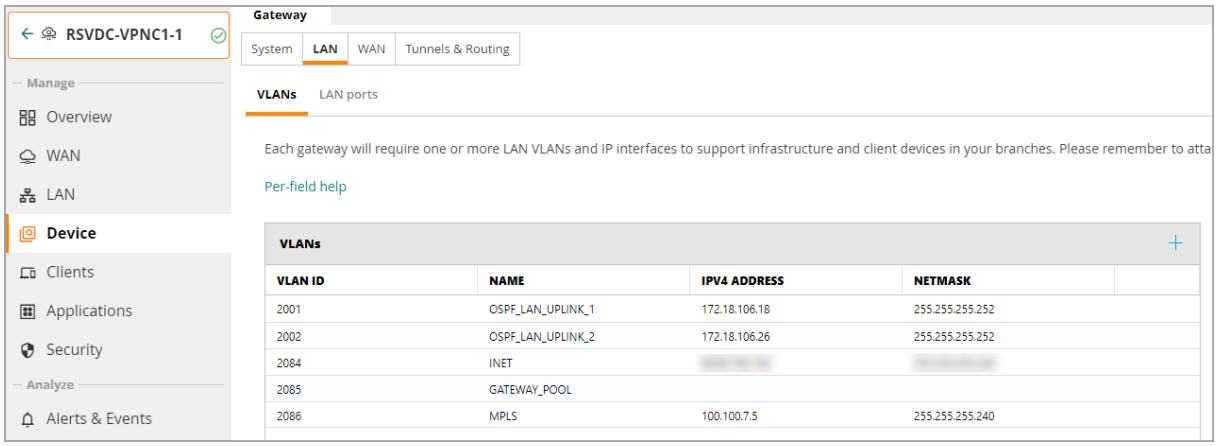


Figure 47: Final VLAN configuration

Configure the WAN Ports

In this procedure, configure the WAN uplinks and map them to the VLANs.

Step 1 Go to the **WAN** tab in **Basic Mode**.

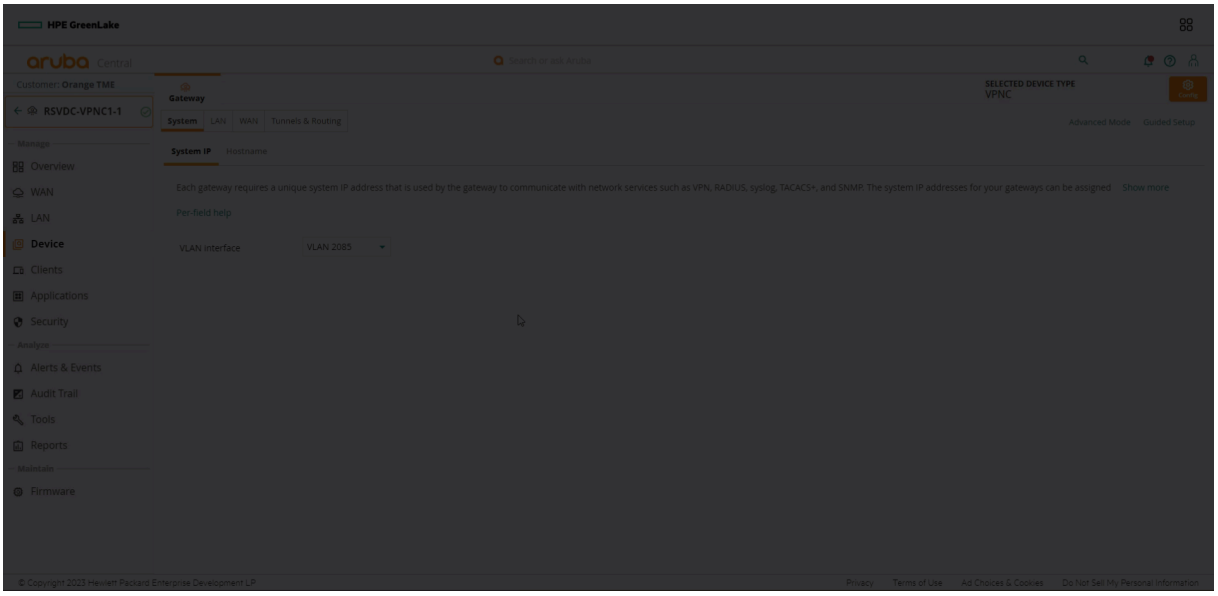
Step 2 In the **Uplinks** table, click the **+** (plus sign).

Step 3 In the **Add/Edit Uplink** window, enter an uplink **Name** and select the **uplink VLAN**.

NOTE:

If **WAN type** is set to *Internet*, enter a public IP address or use a private address and configure 1:1 NAT translation on the internet edge firewall. If **WAN type** is set to *MPLS*, the uplink name must match between the VPNC and BGW to enable automated tunnel orchestration between gateways.

I AM HERE!!!!



NOTE:

While this example uses the name **MPLS** for the uplink, it is common to use a provider name to represent the private transport.

Onboard VPNC to Central

Static Provisioning (One Touch Provisioning)

The VPNCs in this deployment do not receive a DHCP address from any of their WAN connections, meaning they cannot communicate with Central. To register these devices with Central, One Touch Provisioning must be used. This step can be skipped if the gateways will connect to a device that assigns them a DHCP address and Internet access.

Step 1 Using the VPNC console port and a terminal, enter the settings below connect to the gateway.

- **Baud rate**: *9600*
- **Data bits**: *8*
- **Parity**: *None*
- **Stop bits**: *1*
- **Flow control**: *None*

Step 2 Select the **static-activate** option from the menu and follow the prompt to configure the WAN connection manually.

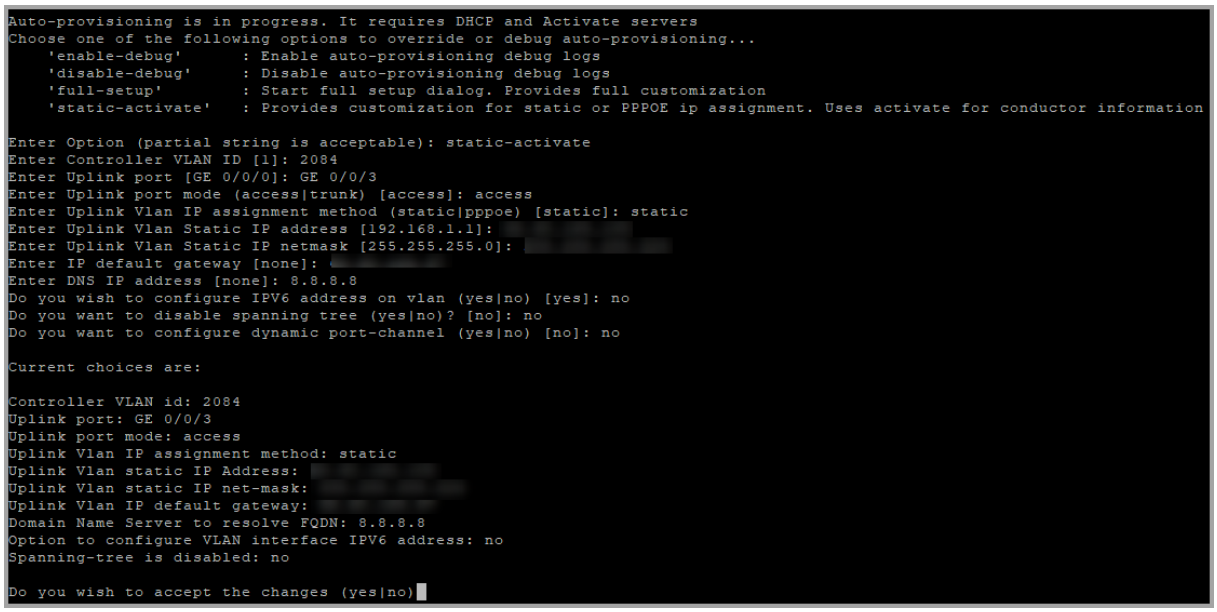


Figure 48: Static-Activate

NOTE:

To bring up a Gateway using DHCP, see the “Configuring the Branch Gateway” section.

Deploying Branch Site

The following chapter of this guide includes procedures to configure three components of an Aruba SD-Branch site. This includes guidance on Branch Gateways, Switches and Access points.

Aruba Branch Gateway Configuration

In this set of procedures, the branch gateway (BGW) is configured in two steps. The first step is the group level configuration, where the bulk of configuration is performed. This includes all common configurations, such as NTP, DNS, and VLANs.

After the group configuration is complete, each BGW's device-specific configuration, such as hostname and IP addressing, is applied. This is applied before the device comes online with preprovisioning.

Create a Branch Gateway Group and Preprovision Gateways

Refer to the "Preparing to Deploy" section to create the branch group and move the gateways to the group.

Configure the Branch Gateway Group

Step 1 In **Global** dropdown, search or select the ***BR-ECSDB*** created in the "Preparing to Deploy" section.

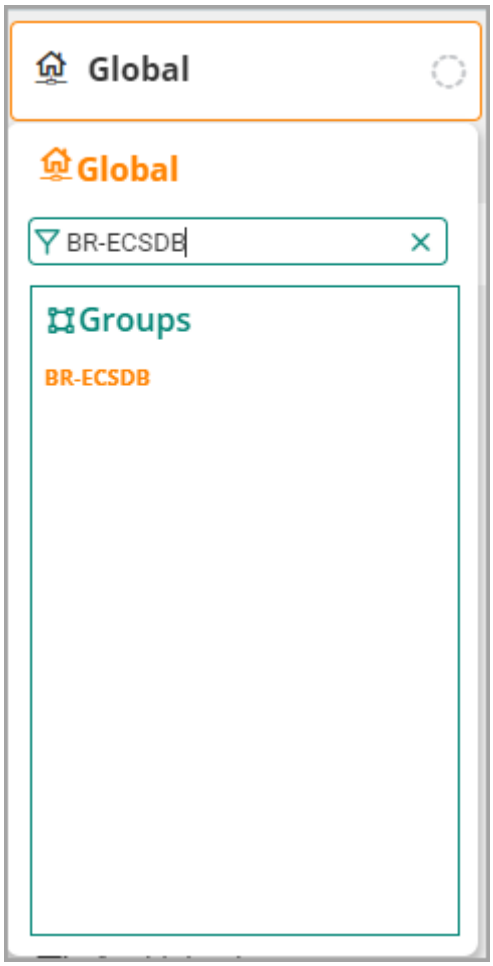


Figure 49: Select Group

Step 2 In the left navigation pane, in the **Manage** section, select **Devices**.

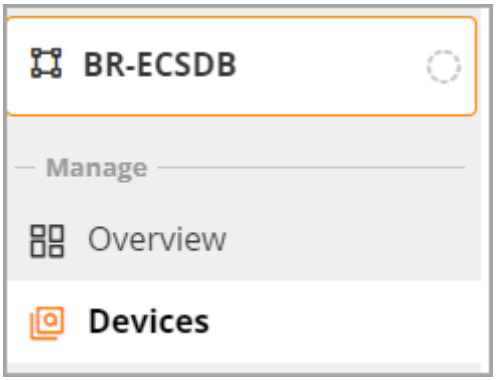


Figure 50: Select Devices

Step 3 Select the **Gateways** tab, then click the gear icon in the upper right corner.

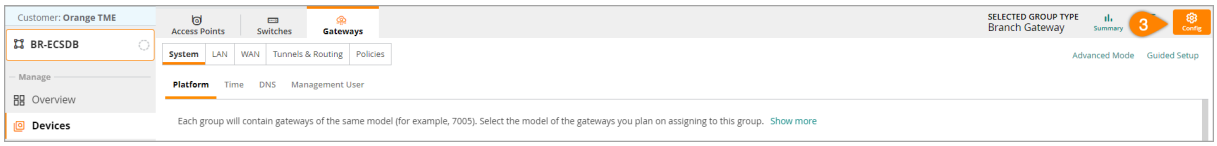


Figure 51: Select Config

Step 4 Click **Cancel**, then click **Exit**.

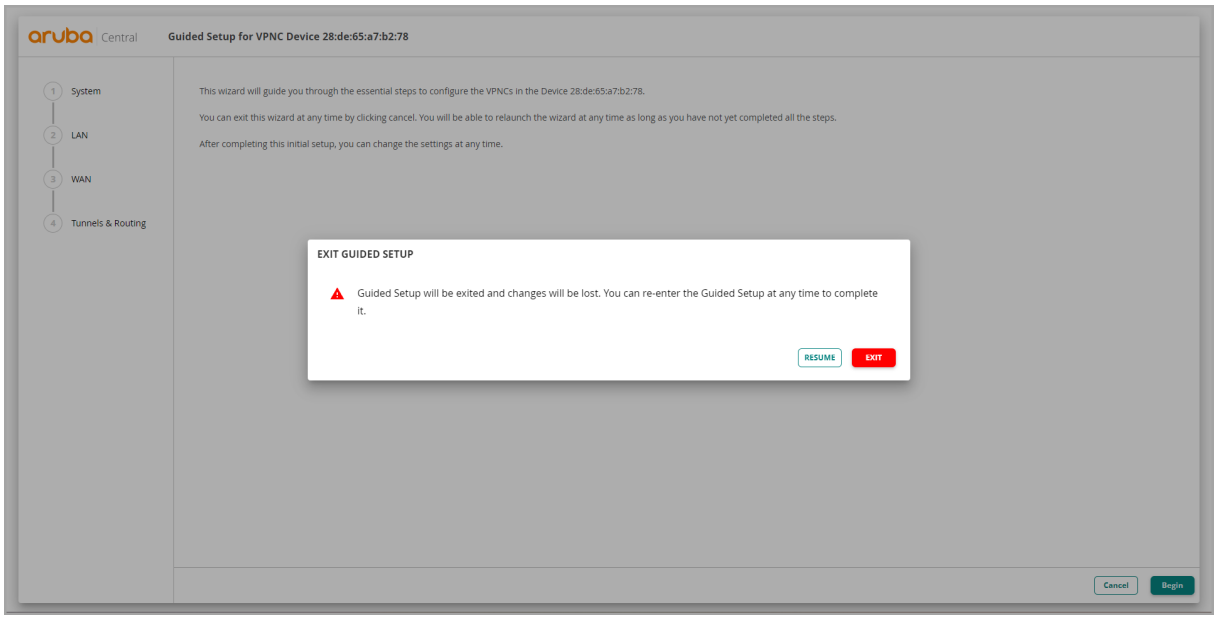


Figure 52: Guided_Setup

Configure Model

Use this procedure to set the gateway model. Each group can contain only a single gateway model.

Step 1 On the **Gateways** tab, in the **System** section, select **Platform**.

Step 2 In the **Model** dropdown select the platform you are standardizing on. In this case, **A9004** is selected.

Configure System IP Pool

Set the configuration approach to *Specify static IP address later*. This is done because the management VLAN will be used as the System IP address. Ensuring that the system IP is set to a VLAN that is trunked throughout the environment is critical for high availability and wired/wireless tunneling best practice.

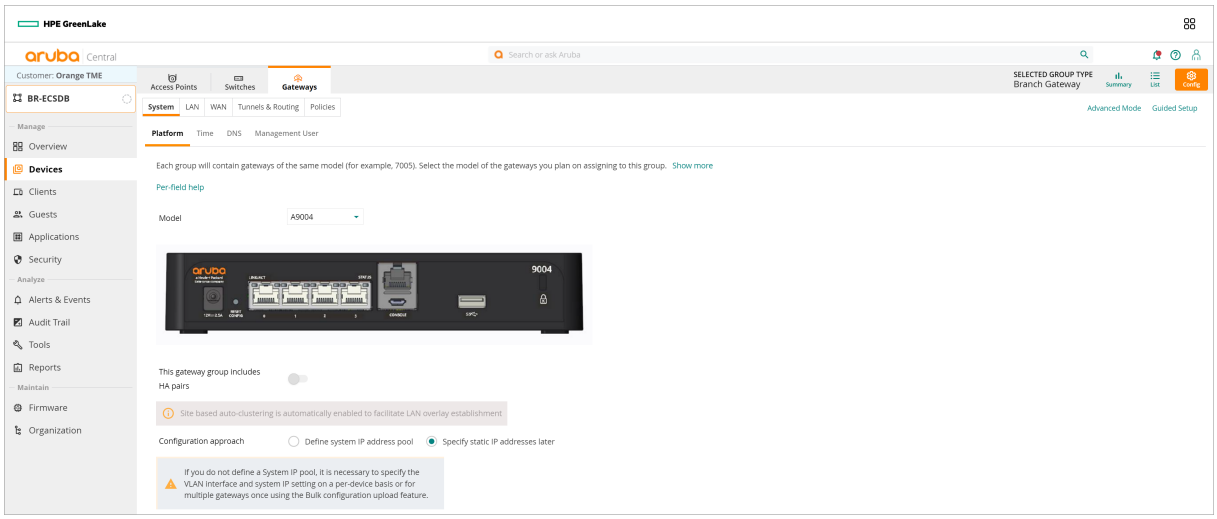


Figure 53: Select Platform

Set the System Time Parameters

Use this procedure to set the network time protocol (NTP) parameters and time zone to keep the BGW clocks synchronized.

Step 1 On the **Gateways** tab, in the **System** section, select **Time**.

Step 2 In the **Public NTP Servers** table, click the **+** (plus sign) to add a public NTP server.

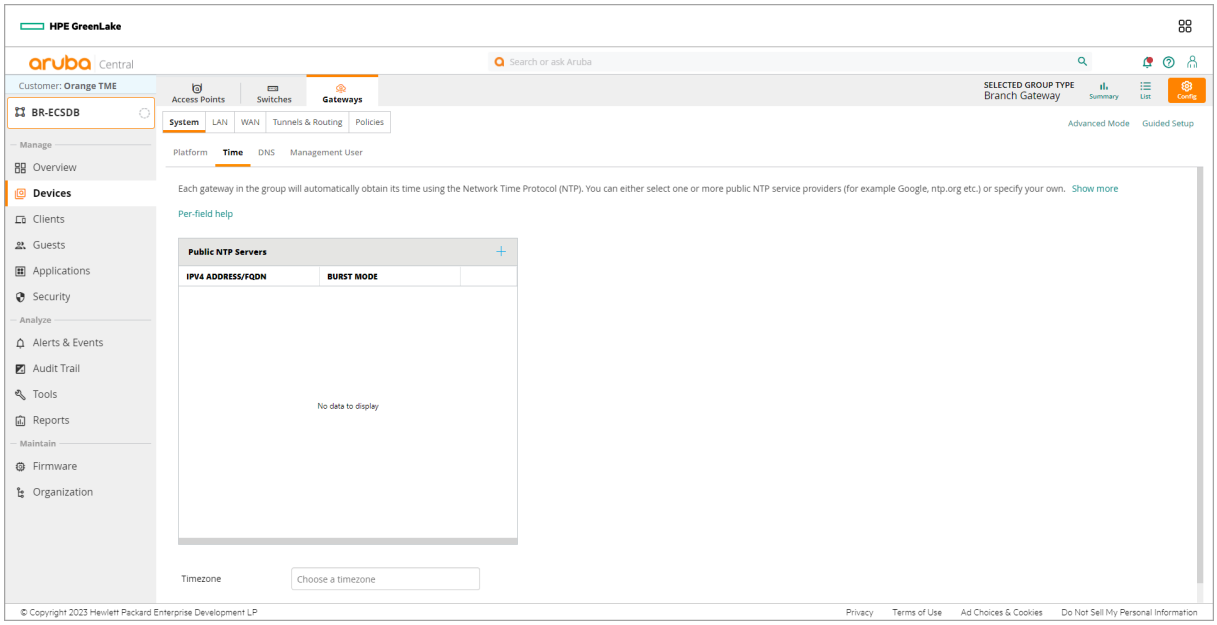


Figure 54: Setting_NTP

Step 3 In the **IPv4 Address/FQDN** column, enter *pool.ntp.org* or other NTP server address.

Step 4 Select **Burst Mode** if this feature is supported by the NTP server. Burst mode provides faster time synchronization.

Step 5 In the **Timezone** dropdown, select the time zone, then click **Save Settings**.

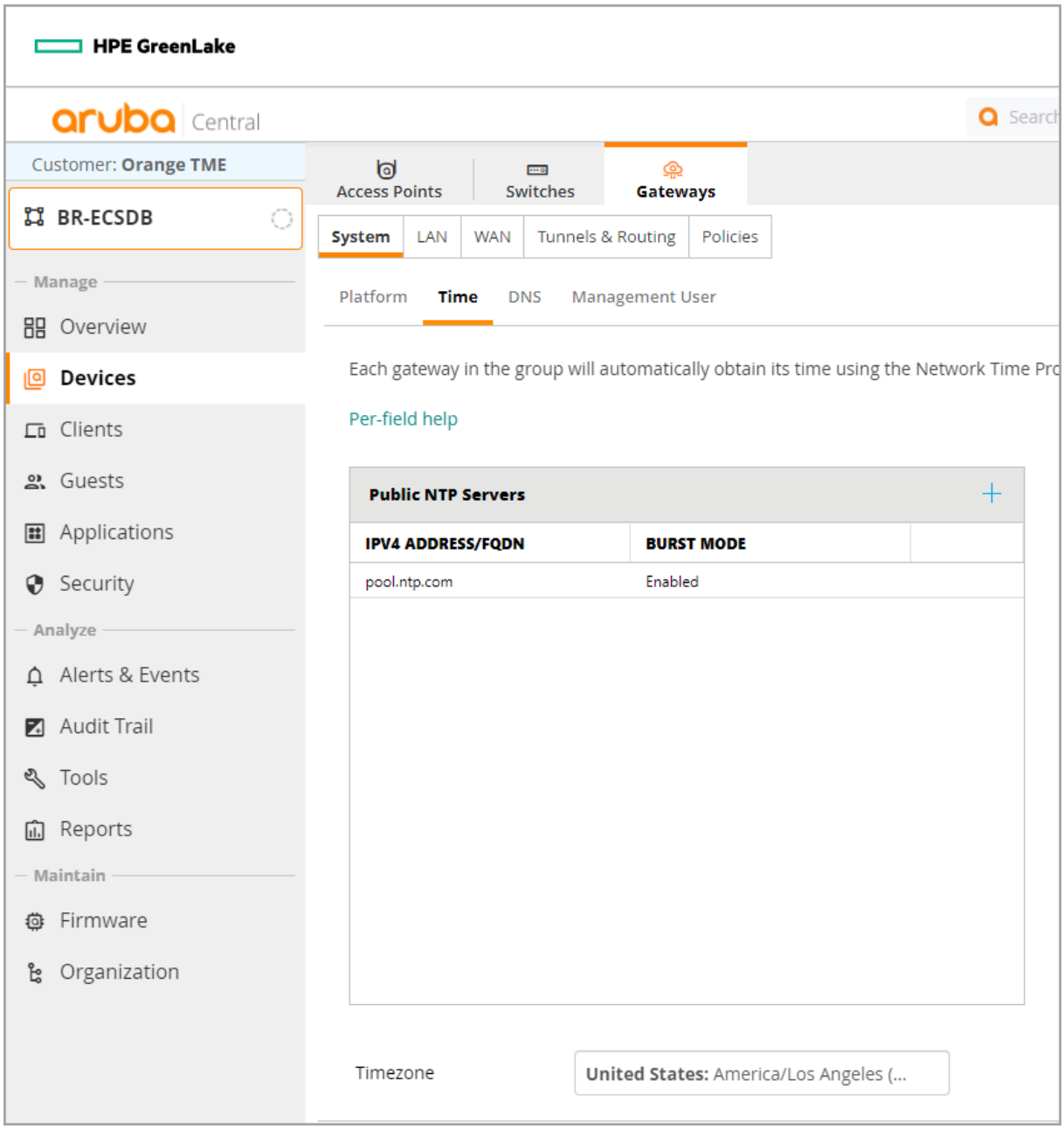


Figure 55: NTP Server

Set DNS Servers

Specify the DNS server(s) the BGW uses to communicate with Central.

Step 1 On the **Gateways** tab, in the **System** section, select **DNS**.

Step 2 Select **Specify DNS servers**.

Step 3 In the **Domain name** text box, enter a domain name (example: *example.local*).

Step 4 In the **Public DNS Servers** table, click the **+** (plus sign) to assign a public DNS server. For a virtual BGW, leave the default DNS provided by the cloud provider and go to Step 6.

Step 5 In the **Provider** dropdown, select one of the listed providers, or select **Alternate DNS** if the desired server is not in the list.

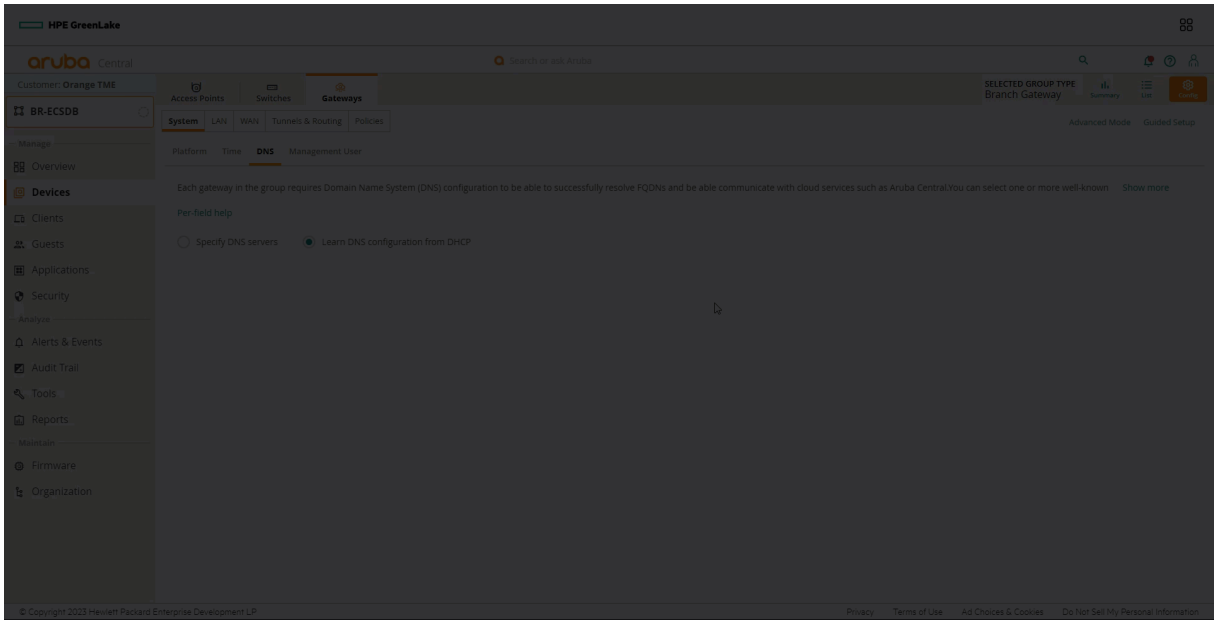


Figure 56: Configuring_DNS

Step 6 Click **Save Settings**.

NOTE:

The Gateway uses this DNS server for DNS lookups. Clients do not use this DNS server

Create a Management User Account

Create a management user account for CLI to access the gateways.

Step 1 On the **Gateways** tab, in the **System** section, select **Management User**.

Step 2 In the **Local management users** table, click the **+** (plus sign).

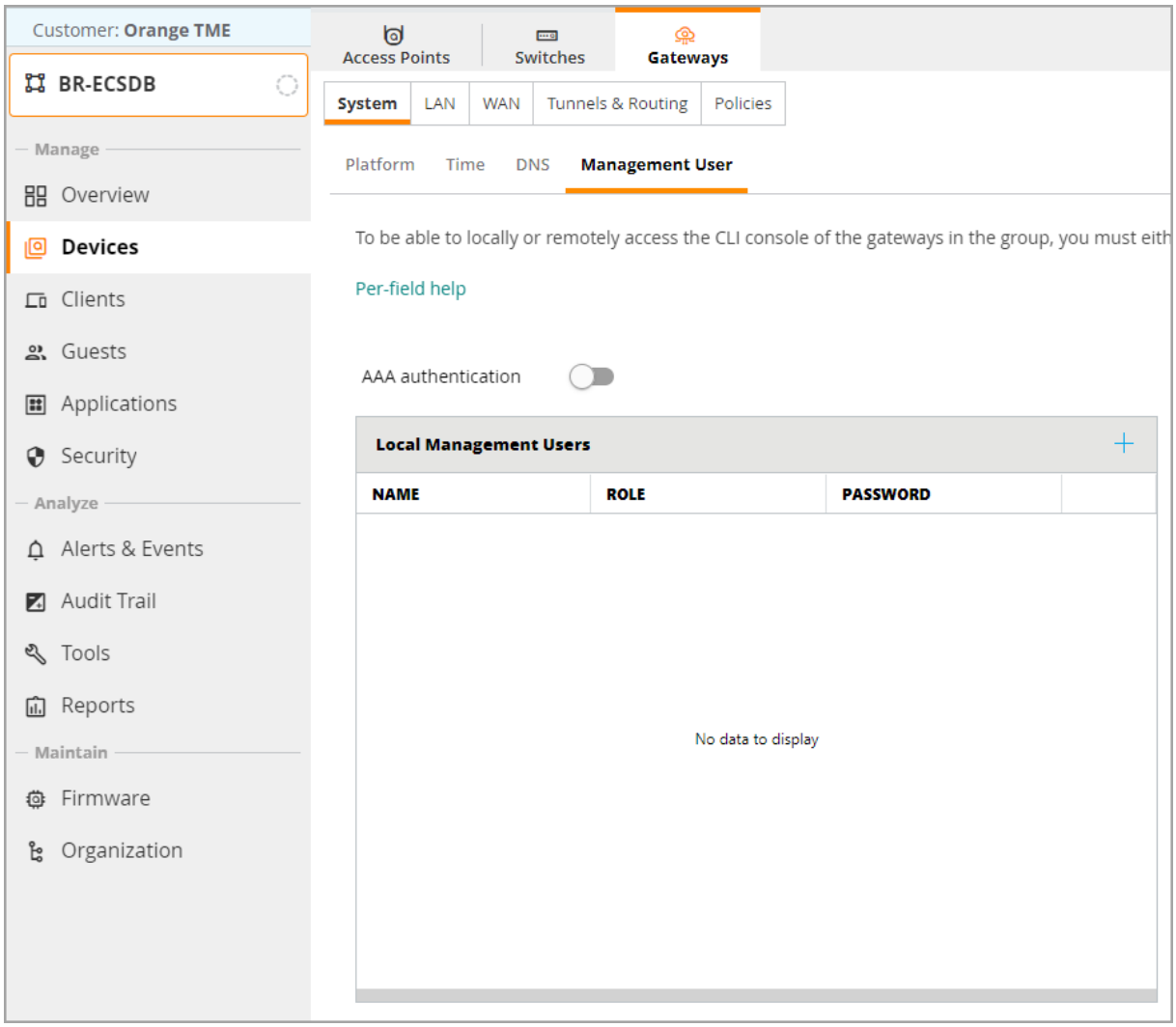


Figure 57: Add MGMT User

Step 3 In the **Add Management User** table, assign the following settings, then click **Save**. - **Name**: *admin* - **Password**: *password* - **Retype Password**: *password* - **Role**: *Super user role*

NOTE:

Create additional users with other roles as needed.

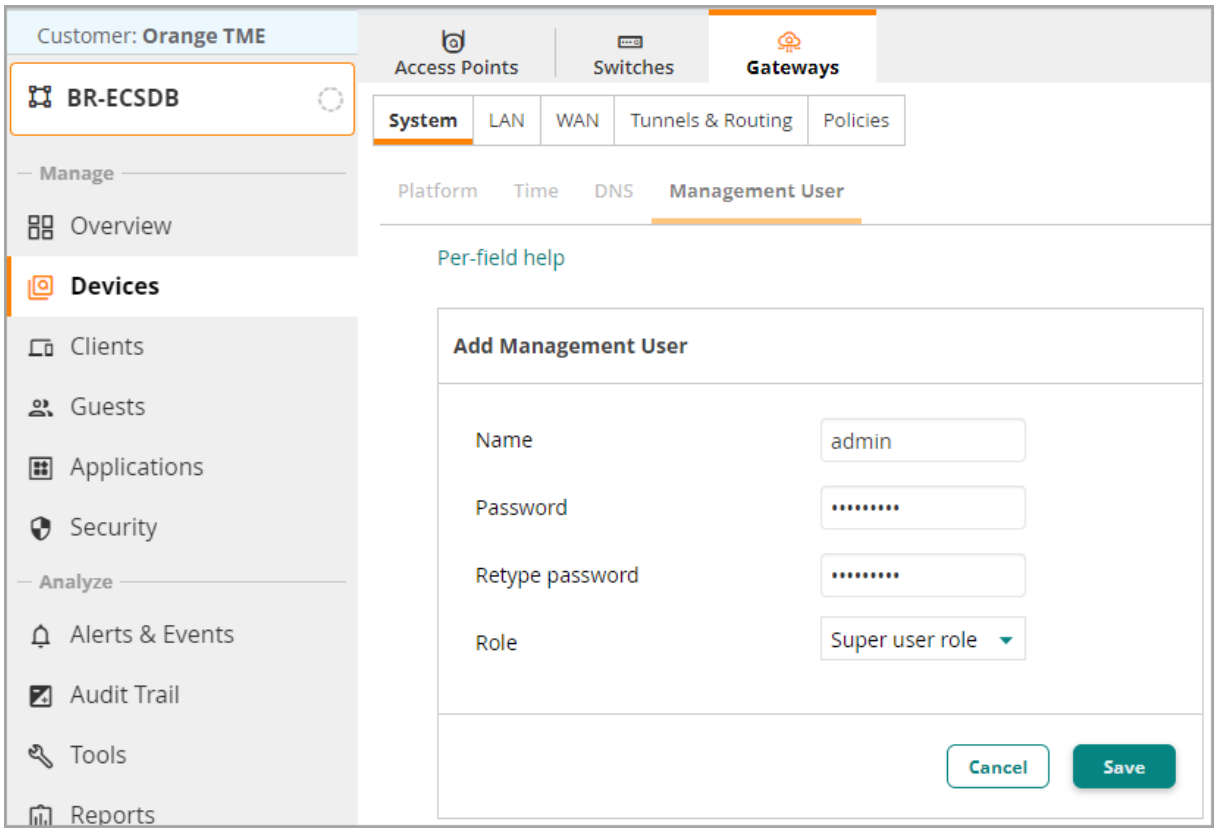


Figure 58: MGMT_Name_PW

Step 3 Click **Save Settings** in the bottom left corner.

Configure VLANs

In this section, the data VLANs are configured. This configuration is at the group level, so none of these VLANs have an IP address assigned.

Step 1 On the right side, click **Basic Mode**.

Step 2 Go to **LAN** and select **VLANs**.

Step 3 On the **VLANs** table, click the **+** (plus sign).

Step 4 In the New VLAN window, configure the below VLANs, then click **Save Settings**. - Select **Enable DHCP relay** for VLANs 1. *10.2.120.98* 2. *10.2.120.99*

Step 5 Repeat steps for all VLANs

VLAN Name	VLAN ID
MGMT	100
Employee	101
Printer	102

VLAN Name	VLAN ID
Camera	103
Guest	104
Reject	105
Critical	106
Quarantine	107

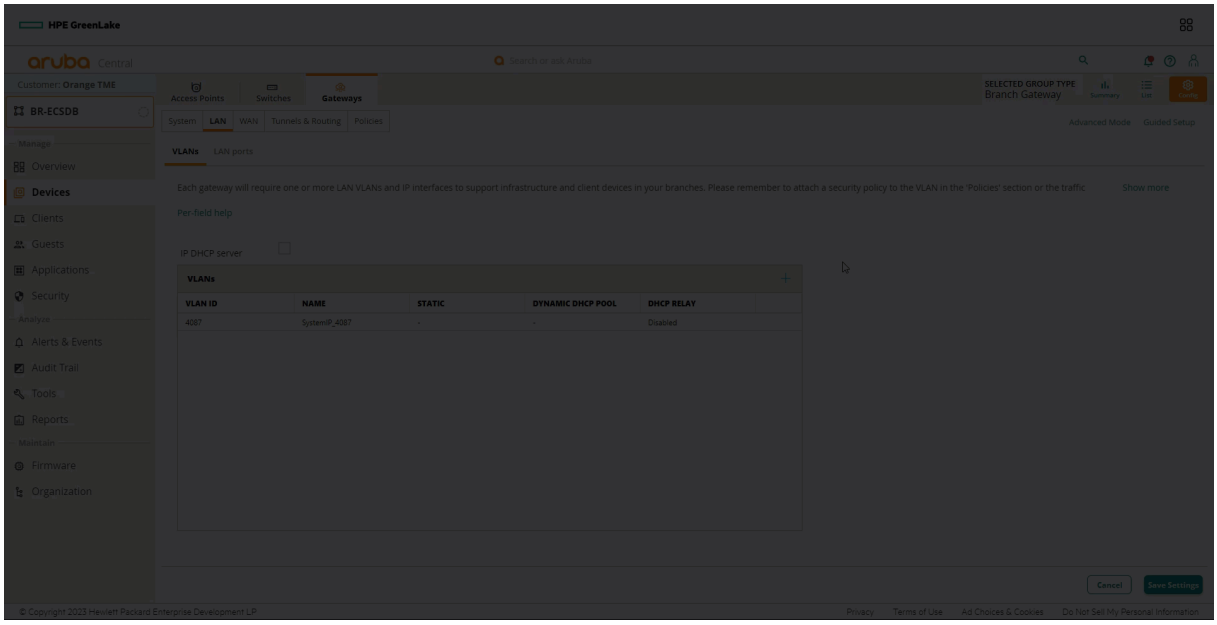


Figure 59: Creating_VLAN

Configure LAN links

In this section, the LAN links are configured.

Step 1 On the right side, click **Basic Mode**.

Step 2 Go to **LAN** and select **LAN ports**.

Step 3 On the **LAN Ports/Port Channels** table, click the **+** (plus sign).

Step 4 Configure the LAN ports with the information in the below table

Name	Port	Mode	Access VLAN	Native VLAN	Allowed VLANs
GE2 Trunk to LAN	GE-0/0/2	trunk	*blank*	100	*blank*
GE3 Trunk to LAN	GE-0/0/3	trunk	*blank*	100	*blank*

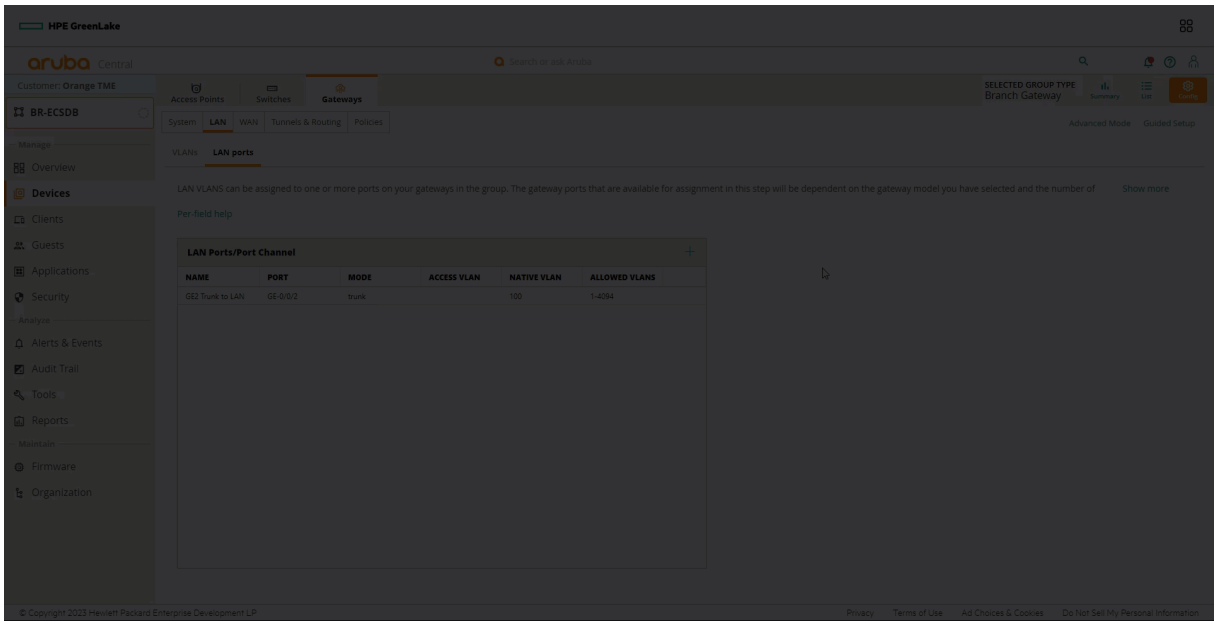


Figure 60: Configure_LAN_Ports

Configure WAN Uplinks

In this section, the WAN uplinks are configured. This configuration is at the group level, so none of these uplinks have an IP address assigned. Port 0/0/0 is used for the Internet connection and port 0/0/1 is used for MPLS. The **Uplink field** is generally the name of the service provider. For MPLS, ensure that the uplink field matches across all devices.

Step 1 On the right side, click **Basic Mode**.

Step 2 Go to **WAN** and select **WAN Details**.

Step 3 On the **WAN Uplinks/Ports** table, click the **+** (plus sign).

Step 4 In the **New WAN Uplink / Port** window configure the MPLS and INET uplinks.

MPLS:

- **Uplink:** *MPLS*
- **WAN Type:** *MPLS*
- **WAN Speed:** *10*
- **Source NAT:** *Unchecked*
- **Use as Back:** *Unchecked*
- **IP Addressing Method:** *Static*
- **Port:** *GE 0/0/1*
- **Secure with ACL:** *Unchecked*

INET

- **Uplink:** *INET*
- **WAN Type:** *INET*
- **WAN Speed:** *20*
- **Source NAT:** Checked
- **Use as Back:** Unchecked
- **IP Addressing Method:** *DHCP*
- **Port:** *GE 0/0/0*
- **Secure with ACL:** *Checked*

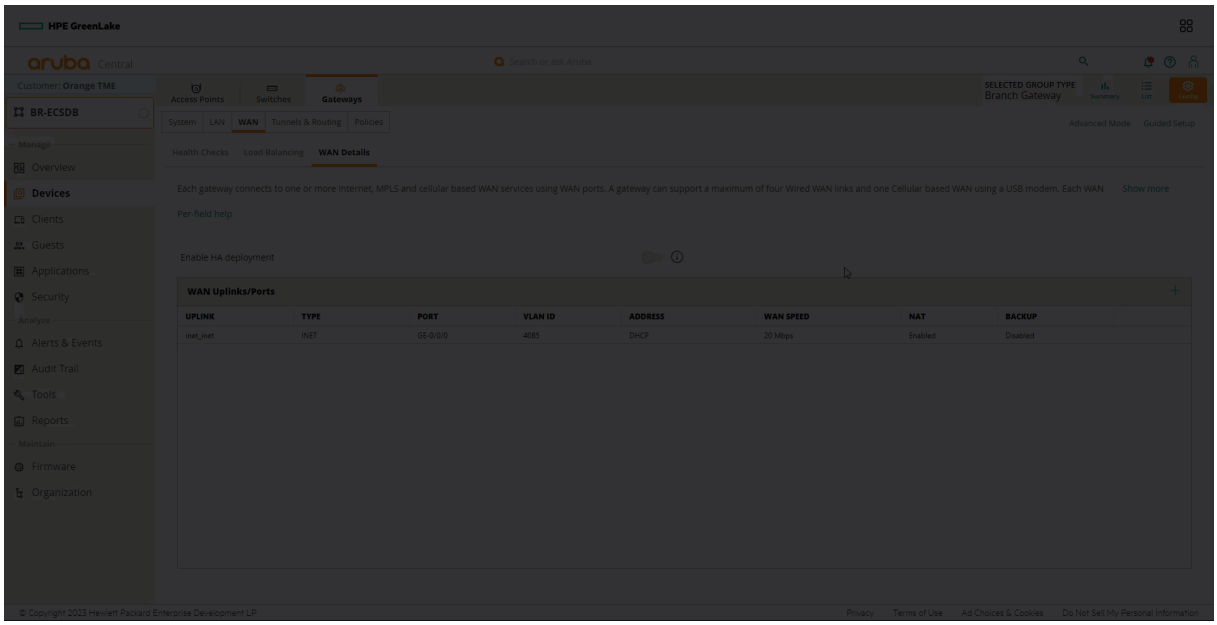


Figure 61: Setting WAN Uplinks

Configure the WAN Load Balancing Algorithm

Uplink utilization is recommended for use as the load balancing algorithm. This moves traffic from oversaturated links to a less used link if the bandwidth threshold is exceeded.

Step 1 On the configuration **Gateways** tab in **Basic Mode**, go to **WAN** and select **Load Balancing**.

Step 2 In the **Load balancing mode** list, select **Uplink utilization**.

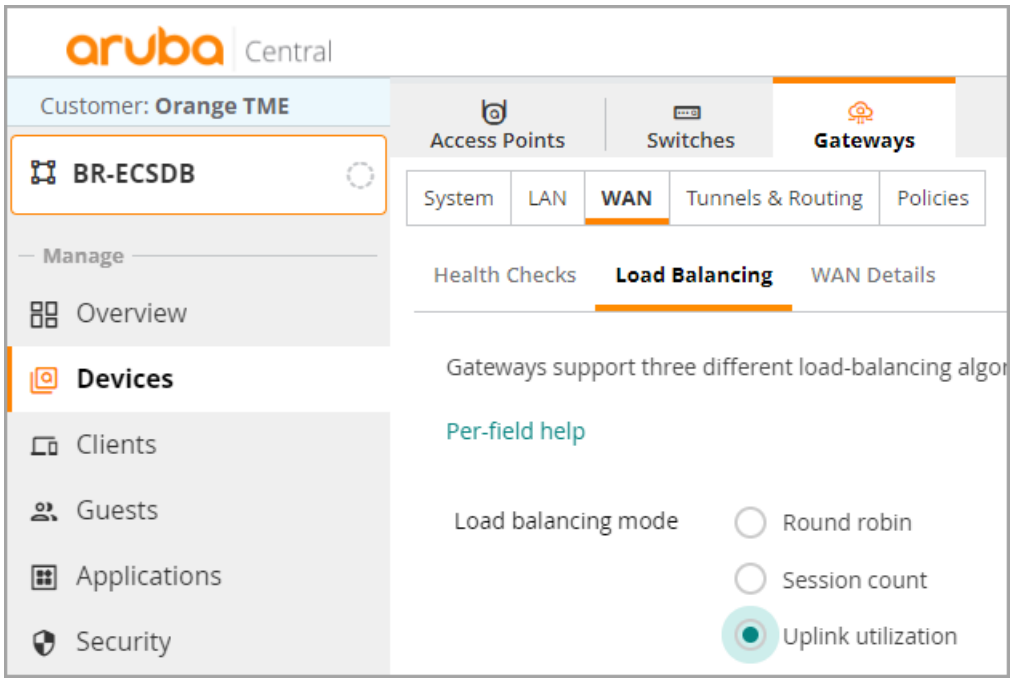


Figure 62: Configure WAN Load Balancing Algorithm

Configure the Overlay and Set the VPNC Preference

Use this procedure to assign data center preferences for tunnel orchestration for the VPN concentrators (VPNCs).

Step 1 In basic mode select **Tunnels & Routing**, then **DC Preference**.

Step 2 In the **DC Preference** table, click the **+** (plus sign) to add a VPNC hub group.

Step 3 In the **Hub Group** dropdown, select a VPNC group to assign the preferred data center.

Step 4 In the **Primary VPNC** dropdown, select the primary VPNC.

Step 5 In the **Secondary VPNC** dropdown, select the secondary VPNC, then click **Save Settings**.

NOTE:

VPNCs do not appear unless they have been configured. See the “Configuring VPNC” section to configure the VPNCs.

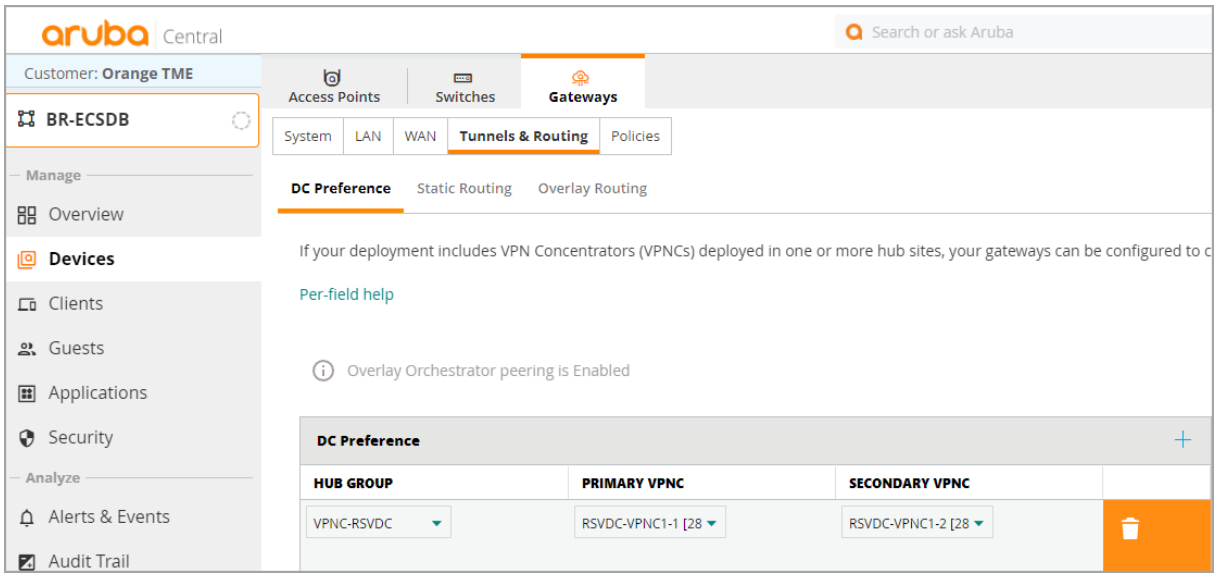


Figure 63: Enabling Overlay

Step 6 Repeat steps 3 to 5 if a secondary data center is used. Groups higher in the list (with lower numbers) are treated as more preferred VPNC groups.

NOTE:

The procedures in guide do not use a second DC; this is just an example.

Enable Overlay Routes

In this procedure, branch subnets are redistributed into the VPN overlay to ensure route reachability with other sites.

Step 1 In **Basic** mode, select **Tunnels & Routing**, then **Overlay Routes**.

Step 3 In **Redistribute connected vlans**, select all the user VLANs and system IP VLAN for overlay redistribution, then click **Save Settings**.

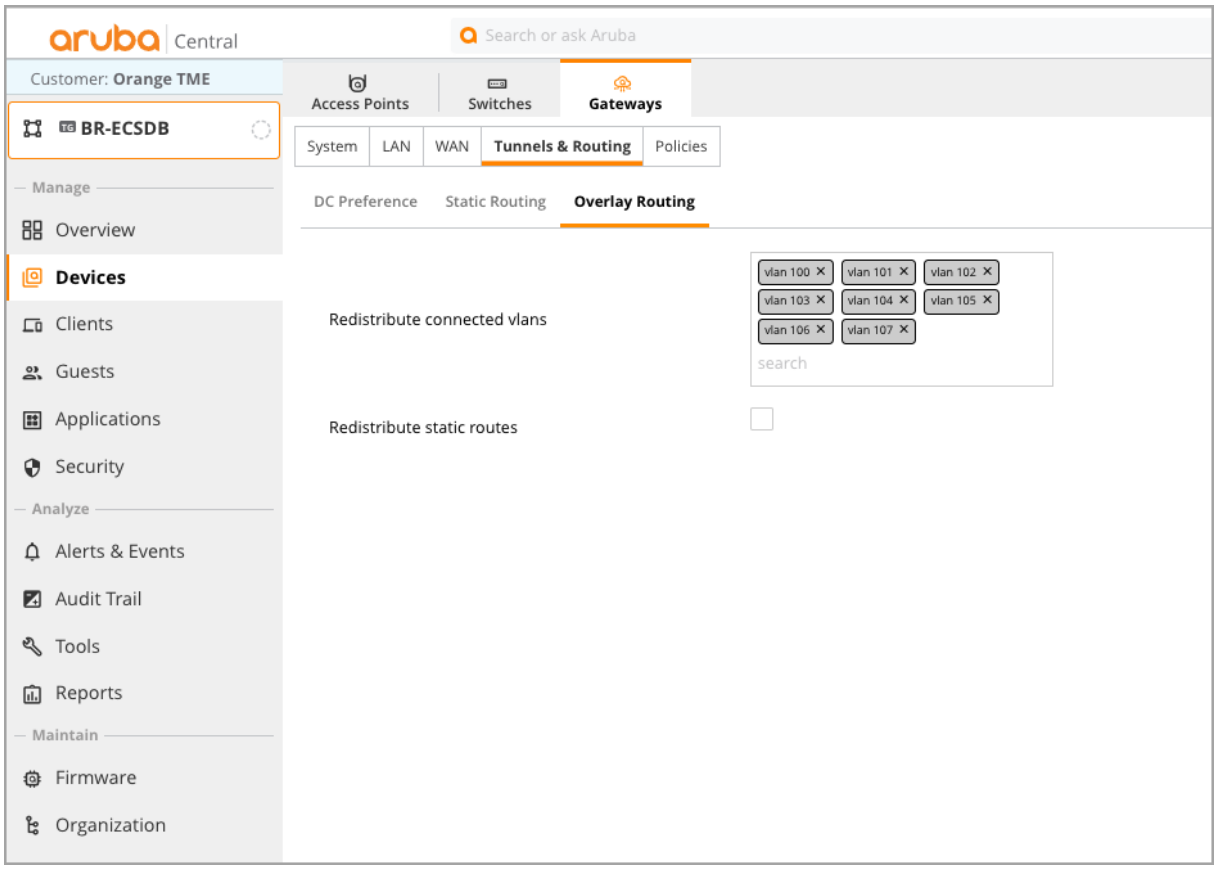


Figure 64: Redistribute_VLANs

Enable DPI and Application Visibility

Deep packet inspection and Application Visibility must be enabled for Dynamic Path Steering and SAAS Express to function. This section describes how to enable these features.

NOTE:

This procedure will cause the gateways to reboot to apply the configuration.

Step 1 Verify that the Gateway configuration mode is in **Advanced Mode**.

Step 2 Select the **Security** tab, then select **Applications**.

Step 3 Expand the **Application Visibility** section.

Step 4 Check the **Deep packet inspection** checkbox.

Step 5 Check the **App performance monitoring** checkbox.

Step 6 Click **Save Settings**.

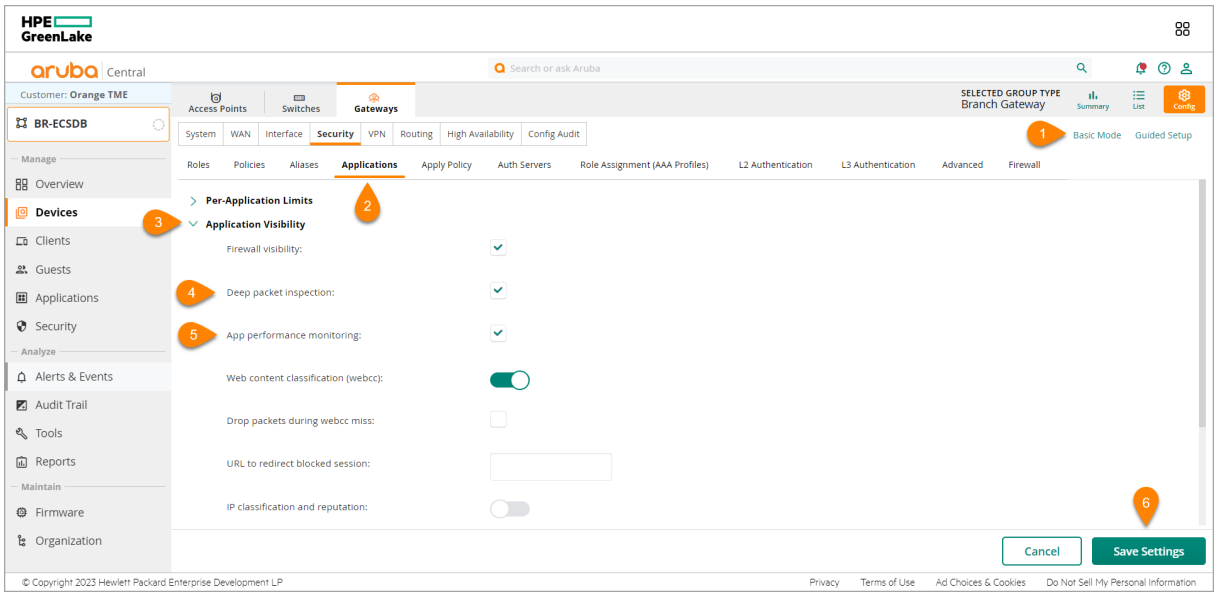


Figure 65: Enable DPI & Application Visibility

NOTE:

Deep packet inspection is enabled by default at the device level, but it is best practice to also enable it at the group level.

Configure Policies for Dynamic Path Steering

The dynamic path steering (DPS) feature allows traffic routing in real-time and traffic load balancing across available uplinks based on the performance of the uplinks. DPS policies and configurations are unique to each environment, based on the organization's applications and performance needs. General guidance on developing a DPS policy can be found in the design section of the guide here. This section describes how to configure a DPS policy to select the optimal WAN path and apply forward error correction (FEC) for voice traffic.

Additional policies should be created based on application requirements.

NOTE:

While this example deployment does not utilize LTE connections, LTE is included in the below policy to facilitate the future addition of LTE uplinks without the need to modify the policy.

Create Policy

Step 1 Verify that the Gateway configuration mode is in **Basic Mode**.

Step 2 Select the **Policies** tab, then select **DPS**.

Step 3 Click the **+** (plus sign) to create a new DPS policy.

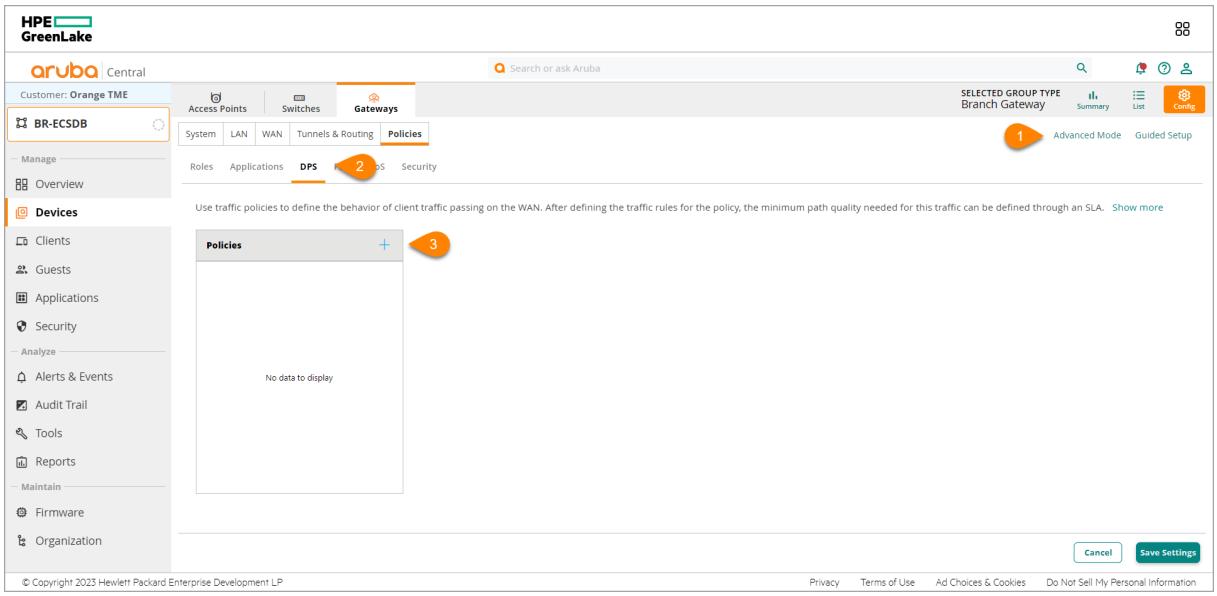


Figure 66: Create DPS Policy

Step 4 In the **Create Policy** window, assign the following settings and click **Save**.

- **Policy Type:** *DPS*
- **Policy Name:** *Protect-Voice*

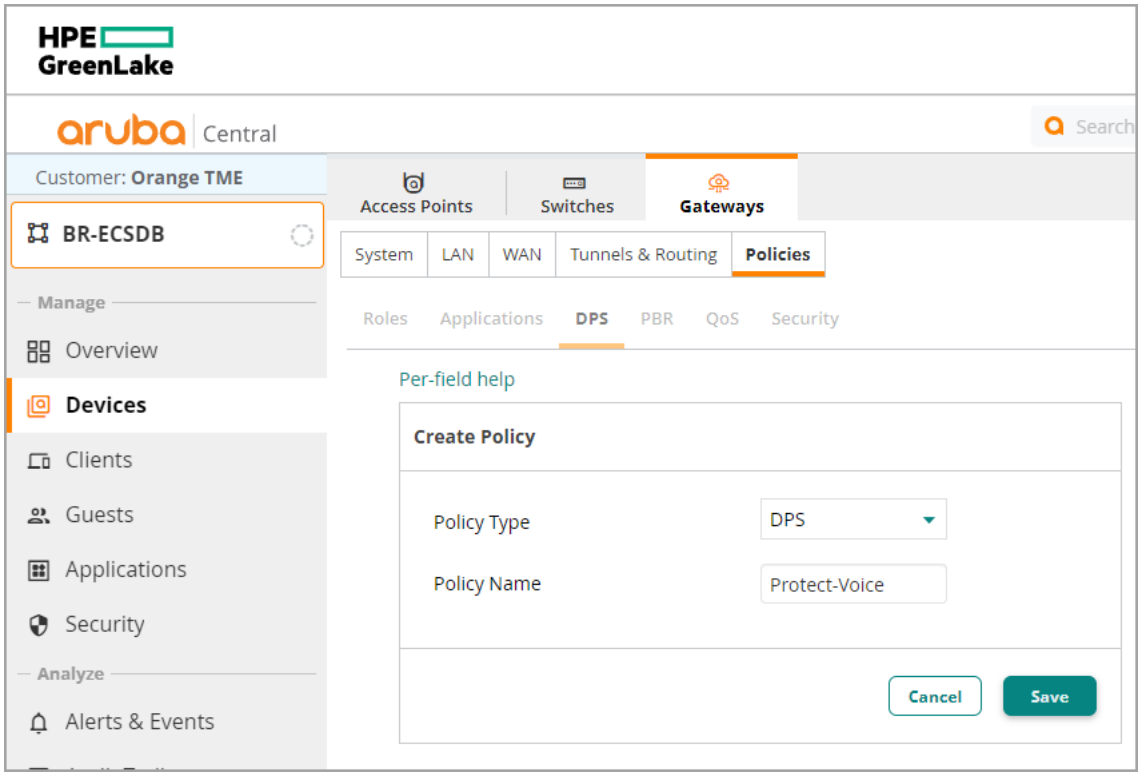


Figure 67: Create DPS Policy

Identify Traffic

Step 1 Select **Protect-Voice**.

Step 2 Click the edit (pencil) icon in the **Traffic Rules** section.

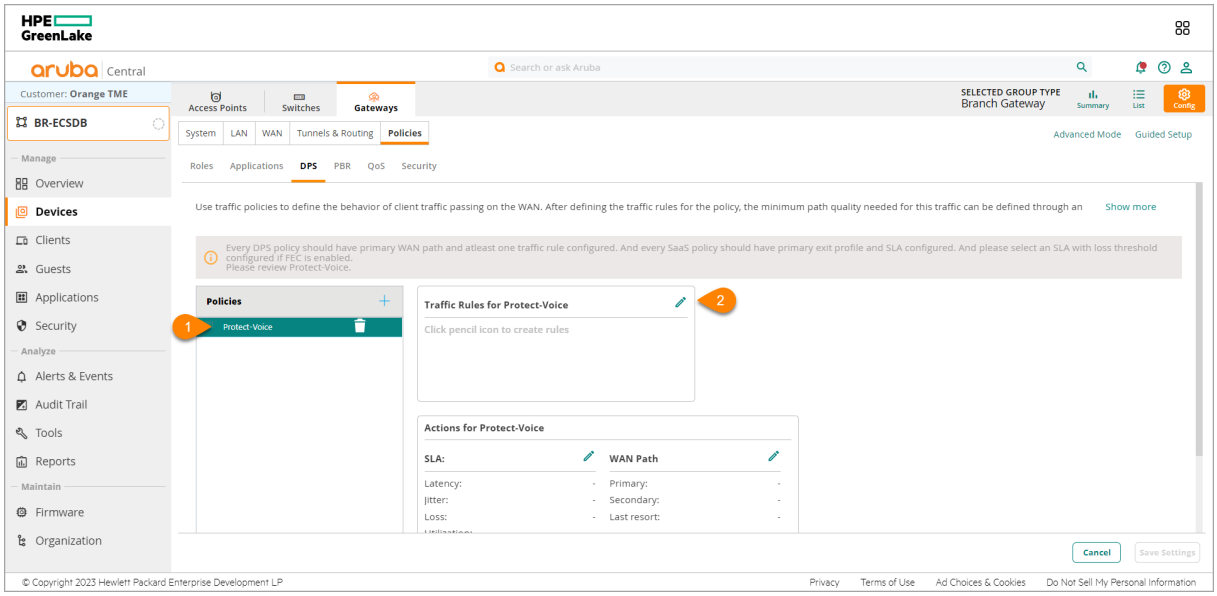


Figure 68: Identify Traffic 1

Step 3 Click the **+** (plus sign) to create a new traffic specification rule.

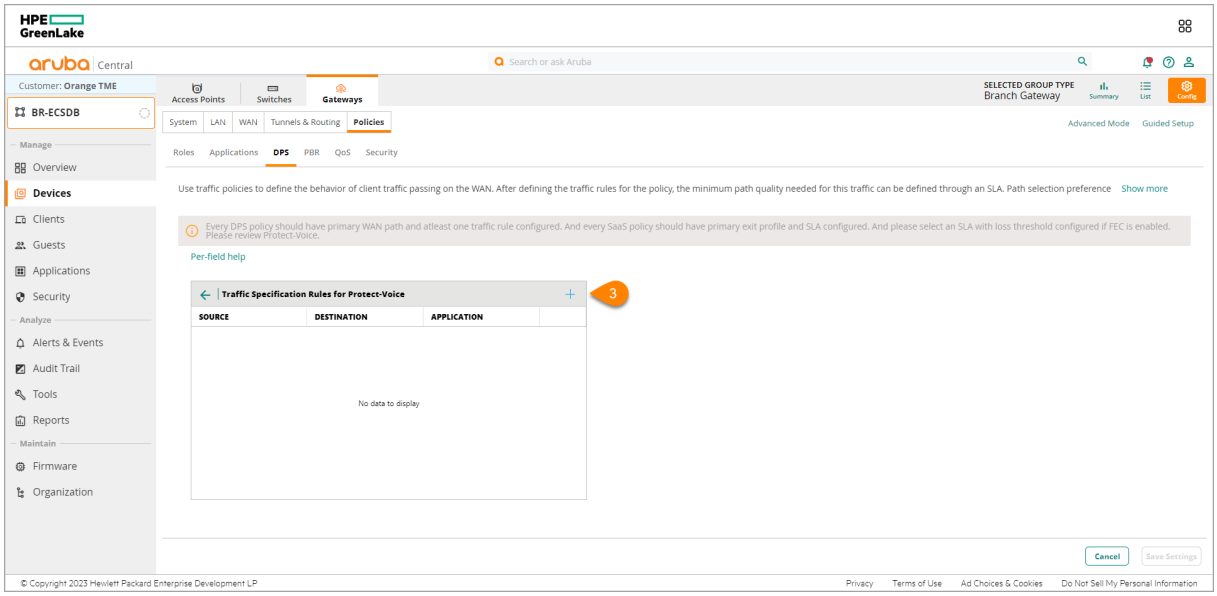


Figure 69: Identify Traffic 2

Step 4 In the **Add Rules for Protect-Voice** window, assign the following settings and click **Save**.

