aruba
a Hewlett Packard Enterprise company

Validated Solution Guide

ESP CAMPUS VOLUME 2

Deployment Guide

Table of Contents

About This Guide

This document is from a family of technology guides called Aruba Validated Solution Guides (VSG). VSGs are cross-portfolio solution guides that cover multiple technology areas, including wired, wireless, data center, SD-WAN, and security. They are validated by Aruba's Solution TME and Solution Quality Assurance teams on an ongoing basis using a rigorous process. A VSG provides prescriptive guidance focused on the Aruba recommended best practices specific to the solution being covered.

The goal is to describe a solution implementation which addresses the primary use cases for customer networks, while avoiding the corner cases. The intent is to enable partners and customers to efficiently install end-to-end solutions using Aruba technology in a consistent and repeatable manner. The result will be improved stability and supportability by limiting the number of deployment variations.

VSGs are categorized into volumes to differentiate each guide type from the others.

Volumes

1 - *Design:* Identify products and technologies to meet customer business requirements
2 - *Deploy:* Step-by-step set of procedures to build the solution
3 - *Operate:* Recommended procedures to maintain and optimize the solution

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

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

The Aruba ESP Campus provides the following benefits:

- Specific functions of individual layers make the network easier to operate and maintain.
- Modular building blocks quickly scale as the network grows.
- Location-independent network access improves employee and guest productivity.
- Hard-to-wire locations receive network connectivity without costly construction.
- Plug-and-play wireless deployment with wired LAN switches preconfigured to recognize APs.
- Centralized control of wireless environment is easy to manage and operate.
- Reliable wireless connectivity, including complete RF spectrum management, is available with key Aruba management features.
- Simplifies configuring, managing, and operating, by using cloud-based controls.

Simple, repeatable designs are easier to deploy, manage, and maintain. This guide shows recommended deployment options and general guidance for which options to use.

Purpose of This Guide

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

Aruba VSG: Campus Design

Design Goals

The overall goal is to create a simple scalable design that is easy to replicate at different sites. The components are limited to a specific set of products to help with operations and maintenance. The design has a target of sub-second failover when a network device or link between two network devices becomes unavailable. The protocols are tuned for a highly available network in all functional areas. This guide can be used to deploy new networks. It is not intended as an exhaustive discussion of all options, but rather to present the most recommended designs, features, software, and hardware.

Audience

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

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

Customer Use Cases

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

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

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

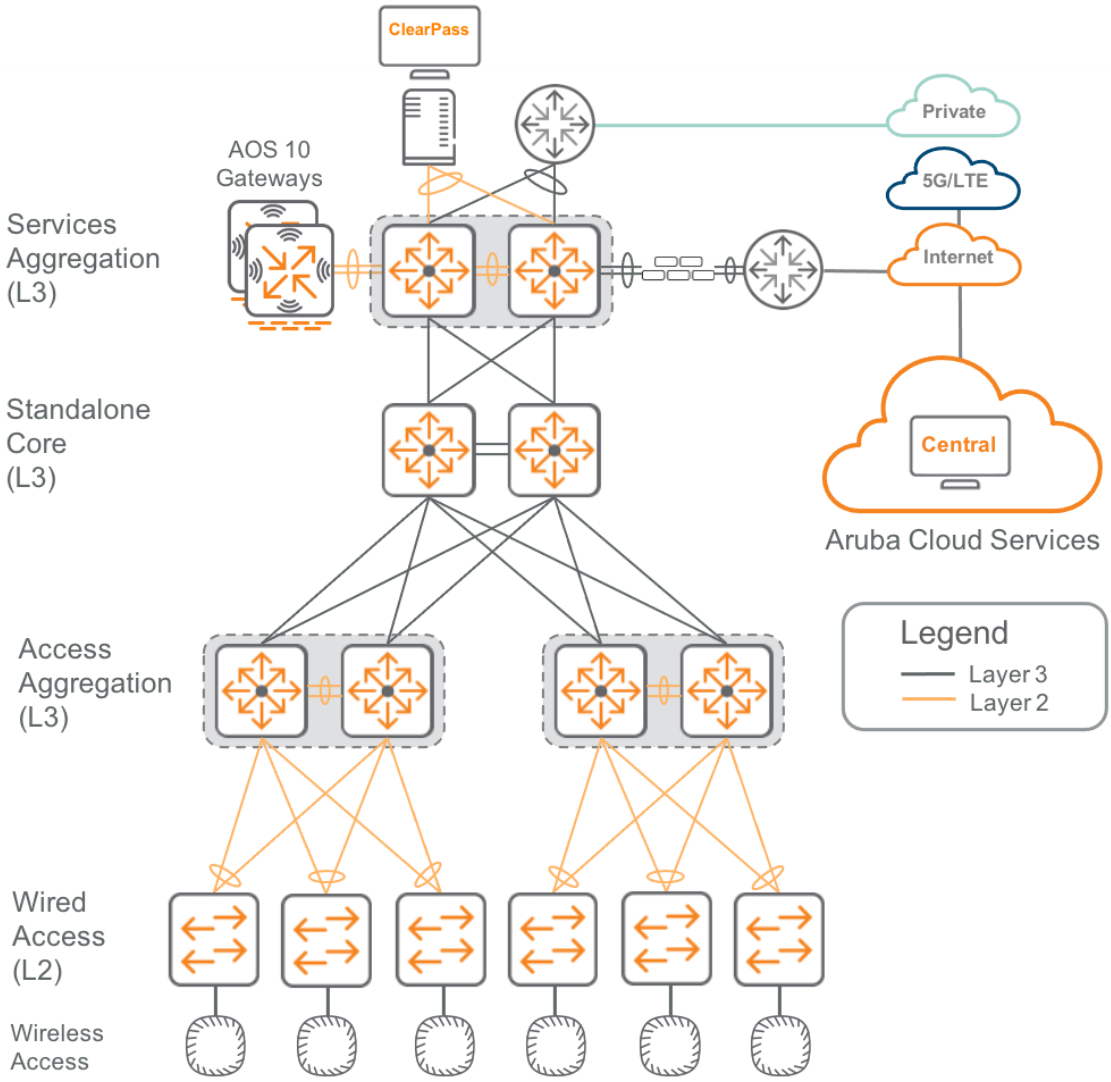
Before wireless became the primary network access method, typical network designs provided two or more wired ports per user. It was common to run two network drops to each user's desk and then have additional ports for conference rooms, network printers, and other shared areas, adding up to just over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

Deploying the Campus Network

This deployment guide is based on the large campus topology referenced in the Campus design guide which includes a three-tier architecture consisting of a routed core, services aggregation, access aggregation, and access. In this design, the access switches are Layer 2 adjacent to the access aggregation and have a single management IP address. Access aggregation switches provide a physical aggregation of access devices for a building and act as the gateway for all downstream access devices. Aggregation and access devices have IP addresses in the 10.X.X.X range for access VLAN's.

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

Campus Topology



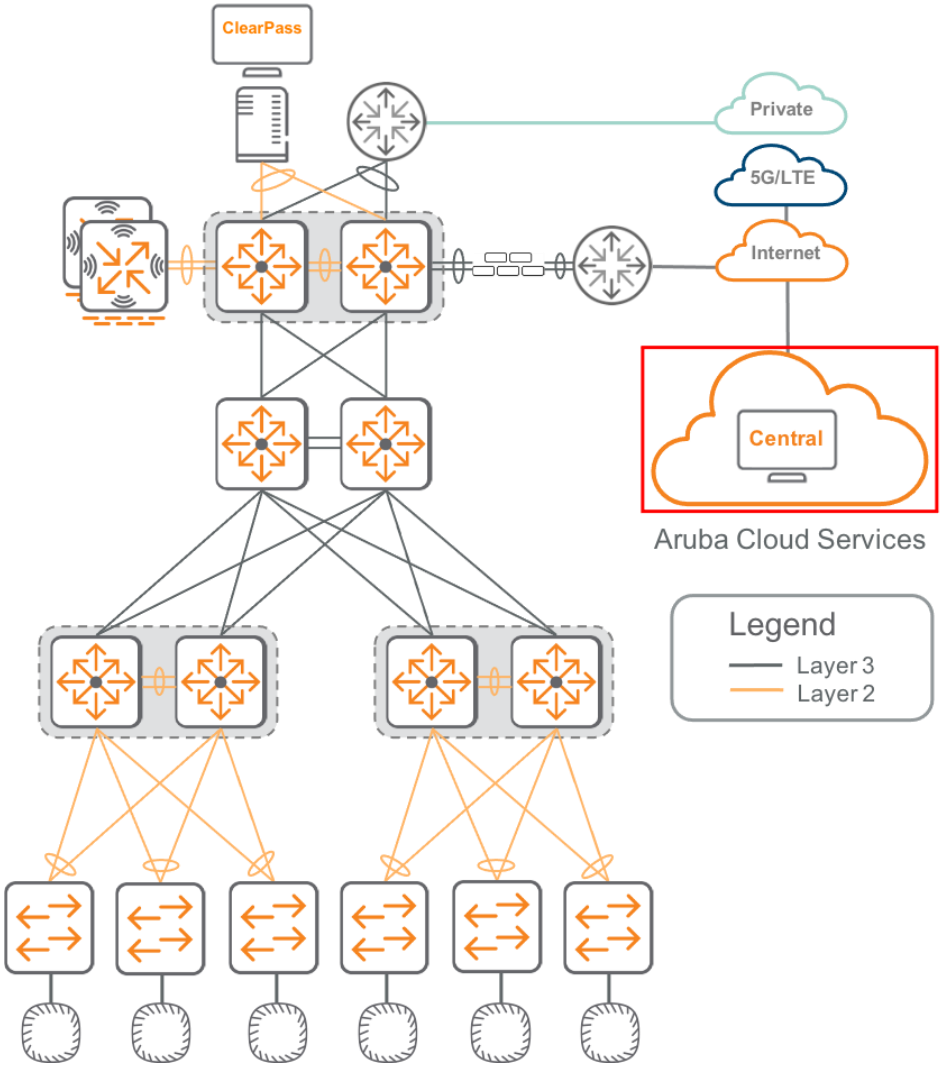
Aruba ESP offers a breadth of services, including onboarding, provisioning, orchestration, analytics, location tracking, and management. AI Insights reveal issues before they impact users allowing an organization to accomplish tasks quickly and easily with intuitive workflow-centric navigation using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

Aruba Central

Aruba Central is a cloud-based platform to configure, manage and monitor the ESP Campus network. Designed as a software-as-a-service subscription-based set of applications, Central provides a standard web-based interface that allows access to the network from anywhere. The hierarchical configurations provide operational efficiency; the monitoring and alerting streamlines day-2 operations and the historical data reporting helps with auditing and troubleshooting.

NOTE:
The content in the Aruba ESP Campus is based on Aruba Central version 2.5.3. To verify the version of Central you are running, select the “?” Icon in the upper right corner of any page and choose “Documentation Center”. The Help page URL will have the Central version listed after the website name.

Aruba Central



Account Home Page

The Aruba Central **Account Home** page provides access to the **Network Operations** application, which is a dashboard for configuration, monitoring, reporting, and troubleshooting.

The **Account Home** page also provides access to global settings. In this guide, the following global setting areas will be used:

- Key Management
- Device Inventory
- License Assignment

Network Operations App

The Aruba Central Network Operations app is the main application for configuring, monitoring, reporting, and troubleshooting your network. You use the navigation bar on the left to change the context of the main screen. In this guide, we focus on configuration and use the following areas:

- *Filter drop-down list*—Select the groups or sites that you need to configure or monitor.
- *Overview*—Review Network Health, WAN Health, Summary of Network status, Wi-Fi Connectivity, and AI Insights.
- *Devices*—Manage and configure Access Points, Switches, and Gateways.
- *Clients*—Manage and configure Clients and Client Profiles.
- *Guests*—Manage and configure Guest Access and Presence Analytics.
- *Firmware*—Set compliance and upgrade firmware across multiple devices, platforms, groups, sites, and labels.
- *Organization*—Manage groups, sites, and labels.
  - *Groups* are the parent level for a two-level hierarchical network configuration (Group and Device levels). You use groups to apply common parameters to a group of devices.
  - *Sites* group all devices into a single location. You use sites to monitor devices, not to configure them.
  - *Labels* provide additional user-defined context for monitoring devices.

Create New Groups

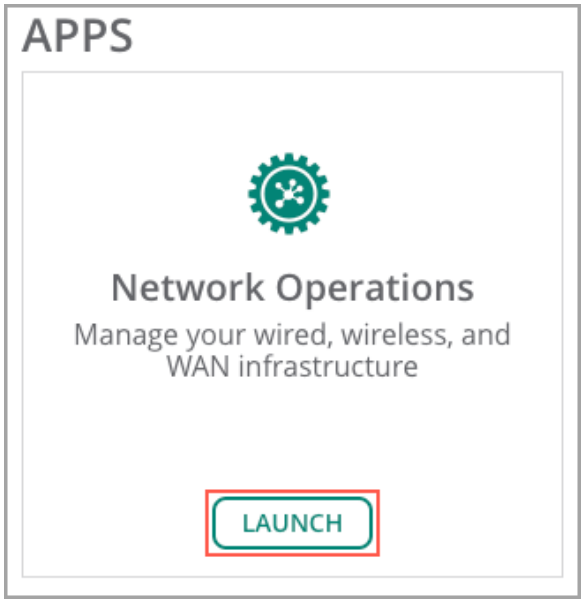
Aruba Central uses a two-level hierarchy for configuration tasks. A device's final configuration is a result of configuration that is applied at the group level, along with configuration applied at a device level. Parameters added at the device level override the configuration performed at the group level. Aruba recommends performing the bulk of the configuration at the group level and only using device-level configurations when specific overrides are needed.

Aruba Central allows the grouping of different types of devices, such as APs, Gateways, and switches in inventory. These devices can be configured using UI workflows or templates, and the preferred configuration method is chosen when creating a new group. If an organization has a large number of Aruba Gateways and switches that require bulk configuration, the configuration template feature can quickly provision the devices.

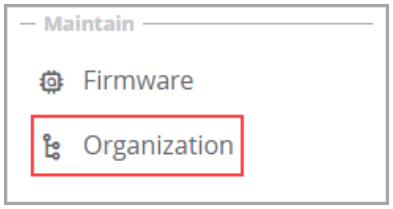
NOTE:
You must assign a group to a device prior to configuring the device.

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

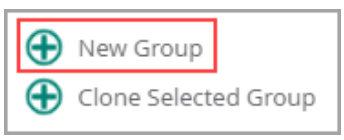
Step 2 On the Aruba Central Account Home page, launch the **Network Operations** app.



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

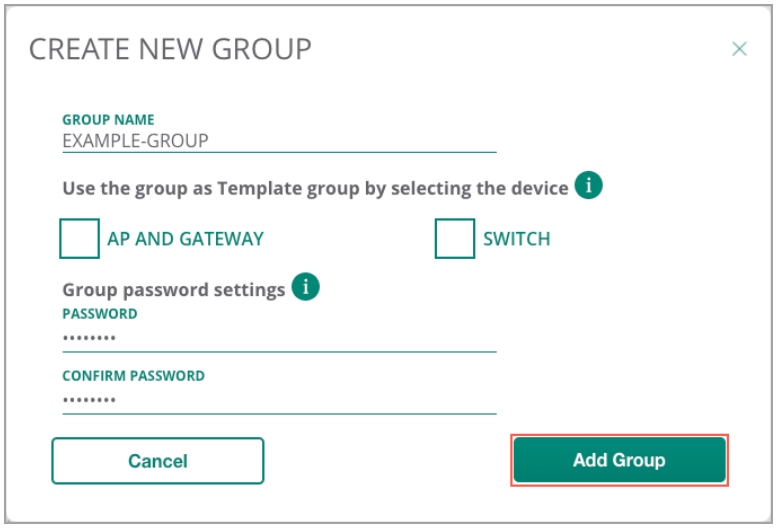


Step 4 On the Groups page in the Manage Groups section, select **New Group**.



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

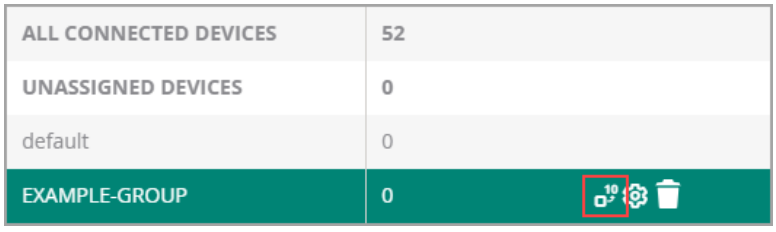
- **GROUP NAME:** *EXAMPLE-GROUP*
- **PASSWORD:** *password*
- **CONFIRM PASSWORD:** *password*



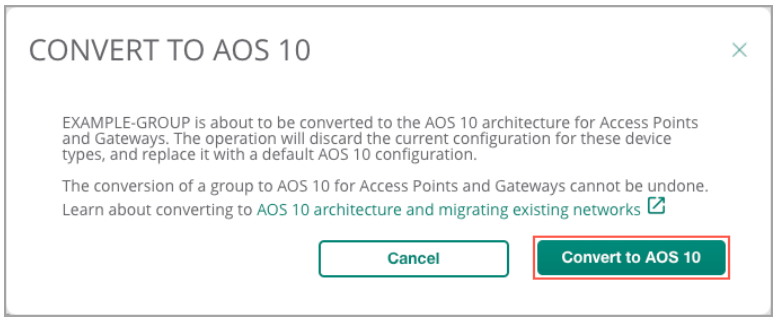
NOTES:
To create a template group, select one of the *device type* checkboxes before adding the group to Central.
The password enables administrative access to the devices interface. This password is used as the login password for all the devices in the group, but it is not the enable password. The same password can be used across multiple groups.

Step 6 Enable **AOS 10** on the newly created group. Locate the group in the Group Name table, and then click the row so the group name is highlighted.

Step 7 In the highlighted row, click the **Convert to AOS 10** icon.



Step 8 In the popup, click **Convert to AOS 10**.



NOTES:
APs and Gateways must both be AOS 10 in order to have bridge, tunnel, and mixed mode SSIDs configured. You cannot mix IAP 8 and AOS 10 APs in the same group. You also cannot mix SD-Branch and AOS 10 Gateways in the same group. Central will allow both of these scenarios but the devices that are not running AOS 10 code will not work. They are allowed to be in the same group for upgrade and initial deployment purposes.
The AOS 10 conversion process is not reversible on the group. An AP or Gateway can be moved to another group and downgraded to a different code version supported by Central.

Step 9 Repeat this procedure for each Group.

Create New Sites

Aruba Central uses sites to organize devices by their geographical locations. You use sites to monitor devices, not to configure them. Sites are created under Organization like Groups and are needed to generate topology data and reporting data across multiple devices in a single interface. Sites will allow for multiple device types in different groups to have a common reporting dashboard within Central.

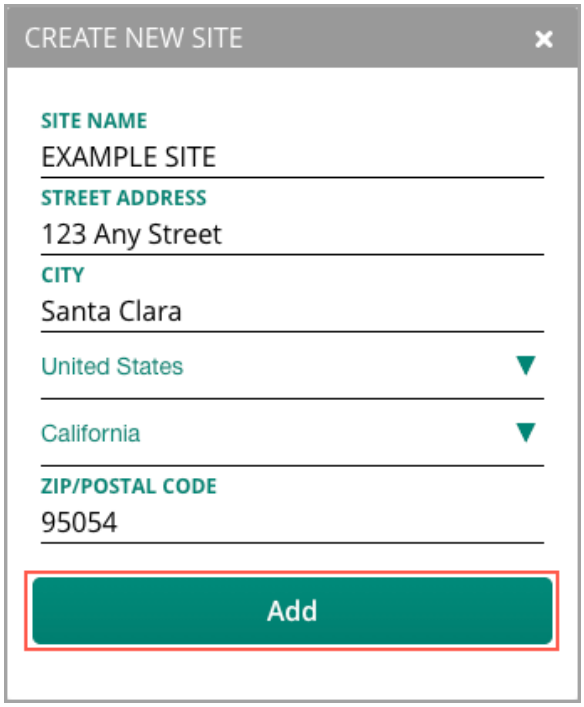
Step 1 On the Aruba Central Account Home page, launch the **Network Operations** app.

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

Step 3 On the Sites and Labels tab, confirm the slider is set to **Sites**, and then at the bottom, click **New Site**.

Step 4 In the Create New Site dialog box, implement the following settings, and then click **Add**.

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



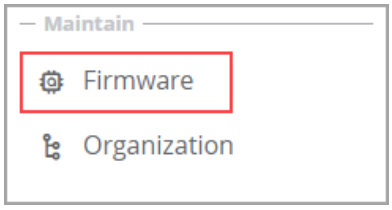
Manage Firmware Compliance

Firmware compliance should be configured with initial setup and will automatically upgrade devices that are connected to Central before they are configured. This is useful with initial deployment as the installed versions of firmware are normally different across devices and platforms. Aruba recommends running the latest updated firmware for the initial deployment.

Aruba Central runs a firmware compliance check and forces firmware upgrades for all devices in the group.

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

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

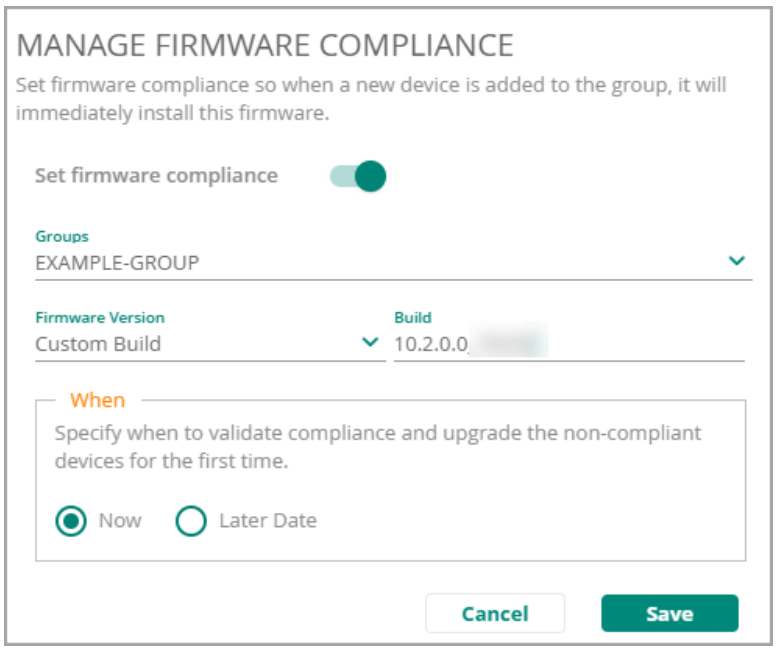


Step 3 On the Access Points page on the top right side, click **SET COMPLIANCE**.

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

Step 5 On the expanded popup, implement the following settings, and then click **Save**.

- **Groups:** *EXAMPLE-GROUP*
- **Firmware Version:** *Custom Build*
- **Build:** *Latest Recommended*
- **When:** *Now*



NOTES:
Choose the build version you want from the drop-down list. There are recommended versions that don't have all the newest features but have fewer known issues and may be a safer selection for a conservative customer.
Select the Now radio button to have the compliance carried out immediately.
This process does not do Live Upgrades and should be turned off after the initial setup. Subsequent upgrades can be done with Live Upgrade, manually, or firmware compliance based on the needs of the deployment.

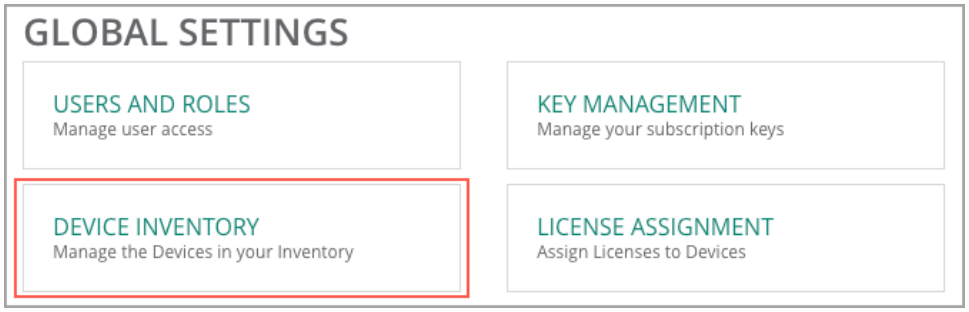
Step 6 Repeat this procedure for all groups.

Add Devices to Inventory

Aruba Central automatically adds purchased devices to the device inventory in a managed Central account. If devices are not in the inventory, they can be manually added using their MAC address and serial number.

Step 1 At the top right of any page, click the **Account Home** icon.

Step 2 On the Account Home page in the Global Settings section, select **DEVICE INVENTORY**.



Step 3 Check the device inventory page to confirm all devices are correctly listed.

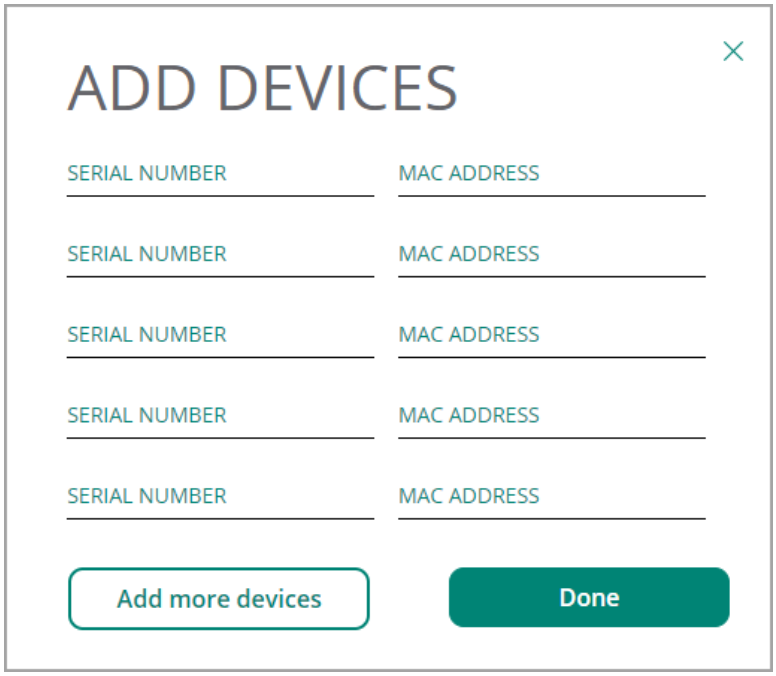
Step 4 If devices are missing, scroll to the bottom of the page, and then click **Add Devices**.

Step 5 In the popup, enter the serial number and MAC address of the missing devices, and then when they are all entered, click **Done**.

- **SERIAL NUMBER:** *serial number*
- **MAC ADDRESS:** *MAC address*

After entering the information and moving to the next line, the system will attempt to add the device to inventory. One of the following messages will appear:

- *Success* - The device has been added to inventory
- *Error* - The serial number or MAC address is incorrect. Check for a typo, but if both are entered correctly, please open a TAC case.
- *Blocked* - This device is currently assigned to another customer. Please open a TAC case. There are occasions where a company has multiple accounts or orders to Aruba, and TAC can resolve the issue.
- *Device Already exists* - This device is already in the inventory.



NOTE:
The Serial Number and MAC Address can be found on the original box or the label on the device.

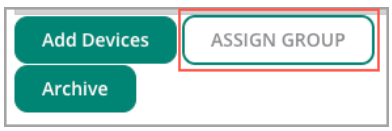
Step 6 Repeat this procedure until all devices are added to inventory.