- **Source:** *Any*
- **Destination:** *Any*

- **Application/Port:** *App Categories*
- **App Categories:** *unified-communications*

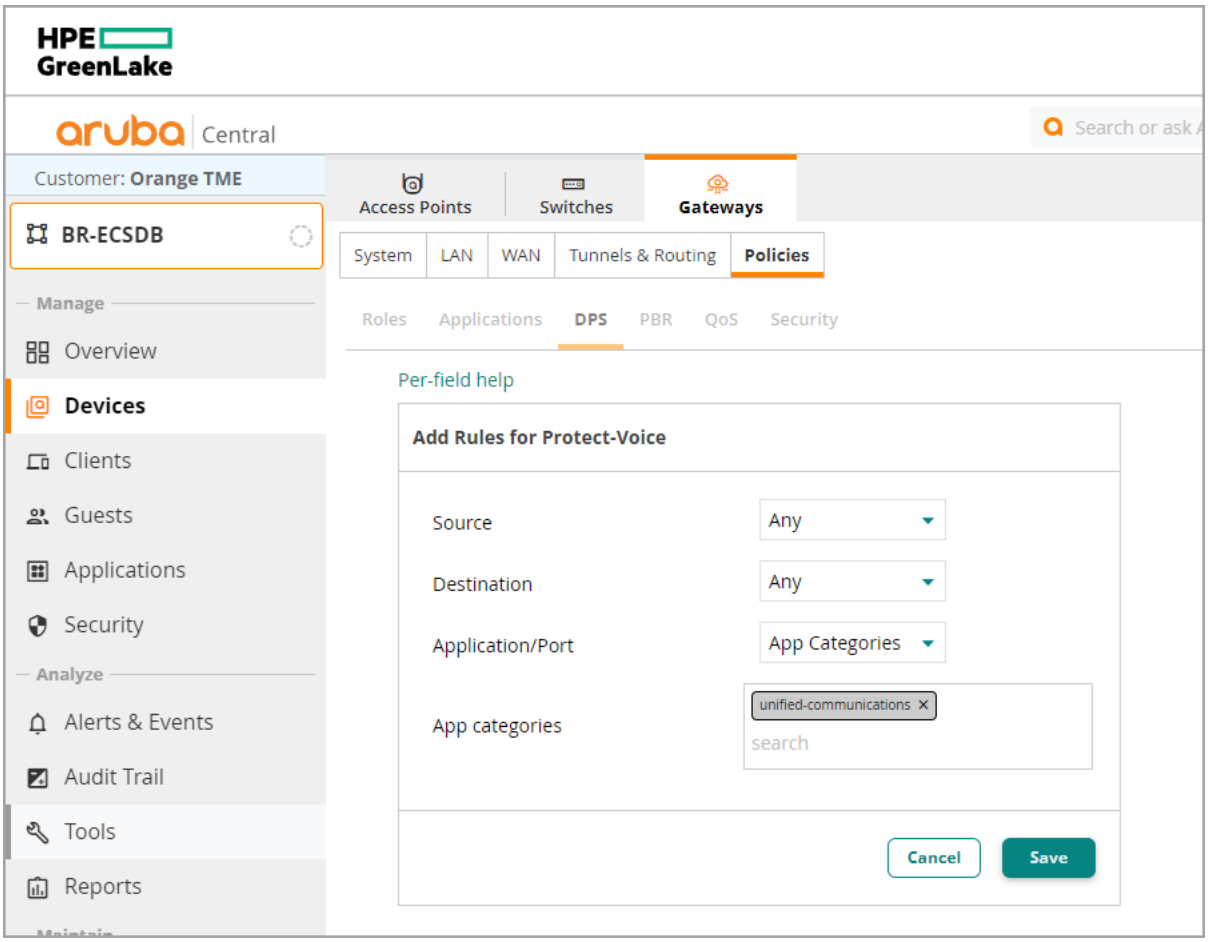


Figure 70: Identify Traffic 3

Step 5 Click the **back arrow.**

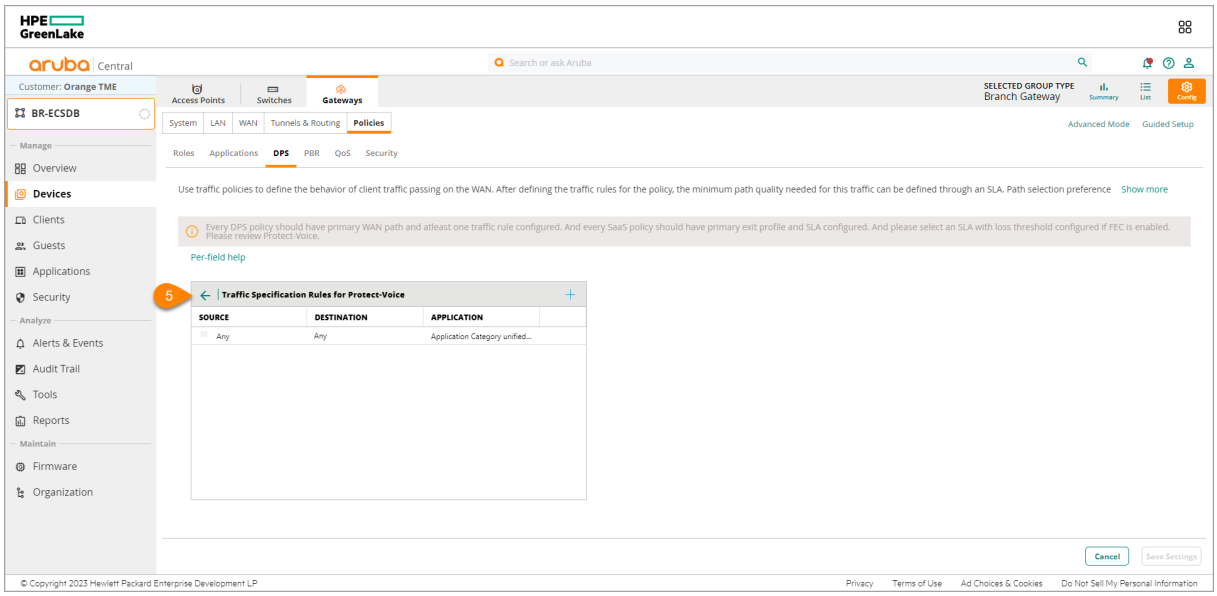


Figure 71: Identify Traffic 4

Set WAN Paths

Step 1 Select **Protect-Voice** and click the **pencil icon** next to WAN Path.

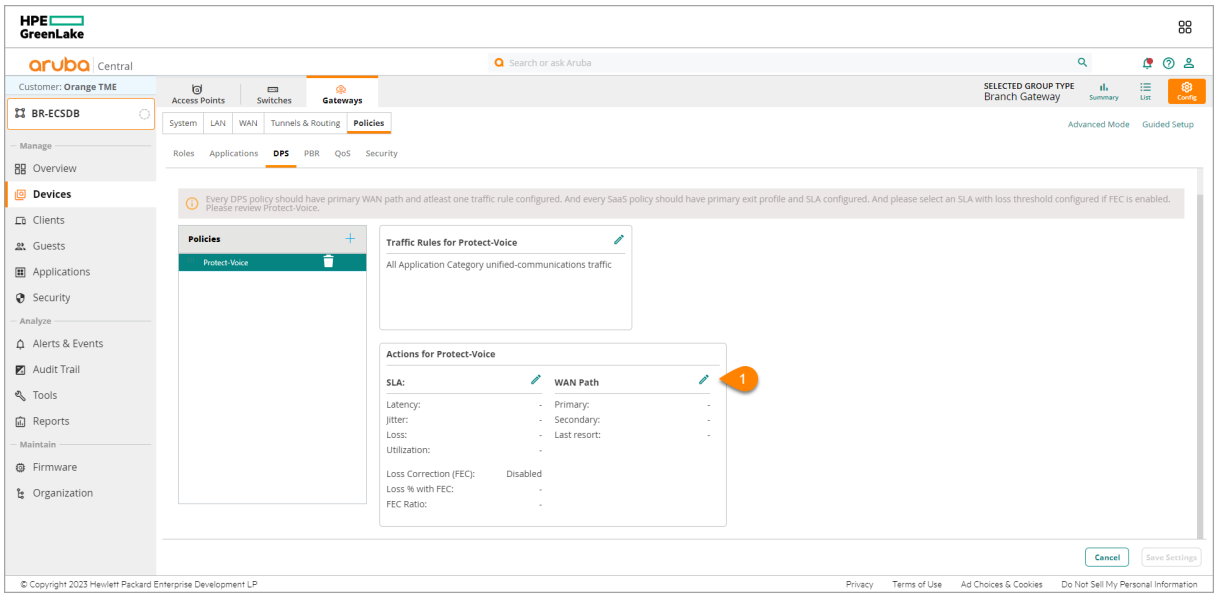


Figure 72: WAN Path 1

Step 2 In the **WAN Path for Protect-Voice** window, assign the following settings and click **Save**.

- **Primary path:** *ALL_MPLS*
- **Secondary path:** *ALL_INET*
- **Last resort path:** *ALL_LTE*

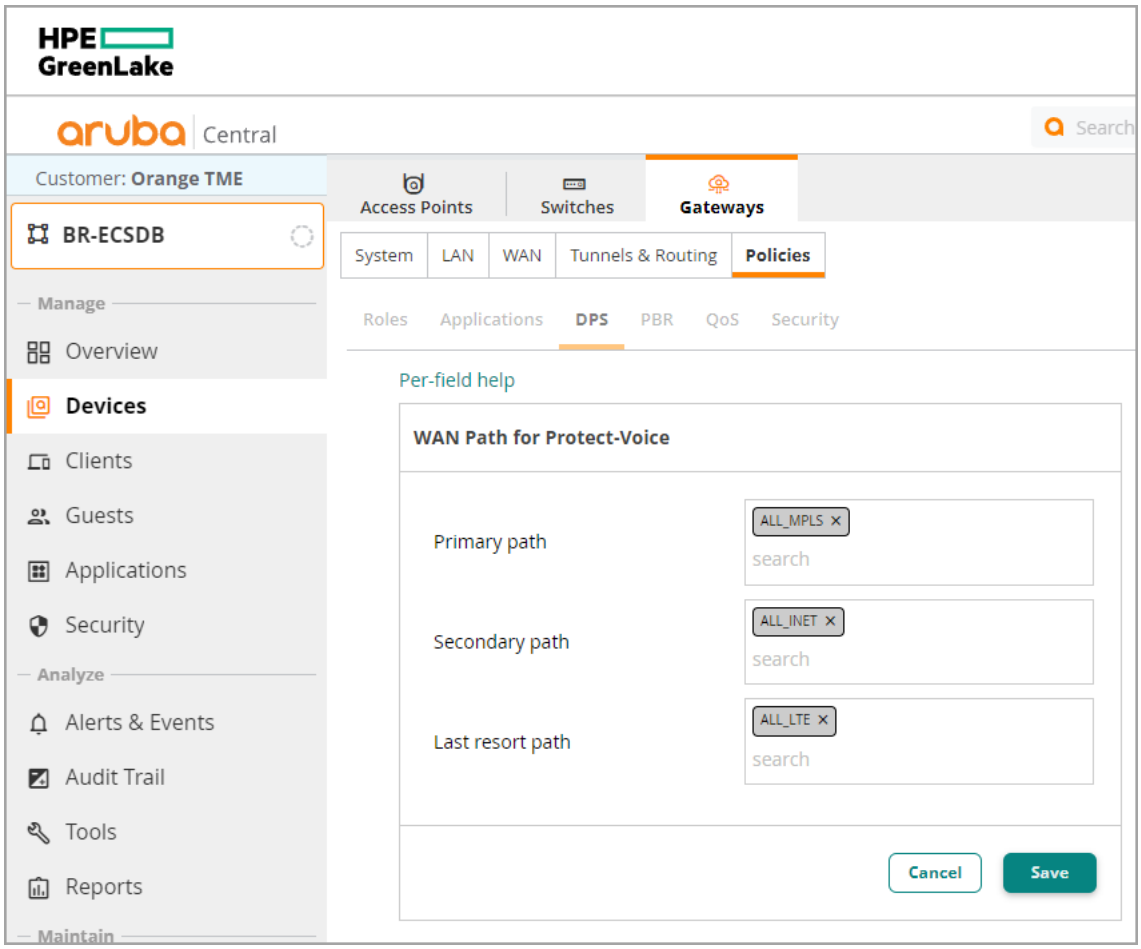


Figure 73: WAN Path 2

Configure SLA

Step 1 Select **Protect-Voice** and click the edit (pencil) icon next to SLA.

Step 2 In the **Select SLA for Protect-Voice** window, assign the following settings and click **Save**.

- **SLA:** *BestforVoice*
- **Loss Correction (FEC):** *Checked*
- **Loss % with FEC:** *5*
- **FEC Ratio:** *1:4*

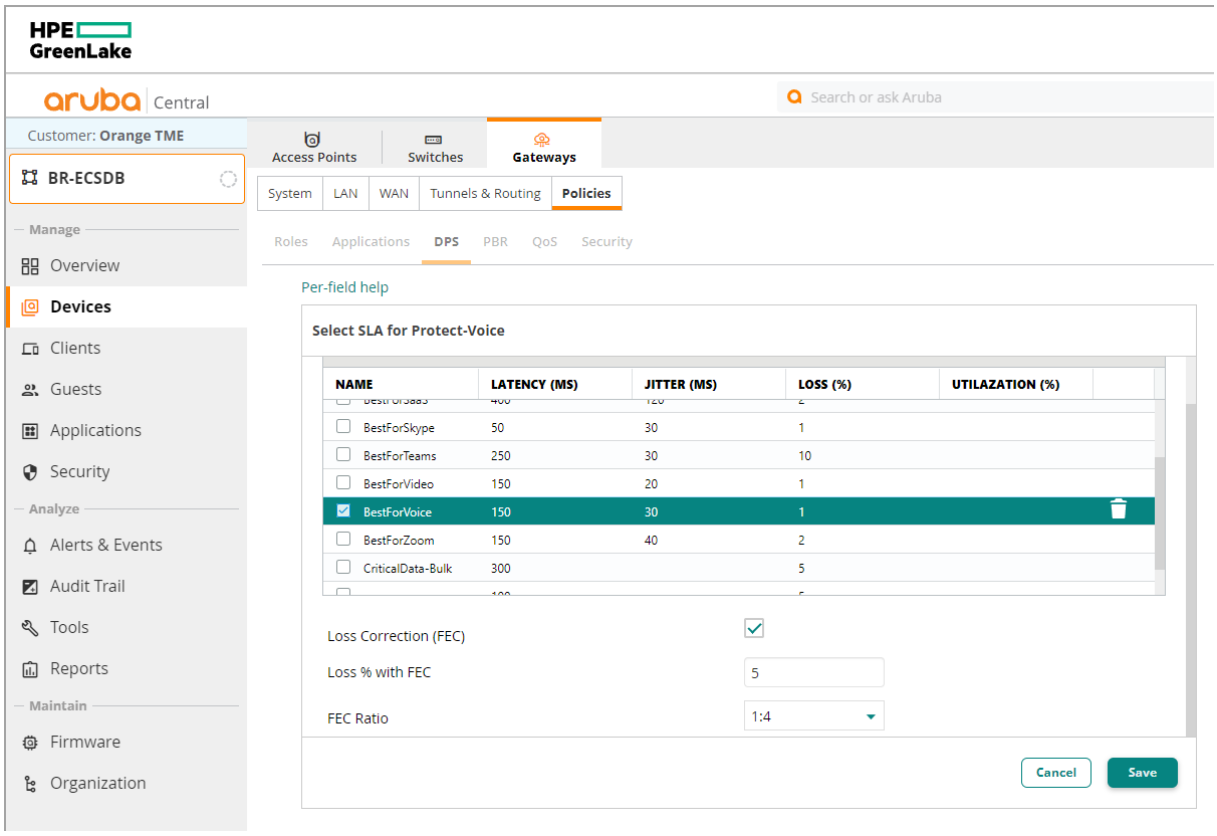


Figure 74: WAN Path 3

Step 3 Review the configuration and click **Save Settings**.

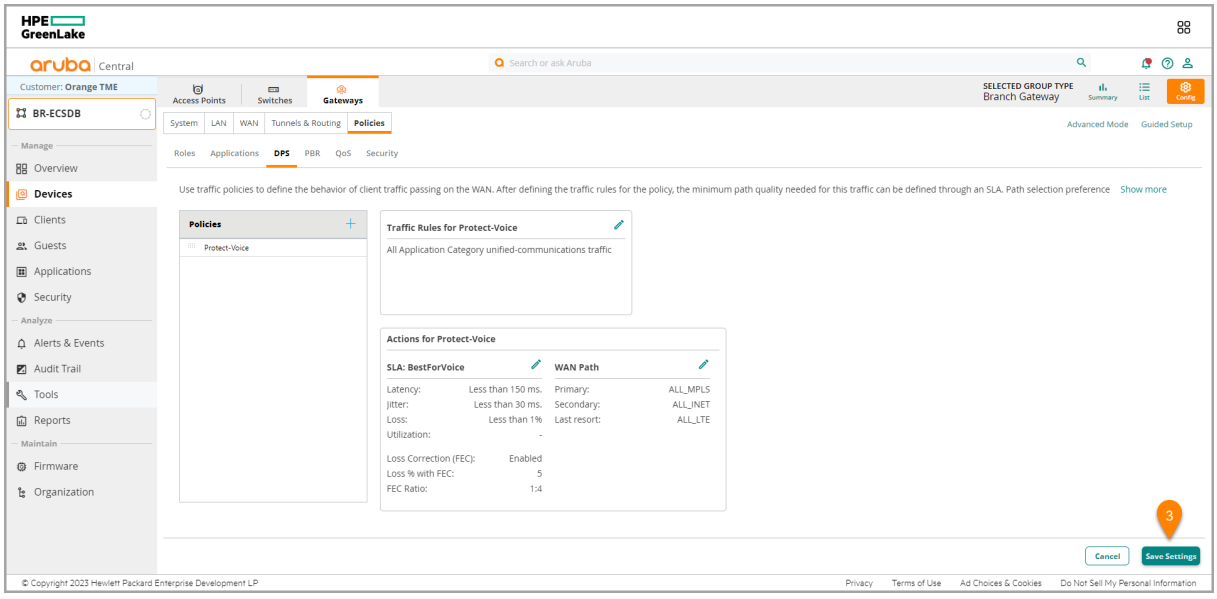


Figure 75: Review Policy DPS

Configure Policies for SAAS Express

The SAAS Express feature allows traffic routing from the best Internet egress point based on the performance of the Internet egress points for the given application. SAAS Express policies and configurations are unique to each environment, based on the organization's applications and performance needs. General guidance developing a SAAS Express policy can be found in the design section of the guide here. This section describes how to configure a SAAS Express policy to optimize Office 365 traffic.

NOTE:

While this example deployment does not utilize LTE connections, LTE is included in the below policy to facilitate the future addition of LTE uplinks without the need to modify the policy.

Additional policies should be created based on application requirements.

Create Policy

Step 1 Verify that the Gateway configuration mode is in **Basic Mode**.

Step 2 Select the **Policies** tab, then select **DPS**.

Step 3 Click the **+** (plus sign) to create a new SAAS Express policy.

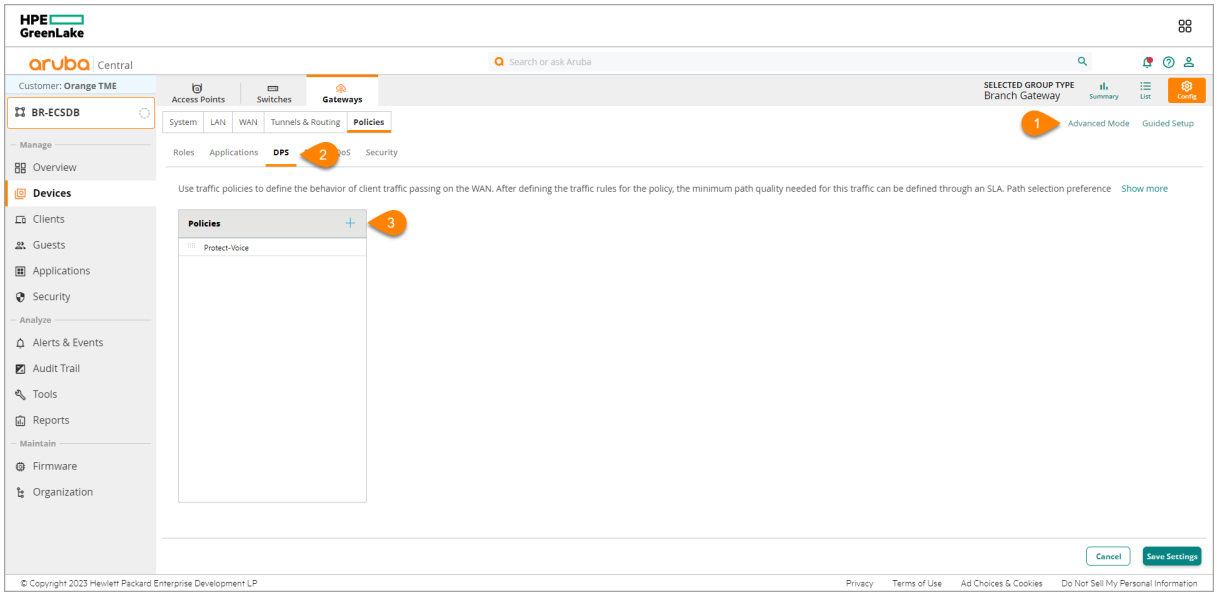


Figure 76: Create SAAS Policy

Step 4 In the **Create Policy** window, assign the following settings and click **Save**.

- **Policy Type:** *SAAS*
- **Application:** *office365*

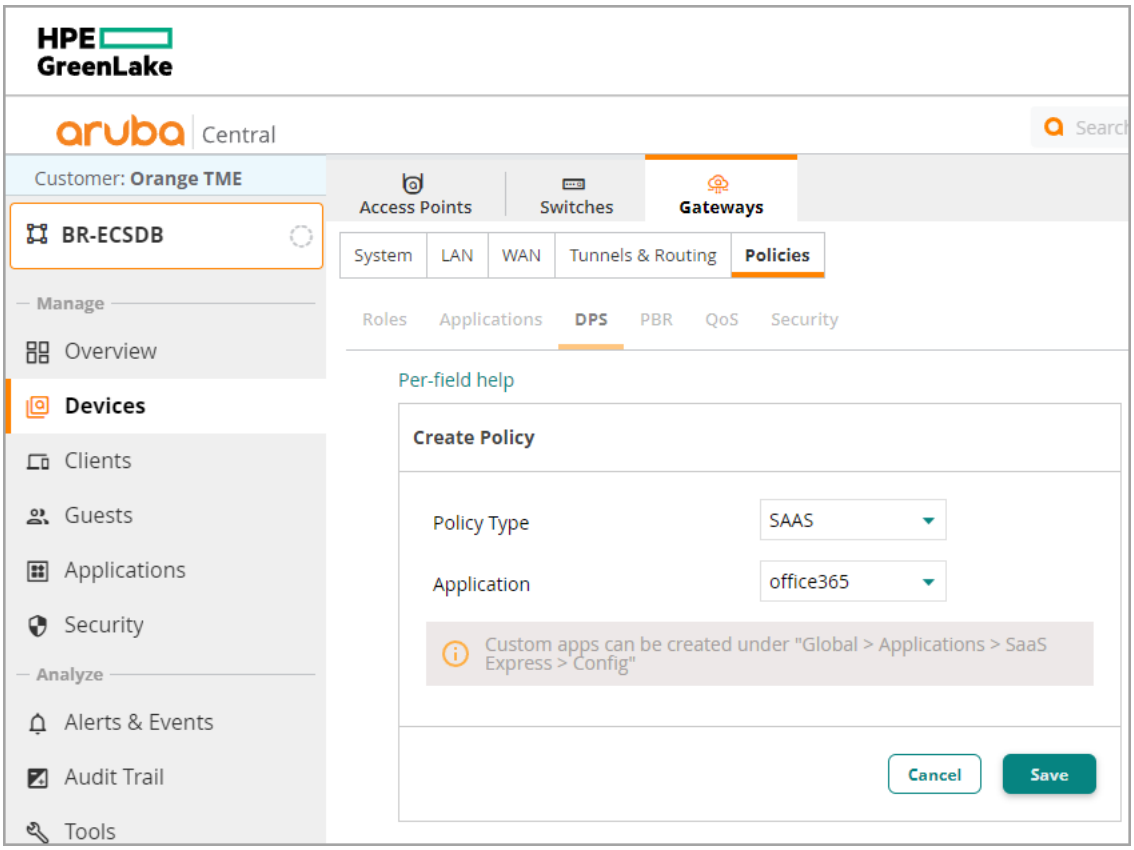


Figure 77: Create SAAS Policy

Configure SLA

Step 1 Select **saas_office365_wp** and click the edit (pencil) icon beside **SLA**.

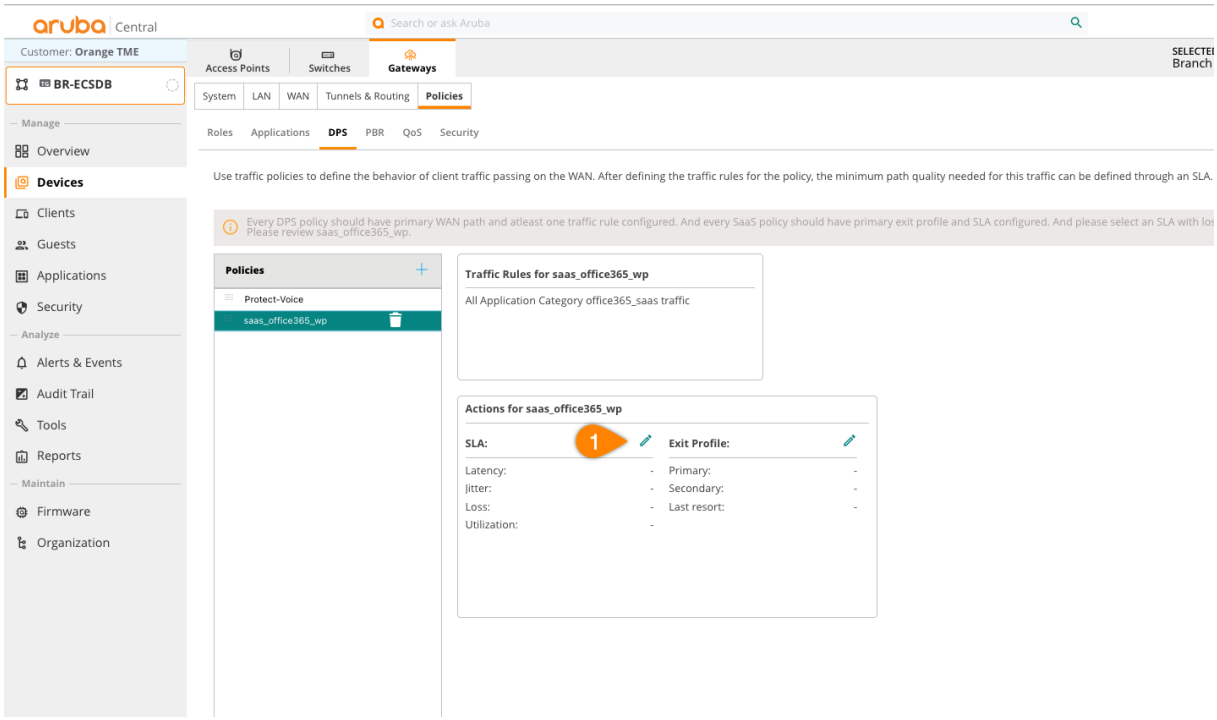


Figure 78: Create SAAS SLA Pencil

Step 2 In the **Select SLA for saas_office365_wp** window, select the **BestforSaaS** SLA.

Step 3 Click **Save**.

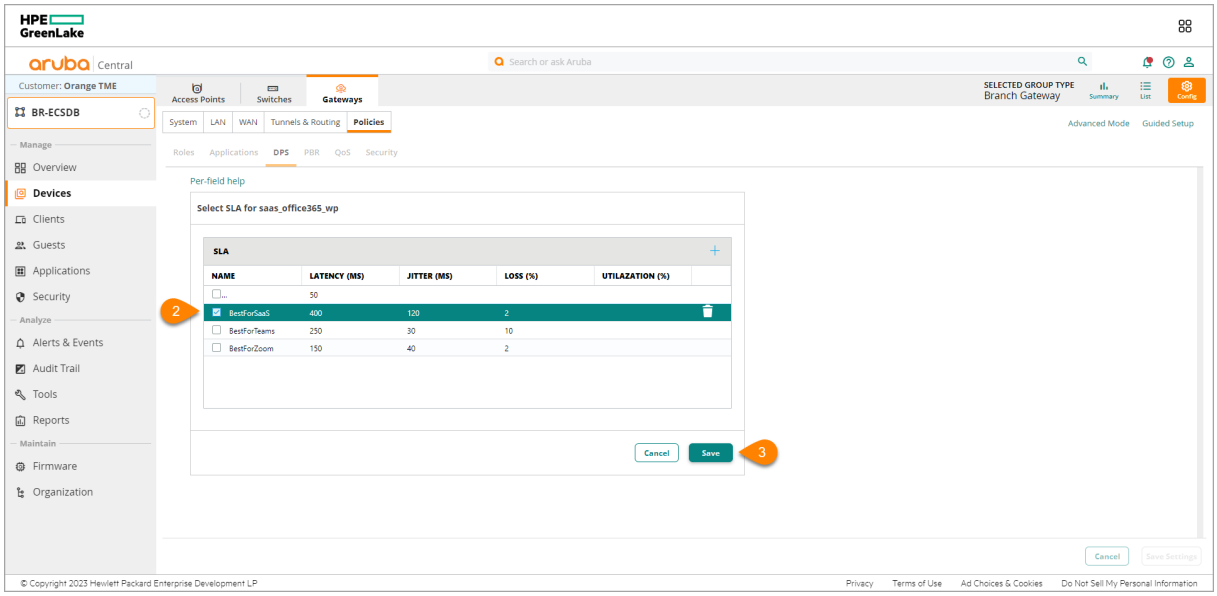


Figure 79: SAAS Express Create SLA

Configure Exit Profile

Step 1 Select **saas_office365_wp** and click the edit (pencil) icon beside **Exit Profile**.

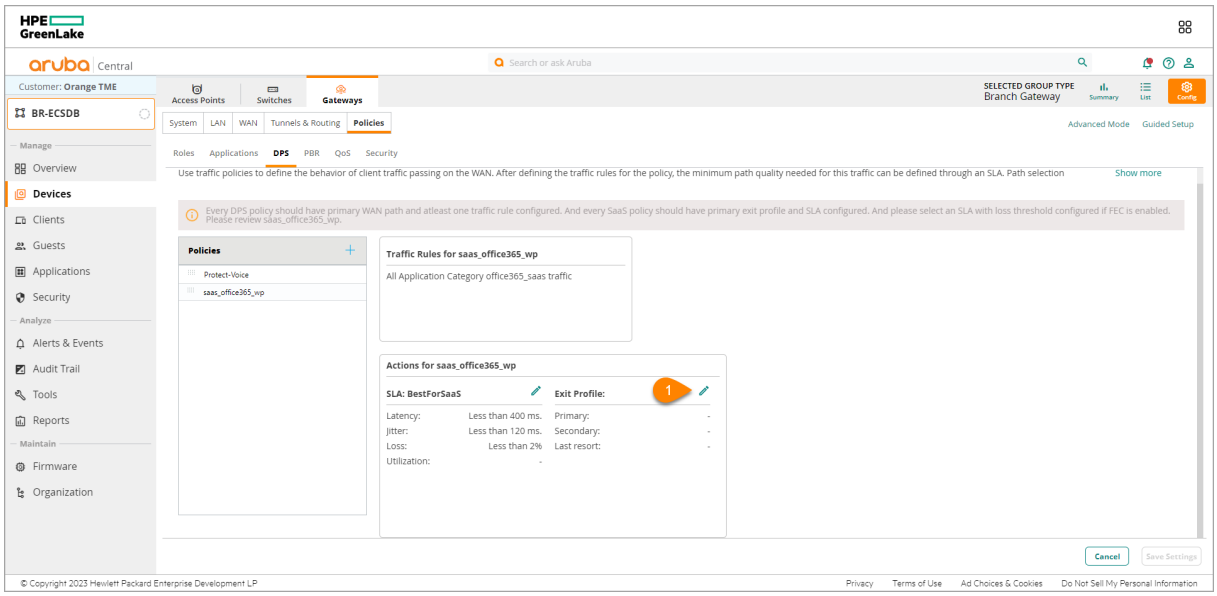


Figure 80: SAAS Express Create Exit Profile Pencil

Step 2 In the **Exit Profile for saas_office365_wp** window, select the default profile **BestForSaaS** and click **Save**.

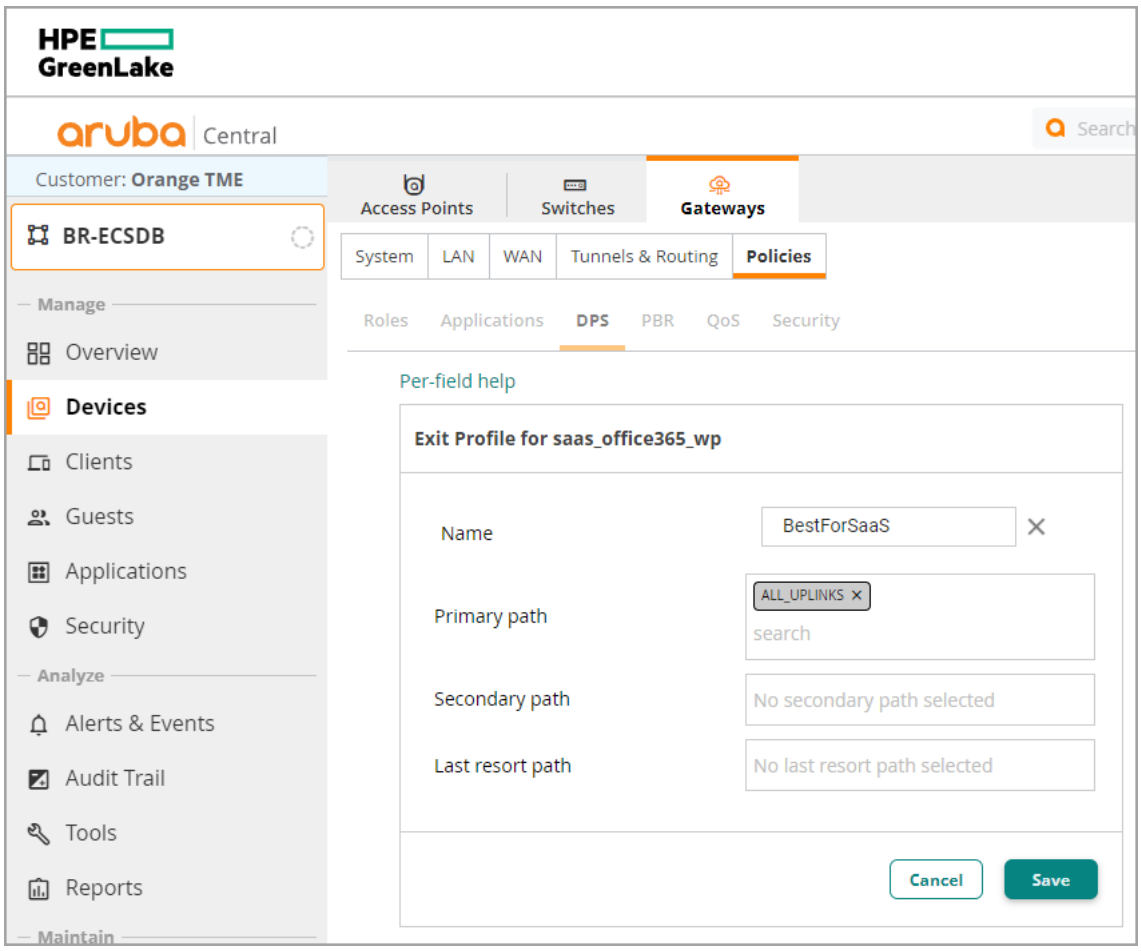


Figure 81: SAAS Express Create Exit Profile 1

Step 3 Review the configuration and click **Save Settings**.

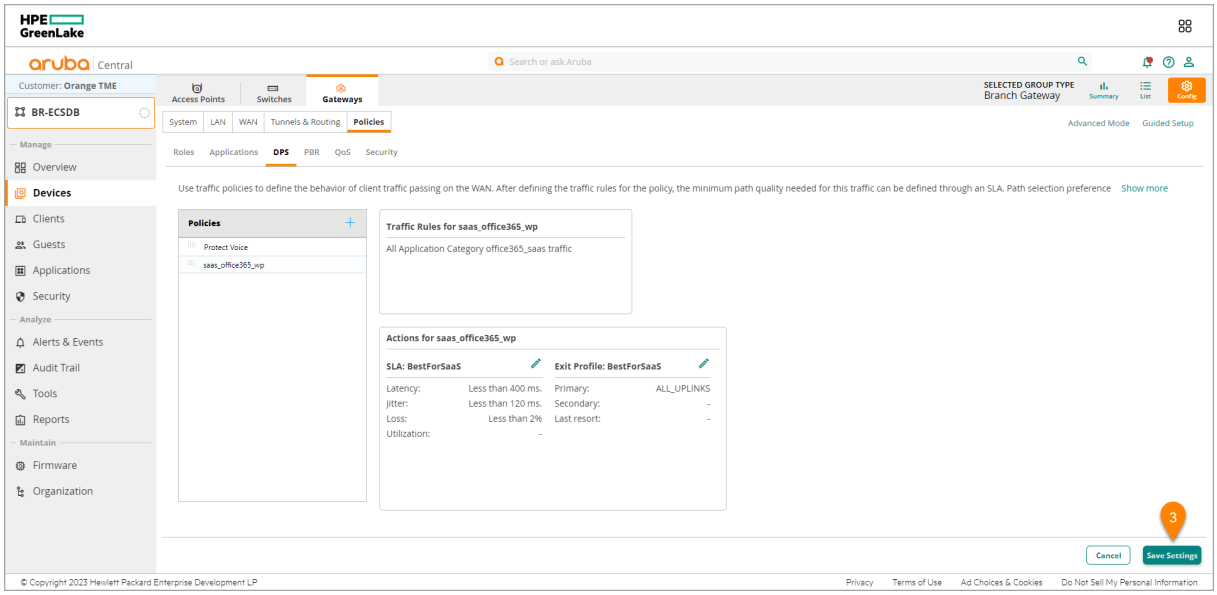


Figure 82: SAAS Express Review Configuration

Configure Branch Gateway at the Device Level

In this section the primary Miami branch gateway is configured. This gateways can be preconfigured offline, and obtain their configuration when connected to Central. Ensure that the Branch Gateways are assigned to the group and site as demonstrated in the Preparing to Deploy section.

Start the Branch Gateway Configuration

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

Step 2 In the dropdown, select the branch gateway group containing the devices.

Step 3 In the left navigation pane, in the **Manage** section, select **Devices** and select the **Gateways** tab.

Step 4 In the **Gateways** table, select the device to configure as the primary branch gateway.

Step 5 In the **Guided Setup** window, click **Cancel**, then click **Exit**.

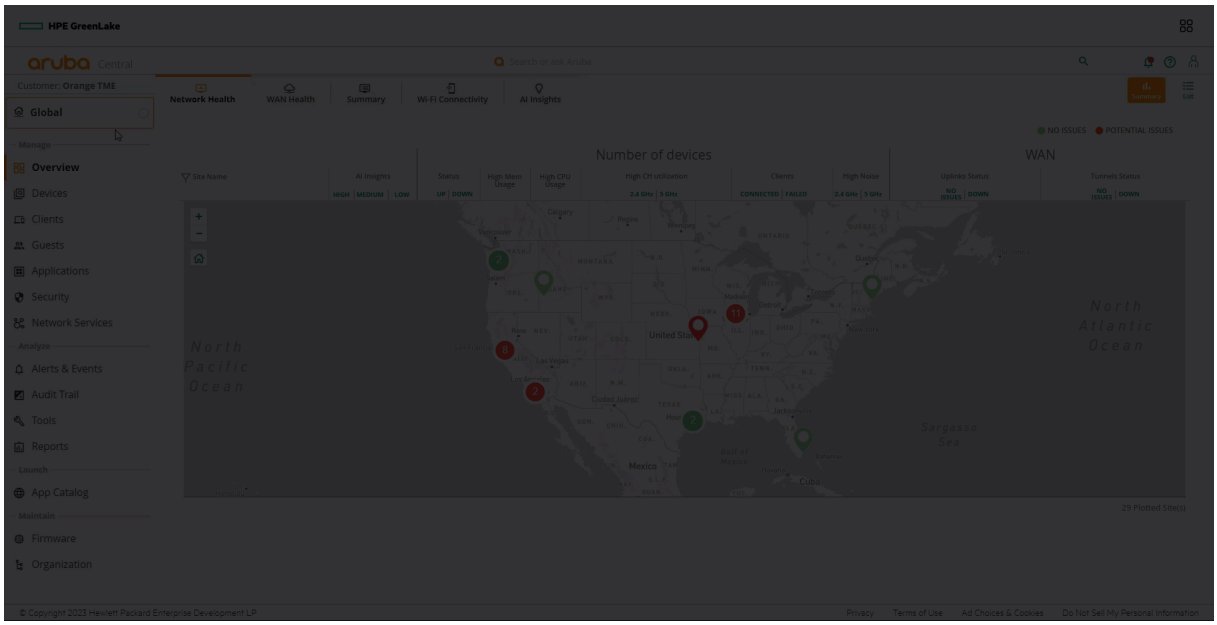


Figure 83: Starting branch configuration

Assign a Hostname

Step 1 Go to the Gateway configuration and verify that **Basic Mode** is enabled.

Step 2 Select **System** and **Hostname**.

Step 3 Click the basic info dropdown and enter the **Hostname**.

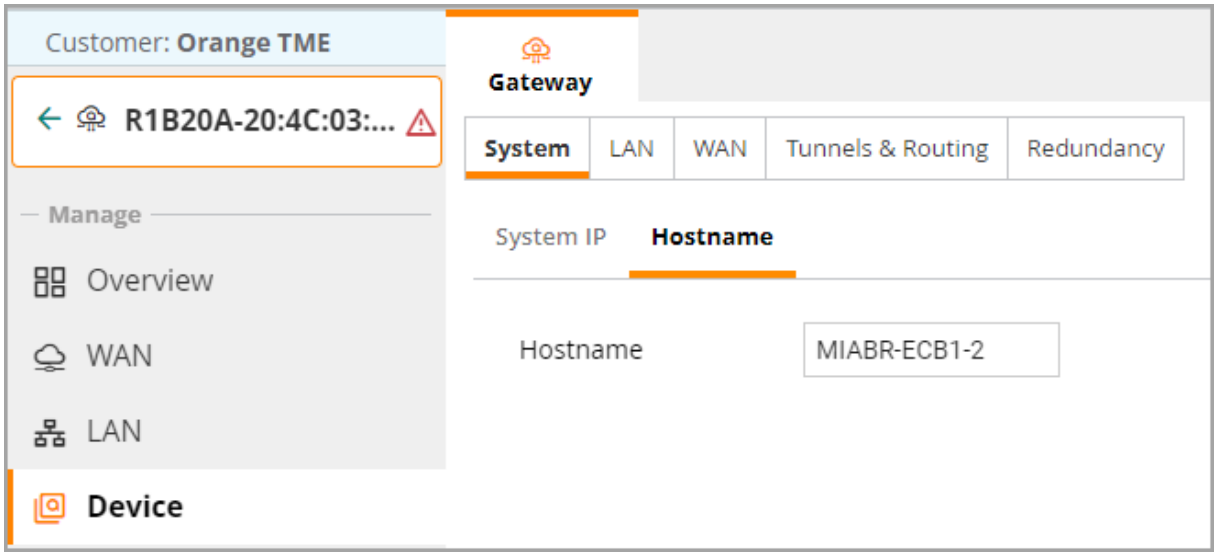


Figure 84: configure Hostname

Assign IP Addresses to the VLAN

Use this procedure to assign LAN VLAN IP addresses. The DHCP relay was preconfigured at the group level.

Step 1 Ensure that the Gateway configuration mode is in **Basic Mode**.

Step 2 Select the **LAN** tab and select **VLANs**.

Step 3 In the **VLANs** table, select one of the VLANs, and click the **edit** (pencil) icon.

Step 4 In the **VLAN** window, assign the following settings, then click **Save**. (These IP address are for the Miami site)

VLAN ID	Description	Network	Default Gateway (VRRP)	MIABR-ECB1-1 IP Address	MIABR-ECB1-2 IP Address
100	MGMT (Gateway System IP)	10.14.0.0	10.14.0.1	10.14.0.2	10.14.0.3
101	Employee	10.14.1.0/24	10.14.1.1	10.14.1.2	10.14.1.3
102	PRINTER	10.14.2.0	10.14.2.1	10.14.2.2	10.14.2.3
103	IoT (smart thermostats, smart access control, and meeting room kiosk.)	10.14.3.0/24	10.14.3.1	10.14.3.2	10.14.3.3
104	Guest	10.14.4.0	10.14.4.1	10.14.4.2	10.14.4.3.
105	Reject	10.14.5.0/24	10.14.5.1	10.14.5/.2	10.14.5.3
106	Critical	10.14.6.0	10.14.6.1	10.14.6.2	10.14.6.3
107	Quarantine	10.14.7.0/24	10.14.7.1	10.14.7.2	10.14.7.3
Sumr		10.14.0.0	——–	——–	——–

Step 5 Repeat step 3 and 4 for all VLANs in the table above.

Figure 85: Assigning an IP to VLAN

NOTE:

Clicking **Save Settings** after changing each VLAN IP is unnecessary. All VLAN IP changes can be saved at the same time.

Configure the MPLS VLAN

The MPLS VLAN must be configured statically with an IP address and gateway. The DNS is used for health checks on the interface.

Step 1 Ensure that the Gateway configuration mode is in **Basic Mode**.

Step 2 Go to **WAN** and select **WAN Details**.

Step 3 Scroll and select the **MPLS** VLAN. (Be sure the local gateway VLAN is selected.)

Step 4 Enter the **IPv4 Address**, **Gateway IP**, **Netmask**, and **DNS Servers** for the MPLS VLAN.

Step 5 Click **Save**.

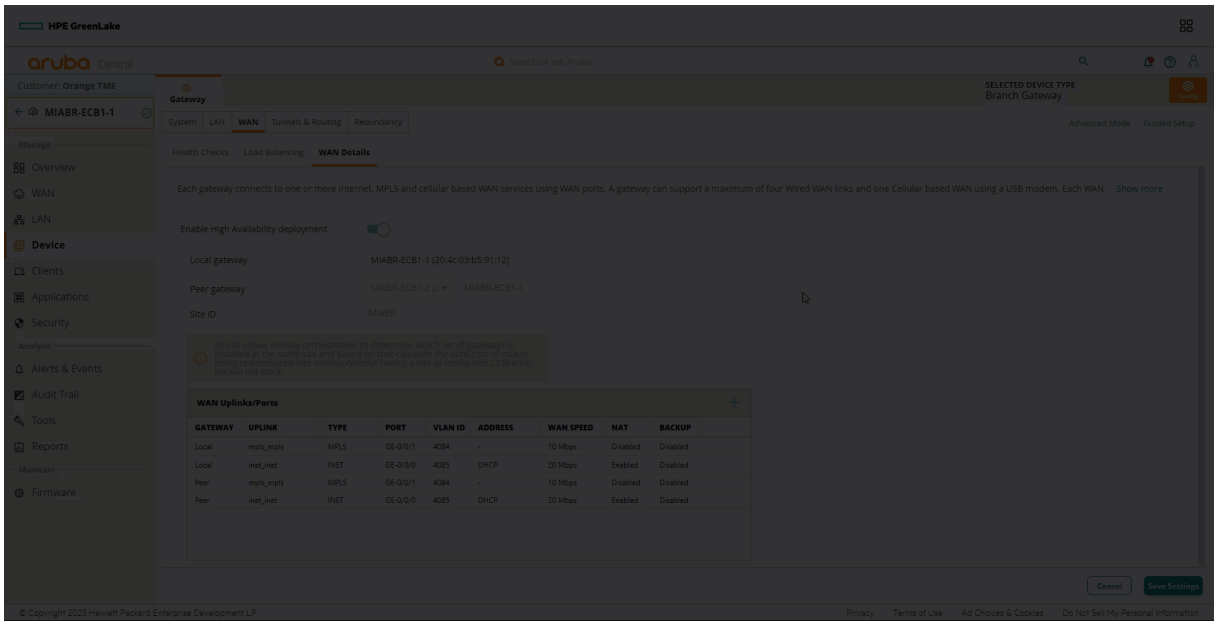


Figure 86: Configuring MPLS IP

Assign System IP Address

Use this procedure to select the Management VLAN as the system IP address.

Step 1 Ensure that the Gateway configuration mode is in **Advanced Mode**.

Step 2 In the **System** section, select **General** and expand **System IP Address**.

Step 3 In the dropdown, select **VLAN 100**.

Step 4 Click **Save Settings**.

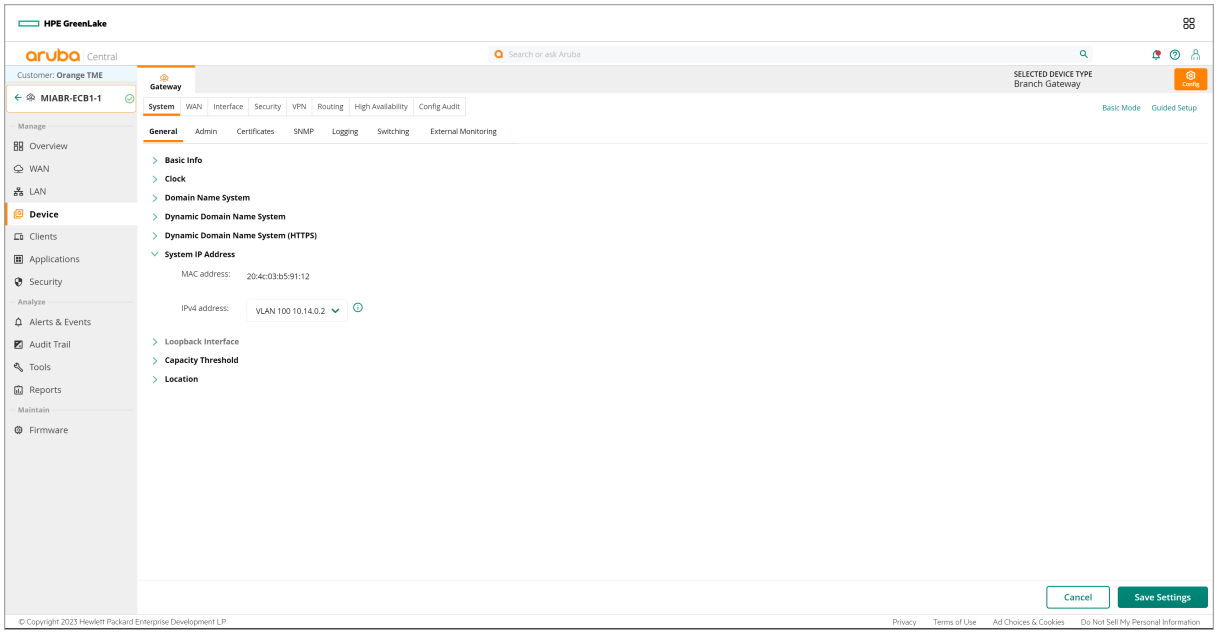


Figure 87: configure Hostname

Configure the LAN Redundancy

Step 1 Ensure that the Gateway configuration mode is in **Basic Mode**.

Step 2 In the **Redundancy** section, select **Preferred Cluster Leader**.

Step 3 Set the **Preferred Cluster Leader** to *MIABR-ECB1-1*.

Step 4 In the **Cluster Virtual Router IPs** table, click the **+** (plus sign).

Step 5 In the **VLAN ID** dropdown, select a LAN VLAN. The IP Address on Local and IP Address on Peer columns should autopopulate with the IP address values.

Step 6 In **Virtual IP** column, enter an IP address; for example, *10.14.0.1*.

Step 7 Repeat steps 3 and 4 for all user VLANs.

Step 8 Click **Save Settings**.

NOTE:

Ensure that **Automatic Clustering** and **Auto Site** are both enabled at the group level by selecting **BR-ECSDB > Select Advanced mode High Availability > Clusters**.

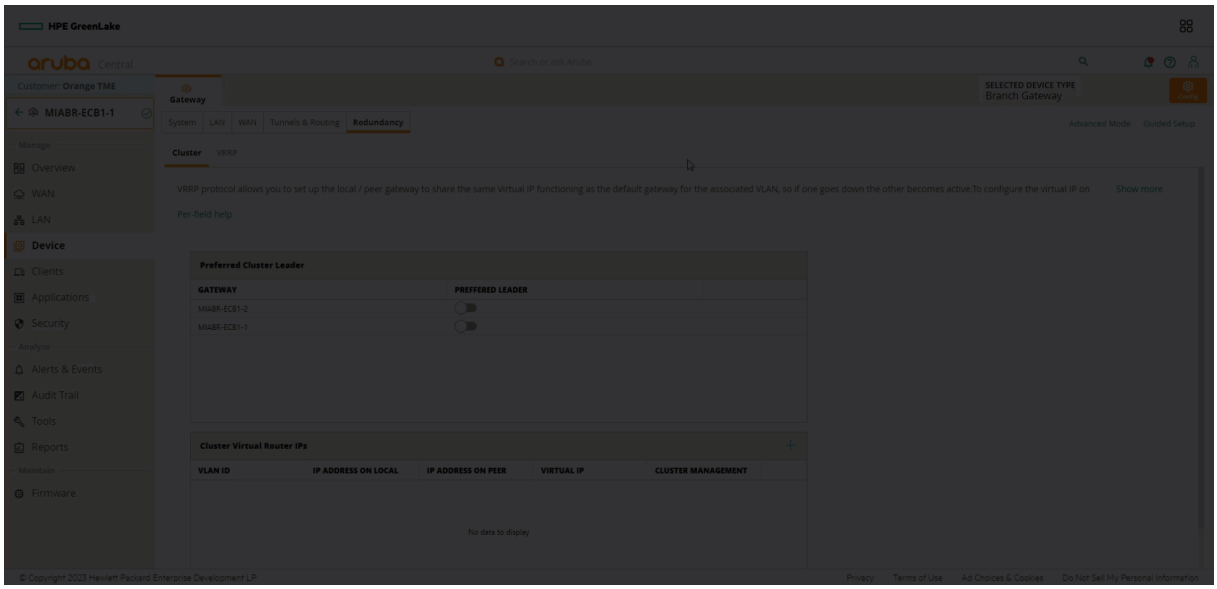


Figure 88: Clustering and VIP

Configure WAN Redundancy for Specific Deployments (Optional)

If only one of each WAN transport is available at a site with redundant gateways, WAN transports can be shared over the LAN. For example, the INET circuit terminates on one gateway and the MPLS circuit terminates on another gateway. As long as the gateways are reachable over the LAN, they can share the respective WAN transports. **This configuration is not used in this deployment because the sites have redundant connections for both INET and MPLS**. In this example, site RS01 is shown, with VLAN 100 used for connectivity between the gateways. Follow these steps to configure WAN redundancy.

Step 1 Verify that the Gateway configuration mode is in **Basic Mode**.

Step 2 Select the **WAN** tab, then select **WAN Details**.

Step 3 Turn on **Enable High Availability deployment**.

Step 4 In the **Peer Gateway** section, select the gateway at each site.

Step 5 Ensure that all the WAN transports appear in the **WAN Uplinks / Ports** table.

NOTE:

As long as both gateways have the same site-id the peer gateway and site ID are populated automatically and grayed out.

Branch Switch Configuration

The primary function of the switch in this branch deployment is to provide power and layer 2 access to wired devices and APs. Each branch deployment should have the same physical connectivity, to minimize differences in the template. OWL has the requirement for two different switch topologies. To accommodate OWL's requirements there will be two switch templates one for the collapsed core and one for the access switch. The majority of the configuration will be the same for both switches, the only difference will be in the uplinks/Downlinks. The following section will leverage templates to configure the switches.

Templates leverage variables to apply unique configuration to switches. Variables are created by using percent sign on both sides of a string in a configuration file. This string is defined by the admin, this string will become a column in a CSV file that will need an input from the admin. Below is an example of how variables are created/formatted.

```
interface Vlan 10
    ip address %VLAN_IP%
```

Switch Name	%VLAN_IP% Variable Input
Example-SW-01	10.0.0.2
Example-SW-02	10.0.0.2

In advanced cases templates might need to take advantage of other template functions such as If, and else statements. If statements are also delineated by a percent sign on both sides of a string. There are a few difference between an if statement variable and a single variable. The following guide will demonstrate how to use variables to allow for flexibility within a configuration file.

Stacking Switches Offline

Before connecting the uplinks to the switches should be stacked, use the following procedure to stack switches before they connect to central.

CAUTION:

Do not connect the switch to the gateway before it is stacked otherwise it will not be able to stack offline without factory reset.

Before starting this procedure check the following:

Step 1 Ensure switches are **AOS-CX 10.7 or Above**

Step 2 All switches are factory default.

Step 3 Switches in the stack are using the reserved auto-stacking ports. - 24 port switches auto stack ports : 25, 26 - 48 port switches auto stack ports: 49, 50

Step 4 Switches are connected in a ring topology.

Step 5 Console connection to the switch.

After going through the checklist above the switches are ready to be stacked.

Step 1 Press the mode button until the LED displays **STK** on the switch that will be the conductor, wait for the conductor to reboot.

Step 2 On the second switch press the LED until it displays **STK**. Wait for the second member to boot.

NOTE:

During stacking operation, the port LEDs are displayed in three different states:Flashing green - Indicates that the member is the conductor. Flashing orange - Indicates that the member is rebooting to join the stack or offline due to error condition. Solid green - Indicates that the member joined the stack and is operational.For more information on stacking LED states, refer to the Monitoring Guide.

Configure the Access Base Features

Use this procedure to configure the access switch base features. The base features include the host name, management user account, banner MOTD, NTP, DNS, TACACS, and AAA.

In the configuration template, perform the following steps:

Step 1 Configure the switch host name.

```
hostname %HOSTNAME%
```

Step 2 Configure the management user account.

```
user admin group administrators password plaintext <password>
```

NOTE:

There must be an admin user account for CLI access to the switch.

Step 3 Configure the login banner. The banner MOTD is normally used as a legal disclaimer to notify users logging into the network that only authorized access is allowed. Consult your own legal team to define the banner MOTD. An example is shown below.

```
banner motd $
************************************************************
NOTICE TO USERS
This is a private computer system and is the property of Aruba Networks. It is for
    authorized use only. Users (authorized or unauthorized) have no explicit or
    implicit expectation of privacy while connected to this system.
...
Unauthorized or improper use of this system may result in administrative
    disciplinary action and civil and criminal penalties. By continuing to use of
    this system, you indicate your awareness of and consent to these terms and
    conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions
    stated in this warning.
************************************************************
$
```

NOTE:

When setting the banner, a delineator breaks the switch from the MOTD context. In this example, the delineator is "$".

Step 4 Configure the NTP servers and time zone.

```
ntp server 10.2.120.98 iburst version 3
ntp server 10.2.120.99 iburst version 3
clock timezone us/pacific
```

Step 5 Configure the DNS servers and domain name.

```
ip dns host 10.2.120.98
ip dns host 10.2.120.99
ip dns domain-name Example.local
```

Configure the Access VLANs

In order to provide client devices with network connectivity, access switches must have the same VLANs as the branch gateways. The access switches also have an additional layer 3 interface for the management VLAN. IGMP, DHCP snooping, and ARP inspection are enabled.

IGMP snooping prevents hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. The feature provides layer 2 switches with a mechanism to prune multicast traffic from ports that do not contain an active multicast listener.

DHCP snooping is enabled globally and enabled for each VLAN to snoop DHCP packets. DHCP snooping prevents DHCP starvation attacks and rogue DHCP servers from servicing requests on the network.

ARP inspection is enabled under the VLAN, but does not take effect unless DHCP snooping also is enabled. ARP inspection stops man-in-the-middle attacks caused by ARP cache poisoning.

In the configuration template, assign the following configuration:

VLAN ID	Description
100	MGMT VLAN
101	Employee
102	Camera
103	IOT
104	Guest
105	Reject
106	Critical
107	Quarantine

Step 1 Configure DHCP snooping globally.

```
dhcpv4-snooping
```

Step 2 Configure the access VLANs, enable DHCP/IGMP snooping, and enable ARP inspection.

```
vlan 100
  name MGMT
  dhcpv4-snooping
  arp inspection
  ip igmp snooping enable
vlan 101
  name EMPLOYEE
  dhcpv4-snooping
  arp inspection
  ip igmp snooping enable
...
vlan 107
  name QUARANTINE
  dhcpv4-snooping
  arp inspection
  ip igmp snooping enable
```

Step 3 Configure the layer 3 interface VLAN.

```
interface vlan 100
  description MGMT
  ip dhcp
```

NOTE:

The IP DHCP command can only be applied to one VLAN interface. The template will fail to apply if multiply Interface VLANs have this configuration.

Configure Device Profiles

Device profiles detect APs dynamically and configure the attached port properly for device management and for tagging the bridged SSIDs. This assists network operators by eliminating manual configuration of ports to which APs are connected.

Device profiles are applied in three steps. First, configure the role to identify the AP, as well as the port tagging. Second, define the LLDP group, which uses LLDP to glean the device OUI to identify if the device is an Aruba AP. Last, associate the role and LLDP group in a device profile configuration.

NOTE:

This procedure can be skipped if ClearPass is used to authenticate Aruba APs.

On each access switch, perform the following steps:

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 100
  vlan trunk allowed 100,101,104-107
```

Step 2 Configure the LLDP group. Create the group and identify the Aruba 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 Aruba 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
```

Configure RADIUS

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

Access switches authenticate devices attempting to connect to the network. The two most common methods to authenticate users are 802.1x and MAC-based authentication. This design supports both methods, as well as dynamic authorization that 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 includes user roles for rejected clients and RADIUS failure scenarios.

On each access switch, perform the following steps:

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 local user roles, set the authentication mode, and set the VLAN.

```
port-access role EMPLOYEE
    reauth-period 120
    vlan access 101
port-access role  CAMERA
    reauth-period 120
    vlan access 102
port-access role  IOT
    reauth-period 120
    vlan access 103
port-access role GUEST
    reauth-period 120
    vlan access 104
port-access role REJECT
  reauth-period 120
  vlan access 105
port-access role CRITICAL
  reauth-period 120
  vlan access 106
port-access role QUARANTINE
    reauth-period 120
    vlan access 107
```

Step 4 Configure AAA authentication on the access ports. Set the client limit, configure 802.1x/MAC authentication, set the authentication order, and configure critical role and the rejection role. Adjust the EAPOL timeout, max requests, and max retry defaults.

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

NOTE:

EAPOL timeout: The amount of time the switch waits for EAP responses before identifying a packet as lost.**Max EAPOL requests**: The number of requests the interfaces can have at one time.**Max retries**: The number of times the switch tries to authenticate the device.

Configure Spanning Tree

Spanning tree is enabled globally on each access switch as a loop prevention mechanism. 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.

On each access switch, perform the following steps:

Step 1 Configure spanning tree globally and enable Rapid Per VLAN Spanning Tree for the access VLANs.

```
spanning-tree mode rpvst
spanning-tree
spanning-tree priority 8
spanning-tree vlan 100-107 priority 15
spanning-tree vlan 100-107
```

Step 2 Configure the supplemental spanning tree features.

```
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
```

Step 3 The final access port configuration should look like the following:

```
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
  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
```

Step 4 Repeat the full interface configuration for each access port. The Collapsed Core switch will be stacked so ensure the stacked interface ports are used e.g 2/1/1.

Configure Access Uplink Ports

Each access switch can have an uplink connection to both BGWs or to an aggregation switch. Each uplink connected to the gateway will be a trunk with the allowed VLANs of 100-107. If the access switch is connected to an aggregation switch the switch will use a lag with the same allowed VLAN's. The native VLAN for the uplink will be VLAN 100. Each uplink has DHCP Snooping trust allowed and ARP inspection trust enabled. The section below will demonstrate how to use If statements in the template to dictate the configuration the switch will receive.

CAUTION:

If DHCP Snooping and ARP inspection trust are not enabled, clients **cannot** get an IP address and connect to the network.

For the access switch template perform the following steps:

Step 1 Configure the uplink interface, then set the native VLAN and the allowed VLANs on the trunk.

```
interface 1/1/24
  description Uplink_GW
  no shutdown
  no routing
  vlan trunk native 100
  vlan trunk allowed 100-107
```

Step 2 Configure ARP inspection trust and DHCP snooping trust.

```
interface 1/1/23
  description Uplink_GW
  no shutdown
  no routing
  vlan trunk native 100
  vlan trunk allowed 100-107
  arp inspection trust
  dhcpv4-snooping trust
```

CAUTION:

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

Step 3 Configure if statement around uplink ports.

```
%if SITE_HAS_AGG=n%
interface 1/1/23
  description Uplink_to_BGW
  no shutdown
  no routing
  vlan trunk native 100
  vlan trunk allowed 100-107
  arp inspection trust
  dhcpv4-snooping trust
interface 1/1/24
  description Uplink_to_BGW
  no shutdown
  no routing
  vlan trunk native 100
  vlan trunk allowed 100-107
  arp inspection trust
  dhcpv4-snooping trust
%endif%
```

Step 5 Configure the LAG.

```
interface lag 1
    no shutdown
    no routing
    vlan trunk native 100
    vlan trunk allowed 100-107
    lacp mode active
    lacp fallback-static
    arp inspection trust
    dhcpv4-snooping trust
```

Step 6 Configure the if statement around the LAG and uplinks

```
%if SITE_HAS_AGG=y%
interface lag 1
    no shutdown
    no routing
    vlan trunk native 100
    vlan trunk allowed 100-107
    lacp mode active
    lacp fallback-static
    arp inspection trust
    dhcpv4-snooping trust
%endif%

%if SITE_HAS_AGG=y%
interface 1/1/23
    no shutdown
    description Uplink_to_AGG
    lag 1
interface 1/1/24
    no shutdown
    description Uplink_to_AGG
    lag 1
%endif%
```

Configure Collapsed Core Uplink Ports

On each access switch, perform the following steps:

Step 1 Configure the LAG's

```
interface lag 1
    no shutdown
    no routing
    vlan trunk native 100
    vlan trunk allowed 100-107
    lacp mode active
    lacp fallback-static
    arp inspection trust
    dhcpv4-snooping trust
interface lag 2
    no shutdown
    no routing
    vlan trunk native 100
    vlan trunk allowed 100-107
    lacp mode active
    lacp fallback-static
    arp inspection trust
    dhcpv4-snooping trust
interface lag 3
    no shutdown
    no routing
    vlan trunk native 100
    vlan trunk allowed 100-107
    lacp mode active
    lacp fallback-static
    arp inspection trust
    dhcpv4-snooping trust
interface lag 4
    no shutdown
    no routing
    vlan trunk native 100
    vlan trunk allowed 100-107
    lacp mode active
    lacp fallback-static
    arp inspection trust
    dhcpv4-snooping trust
```

Step 2 Configure the uplink interfaces, then set the native VLAN and the allowed VLANs on the trunk.

```
interface 1/1/23
  description Uplink_GW
  no shutdown
  no routing
  lag 1
interface 1/1/24
  description Uplink_GW
  no shutdown
  no routing
  lag 1
interface 2/1/23
  description Uplink_GW
  no shutdown
  no routing
  lag 2
interface 2/1/24
  description Uplink_GW
  no shutdown
  no routing
  lag 2
```

Step 3 Configure downlinks to access switches

```
interface 1/1/1
  description Uplink_GW
  no shutdown
  no routing
  lag 3
interface 1/1/2
  description Uplink_GW
  no shutdown
  no routing
  lag 4
interface 2/1/1
  description Uplink_GW
  no shutdown
  no routing
  lag 3
interface 2/1/2
  description Uplink_GW
  no shutdown
  no routing
  lag 4
```

Applying the Template Configuration

After the template configuration is created, there should be two configuration files one for the access, and one collapsed core file. The only difference being the uplinks and the stacking ports configuration for the Collapsed core. This procedure walks through steps to get the configuration into Central.