Assign Devices to Groups

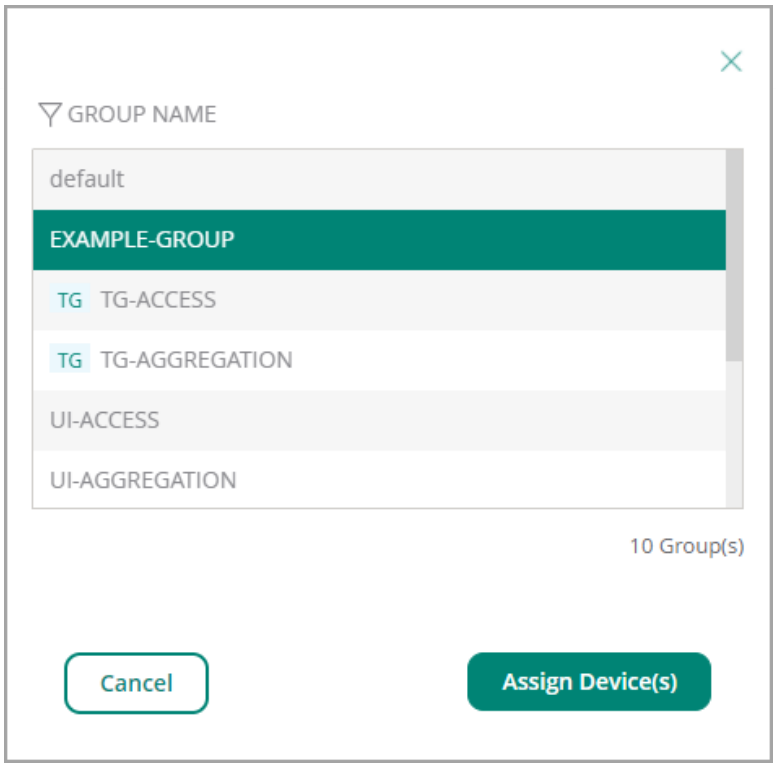
Use this procedure to assign devices to groups.

While you are in the inventory section, you can assign your devices to the groups created earlier. Once they are assigned to a group with a firmware compliance set, a code upgrade will begin if the device is not within compliance.

Step 1 On the Device Inventory page, select the device or group of devices, and then click **ASSIGN GROUP**.



Step 2 On the Group Name popup, choose the group name, and then click **Assign Device(s)**.



NOTE:
Most access devices automatically provision themselves because they support zero touch provisioning (ZTP) which allows them to download their provisioning parameters from the Activate server. Newly added devices are assigned to the ‘default’ group, which is why it is important to assign them to their desired groups as soon as possible.

Step 3 Repeat this procedure until all devices are assigned to groups.

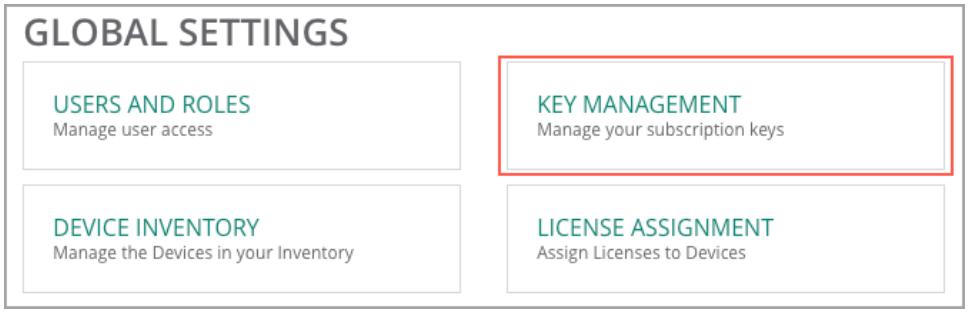
Add Device Subscription Keys

Use this procedure to add device subscription keys to your Central account.

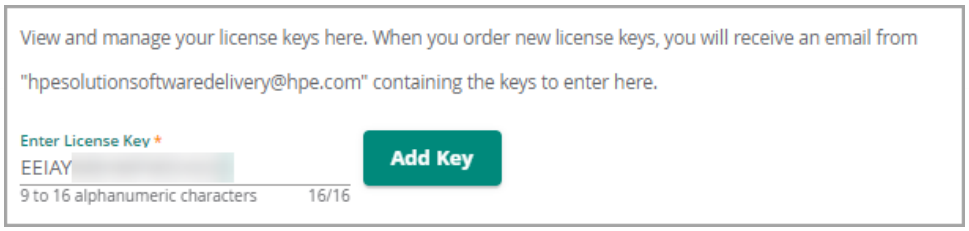
After the devices are in inventory, add subscription keys to configure and manage them in Aruba Central.

Step 1 At the top right of any page, click the **Account Home** icon.

Step 2 On the Account Home page in the Global Settings section, select **KEY MANAGEMENT**.

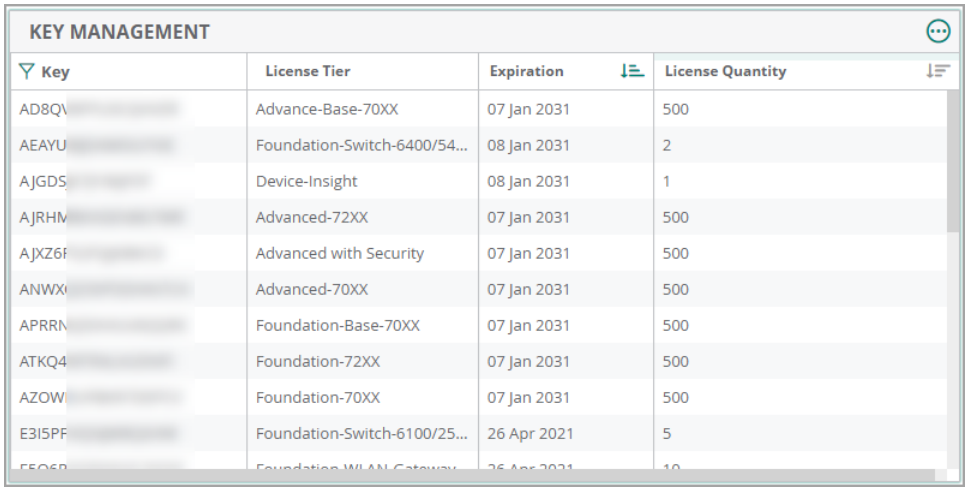


Step 3 On the Key Management page, enter a subscription key, and then click **Add Key**.



Step 4 Repeat the previous step for each subscription key.

NOTE:
The Key Management page also displays the status and expiration dates for the existing licenses.

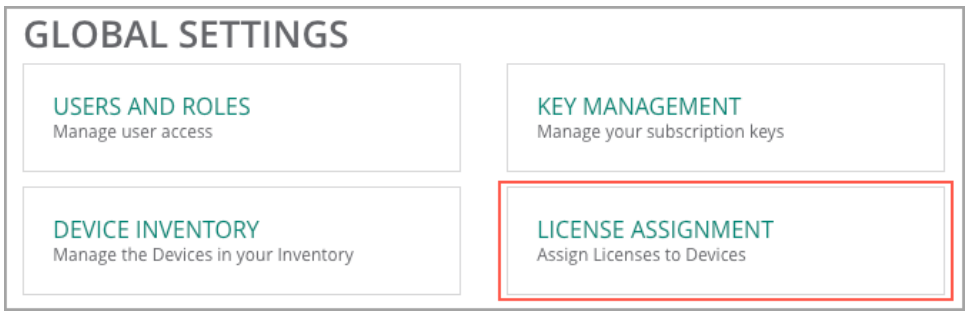


Assign Subscriptions to Devices

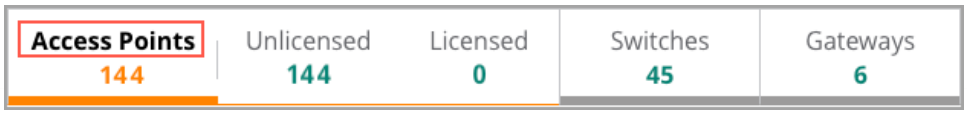
After adding subscription keys, assign a subscription to each device for configuration and management. Central allows automatic license assignment using the Auto Subscribe option. Alternatively, subscription keys can be assigned manually.

Step 1 At the top right of any page, click the **Account Home** icon.

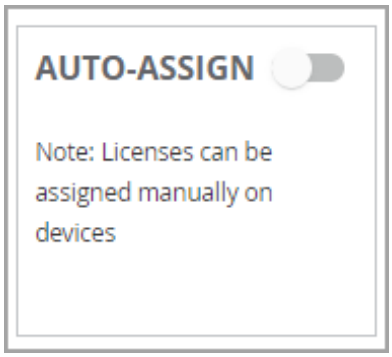
Step 2 On the Account Home page in the Global Settings section, select **LICENSE ASSIGNMENT**.



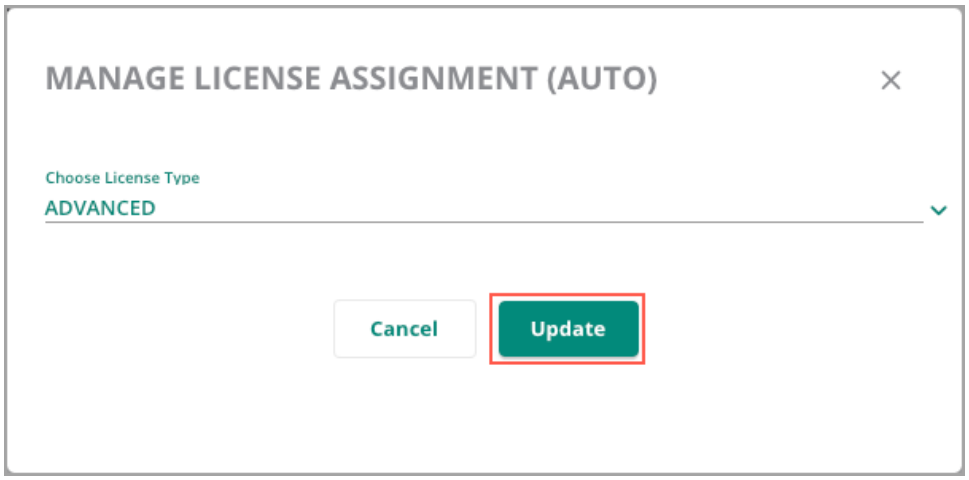
Step 3 At the top of the page, the default device type is **Access Points**.



Step 4 To assign licenses automatically to this device type, click the **AUTO-ASSIGN** slider to the right. If you do not want to assign licenses automatically, skip the next two steps.

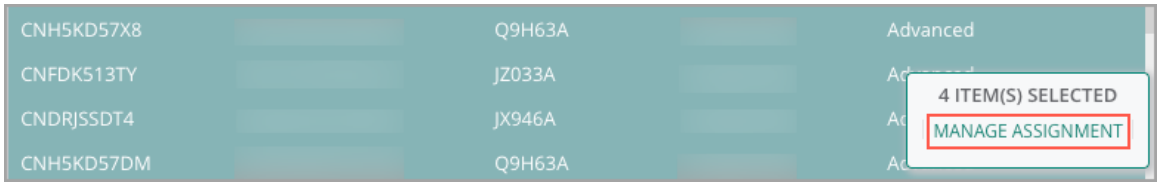


Step 5 On the popup, choose the License Type to automatically assign all devices of this type, and then click **Update**.

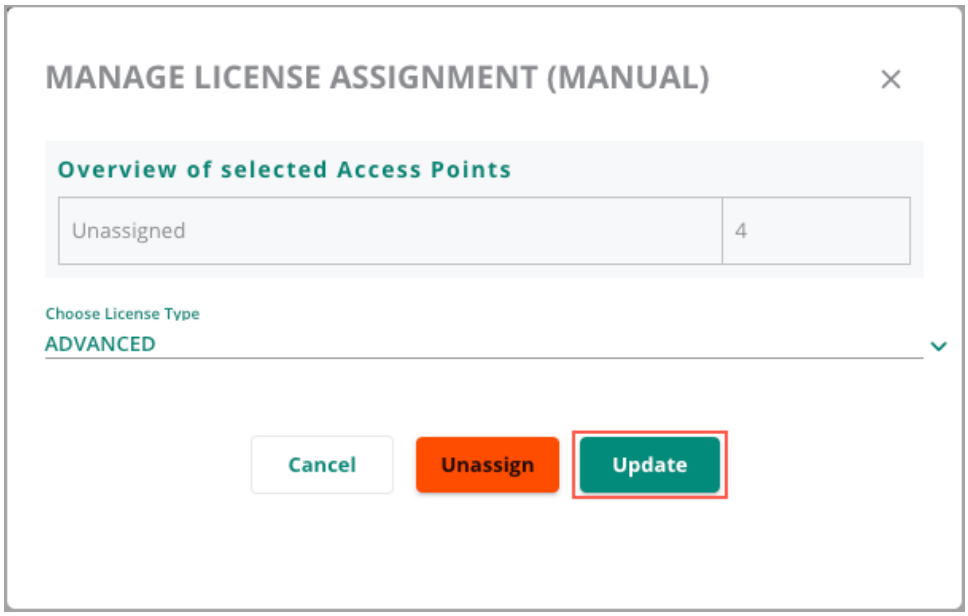


Step 6 To assign licenses manually, leave the **Auto-Assign** slider off, and then select one or more devices from the list.

Step 7 At the bottom of the selection section, click **MANAGE ASSIGNMENT**.



Step 8 On the popup, choose the License Type to assign the selected devices, and then click **Update**.



Step 9 Repeat this procedure for all the devices.

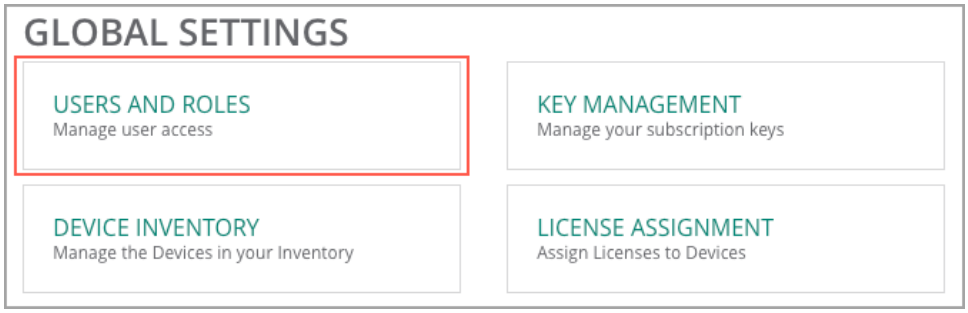
Create New Users

Use this procedure to create new users and roles.

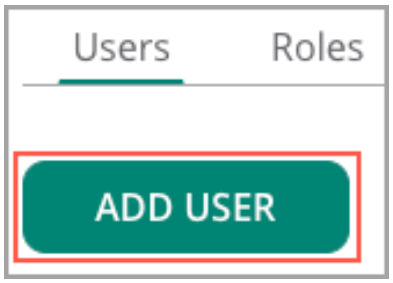
NOTE:
For detailed information on setting up user access, search for “user and roles” in the Documentation Center home page after selecting the question mark icon in the upper right corner of any web page in Central.

Step 1 At the top right of any page, click the **Account Home** icon.

Step 2 On the Account Home page in the Global Settings section, select **USERS AND ROLES**.

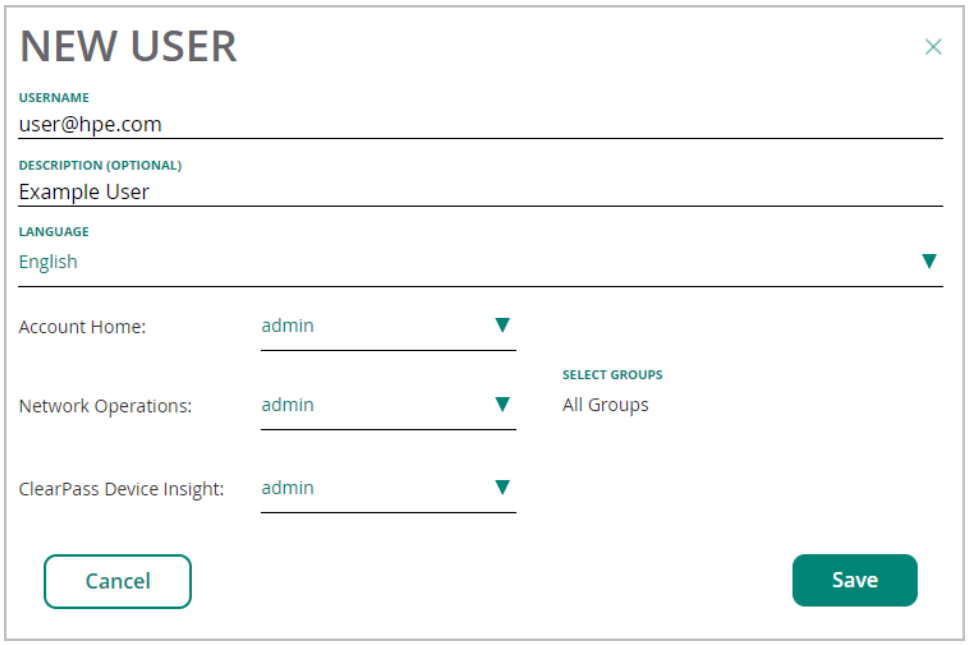


Step 3 On the Users and Roles page, click **ADD USER**.



Step 4 On the popup, implement the following settings, and then click **Save**.

- **Username:** *user@hpe.com*
- **Description:** *Example user*
- **Language**: *English*
- **Account Home**: *admin*
- **Network Operations**: *admin*
- **ClearPass Device Insight**: *admin*
- **Select Groups:** *All Groups*



NOTES:
The *Account Home* allows you to select a user role for the Account Home page
The *Network Operations* allows you to select a user role for the Network Operations application
The *ClearPass Device Insight* allows you to select a user role for the ClearPass Device Insight application
The *Select Group* allows you to select the groups this user can access

ClearPass Policy Manager

ClearPass Policy Manager provides role and device-based secure network access control for IoT, BYOD, corporate devices, as well as employees, contractors and guests across wired, wireless, and VPN infrastructure. With a built-in context-based policy engine, RADIUS, TACACS+, non-RADIUS enforcement using OnConnect, device profiling, posture assessment, onboarding, and guest access options, ClearPass is unrivaled as a foundation for network security for organizations of any size.

NOTE:
The content in the ESP Campus is based on ClearPass Policy Manager version 6.9. This guide does not cover the initial turn up and implementation of ClearPass. The ClearPass platform needs to be installed and patched to version 6.9 before implementing the steps in the subsequent sections of this guide. For details on ClearPass deployment, please refer to the following link: ClearPass Policy Manger 6.9 Deployment Guide

Campus Wired Connectivity

The Aruba CX portfolio provides a variety of form factors which include models with the latest networking standards. The switches are available in modular and stackable options to satisfy a diverse set of requirements. They use a cloud-native operating system called AOS-CX which is designed with a focus on network resiliency utilizing a database centric operational model. With features like always-on PoE, Virtual Switching Framework (VSF) and Virtual Switching Extension (VSX), organizations can rely on the network infrastructure for their mission critical traffic. VSF provides switch stacking at the access layer and VSX provides high availability at the aggregation layer.

AOS-CX allows a variety of two-tier and three-tier options from a Layer 3 routed access layer all the way to switched Layer 2 access with a redundant Layer 3 aggregation and core. Most large organizations adopt a model where the aggregation layer provides Layer 2 towards the access switches and Layer 3 towards a fully routed core. To ensure this design has maximum resiliency without added complexity, Aruba created a high availability system that supports multi-chassis link-aggregation (MC-LAG) while keeping the control plane of each switch independent. This capability is called Aruba VSX and provides a redundant, loop-free topology that does not require the spanning tree protocol. VSX also provides DHCP redundancy, native active-active default gateway, and active-active Layer 2 and Layer 3 forwarding without blocked uplinks.

Wired Core

The core layer of the LAN is a critical part of the scalable network, yet it is one of the simplest by design. The aggregation layer provides the fault and control domains, and the core represents the nonstop connectivity between the aggregation switch pairs. For the fastest core layer convergence, build triangles not squares in order to take advantage of ECMP routing, which provides the best deterministic convergence. ECMP is an advanced routing strategy where next-hop packet forwarding occurs over multiple paths with identical routing metric calculations.

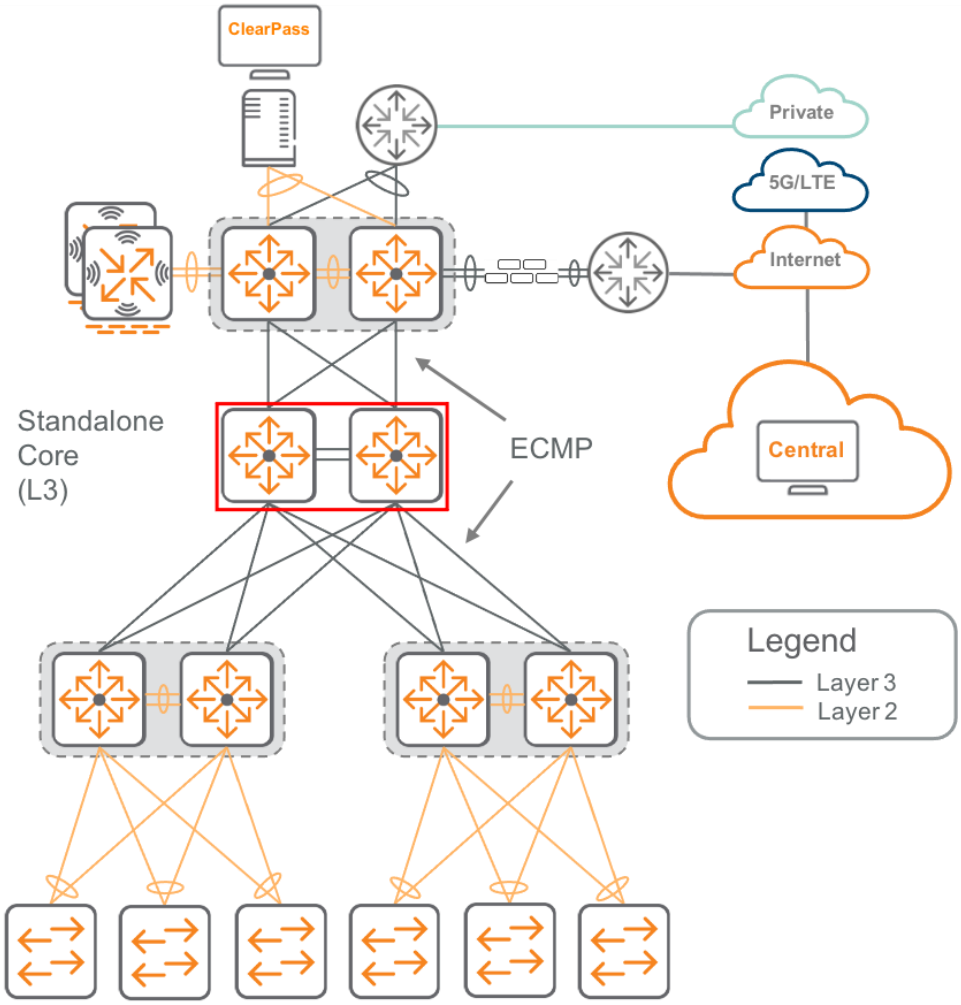
The core layer provides high-speed Layer 3 connectivity for the aggregation layer switches. It can also provide services aggregation functions when needed. The decision to use a standalone core layer depends on the number of aggregation layer switches and if services are combined in a single location or spread across several aggregation blocks. With this Aruba ESP Campus architecture, an organization can start with a combined core and services design, and then migrate to a standalone core when needed. The ECMP uplinks between the access aggregation switches, and the core layer remains the same with either model.

Configuring the Core with Template Groups

The core switches are configured with CLI commands because in most cases they will be the first devices deployed. This section will discuss how to import the core switches into Central with template groups for monitoring and configuration.

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

Wired Core



Configure the Core Base Features

Use this procedure to configure the core switch base features. The base features include the hostname, management user account, banner message of the day (MOTD), Network Time Protocol (NTP), Domain Name System (DNS), Terminal Access Controller Access Control System (TACACS), and Authentication, Authorization and Accounting (AAA) servers.

Step 1 Configure the Switch host name.

```
hostname Core-Switch
```

Step 2 Configure the management user account.

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

NOTE:
There must be an admin user account for command line interface (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.

```
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 will break the switch from the MOTD context. In this example, the delineator is the "$".

Step 4 Configure the NTP servers and timezone.

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

Step 5 Verify the NTP configuration with the **show ntp status** command.

There are several things to look for:

- 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.

```
8400-C1-1# show ntp status
NTP Status Information

NTP                          : Enabled
NTP Authentication           : Disabled
NTP Server Connections       : Using the default VRF

System time                  : Tue Mar 30 22:07:36 PDT 2021
NTP uptime                   : 6 days, 5 hours, 20 minutes, 41 seconds

NTP Synchronization Information

NTP Server                   : 10.2.120.98 at stratum 3
Poll interval                : 1024 seconds
Time accuracy                : Within -0.001049 seconds
Reference time               : Tue Mar 30 2021 21:44:23.286 as per US/Pacific
```

Step 6 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.com
```

Step 7 Configure the TACACS servers.

```
tacacs-server host 10.2.120.94 key Plaintext <key>
tacacs-server host 10.2.120.95 key Plaintext <key>
```

Step 8 Configure the TACACS server group. Create the server group and use the IP addresses from the TACACS server hosts configured previously.

Server group name: *ClearPass*

```
aaa group server tacacs ClearPass
    server 10.2.120.94
  server 10.2.120.95
```

NOTE:
TACACS servers groups allow the switch to fallback to a secondary server if the primary server is down.

Step 9 Configure AAA for the TACACS server group. The AAA commands point to the TACACS server group configured previously. Configure the start and stop time of each session and a fallback mechanism in case the TACACS server is down or unreachable.

```
aaa authentication login ssh group ClearPass local
aaa authentication login console group ClearPass local
aaa authorization commands default group  local ClearPass
aaa accounting all default start-stop group ClearPass local
aaa authentication allow-fail-through
```

NOTE:
Devices use TACACS for both console and SSH access with a fall back to local authentication. All devices should have a local backup account on the switch to allow access when the TACACS server is unreachable.

Step 10 Configure TACACS server tracking.

```
tacacs-server tracking user-name TrackUser plaintext <password>
```

NOTE:
The tracking account used with the TACACS server should only have permissions to log in and nothing else.

Step 11 Verify the TACACS server configuration with the **show tacacs-server statistics** command.

There are several things to look for:

- Round Trip Time
- Auth Start
- Auth Accepts
- Tracking Requests
- Tracking Responses

The non-zero values indicate the TACACS service is reachable by the switch.

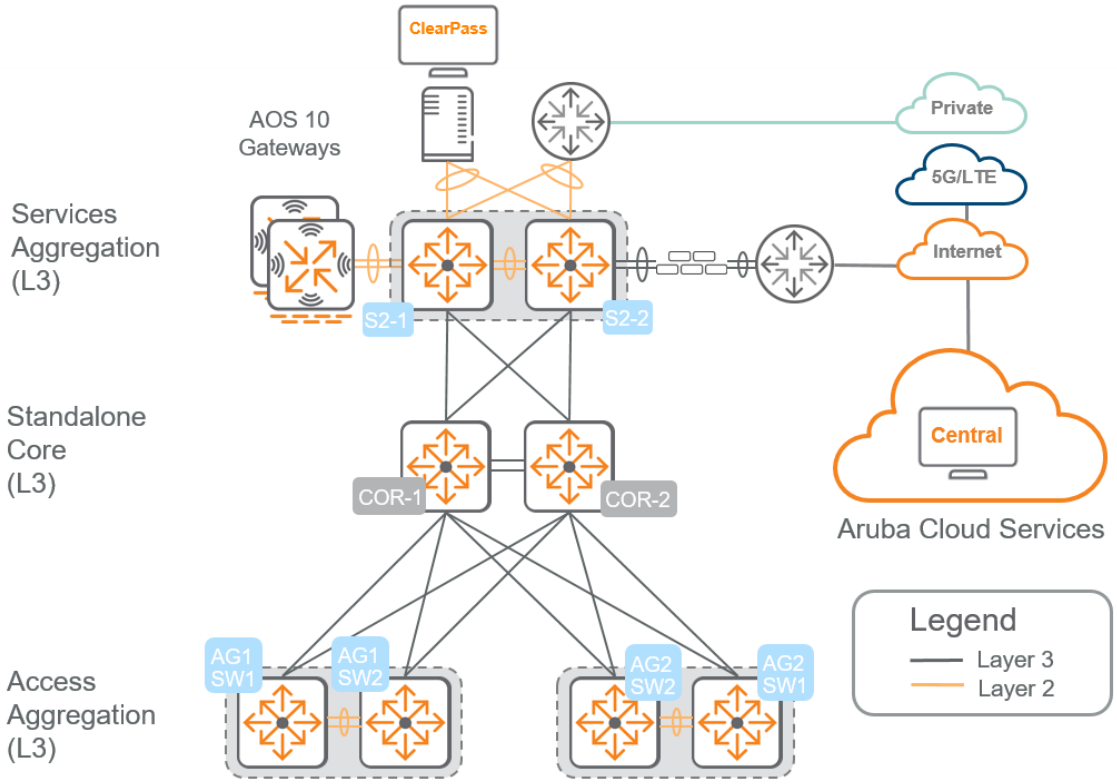
```
8400-C1-1# show tacacs-server statistics
 Server Name     : 10.2.120.94
 Auth-Port       : 49
 VRF             : default
 Authentication Statistics
-----------------------------------------------
 Round Trip Time(ms)       : 81
 Pending Requests          : 0
 Timeout                   : 0
 Unknown Types             : 0
 Packet Dropped            : 0
 Auth Start                : 8
 Auth challenge            : 1
 Auth Accepts              : 5
 Auth Rejects              : 0
 Auth reply malformed      : 0
 Tracking Requests         : 4
 Tracking Responses        : 4
 ...
```

Configure OSPF Routing

OSPF is a link-state Layer 3 routing protocol and is the primary feature to enable on the core of the network. OSPF routes packets between other devices on the network. In this design, OSPF uses area 0 or the “backbone area” for the entire campus network. The router loopback IP address is the OSPF router ID.