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

Step 2 Go to **Global > Groups**. In the **Groups** list, select **BR-ECSDB**.

Step 3 On the **Switches List** page at the top right, click **Config**.

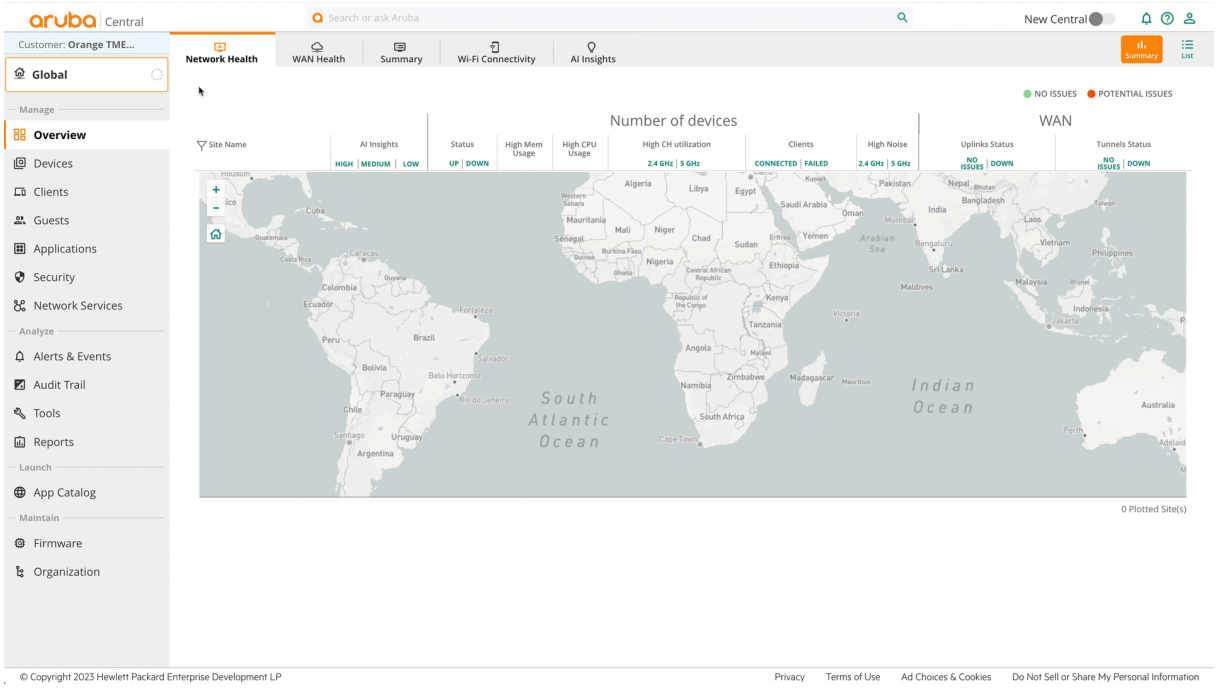


Figure 89: nav_to_sw_group_template_config

Step 4 On the **Switches Template** section at the top right, click the **+** (plus sign) symbol.

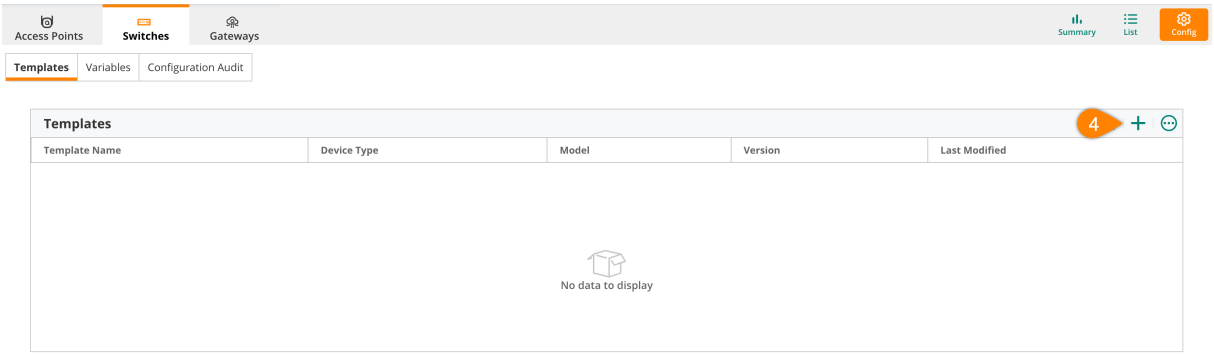


Figure 90: Click Template Config

Step 5 On the **Add Template** window in the **Basic Info** section, assign the following settings, then click **Next**.

- **Template Name:** *BR-ACC*
- **Device Type:** *Aruba CX*
- **Model:** *6200*
- **Part Name:** *All*
- **Version:** *All*

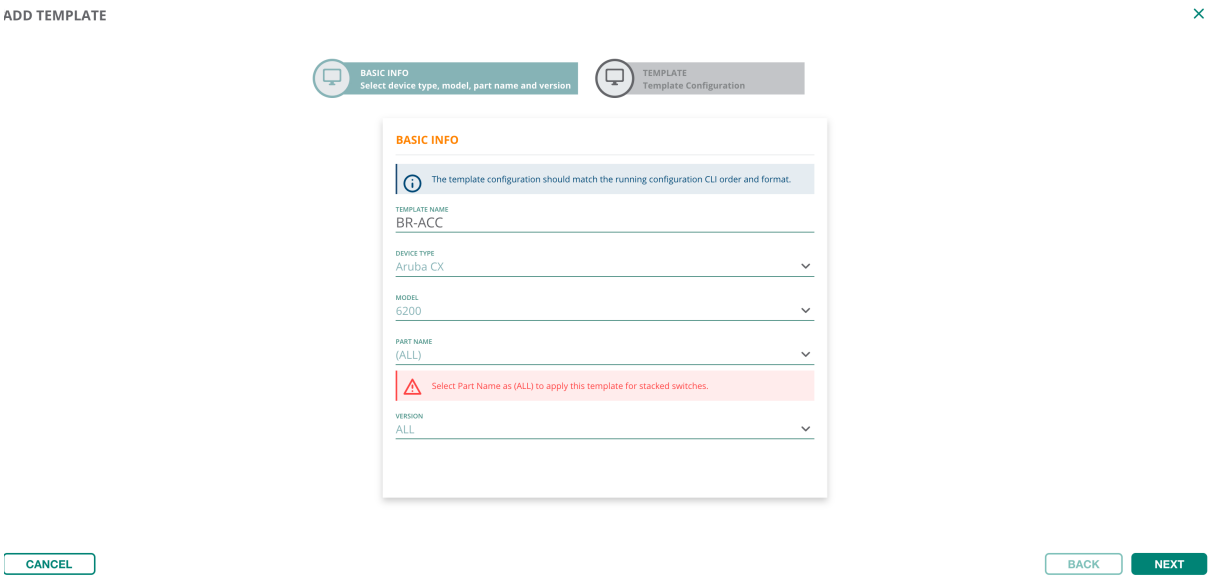


Figure 91: Low_Traffic_site_template_creation-1318605-1321132

Step 6 In the **Edit Template** section, paste the **access configuration** in the box, then click **SAVE**.

CAUTION:

All variables must be enclosed with percent “%” symbols.

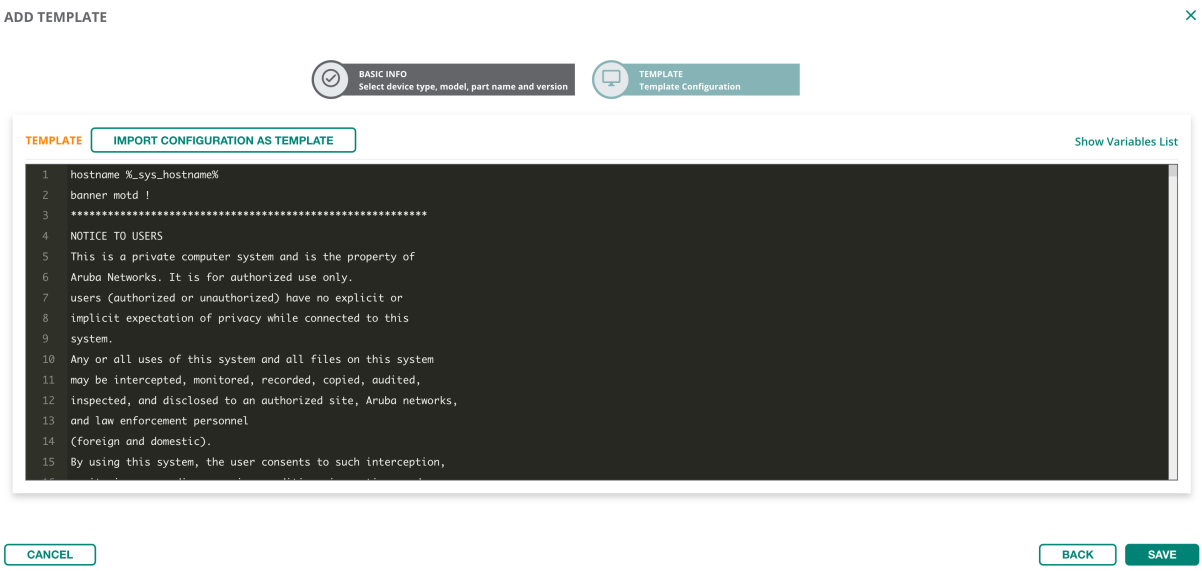


Figure 92: 2023-11-29_20-34-17

Step 7 Repeat steps 4-6 for the collapsed core with the following details - **Template Name:** *BR-AGG* - **Device Type:** *Aruba CX* - **Model:** *6300* - **Part Name:** *All* - **Version:** *All*

Upload the Access Switch Variables

Use this procedure to upload the variables for the access switches into Central.

Step 1 On the **Devices > Switches** page, select the **Variables** tab, then click **DOWNLOAD SAMPLE VARIABLES FILES**.

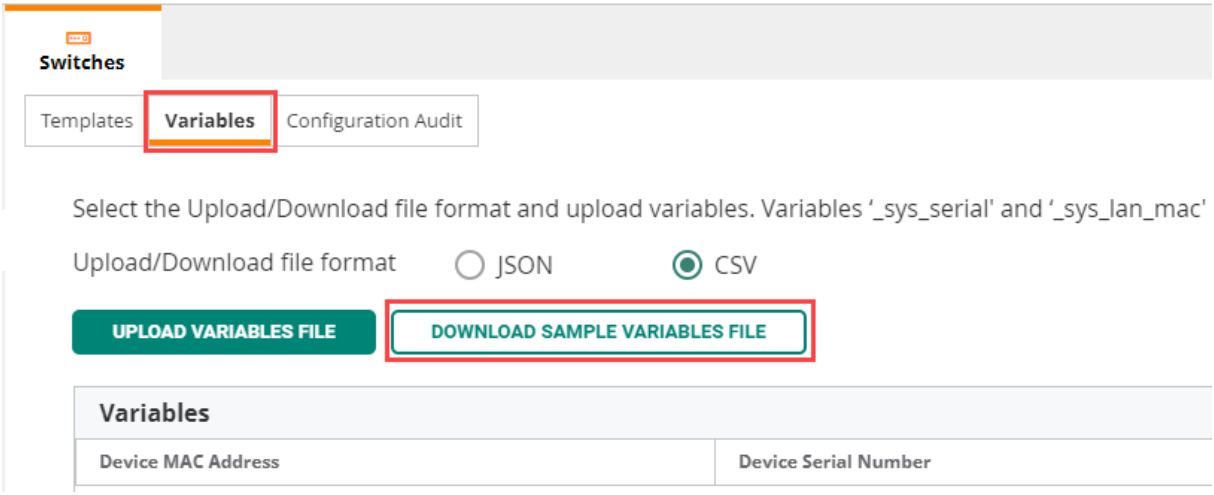


Figure 93: Download Variables

Step 2 Open the CSV file in an editor, enter the proper value for each variable, and enter **Y** in the modified column. **Save** the file on your computer.

Switch Serial	Switch Mac	%HOSTNAME% Variable Input	%if SITE_HAS_AGG% Variable	Modified
SG1AKW50LJ	44:5b:ed:37:62:c0	HOUBR-ECB-1CR1	n	Y
TW14KNK051	38:10:f0:25:6f:c0	MIABR-ECB1-CR1	n	Y
SG12KN5052	8c:85:c1:5d:c1:40	SFOBR-ECB1-CR1	—-	Y
SG12KN505R	8c:85:c1:60:5f:00	SFOBR-ECB1-CR1	—-	Y
SG0BKW506D	8c:85:c1:50:e0:00	SFOBR-CR1-AC1	y	Y
SG0BKW5070	8c:85:c1:50:93:c0	SFOBR-CR1-AC1	y	Y

CAUTION:

Change the **modified** column to **Y** for each device. For the Aggregation switch leave the variables that don't apply blank

Step 3 On the **Variables** tab, click **Upload Variables Files**, find the updated CSV file on your computer, then click **Open**.

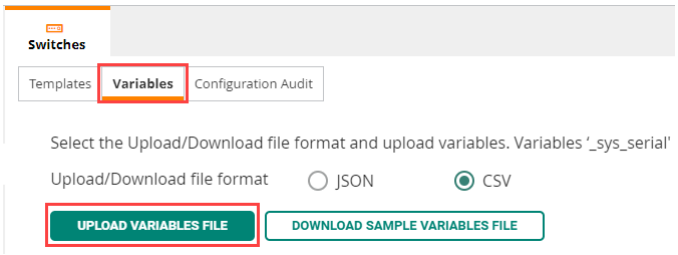


Figure 94: Upload Variables

Stacking Collapsed Core Switches Offline

Before connecting the uplinks to the collapsed core, they should be stacked. Use the following procedure to stack switches before they connect to central. For the Houston and Miami sites the switches do not need to be stacked so they can be connected directly to the branch gateways.

CAUTION:

Do not connect the switch to the gateway before it is stacked otherwise it will not be able to stack offline without factory reset.

Before starting this procedure check the following:

1. Ensure switches are **AOS-CX 10.7 or Above**
2. All switches are factory default.
3. Switches in the stack are using the reserved auto-stacking ports.

4. Switches are connected in a ring topology.
5. Console connection to the switch.

After going through the checklist above the switches are ready to be stacked.

1. Press the mode button until the LED displays **STK** on the switch that will be the conductor, wait for the conductor to reboot.
2. On the second switch press the LED until it displays **STK**. Wait for the second member to boot.

NOTE:

During stacking operation, the port LEDs are displayed in three different states:Flashing green - Indicates that the member is the conductor. Flashing orange - Indicates that the member is rebooting to join the stack or offline due to error condition. Solid green - Indicates that the member joined the stack and is operational.For more information on stacking LED states, refer to the Monitoring Guide.

###

3. Connect the uplinks to the branch gateway.
4. Verify all switches are online and stacked. Go to **Devices > Switches > List** and verify that the switches are **In sync**.

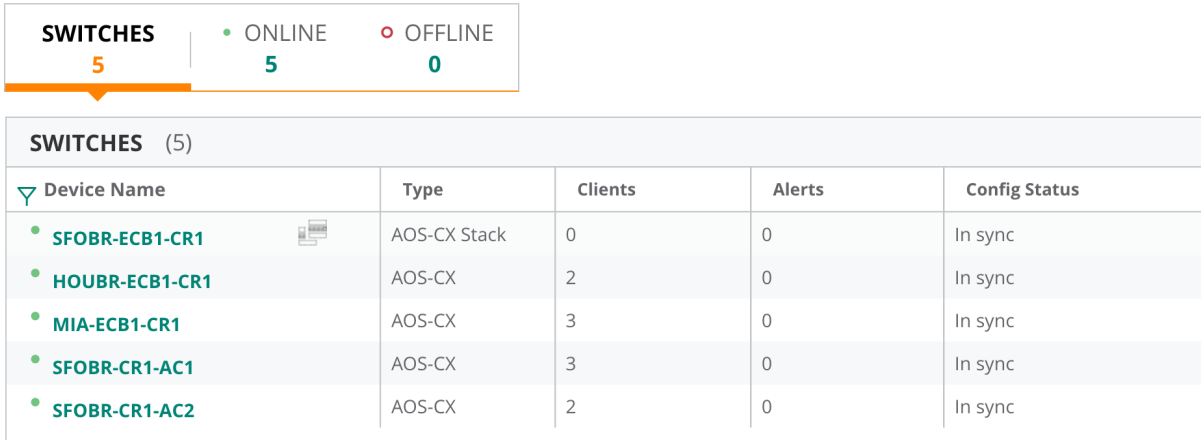


Figure 95: 2023-11-29_21-09-09

Aruba Branch Access Point (AP) Configuration

This section describes the creation and configuration of the AP group to support wireless service in the branches.

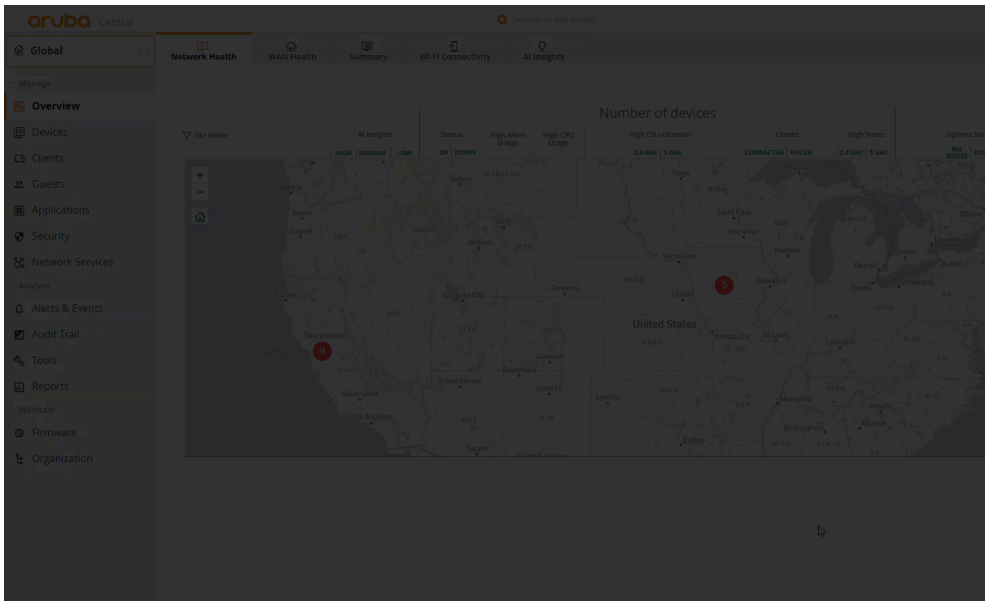
Open the AP Group

This procedure locates and opens the AP group

Step 1 In the **Global** dropdown, search or select the group you created in the previous section.

Step 2 In the left navigation pane, in the **Manage** section, select **Devices**.

Step 3 Select the **AP** tab, then click the gear icon in the upper right corner.



Step 4 Click **Cancel**, then click **Exit**.

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. 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 From the **Access Point** page, select the **WLANs** tab. On the bottom left of the **Wireless SSIDs** table, click **(+) Add SSID**.

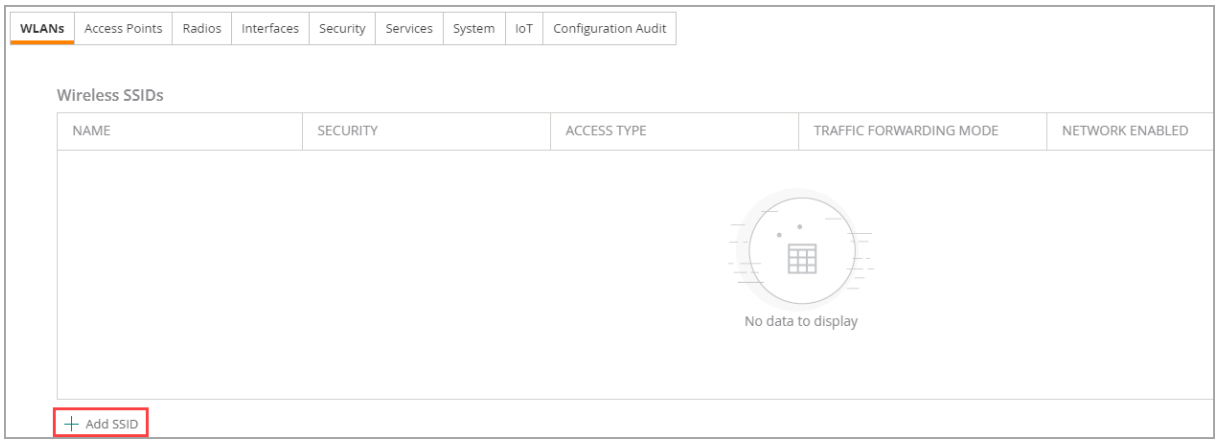


Figure 96: Add SSID

Step 2 In the **Create a New Network** page on the **General** tab, expand **Advance Settings**.

Step 3 Configure SSID Name: **EXAMPLE-CORP**

Step 4 Click the **+** (plus sign) to expand **Broadcast/Multicast**.

- Change the **Broadcast filtering** to *All*.
- Enable **DMO**, and set the **DMO Client Threshold** to *40*.

NOTE:

A **DMO Client Threshold** of 40 is the recommended initial value and should be adjusted based on actual performance.

Step 5 Click the **+** (plus sign) to expand **Transmit Rates (Legacy Only)**.

- Set **2.4 GHz** to **Min:** *5* and **Max:** *54*.
- Set **5 GHz** to **Min:** *18* and **Max:** *54*.

Step 6 Click **Next**

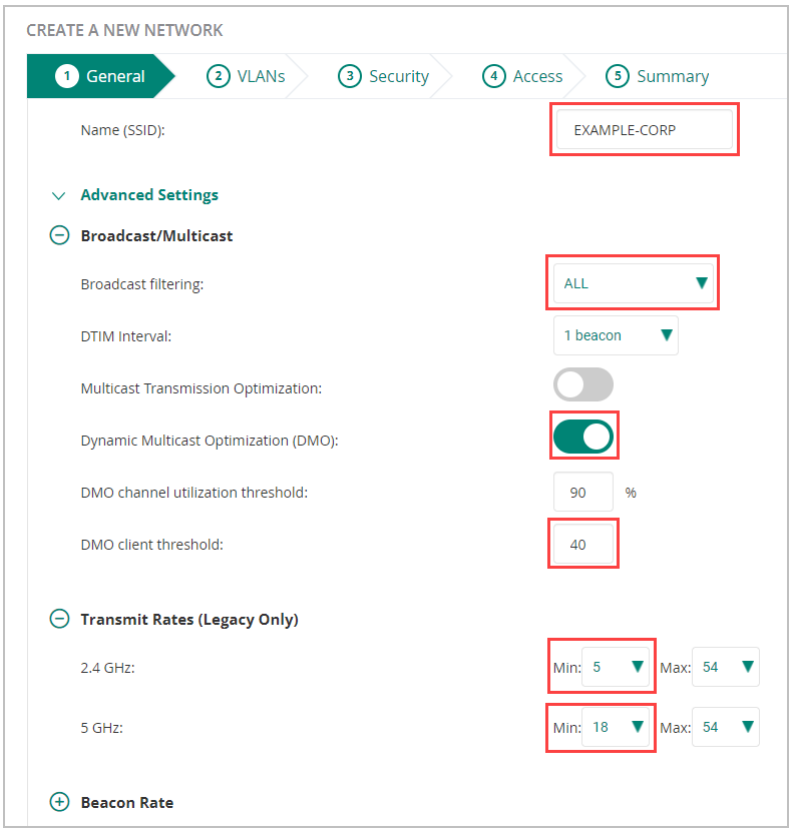


Figure 97: General SSID Configuration

Configure SSID VLAN

On the **VLANs** tab, assign the following settings:

Step 1 Set the **Traffic Forwarding Mode** to *Tunnel*.

Step 2 Set the **Primary Gateway Cluster:** *UI-BGW-01-AUTO site cluster*. Leave the **Secondary Gateway Cluster:** *None (default)*.

Step 3 Set the **Client VLAN Assignment:** *Static (default)*.

Step 4 Select the **Employee VLAN (101)**.

Step 5 Click **Next**.

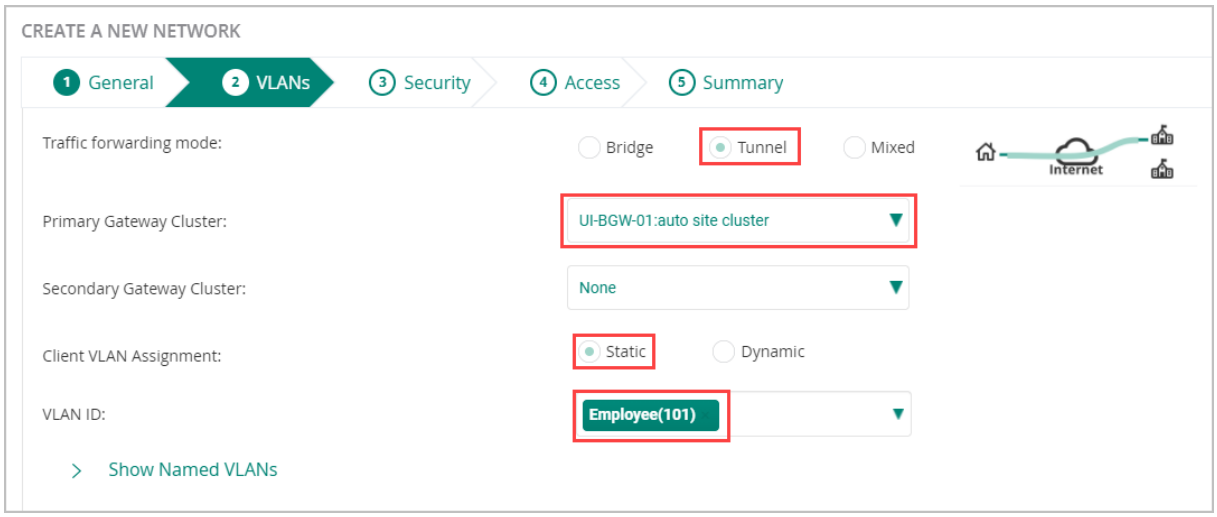


Figure 98: Configuring VLAN

NOTE:

When tunneling to the branch gateway, ensure the VLAN line protocol is up, by verifying that the VLAN is trunked or **forced operational state up** is configured on the branch gateway

Configure SSID Security Settings

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

On the **Security** tab, assign the following settings:

Step 1 Security Level: *Slide to Enterprise*

Step 2 Key Management: *WPA3 Enterprise CMM 128*

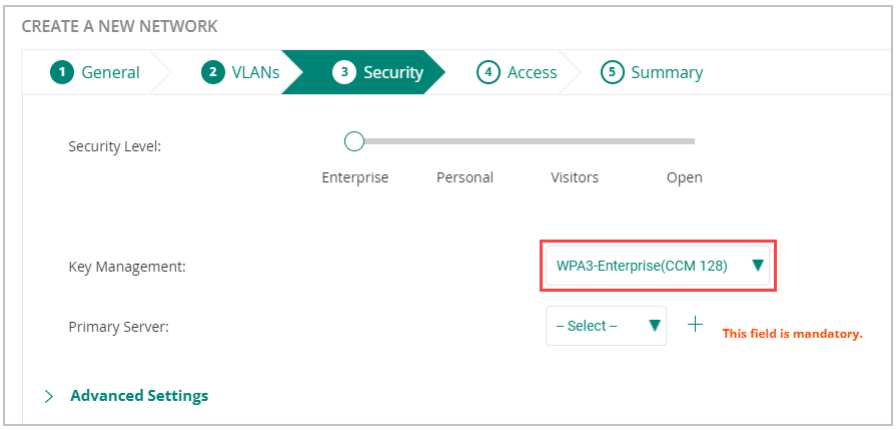


Figure 99: Enabling dot1x

Step 3 On the **Security** tab, click the **+** (plus sign) next to **Primary Server**.

Step 4 In the **New Server** window, assign the following settings, then click **OK**.

- Set **Server Type** to *RADIUS*.
- Name the server *cppm-01*
- Enter the RADIUS **IP Address:** *10.2.120.94*
- Enter the **Shared Key:** *shared key*

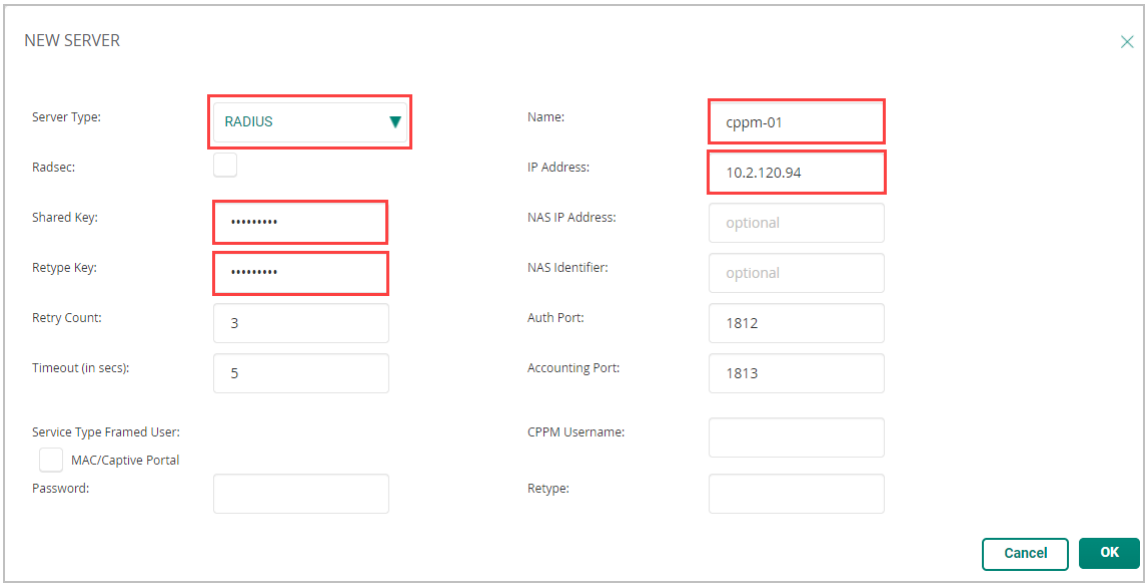


Figure 100: Adding Radius Server

NOTE:

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

Step 6 Repeat the two previous steps for the second CPPM server using the appropriate values.

Step 7 Enable **Load Balancing** by selecting the toggle.

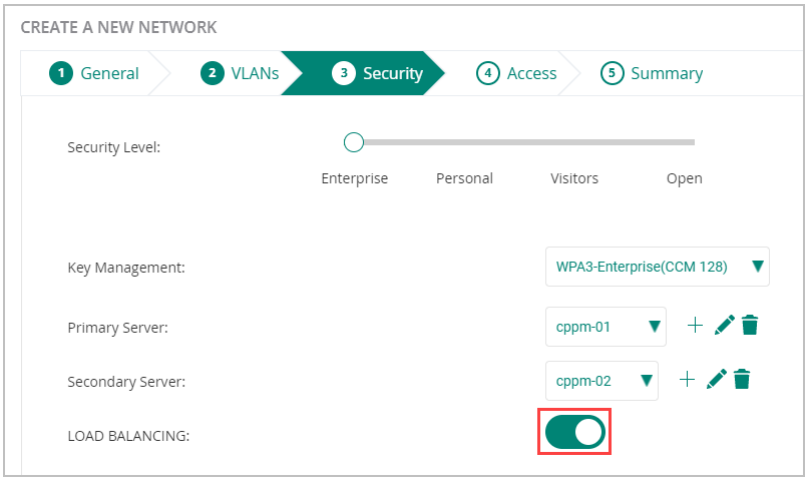


Figure 101: Enabling Load Balancing

NOTE:

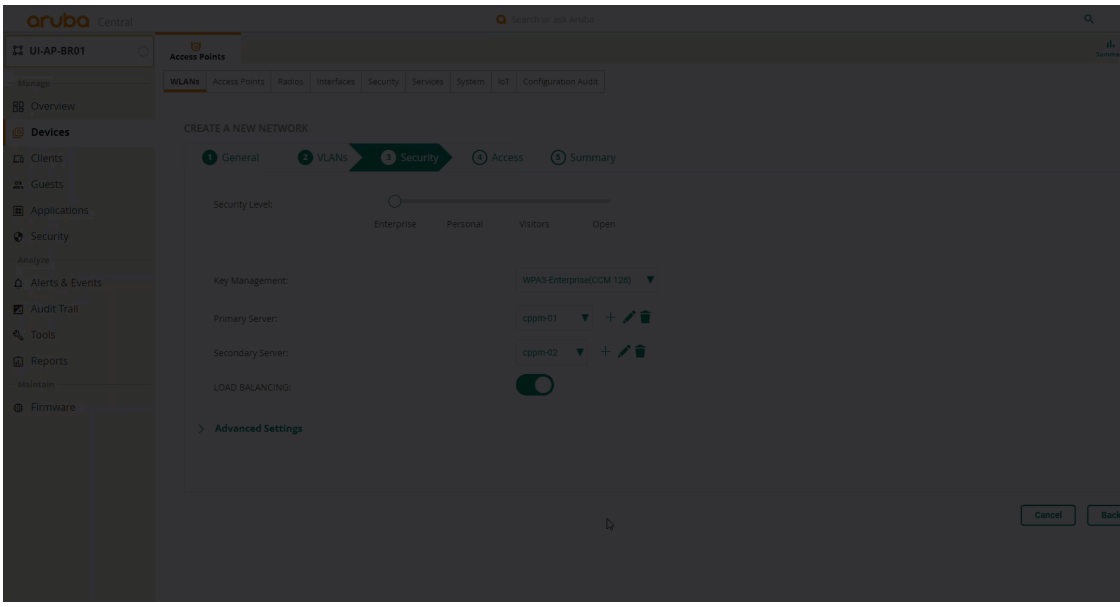
Best practice is to deploy 2 RADIUS servers and enable load balancing.

Step 8 On the **Security** tab, expand **Advanced Settings** and scroll down.

Step 9 Click the **+** (plus sign) to expand **Fast Roaming**.

Step 10 Ensure that **Opportunistic Key Caching** is enabled.

Step 11 Enable **802.11K**.



Configure Network Access Rules

Tunnel mode SSID restrictions are configured on the Gateway.

Step 1 On the **Access** tab, ensure that the **Access Rules** is set to **Unrestricted**.

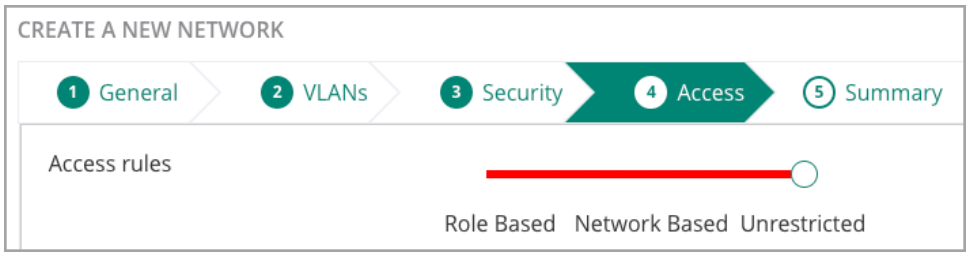


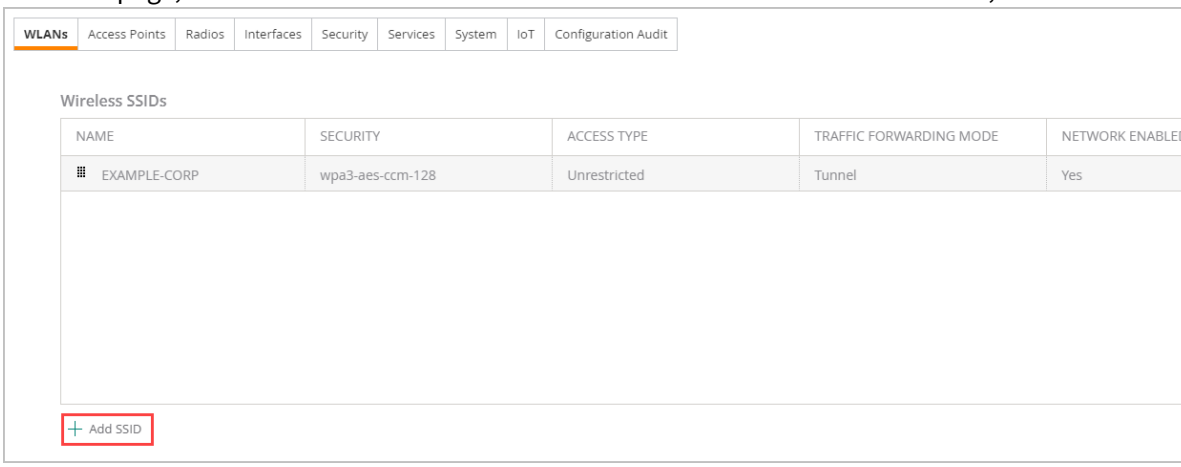
Figure 102: Set Access

Step 2 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 Configure SSID Name: **EXAMPLE-GUEST**

Step 3 On the **Create a New Network** page of the **General** tab, expand **Advance Settings**.

Step 4 Click the **+** (plus sign) sign to expand **Broadcast/Multicast**.

- Change the **Broadcast filtering** to *All*.
- Enable **DMO**, and set the **DMO Client Threshold** to *40*.

NOTE:

A **DMO Client Threshold** of 40 is the recommended initial value and should be adjusted based on actual performance results.

Step 5 Click the **(+)** sign to expand **Transmit Rates (Legacy Only)**.

- Set **2.4 GHz** to **Min:** *5*, **Max:** *54*.
- Set **5 GHz** to **Min:** *18*, **Max:** *54*.

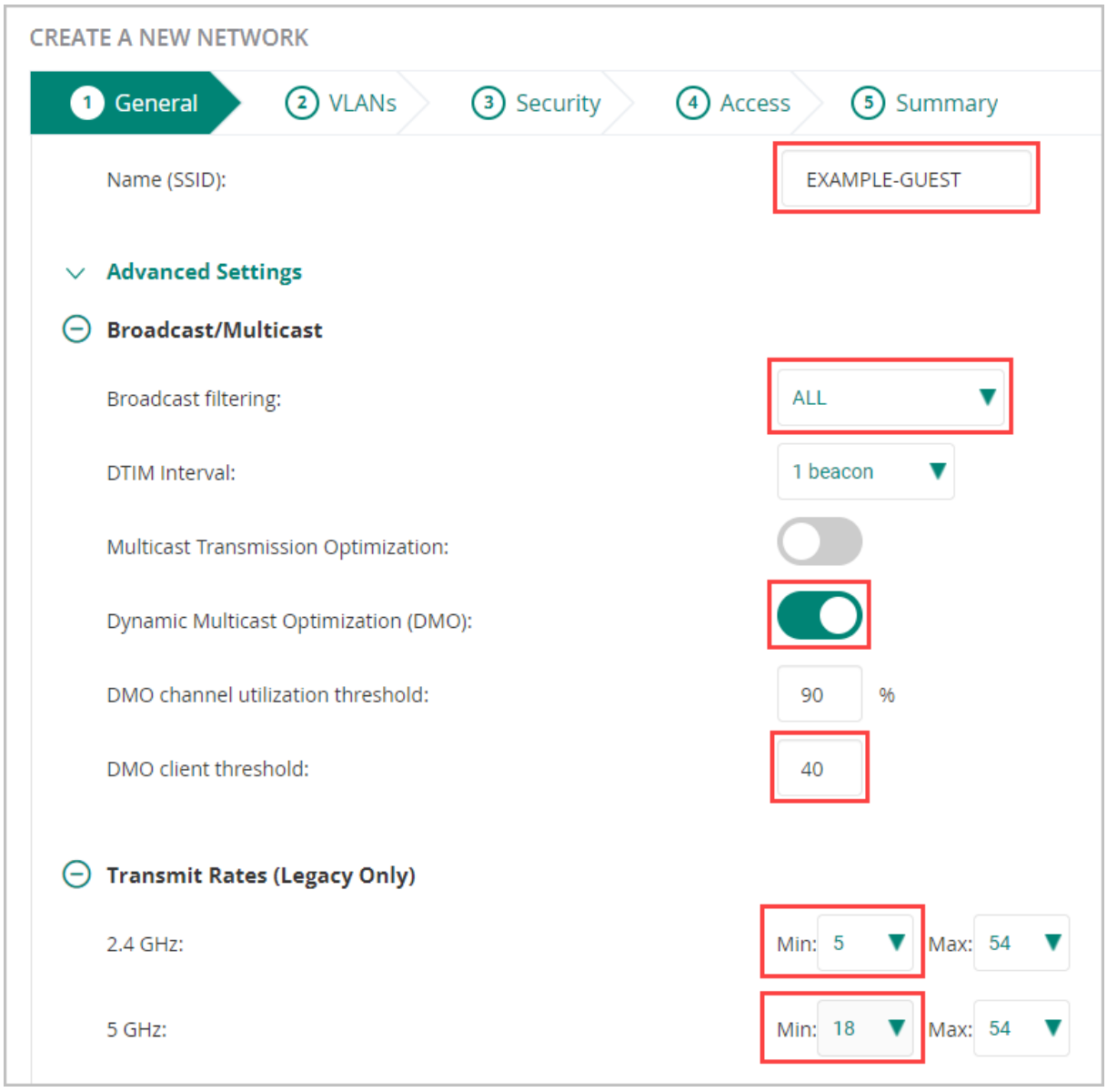
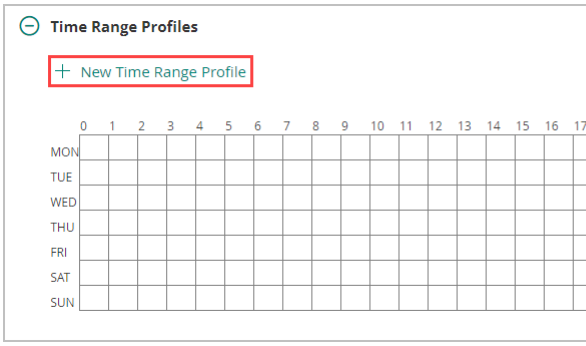


Figure 103: General SSID Configuration

Step 6 On the **General** tab, scroll down, and click the **+** (plus sign) to expand **Time Range Profiles**.



Step 7 In the middle of the section, click **(+) New Time Range Profile**.

Step 8 In the **New Profile** window, assign the following settings, then click **Save**.

- Configure the **Name**: *Visitor Weekdays*.

- Ensure the **Type** is *Periodic*.
- Set **Repeat** to *Daily*.
- Set the **Day Range:** *Monday - Friday (Weekdays)* (This can be changed to fit other environments).
- Set the **Start Time Hours:** *7*, **Minutes:** *0*.
- Set the **End Time Hours:** *18*, **Minutes:** *0*.

Figure 104: Configuring Time profile

Step 9 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**.

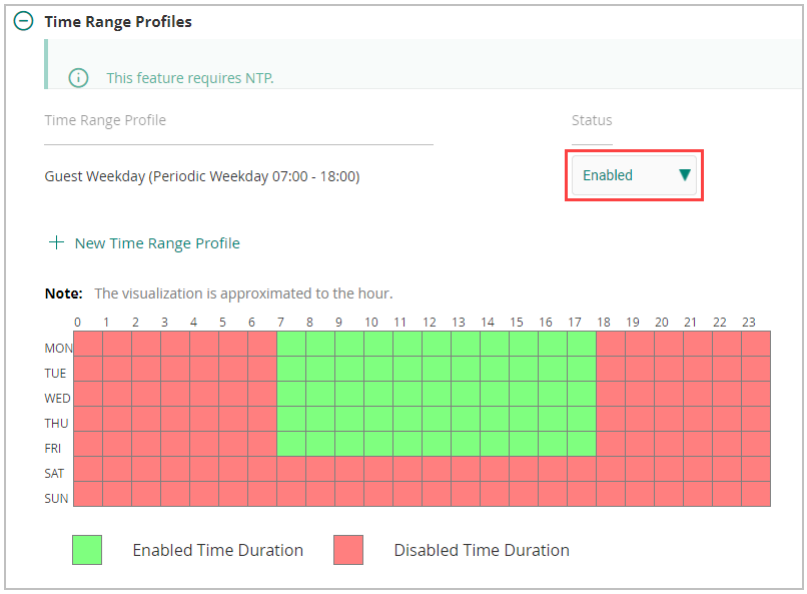


Figure 105: Enable Time profile

Configure VLANs

Step 1 On the **VLANs** tab, assign the following settings, then click **Next**. - Set the **Traffic Forwarding Mode** to *Tunnel*. -

Table of contents {: .text-delta } - TOC {:toc}

```
<script type="application/ld+json">
 {
    "@context": "http://schema.org",
    "@type": "Organization",
    "name": "Aruba Networks",
    "url": " https://arubanetworking.hpe.com/techdocs/VSG/",
    "description": "This section details how to use Aruba Central to ensure the
       topology is functional.",
    "keywords": {
        "WAN HA": "WAN Redundancy",
        "Clustering": "site clustering",
        "Branch gateway": "BGW"
    },
    "sameAs": [" https://en.wikipedia.org/wiki/Aruba_Networks",
        " https://www.facebook.com/arubanetworks/",
        " https://twitter.com/ArubaNetworks",
        " https://www.linkedin.com/company/aruba-a-hewlett-packard-enterprise-
           company",
        " https://www.youtube.com/c/arubanetworks/",
        " https://www.youtube.com/c/ABCNetworking",
        " https://community.arubanetworks.com/"
    ],
    "parentOrganization": {
        "@type": "Organization",
        "name": "Hewlett Packard Enterprise",
        "url": " https://www.hpe.com/us/en/home.html"
    },
    "owns": {
        "@type": "ProductGroup",
        "name": "Aruba Instant On",
        "url": " https://www.arubainstanton.com/",
        "logo": " https://www.arubainstanton.com/skin-solutionfuse-instant-on/img/
           aio-logo-drk-txt.svg",
        "description": "Let the network do the talking. Find access points and
           switches designed for small business. Get Wi-Fi up and running in
           minutes."
    },
    "address": {
        "@type": "PostalAddress",
        "addressLocality": "San Jose, CA",
        "postalCode": "95002",
        "streetAddress": "6280 America Center Dr"
    },
    "faxNumber": "+1-408-752-0626",
    "telephone": "+1-408-941-4300",
    "logo": " https://arubanetworking.hpe.com/wp-content/themes/Aruba2015/images/
       aruba_hp_lockup_140x68-01.svg"
 }
</script>
<script type="application/ld+json">
{
  "@context": " https://schema.org/",
  "@type": "WebSite",
   "url" : " http://arubanetworking.hpe.com/",
  "name": "Aruba Networks",
  "potentialAction": {
        "@type": "SearchAction",
        "target": " https://arubanetworking.hpe.com/gsa-search/#stq={
           search_term_string}",
        "query-input": "required name=search_term_string"
      }
}]
</script>
```

- **VLAN ID:** *Guest(104)*.

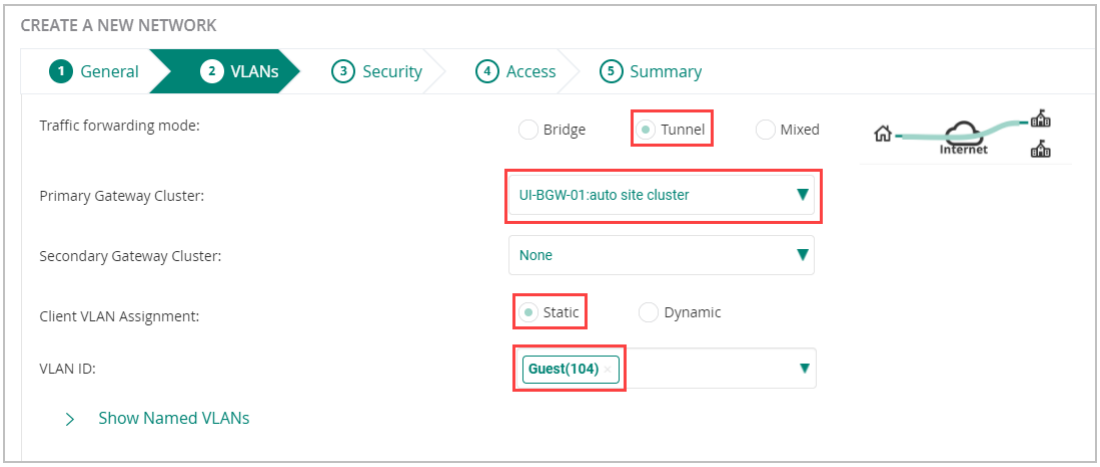


Figure 106: Set tunneling

NOTE:

When tunneling to the branch gateway, ensure that the VLAN line protocol is up by verifying the VLAN is trunked or **forced operational state up** is configured on the branch gateway

Configure Security

Step 1 On the **Security** tab, assign the following settings. - Set the **Security Level** to *Visitors*. - **Captive Portal Type:** *External*.

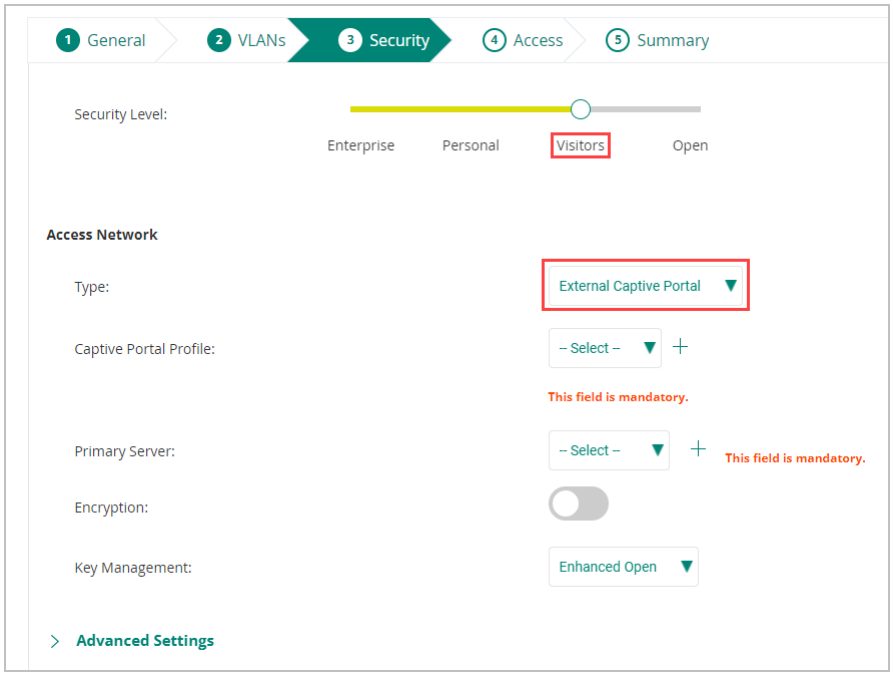


Figure 107: enable Captive portal

Step 2 In the **Splash Page** section, click the **+** (plus sign) next to **Captive Portal Profile**.

Step 3 In the **External Captive Portal-New** window, assign the following settings, then click **OK**.

- Enter the **Name:** *CPPM-Portal*.
- Set the **Authentication Type:** *RADIUS Authentication*.
- Enter the Clearpass **IP or Hostname:** *cppm.example.local*.
- Enter the captive portal **URL:** */guest/example_guest.php*.
- Verify the **Port** is *443*.
- Set the **Redirect URL:** *http://arubanetworking.hpe.com*.

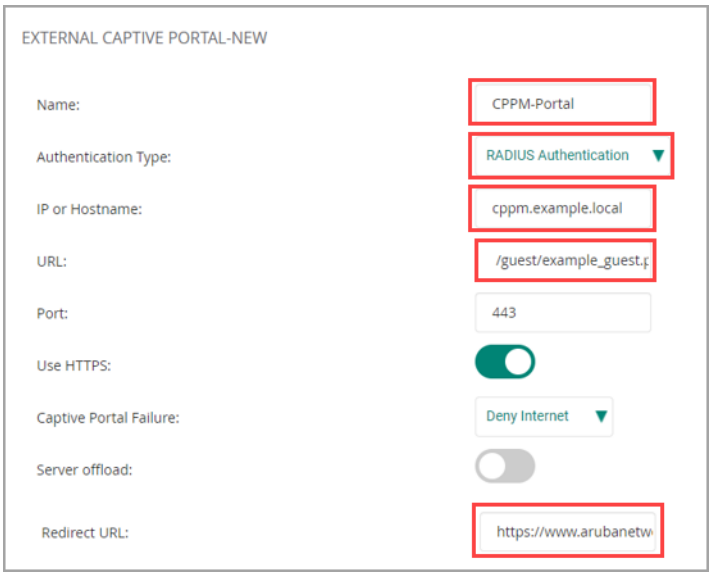
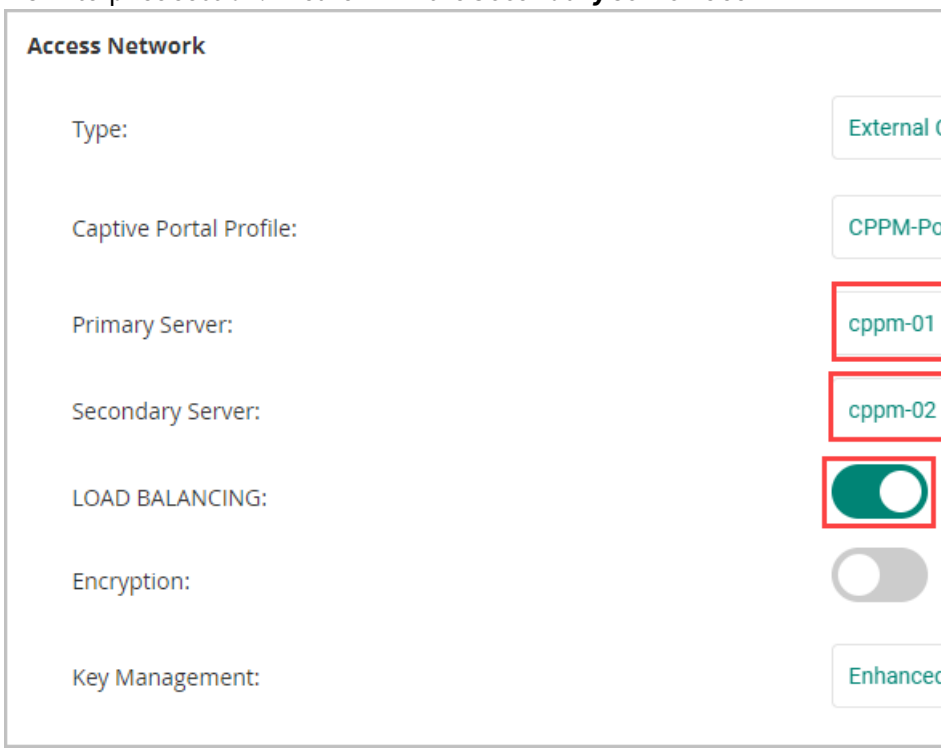


Figure 108: Redirect configuration

Step 4 On the **Security** tab of the **Splash Page** section, click the dropdown next to **Primary Server**. Select the RADIUS server created in the WPA3 Enterprise section. Ensure THAT the **Secondary server** is selected as well. Enable **Load Balancing**.



Step 5 If the RADIUS server was not created in the WPA3 Section, follow the steps BELOW to configure the RADIUS Server.

Step 6 On the **Security** tab, click the **+** (plus sign) next to **Primary Server**.

Step 7 In the **New Server** window, assign the following settings, then click **OK**. - Set **Server Type** to *RADIUS*. - Name the server *cppm-01*. - Enter the RADIUS **IP address**: *10.2.120.94*. - Enter the **Shared Key:** *shared key*.

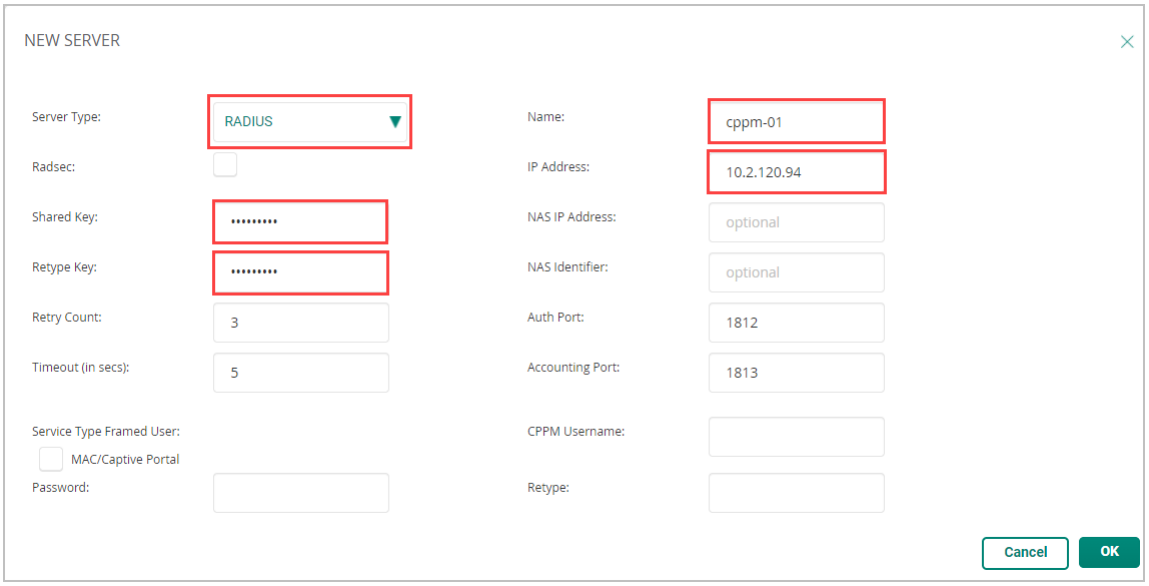


Figure 109: Adding Radius Server

NOTE:

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

Step 8 Repeat the two previous steps for the second CPPM server using the appropriate values.

Step 9 Enable **Load Balancing** by selecting the toggle, then click **Next**.

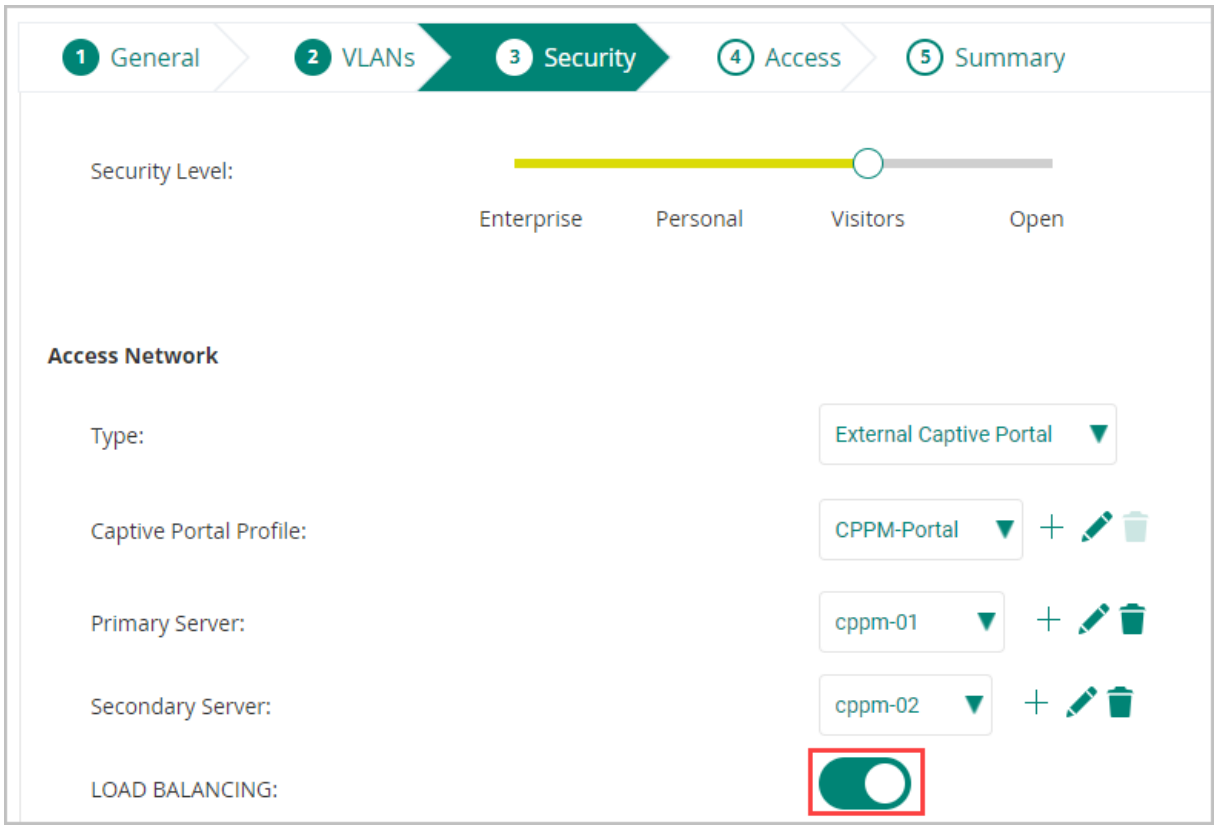


Figure 110: Enable Load balancing

NOTE:

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

Configure Access For Guest SSID

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

Step 1 On the **Access** tab, move the slider to **Network Based**.

Step 2 Select the **Allow any to all destinations** rule, then click the **pencil** icon.

Step 3 In the **Access Rules** window, change the action from *Allow* to *Deny*, then click **OK**.

Step 4 On the **Access** tab, select **(+) Add Rule**.

Step 5 In the **Access Rules** window, assign the settings in the table below, then click **OK**.

Step 6 Repeat step 4 and 5 for each row in the table.

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 must always be the last entry in the Access Rules to prevent unauthorized access to internal network resources.

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

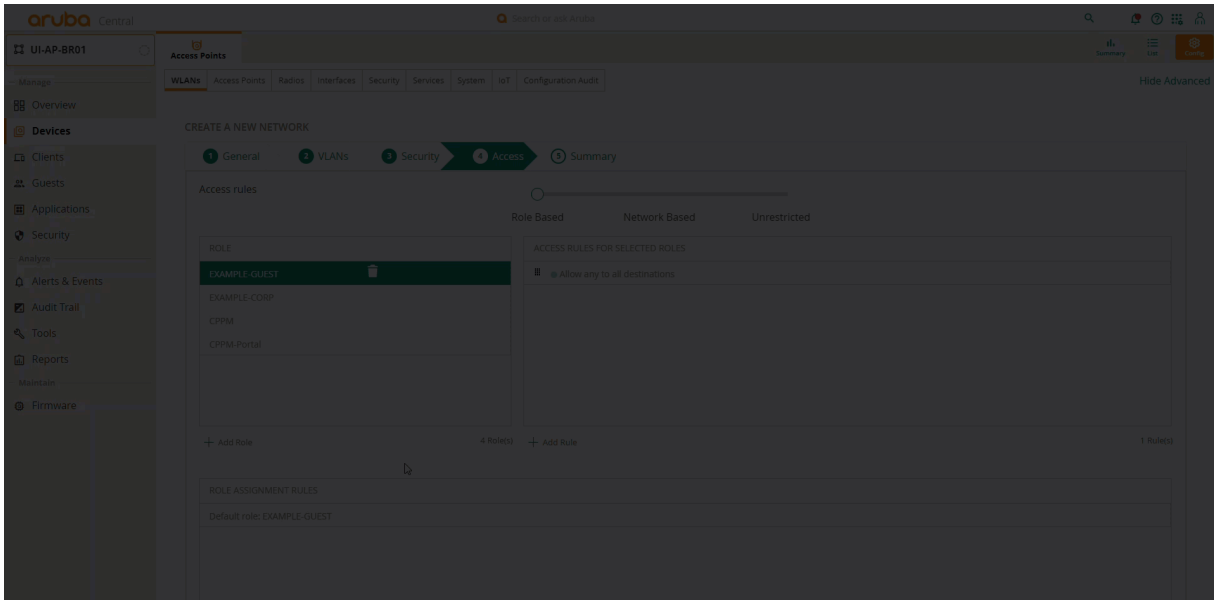
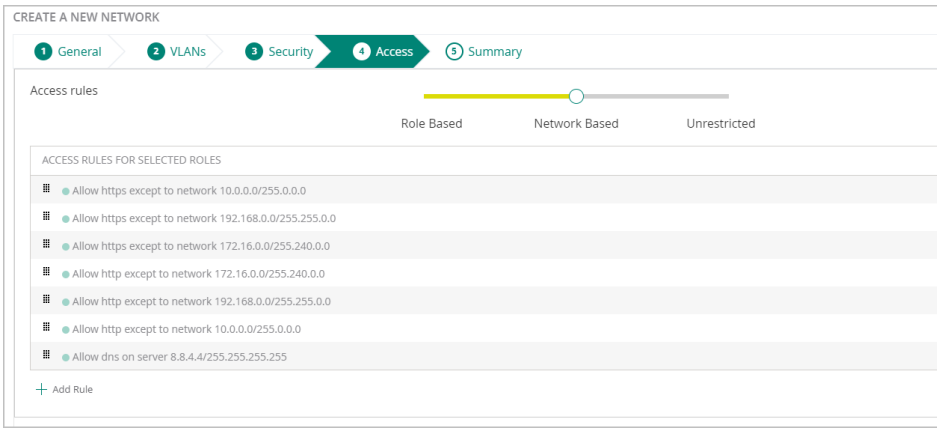


Figure 111: Configuring Access Control list



Step 7 Review the ACL, and select **Next**.

Step 8 On the **Summary** tab, review the settings, and click **Finish**.