The procedure also configures the uplink ports from the core switch to the aggregation switch. The uplink ports are point-to-point for ECMP routing. In this design, a 172.18.10X.X/30 network and mask is used because each subnet only needs two IP addresses. The topology below is a reference point for the configuration. The OSPF commands will only be applied to the core switches at this time.

OSPF Topology



Step 1 Configure OSPF globally. Create the router OSPF process with area 0 and enable passive-interface default to avoid unwanted OSPF adjacencies. Select a router-id that is unique to this device, as it will also be used as the loopback 0 IP address. If there are 8400 or 6400 switches in the core with redundant management modules, enable graceful restart.

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

Step 2 Configure OSPF and PIM sparse mode on the loopback interface. Create the loopback 0 interface and configure the IP address using the router ID from the previous step. Enable OSPF with area 0.

```
interface loopback 0
  ip address 10.0.0.1/32
  ip ospf 1 area 0
```

Step 3 Configure OSPF on the physical interfaces. Configure a large IP MTU, turn off OSPF passive mode, set the OSPF network to point-to-point, and enable OSPF using the router process and area.

```
interface 1/1/1
  description CORE_TO_AG1
  no shutdown
  ip mtu 9198
  ip address 172.18.103.2/30
  no ip ospf passive
  ip ospf network point-to-point
  ip ospf 1 area 0
```

Step 4 Repeat the previous step for each core to aggregation interface on the switch.

Example: Core 1 Switch

Core 1 IP Address	Subnet	Peer Device
172.18.100.1	172.18.100.0/30	Core-2
172.18.100.5	172.18.100.0/30	Core-2
172.18.106.2	172.18.106.0/30	S2-1
172.18.106.10	172.18.106.0/30	S2-2
172.18.102.2	172.18.106.0/30	AG2-1
172.18.102.10	172.18.102.0/30	AG2-2
172.18.103.2	172.18.103.0/30	AG1-1
172.18.103.10	172.18.103.0/30	AG1-2

Example: Core 2 Switch

Core 2 IP Address	Subnet	Peer Device
172.18.100.2	172.18.100.0/30	Core-2
172.18.100.6	172.18.100.0/30	Core-2
172.18.106.6	172.18.106.0/30	S2-1
172.18.106.14	172.18.106.0/30	S2-2
172.18.102.6	172.18.106.0/30	AG2-1
172.18.102.14	172.18.102.0/30	AG2-2
172.18.103.6	172.18.103.0/30	AG1-1
172.18.103.14	172.18.103.0/30	AG1-2

Step 4 Verify the OSPF configuration with the **show ip ospf neighbors** command.

There are a couple of things to look for:

- The neighbor addresses on the active OSPF interfaces are correct
- The neighbor IDs match the loopback IP address of the other device
- The neighbor state is **FULL** to all adjacent switches

These values indicate OSPF neighbors are reachable.

```
8400-C1-1# show ip ospf neighbors
# OSPF Process ID 1 VRF default

Total Number of Neighbors: 14

Neighbor ID      Priority  State             Nbr Address       Interface
-------------------------------------------------------------------------
10.0.3.1         n/a       FULL              172.18.103.1       1/1/1
10.0.3.2         n/a       FULL              172.18.103.9       1/1/2
10.0.2.1         n/a       FULL              172.18.102.1       1/1/3
...
```

NOTE:
The verification commands were run after the aggregation switches were configured with OSPF. If the aggregation switches have not been configured, the **show ip ospf neighbors** command will not display neighbors.

Configure Multicast Routing

IP multicast allows a single IP data stream to be replicated by the network and sent from a single source to multiple receivers. This design is based on Protocol Independent Multicast (PIM) sparse-mode and Multicast Source Discovery Protocol (MSDP) for multicast operation. MSDP allows for active-active multicast rendezvous points (RP). MSDP relies on Bootstrap Router (BSR) and RP-Candidate configuration which automatically choose which device becomes the BSR and RP.

The RP is the root of the multicast tree when using sparse mode. Multiple RPs can be configured for redundancy, although normally, only one RP is active at a time for each multicast group. Multiple RPs can be active if MSDP is enabled because it allows a multicast domain to share source tree tables between RPs. MSDP allows switches to have Inter and Intra Domain active-active redundancy using an Anycast IP address as the RP. Anycast is a networking technique that allows for multiple devices to share the same IP address. Based on the location of the user request, the switches send the traffic to the closest device in the network which reduces latency and increases redundancy.

In a Campus, MSDP is needed for intra domain redundancy and should be enabled on the core switches in either the two-tier or three-tier topologies. The RP candidate announcement, in combination with MSDP, advertises the Anycast IP address to neighboring devices. Neighboring devices will not know what devices want to be the RP unless BSR is enabled. The BSR is elected from a list of candidate-BSRs configured on the network. There can only be a single active BSR, and it advertises RP information to all PIM-enabled routers, freeing the administrator from having to statically configure the RP address on each router in the network. BSR, RP, and MSDP should be enabled on the core switches to identify the active RP and notify neighboring devices.

Step 1 Configure multicast routing globally.

```
router pim
  enable
```

Step 2 Create a new loopback interface with the Anycast IP address. Enable PIM sparse mode and OSPF.

Anycast IP: *10.0.0.100/32*

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

Step 3 Configure RP and BSR candidate source IP interface using the Anycast IP address, set the RP candidate group prefix, and the BSR candidate priority.

```
router pim
  enable
  rp-candidate source-ip-interface 10.0.0.100
  rp-candidate group-prefix 224.0.0.0/4
  bsr-candidate source-ip-interface 10.0.0.100
  bsr-candidate priority 1
```

NOTE:
The RP candidate group prefix should be adjusted based on your network requirements.

Step 4 Configure MSDP globally. The MSDP peer is the IP address of loopback 0 interface on the adjacent core switch. The local loopback 0 interface is the connect-source.

Example: Core 1 Switch

```
router msdp
enable
ip msdp peer 10.0.0.2
 connect-source loopback0
```

Example: Core 2 Switch

```
router msdp
enable
ip msdp peer 10.0.0.1
 connect-source loopback0
```

Step 5 Configure PIM sparse-mode on the loopback 0 interface.

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

Step 6 Configure PIM sparse-mode on the physical interfaces.

```
interface 1/1/1
  description CORE_TO_AGG1
  no shutdown
  ip mtu 9198
  ip address 172.18.103.2/30
  no ip ospf passive
  ip ospf network point-to-point
  ip ospf 1 area 0
  ip pim-sparse enable
```

Step 7 Repeat the previous step for each interface between the core and aggregation switches.

Step 8 Verify the multicast configuration with the **show ip msdp summary** and **show ip pim neighbor** commands.

There are a couple of things to look for:

- The MSDP peer state is up
- The PIM neighbor count and IP addresses are correct for the participating devices

These values indicate MSDP and PIM sparse mode are active.

```
8400-C1-1# show ip msdp summary

VRF: default
MSDP Peer Status Summary
Peer address     State    Uptime(Downtime)     Reset Count     SA Count
10.0.0.2         up       6d 4h 32m            0               4
```

```
8400-C1-1# show ip pim neighbor

PIM Neighbor

VRF                         : default
Total number of neighbors : 8

IP Address                  : 172.18.100.6
Interface                   : 1/2/5
Up Time (HH:MM:SS)          : 7 days 09:16:04
Expire Time (HH:MM:SS)      : 00:01:32
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:01:45

IP Address                  : 172.18.102.1
Interface                   : 1/1/3
Up Time (HH:MM:SS)          : 00:30:40
Expire Time (HH:MM:SS)      : 00:01:36
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:01:45
...
```

NOTE:
The verification commands were run after the aggregation switches were configured with PIM-SM. If the aggregation switches have not been configured, the **show ip pim neighbor** will not display neighbors.

Import the Core Switches

Use this procedure to create template groups for the core switches, and then import them into Central.

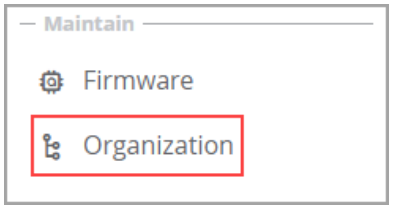
The Aruba 8400 and 6400 series are used as core switches and they only support template groups in Central 2.5.3. Aruba recommends creating a template group for each core switch because they have different IP address on each interface and a single template is difficult to maintain with a long list of variables.

If 8300 series switches are used in the core, Aruba recommends a UI Group to monitor and maintain them within Central. UI Groups support MultiEdit which allows both core switches to be managed without maintaining a long list of variables.

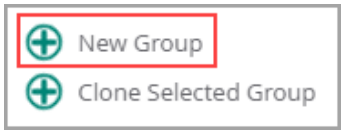
Step 1 Navigate to **Central** and login using administrator credentials.

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

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

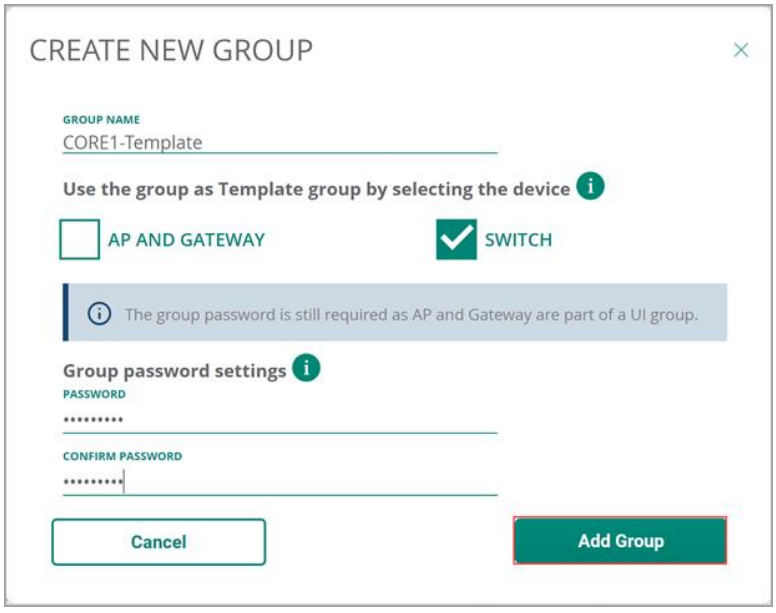


Step 4 On the Groups page in the Manage Groups section, select **New Group**.



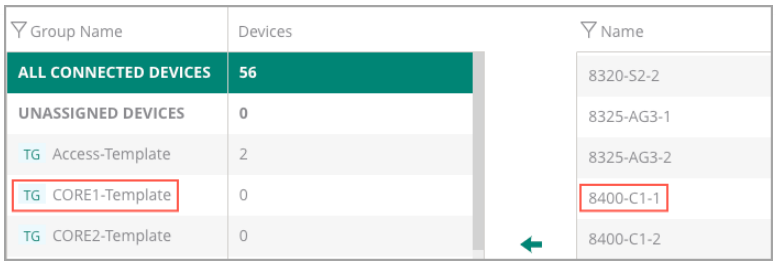
Step 5 On the Create New Group page, implement the following settings, and then click **Add Group**.

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

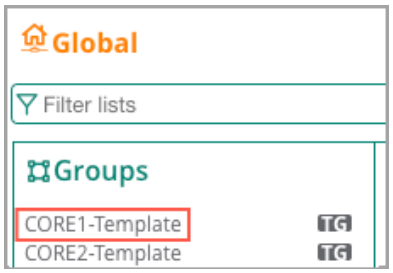


NOTE:
The password enables administrative access to the devices interface. This password is used as the login password for all the devices in the group, but it is not the enable password. The same password can be used across multiple groups.

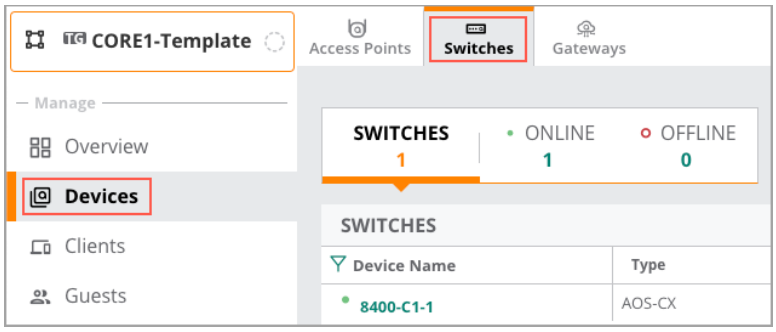
Step 6 Repeat the previous step for the second core switch. **Step 7** On the Groups page, in the Manage Groups section, drag the core Switch from the left side to the template group on the right side.



Step 8 At the top left of the page, navigate to **Global > Groups**, and then from the Groups list, select **CORE1-Template**.



Step 9 From the left menu, select **Devices**, and then select **Switches**.

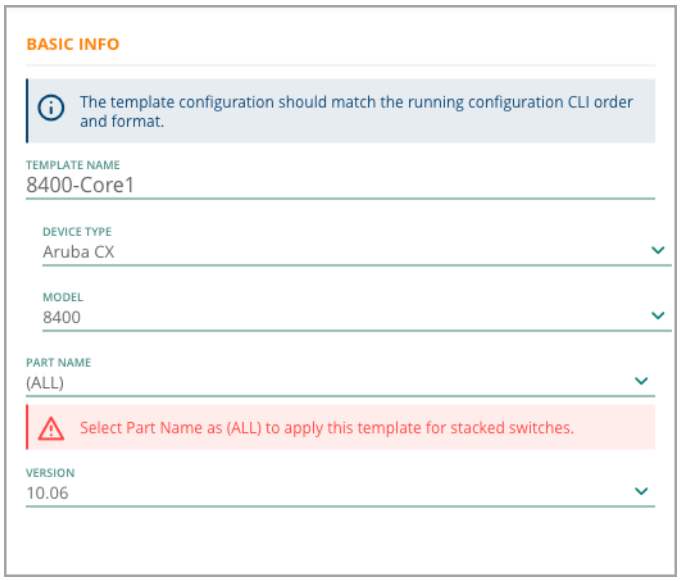


Step 10 On the Switches List page in the top right, click **Config**.

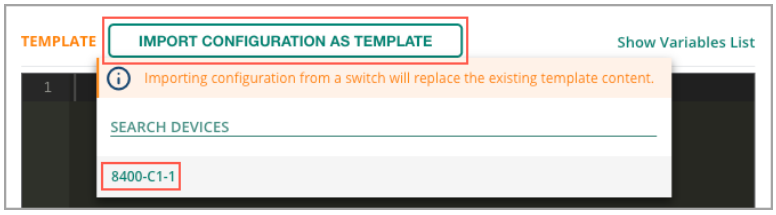
Step 11 On the Switches Template section in the top right, click the **+** symbol.

Step 12 On the Add Template popup in the Basic Info section, implement the following settings, and then click **Next**.

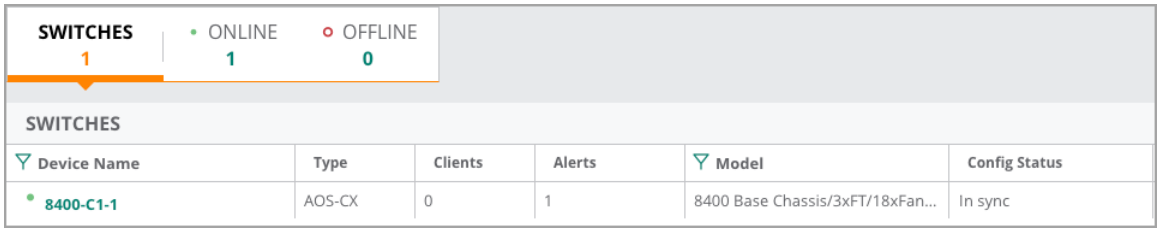
- **Template Name:** *8400-Core1*
- **Device Type:** *Aruba CX*
- **Model:** *8400*
- **Part Name:** *(ALL)*
- **Version:** *10.06*



Step 13 In the Template section, select **Import Configuration as Template**, select **8400-C1-1**, and then click **Save**.



Step 14 From the left menu, navigate to **Devices > Switches > List**, and then verify the configuration status is **In sync**.



Step 15 Repeat this procedure for the second core Switch.

Example: Core Switch Template

Core Switch Template

Wired Aggregation

The aggregation layers primary function is to give access switches a common connection point and to act as the boundary between Layer 2 switching and Layer 3 routing. The aggregation layer increases network scalability by providing a single place to interconnect the access layer switches, providing high performance, and single hop connectivity between all switches in the aggregation block.

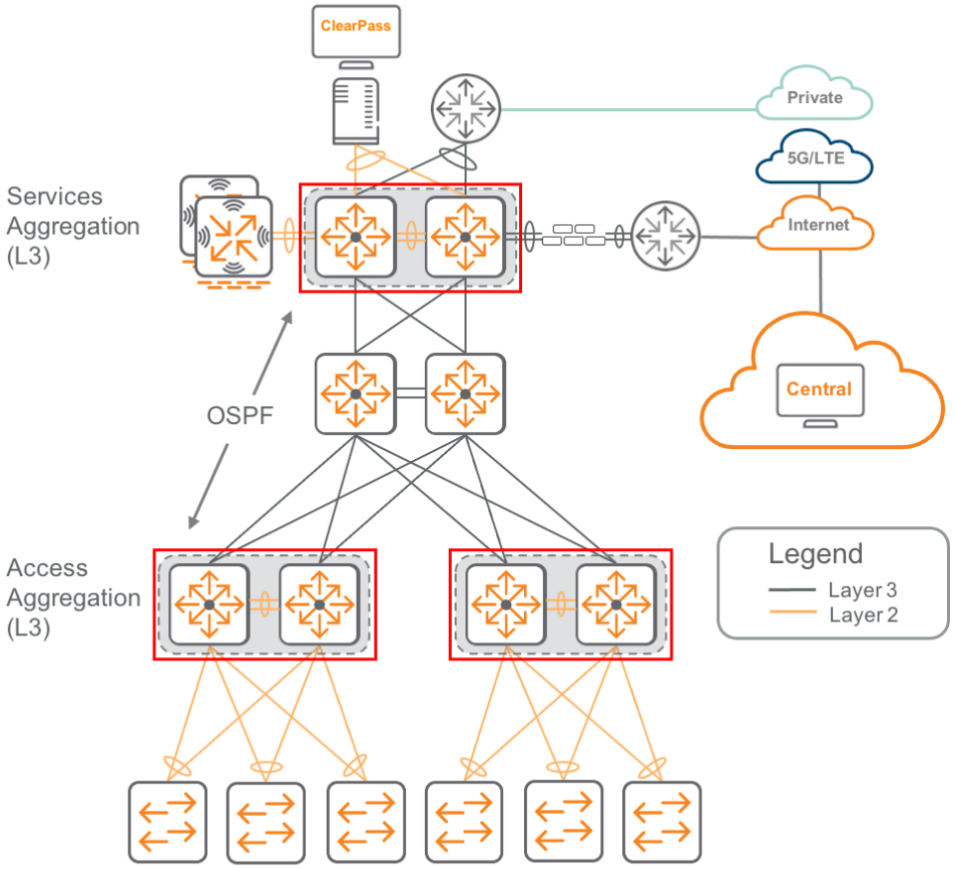
The aggregation layer provides Layer 3 services, routing LAN traffic between networks in and out of the campus. Because Layer 2 networks are terminated at the aggregation layer, it segments the network into smaller broadcast domains to reduce the size of the MAC learning and IPv4/IPv6 tables for the local devices. The service-aggregation layer also becomes the ideal location for connecting other network services, such as the WAN aggregation, Internet DMZ, and edge data centers for an organization.

Configuring the Aggregation with UI Groups

The access-aggregation layer provides connectivity for the access switches and connects to the core layer using ECMP uplinks. The service-aggregation layer provides connectivity to the external networks in the campus and connects to the core layer using ECMP uplinks. The aggregation switches are Layer 3 and utilize OSPF for the routing protocol.

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

Wired Aggregation



Configure the Aggregation Base Features

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

Step 1 Configure the Switch host name.

```
hostname Aggregation-Switch
```

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.

```
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 will break the switch from the MOTD context. In this example, the delineator is the "$".

Step 4 Configure the NTP servers and timezone.

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

Step 5 Verify the NTP configuration with the **show ntp status** command.

There are several things to look for:

- 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.

```
6405-AG2-1# show ntp status
NTP Status Information

NTP                          : Enabled
NTP Authentication           : Disabled
NTP Server Connections       : Using the default VRF

System time                  : Thu Apr  1 02:08:57 PDT 2021
NTP uptime                   : 1 minutes, 59 seconds

NTP Synchronization Information

NTP Server                   : 10.2.120.98 at stratum 3
Poll interval                : 64 seconds
Time accuracy                : Within 0.000099 seconds
Reference time               : Thu Apr  1 2021  2:05:37.589 as per US/Pacific
```

Step 6 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.com
```

Step 7 Configure the TACACS servers with a plaintext key.

```
tacacs-server host 10.2.120.94 key Plaintext <key>
tacacs-server host 10.2.120.95 key Plaintext <key>
```

Step 8 Configure the TACACS server group. Create the server group and use the IP addresses from the TACACS server hosts configured previously.

Server group name: *ClearPass*

```
aaa group server tacacs ClearPass
    server 10.2.120.94
  server 10.2.120.95
```

NOTE:
TACACS server groups allow the switch to fallback to a secondary server if the primary server is down.

Step 9 Configure AAA with the TACACS server group. The AAA commands point to the TACACS server group configured previously. Configure the start and stop time of each session. Enable a fallback mechanism in case the TACACS server is down or unreachable.

```
aaa authentication login ssh group ClearPass local
aaa authentication login console group ClearPass local
aaa authorization commands default group  local ClearPass
aaa accounting all default start-stop group ClearPass local
aaa authentication allow-fail-through
```

NOTE:
Devices use TACACS for both console and SSH access with a fall back to local authentication. All devices should have a local backup account on the switch to allow access when the TACACS server is unreachable.

Step 10 Configure TACACS server tracking.

```
tacacs-server tracking user-name TrackUser plaintext <password>
```

NOTE:
The tracking account used with the TACACS server should only have permissions to log in and nothing else.

Step 11 Verify the TACACS server configuration with the **show tacacs-server statistics** command.

There are several things to look for:

- Round Trip Time
- Auth Start
- Auth Accepts
- Tracking Requests
- Tracking Responses

The non-zero values indicate the TACACS service is reachable by the Switch.

```
6405-AG2-1# show tacacs-server statistics
 Server Name     : 10.2.120.94
 Auth-Port       : 49
 VRF             : default
 Authentication Statistics
-----------------------------------------------
 Round Trip Time(ms)       : 78
 Pending Requests          : 0
 Timeout                   : 0
 Unknown Types             : 0
 Packet Dropped            : 0
 Auth Start                : 11
 Auth challenge            : 3
 Auth Accepts              : 9
 Auth Rejects              : 0
 Auth reply malformed      : 0
 Tracking Requests         : 4
 Tracking Responses        : 4
...
```

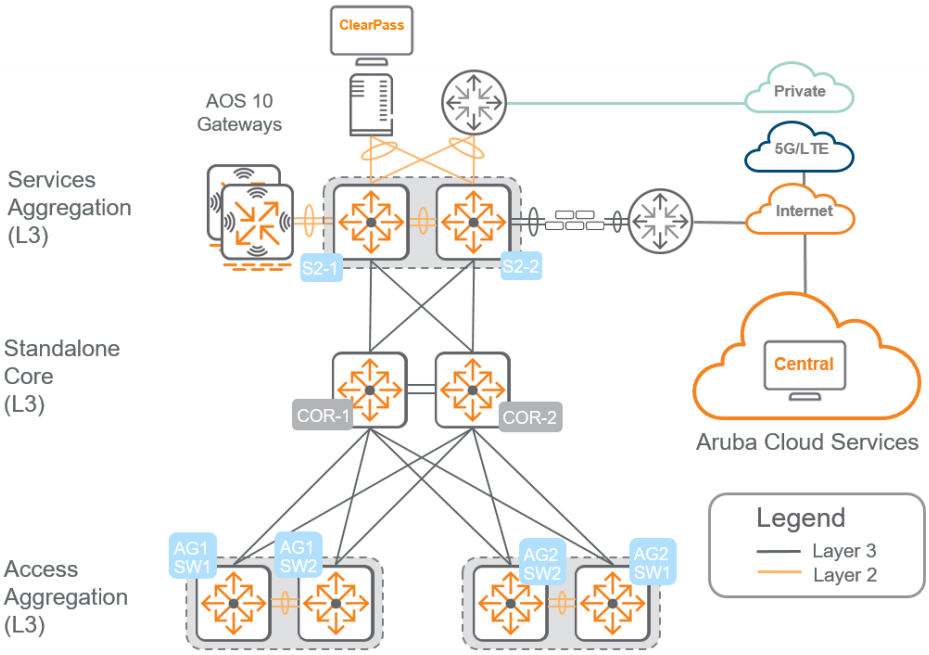
Configure OSPF and Multicast Routing

Aggregation switches use OSPF to advertise the interface VLAN's connected to the network. The OSPF instance running on the aggregation switches establish an OSPF neighbor with the core switches. In this design, OSPF uses area 0 or the "backbone area" for the entire campus network.

In addition to enabling OSPF, PIM-Sparse mode is configured on the OSPF point to point links. This ensures PIM neighbor relationships are established to the core switches which allows multicast streams to flow to the interface VLAN's.

Each uplink will have a 172.18.10X.X/30 mask because point to point subnets only need two IP addresses. The topology below is used as a reference point for the configuration and the commands will only be applied to the aggregation switches at this time.

OSPF Topology



Step 1 Configure OSPF globally. Create the router OSPF process with area 0 and enable passive-interface default to avoid unwanted OSPF adjacencies. Select a router-id that is unique to this device, as it will also be used as the loopback 0 IP address. If there is an 8400 or 6400 in the core with redundant management modules, enable graceful restart.

```
router ospf 1 area 0
  passive-interface default
  router-id 10.0.3.1
  graceful-restart restart-interval 30
```

Step 2 Configure multicast routing globally.

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

Step 3 Configure OSPF and PIM sparse mode on the loopback interface. Create the loopback 0 interface and configure the IP address using the router ID from the previous step. Enable OSPF with area 0 and PIM sparse mode.

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

Step 4 Configure OSPF and PIM spare mode on the physical interfaces. Configure a large IP MTU, turn off passive mode, and enable OSPF as point-to-point using the router process and area. Enable PIM sparse mode.

```
interface 1/1/1
description AG1_TO_CORE
no shutdown
ip mtu 9198
ip address 172.18.103.1/30
no ip ospf passive
ip ospf network point-to-point
ip ospf 1 area 0
ip pim-sparse enable
```

Step 5 Repeat the previous step for each interface between the aggregation and core Switches.