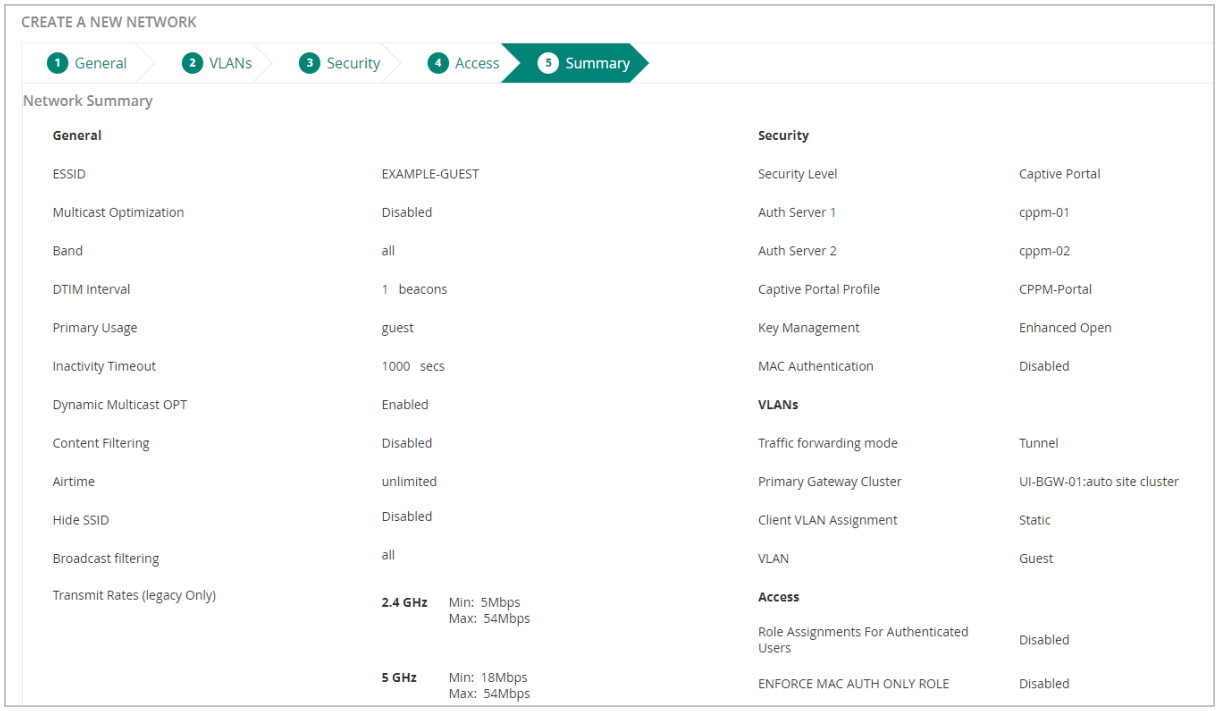


Figure 112: Summary Configuration

I AM HERE!!!!

Configure the WLAN Access Points

After a branch is operational, the access points automatically create a virtual controller (VC) cluster and join the default group.

Assign the WLAN AP Group

Step 1 In the dropdown, verify that **All Devices** is selected.

Step 2 In the left navigation pane, in the **Manage** section, select **Devices.**

Step 3 On the **Access Points** tab, in the **Access Points** section, identify the MAC addresses of the AP and assign the AP to the **UI-AP-BR01** group.

Step 4 In the left navigation pane, in the **Maintain** section, select **Organization**.

Step 5 Drag the virtual controller into the configured AP group. All access points in the site are automatically moved to the AP group.

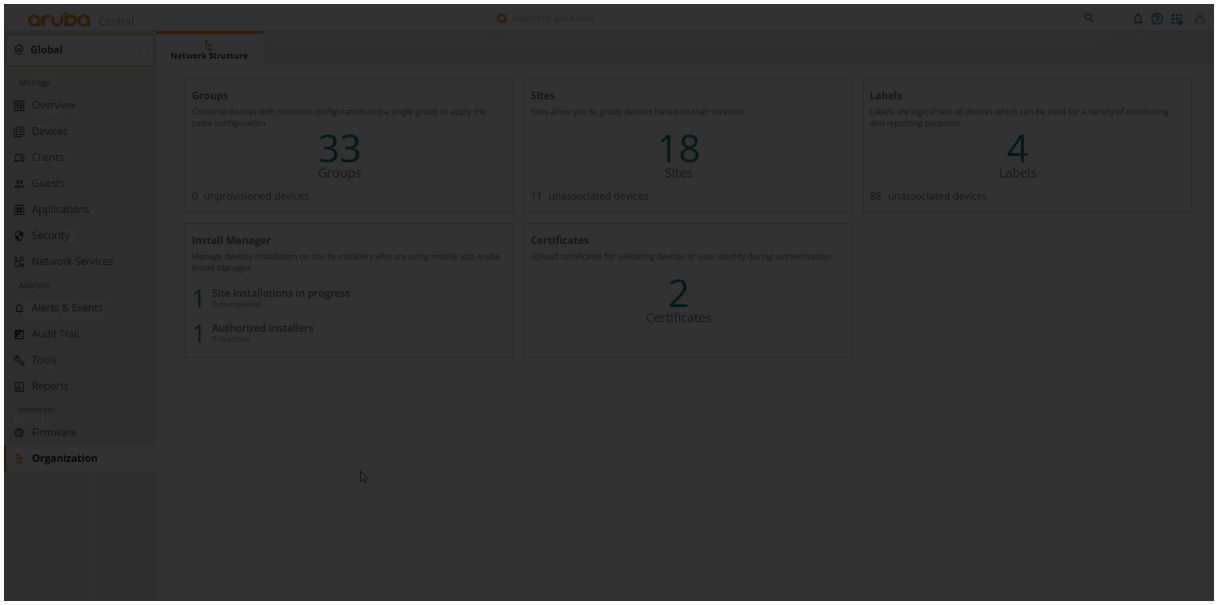


Figure 113: moving AP's

Assign WLAN Access Points to Site

The following procedure assigns access points to a site. Creating sites was shown in the "preparing to Deploy" section of the guide.

Step 1 Go to **Organization** and select **Site**

Step 2 Select **Unassigned** devices and assign the APs to the correct site. Click **Yes**

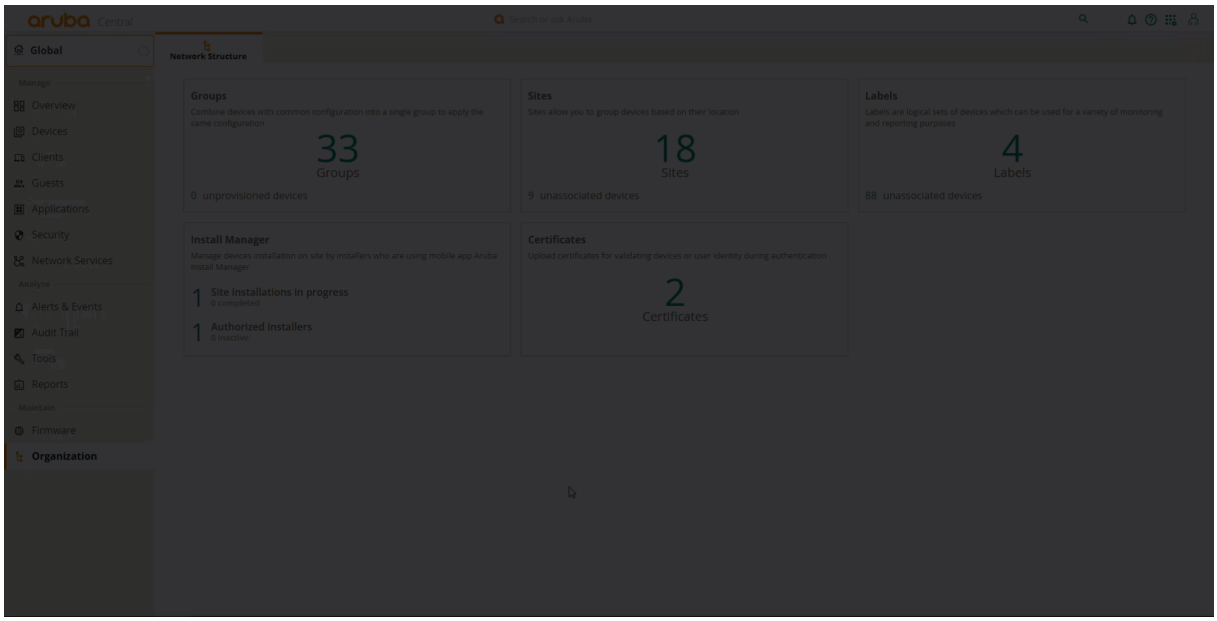


Figure 114: Assigning AP's to site

Rename the Access Points

Step 1 Go to the **UI-AP-BR01** group.

Step 2 Select **Configuration**.

Step 3 Select the AP, then click the **pencil** icon.

Step 4 Enter the new AP name. In this example, it is *RS01-AP01*. Click **Save Settings**.

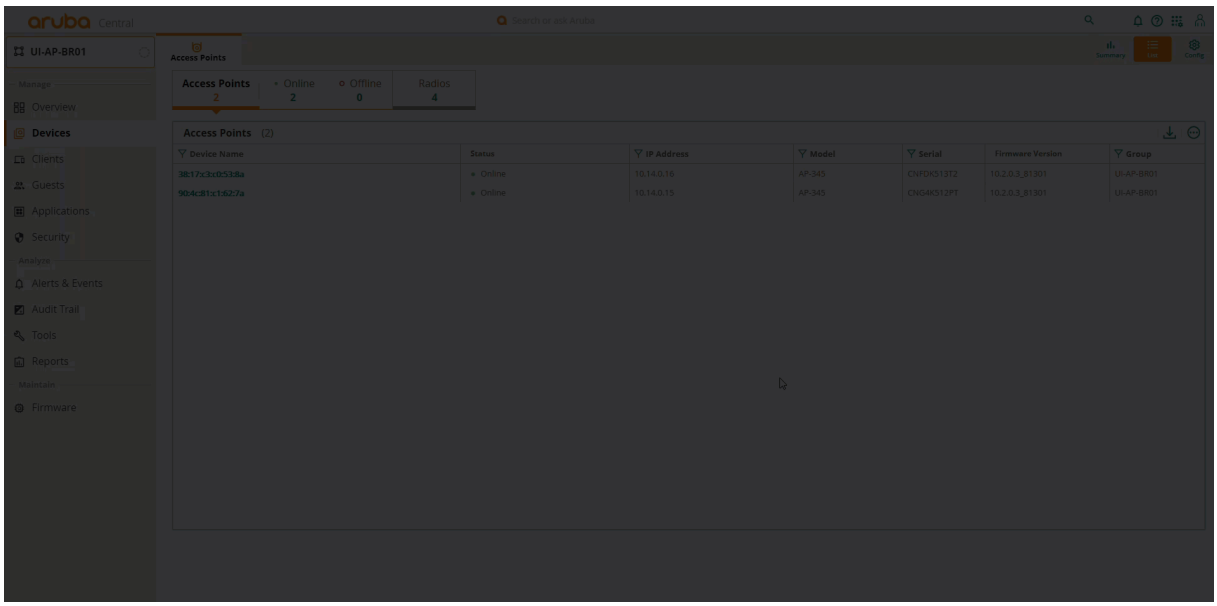


Figure 115: Naming AP's

SD-Branch Security

Aruba Edgeconnect SD-Branch includes security capabilities that enable admins to centralize network policy and propagate policy across the SD-Branch Fabric .

The following sections of this guide builds on the branches configured in the configured in the following section: This section of the guide will demonstrate how to configure, UBT and Centralized Multi-Site Fabric, and how to create policies.

The topology configured in the previous section is illustrated below with the to-be configuration of the logical topology.

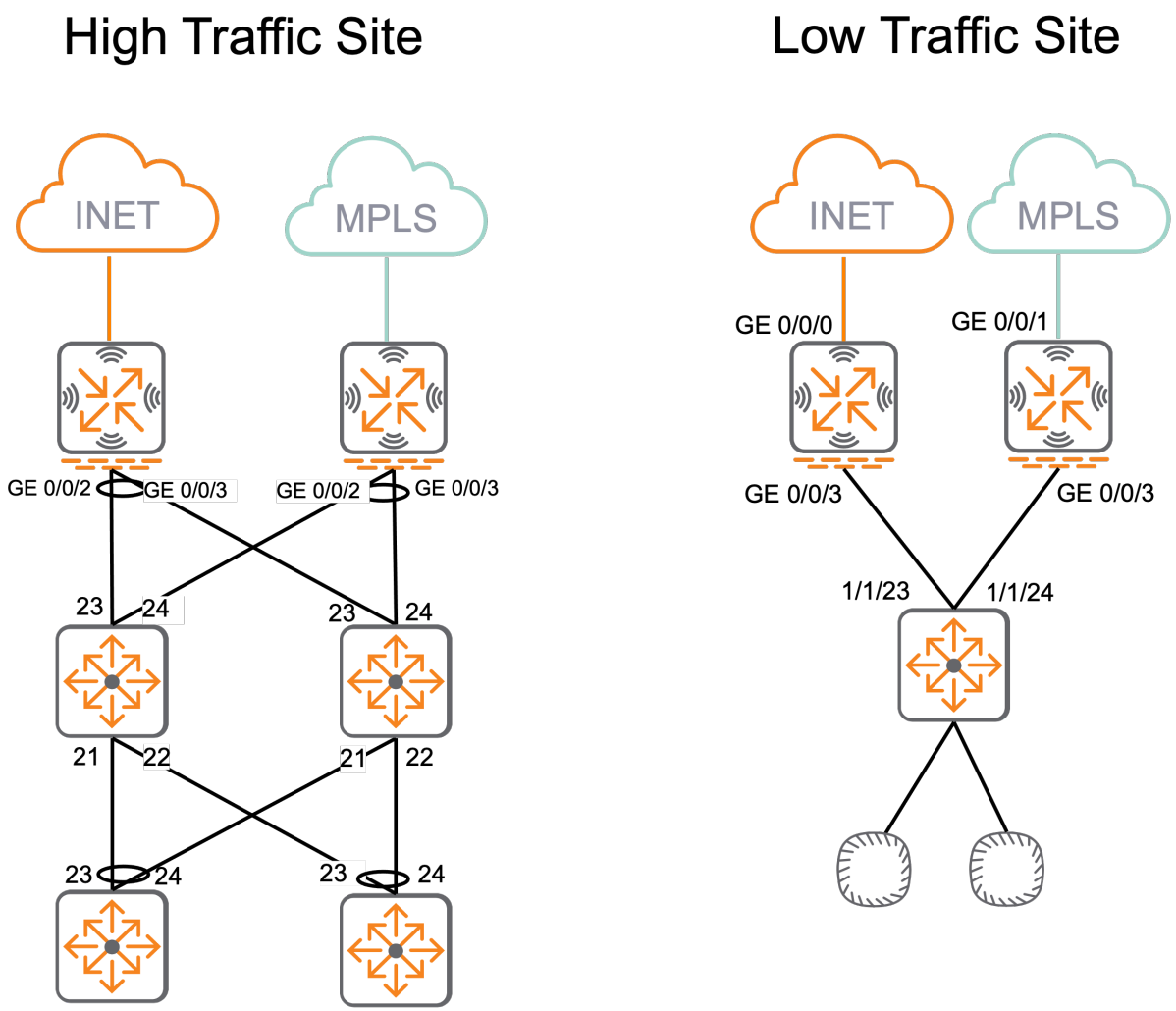


Figure 116: Logical_site_topology

Enabling Centralized Multi-Site Fabric

OWL Corp. plans to implement role-based policy to simplify network policy across the SD-WAN Fabric. They have requested enabling User Based Tunneling (UBT) at each branch site, with policy extended between branches.

The following procedures will demonstrate how to change the Switch and Gateway configurations, in order to enable role-based policy with UBT and Multi-Site Fabric. UBT centralizes policy at the Branch gateway. Multi-Site Fabric enables carrying the user role policy across the WAN, with enforcement at the destination branch gateway or VPNC.

Centralized Multi-Site Fabric Requirements

- Jumbo frames enabled on all Gateway VLANs
- Removal of user VLAN's from switches and access points.
- Large MTU configured on switch VLANs (9198 MTU)
- Change switch user roles to use gateway roles instead of VLANs
- UBT-Client-VLAN: this guide uses VLAN 2000 .

NOTE:

AP configuration do not require adjustment, since APs are already set to tunnel. No additional roles are needed for access points. The gateways will proxy the RADIUS request and apply roles based on the role returned from Clearpass. The gateway role will contain the policy configured below.

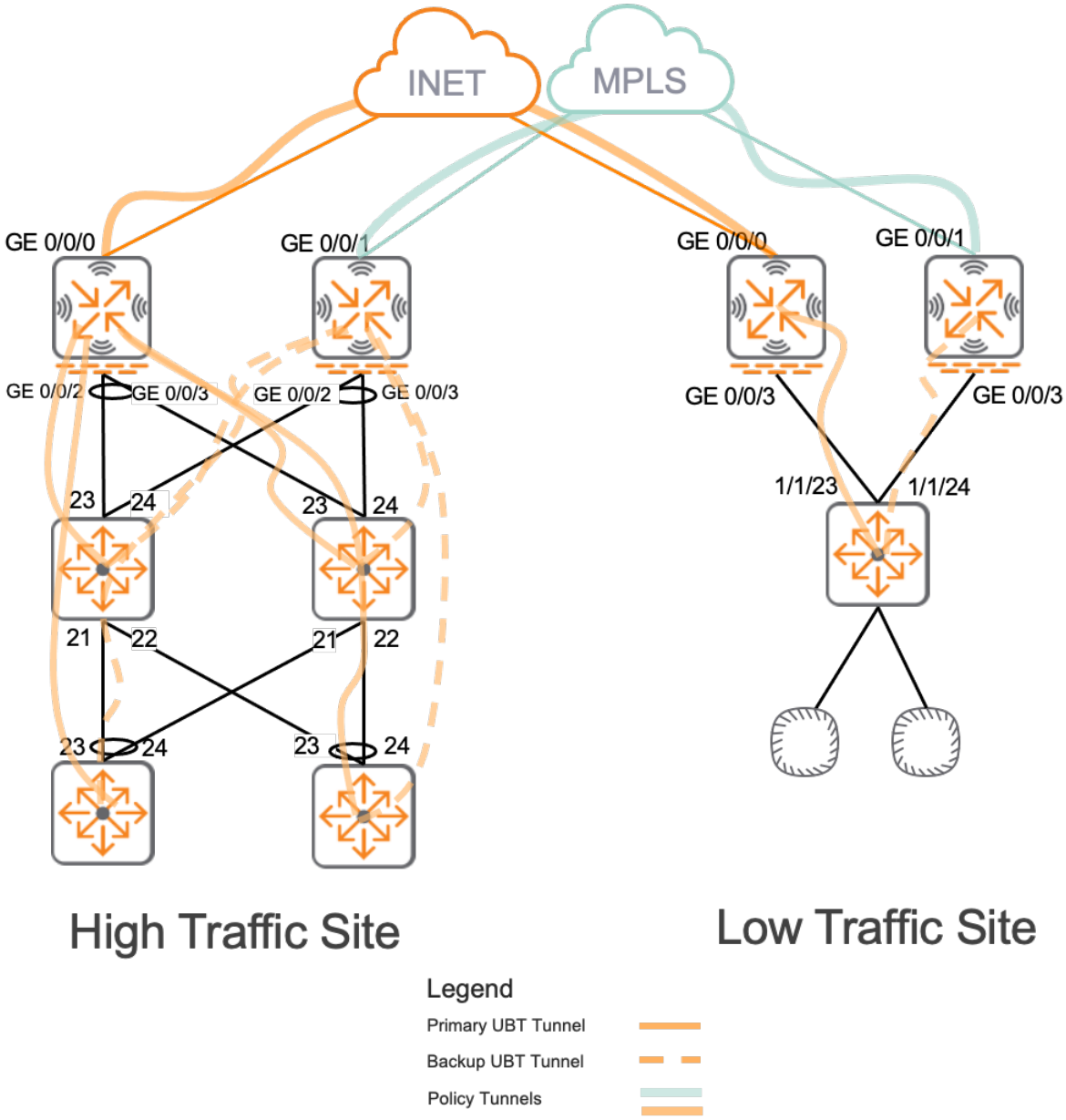


Figure 117: image-20240131091215658

Policy Requirements

All devices are assigned a user role. The level of access is determined by the user role. The following policies are configured.

Role	Allowed Access
EMPLOYEE	Printers, Internal Applications, DNS, DHCP, AD, Internet
IT-ADMIN	All Network Nodes , Internet
IT-SUPP	Employees, Printers, IOT-INTERNAL, IOT-LMT-INET, IOT-NO-INET, REJECT, Internet

Role	Allowed Access
VISITOR	Internet, Captive Portal, DHCP
PRINTER	Internal Applications (Employee, IT-Admins and IT-SUPP all should be able to initiate connections to printers, but the printer should not be able to initiate connections.)
IOT-NO-INET	IOT-NO-INET
IOT-INTERNAL	Internal Applications (padlock systems, asset tracking.)
IOT-LMT-INET	SaaS (Water systems, Air Quality Monitor, Smart thermostats .)
REJECT	Internet (All devices with reject role are profiled by ClearPass.)
QUARANTINE	Internal Applications.
CRITICAL	Internet, AD, DNS.
SECURITY	Internal Applications (Security Camera DVR, RFID Database)

NOTE:

The policy examples below do not represent all established OWL policies. The instructions provide information for only policies affected by this section's requirements

Enabling Multi-Site Fabric

This section illustrates how to enable Multi-Site Fabric, enabled between specific groups. The section also detail the centralized configuration of user roles using the Global Policy Manager.

It is imperative to configure user roles within the Global Policy Manager, where the mapping of policy ID to user roles takes place. The assigned policy ID is carried between branches, allowing the propagation of policy. The Policy ID received by destination branches is also used for reverse lookups of roles configured in Global Policy Manager, ensuring the enforcement of role-to-role policies.

NOTE:

For admins who do not intend to enable Multi-Site Fabric, user roles and policies can be configured at the group level.

Configure Global Client Roles

Step 1 On the **Global** page, in the left menu, click **Security**.

Step 2 Click the **Client Roles** tab at the top of the page.

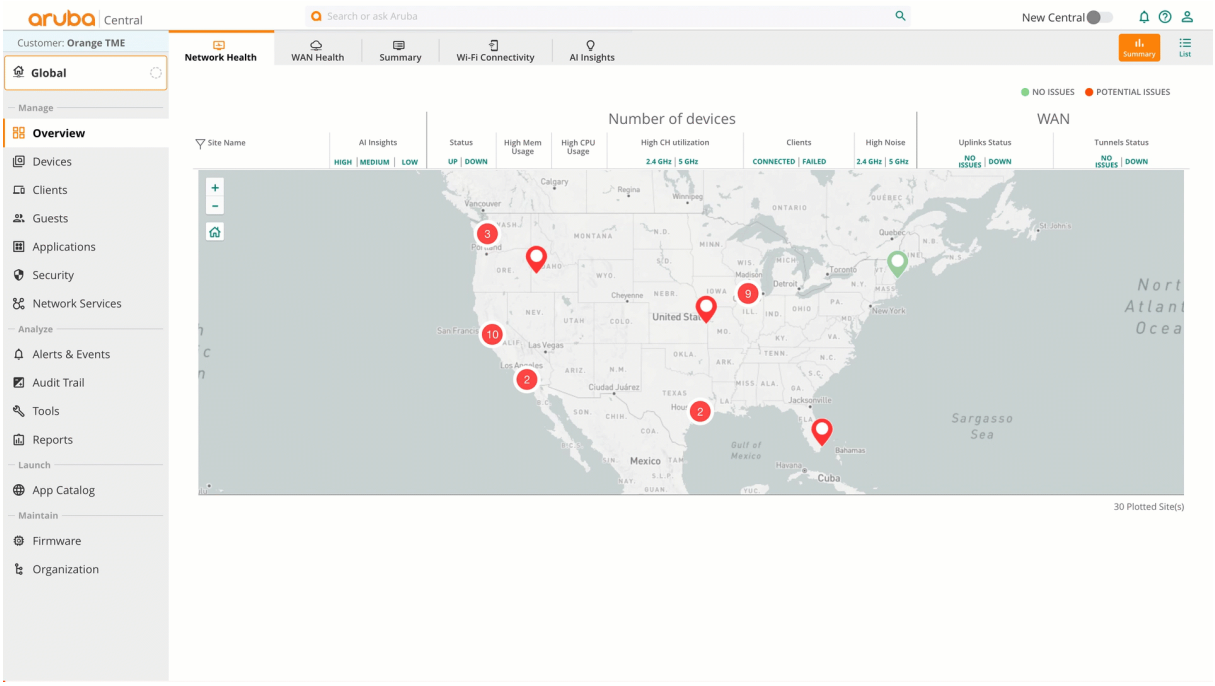
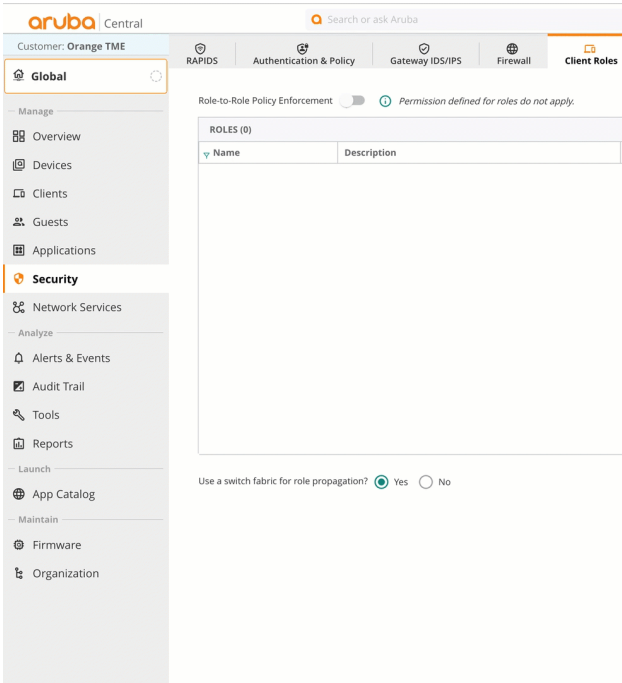


Figure 118: Navigation to security page

NOTE:

All user roles configured before Aruba Central 2.5.6 were automatically configured in Global Policy Manager. Delete roles that are not needed and skip adding the roles.

Step 3 Click the **+** (plus sign) in the **Roles** table.



Step 4 Enter the following **User Role** name: *EMPLOYEE*. Click **Save**.

Step 5 Repeat Steps 3 to 4 for the list of user roles below.

- IT-ADMIN

- IT-SUPP
- VISITOR
- PRINTER
- IOT-NO-INET
- IOT-INTERNAL

- IOT-LMT-INET
- REJECT
- QUARANTINE
- CRITICAL
- SECURITY

Step 6 Hover over the ***EMPLOYEE*** role that was created and click the **edit** (pencil) icon.

Step 7 In the **Permissions** table, click the **edit** (pencil) icon.

- Click the **PRINTER** box in **Allow Source to Destination**.
- Click **Assign**.
- Click **Save**.

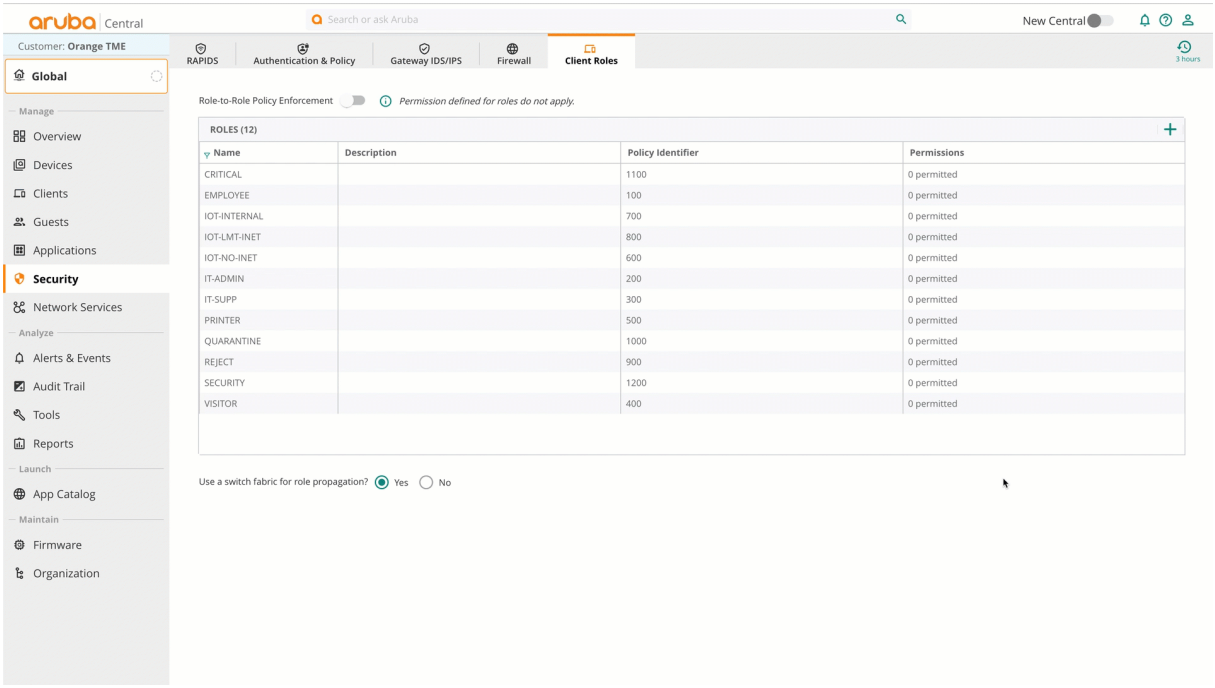


Figure 119: Assigning role to role permissions

Step 8 Repeat step 7 for the role-to-role permissions below. Application-level permissions are configured in the “Updating Gateway Configuration” section.

Role	Allowed Access
EMPLOYEE	Printers

Role	Allowed Access
IT-ADMIN	All Network Nodes
IT-SUPP	Employees, IT-ADMIN, Printers, IOT-INTERNAL, IOT-LMT-INET, IOT-NO-INET, REJECT
PRINTER	Employee, IT-Admins and IT-SUPP should all be able to initiate connections to printers but the printer should not be able initiate connections.
IOT-NO-INET	IOT-NO-INET

NOTE:

Configuring one role automatically configures other roles that are allowed to the destination.

Enable Role to Role Policy across branches

Step 9 At the bottom of the page, select *No* in **Use a switch fabric for role propagation?** Select **No.**

Step 10 Click **Branch** and click the **+** (plus sign.

- Select the **BR-ECSDB** group.
- Select the **VPNC-RSVDC** group.
- Click **Assign**.
- Click **Save**.

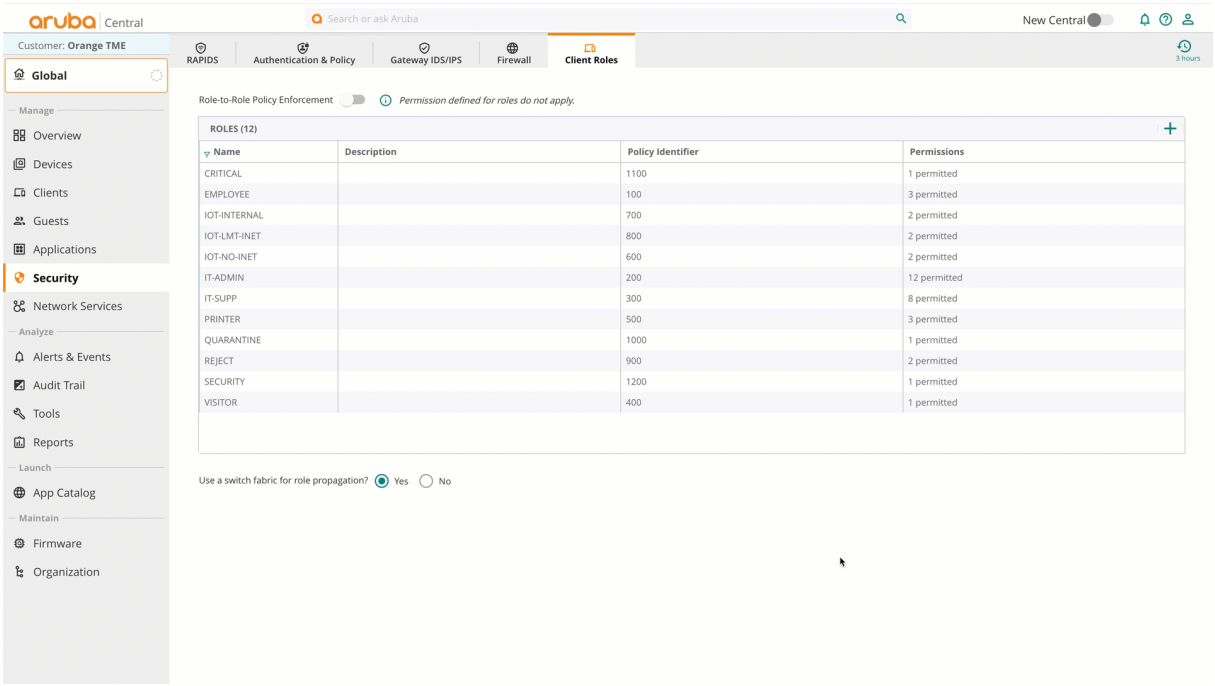


Figure 120: Selecting role-to-role groups-1972299

CAUTION:

Two groups must be selected or roles and policy cannot be pushed to the group. SD-Branch role propagation and role propagation across a switch fabric are mutually exclusive.

Step 12 At the top of the page, click the **Role-to-Role Policy Enforcement** slider.

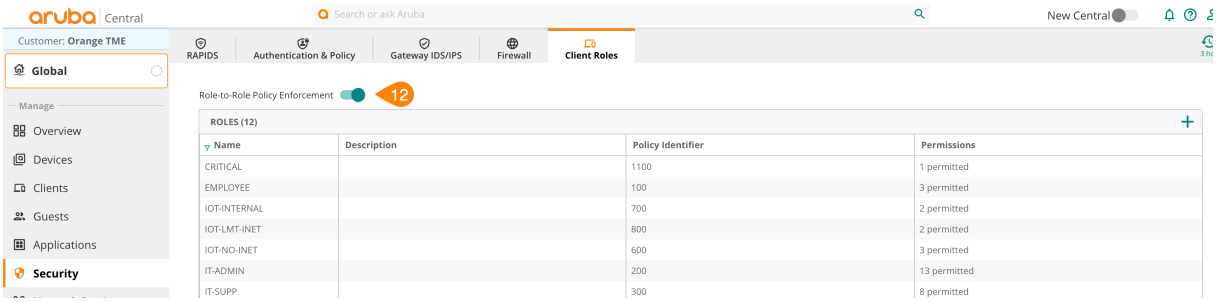


Figure 121: Enable Role-to-Role Policy-1970841

Step 13 Scroll down the page and click **Save**.

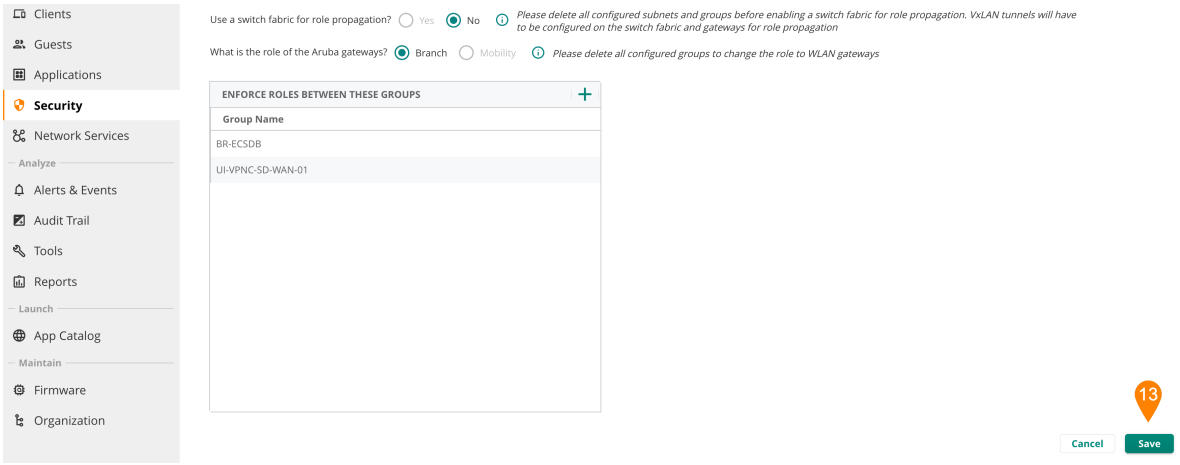


Figure 122: Save Settings

SD-Branch User Based Tunneling

This section demonstrates changes needed for the switch and gateway to allow UBT at a branch site. APs are already set to tunnel and do not require adjustment. No additional roles are needed for access points.

Update Switch Template Configuration

The switch template must be updated first.

Four configuration changes for the switch are required: adjusting MTU size, removing unused VLAN's, enabling UBT and adjusting user roles.

Adjusting the MTU size on the switch disrupts service and causes the switches to lose connection to the gateways. The connection is restored after gateway configuration when the MTUs match. .

Step 1 In the **BR-ECSDB** group, click the **Switch** tab.

Step 2 In the **Switches List** page at the top right, click **Config**.

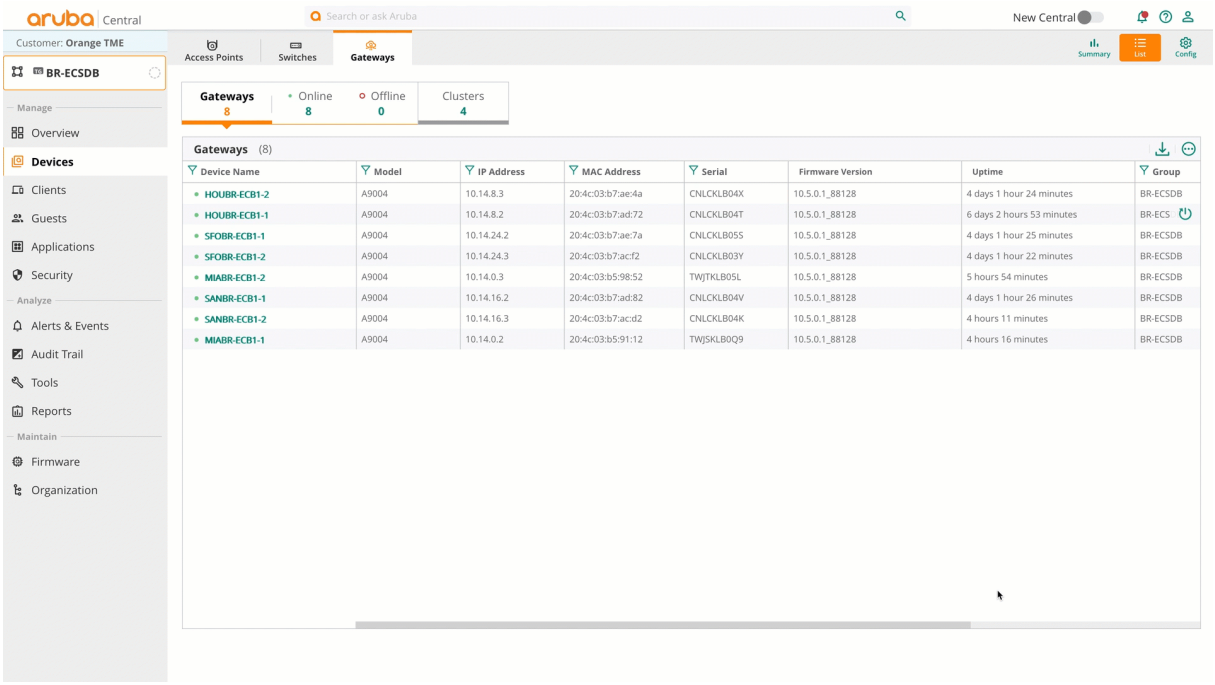


Figure 123: navigate_sw_template_config

Step 3 In the **Switches Template** section, hover over the **BR-ACC** template and click the **edit** (pencil) icon.

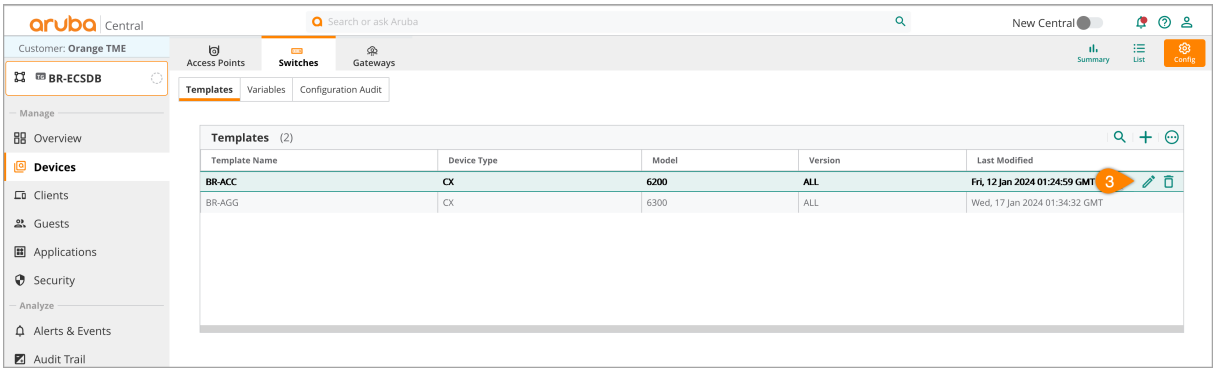


Figure 124: edit template

Configuring UBT Client VLAN

The original template configuration is shown below. The following VLANs will be adjusted.

Step 1 Adjust the VLAN's configuration.

```
vlan 101
    name EMPLOYEE
    dhcpv4-snooping
    arp inspection
    ip igmp snooping enable
vlan 102
    name CAMERA
    dhcpv4-snooping
    arp inspection
    ip igmp snooping enable
vlan 103
    name IOT
    dhcpv4-snooping
    arp inspection
    ip igmp snooping enable
vlan 104
    name VISITOR
    dhcpv4-snooping
    arp inspection
    ip igmp snooping enable
vlan 105
    name REJECT
    dhcpv4-snooping
    arp inspection
    ip igmp snooping enable
vlan 106
    name CRITICAL
    dhcpv4-snooping
    arp inspection
    ip igmp snooping enable
vlan 107
    name QUARENATINE
    dhcpv4-snooping
    arp inspection
    ip igmp snooping enable
```

Step 2 Reconfigure the VLANs as:

```
vlan 100
    name MGMT
vlan 101
    name EMPLOYEE
vlan 102
    name CAMERA
vlan 103
    name IOT
vlan 104
    name VISITOR
vlan 105
    name REJECT
vlan 106
    name CRITICAL
vlan 107
    name QUARENATINE
vlan 2000
  name UBT_CLIENT
  dhcpv4-snooping
  arp inspection
  ip igmp snooping enable
```

Step 4 Ensure VLANs are on the uplinks and the MTU is set.

```
interface 1/1/23
  description Uplink_GW
  no shutdown
  no routing
  mtu 9198
  vlan trunk native 100
  vlan trunk allowed 100-107
  arp inspection trust
  dhcpv4-snooping trust
interface 1/1/24
  description Uplink_GW
  no shutdown
  no routing
  mtu 9198
  vlan trunk native 100
  vlan trunk allowed 100-107
  arp inspection trust
  dhcpv4-snooping trust
```

Step 3 Adjust the MTU on VLAN 100, so users can access the network.

```
interface vlan 100
  description MGMT
  ip mtu 9198
  ip dhcp
```

Configure UBT

For switch-to-tunnel traffic to the gateways, the UBT VLAN must point to the gateway's IP address, which is a new variable in the template.

Step 1 Define the UBT client VLAN and create the UBT zone in the default VRF.

- **UBT Client VLAN:** *2000*
- **UBT Zone:** *branch*

```
ubt zone branch vrf default
  primary-controller ip %gateway_1_sys_ip%
  backup-controller ip %gateway_2_sys_ip%
  enable

ubt-client-vlan 2000
```

Adjust User Roles

The roles must be adjusted to point to the gateway roles. The names must match the names on the gateway. The gateway map the VLAN to the roles and enforces role-to-role policy. The original configuration in the template below shows the user roles to be adjusted.

```
port-access role ARUBA-AP
  auth-mode device-mode
  vlan trunk native 100
  vlan trunk allowed 100,101,104-107
port-access role REJECT
    reauth-period 120
    vlan access 105
port-access role EMPLOYEE
    reauth-period 120
    vlan access 101
port-access role  PRINTER
    reauth-period 120
    vlan access 102
port-access role  IOT
    reauth-period 120
    vlan access 103
port-access role GUEST
    reauth-period 120
    vlan access 104
port-access role REJECT
    reauth-period 120
    vlan access 105
port-access role CRITICAL
  reauth-period 120
  vlan access 106
port-access role QUARANTINE
    reauth-period 120
    vlan access 107
```

Step 1 Remove the **VLAN access** line from the roles displayed above and replace them with the following **VLAN access** line: - *gateway-zone zone branch gateway-role* and the respective role name.

```
port-access role EMPLOYEE
    reauth-period 120
    gateway-zone zone branch gateway-role EMPLOYEE
port-access role SECURITY
    reauth-period 120
    gateway-zone zone branch gateway-role SECURITY
port-access role IOT-NO-INET
    reauth-period 120
    gateway-zone zone branch gateway-role IOT-NO-INET
port-access role IOT-INETERNAL
    reauth-period 120
    gateway-zone zone branch gateway-role IOT-INETERNAL
port-access role IOT-LMT-INET
    reauth-period 120
    gateway-zone zone branch gateway-role IOT-LMT-INET
port-access role VISITOR
    reauth-period 120
    gateway-zone zone branch gateway-role VISITOR
port-access role INFRA-DEVICE
   reauth-period 120
   gateway-zone zone branch gateway-role INFRA-DEVICE
port-access role PRINTER
   reauth-period 120
   gateway-zone zone branch gateway-role PRINTER
port-access role IT-ADMIN
   reauth-period 120
   gateway-zone zone branch gateway-role IT-ADMIN
port-access role IT-SUPP
   reauth-period 120
   gateway-zone zone branch gateway-role IT-SUPP
port-access role REJECT
    reauth-period 120
    gateway-zone zone branch gateway-role REJECT
port-access role CRITICAL
    reauth-period 120
    vlan access 106
port-access role QUARANTINE
   reauth-period 120
   gateway-zone zone branch gateway-role QUARANTINE
```

Step 2 Remove the old VLAN's from the AP role.

```
port-access role ARUBA-AP
  auth-mode device-mode
  vlan trunk native 100
  vlan trunk allowed 100
```

Update Gateway Configuration

The gateways require three changes to enable user based tunneling: MTU size must be increased, and both VLAN-to-role mapping and network policy must be configured in the group. This section demonstrates the process.

Adjusting VLAN MTU

Step 1 Select the **Gateways** tab, then click the gear icon in the upper right corner.

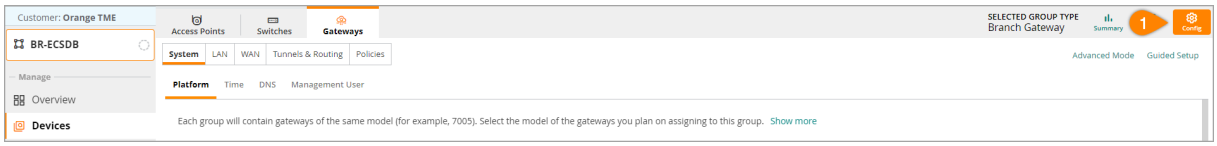


Figure 125: bgw-select-config-2

Step 2 Select **LAN**. Click **Lan Ports**

Step 3 Hover over the **GE0/0/2** interface, then select the pencil icon.

Step 5 Check the **Jumbo Frames** box.

Step 6 Select **Save**.

Step 7 Repeat steps 3-6 for the **GE0/0/3** interface.

Step 8 Click **Save Settings**

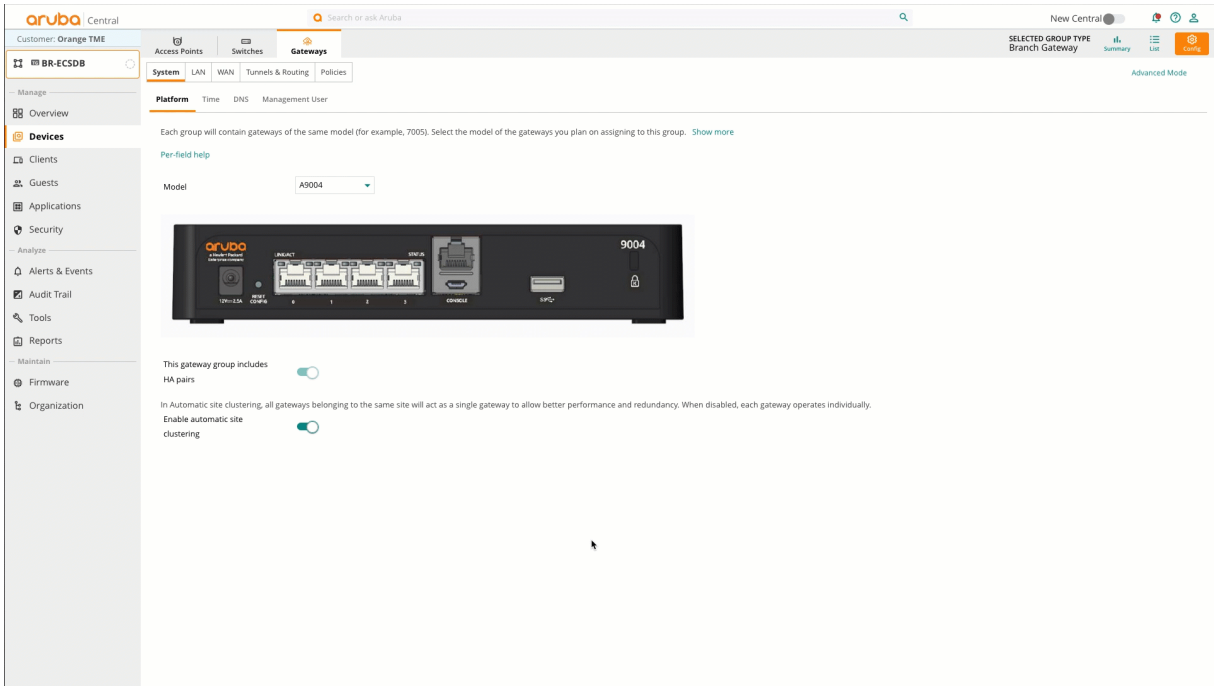


Figure 126: enabling jumbo frames

Associate VLANs to User Roles

Roles are established within the group from global policy manager . However, these roles lack VLAN association. Consequently, during authentications, clients are assigned a role with VLAN 1 by default instead of being placed in the appropriate VLAN. The following procedure demonstrates how to associate VLANs to roles.

Step 1 Ensure the Gateway configuration is in **Advanced Mode**. Select the **Security tab.**

Step 2 Select the **Roles** tab.

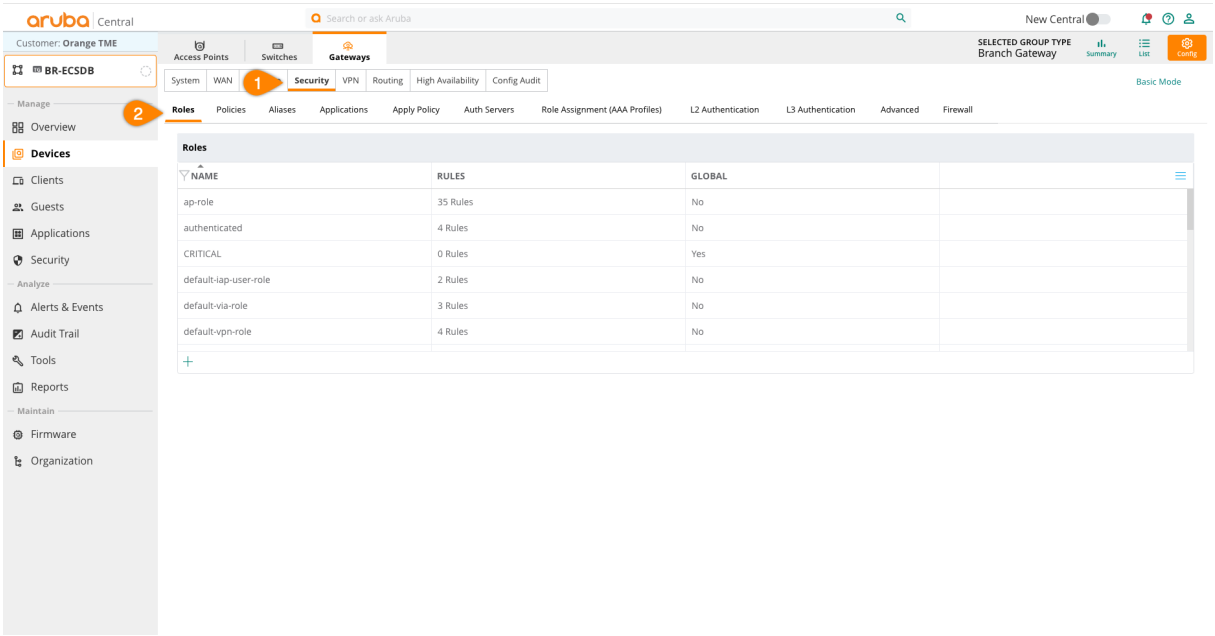


Figure 127: Navigation to roles

Step 3 Select the **Critical** role.

Step 4 Scroll down and select the **More** tab. In the more tab, set the **VLAN ID** and the max sessions.

- VLAN: *106*
- Max Sessions: *10000*

Step 5 Click **Save Settings**.

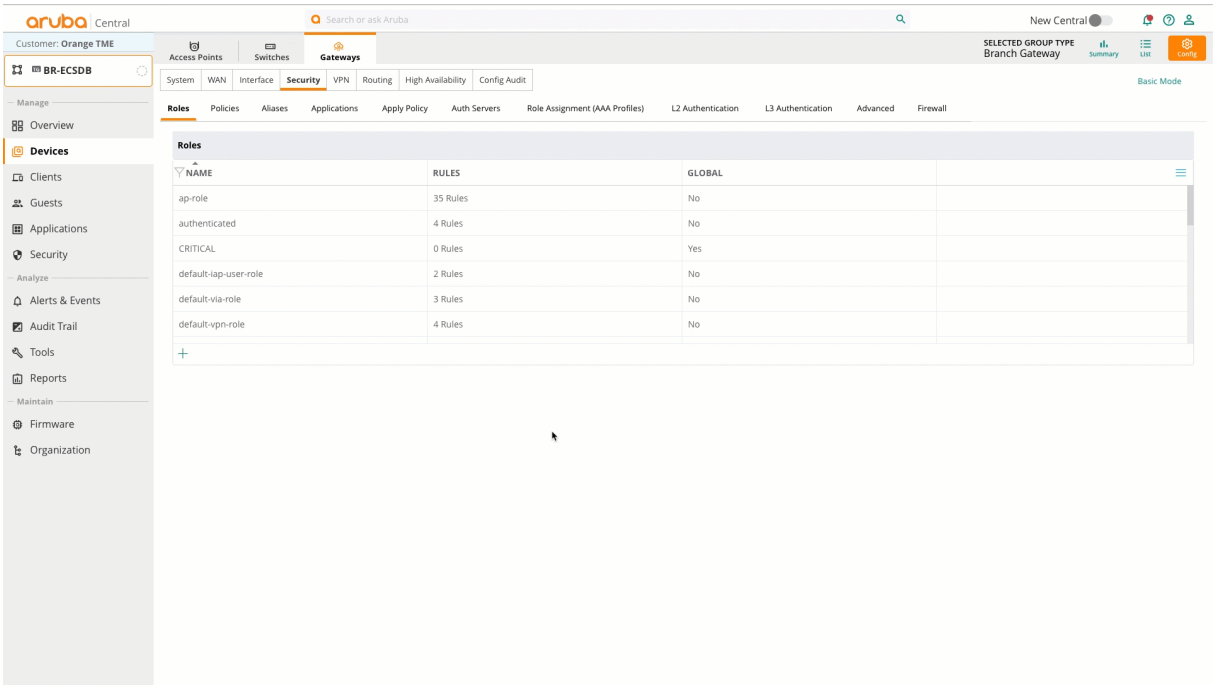


Figure 128: Connecting VLAN to user Role

NOTE:

The VLAN List displays VLAN IDs. Named VLANs also can be used to associate the VLAN to the user role. In the example above, the VLAN ID is used.

Step 6 Repeat steps 3 to 5 for all roles.

User Role	VLAN ID
EMPLOYEE	101
PRINTER	102
IOT-INTERNAL	103
IOT-LMT-INET	103
IOT-NO-INET	103
GUEST	104
REJECT	105
CRITICAL	106
QUARANTINE	107

Configuring Network Policy with User Roles

Global policy manager can configure only role-to-role policies. For more granular policies, such as applications or network protocols, the configuration be made in the group. This section walks through the process of configuring URL and IP-based policies specifically for the *Visitor* user role.

Role	Allowed Access	Denied Access
VISITOR	Internet, Captive Portal (cppm.example.local), DHCP/DNS(10.2.120.99/98)	RFC1918

Step 1 On the **Gateway** tab on the top right side, select **Basic Mode**.

Figure 129: select basic mode

Step 2 Select the **Policies** tab. Click **Applications**.

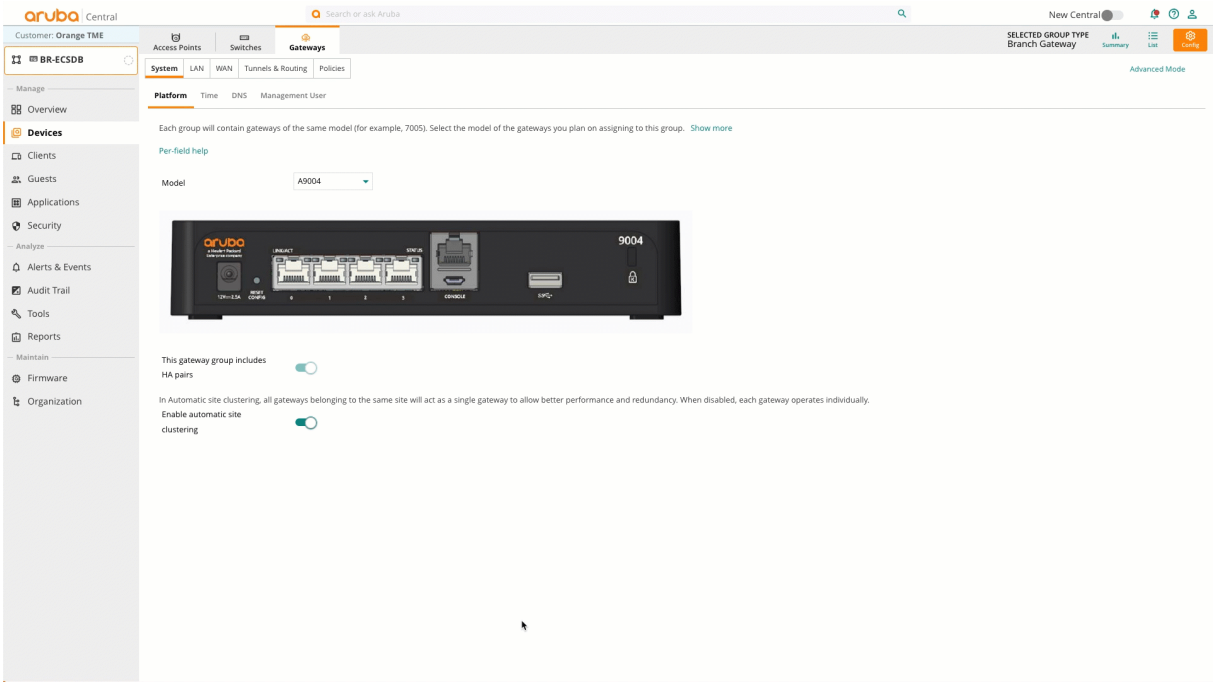


Figure 130: Navigation_to_polices

Step 3 Click the **+** (plus sign) beside **Network Aliases.** In the **Name** field, enter *ad server*.

Step 4 Click the **+** (plus sign) in the **User Rules** table.

Step 5 In the new row's **Type Column**, click **Name**. Scroll to select **Host**. In the **IP Address** field, enter *10.2.120.98*.

Step 6 Repeat step 4. Click **Name**. Scroll to select the **Host**. In the **IP Address** field, enter *10.2.120.99*.

Step 7 Click **Save**.

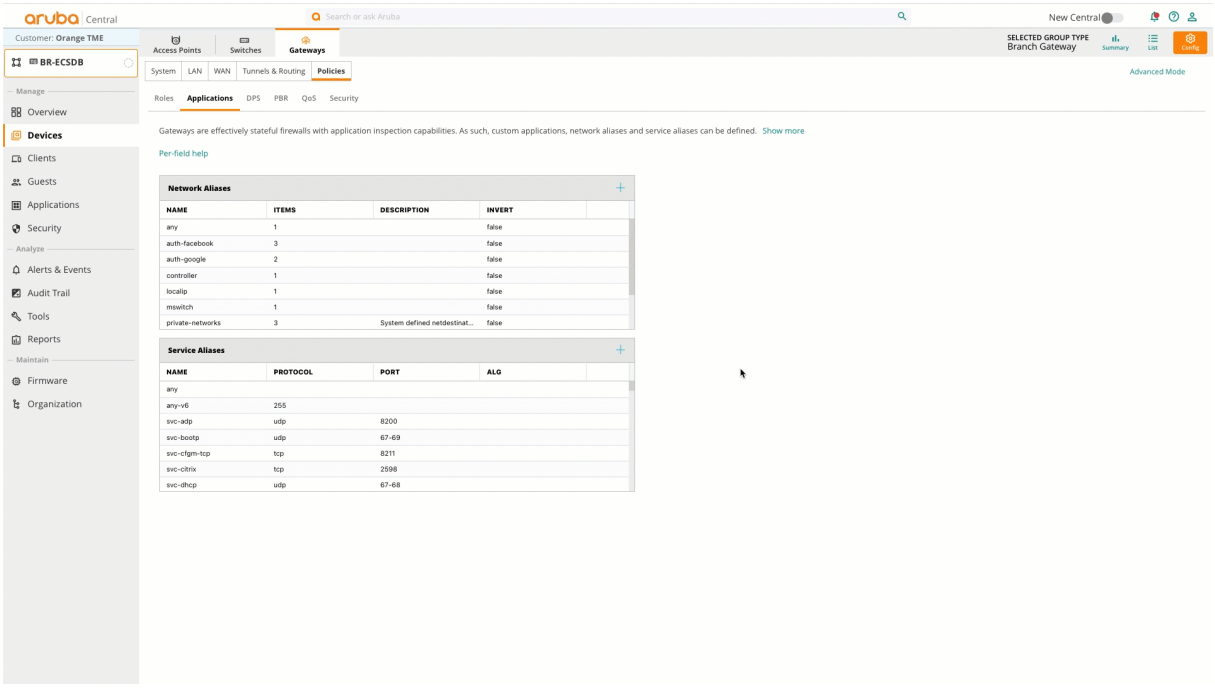


Figure 131: ad_network_alias

Step 7 Click the **+** (plus sign) beside **Network Aliases**. In the **Name** field, enter *rfc1918*.

Step 8 Click the **+** (plus sign) in the **User Rules** table.

Step 9 In the new row's **Type Column**, click **Name**. Scroll to select **Network**. Enter the first range, then repeat step 8 for the remaining ranges.

- IP/Mask: 192.168.0.0/255.255.0.0
- IP/Mask: 172.16.0.0/255.240.0.0
- IP/Mask: 10.0.0.0/255.0.0.0

Step 10 Click **Save**.

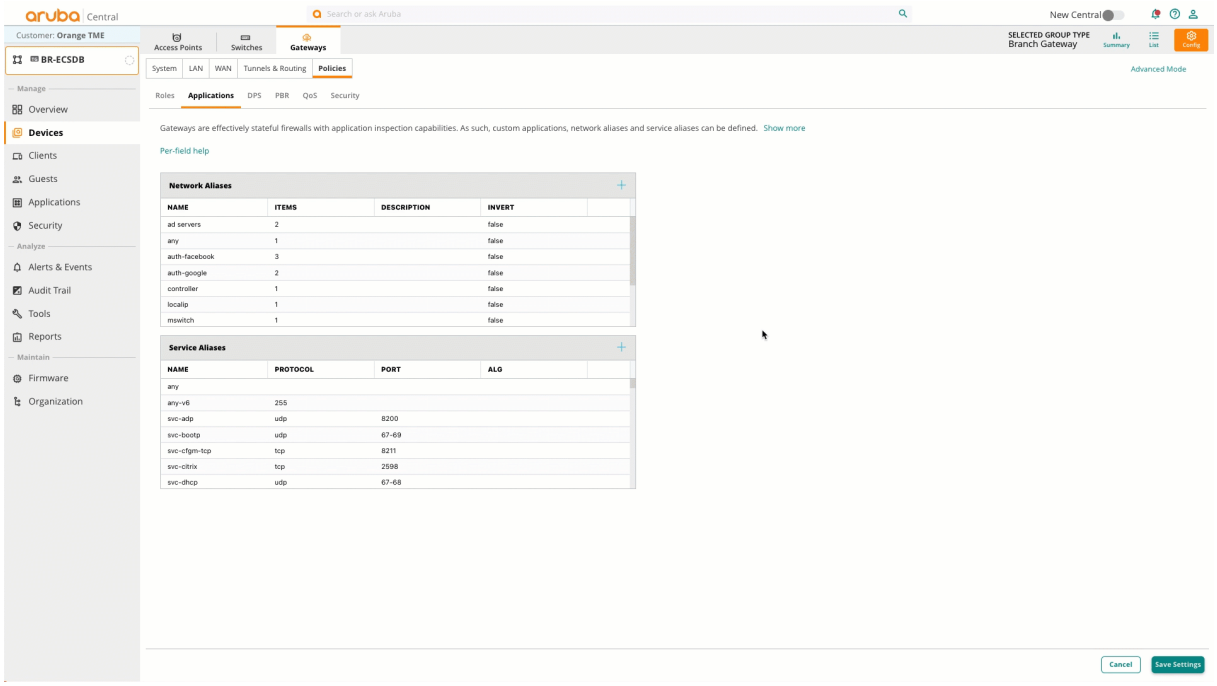


Figure 132: RFC1918

Step 11 Click the "**+** (plus sign) beside **Network Aliases**. In the **Name** field, enter *captive portal*.

Step 12 Click the **+** (plus sign) in the **User Rules** table.

Step 13 With the **Name** field selected, enter *cppm.example.local*

Step 14 Click **Save**.

Step 15 Click **Save Settings**.

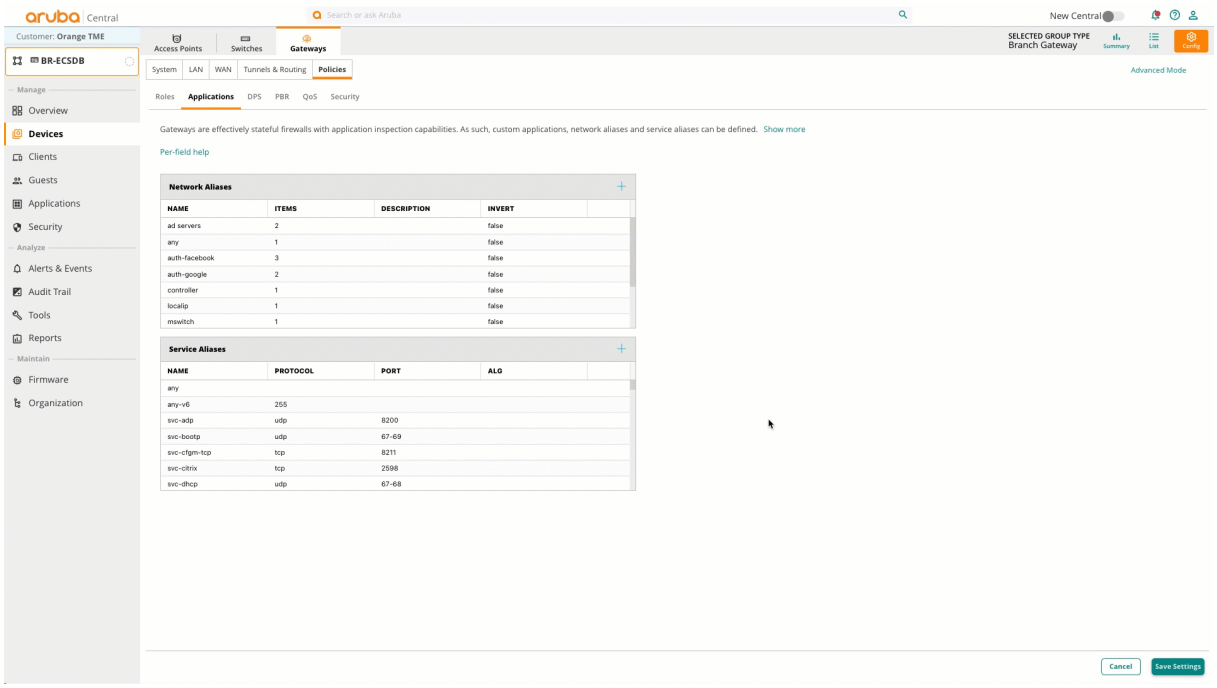


Figure 133: url rule

Step 16 Click the **Security** tab next to **QOS**.