Example: Aggregation 1 Switches

AG1 IP Address	Source Device	Peer Device	Subnet
172.18.103.1	AG1-SW1	Core 1	172.18.103.0/30
172.18.103.9	AG1-SW2	Core 1	172.18.103.0/30
172.18.103.5	AG1-SW1	Core 2	172.18.103.0/30
172.18.103.13	AG1-SW2	Core 2	172.18.103.0/30

Example: Aggregation 2 Switches

AG2 IP Address	Source Device	Peer Device	Subnet
172.18.102.1	AG2-SW1	Core 1	172.18.106.0/30
172.18.102.9	AG2-SW2	Core 1	172.18.102.0/30
172.18.102.5	AG2-SW1	Core 2	172.18.106.0/30
172.18.102.13	AG2-SW2	Core 2	172.18.102.0/30

Example: Service Aggregation Switches

Service AG IP Address	Source Device	Peer Device	Subnet
172.18.106.1	S2-1	Core 1	172.18.106.0/30
172.18.106.9	S2-2	Core 1	172.18.106.0/30
172.18.106.13	S2-2	Core 2	172.18.106.0/30
172.18.106.5	S2-1	Core 2	172.18.106.0/30

Step 6 Verify the OSPF and PIM configurations are working with the **show ip ospf neighbors**, **show ip route** and **show ip pim neighbor** commands.

There are several things to look for:

- Neighbors on all of the active OSPF interfaces
- Neighbor IDs match the loopback of the other switch
- Neighbor State should be **FULL** to all adjacent switches
- VLANs subnets from other aggregation switches
- MSDP State is up
- PIM neighbors count is correct for the number of participating devices

The values indicate the OSPF neighbors are reachable, routing tables are propagated, and PIM is operational.

```
6405-AG2-1# show ip ospf neighbors
OSPF Process ID 1 VRF default
==============================

Total Number of Neighbors: 2

Neighbor ID      Priority  State             Nbr Address       Interface
-------------------------------------------------------------------------
10.0.0.1         n/a       FULL              172.18.102.2       1/3/47
10.0.0.2         n/a       FULL              172.18.102.6       1/3/48
```

```
6405-AG2-1# show ip route
Displaying ipv4 routes selected for forwarding

'[x/y]' denotes [distance/metric]

0.0.0.0/0, vrf default
        via  172.18.102.2,  [110/10],  ospf
        via  172.18.102.6,  [110/10],  ospf
10.0.0.1/32, vrf default
        via  172.18.102.2,  [110/10],  ospf
10.0.0.2/32, vrf default
        via  172.18.102.6,  [110/10],  ospf
...
```

```
6405-AG2-1# show ip pim neighbor

PIM Neighbor

VRF                         : default
Total number of neighbors : 2

IP Address                  : 172.18.102.2
Interface                   : 1/3/47
Up Time (HH:MM:SS)          : 00:00:55
Expire Time (HH:MM:SS)      : 00:01:20
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:01:45
...
```

Configure the Aggregation VLANs

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

The Layer-3 aggregation switch is the default gateway for access switches and will advertise the interface VLAN's to the rest of the network.

Step 1 Configure the access VLAN numbers and names.

```
vlan 2
  name ZTP_NATIVE
vlan 3
  name EMPLOYEE
...
vlan 14
  name CRITICAL_AUTH
vlan 15
  name MGMT
```

Step 2 Configure the Layer 3 interface VLAN. Configure a large IP MTU, set IP helper addresses, and enable OSPF using the router process and area. Enable IGMP and PIM sparse mode.

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

NOTE:
The **ip helper-address** command allows centralized DHCP servers to provide end-station IP addresses for the VLAN by forwarding requests the IP address of the central DHCP server. If there are more than one DHCP server servicing the same VLAN, list multiple helper commands on the interface and the DHCP client accepts the first offer it receives.

Step 3 Repeat the previous step for each VLAN.

Example: Access Aggregation

VLAN Name	VLAN ID	Access Agg 1	Access Agg 2	Network/Mask	Reserved Active gateway IP	IP helper address
ZTP_NATIVE	2	10.2.2.2	10.2.2.3	10.2.2.0/24	10.2.2.1	10.2.120.9810.2.120.99
EMPLOYEE	3	10.2.3.2	10.2.3.3	10.2.3.0/24	10.2.3.1	10.2.120.9810.2.120.99
BLDG_MGMT	4	10.2.4.2	10.2.4.3	10.2.4.0/24	10.2.4.1	10.2.120.9810.2.120.99
CAMERA	5	10.2.5.2	10.2.5.3	10.2.5.0/24	10.2.5.1	10.2.120.9810.2.120.99
PRINTER	6	10.2.6.2	10.2.6.3	10.2.6.0/24	10.2.6.1	10.2.120.9810.2.120.99
VISITOR	12	10.2.12.2	10.2.12.3	10.2.12.0/24	10.2.12.1	10.2.120.9810.2.120.99
REJECT_AUTH	13	10.2.13.2	10.2.13.3	10.2.13.0/24	10.2.13.1	10.2.120.9810.2.120.99
CRITICAL_AUTH	14	10.2.14.2	10.2.14.3	10.2.14.0/24	10.2.14.1	10.2.120.9810.2.120.99
MGMT	15	10.2.15.2	10.2.15.3	10.2.15.0/24	10.2.15.1	10.2.120.9810.2.120.99

Example: Service Aggregation 1

VLAN Name	VLAN ID	Service Agg 1	Service Agg 2	Network/Mask	Reserved Active gateway IP	IP helper address
EMPLOYEE	103	10.6.103.2	10.6.103.3	10.6.103.0/24	10.6.103.1	10.2.120.98 10.2.120.99
BLDG MGMT	104	10.6.104.2	10.6.104.3	10.6.104.0/24	10.6.104.1	10.2.120.98 10.2.120.99
CAMERA	105	10.6.105.2	10.6.105.3	10.6.105.0/24	10.6.105.1	10.2.120.98 10.2.120.99
PRINTER	106	10.6.106.2	10.6.106.3	10.6.106.0/24	10.6.106.1	10.2.120.98 10.2.120.99
VISITOR	112	10.6.112.2	10.6.112.3	10.6.112.0/24	10.6.112.1	10.2.120.98 10.2.120.99
REJECT_AUTH	113	10.6.113.2	10.6.113.3	10.6.113.0/24	10.6.113.1	10.2.120.98 10.2.120.99
CRITICAL_ AUTH	114	10.6.114.2	10.6.114.3	10.6.114.0/24	10.6.114.1	10.2.120.98 10.2.120.99
MGMT	15	10.6.15.2	10.6.115.3	10.6.15.0/24	10.6.15.1	10.2.120.98 10.2.120.99

Configure VSX and Spanning Tree

VSX is a virtualization technology used to logically combine two AOS-CX switches into a single logical device. From a management/control plane perspective, each switch is independent of the other, while the Layer 2 switch ports are treated like a single logical switch. VSX is supported on 6400, 8320, 8325, and 8400 models, but it is not supported on Aruba CX 6300, 6200, or 6100 models. VSX should only be enabled if the devices are positioned in a collapsed core or aggregation layer.

Spanning tree should be enabled on all devices as a heavy-handed loop prevention mechanism. This is done regardless of network topology to prevent accidental loops. Gateways and access switches will have high bridge ID's to prevent them from becoming the root bridge of the network. Any Layer 3 device will be left at the default priority, as it is unlikely Layer 2 VLANs will be stretched across them so there is not a need to configure STP on them. The root bridge must be the aggregation switches.

Step 1 Configure a LAG interface as the inter-switch link (ISL) for VSX synchronization. Allow all VLANs on this LAG for easier configuration management and the automatic enablement of VLANs in VSX.

```
interface lag 128
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
```

Step 2 Configure a Keepalive VRF and assign it to an interface. Create a new VRF and assign it to a direct interface that interconnects both VSX switches.

```
vrf VSX_KEEPALIVE

interface 1/1/1
    ip address 10.99.99.1/30
    vrf attach VSX_KEEPALIVE
```

Step 3 Configure VSX and enable it on the ISL link interface. Use the same LAG ID configured previously for the inter-switch link. Configure the IP address of the peer switch and source IP address of the existing switch in the Keepalive VRF from the previous step. Configure one switch with primary and one with the secondary role. The system-mac should be unique on each switch and not overlap with the active gateway MAC.

Example: Primary VSX Switch

```
vsx

inter-switch-link 128
    keepalive peer 10.99.99.2 source 10.99.99.1 vrf VSX_KEEPALIVE
    role primary
    system-mac 02-10-99-99-01-00
    vsx-sync aaa acl-log-timer bfd-global bgp copp-policy dhcp-relay dhcp-server dhcp-
snooping dns icmp-tcp lldp loop-protect-global mac-lockout mclag-interfaces neighbor
ospf qos-global route-map sflow-global snmp ssh stp-global time vsx-global
```

Example: Secondary VSX Switch

```
vsx

inter-switch-link 128
    keepalive peer 10.99.99.1 source 10.99.99.2 vrf VSX_KEEPALIVE
    role primary
    system-mac 02-10-99-99-02-00
    vsx-sync aaa acl-log-timer bfd-global bgp copp-policy dhcp-relay dhcp-server dhcp-
snooping dns icmp-tcp lldp loop-protect-global mac-lockout mclag-interfaces neighbor
ospf qos-global route-map sflow-global snmp ssh stp-global time vsx-global
```

Step 4 Configure the active gateway. Use the primary Switches internal MAC address and IP address.

Example: VLAN 2 on Primary VSX Switch

```
interface vlan 2
    active-gateway ip mac 02-10-99-99-01-00
    active-gateway ip 10.2.2.1
    description ZTP_Native
    ip mtu 9198
    ip address 10.2.2.2/24
    ip helper-address 10.2.120.98
    ip helper-address 10.2.120.99
```

Example: VLAN 2 on Secondary VSX Switch

```
interface vlan 2
    active-gateway ip mac 02-10-99-99-01-00
    active-gateway ip 10.2.2.1
    description ZTP_Native
    ip mtu 9198
    ip address 10.2.2.3/24
    ip helper-address 10.2.120.98
    ip helper-address 10.2.120.99
```

Step 5 Configuring spanning tree globally. Enable Rapid Per VLAN STP for the access VLANs and set the highest priority in preparation for VSX.

Example: Access Aggregation STP

```
spanning-tree mode rpvst
spanning-tree
spanning-tree priority 0
spanning-tree vlan 1-3,5-6,13-15
```

Example: Service Aggregation STP

```
spanning-tree mode rpvst
spanning-tree
spanning-tree priority 0
spanning-tree vlan 1-6,12-15
```

Step 6 Configure the MC-LAG interface for the downstream access switches. Enable spanning tree root guard and LACP fallback to allow ZTP of access switches. Configure the downstream VLANs as trunk and set the native VLAN to anything other than 1 and allow the previously created access VLANs. Enable LACP mode active and PIM sparse mode.

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

Step 7 Repeat the previous step for each MC-LAG interface required for the connected access switches.

Step 8 Configure MC-LAG on the downstream interfaces. Enter the LAG ID configured previously for the downstream interface.

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

Step 9 Repeat the previous step for each MC-LAG interface.

Step 10 Verify the VSX and MC-LAG configurations with the **show vsx status**, **show interface brief**, and **show lacp interface** commands.

There are several things to look for:

- The VSX operational state is “In-Sync” and the peer is reachable
- The access VLANs are up
- The forwarding state is up for all LACP interfaces

These values indicate VSX, LACP, and the VLANs are operational.

```
6405-AG2-1# show vsx status
VSX Operational State
---------------------
  ISL channel             : In-Sync
  ISL mgmt channel        : operational
  Config Sync Status      : In-Sync
  NAE                     : peer_reachable
  HTTPS Server            : peer_reachable

Attribute           Local               Peer
------------        --------            --------
ISL link            lag128              lag128
ISL version         2                   2
System MAC          00:00:10:00:06:01   00:00:10:00:06:01
Platform            6405                6405
Software Version    FL.10.06.0001       FL.10.06.0001
Device Role         secondary           primary
```

```
6405-AG2-1# show interface brief
--------------------------------------------------------------------------------
Port  Native Mode Type Enabled Status Reason Speed   Description
      VLAN                                          (Mb/s)
--------------------------------------------------------------------------------
vlan1  --    --        yes     up    --
vlan2  --    --        yes     up    --      SW_ZTP
...
vlan14 --    --        yes     up    --      CRITICAL_AUTH
vlan15 --    --        yes     up    --      MGMT
```

```
6405-AG2-1# show lacp interfaces

State abbreviations :
A - Active        P - Passive      F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync     O - OutofSync
C - Collecting    D - Distributing
X - State m/c expired              E - Default neighbor state

Actor details of all interfaces:
------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr Forwarding
           Name       Id    Pri                             Pri    Key  State
------------------------------------------------------------------------------
1/3/1      lag11(mc)  1129  1     ALFNCD  00:00:10:00:06:01 65534  11   up
1/3/2      lag12(mc)  1130  1     ALFNCD  00:00:10:00:06:01 65534  12   up
...

Partner details of all interfaces:
------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr
           Name       Id    Pri                             Pri    Key
------------------------------------------------------------------------------
1/3/1      lag11(mc)  29    1     ALFNCD  64:e8:81:c1:c4:00 65534  1
1/3/2      lag12(mc)  29    1     ALFNCD  64:e8:81:c5:a2:40 65534  1
...
```

Import the Aggregation Switches

Use this procedure to create templates for configured aggregation switches and import them into Central.

When bringing an aggregation switch into Central it is recommended to use a UI Group which allows the use of MultiEdit. This is beneficial in the case that aggregation switches were configured onsite by an admin and will allow admins to incrementally change aggregation switches as needed without the need to edit the template across all aggregation switches. This procedure will walk through how to import an already configured aggregation switch into central. It is important to note that the switches will be configured before bringing them into Central; MultiEdit will act as a day 2 configuration tool.