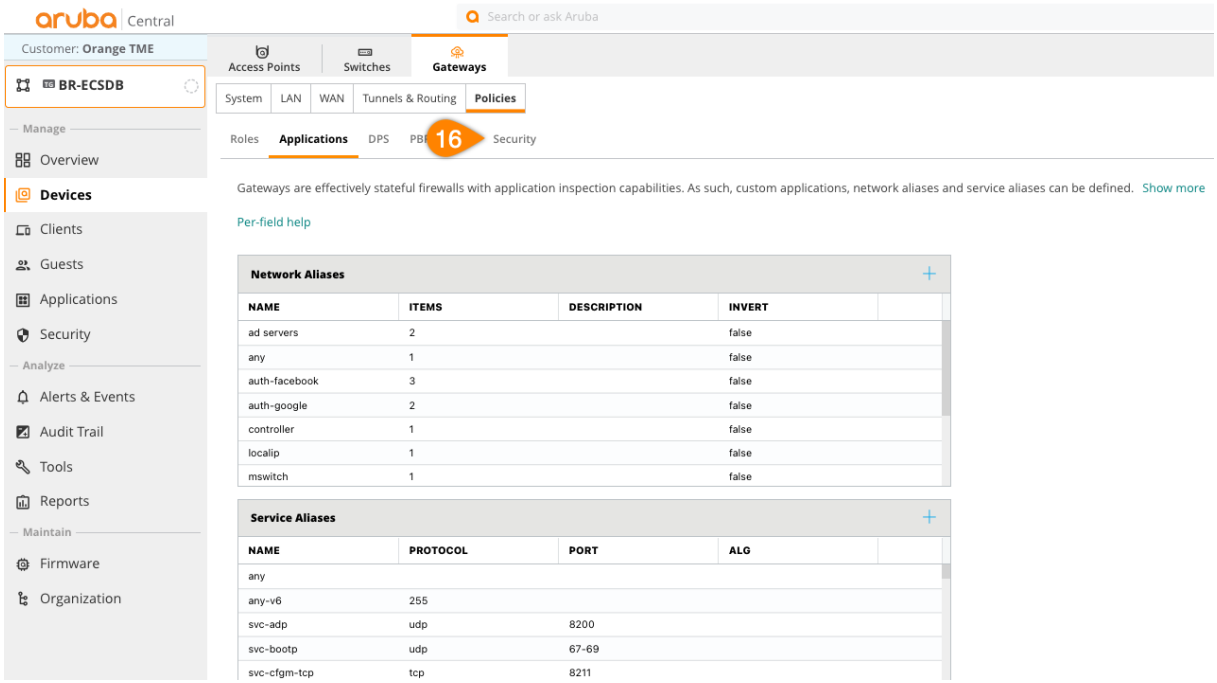


Figure 134: navigation_to_apply_rules

Step 17 In the **Roles** table, select the **Visitor** role.

Step 18 In the **Policies** table click the **+** (plus sign) symbol and enter *visitor_net_policy*.

NOTE:

The Visitor user role was created using global client roles. If the user role was not created using global client roles or if the deployment is not using multi site fabric, the User role can be created in the group by clicking the **Roles** tab on the page below.

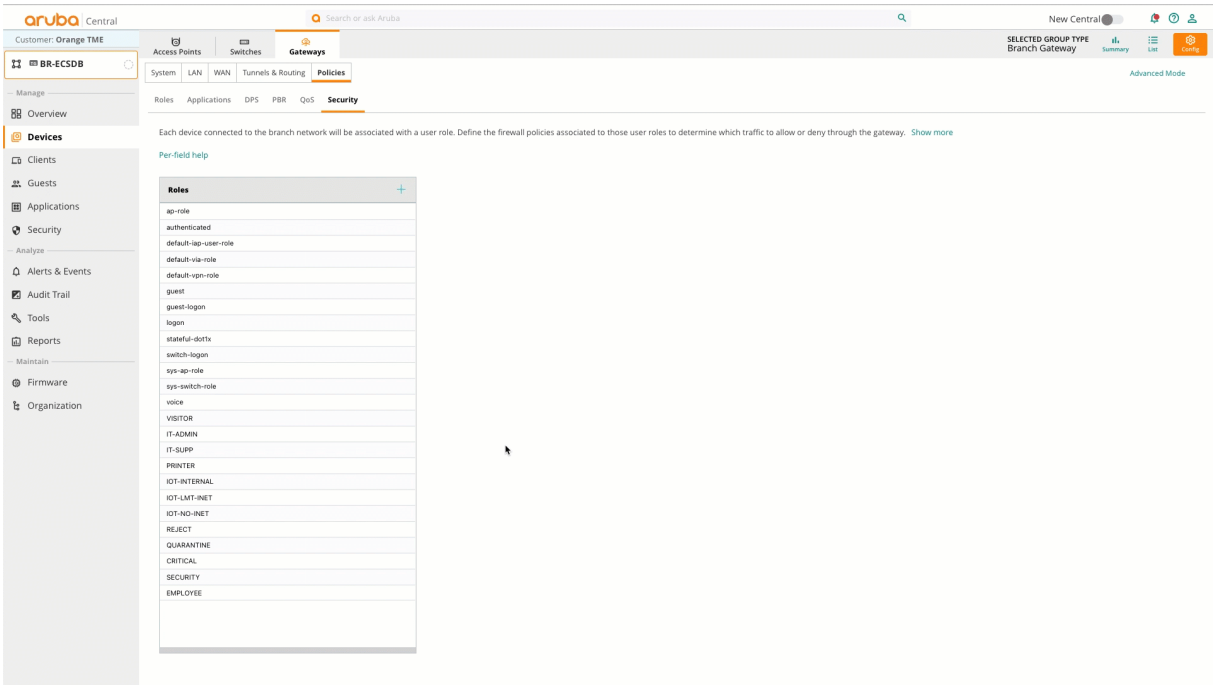


Figure 135: Create visitor policy

Step 20 In the **Rules** table click the **+** (plus sign) to create a new rule.

Step 21 In the **Rule** table, assign the following:

- **Source:** *Any*
- **Destination:** *Network Alias*
- **Destination Alias:** *ad server*
- **Service/App:** *sys-svc-dns*
- **Action:** *Permit*

Step 22 Click **Save**.

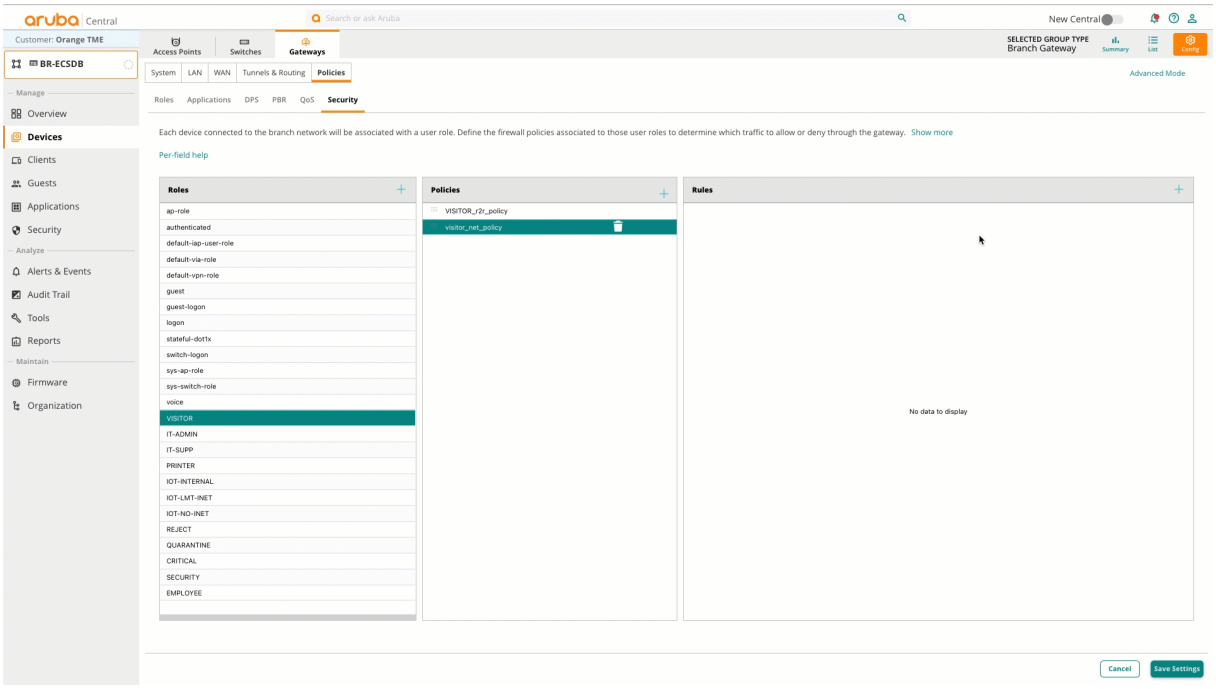


Figure 136: adding rules to policy

Step 23 Repeat Steps 18 to 20 to complete the table below. Then click **Save Settings**. The completed policy is illustrated below.

Source	Destination	Service	Action
Any	AD Servers	DNS	Permit
Any	AD Servers	DHCP	Permit
Any	Captive Portal	Https	Permit
Any	RFC1918	Any	Deny
Any	Any	Any	Permit

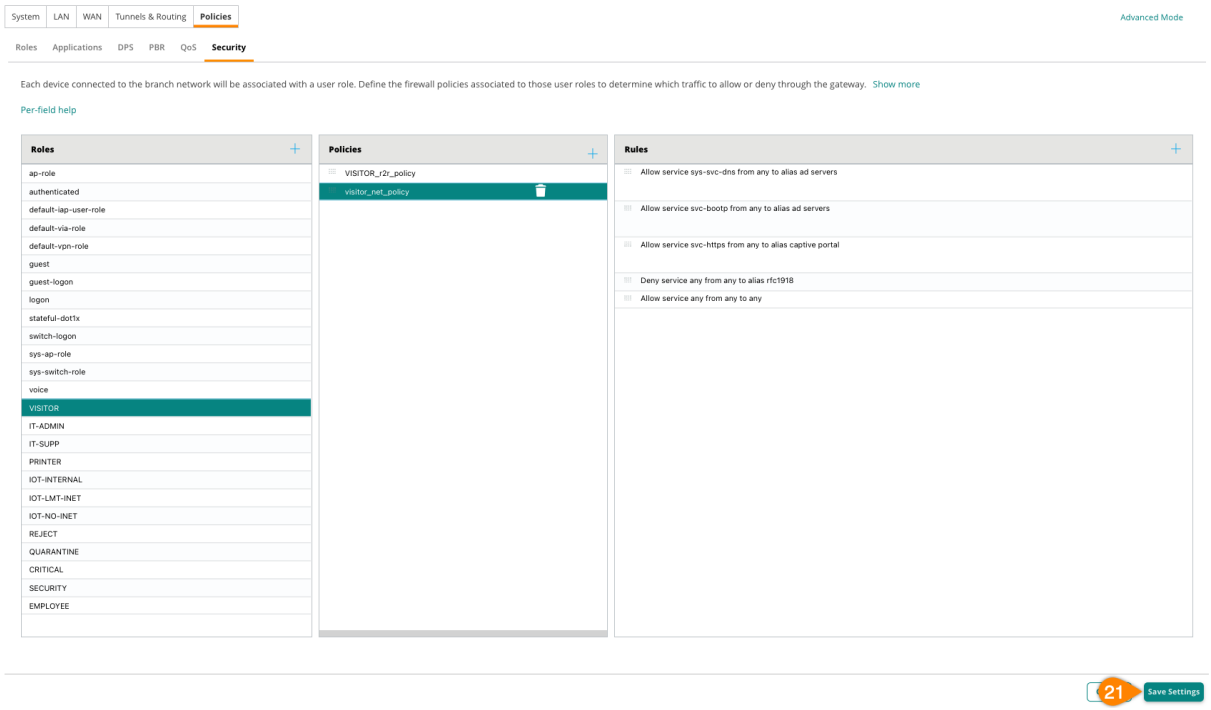


Figure 137: complete visitor policy-5016929

Summary

Successful flow of information is critical for a well-run organization.

The Aruba SD-Branch design is a prescriptive solution based on best practice and tested topologies. SD-Branch facilitates building a robust WAN network to accommodates the organization's network requirements.

For users located at a headend site or at a smaller branch site, the design provides a consistent set of features and functions for reliable network access, improving user satisfaction and productivity while reducing operational expense.

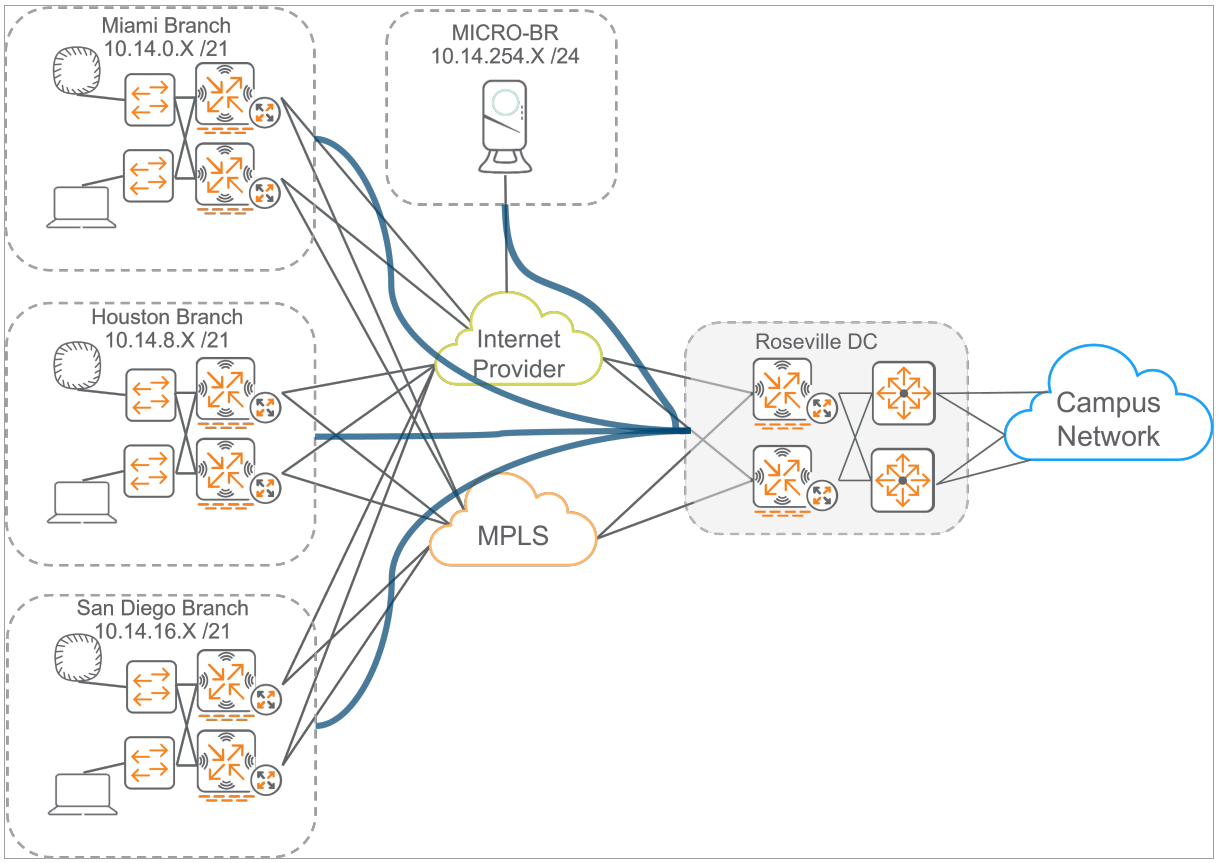


Figure 138: Network_Overview

The Aruba SD-Branch design provides a consistent and scalable method of building the network, improving overall usable network bandwidth and resilience, and making the WAN easier to deploy, maintain, and troubleshoot.

Aruba Microbranch

The Microbranch architecture provides remote teleworkers and small branches with wireless connectivity and secure access to corporate resources.

Zero Touch Provisioning (ZTP) simplifies Microbranch deployment, requiring only an Internet connection to provision an AP, upgrade firmware, and deploy configuration through Aruba Central.

Microbranch supports three SSID operating models:

- **Routed Layer 3 SSIDs** optimize traffic patterns, while allowing access to internal corporate resources.
- **NATed Layer 3 SSIDs** provide access to Internet services, but do not allow access to the internal corporate network.
- **Layer 2 Tunneled SSIDs** forward all traffic to the data center VPNC, including Internet traffic. Note that tunneling Layer 2 traffic may introduce suboptimal traffic patterns.

Organizational requirements at Microbranch locations should be considered before choosing a deployment model. The following sections demonstrate how to configure a Microbranch AP in all three modes.

Aruba Layer 3 Microbranch AP Configuration

Layer 3 Microbranch also referred to as Distributed Layer 3 (DL3). Allows admins the ability to provide three different types of access, Routed Layer 3, Nated Layer 3 and Fully-tunneled access. This guide will demonstrate, all three types of access.

Full Tunnel uses Policy based routing and will be shown as a optional section of the guide.

This guide demonstrates how to configure two types of Microbranch SSIDs:

- *EXAMPLE-CORP* is a Routed Layer 3 SSID that provides access to corporate resources. It is assigned VLAN ID 101 and prefix 10.14.200.0/24, which is advertised to the broader campus network.
- *EXAMPLE-GUEST* is a NATed Layer 3 SSID that provides only Internet access. It is assigned VLAN 100 and prefix 192.168.0.0/24, which is only routed locally.

NOTE:

This guide uses the VPNC configured in the hub & spoke section. To configure a VPNC, review the “Deploying VPNC” section.

The illustration below shows the Microbranch topology.

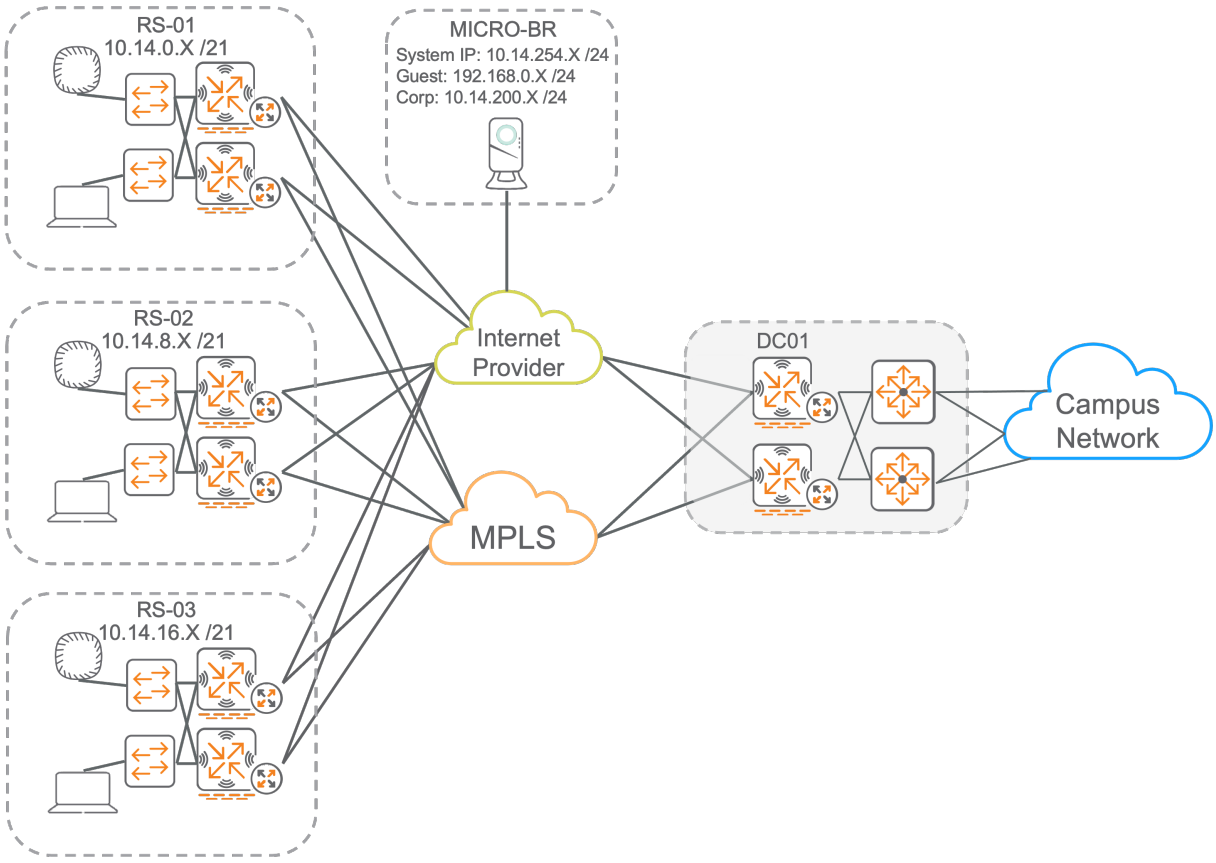


Figure 139: Micro-Branch

Create a Microbranch AP Group

Step 1 In the left navigation pane, in the **Maintain** section, select **Organization**.

Step 2 In the left navigation pane, click **Global**, then select the **Groups** column heading.

Step 3 To create a **New Group**, in the upper right, click **+** (plus sign).

Step 4 In the **Add Group** window, enter a name, click the **Access Point** checkbox, then click **Next**.

Step 5 Leave *ArubaOS 10* selected in **Architecture for access points and gateways in this group**. Click the **Microbranch** radio button under **Network role of the access points in this group**, then click **Add**.

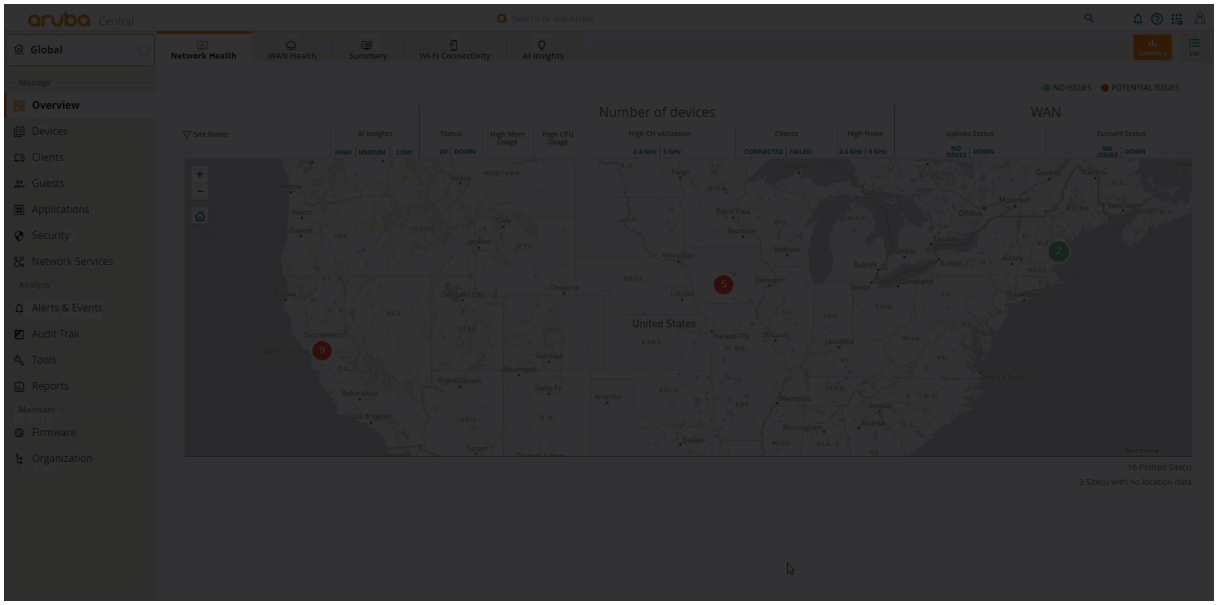


Figure 140: Creating AP Group

Configure System IP Pool

The System IP Pool assigns IP addresses to access points dynamically, as required for Microbranch AP setup.

APs use their assigned IP for the inner tunnel IP address and to source traffic such as RADIUS, TACACS+, and SNMP. The System IP Pool is applied to the Microbranch group in a future step.

Step 1 Select the **Global** group. In the left navigation pane, click **Network Services**.

Step 2 Select the **IP Address Manager** tab.

Step 3 In the upper right, click **+** (plus sign).

Step 4 In the **Add System IP Pools** window, enter the following: - **Pool Name:** *System IP Pool* - **Start address:** *10.14.254.1* - **End address:** *10.14.254.100*

Step 5 Click **Save**.

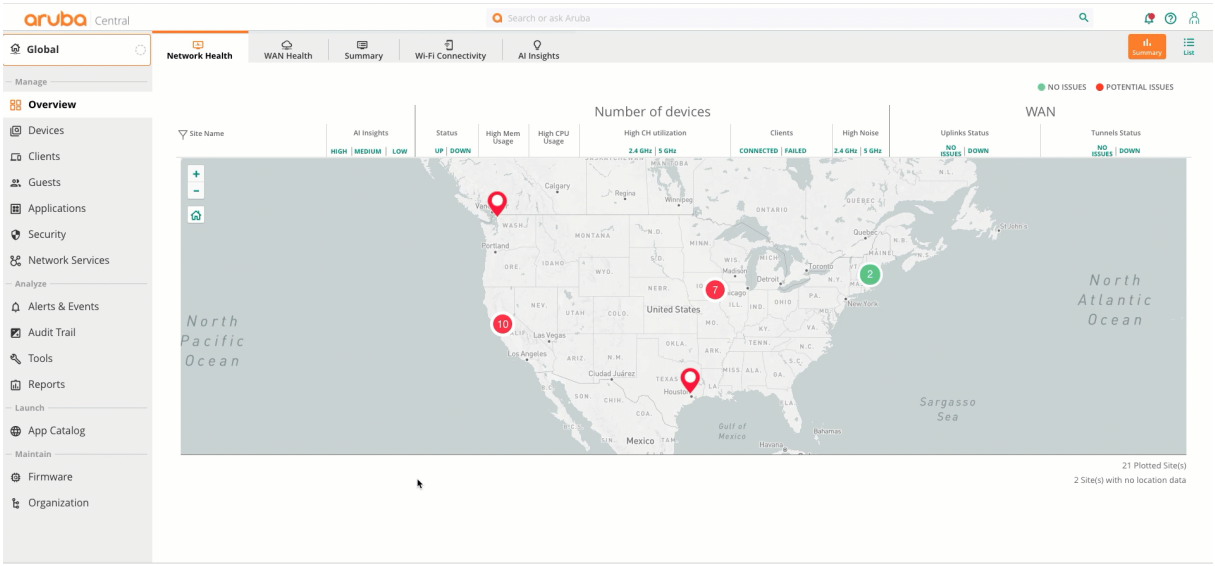


Figure 141: Configuring Address Pool

Configure VLAN DHCP Pool

A **Shared DHCP Pool** is configured for later assignment to the *EXAMPLE-CORP* VLAN.

Step 1 Select the **Global** group. In the left navigation pane, select **Network Services**.

Step 2 Select the **IP Address Manager** tab, then select the **Shared DHCP Pools** tab.

Step 3 To create a DHCP pool, in the upper right, click **+** (plus sign).

Step 4 In the **Add Shared DHCP Pool** window, enter the following: - **Pool Name:** *EXAMPLE-CORP* - **Start address:** *10.14.200.1* - **End address:** *10.14.200.255* - **Hosts per DHCP VLAN:** *20*

Step 5 Click **Save**.

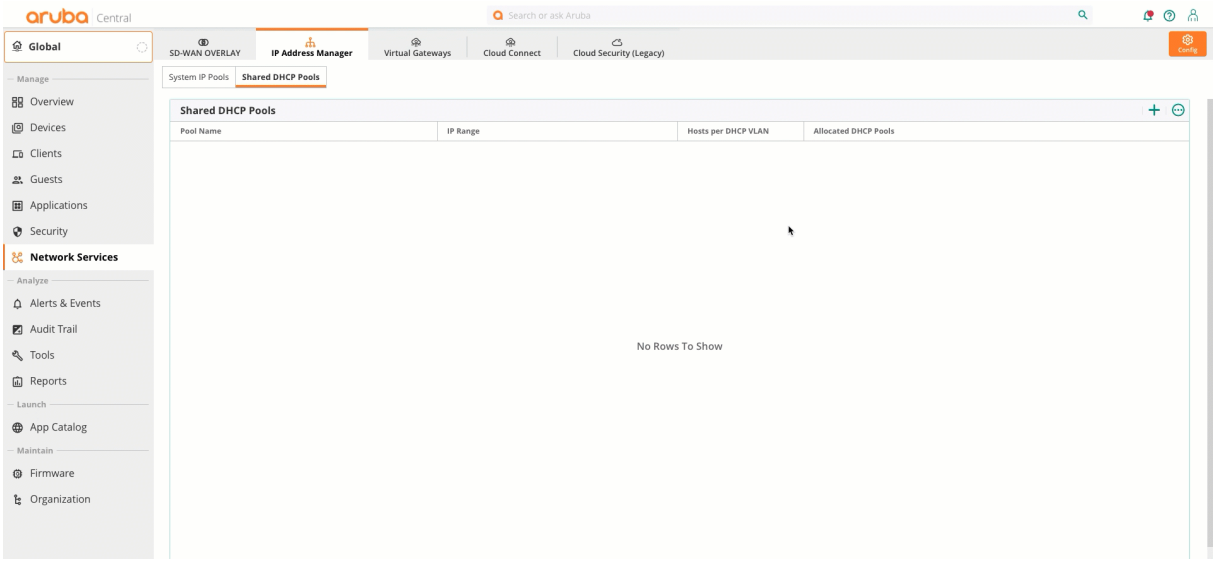


Figure 142: Configuring Shared DHCP Pools

Set AP Device Password

Step 1 In the **Global** dropdown, search and select the Microbranch AP group created previously.

Step 2 In the left navigation pane under **Manage**, select **Devices**.

Step 3 Select the **Access Points** tab. In the upper right corner, click the **Config** (gear) icon.

Step 4 Enter a device password in the **Password** field, re-enter the password in the **Confirm password** field, then click **Set Password**.

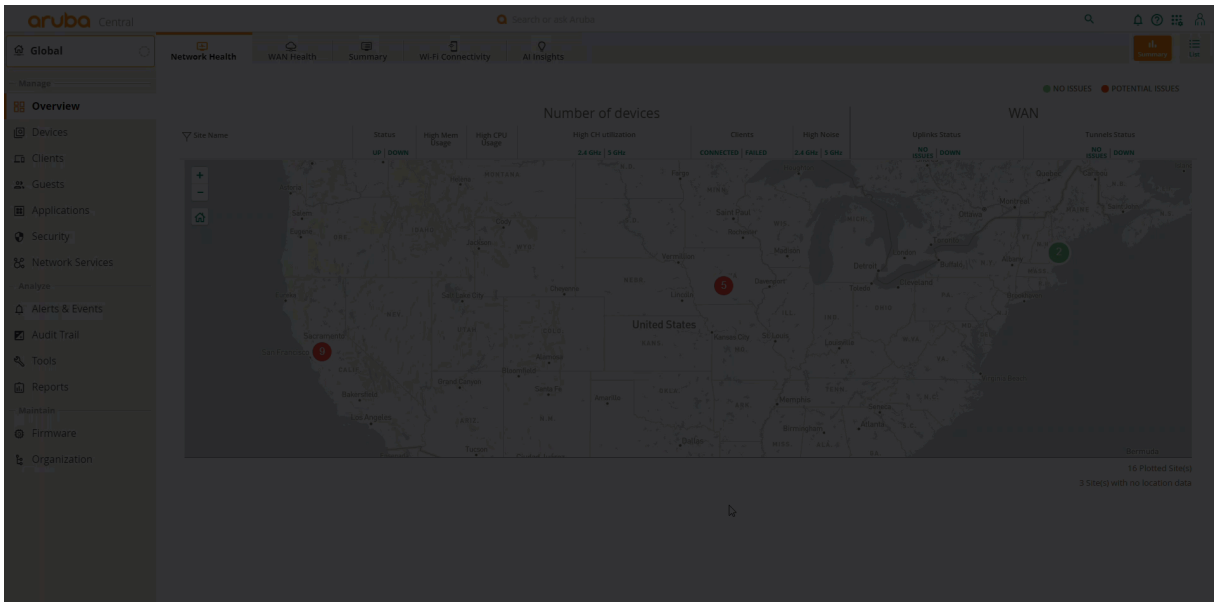


Figure 143: AP Group Navigation

Configure Country Code

It is important to assign the proper country code to ensure that APs operate in compliance with local regulatory restrictions.

Step 1 In the **UI-MICRO-AP-01 > Devices** configuration panel, in the **System** tile, select **Properties**.

Step 2 In the **Set country code** field, select the appropriate country code from the dropdown.

Step 3 Click **Save**.

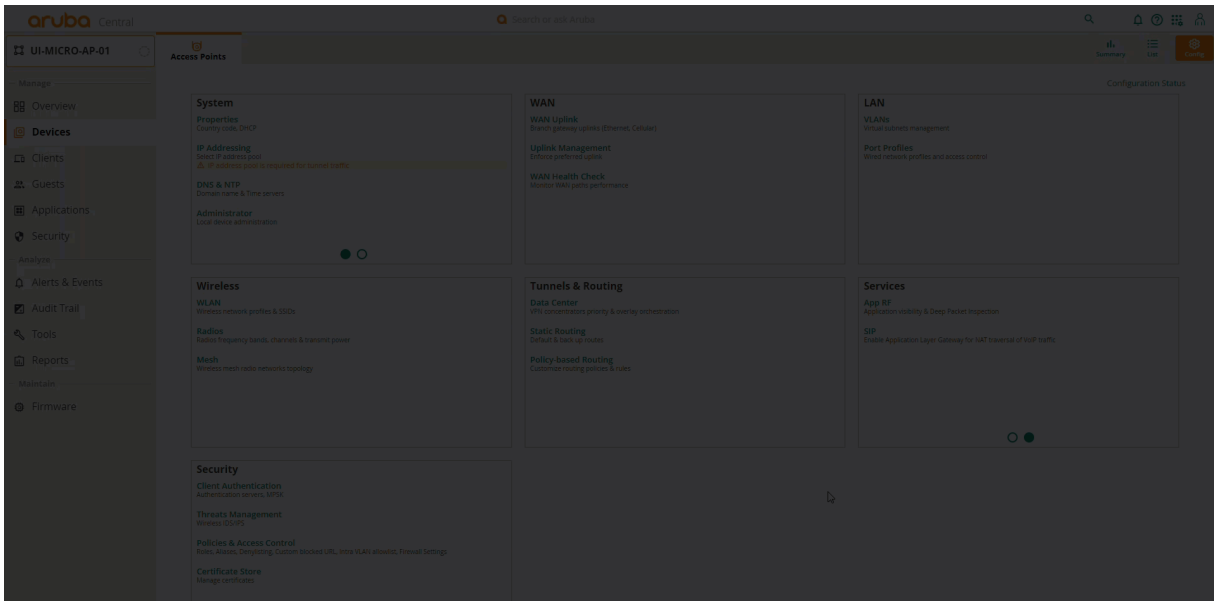


Figure 144: configuring Country Code

Assign System IP Pool to AP Group

Step 1 In the **UI-MICRO-AP-01 > Devices** configuration panel, in the **System** tile, select **IP Addressing**.

Step 2 Click **+** (plus sign).

Step 3 In the **Select IP Address Pool** field, select the previously configured *System IP Pool*.

Step 4 Click **Save**.

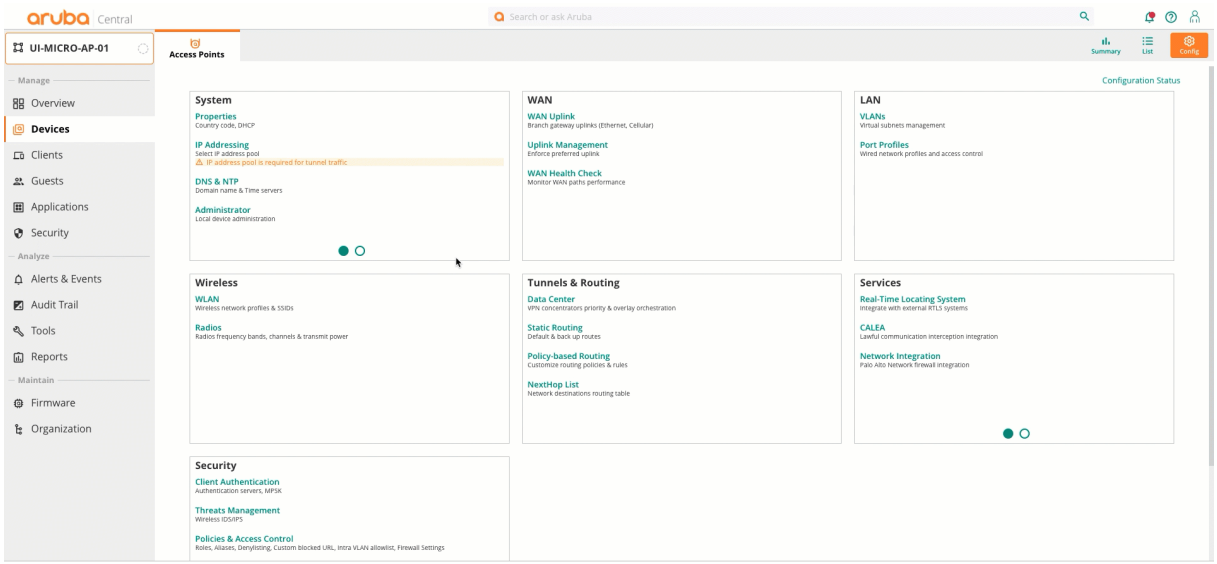


Figure 145: SystemIP Pool

Configure DNS and NTP

Step 1 In the **UI-MICRO-AP-01 > Devices** configuration panel, in the **System** tile, select **DNS & NTP**.

Step 2 In the **Domain Name** field, enter the domain name.

Step 3 To add a DNS server, in the **DNS SERVERS** header, click **+** (plus sign).

Step 4 In the dropdown, select a DNS service.

Step 5 Click **Save**.

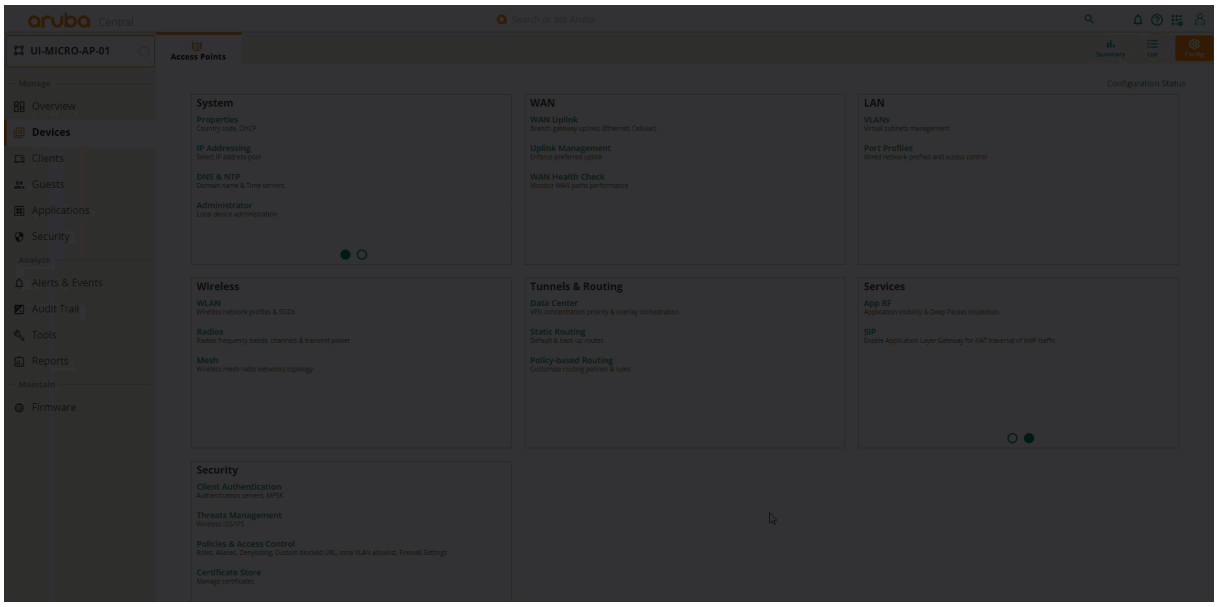


Figure 146: Configuring DNS

Step 6 Expand the **NTP** section, and click **> NTP**.

Step 7 To add a NTP server, in the **PUBLIC NTP SERVERS** header, click **+** (plus sign).

Step 8 In the new empty field, enter an **NTP** server name or IP address.

Step 9 In the **Timezone** field, select a timezone from the dropdown.

Step 10 Click **Save**.

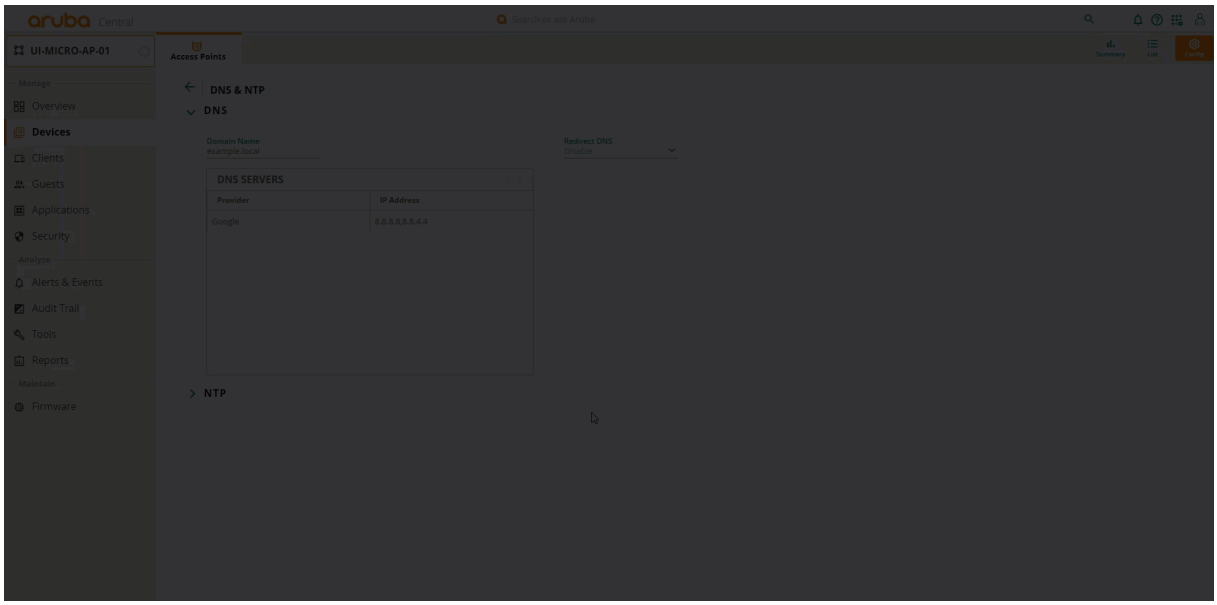


Figure 147: Configuring NTP

Configure WAN Uplink

The WAN uplink identifies the interface assigned a WAN IP address. Tunnel Orchestrator uses this WAN IP address to create tunnels between devices.

Step 1 In the **UI-MICRO-AP-01 > Devices** configuration panel, in the **WAN** tile, select **WAN Uplink**.

Step 2 On the right side, click **+** (plus sign).

Step 3 In the **Uplink Name**, enter the uplink interface name.

Step 4 Click **Save**.

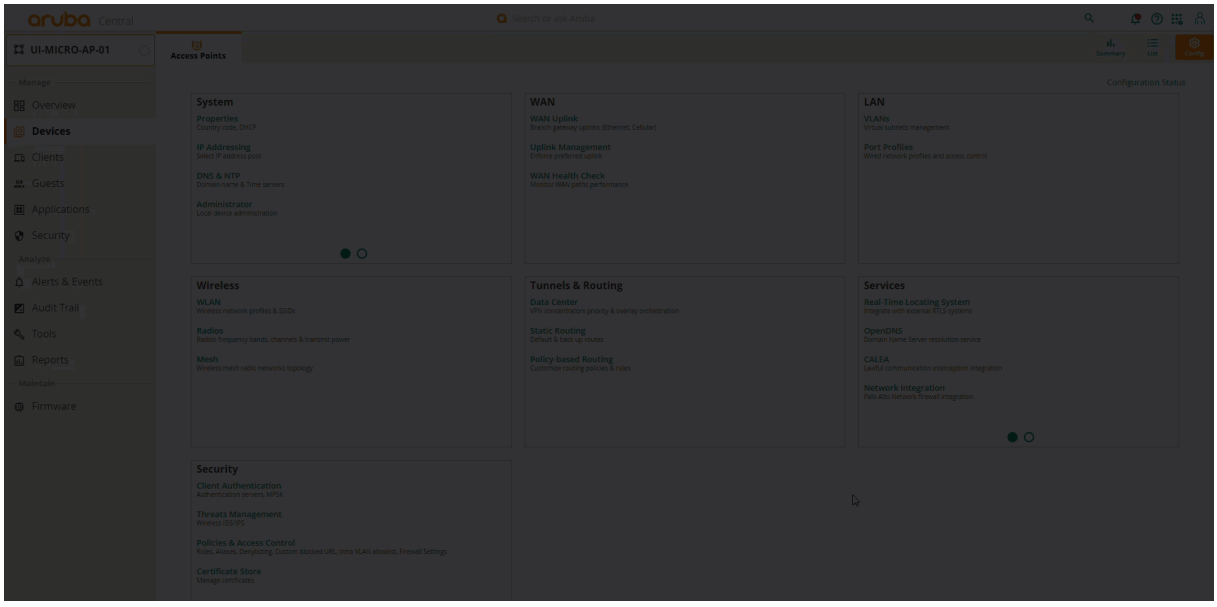


Figure 148: Config

Configure WAN Health Check

A WAN Health Check measures latency and packet loss on WAN uplinks using ICMP or UDP probes. UDP-based probes add measurement of jitter and generation of MoS scores.

Step 1 Go to the **UI-MICRO-AP-01 > Devices** configuration panel, in the **WAN * tile, select** WAN Health Check**.

Step 2 Click the slider right of **Monitor WAN health**.

Step 3 Click the **Custom** radio button.

Step 4 In the **Protocol** field, click the dropdown and select **UDP**.

Step 5 Click **Save**.

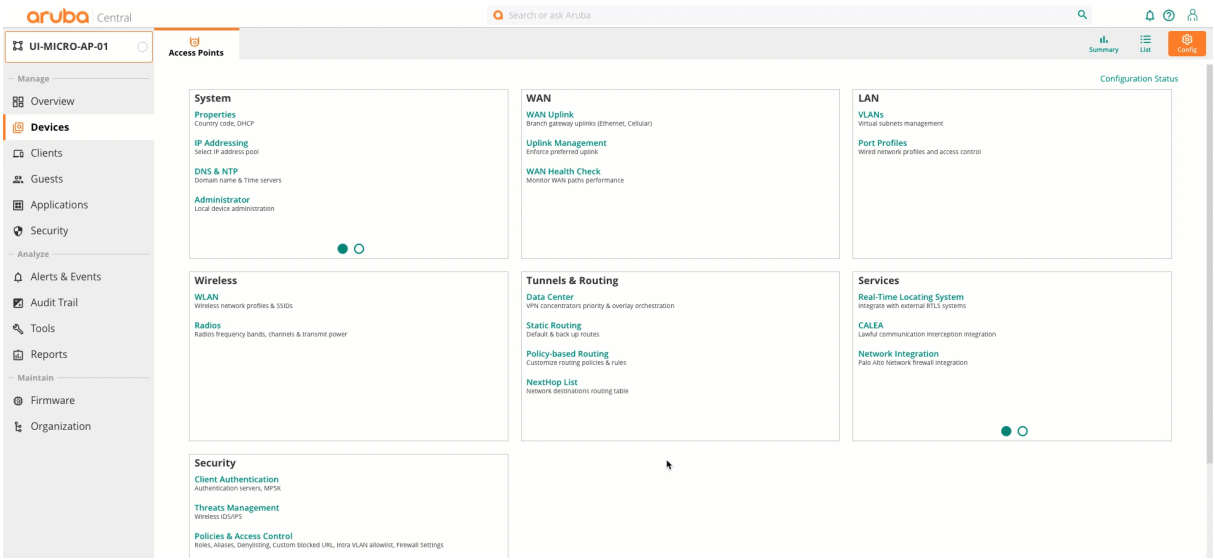


Figure 149: Configuring WAN Health Check

Configure Hub Site

Step 1 Go to the **UI-MICRO-AP-01 > Devices** configuration panel. In the **Tunnels & Routing** tile, select **Data Center**.

Step 2 In the **Data Center** header, click **+** (plus sign).

Step 3 In the **HUB GROUP** dropdown, select the VPNC Group configured in *Hub and Spoke Deployment*.

Step 4 In the **Cluster Name** dropdown, select the cluster configured in *Hub and Spoke Deployment*.

Step 5 Click **Save**.

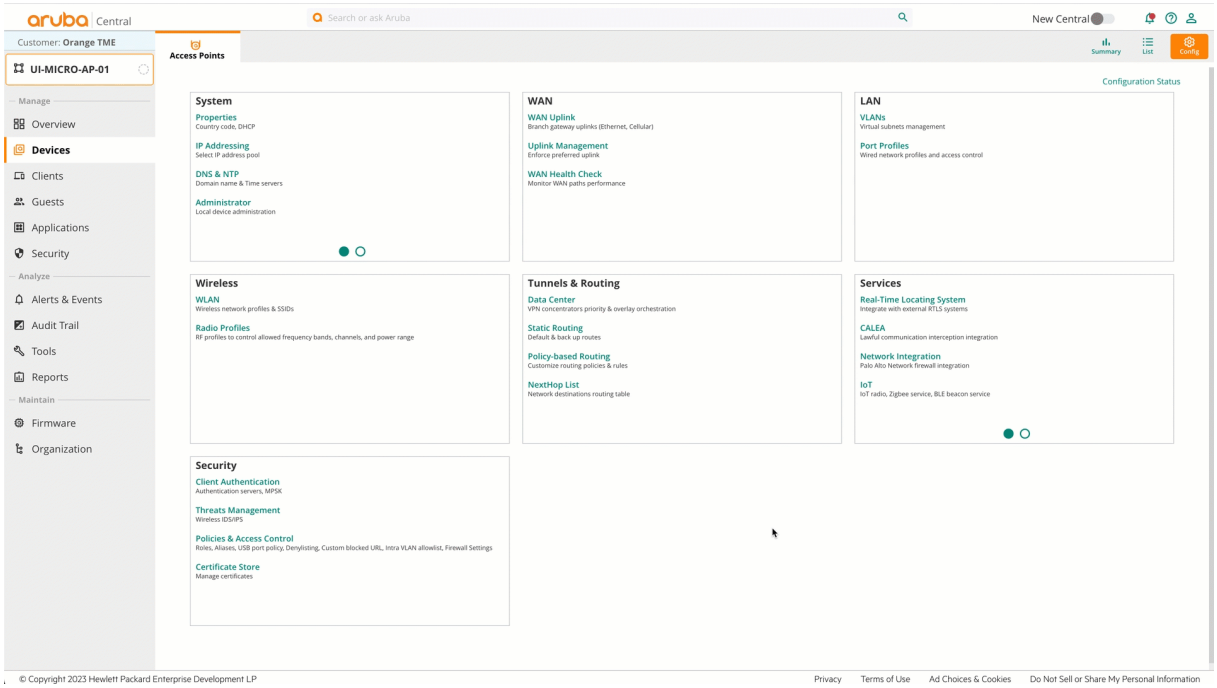


Figure 150: configure_hub-8257684

Configure VLANs

Create VLANs for the route *EXAMPLE-CORP* SSID and the *EXAMPLE-GUEST* SSID.

Step 1 Go to the **UI-MICRO-AP-01 > Devices** configuration panel, in the **LAN** tile, select **VLANs**.

Step 2 In the **VLANs** header, click **+** (plus sign).

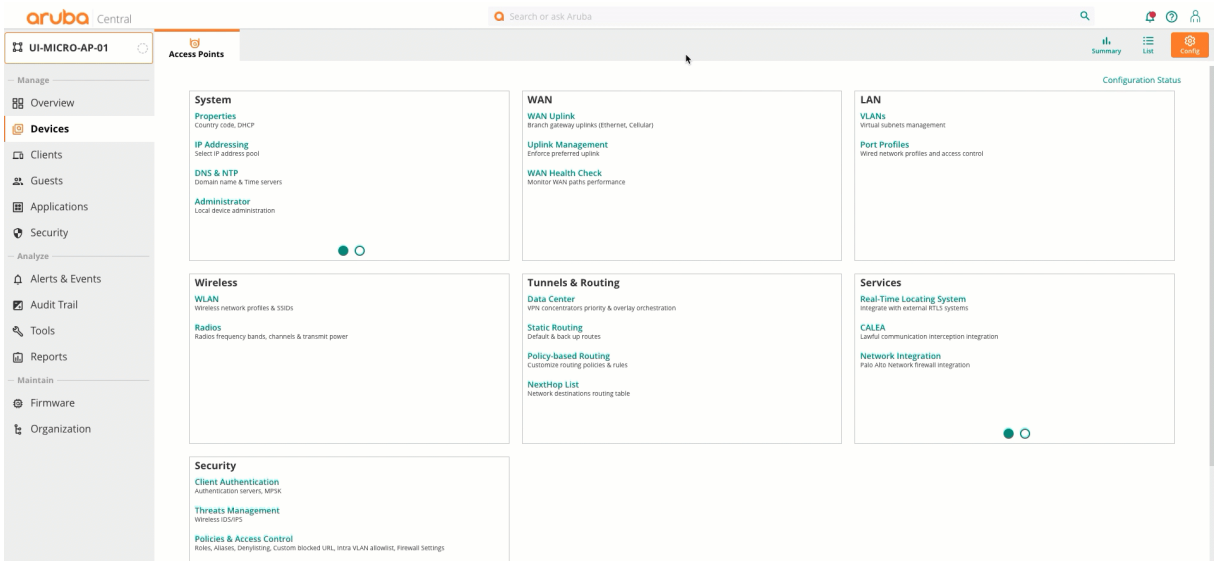


Figure 151: Navigating to VLAN Creation

CAUTION:

Do not use the same VLAN ID at a Microbranch site and on the VPNC. If the same VLAN ID is configured on both, a Layer 2 tunneled SSID is created operationally, even if the configuration specifies Layer 3 Routed or NATed.

Step 3 In the new VLAN form, enter the following field values. - **DHCP Profile Name:** *EXAMPLE-CORP* - **VLAN ID:** *101* - Click the **Routed** radio button - **DHCP Pool:** *EXAMPLE-CORP* - **Excluded addresses:** *5* - **Domain name:** *example.local* - **DNS Server:** *Specify Servers - 10.2.120.98,10.2.120.99*

Step 4 Leave other fields at their default values.

Step 5 Click **Save**.

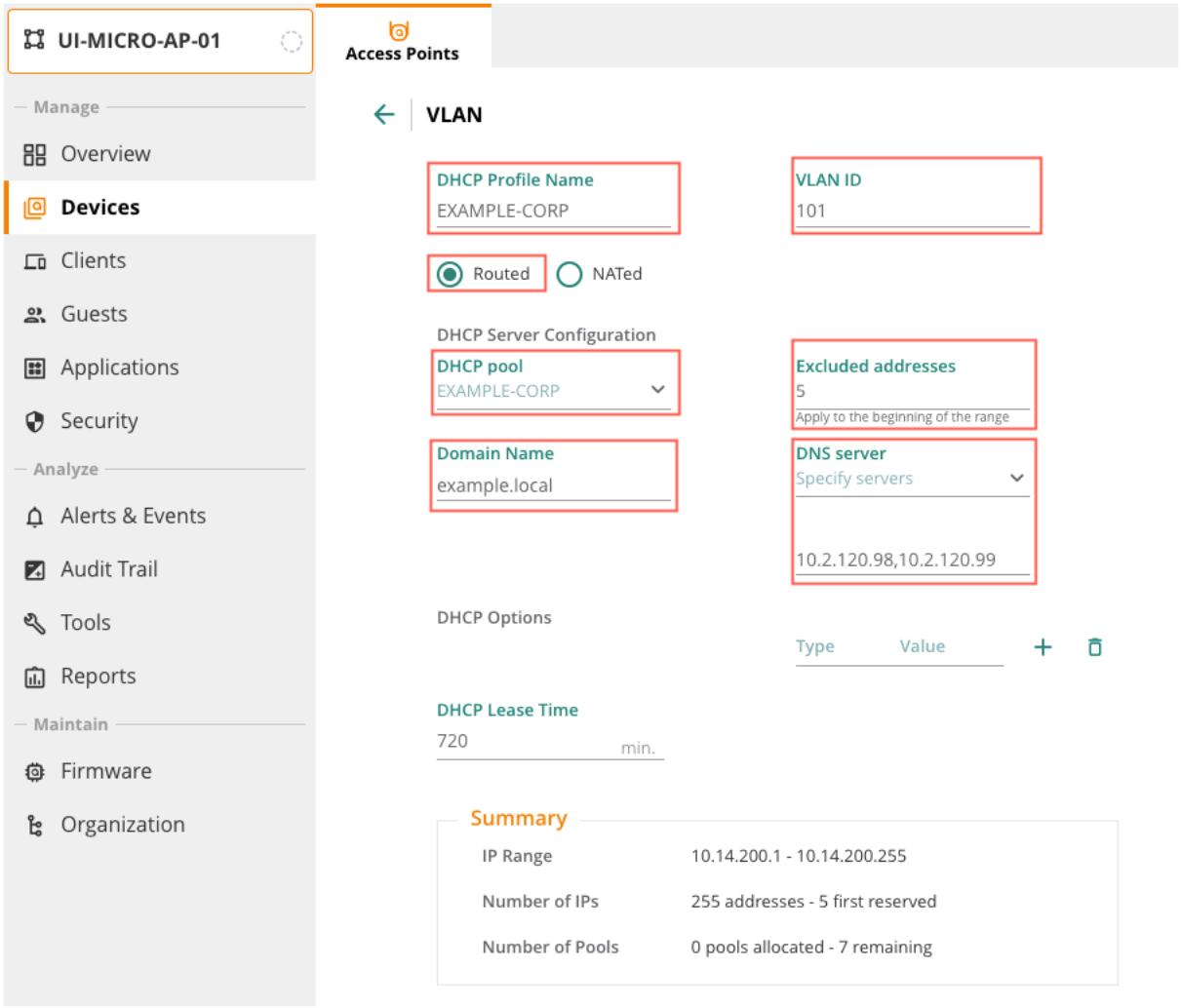


Figure 152: Configure Example Corp VLAN

Step 6 In the **VLANs** header, click **+** (plus sign).

Step 7 In the new VLAN window, enter the following field values.

- **DHCP Profile Name:** *EXAMPLE-GUEST*
- **VLAN ID:** *100*

- Click the **NATed** radio button
- **Subnet:** *192.168.0.0*
- **Subnet Mask:** *255.255.255.0*
- **Domain name**: *example.local*
- **DNS Server:** *AP Assigned DNS Server*
- **Excluded addresses:** *5*

Step 8 Leave other fields at their default values.

Step 9 Click **Save**.

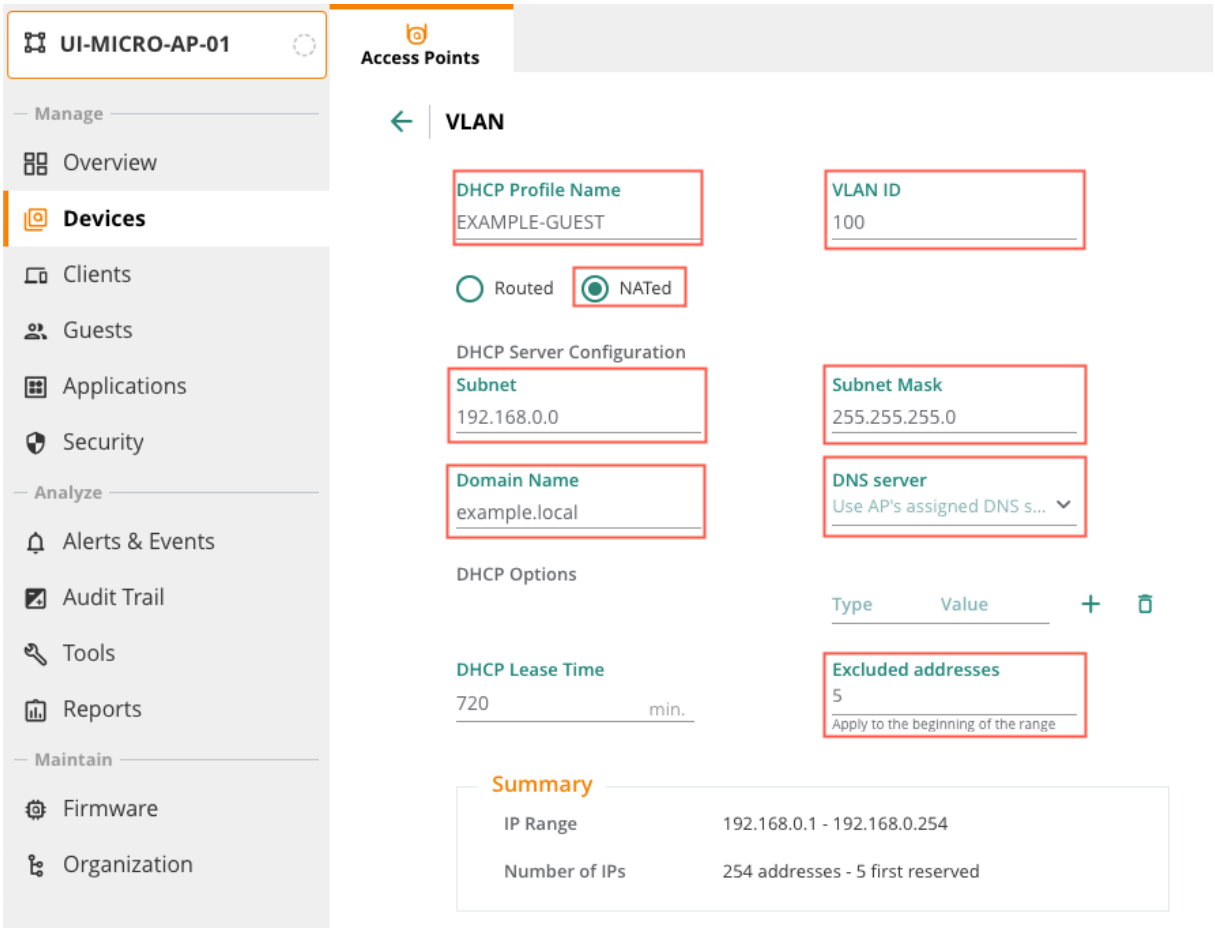


Figure 153: Configure Example Guest VLAN

Configure the WPA3-Enterprise Wireless LAN

The following procedure creates a secure, routed SSID for accessing internal resources.

Step 1 Go to the **UI-MICRO-AP-01 > Devices** configuration panel. In the **Wireless** tile, select **WLAN**.

Step 2 Near the bottom left of the **WLANs** tab, click **+ Add SSID**.

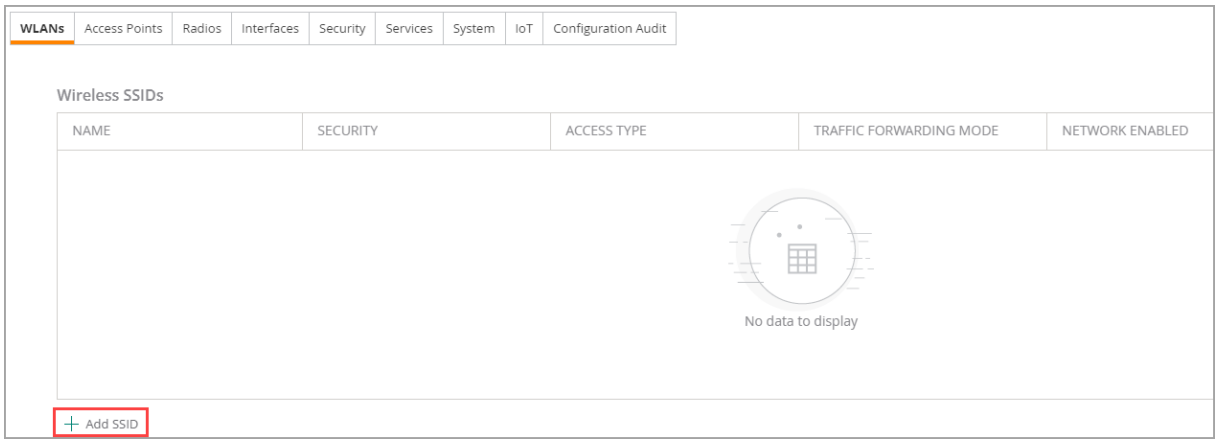


Figure 154: Add SSID

Step 3 On the **General** tab, set the **SSID Name** field to *EXAMPLE-CORP*.

Step 4 To display additional settings, click **> Advanced Settings**.

Step 5 To expand broadcast/multicast options, click **(+) Broadcast/Multicast**.

Step 6 In the **Broadcast filtering** dropdown, select *All*.

Step 7 To expand legacy transmission rate options, click **(+) Transmit Rates (Legacy Only)**.

Step 8 In the **2.4 GHz** section, set the following values. - **Min:** *5* - **Max:** *54*

Step 9 In the **5 GHz** section, set the following values. - **Min:** *18* - **Max:** *54*

Step 10 Click **Next**.

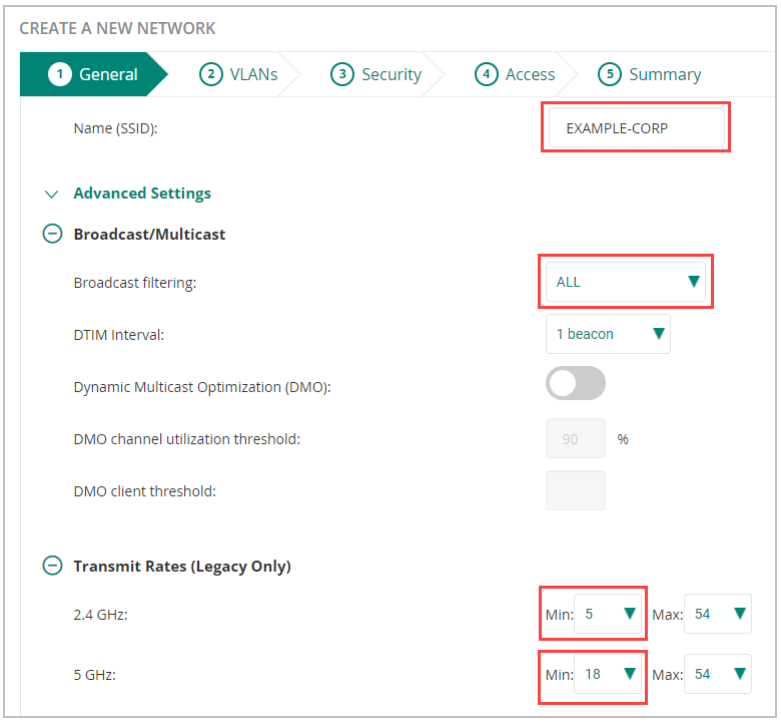


Figure 155: General Configuration

Configure SSID VLAN

On the VLANs tab, enter the following values, then click **Next**. - **Traffic forwarding mode:** *L3 Routed/-NATed*. - **Client VLAN Assignment:** *Static* - **VLAN ID**: *EXAMPLE-CORP (vlan:101)*

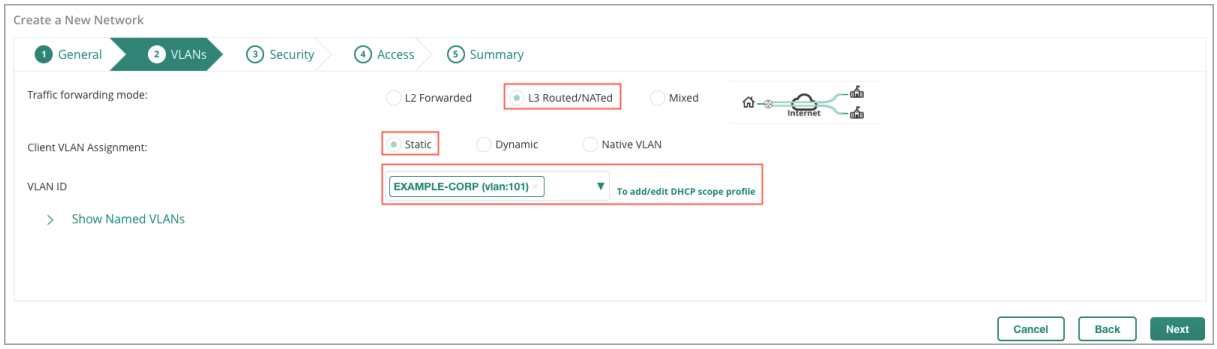


Figure 156: Setting VLAN

Configure SSID Security Settings

Enable 802.1X authentication and encryption on the SSID.

Step 1 To set the security level, move the **Security Level** slider to *Enterprise*.

Step 2 From the **Key Management** dropdown, select *WPA3 Enterprise(CMM 128)*.

CAUTION:

Use WPA3 when possible to benefit from significant security improvements over WPA2. Consult endpoint documentation to confirm that Microbranch devices support WPA3. If devices do not support WPA3, use WPA2-Enterprise.

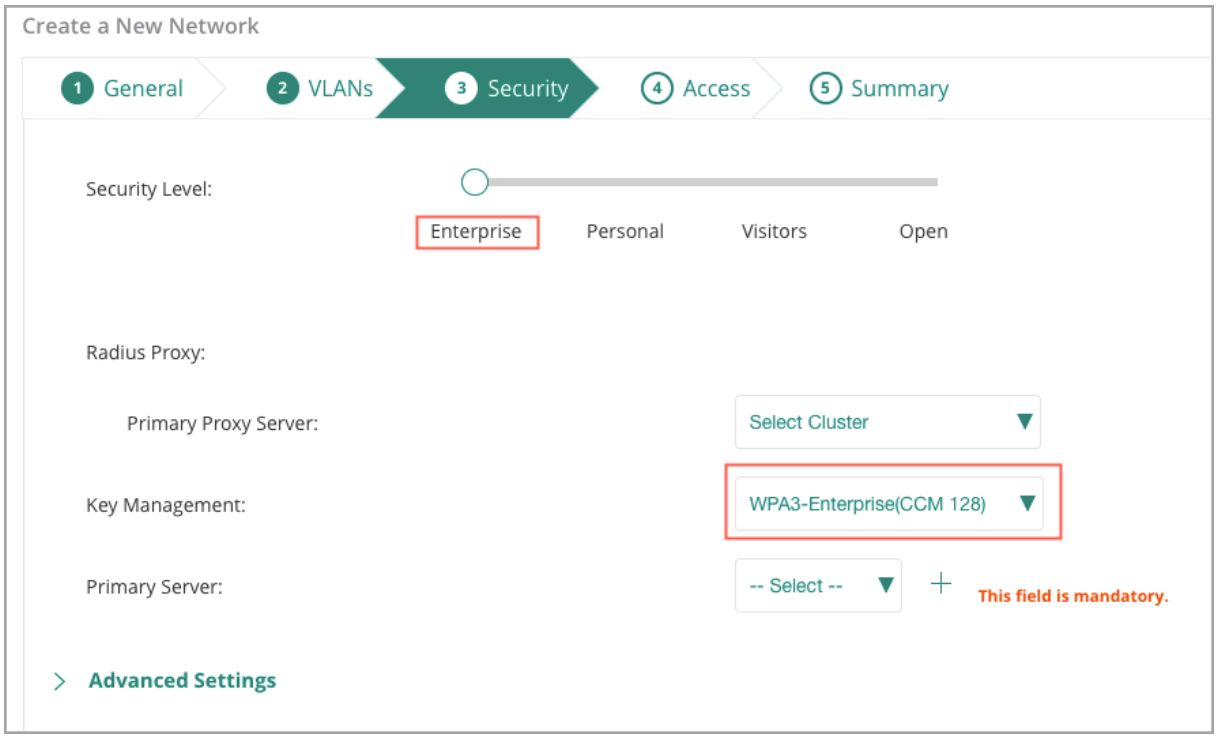


Figure 157: Enabling dot1x

Step 3 To add a primary RADIUS server, beside the **Primary Server** field, click **+** (plus sign).

Step 4 In the **NEW SERVER** window, enter the following values, then click **OK**.

- **Server Type:** *RADIUS*
- **Name:** *cppm-01*
- **IP Address:** *10.2.120.94*
- **Shared Key:** *< Enter the RADIUS server shared key >*
- **Retype Key:** *< Re-enter the RADIUS server shared key >*

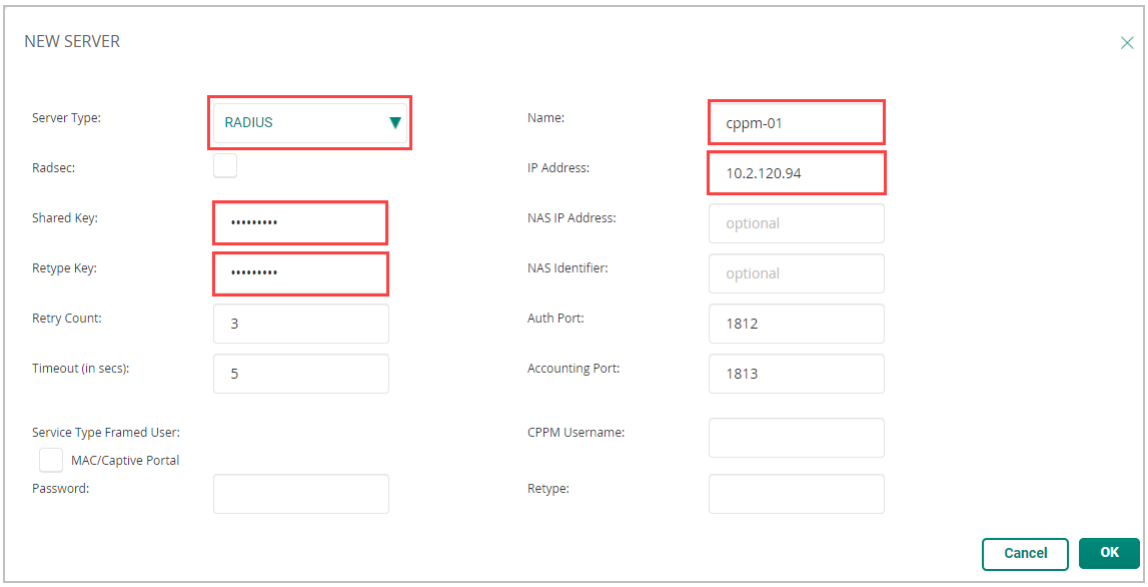


Figure 158: Adding Radius Server

NOTE:

It is important to record the **Shared Key** for use when configuring ClearPass Policy Manager.

Step 5 To add a secondary RADIUS server, beside the **Secondary Server** field, click **+** (plus sign).

Step 6 Repeat step 4 with appropriate values for the secondary RADIUS server.

Step 7 To enable **Load Balancing**, click the slider.

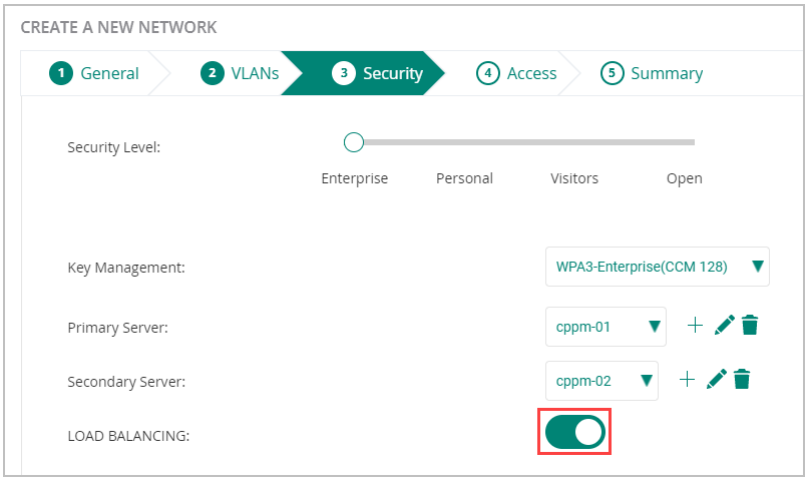
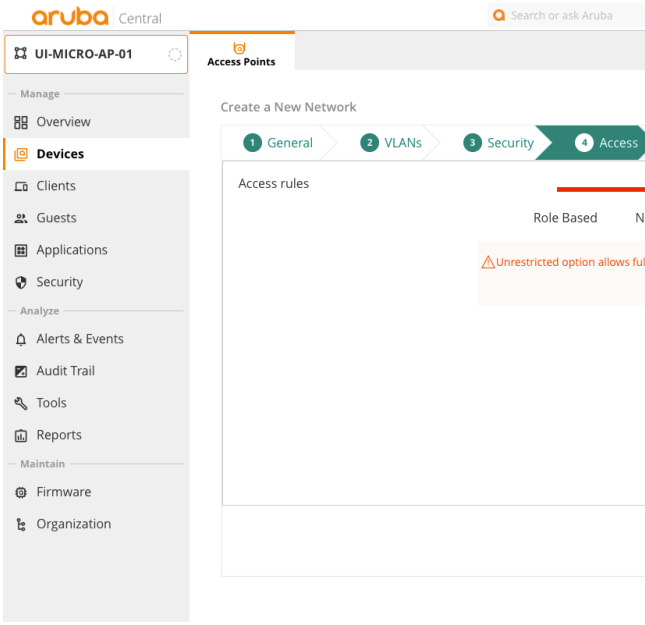


Figure 159: Enabling Load Balancing

Step 8 Click **Next**.

Configure Network Access Rules

Network access rules apply policy enforcement for an SSID based on the role or IP address of a device.



Step 1 Leave the default setting of **Unrestricted**, then click **Next**.

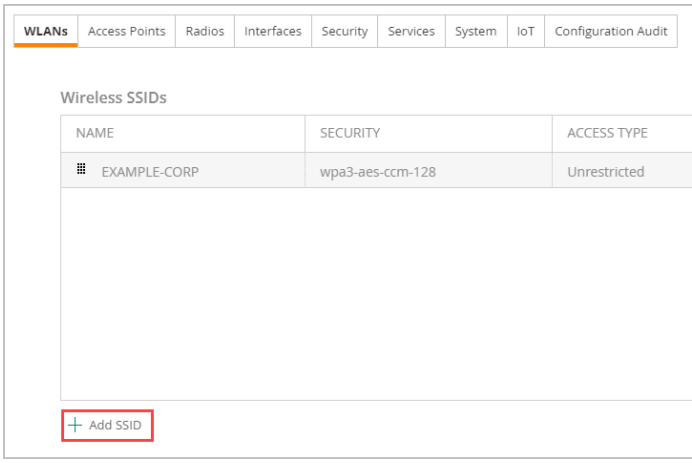
Step 2 On the **Summary** tab, review all settings and click **Finish**.

Configure the Visitor Wireless LAN

The following procedure creates a NATed SSID with a captive portal for guest Internet access.

Create Visitor SSID

Step 1 In the **UI-MICRO-AP-01 > Devices** configuration panel, in the **Wireless** tile, select **WLAN**.



Step 2 On the bottom left of the **WLANs** tab, click **+ Add SSID**.

Step 3 On the **General** tab, set the **SSID Name** field to *EXAMPLE-GUEST*.

Step 4 To display additional settings, click **> Advanced Settings**.

Step 5 To expand broadcast/multicast options, click **(+) Broadcast/Multicast**.

Step 6 In the **Broadcast filtering** dropdown, select *All*.

Step 7 To expand legacy transmission rate options, click **(+) Transmit Rates (Legacy Only)**.

Step 8 In the **2.4 GHz** section, set the following values. - **Min:** *5* - **Max:** *54*

Step 9 In the **5 GHz** section, set the following values. - **Min:** *18* - **Max:** *54*

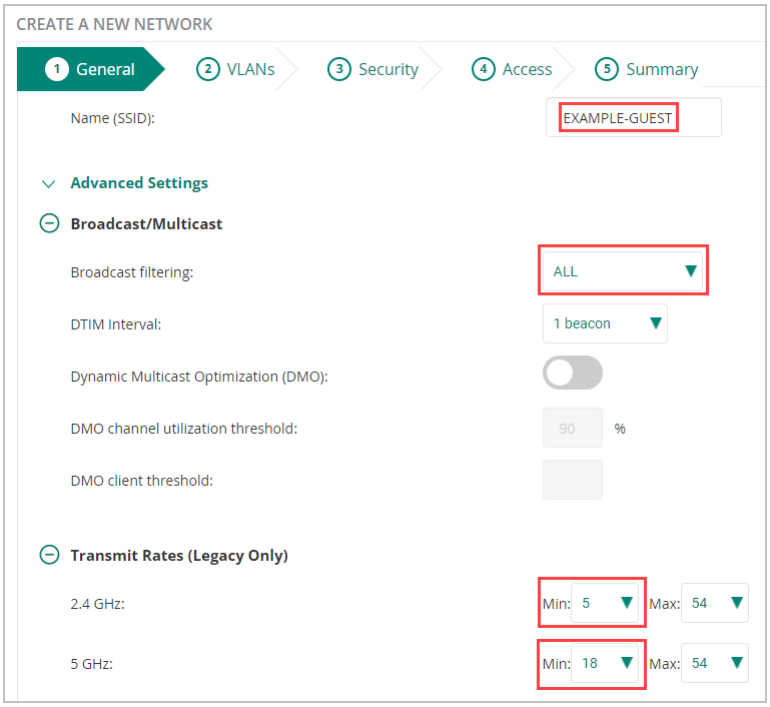


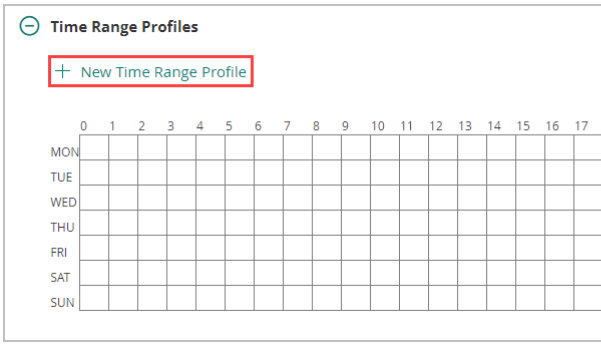
Figure 160: General SSID Configuration

NOTE:

Setting the time range for guest access is optional. Skip steps 11-14, if not applicable.

Step 10 Click **Next** to skip this configuration.

Step 12 To display time range options, click **(+) Time Range Profiles**.



Step 13 To create a new time range, click **+ New Time Range Profile**.

Step 14 In the **NEW PROFILE** window, enter the following values, then click **Save**.

- **Name:** *Guest Weekdays*
- **Type:** *Periodic*
- **Repeat:** *Daily*
- **Day Range:** *Monday - Friday (Weekdays)*
- **Start Time:**
  - **Hours:** *7*

  - **Minutes:** *0*

- **End Time:**
  - **Hours:** *18*
  - **Minutes:** *0*

- Click **Save**.

Figure 161: Configuring Time profile

Step 14 The new time range appears in the **Time Range Profiles** list. To enable the profile, click the **Status** dropdown beside the name, select **Enabled**, then click **Next**.

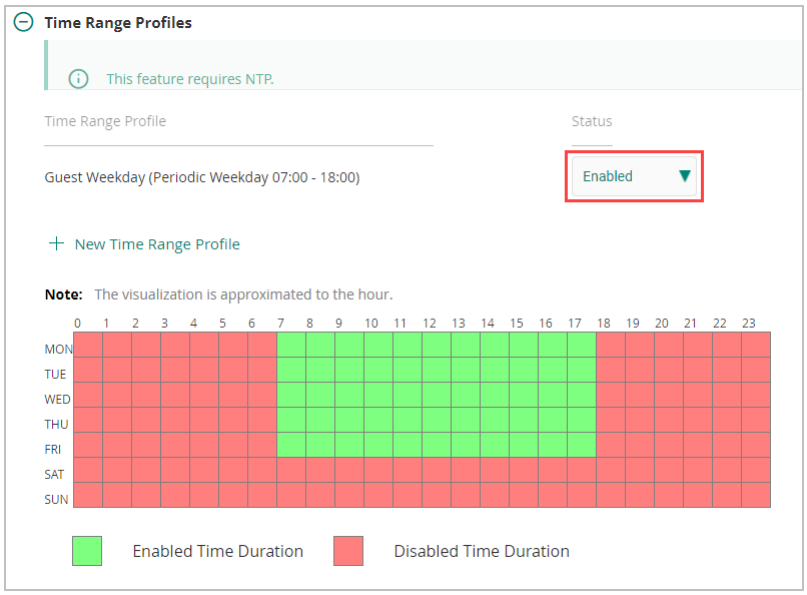
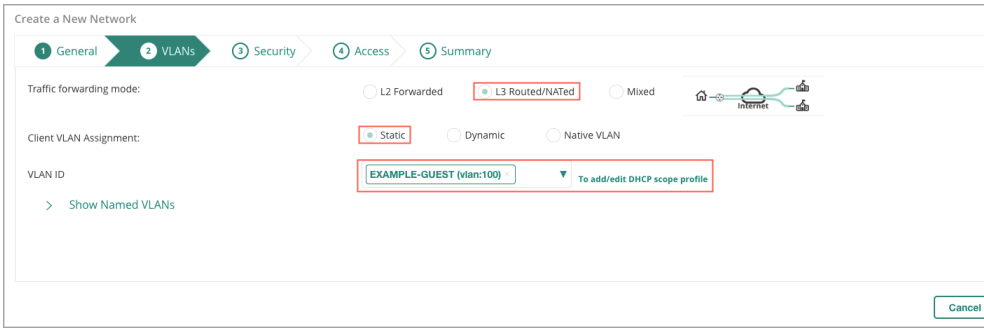


Figure 162: Enable Time profile

Configure VLANs

On the VLANs tab, enter the following values, then click **Next**.

- **Traffic Forwarding Mode:** *L3 Routed/NATed*.
- **Client VLAN Assignment:** *Static*
- **VLAN ID:** *Example-Guest(100)*



Configure Security

Enable a web-based captive portal.

Step 1 To set the security level, move the **Security Level** slider to **Visitors**.

Step 2 In the **Access Network** section, click the **Type** dropdown and select **External Captive Portal**.

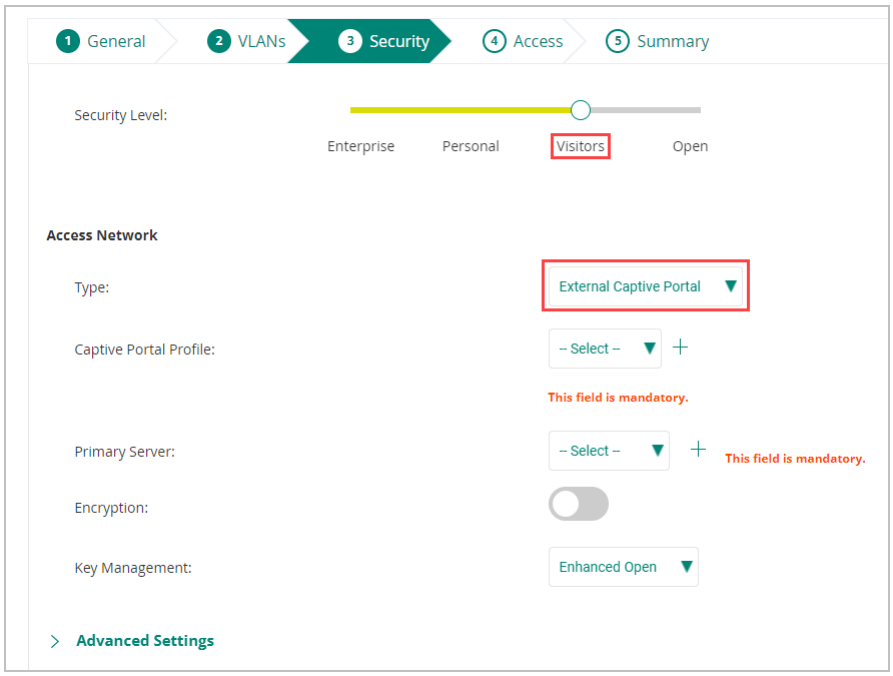


Figure 163: enable Captive portal

Step 2 To create a captive portal profile, click the **+** (plus sign) beside the **Captive Portal Profile** dropdown.

Step 3 In the **External Captive Portal-New** window, enter the following values, then click **OK**.

- **Name:** *CPPM-Portal*
- **IP or Hostname:** *10.2.120.92*
- **URL:** */guest/mb_guest_portal.php*
- **Port:** *443*
- **Redirect URL:** *http://arubanetworking.hpe.com*

CAUTION:

The **IP or Hostname** field cannot be set to an FQDN for Layer 3 NATed SSIDs. The DNS request from the AP will be NATed and cannot resolve the FQDN correctly.

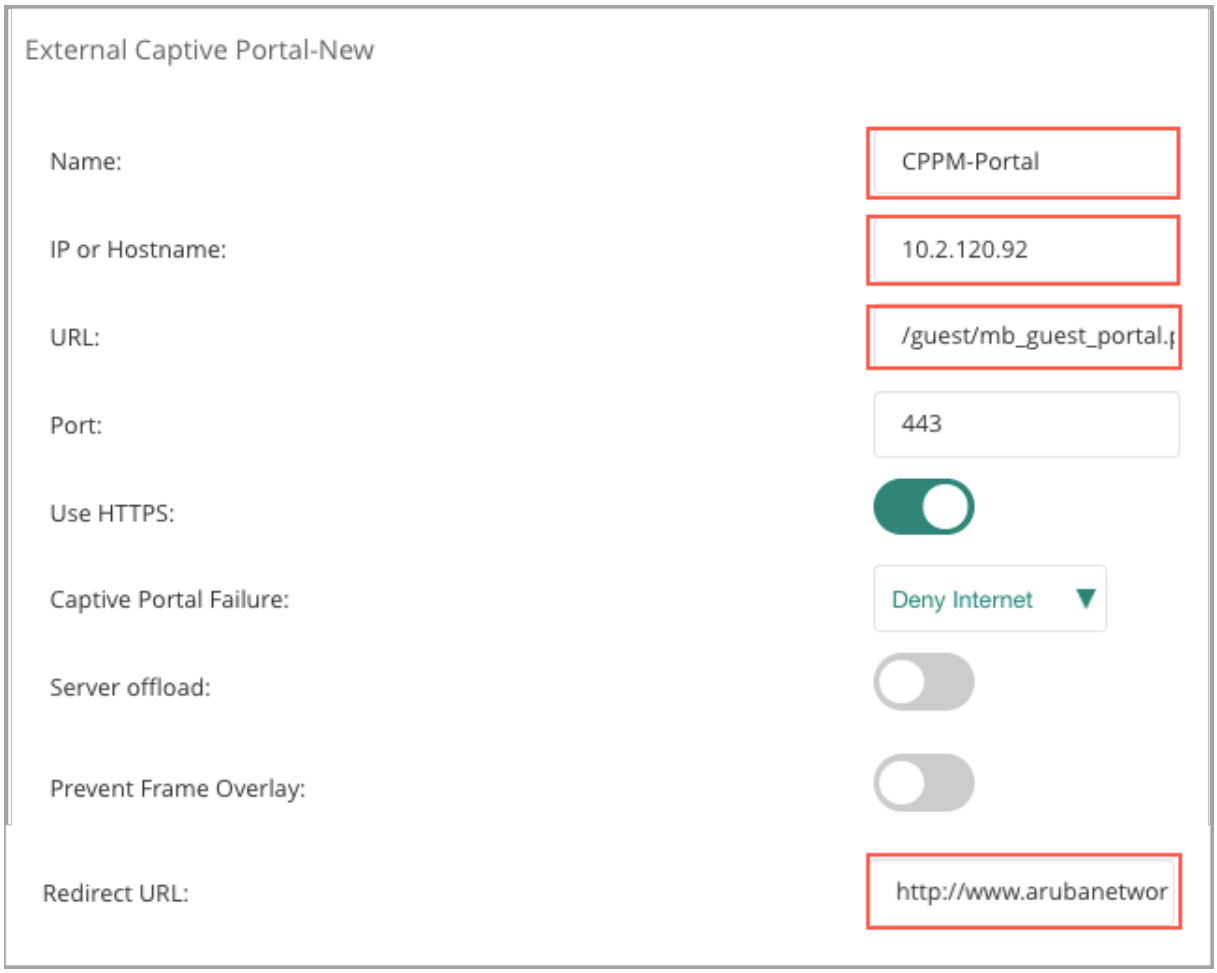


Figure 164: Captive Portal Configuration-2928543

Step 4 To set the primary RADIUS server, click the **Primary Server** dropdown and select the previously created primary RADIUS server.

Step 5 To set the secondary RADIUS server, click the **Secondary Server** dropdown and select the previously created secondary RADIUS server.

Step 6 To enable **Load Balancing**, toggle the slider.

Step 7 Click **Next**.

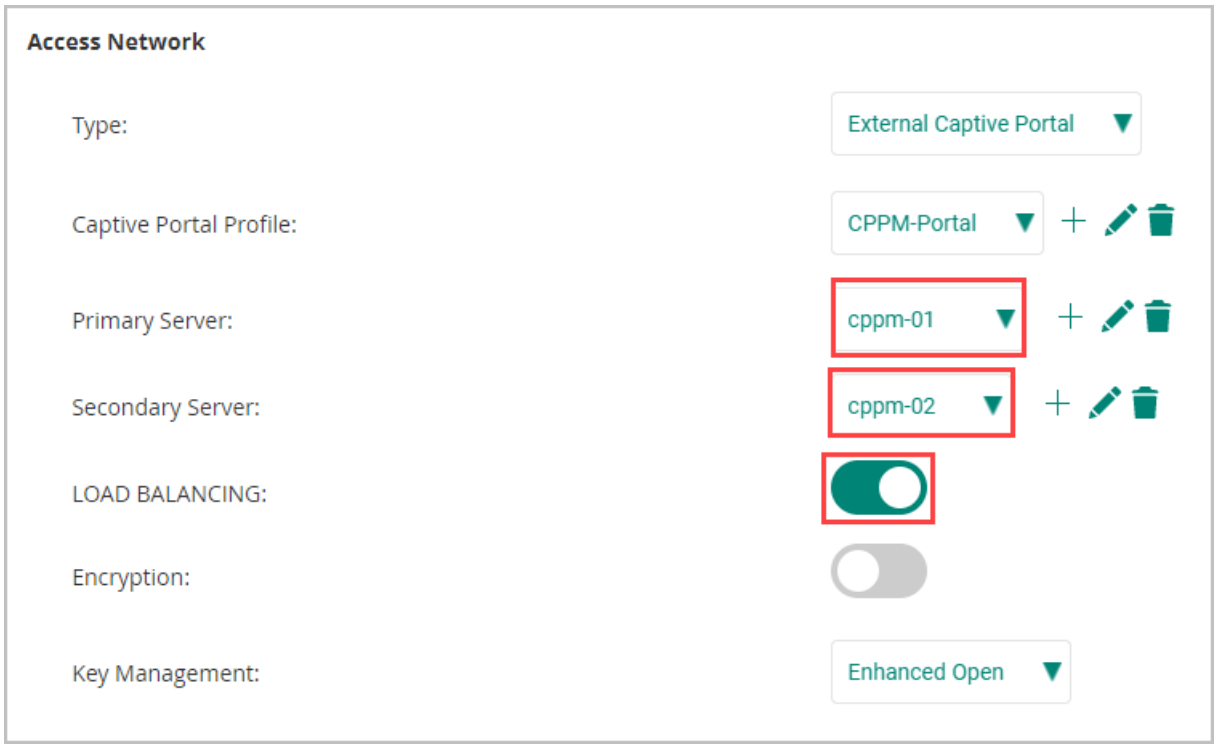


Figure 165: Configuring Radius Servers

NOTE:

Refer to *Configure SSID Security Settings* in the *Configure the WPA3-Enterprise Wireless LAN* section to create new RADIUS servers.

Configuring Access For Guest SSID

Pre- and post-authentication roles apply access restrictions to clients associated to an SSID. The pre-authentication role *EXAMPLE-DENY* denies all access except DNS, DHCP, and web access to the CPPM server. The *EXAMPLE-GUEST* post-authentication role allows access to all destinations. It is not necessary to block guests from internal networks in the post-authentication role because clients associated to the *EXAMPLE-GUEST* SSID cannot initiate connections to internal resources.

Configure Deny Role

Step 1 On the **Access** tab, move the slider to **Role Based**

Step 2 To create a new role, in the lower left, click **+ Add Roll**.

Step 3 In the **Add Roll** window, enter *EXAMPLE-DENY* in the **Role** field, then click **OK**.

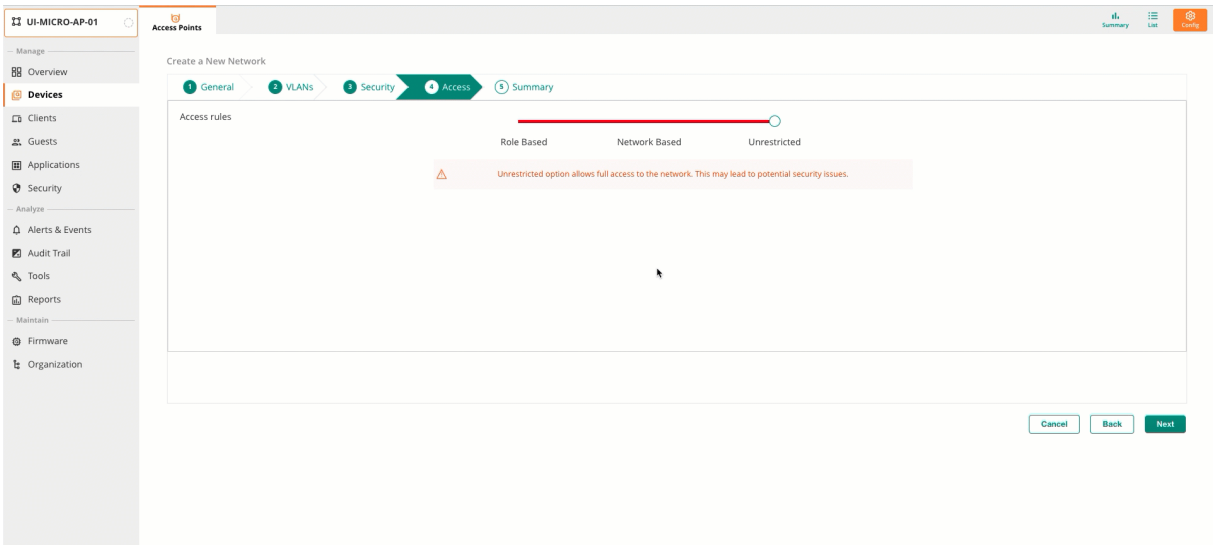


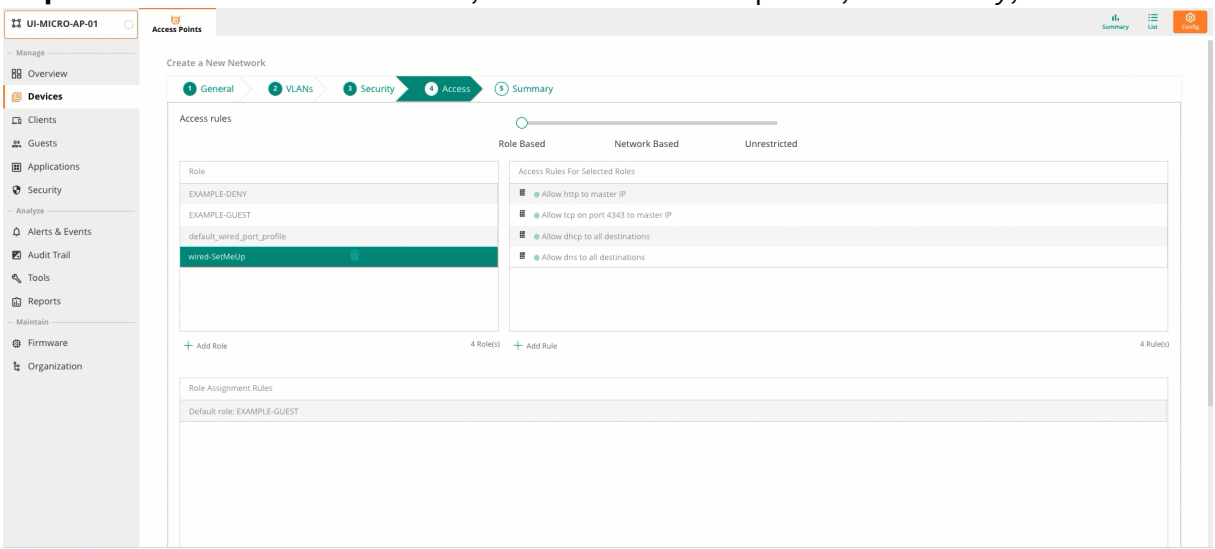
Figure 166: Creating Roles

Configure Deny ACL

Step 1 In the **Role** tile, select **EXAMPLE-DENY**.

Step 2 In the **Access Rules For Selected Roles** tile, select *Allow any to all destinations*, then click the **edit** (pencil) icon.

Step 3 In the **Access Rules** window, click the **Action** dropdown, select *Deny*, then click **OK**.



Step 4 To configure additional access rules, click **+ Add Rule**.

Step 5 In the **Access Rules** window, enter the values from the first row in the table below and click **OK**.

Rule Type	Service type	Service	Action	Destination	Network
Access control	Network	HTTPS/HTTP	Allow	To Particular Server	10.2.120.92
Access control	Network	DNS	Allow	To Particular Server	10.2.120.98

Rule Type	Service type	Service	Action	Destination	Network
Access control	Network	DNS	Allow	To Particular Server	10.2.120.99
Access control	Network	DHCP	Allow	To all destinations	N/A

Step 6 Repeat steps 4 and 5 for each row in the table.

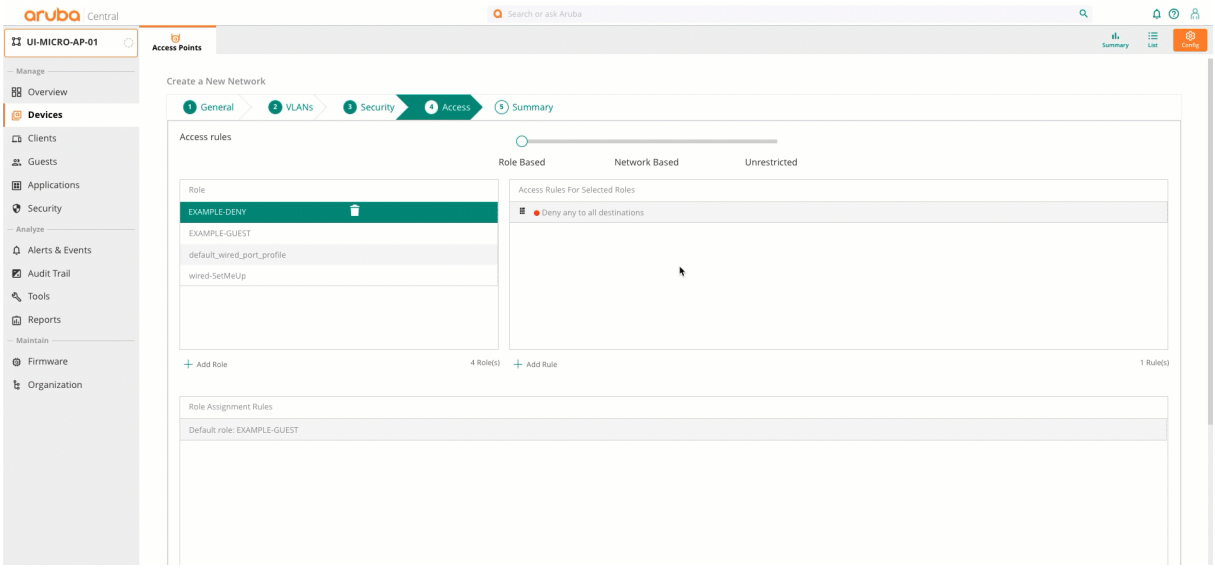


Figure 167: Configuring Access Rules

Step 7 In the **Assign Pre-Authentication Role** dropdown, select *EXAMPLE-DENY*

Step 8 Click **Next**.

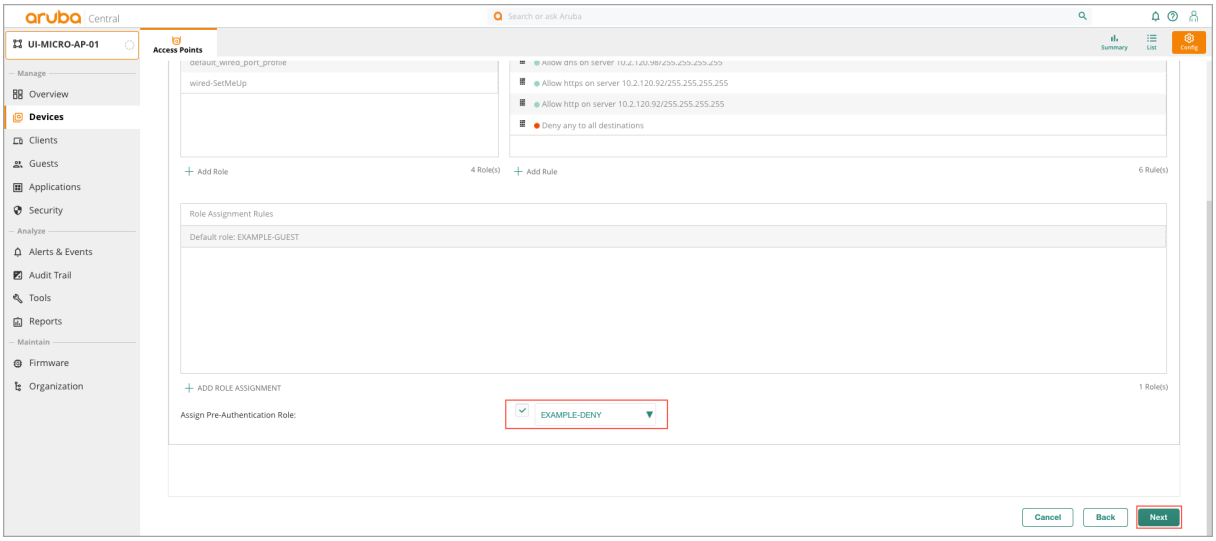


Figure 168: image-20220518204544679

(Optional) Routed Layer 3 Full-Tunnel Configuration

In highly secure deployments all traffic might need to be securely tunneled back to security appliances to ensure compliance, before forwarding to the appropriated destinations. The following section demonstrates how to configure a full tunnel.

To configure full-tunnel in Layer 3 Microbranch deployments, the Data Center deployment should be adjusted, and a **Policy-Based Routing (PBR)** policy should be created . With a rule stating that all traffic to any destination should be forwarded to either a VPNC or pair of VPNCs (via next hop list), through the secure IPsec tunnel. The PBR policy is then assigned to the user role(s). The users or devices who are assigned to the user role have all their user traffic forwarded to the data center via the secure tunnel.

Configure Hub Priority

Previously in the guide the hub site was configured as a site cluster which load balances based on route across the cluster, when full tunneling this can cause Asymmetric routing with a full tunnel deployment. To avoid this Manual Hub deployment should be used, this will Force the AP's to tunnel to a single gateway. If the primary gateway fails the tunnels will failover to the next gateway in the group.

Step 1 Go to the **UI-MICRO-AP-01 > Devices** configuration panel. In the **Tunnels & Routing** tile, select **Data Center**.

Step 2 In the **Data Center** header, hover over the configured group and select the trash can.

Step 3 Click **Save**.

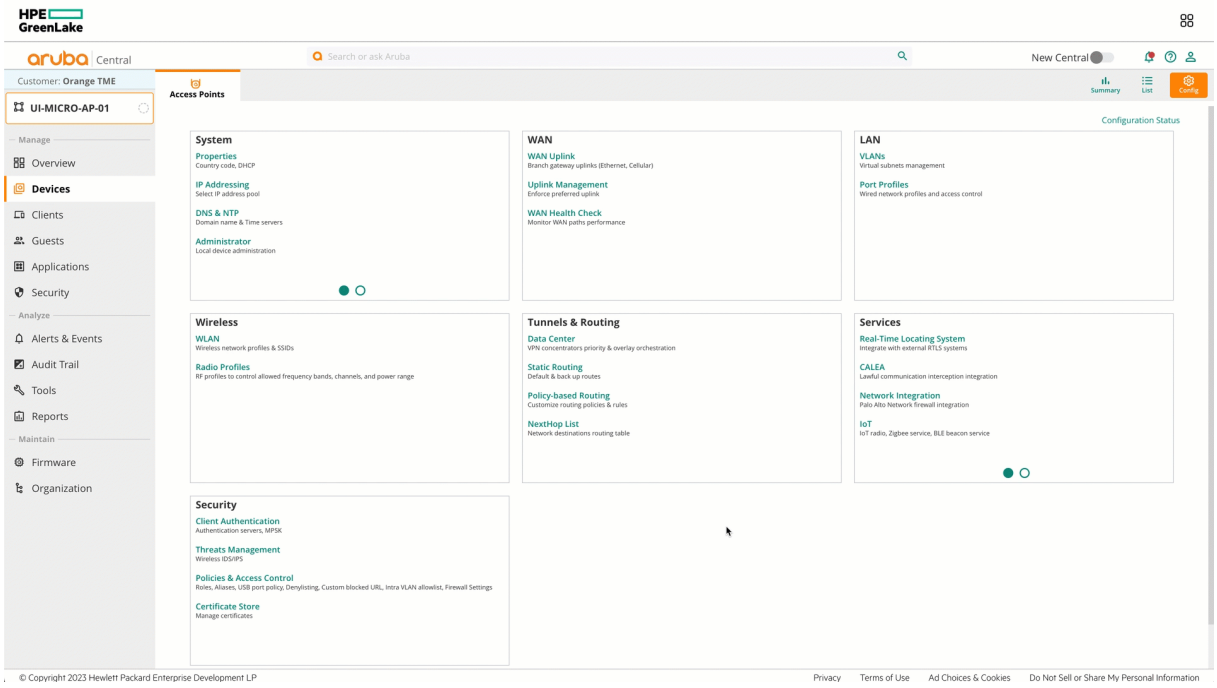


Figure 169: deleting_Clustered_hub_group

Step 4 In the **Tunnels & Routing** tile, select **Data Center**.

Step 5 Select the **Hubs** radio button

Step 6 In the **Data Center** header, click **+** (plus sign)

Step 7 In the **HUB GROUP** dropdown, select the VPNC Group configured in *Hub and Spoke Deployment*.

Step 8 In the **Cluster Name** dropdown, select the *RSVDC-VPNC-1* configured in *Hub and Spoke Deployment*.

Step 9 In the highlighted **VPNC-RSVDC** header click **+** (plus sign), select *RSVDC-VPNC-2*.

Step 10 Click **Save**.

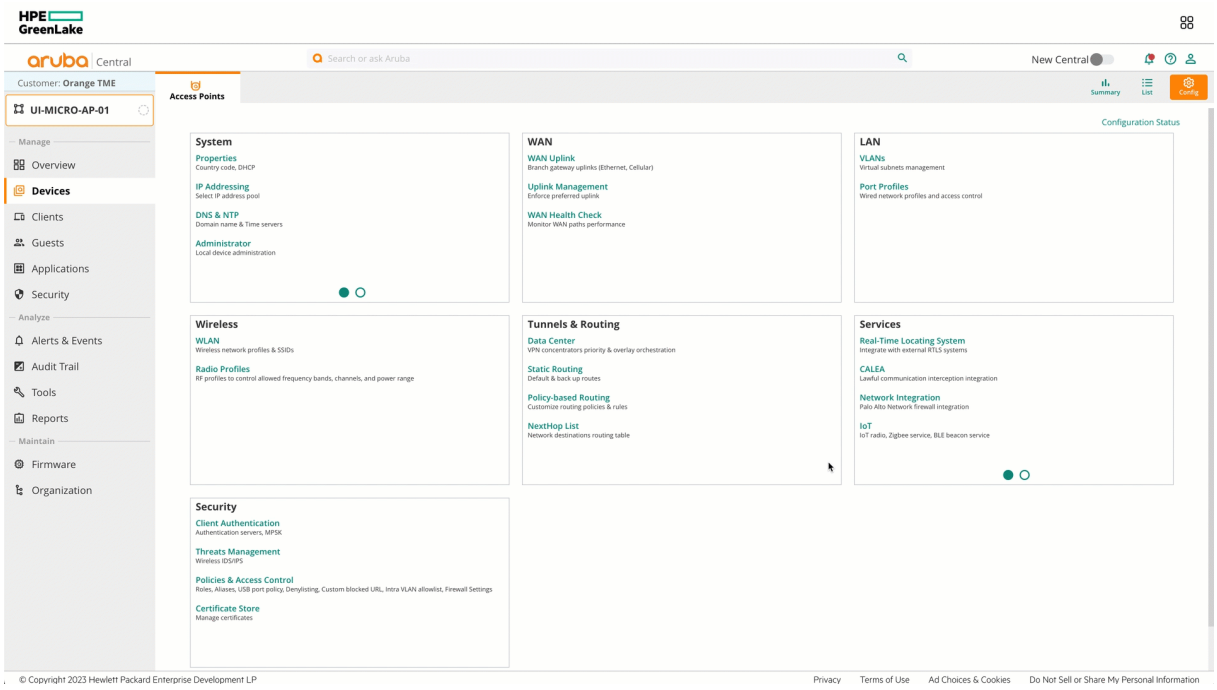


Figure 170: set_manual_hub_priority

Create PBR policy for full-tunnel

Step 1 Go to the group **UI-MICRO-AP-01 > Devices** page. In the **Tunnels & Routing** tile, select **Policy-based Routing**.

Step 2 Near the top right of the **Policies** tab, click **+** (plus sign).

Step 3 Enter a PBR policy name *(eg: EXAMPLE-PBR-DL3-FULL-TUNNEL)*.

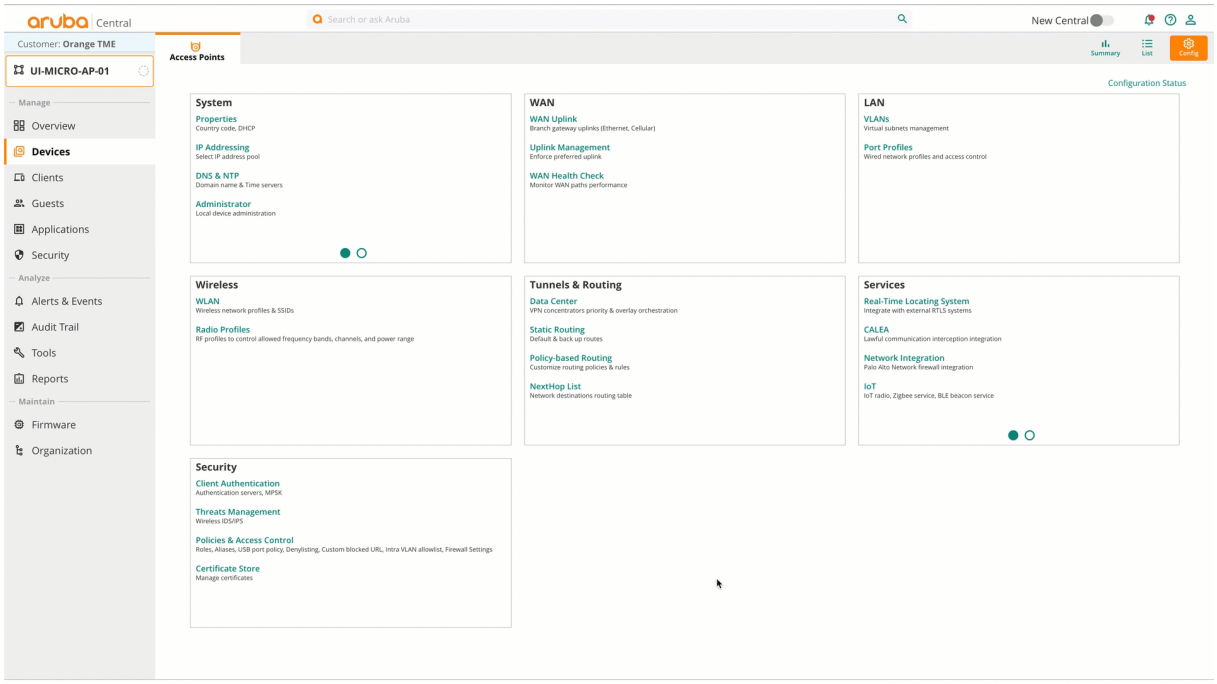


Figure 171: create_pbr_policy

NOTE:

When a new PBR policy is added, a default rule to forward any traffic to internet is created automatically.

Step 5 Mouse-over *EXAMPLE-PBR-DL3-FULL-TUNNEL* policy and click the **edit** (pencil) icon on the right.

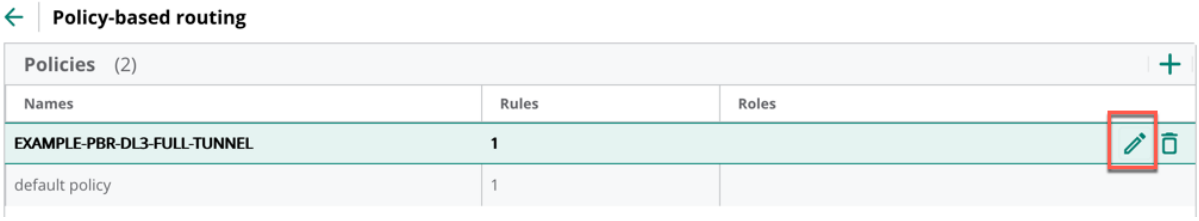


Figure 172: image-20230928141634927

Step 6 Mouse-over the default rule that was created automatically.

Step 7 Click the **edit** (pencil) icon on the right.

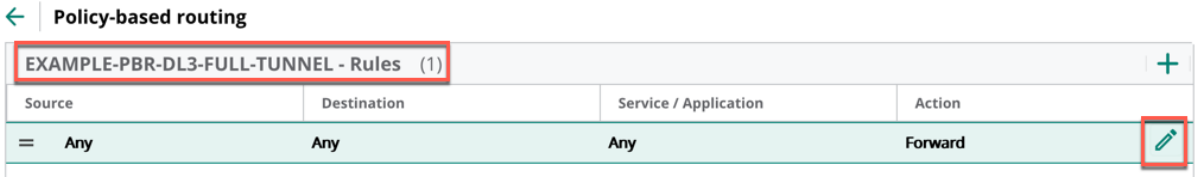


Figure 173: image-20230928141818901

Step 8 Click the **EDIT RULE** table. Perform either (1) or (2) based on the requirement as mentioned.

To forward all the user traffic to terminate on to a single VPNC, enter below details and click **OK** -
Source: *Any*

- **Destination:** *Any*
- **Service/App:** *Any*
- **Action:** *Forward to IPSec Map to VPNC*
- **VPNC**: *The VPNC to terminate traffic*
- **Uplink Tag**: *The uplink of the VPNC*

Figure 174: image-20230929101758372

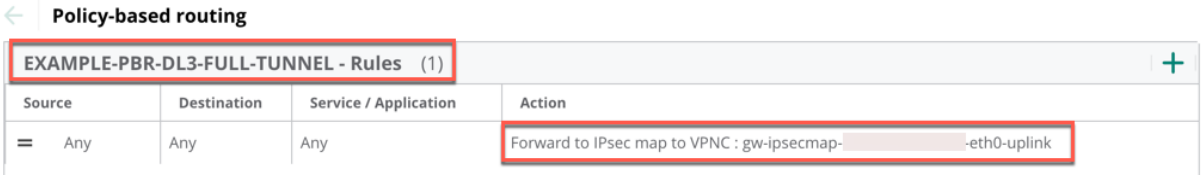


Figure 175: image-20231002145937585

Step 9 To forward all the user traffic to nexthop devicesusing nexthop list, enter below details and click **OK**

- **Source**: *Any*

- **Destination:** *Any*
- **Service/App:** *Any*
- **Action:** *Forward to Nexthop List*
- **Name of next-hop-list**: *< select the nexthop list name >*

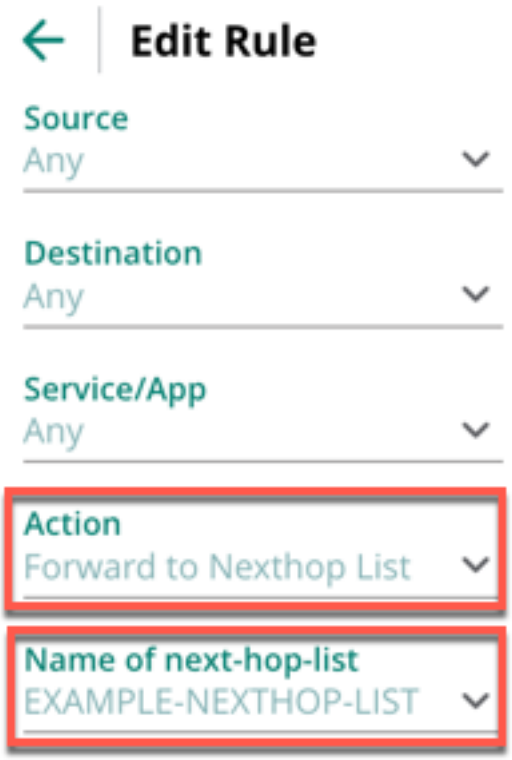


Figure 176: image-20231002155648848

Step 10 Click **Save**.

Apply PBR Policy for Full-Tunnel to User Role

Step 1 Go to the group **UI-MICRO-AP-01 > Devices** page. In the **Security** tile, select **Policies & Access Control**.

Step 2 Expand the **Roles** section.

Step 3 Select the user role to which to apply the PBR policy.

Step 4 In the **Rules** window, click **+** (plus sign).

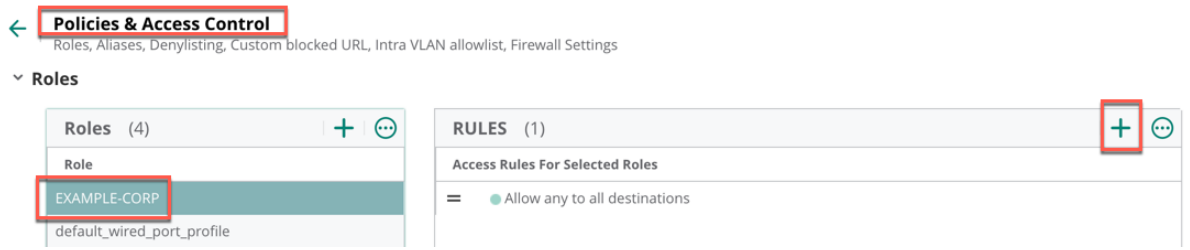


Figure 177: image-20231002165508884

Step 5 In the **ADD RULE** window, enter the following values, then click **OK**.

- **Rule Type:** *Policy-Based Routing*
- **Add Existing Policy:**
- **Policy Name:** *EXAMPLE-PBR-FULL-TUNNEL*

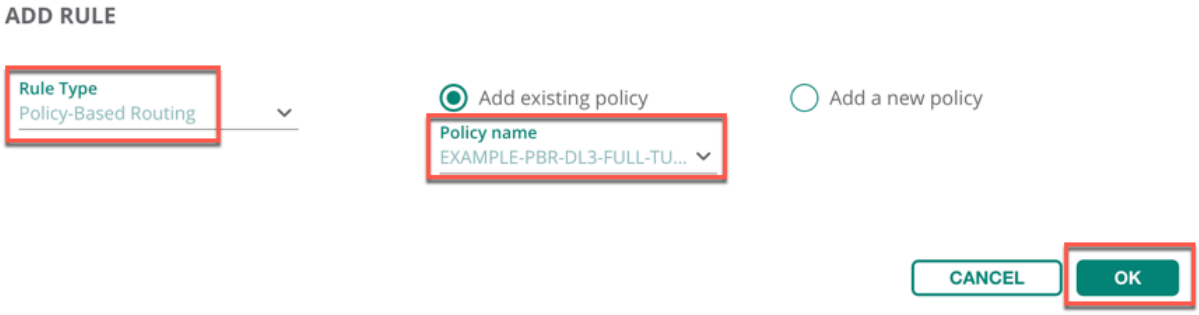


Figure 178: image-20231002165549846

Step 6 The PBR policy configured for full-tunnel is assigned to the user role.

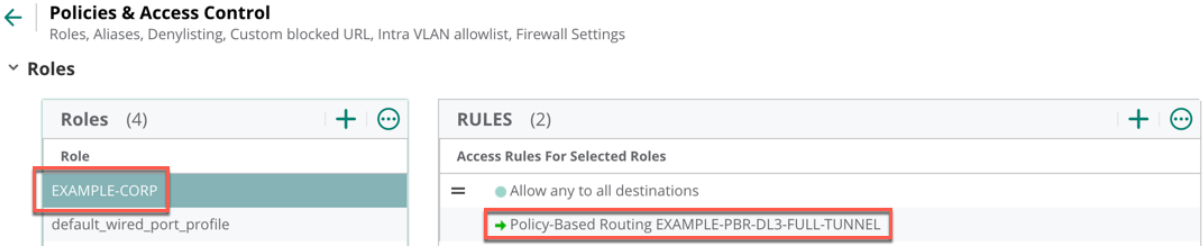


Figure 179: image-20231002165647469

Step 7 Click **Save**.

NOTE:

When a user is assigned a user role and the user traffic flows, all the access rules for the user role are applied first and if there is a PERMIT, the PBR policy is then applied to that specific user traffic.

Assign a Microbranch AP to a Group

Step 1 In the left navigation pane, click **Global**, then select the **Groups** column heading.

Step 2 Expand the **Unprovisioned devices** group by clicking the expansion icon (**>**) next to its name.

Step 3 Select the *Microbranch* AP.

Step 4 Click the **Move Devices** icon.

Step 5 In the **Destination Group** dropdown, select *UI-Micro-AP01*.

Step 6 Click **Move**.

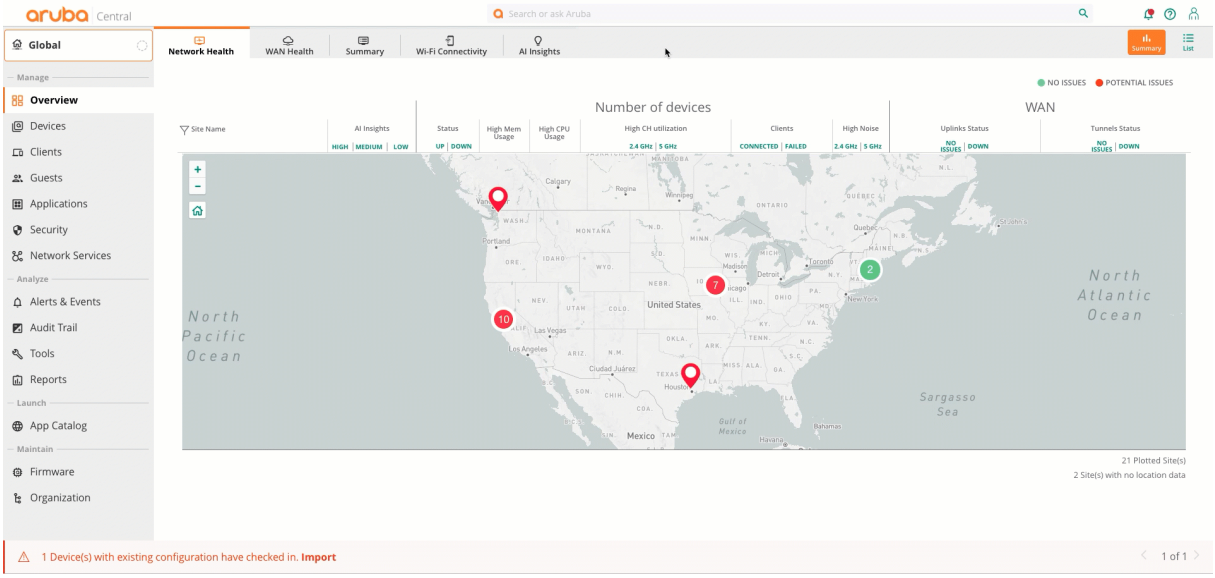


Figure 180: Moving Ap

Assign a Microbranch AP to a Site

The following procedure assigns the VPNCs to a site.

Step 1 Go to **Organization** and select **Site**.

Step 2 Select **Unassigned** devices.

Step 3 Select the *Microbranch* AP on the right side, then drag the AP to the **ESP-MB01** site.

Step 4 Click **Yes**.

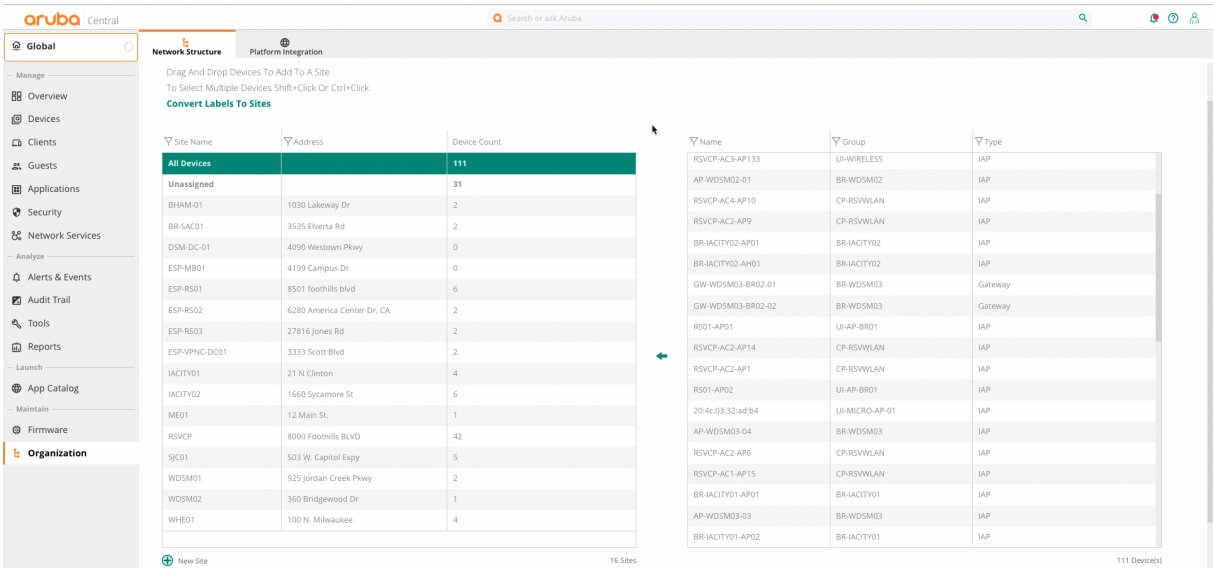


Figure 181: Adding microbranch AP to site

Monitor Microbranch AP Routing Overlay

The route orchestrator redistributes the routes between the headend VPNCs and the Microbranch APs. All the overlay routing information such as control connections, routes advertised, routes learned, etc. can be monitored in the AP device page.

Step 1 Go to **AP Group > Devices > Access Points > List**.

Step 2 Select an **AP**.

Step 3 Under **Overview**, click **Routing** tab.

Step 4 Select **Overlay** tab.

Step 5 The Overlay summary table displays an overview of control connection state, number of interfaces, number of routes advertised from AP and number of routes learned by the AP

Step 6 Under the **Overlay details**, in the dropdown box, select **Routes advertised** which displays all the routes advertised from the AP.

Step 7 Under the **Overlay details**, in the dropdown box, select **Routes learned** which displays all the routes learned by the AP.

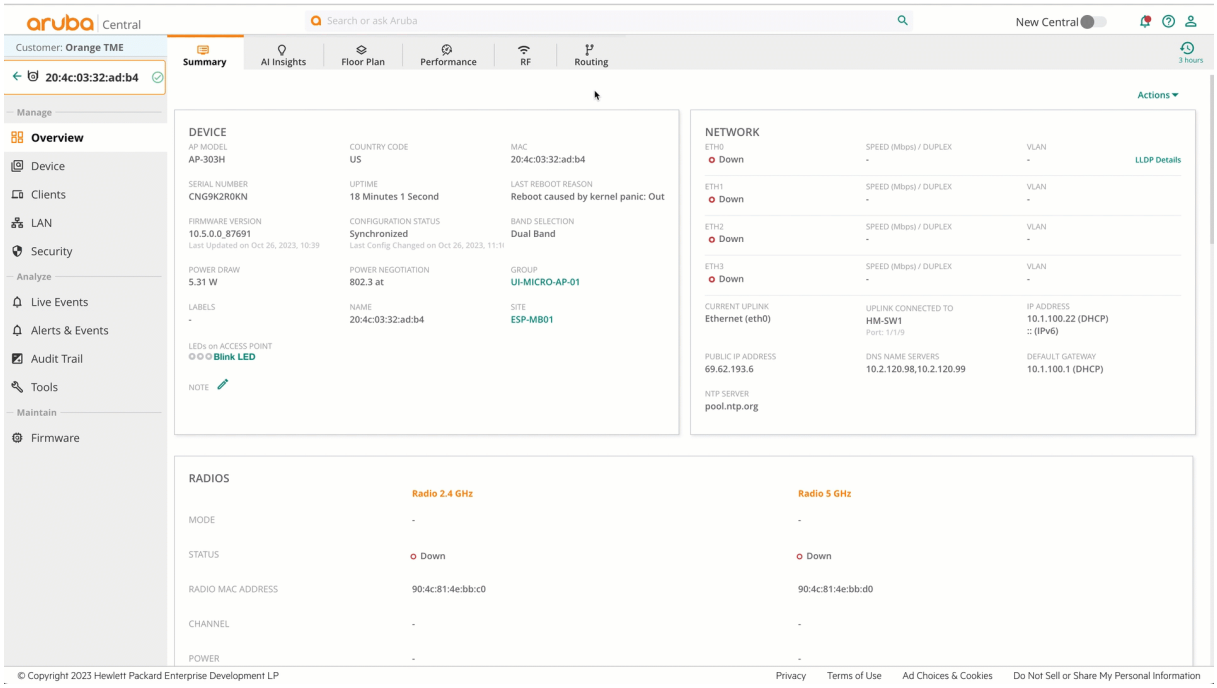


Figure 182: mb_route_table

Aruba Microbranch Centralized Layer 2 (CL2) Overview

Centralized Layer 2 (CL2) is an extension of previously introduced Remote Access Point (RAP). CL2 forwarding provides flexible options:

- All user traffic can be tunneled entirely to the data center.

CL2 is supported for both wireless and wired clients. In CL2 mode, Microbranch AP does not act as DHCP server or as a gateway for the clients. DHCP server and Default GW reside in the data center, so DHCP requests from the client are tunneled to the data center. CL2 also extends the corporate VLAN or broadcast domain to remote branches.

Common usage for CL2 includes, but is not limited to:

- Remote deployments that must perform security policy checks at the data center
- Remote deployments that require VLAN extension and DHCP scopes from the data center to the branches

The AP follows its routing table to forward traffic, so any user traffic is sent via the AP's default gateway (to the AP's WAN uplink to the ISP network).

In addition, the Overlay Route Orchestrator (ORO), that helps to advertise data center routes to APs dynamically, does not serve a role in CL2. Therefore, when using CL2, a policy must be defined to redirect or forward user traffic to the data center using Policy-Based Routing (PBR). The PBR policy action "forward to cluster" is designed specifically to enable CL2 mode to redirect traffic to VPNC clusters.

User Traffic Flow in CL2

After the user is authenticated, the VLAN configured for CL2 is assigned to the client. Two options are available to handle the user traffic flow or the APs' data forwarding decision to forward all user traffic to the data center or to forward only a select subset of user traffic to the data center:

- **Split-tunnel:** The AP tunnels only the user traffic destined to access resources at data center, while other traffic can be NATed locally to an AP WAN uplink (Internet or cellular).
- **Full-tunnel:** The AP tunnels all the user traffic to the data center.

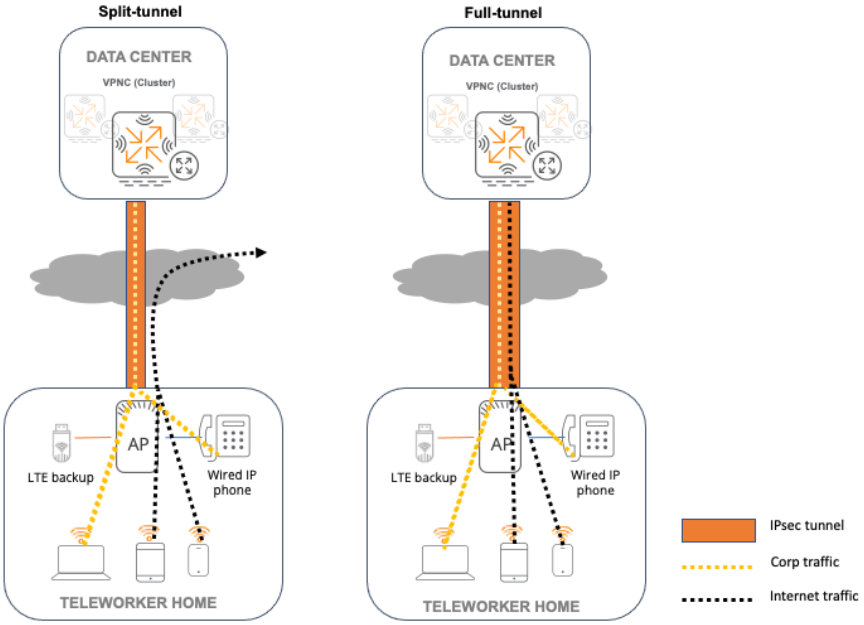


Figure 183: CL2-split-full-tunnel-diagram

Split-Tunnel in CL2

The split-tunnel optimizes traffic flow by directing only corporate traffic back to the data center through the secure IPsec tunnel, while Internet application traffic can be bridged locally to the AP WAN uplink by source-NAT with AP uplink IP. This ensures that non-corporate Internet traffic does not incur the overhead of a round trip to the data center VPNCs, which decreases traffic on the WAN link and minimizes latency for voice/video applications such as Zoom, Teams, etc.

By default, all user traffic is NATed locally to the AP WAN uplink and does not allow access to corporate resources. To allow access to internal resources with CL2, engage split-tunneling by configuring **Policy-Based Routing (PBR)** policy with two or more rules. Traffic matching a PBR rule with the action "*forward to cluster*" is securely tunneled to the UDG (User Designated Gateway). If traffic does not match a PBR rule, the traffic is src-NATed with the AP uplink's IP and sent to the uplink.

Full-Tunnel in CL2

In full-tunnel mode, the Microbranch AP forwards all user traffic securely via the IPsec tunnel to the VPNC clusters at the data center instead of using its own routing table for routing decision. Full-tunneling may required to perform additional required security checks at the data center and/or to provide centralized access for all user traffic. Typical usage would include networks for banking and insurance that require scrutinizing user traffic at the data center for added security and other similar business situations.

To configure full-tunnel in CL2 Microbranch deployments, a **Policy-Based Routing (PBR)** policy is created first with a rule stating that any user traffic to any destination must be forwarded to the cluster through the secure IPsec tunnel. Traffic matching any PBR rule with the action "*forward to cluster*" is securely tunneled to the UDG (User Designated Gateway).

NOTE:

By default, all user traffic is sent to the AP's WAN uplink, so data center resources cannot be accessed. PBR rules must be configured to send authorized user traffic to the data center to access internal resources.

Determine UDG (User Designated Gateway) for Clients in CL2

For overlay cases, unlike DL3 where the routing table in AP (populated by ORO) determines the VPNC that client traffic terminates, using CL2 the AP receives the *bucket map* from the data center to map clients to the VPNC, also known as UDG (User Designated Gateway).

Any time a client sends traffic to the data center, the AP checks its bucket map, determines the client's UDG, and forwards the traffic through the pre-established IPsec tunnel to the UDG/VPNC assigned to the client. This helps with load balancing in addition to assigning clients to a specific UDG/VPNC in the data center cluster.

The screenshot below displays the bucket map that the AP receives from the data center. The client (in Station list) connected to the AP is assigned to the UDG/VPNC with index 1 and IP 172.30.28.33. The traffic from the client destined to the data center is sent via the secured IPSec tunnel to UDG/VPNC.

```
-MB-515-                    !# show overlay bucketmap

Cluster auto_gwcluster_215_0 radio=0 zone=0 - Num UACs 2
---------------------------------------------------------
Index  ArrayIdx  UAC IP         Num STAs
-----  --------  ------         --------
0      0         172.30.28.32   0
1      1         172.30.28.33   1
Station List
------------
UAC Index  Station Mac         BSSID
---------  -----------         -----
1          7E:DA:              9C:8C:
Bucket Map
----------
Bucket Idx Range  Bucket Map
----------------  ----------
[0-31]            0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[32-63]           0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[64-95]           0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[96-127]          0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[128-159]         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[160-191]         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[192-223]         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[224-255]         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
-                 Standby Map
[0-31]            1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[32-63]           1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[64-95]           1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[96-127]          1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
[128-159]         0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[160-191]         0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[192-223]         0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
[224-255]         0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Statistics:Bmap Updates=5; UAC:Adds=2 Deletes=0; STA:Adds=0 Deletes=17 moves=0 errs=0 copies=0
```

Figure 184: CL2-bucketmap

This set-up also can be observed on the **Client Details** page in the Aruba Central user interface. The UDG where the client traffic is tunneled and the UDG IP are displayed in the screenshot below.

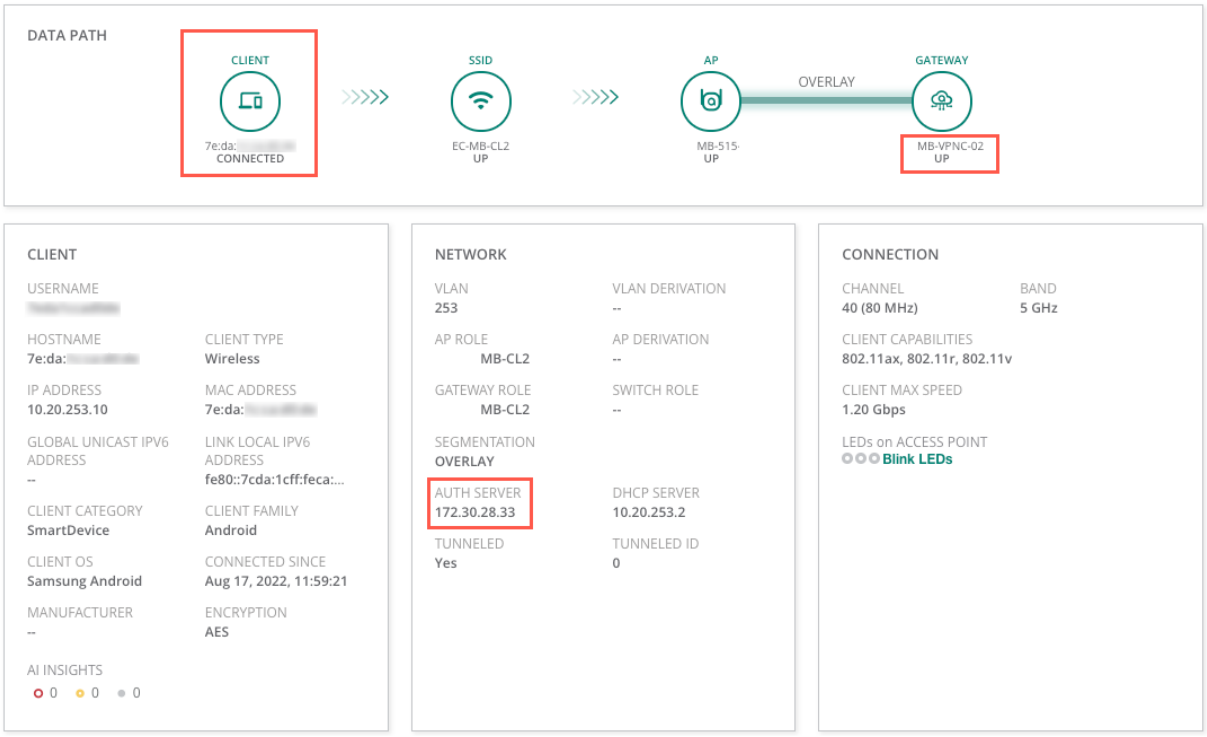


Figure 185: CL2-client-UI

Aruba CL2 VPNC Configuration

This guide provides the configuration steps required for VPNCs at the data center for CL2 mode Microbranch deployments. VLAN ID 253 (10.20.253.0/24) is the VLAN configured on the VPNC that will be extended to the AP. *UI-MICRO-VPNC-01* is the group in which the data canter VPNCs are added.

NOTE:

This guide uses the VPNC configured in the hub and spoke section. To configure a VPNC, review the “Deploying VPNC” section. This section describes only the VPNC configurations required for CL2 mode in Microbranch deployments.

Configure CL2 VLAN

The VLAN configured in the VPNC is extended to Microbranch AP in CL2 mode deployments. The configuration of CL2 VLAN ID 253 is performed at the **VPNC group level**.

NOTE:

The DHCP server can reside in the data center to allocate the IP address for VLAN ID 253 to clients connected in CL2 mode. It should be reachable through VPNC.

Step 1 Go to the **UI-MICRO-VPNC-01 > Devices > Gateways** UI page.

Step 2 Select the **Interfaces** tab.

Step 3 Select the **VLANs** tab.

Step 4 In the **VLANs** window, click the **+** (plus sign) at the bottom left.

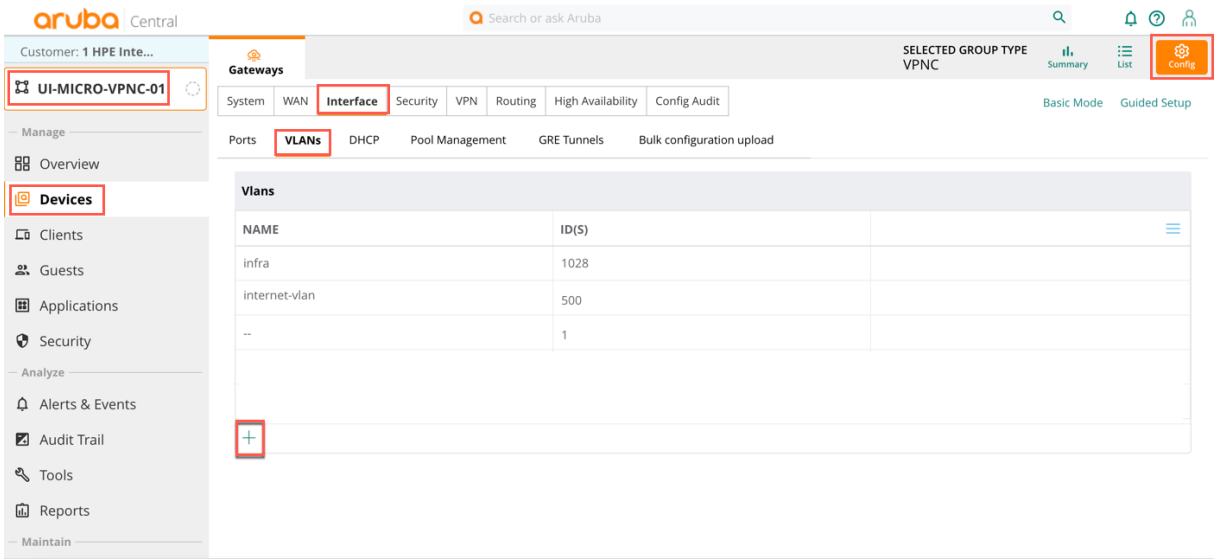


Figure 186: CL2-VPNC-VLAN-Add

Step 5 In the **New VLAN** window, enter: - **VLAN Name:** *tunneled_users* - **VLAN ID/Range:** *253*

Step 6 Click **Save Settings**.

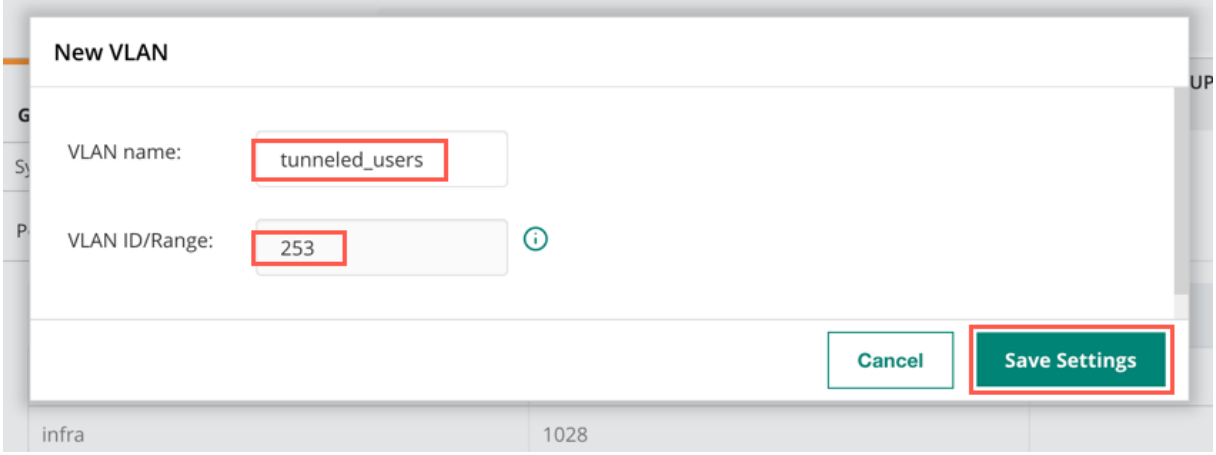


Figure 187: CL2-VPNC-VLAN-New

Assign the CL2 VLAN to the VPNC LAN Port Interface

The newly created VLAN ID 253 for CL2 mode must be assigned to the VPNC LAN port interface so it can reach the DHCP server when a DHCP request comes through the tunnel.

Step 1 Go to the **UI-MICRO-VPNC-01 > Devices > Gateways** page.

Step 2 Select the **Interfaces** tab.

Step 3 Select the **Ports** tab.

Step 4 Select the **LAN port interface** (example: *GE-0/0/7*)

Step 5 In the port interface window, add the following: - **Allowed VLANs:** *253*

Step 6 Click **Save Settings**.

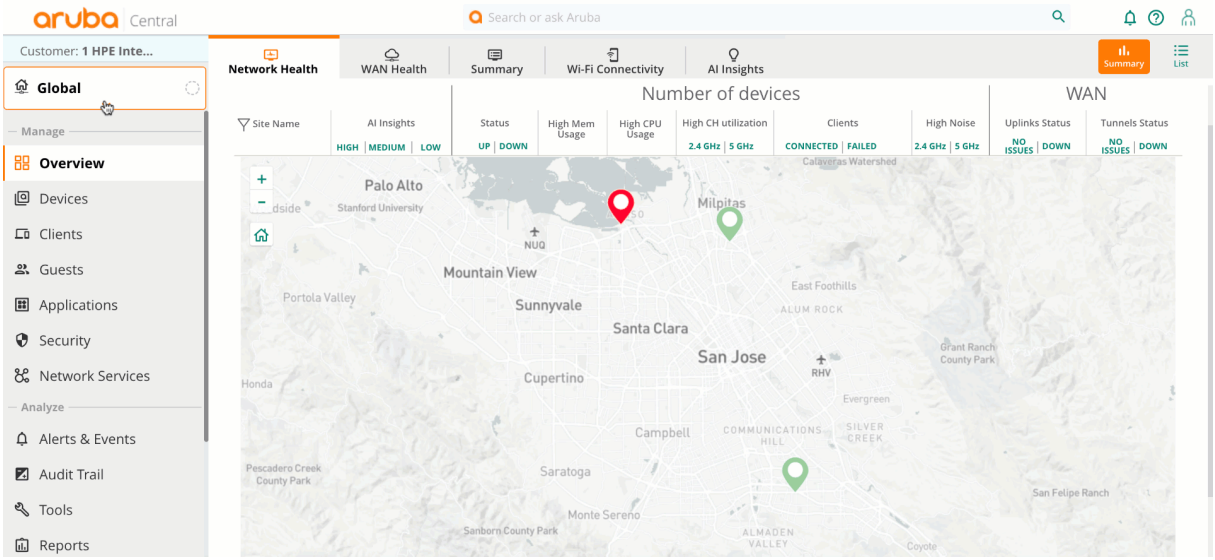


Figure 188: CL2-VPNC-assign-VLAN-LAN-port-interface

Configuring CL2 Microbranch AP

This guide demonstrates the configuration of Centralized Layer 2 (CL2) mode SSID in Microbranch. *EXAMPLE-CL2* is a Centralized Layer 2 SSID providing access to both corporate resources and non-corporate resources through the Internet.

VLAN ID 253 is the tunneled user VLAN extended from the data center VPNC and assigned to the SSID (through clustering functionality). The VLAN ID 253 should be configured only in VPNC and not in the Microbranch AP.

The topology below illustrates the Microbranch.

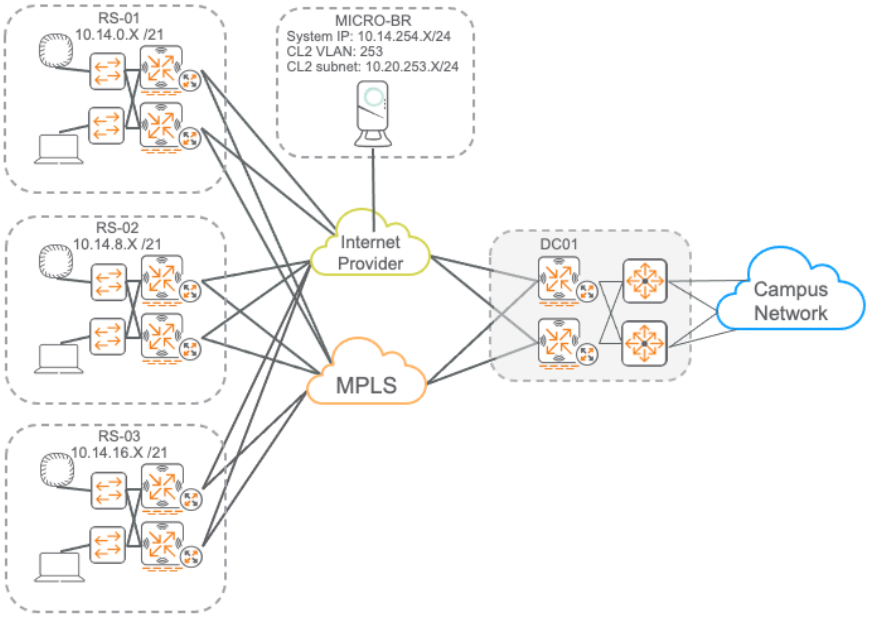


Figure 189: CL2-Topology

Create a Microbranch AP Group

Step 1 Click the context filter **Global**.

Step 2 Hover over **Groups** column heading and click the **settings icon**.

Step 3 To create a New Group, in the upper right, click **+** (plus sign).

Step 4 In the **Add Group** window, enter a name. Click the **Access Point** checkbox, and click **Next**.

Step 5 Leave *ArubaOS 10* selected under **Architecture for access points and gateways in this group**. Click the **Microbranch** radio button under **Network role of the access points in this group**, then click **Add**.

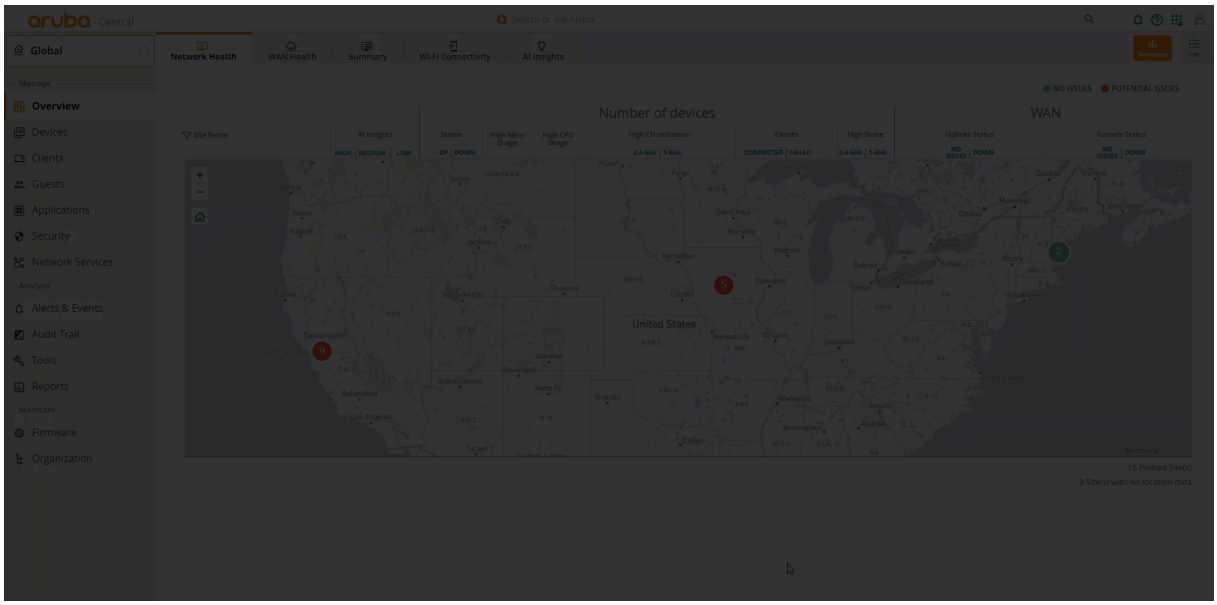


Figure 190: Creating AP Group

Configure System IP Pool

The System IP Pool dynamically assigns IP addresses to access points, which is required for Microbranch AP setup. APs use the assigned IP as the system IP for the inner tunnel IP address and as a management address to source traffic such as RADIUS, TACACS+, and SNMP. The System IP Pool is applied to the Microbranch group in a future step.

Step 1 Select the **Global** group. In the left navigation pane, click **Network Services**.

Step 2 Select the **IP Address Manager** tab.

Step 3 In the upper right, click **+** (plus sign).

Step 4 In the **Add System IP Pools** window, enter the following: - **Pool Name:** *System IP Pool*

- **Start address:** *10.14.254.1*
- **End address:** *10.14.254.100*

NOTE:

The system IP pool is global and applied to all APs in the group. When designing the system IP pool size, account for all APs in the Microbranch group.

Step 5 Click **SAVE**.

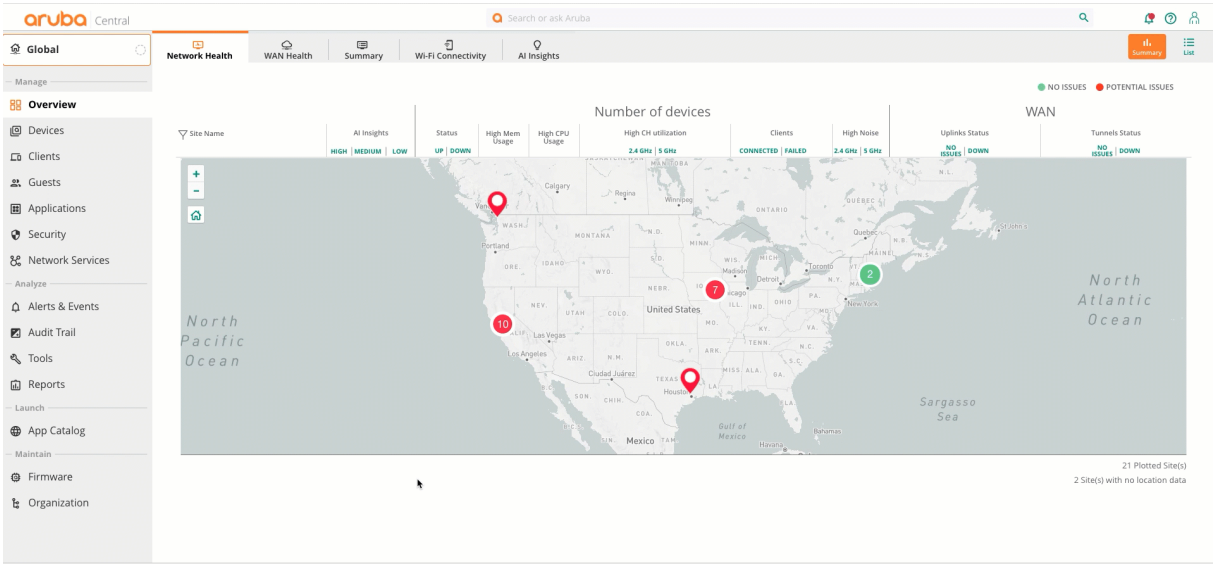


Figure 191: Configuring Address Pool

NOTE:

Global VLAN DHCP pool is not required for Centralized Layer 2 (CL2) mode SSID. In CL2, the external DHCP server at the data center is used to define DHCP scope for the clients.

Set AP Device Password

Step 1 In the **Global** dropdown, search and select the Microbranch AP group previously created.

Step 2 In the left navigation pane under **Manage**, select **Devices**.

Step 3 Select the **Access Points** tab. In the upper right corner, click the **config** (gear) icon.

Step 4 Enter a device password in the **Password** field. Reenter the password in the **Confirm password** field, then click **Set Password**.

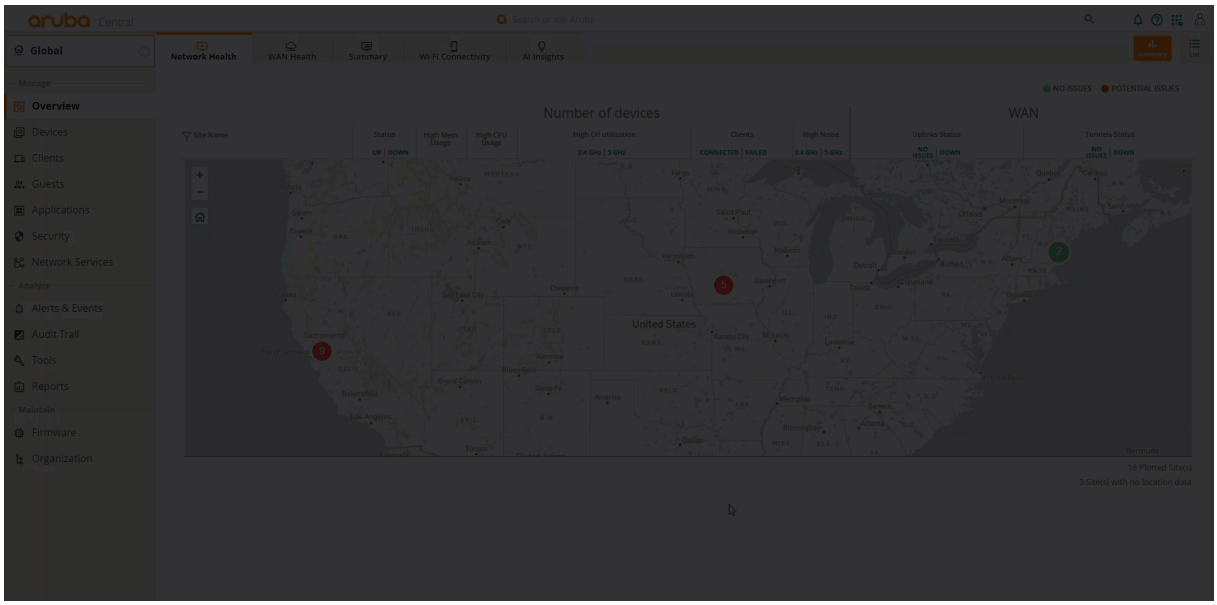


Figure 192: AP Group Navigation

Configure Country Code

It is important to assign the proper country code to ensure that APs operate in compliance with local regulatory restrictions.

Step 1 On the group **UI-MICRO-AP-01 > Devices** page, in the **System** tile, select **Properties**.

Step 2 In the **Set country code** field, select the appropriate country code from the dropdown.

Step 3 Click **Save**.

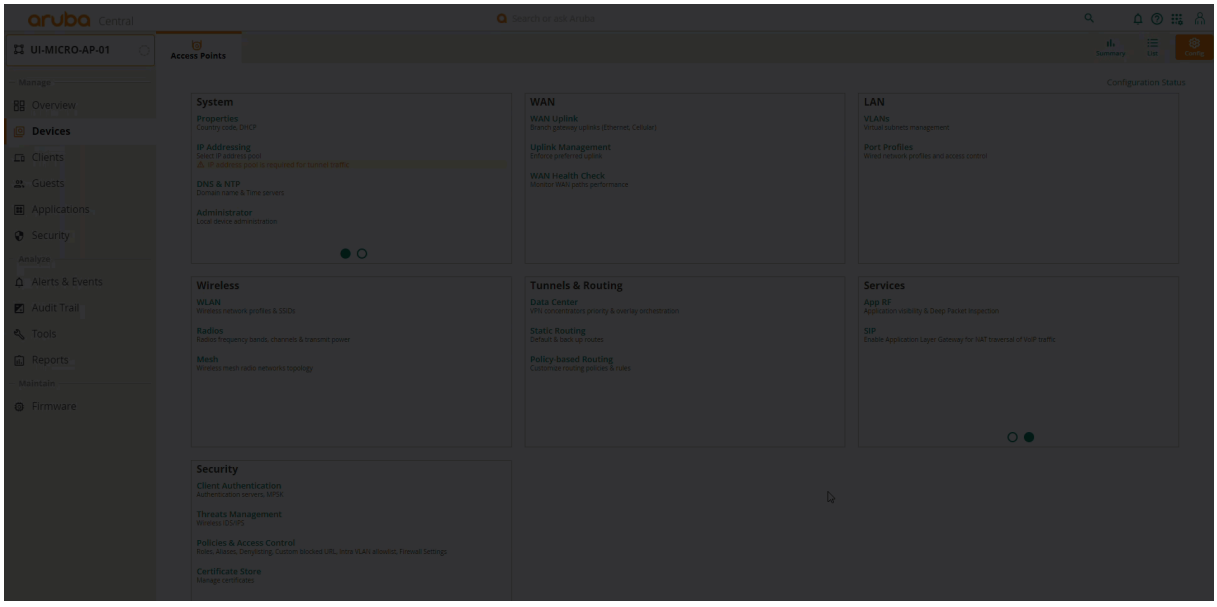


Figure 193: configuring Country Code

Assign the System IP Pool to AP Group

Step 1 On the group **UI-MICRO-AP-01 > Devices** page, in the **System** tile, select **IP Addressing**.

Step 2 Click **+** (plus sign).

Step 3 In the **Select IP Address Pool** field, select the previously configured *System IP Pool*.

Step 4 Click **Save**.

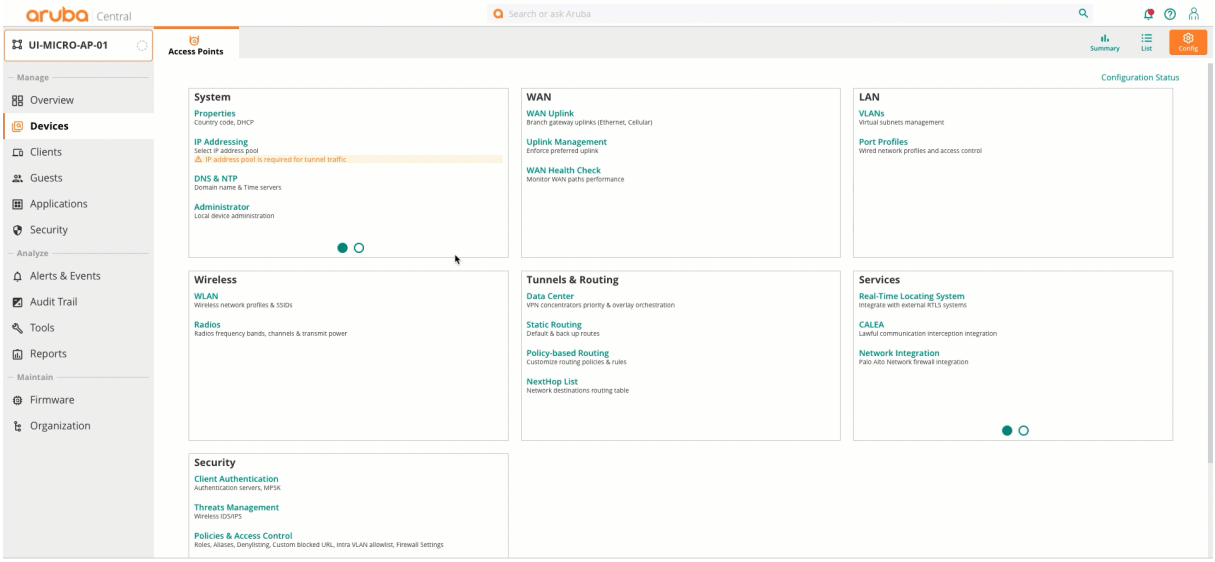


Figure 194: SystemIP Pool

Configure DNS and NTP

Step 1 On the group **UI-MICRO-AP-01 > Devices** page, in the **System** tile, select **DNS & NTP**.

Step 2 In the **Domain Name** field, enter the domain name.

Step 3 To add a DNS server, in the **DNS SERVERS** header, click **+** (plus sign).

Step 4 Select a DNS service from the dropdown.

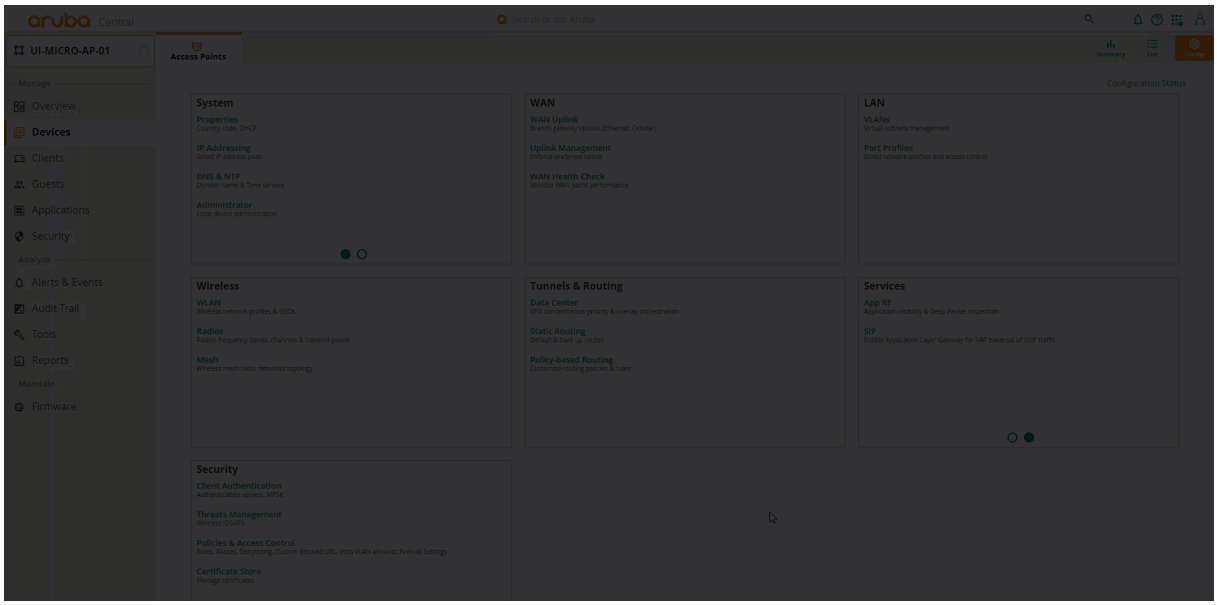


Figure 195: Configuring DNS

Step 5 To expand the **NTP** section, click **> NTP**.

Step 6 To add an NTP server, in the **PUBLIC NTP SERVERS** header, click **+** (plus sign).

Step 7 In the new empty field, enter an **NTP** FQDN or IP address.

Step 8 In the **Timezone** field, select a timezone from the dropdown.

Step 9 Click **Save**.

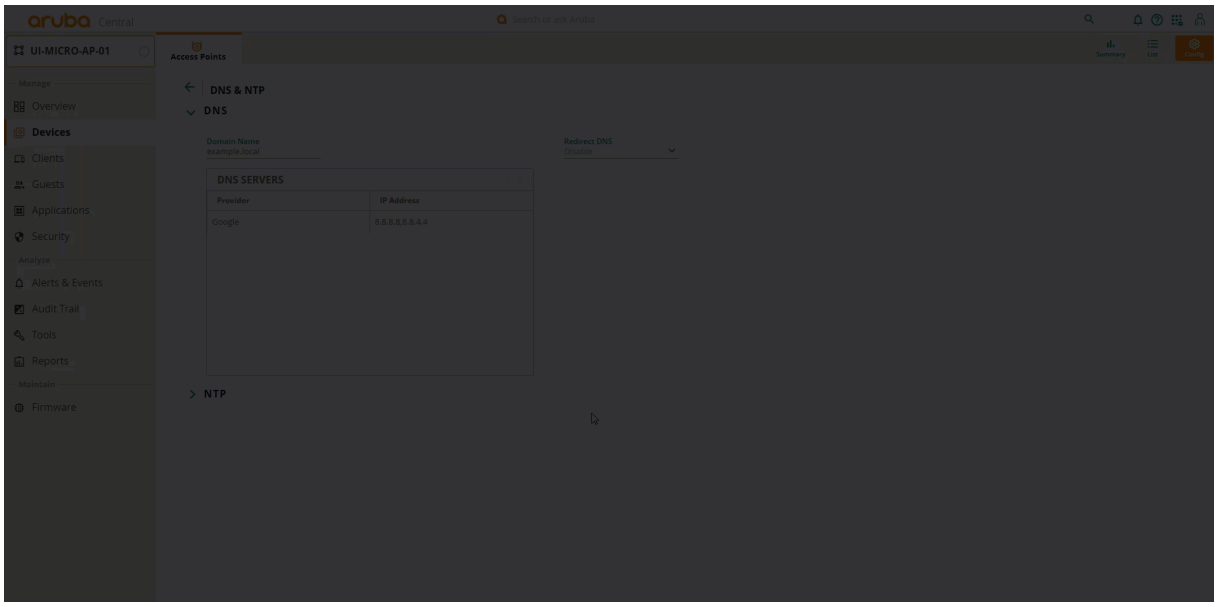


Figure 196: Configuring NTP

Configure WAN Uplink

The WAN uplink identifies the interface assigned a WAN IP address. Tunnel Orchestrator uses the WAN IP address to create tunnels between devices. The WAN Uplink name is used in the Tunnel Matching algorithm and it will try to match the same name on the other side of the tunnel. If the labels do not match, then it is attempted to match any other WAN label.

Step 1 On the group **UI-MICRO-AP-01 > Devices** page, in the **WAN** tile, select **WAN Uplink**.

Step 2 On the right side, click **+** (plus sign).

Step 3 In the **Uplink Name** field, enter the uplink interface name.

Step 4 Click **Save**.

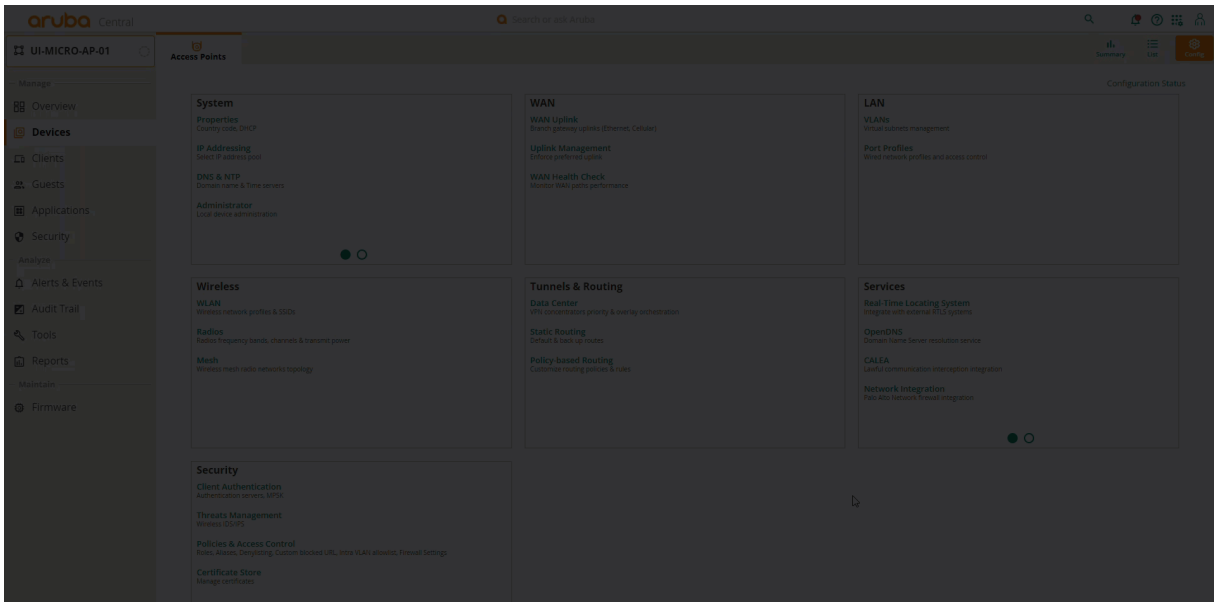


Figure 197: Config

Configure WAN Health Check

A WAN Health Check measures the quality of the WAN uplink. Latency and packet loss on WAN uplinks are calculated using ICMP or UDP probes. UDP-based probes add measurement of jitter and generate MoS scores.

Step 1 Go to the group **UI-MICRO-AP-01 > Devices** page. In the **WAN** tile, select **WAN Health Check**.

Step 2 To the right of **Monitor WAN health**, click the slider.

Step 3 Click the **Custom** radio button.

Step 4 In the **Protocol** field, click the dropdown and select *UDP*.

NOTE:

We recommend using **pqm.arubanetworks.com** as the remote FQDN (Fully Qualified Domain Names) for Health Check probes.

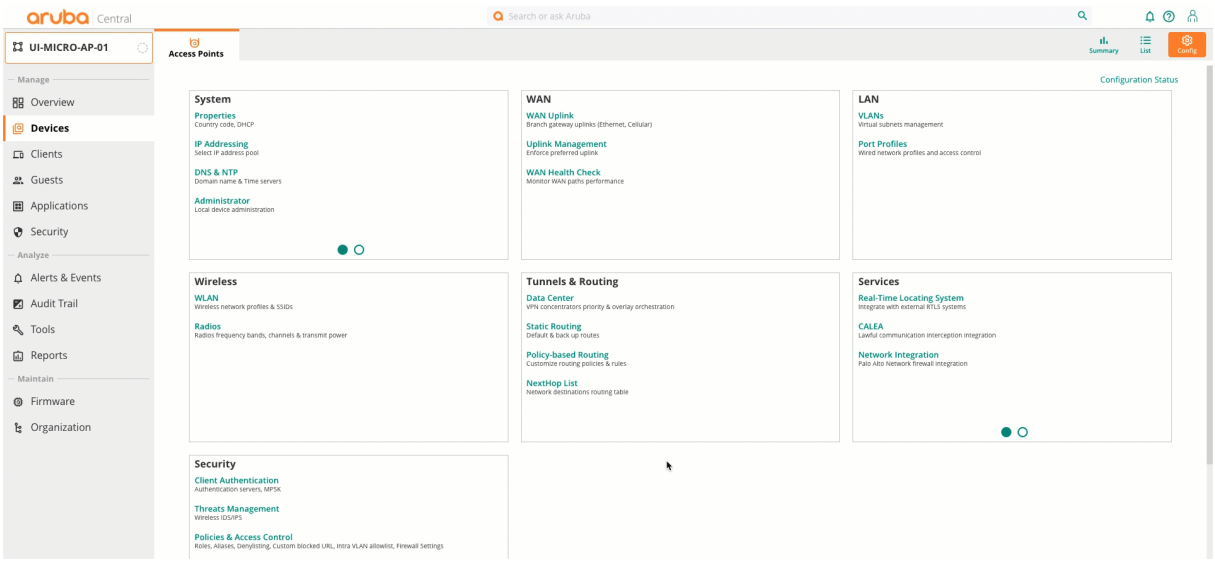


Figure 198: Configuring WAN Health Check

Configure the WPA3-Enterprise Wireless LAN

The following procedure creates a secure, CL2 mode SSID for accessing internal resources as well as non-internal resources.

Step 1 Go to the group **UI-MICRO-AP-01 > Devices** page. In the **Wireless** tile, select **WLAN**.

Step 2 Near the bottom left of the **WLANs** tab, click **+ Add SSID**.

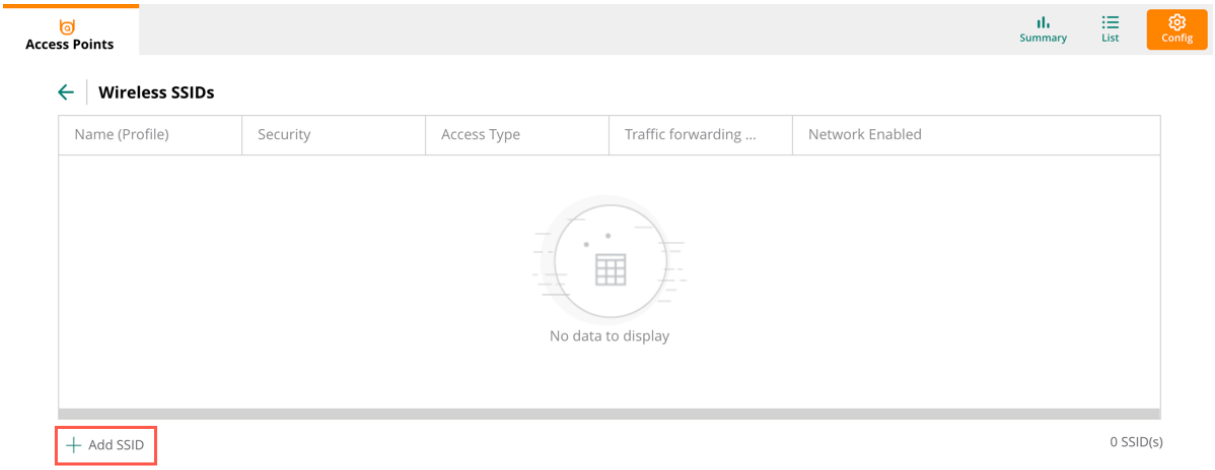


Figure 199: CL2-WLAN-SSID-Add

Step 3 On the **General** tab, set the **SSID Name** field to *EXAMPLE-CL2*.

Step 4 To display additional settings, click **> Advanced Settings**.

Step 5 To expand broadcast/multicast options, click **(+) Broadcast/Multicast**.

Step 6 In the **Broadcast filtering** dropdown, select *All*.

Step 7 To expand legacy transmission rate options, click **(+) Transmit Rates (Legacy Only)**.

Step 8 In the **2.4 GHz** section, assign the following values. - **Min:** *5* - **Max:** *54*

Step 9 In the **5 GHz** section, assign the following values. - **Min:** *18* - **Max:** *54*

Step 10 Click **Next**.

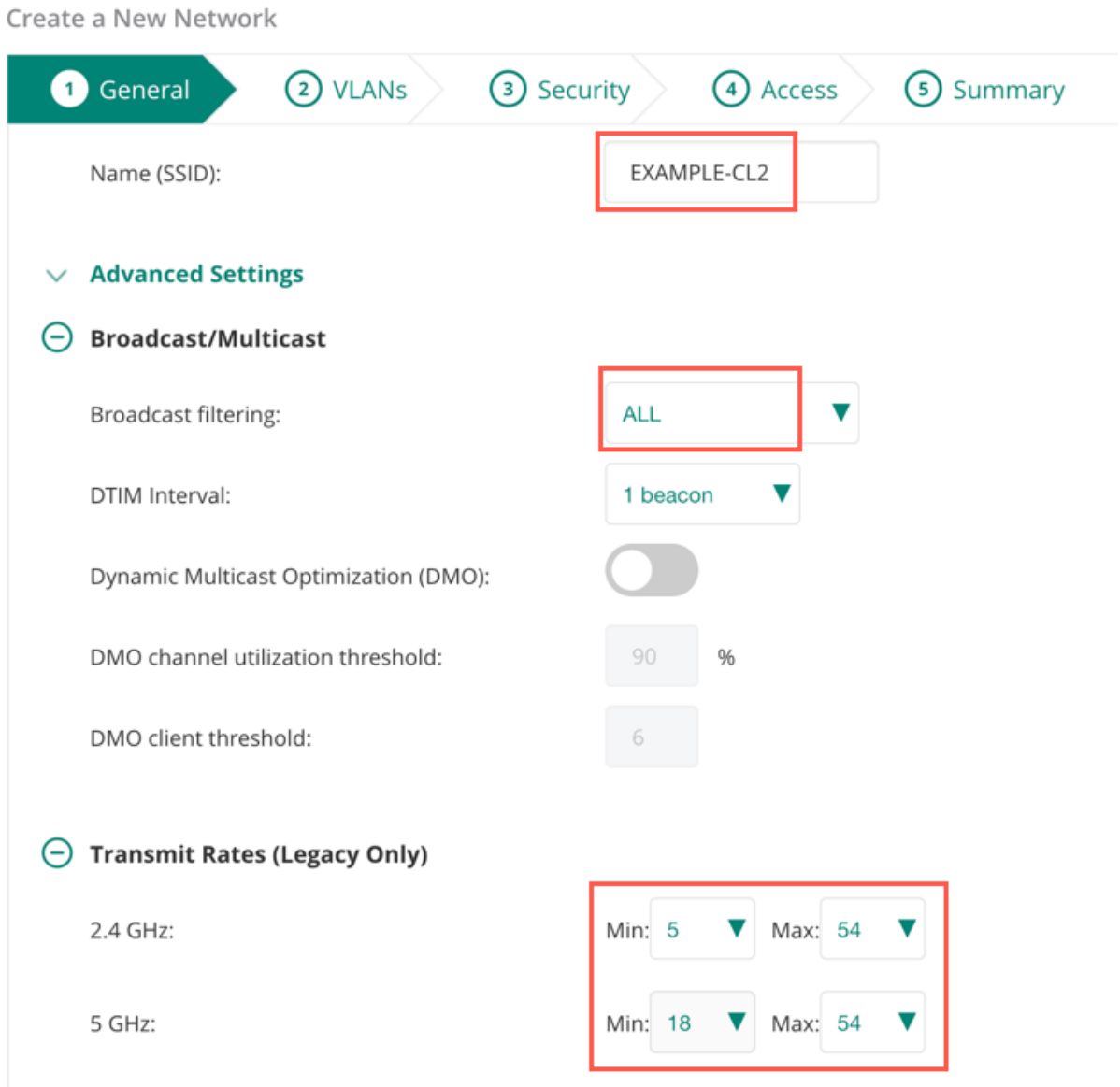


Figure 200: CL2-WLAN-SSID-General

Configure SSID VLAN

On the **VLANs** tab, enter the following values, then click **Next**.

- **Traffic forwarding mode:** *L2 Forwarded*
- **Primary Gateway Cluster:** Select the primary *VPNC headend cluster* to terminate the L2 tunnel from drop-down menu
- **Secondary Gateway Cluster:** (optional) Select the *backup VPNC headend cluster* for VPNC redundancy from the dropdown
- **Client VLAN Assignment:** *Static*
- **VLAN ID**: From the dropdown, select the desired VLAN for users. Example: *tunneled_users (vlan:253)*

NOTE:

The VLAN ID in the dropdown are automatically populated from the selected VPNC Gateway cluster and these are the VLANs already configured on the VPNC side.

NOTE:

CL2 is dependent of having cluster on the VPNC side. In CL2, the VLAN ID and the headend VPNC clusters are selected while configuring the SSID itself without the need to configure them seperately.

Configure SSID Security Settings

Enable 802.1X authentication and encryption on the SSID.

Step 1 To set the security level, move the **Security Level** slider to **Enterprise**.

NOTE:

CL2 mode SSID uses VPNC clusters as the radius proxy when authentication is required.

Step 2 From the **Key Management** dropdown, select *WPA3 Enterprise(CMM 128)*.

CAUTION:

Use WPA3 when possible to benefit from significant security improvements over WPA2. Consult the endpoint documentation to confirm that Microbranch devices support WPA3. If the devices do not support WPA3, use WPA2-Enterprise.

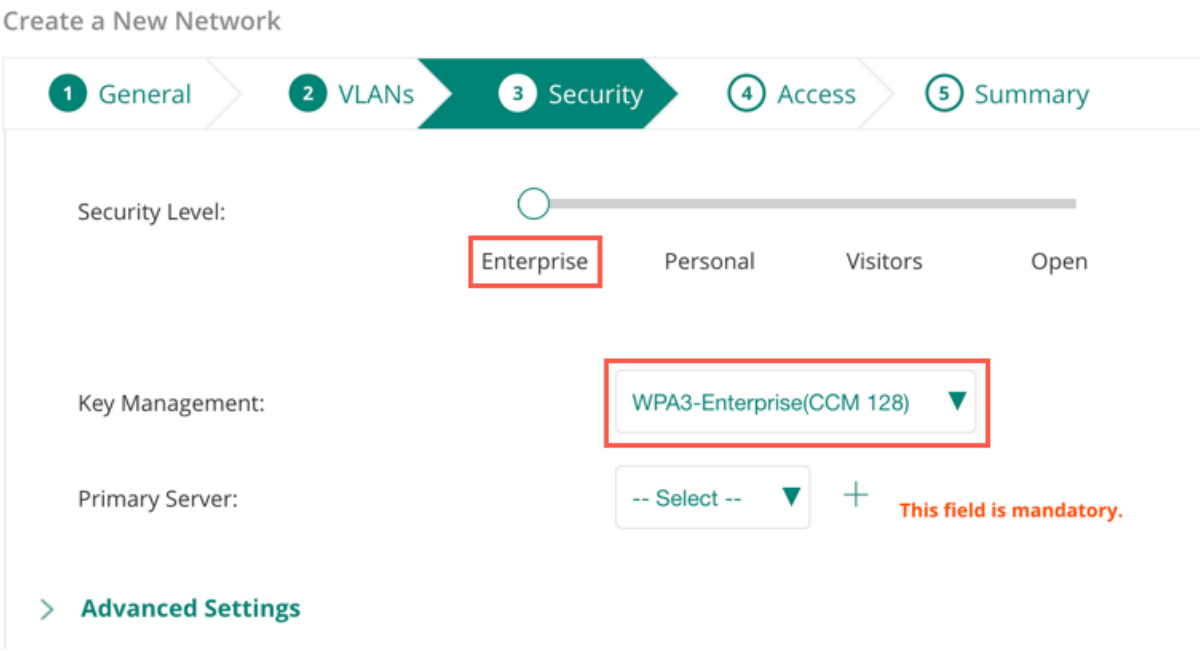


Figure 201: CL2-WLAN-SSID-Security-01

Step 3 To add a primary RADIUS server, beside the **Primary Server** field, click **+** (plus sign).

Step 4 In the **NEW SERVER** window, enter the following values, then click **OK**.

- **Server Type:** *RADIUS*
- **Name:** *cppm-01*
- **IP Address:** *10.2.120.94*
- **Shared Key:** *Enter the RADIUS server shared key*
- **Retype Key:** *Re-enter the RADIUS server shared key*

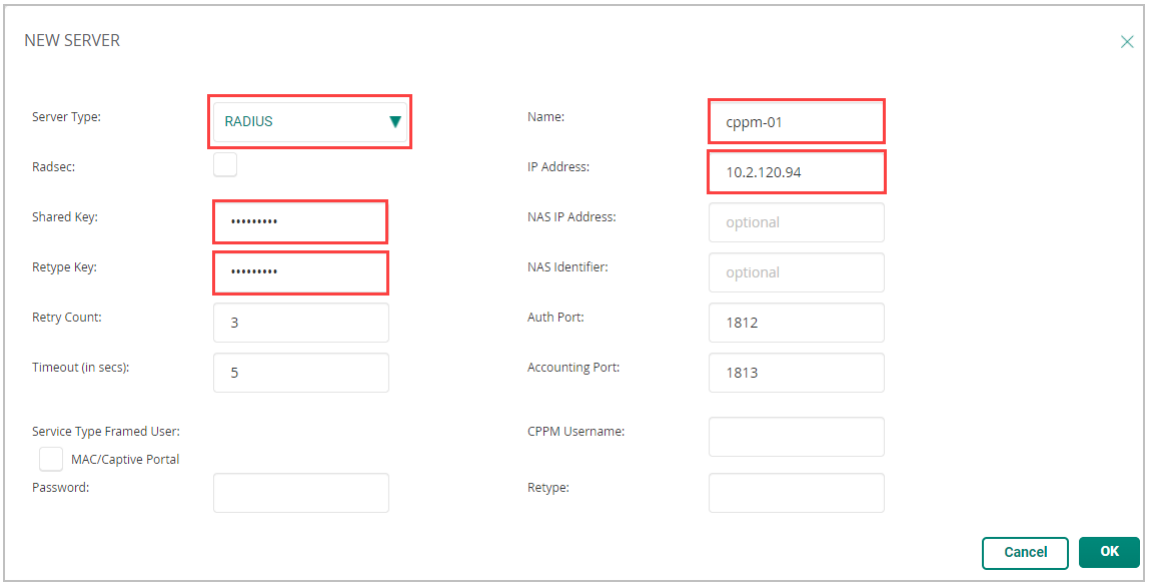


Figure 202: Adding Radius Server

NOTE:

It is important to record the **Shared Key** for use when configuring ClearPass Policy Manager.

Step 5 To add a secondary RADIUS server, beside the **Secondary Server** field, click **+** (plus sign).

Step 6 Repeat step 4 with appropriate values for the secondary RADIUS server.

Step 7 To enable **Load Balancing**, click the toggle.

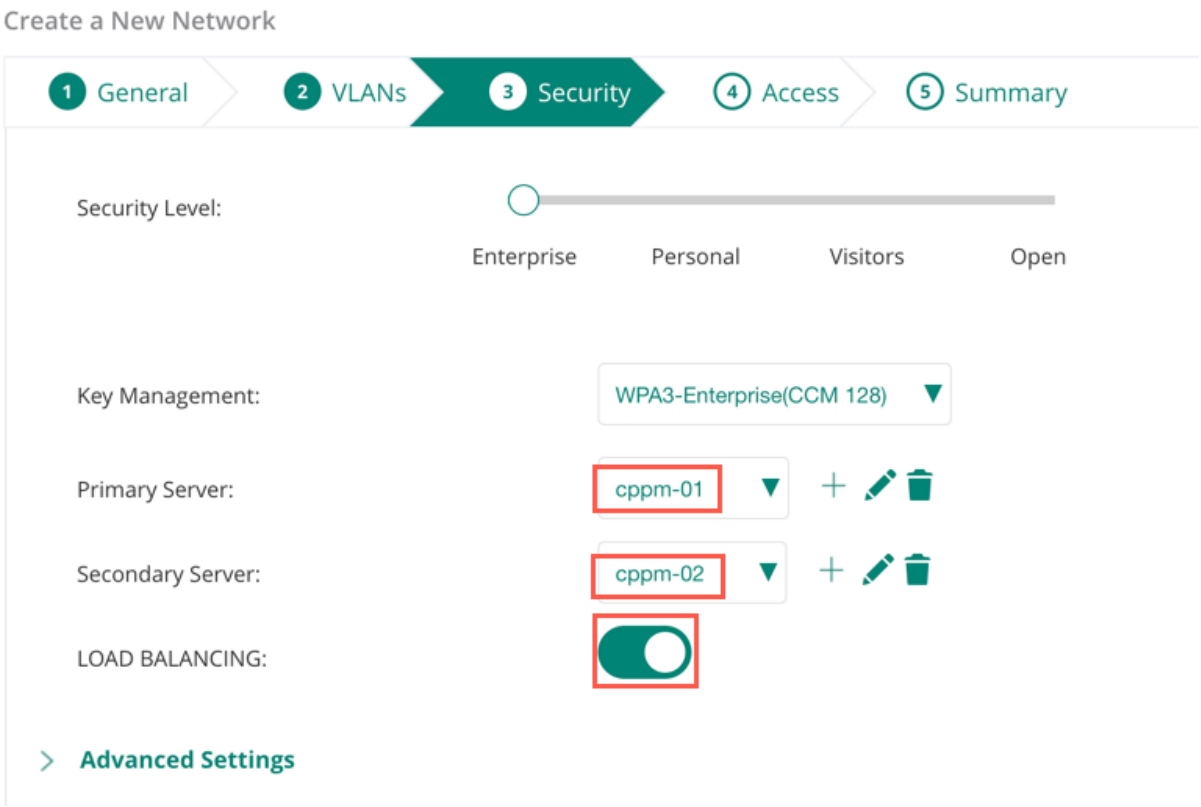
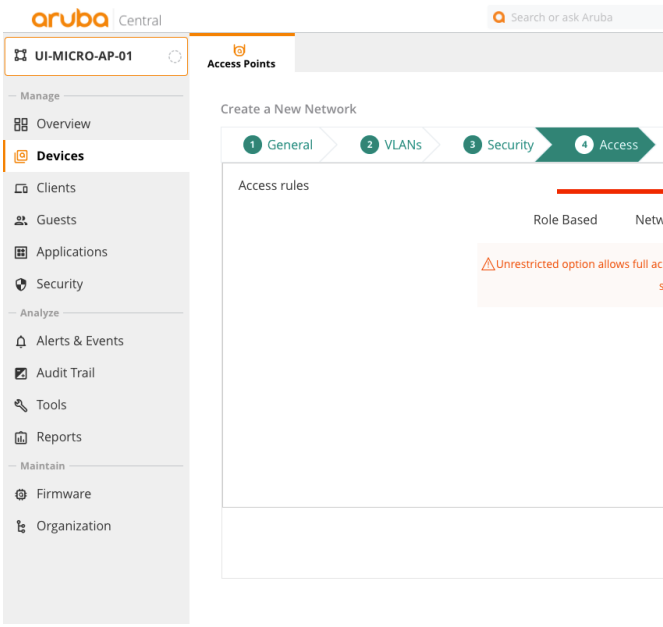


Figure 203: CL2-WLAN-SSID-Security-02

Step 8 Click **Next**.

Configure Network Access Rules

Network access rules apply policy enforcement for an SSID based on the role or IP address of a device.



Step 1 Leave the default setting of *Unrestricted*, then click **Next**.

Step 2 On the **Summary** tab, review all settings and click **Finish**.

CAUTION:

At this point, access to internal resources at the data center are restricted. By default in CL2 mode, the Microbranch AP routes all user traffic to its WAN uplink instead of sending them through the tunnel to the data center.

For the CL2 mode, to handle the user traffic flow at the AP and determine whether to forward all the user traffic to the data center or forward only a selective subset of user traffic to the data center, two options are available.

Step 1 Split-tunnel: The AP tunnels only the user traffic destined to access resources at the data center while other traffic can be locally NATed to the AP WAN uplink (Internet or cellular)

Step 2 Full-tunnel: The AP tunnels all user traffic to the data center

Configure Split-Tunnel in CL2

By default, all user traffic is locally NATed to the AP WAN uplink and does not have access to corporate resources. To allow access to internal resources for CL2, split-tunnel mode is activated by configuring **Policy-Based Routing (PBR)** policy with two or more rules and assigning the PBR policy to one or more user roles. The users or devices assigned to the user role(s) have their user traffic redirected accordingly either through the tunnel to the data center or broken out locally through the AP WAN uplink based on the individual rules configured in the PBR policy.

Create PBR Policy for Split-Tunnel

Step 1 Go to the group **UI-MICRO-AP-01 > Devices** page. In the **Tunnels & Routing** tile, select **Policy-based Routing**.

Step 2 Near the top right of the **Policies** tab, click **+** (plus sign) .

Step 3 Enter the PBR policy **Name**, example: *EXAMPLE-PBR-SPLIT-TUNNEL*

Step 4 Click **OK**

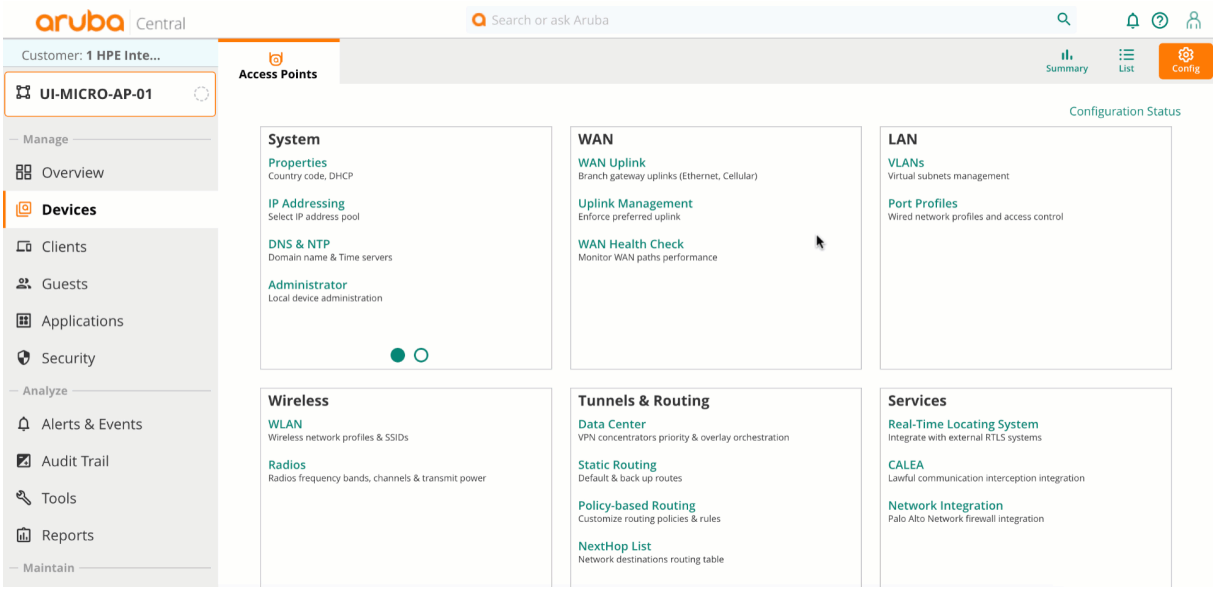


Figure 204: CL2-PBR-Split-Tunnel-New-PBR

NOTE:

When a new PBR policy is added, a default rule to forward all traffic to internet is created automatically.

Step 5 Mouse-over *EXAMPLE-PBR-SPLIT-TUNNEL* policy.

Step 6 Click the **edit** (pencil) icon on the right

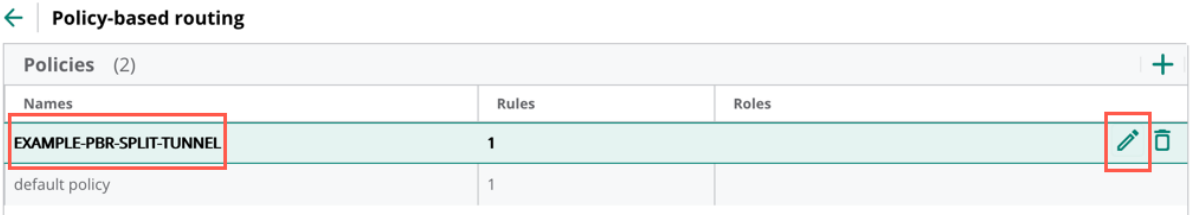


Figure 205: CL2-PBR-Split-Tunnel-edit-policy

Step 7 Near the top right of the **Rules** tab, click **+** (plus sign).

Figure 206: CL2-PBR-Split-Tunnel-add-rule

Step 8 In the **ADD RULE** table, enter the following values, then click **OK**

- **Source:** *Any*
  - Other dropdown options can be selected, such as host, network, alias, etc.
- **Destination:** *Network*
  - Other dropdown options can be selected, such as host, alias, any, etc.
- **Network address:** *<eg: 10.20.253.0> (Internal resource network at Data Center to be accessed by user)*
- **Netmask:** *<eg: 255.255.255.0>*
- **Service/App:** *Any*
  - Other dropdown options can be selected, such as app category, application, protocol, service, TCP, UDP, Web Category, Web Reputation etc.
- **Action:** *Forward to Cluster*

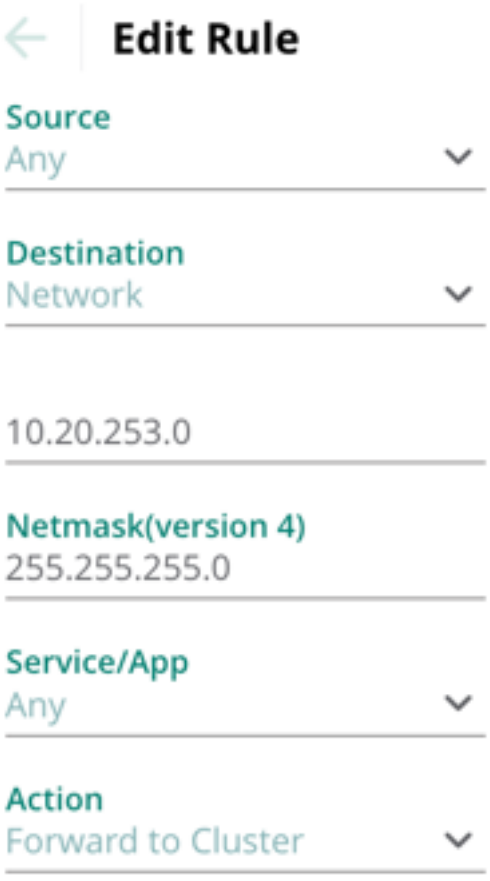


Figure 207: CL2-PBR-Split-Tunnel-rule-add-values

Step 9 The newly created rule is added to the *EXAMPLE-PBR-SPLIT-TUNNEL* policy

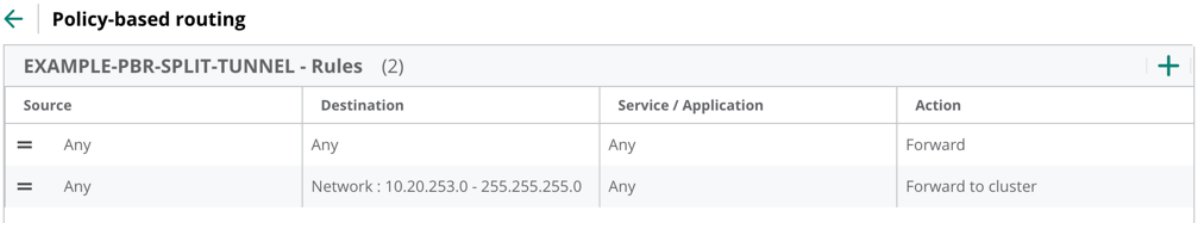


Figure 208: CL2-PBR-Split-Tunnel-list-rules

Step 10 Drag the newly created rule to the top and click **Save**

```
![CL2-PBR-Split-Tunnel-drag-rules](Media/cl2-pbr-split-tunnel-drag-rules.gif)
```

NOTE:

The order of rules in a PBR policy is important. The first rule to match the user traffic takes precedence.

Apply PBR Policy for Split-Tunnel to User Role

Step 1 Go to the group **UI-MICRO-AP-01 > Devices** page. In the **Security** tile, select **Policies & Access Control**.

Step 2 Expand the **Roles** section.

Step 3 Select the user role to which to apply the PBR policy

Step 4 In the **Rules** window, click **+** (plus sign)

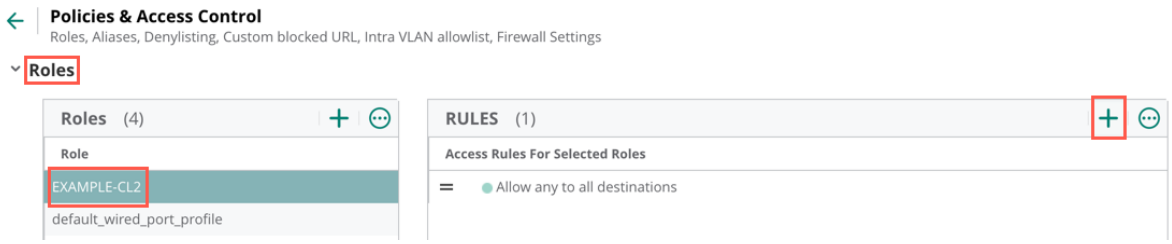


Figure 209: CL2-PBR-assign-role

Step 5 In the **ADD RULE** window, enter the following values, then click **OK**.

- **Rule Type:** *Policy-Based Routing*
- **Add Existing Policy:**
- **Policy Name:** *EXAMPLE-PBR-SPLIT-TUNNEL*

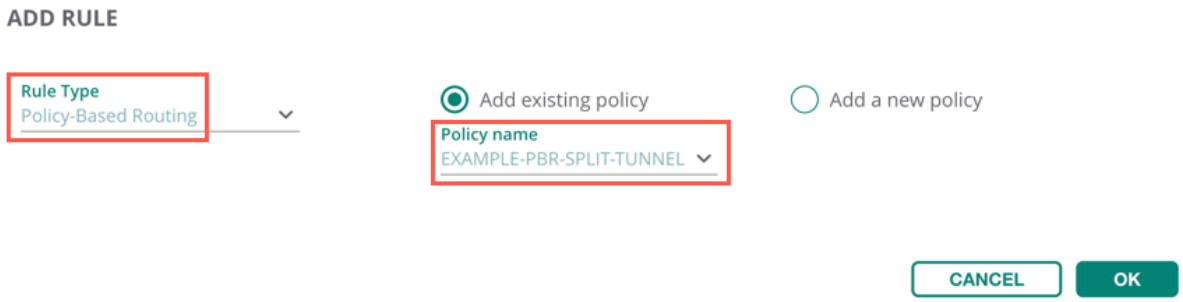


Figure 210: CL2-PBR-Split-Tunnel-assign-user-role

Step 6 The PBR policy is assigned to the user role.

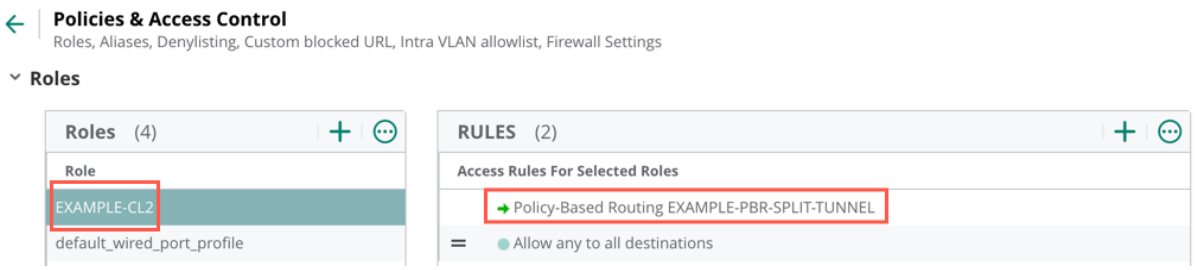


Figure 211: CL2-PBR-Split-Tunnel-assign-PBR-user-role

Step 7 Click **Save**

NOTE:

When a user is assigned a user role and the user traffic flows, all the access rules for the user role are applied first and if there is a PERMIT, the PBR policy is then applied to that specific user traffic.

Configure Full-Tunnel in CL2

To configure full-tunnel in CL2 Microbranch deployments, a **Policy-Based Routing (PBR)** policy should be created first with a rule stating that all user traffic to any destination should be forwarded to the cluster through the secure IPsec tunnel. The PBR policy is then assigned to the user role(s). The users or devices who are assigned to the user role have all their user traffic forwarded to the data center via the secure tunnel.

Create PBR policy for full-tunnel

Step 1 Go to the group **UI-MICRO-AP-01 > Devices** page. In the **Tunnels & Routing** tile, select **Policy-based Routing**.

Step 2 Near the top right of the **Policies** tab, click **+** (plus sign).

Step 3 Enter a PBR policy name *(eg: EXAMPLE-PBR-FULL-TUNNEL)*.

Step 4 Click **OK**.

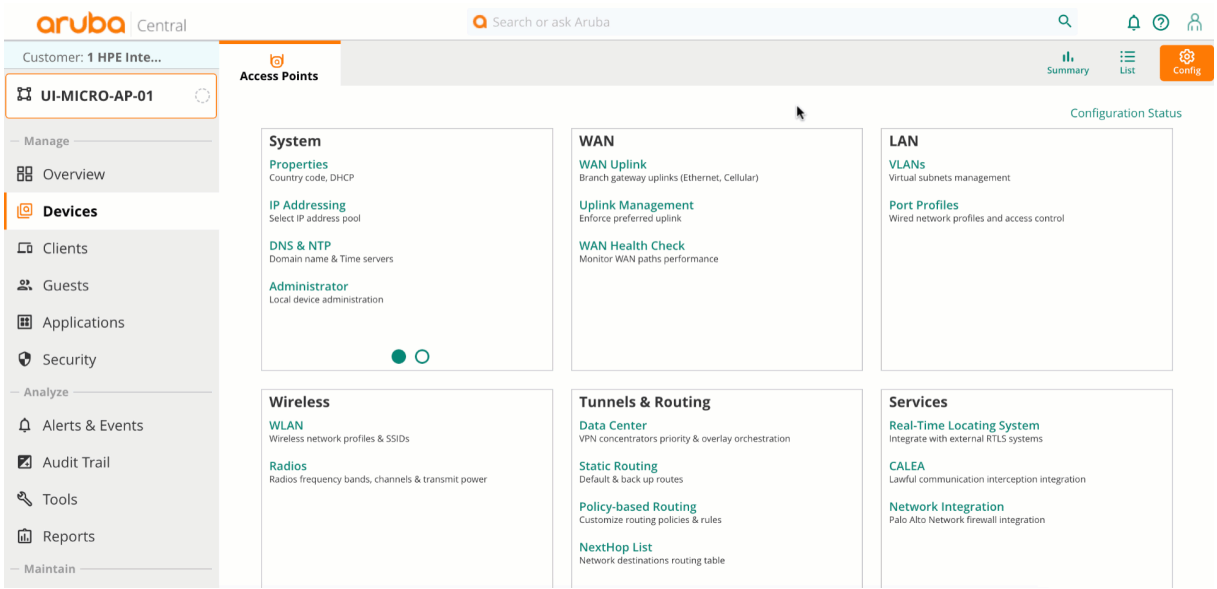


Figure 212: CL2-PBR-Full-Tunnel-New-PBR

NOTE:

When a new PBR policy is added, a default rule to forward any traffic to internet is created automatically.

Step 5 Mouse-over *EXAMPLE-PBR-FULL-TUNNEL* policy and click the **edit** (pencil) icon on the right.

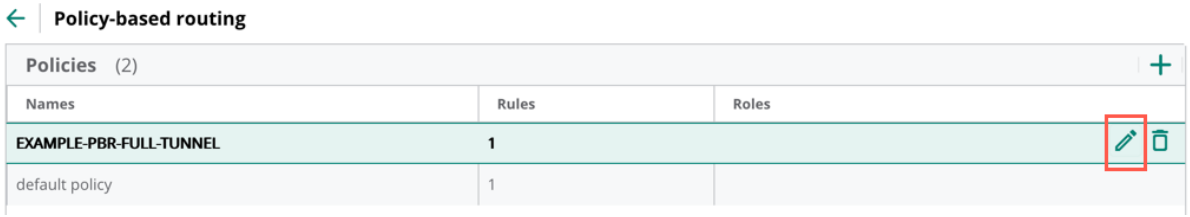


Figure 213: CL2-PBR-Full-Tunnel-edit-policy

Step 6 Mouse-over the default rule that was created automatically.

Step 7 Click the **edit** (pencil) icon on the right.

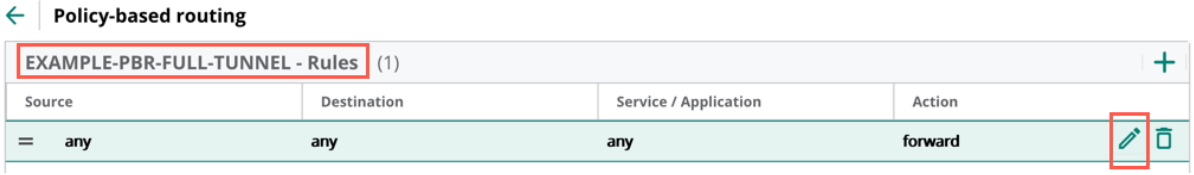


Figure 214: CL2-PBR-Full-Tunnel-edit-rule

Step 8 In the **EDIT RULE** table, enter the following values, then click **OK**.

- **Source:** *Any*
- **Destination:** *Any*
- **Service/App:** *Any*
- **Action:** *Forward to Cluster*

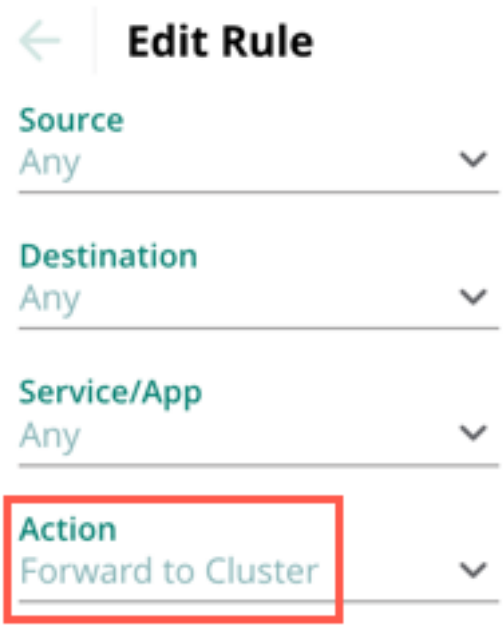


Figure 215: CL2-PBR-Full-Tunnel-edit-rule-Forward-to-cluster

Step 9 The edited rule with action “forward_to_cluster” displays in the *EXAMPLE-PBR-FULL-TUNNEL* policy.

Figure 216: CL2-PBR-Full-Tunnel-rule-Forward-to-cluster

Step 10 Click **Save**.

Apply PBR Policy for Full-Tunnel to User Role

Step 1 Go to the group **UI-MICRO-AP-01 > Devices** page. In the **Security** tile, select **Policies & Access Control**.

Step 2 Expand the **Roles** section.

Step 3 Select the user role to which to apply the PBR policy.

Step 4 In the **Rules** window, click **+** (plus sign).

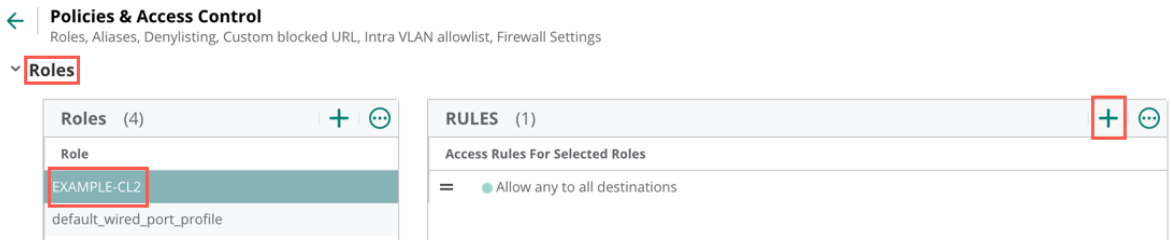


Figure 217: CL2-PBR-assign-role

Step 5 In the **ADD RULE** window, enter the following values, then click **OK**.

- **Rule Type:** *Policy-Based Routing*
- **Add Existing Policy:**
- **Policy Name:** *EXAMPLE-PBR-FULL-TUNNEL*

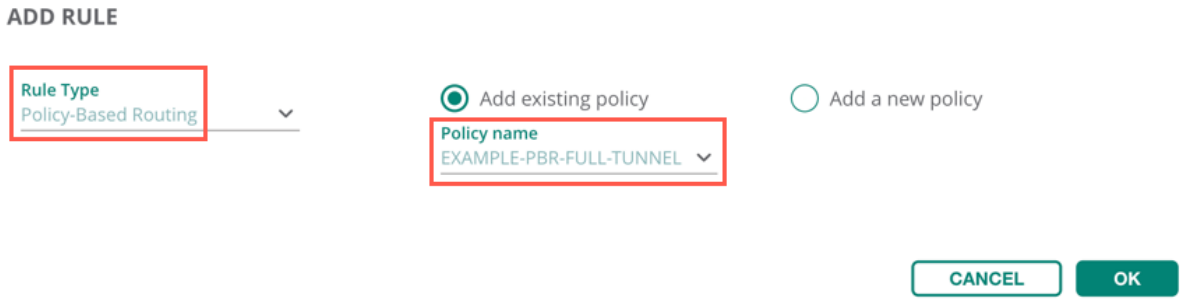


Figure 218: CL2-PBR-Full-Tunnel-assign-user-role

Step 6 The PBR policy configured for full-tunnel is assigned to the user role.

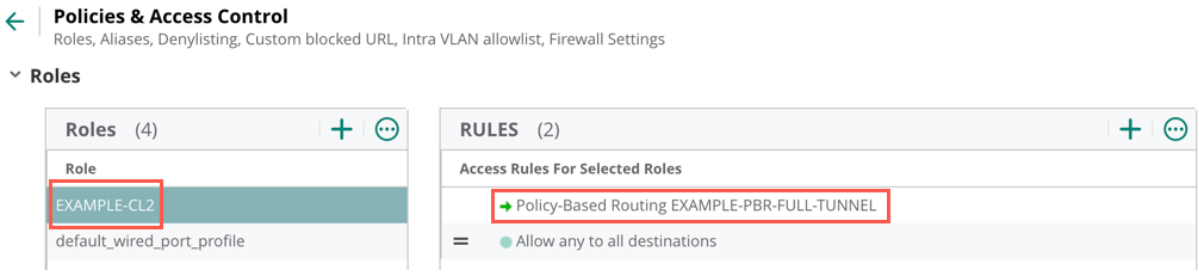


Figure 219: CL2-PBR-Full-Tunnel-assign-user-role-list

Step 7 Click **Save**.

NOTE:

When a user is assigned a user role and the user traffic flows, all the access rules for the user role are applied first and if there is a PERMIT, the PBR policy is then applied to that specific user traffic.

Assign a Microbranch AP to a Group

Step 1 In the left navigation pane, click **Global**, then select the **Groups** column heading.

Step 2 Expand the **Unprovisioned devices** group by clicking the expansion icon (**>**) next to its name.

Step 3 Select the Microbranch AP.

Step 4 Click the **Move Devices** icon.

Step 5 In the **Destination Group** dropdown, select **UI-Micro-AP01**.

Step 6 Click **Move**.

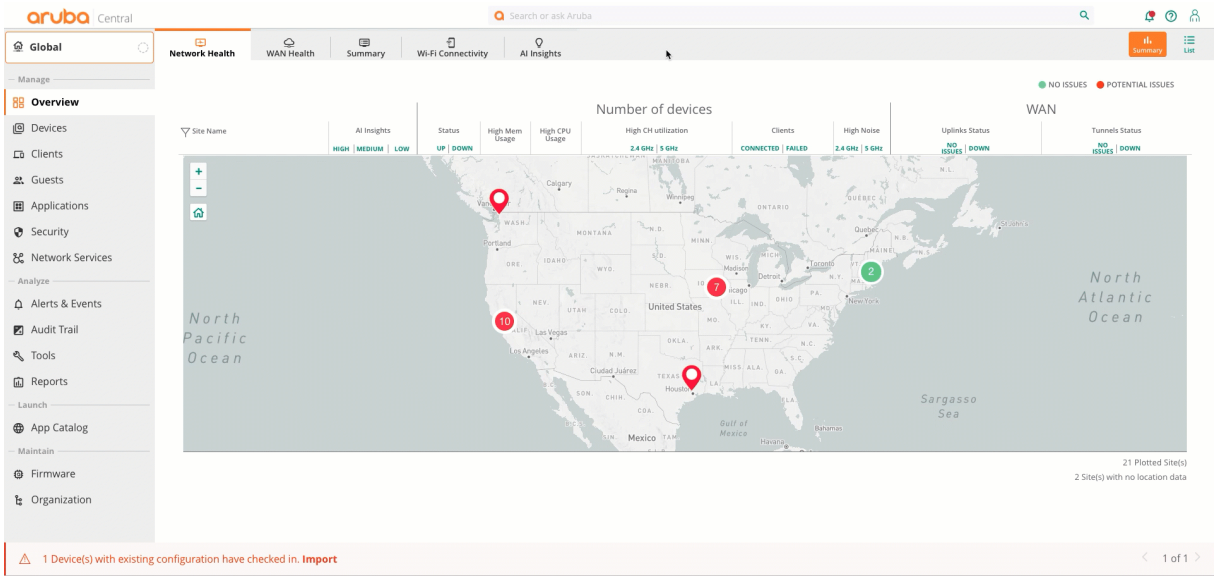


Figure 220: Moving Ap

Assign a Microbranch AP to a Site

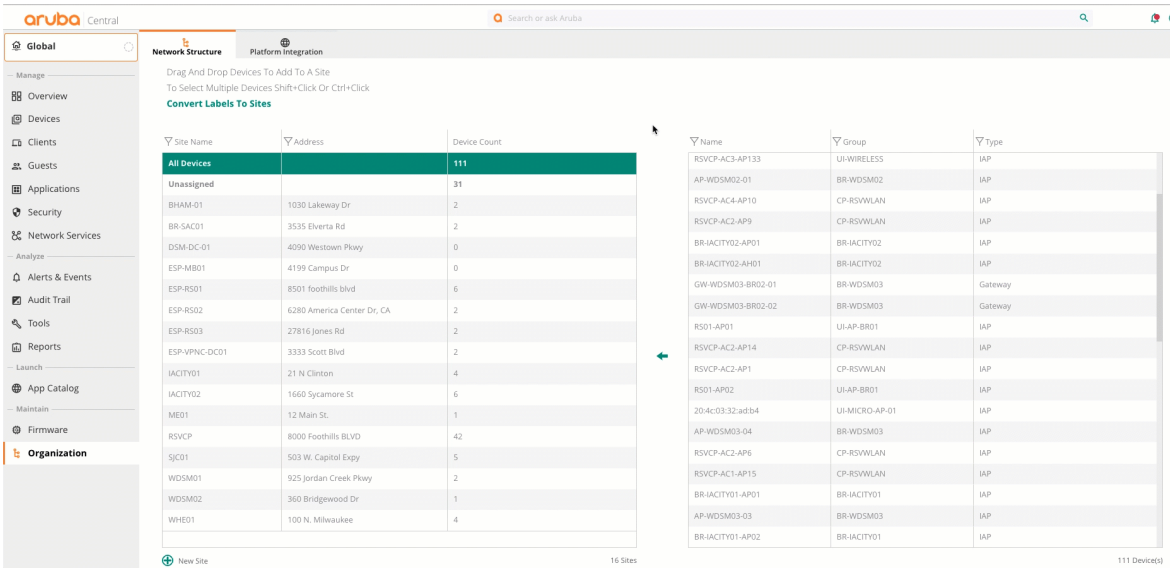
The following procedure assigns the APs to a site.

Step 1 Go to **Organization** and select **Site**.

Step 2 Select **Unassigned** devices.

Step 3 Select the Microbranch AP on the right side, then drag the AP to the **ESP-MB01** site.

Step 4 Click **Yes**.



Monitor Microbranch Site Tunnels

The tunnels for the Microbranch sites can be monitored under SD-WAN overlay tab in a map view along with the tunnel details.

Step 1 Go to **Global > Network Services > SD-WAN Overlay**.

Step 2 Select **Tunnel**.

Step 3 Under **Overlay Tunnel Orchestrator Topology**, click **Spokes** tab.

Step 4 Under the **Spokes Groups**, select the **Microbranch group** where the Microbranch AP resides.

Step 5 In the search filed, select a **Microbranch site** (for which the tunnel details need to be viewed)

1. Hover over the Microbranch site pin location and view the name, total number of tunnels and their status.
2. Hover over the DC pin location(s) to view the headend VPNC(s) and their status.
3. Hover over the tunnel links between the AP and DC, and view their tunnel status.

NOTE:

The number next to the DC pin represents the data center preferences. For example: Number “1” represent primary data center cluster, “2” represents secondary data center cluster and so on.

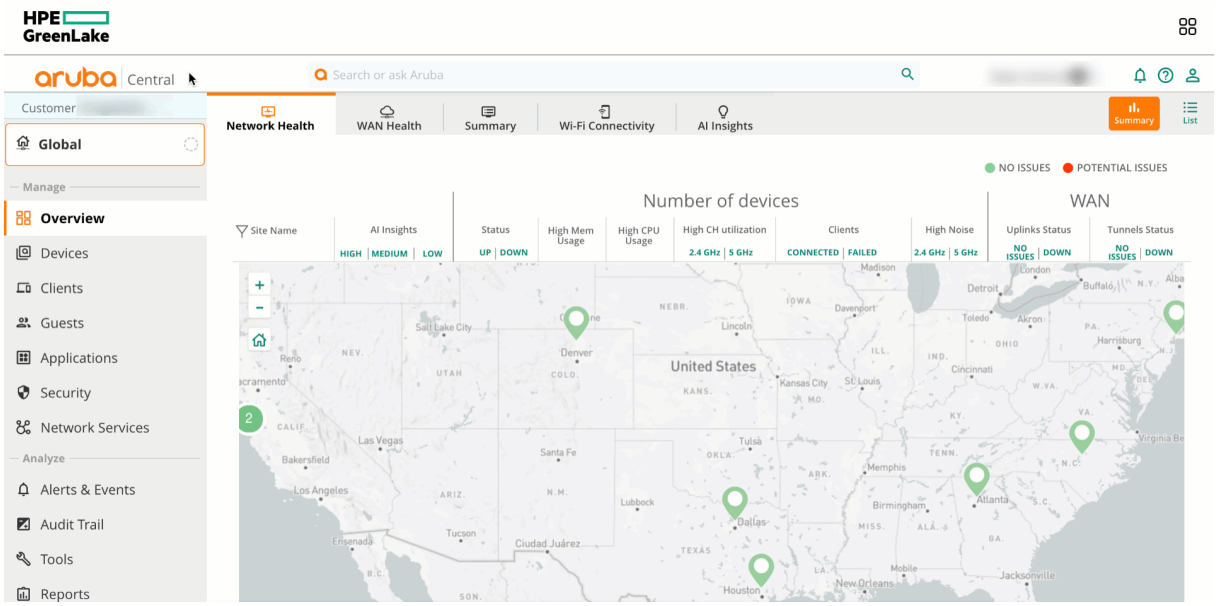


Figure 221: sdwanoverlay-tunnel-status

In CL2, the Microbranch AP establishes tunnels to all VPNCs in primary cluster as well to VPNCs in secondary cluster. In below screenshots, there are total of three IPSec tunnels established from Microbranch AP:

- Two tunnels established to the two VPNCs in primary DC.
- One tunnel established to the one VPNC in secondary DC.

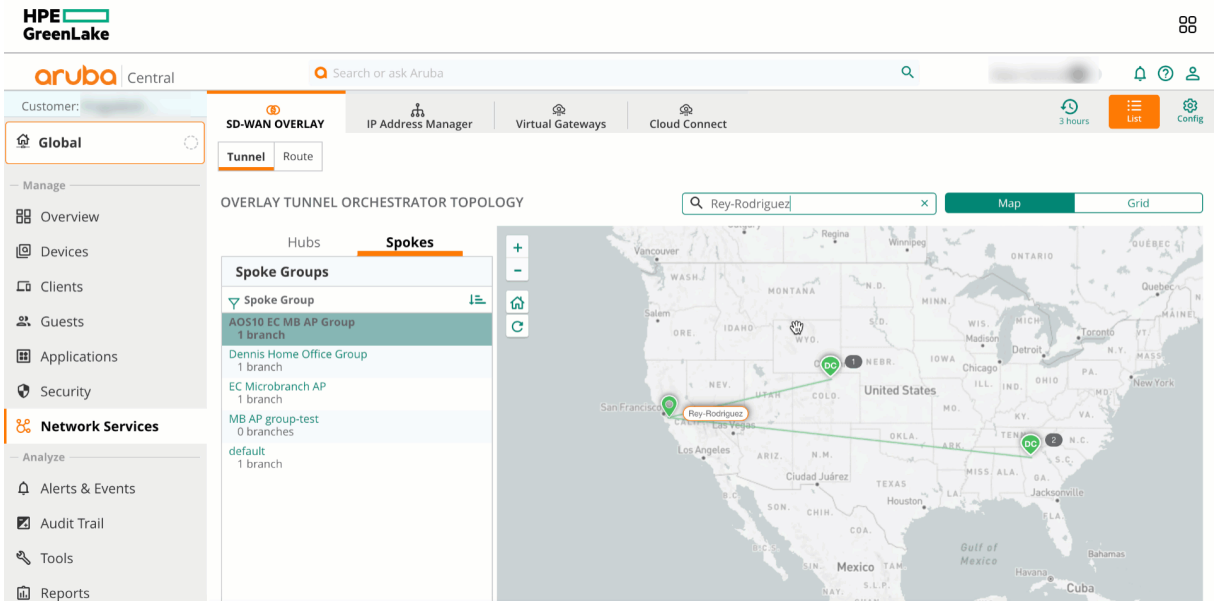


Figure 222: sdwanoverlay-tunnels-both-DC-clusters

```
Rey-Rodriguez-MB-AP# show crypto ipsec stats

IPSEC STATS
-----------
MAP NAME                                        IP ADDR         DEVNAME  TX/RX PACKETS   TX/RX BYTES          TX/RX DROPS  TX/RX ERRORS
--------                                        -------         -------  -------------   -----------          -----------  ------------
gw-ipsecmap-20:4c:            -uplink-eth0      10              tun0     449252/448863   49131332/49090320    0/0          0/0
gw-ipsecmap-20:4c:            -uplink-eth0      10              tun1     431001/430611   47135200/47093554    0/0          0/0
gw-ipsecmap-02:1a:            -uplink-eth0      10              tun2     449725/449317   49183020/49140660    0/0          0/0
```

Figure 223: image-20230920144053194

More details about the tunnels such as tunnel endpoints, public IP, private IP, SPI, next rekey, tunnel event logs, etc. can also be viewed.

Step 1 Click the tunnel link between the Microbranch AP and the DC

Step 2 In the pop-up window, expand each row to view individual tunnel details

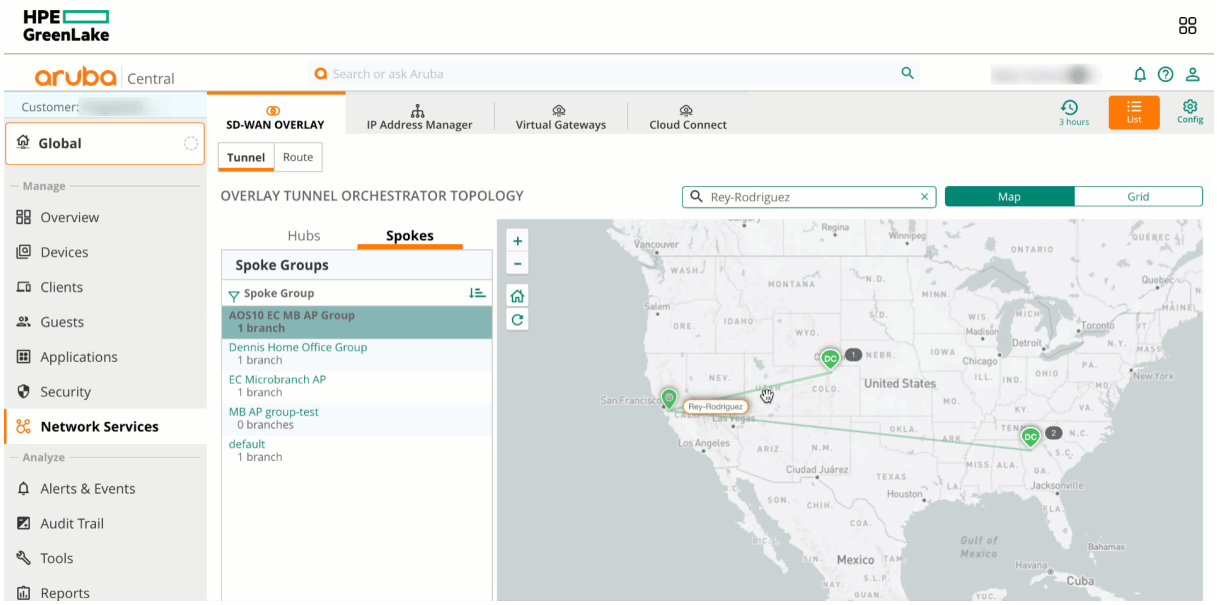


Figure 224: sdwanoverlay-tunnel-details

The **control channel state** for the Microbranch AP can also be viewed by selecting the control connection as below:

Step 1 Go to **Global > Network Services > SD-WAN Overlay > Tunnel > Spokes**

Step 2 Under the **Spokes Groups**, select the **Microbranch group** where the Microbranch AP resides.

Step 3 In the search filed, select a **Microbanch site** (for which the control channel state need to be viewed)

Step 4 Scroll to the bottom and select **Control Connections**

Step 5 Expand the row to view more details

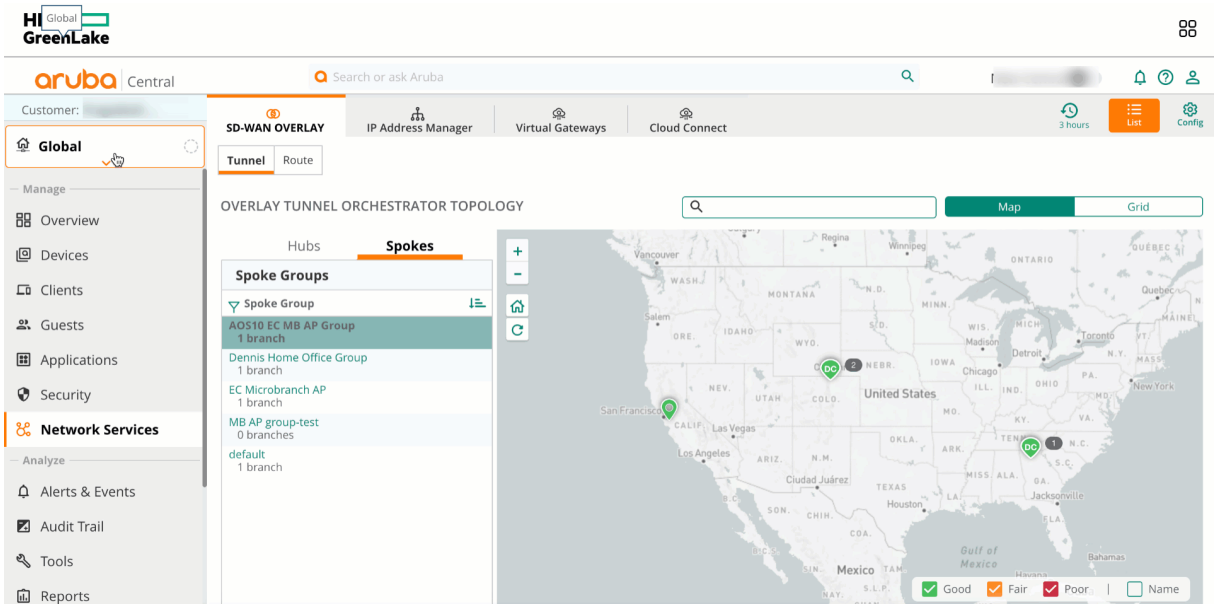


Figure 225: sdwanoverlay-tunnel-control-connection

Monitor Microbranch Site Routes

For each Microbranch site, the routes learnt from the Microbranch AP and the routes advertised to the Microbranch AP can be monitored in SD-WAN overlay tab as below.

Step 1 Go to **Global > Network Services > SD-WAN Overlay**.

Step 2 Select **Routes**.

Step 3 Under **Overlay Tunnel Orchestrator Topology**, click **Spokes** tab.

Step 4 Under the **Spokes Groups**, select the **Microbranch group** where the Microbranch AP resides.

Step 5 In the search filed, select a **Microbranch site** (for which the route details need to be viewed).

Step 6 Scroll to the bottom to view control connections details for the Microbranch AP in the above selected site.

Step 7 Under **Routes Learned** column, the number denotes the number of routes learned from this Microbranch AP.

1. Click on the number to view the actual routes learned from the Microbranch AP.

Step 8 Under **Routes Advertised** column, the number denotes the number of routes advertised to this Microbranch AP (and eventually stored in the route table).

1. Click on the number to view the actual routes advertised to the Microbranch AP.

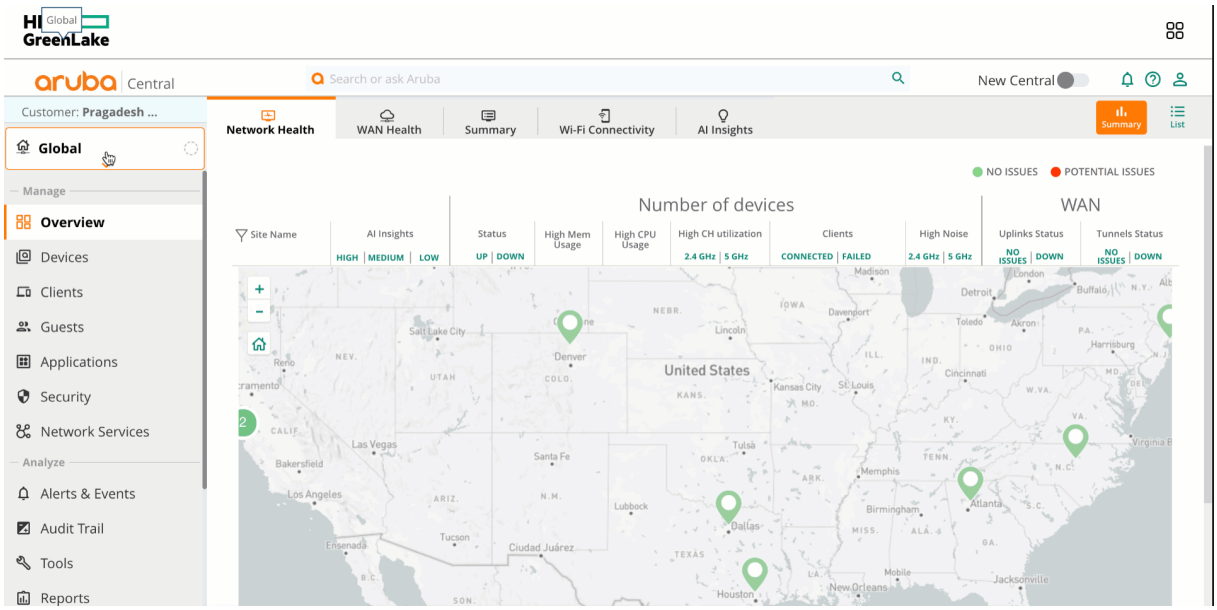


Figure 226: sdwanoverlay-routes

The Microbranch uplink statistics such as WAN status, type, availability, usage, throughput, utilization, etc. can be viewed under **Global > Overview > WAN Health > List > Transport**

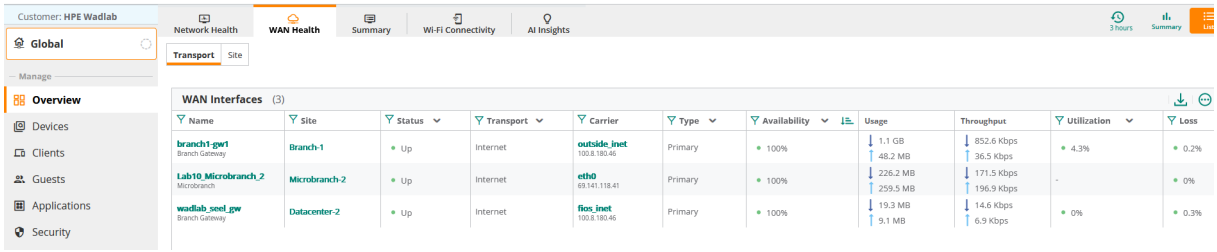


Figure 227: Microbranch-WAN-Health

Validated Hardware

The following hardware and software versions were validated for this guide. For compatibility, please upgrade to the versions listed below (or higher).

Wireless Gateways

Product Name	Software Version
Aruba 7240XM	10.4
Aruba 9240	10.4
Aruba 9012	10.4
Aruba 9004	10.4

Wireless Access Points

Product Name	Software Version
Aruba AP 500 Series	10.4
Aruba AP 300 Series	10.4

Wired Access

Product Name	Software Version
Aruba CX 6400	10.10.0002
Aruba CX 6300	10.10.0002
Aruba CX 6200	10.10.0002
Aruba 3810	16.11.0005
Aruba 2930M/F	16.11.0005

Management and Orchestration

Product name	Software version
Aruba Central	2.5.6
Aruba ClearPass Policy Manager	6.9.11

Verifying Aruba SD-Branch Hub Spoke Topology

This section explains how to verify the SD-Branch topology.

Verify SD-WAN Tunnels

Check the VPNCs first because they manage the aggregation of all branch gateway tunnels.

To verify that the tunnels are up, navigate to the **UI-VPNC-SD-WAN** and select one of the VPNCs. Select **WAN** from the left navigation pane to view and verify that all tunnels are up.

Repeat this step for the second VPNC.

Verify that the following is displayed:

- **Status** is *Up*.
- **Availability** is trending upward or *100%*.

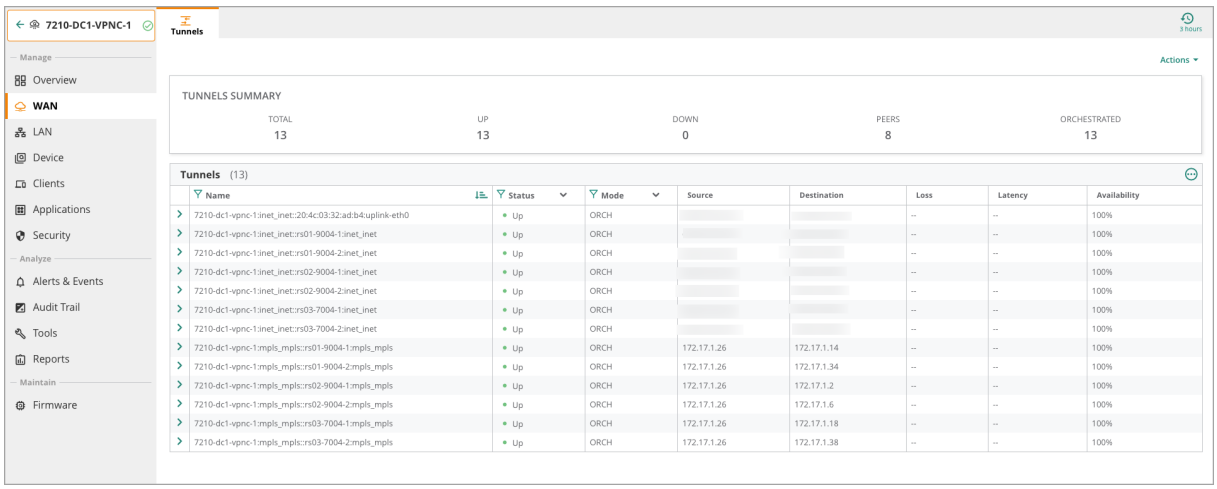


Figure 228: VPNC Tunnels

Click **Tools** on the left menu. Select the **Console** tab, log into the console, and use the **show crypto ipsec sa** option to see the tunnel type

Verify that the following is displayed:

- **Tunnel Type** is *Hubandspoke.*
- **Flags** display *UTIt.*

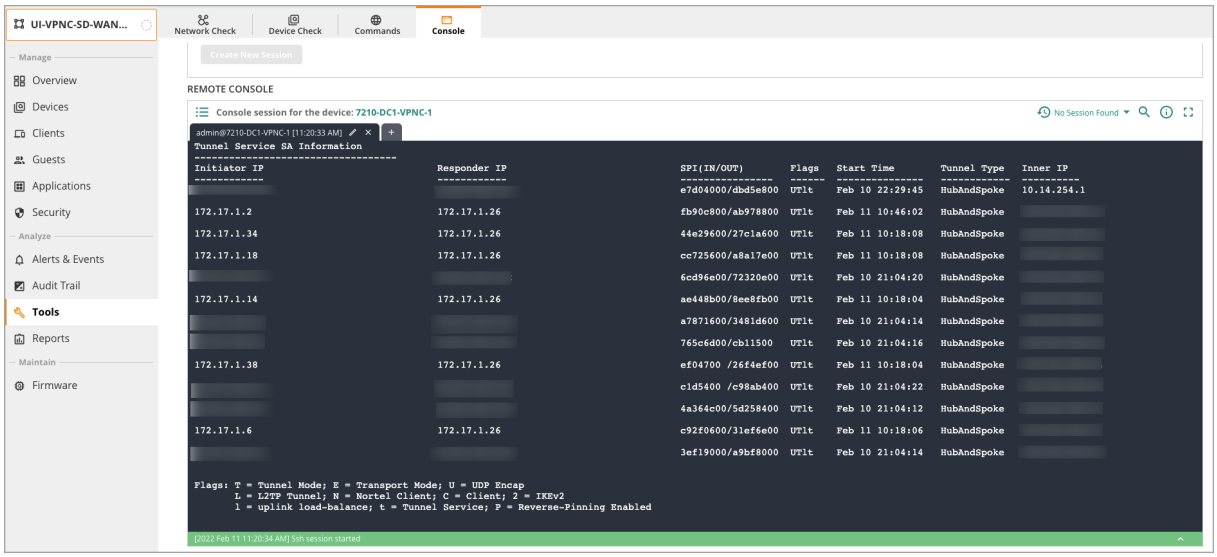


Figure 229: Tunnel Security association

Go to **UI-BGW-01** and select one of the Branch Gateways. Select **WAN**, then select the **Tunnels** tab.

Verify that the following is displayed:

- **Status** is *Up*
- **Availability** is trending upward or *100%*

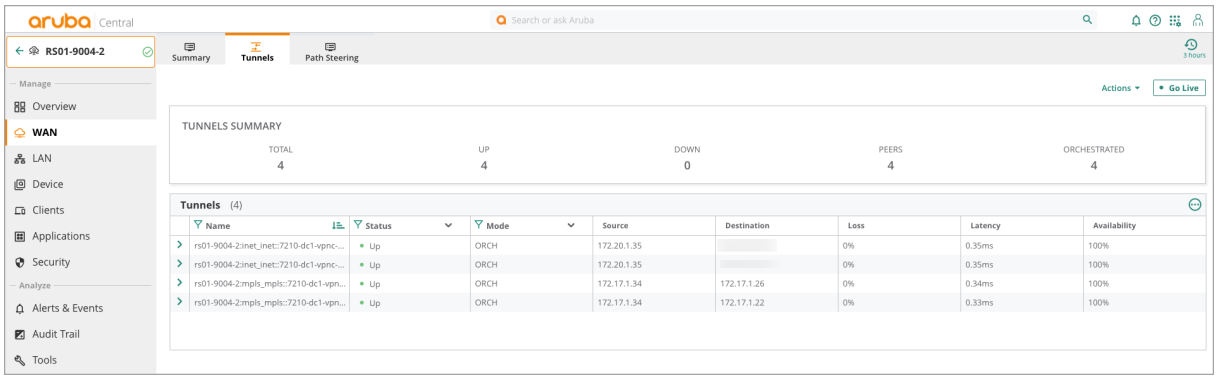


Figure 230: Branch Tunnels

Verify Routes

Select the **UI-VPNC-SD-WAN** group. Select one of the Branch gateways. On the **Overview** page, select the **Routing** tab.

Select **Overlay**, then change the overlay details to **Routes learned**.

Verify that summarized routes are learned using the overlay.

Ensure the following is displayed:

- **Summary** routes from each branch

- **Availability** is trending upward or *100%*.

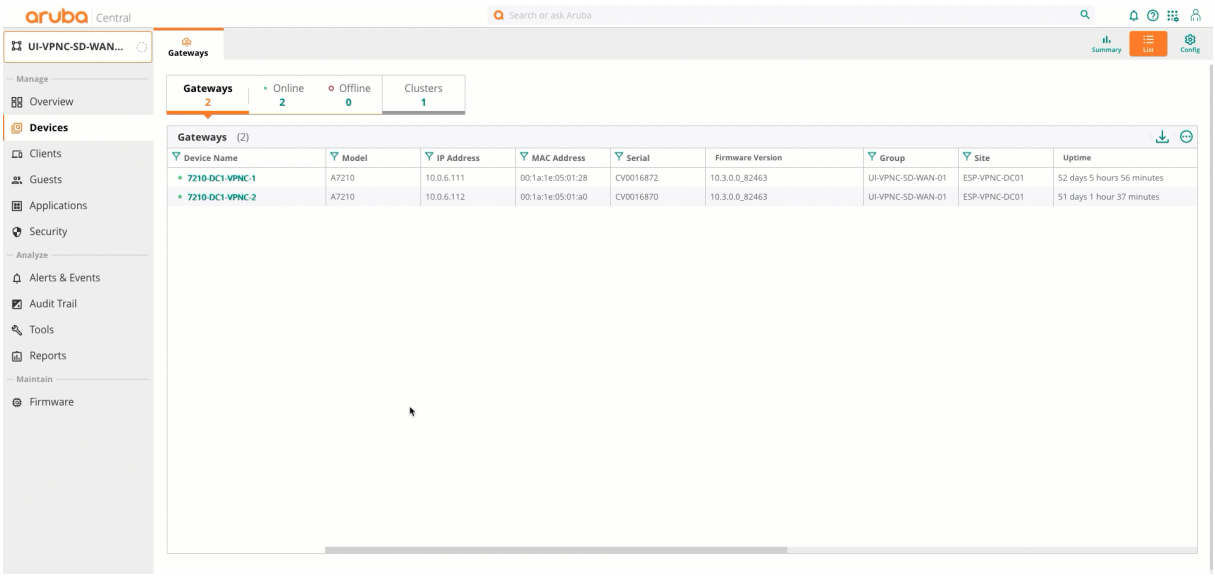


Figure 231: Verify VPNC Route table

Select the **UI-BGW-01** group. Select one of the Branch Gateways. On the **Overview** page, select the **Routing** tab.

Select **Overlay** and change the overlay details to **Routes learned**. Verify that routes are learned via using overlay.

Ensure the following is displayed:

- A summary route for the campus network is learned via the **Overlay**.

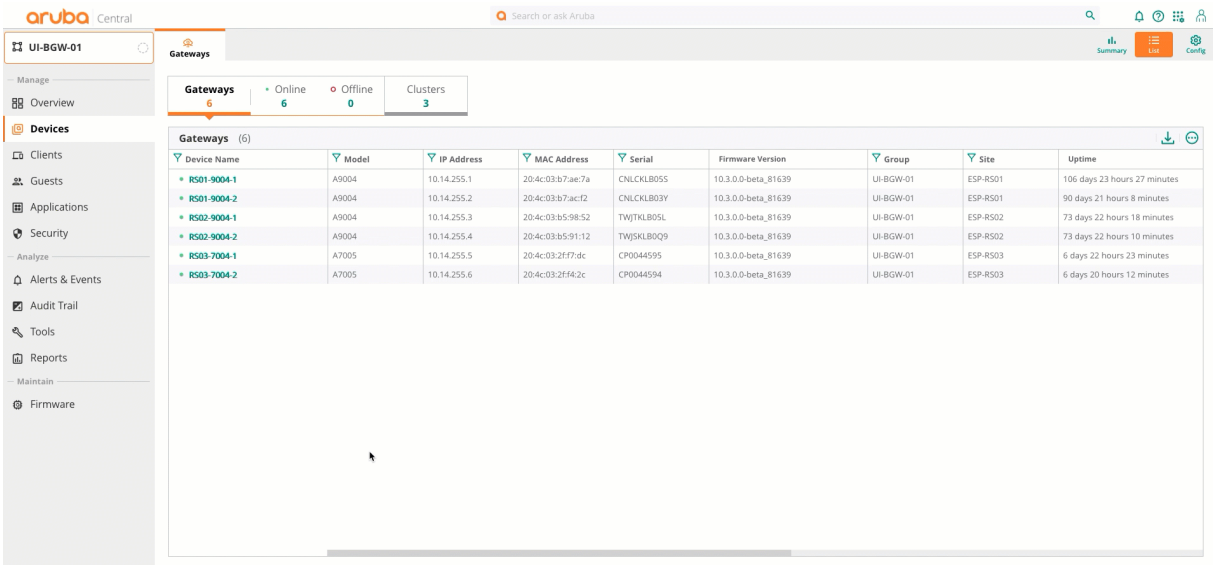


Figure 232: Verify BGW Route Table

Verify NTP

Verify the NTP configuration using the **show ntp status** command.

Verify that the following is displayed:

- The **NTP status** is *enabled*.
- The **NTP server connections** are in the *default VRF*.
- The **reference time** is correct for the timezone

These values indicate the NTP service is reachable by the switch.

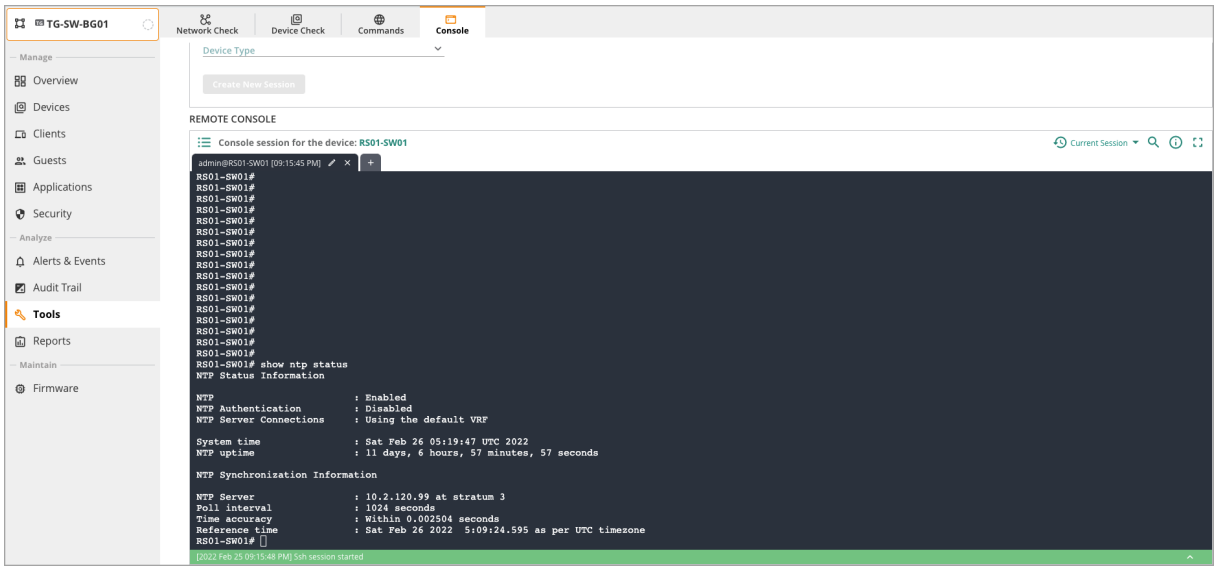


Figure 233: Verify NTP

Verify DHCP Snooping

Verify the DHCP Snooping and ARP inspection configurations using the **show dhcpv4-snooping statistics**, **show dhcpv4-snooping binding**, and **show arp inspection statistics vlan** commands.

Verify that the following is displayed:

- **Packet-Type**: server, **Action** is *forward*.
- **Packet-Type**: client, **Action** is *forward*.

The non-zero values indicate that DHCP snooping is actively forwarding traffic from servers and clients.

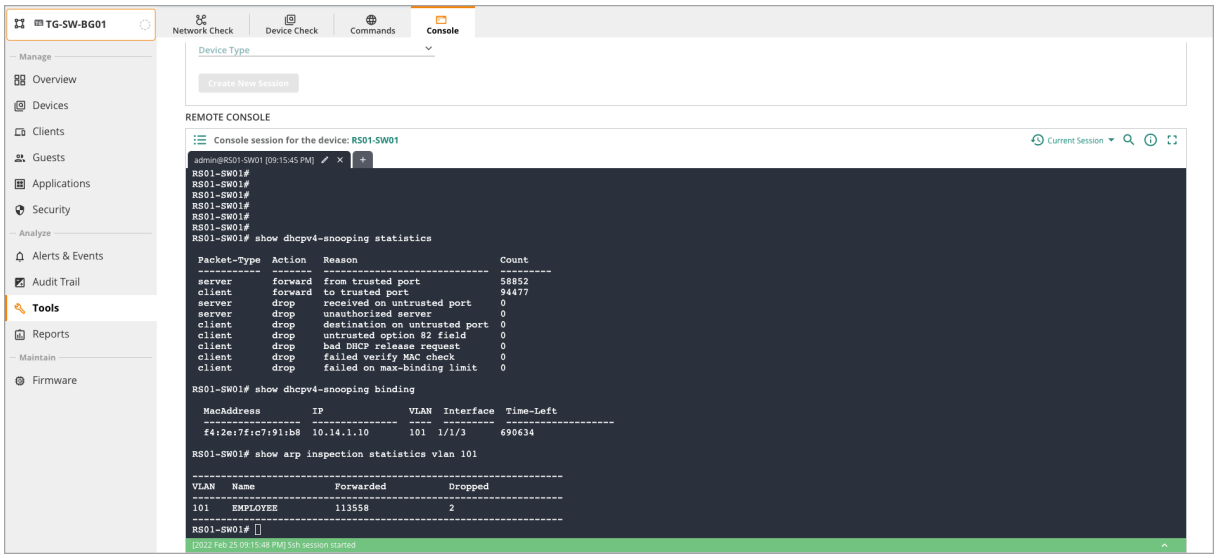


Figure 234: Verifying DHCP-Snooping

Verify Radius

Verify the RADIUS configuration using the **show radius-server** command.

Ensure the following is displayed:

- Both servers are reachable, without a "*" before their name.
- The **VRF** is set to *default*.

These values indicate that the RADIUS servers are reachable in the correct VRF.

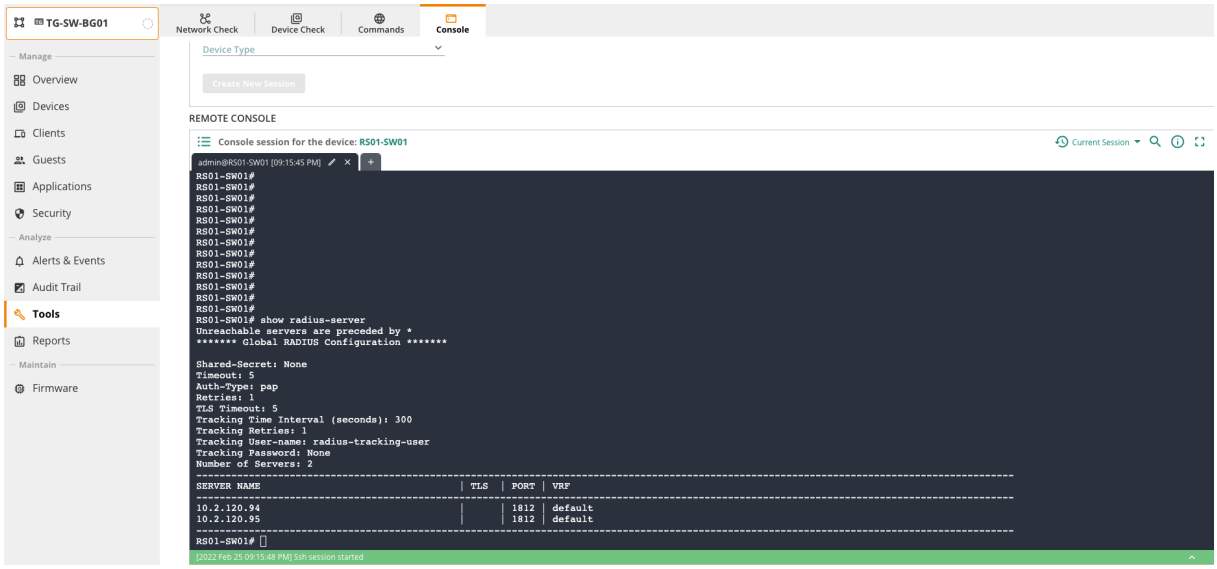


Figure 235: Verify Radius Connectivity

Verify Device Profile and Radius Authentication

Verify the device profile configuration using the **show port-access clients** and **show port-access device-profile all** commands.

Verify that the following is displayed:

- **Radius Onboarding** displays *Success*.
- The **Authorization Details** are applied.
- The **VLAN** is displayed.
- The **device-profile onboarding method** is a *Success*.
- The **profile name** and **LLDP group state** are applied

These values indicate the device profiles are applied and devices are onboarded.

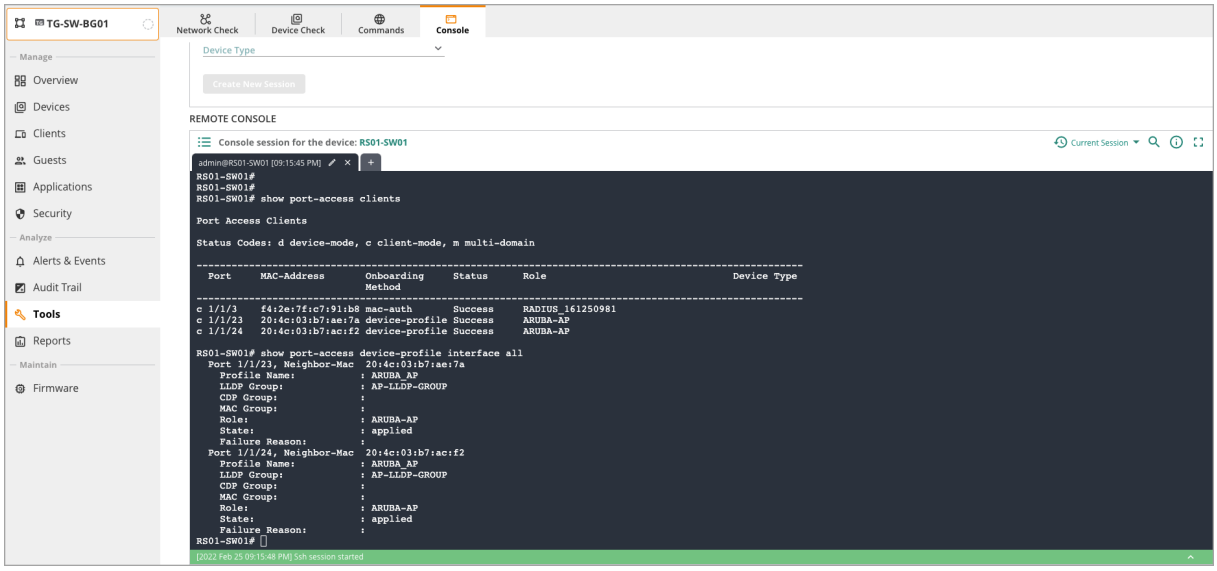


Figure 236: verifying Device profiles and Radius Authentication

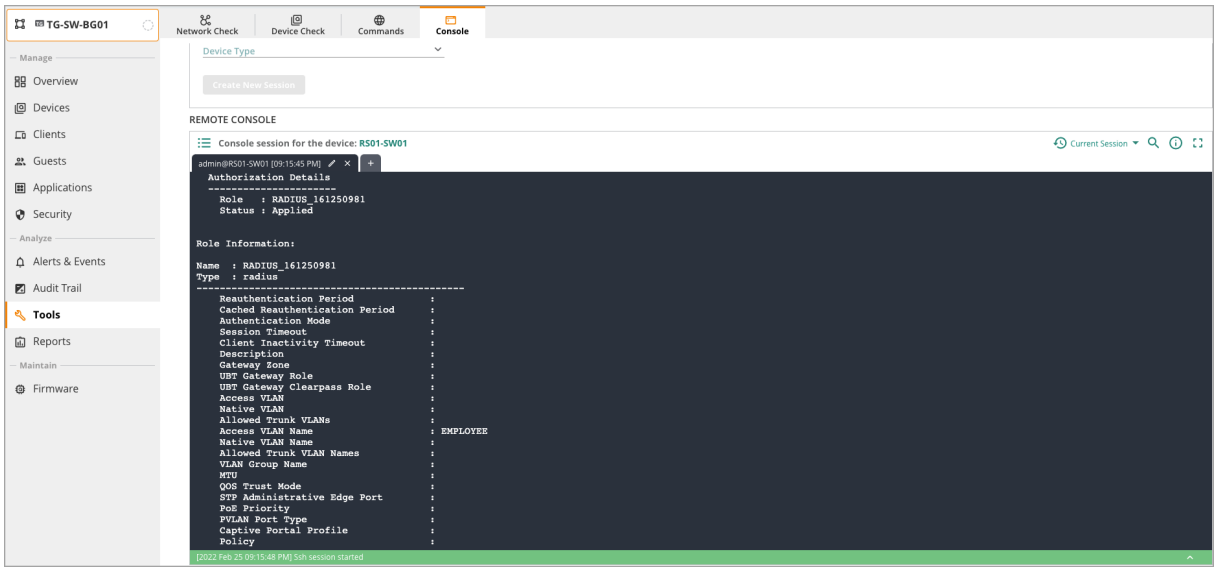


Figure 237: Verify Radius profile is applied

www.arubanetworks.com

3333 Scott Blvd. Santa Clara, CA 95054
1.844.472.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550