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

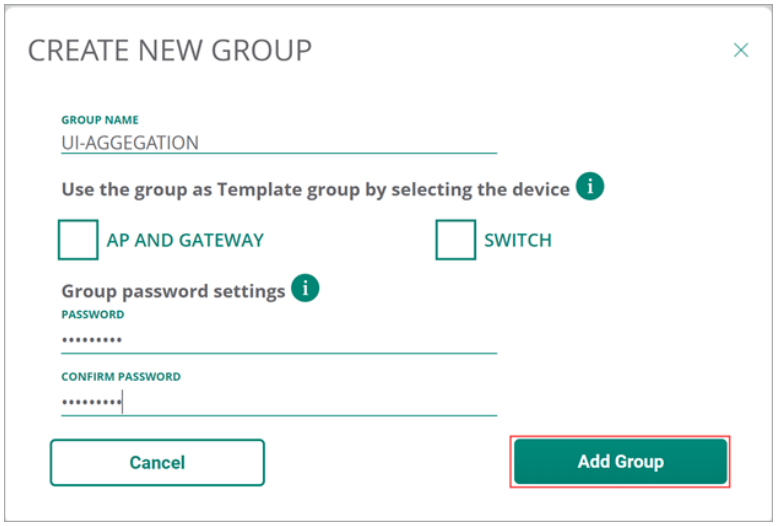
Step 2 On the Aruba Central Account Home page, launch the **Network Operations** app.

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

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

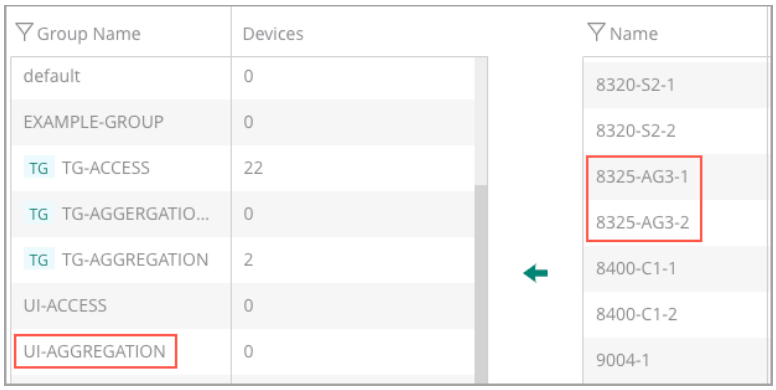
Step 5 On the Create New Group page, implement the following settings, and then click **Add Group**.

- **GROUP NAME:** *UI-Aggregation*
- **PASSWORD:** *password*
- **CONFIRM PASSWORD:** *password*

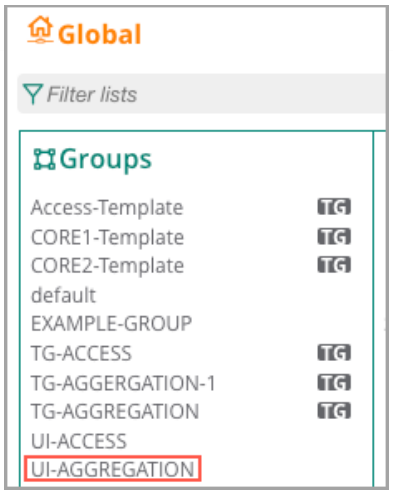


NOTE:
The password enables administrative access to the devices interface. This password is used as the login password for all the devices in the group, but it is not the enable password. The same password can be used across multiple groups.

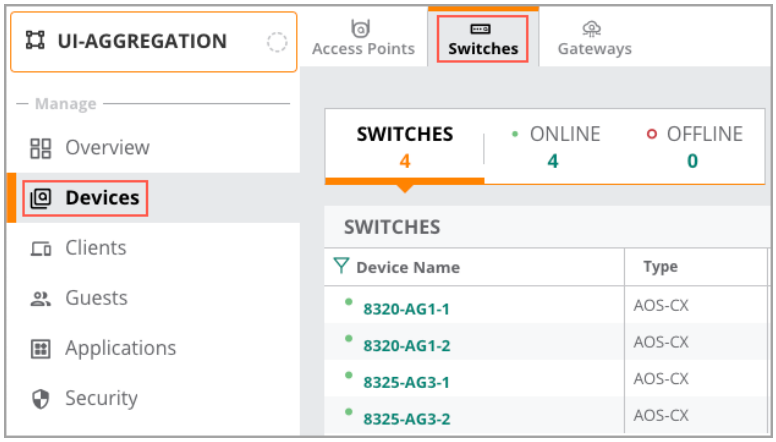
Step 6 On the Groups page, in the Manage Groups section, drag the aggregation switches from the right side to the UI Group on the left side.



Step 7 At the top left of the page, navigate to **Global > Groups**, and then from the Groups list, select **UI-Aggregation**.

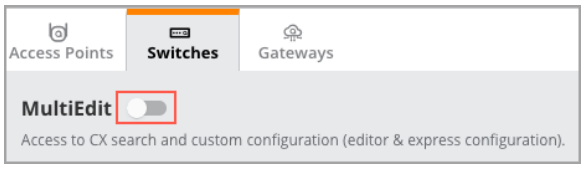


Step 8 From the left menu, select **Devices**, and then on the tab menu bar, select **Switches**.

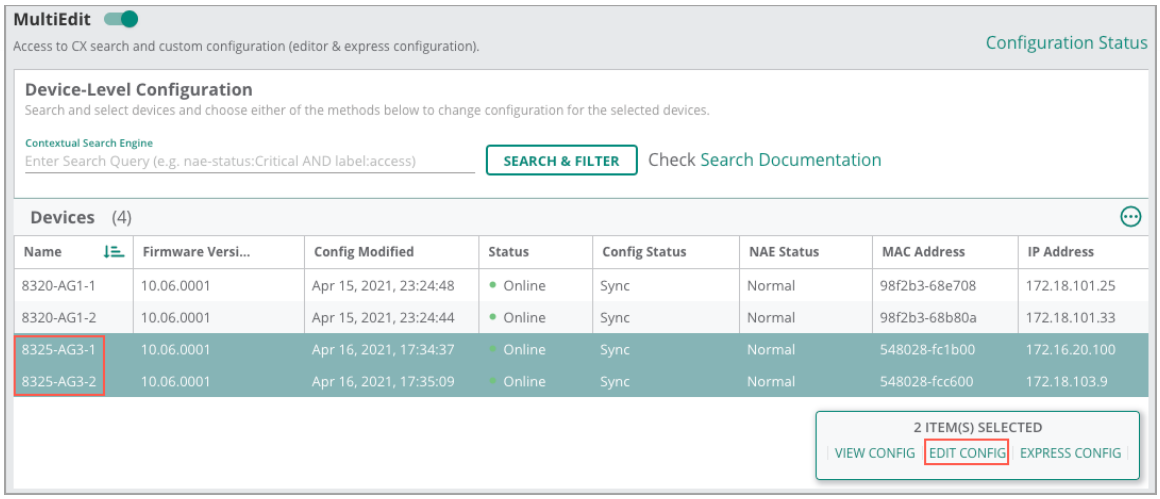


Step 9 On the Switches List page in the top right, click **Config**.

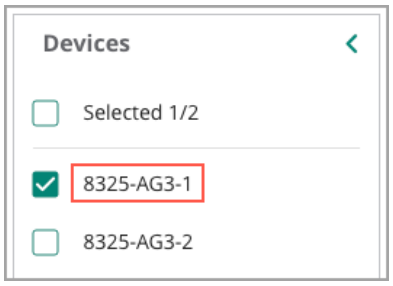
Step 10 On the Switches page, move the **MultiEdit** slider to the right.



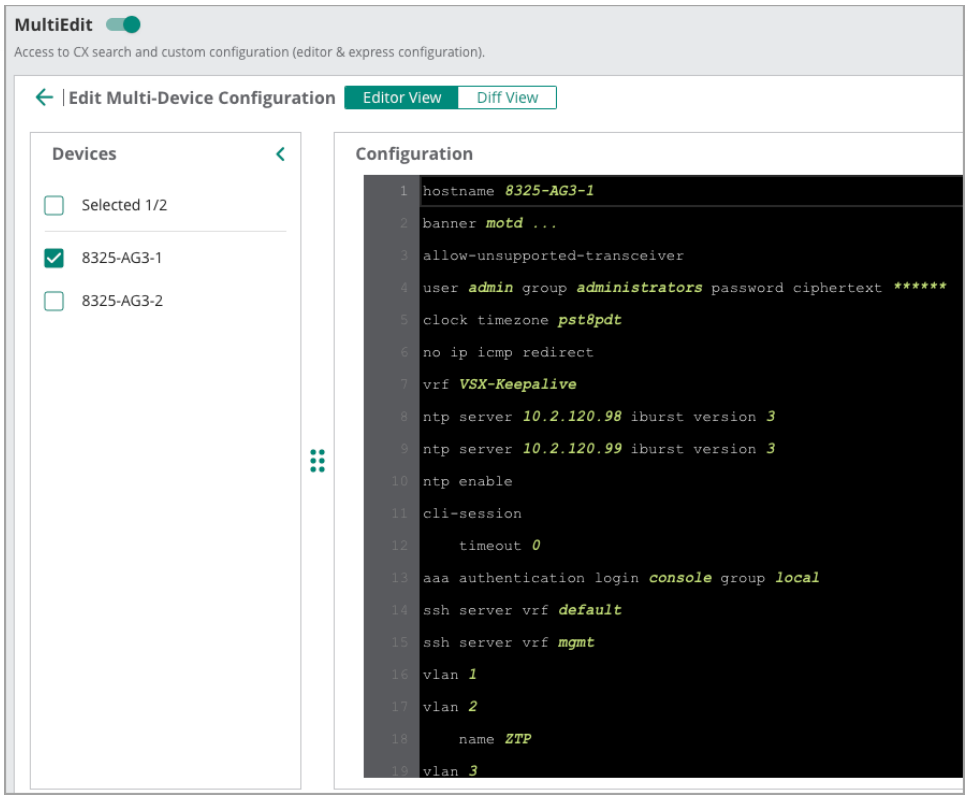
Step 11 On the Switches page, click the aggregation switches to highlight them, and then in the lower right, click **Edit Config**.



Step 12 From the menu on the left, select one aggregation switch.

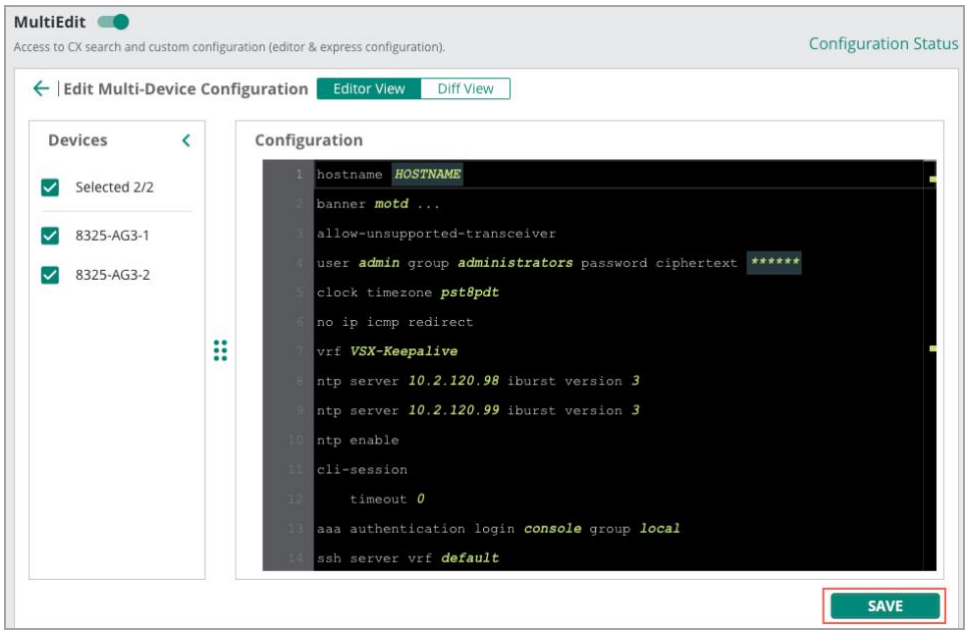


Step 13 Using your favorite SSH tool, log into the CLI of the selected aggregation switch, copy the running configuration, and then paste it into the Configuration section of the MultiEdit page.

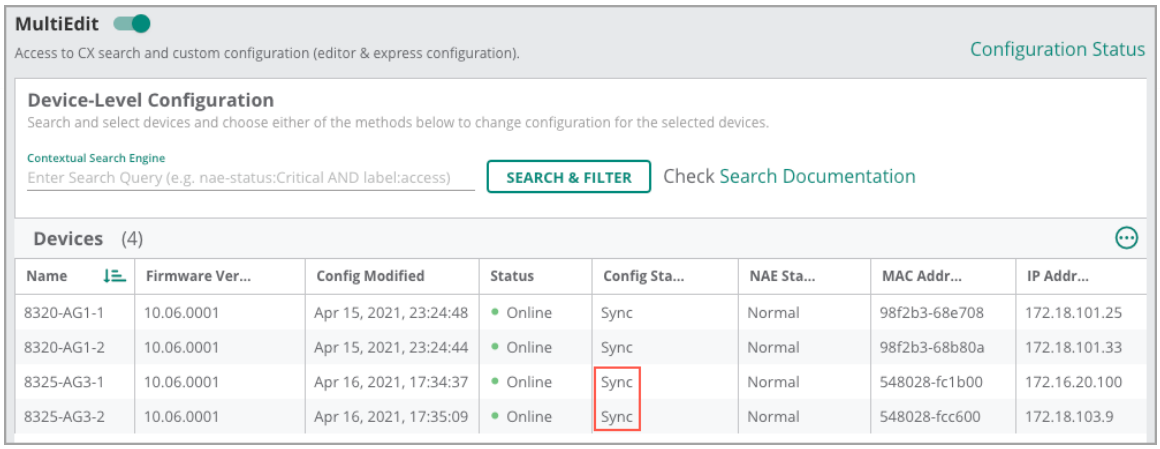


Step 14 Repeat the previous two steps for the second aggregation Switch.

Step 15 From the menu on the left, select both aggregation Switches, and then at the bottom right, click Save.



Step 16 On the Switches Config page, confirm the Status is **Sync**.



Name	Firmware Ver...	Config Modified	Status	Config Sta...	NAE Sta...	MAC Addr...	IP Addr...
8320-AG1-1	10.06.0001	Apr 15, 2021, 23:24:48	Online	Sync	Normal	98f2b3-68e708	172.18.101.25
8320-AG1-2	10.06.0001	Apr 15, 2021, 23:24:44	Online	Sync	Normal	98f2b3-68b80a	172.18.101.33
8325-AG3-1	10.06.0001	Apr 16, 2021, 17:34:37	Online	Sync	Normal	548028-fc1b00	172.16.20.100
8325-AG3-2	10.06.0001	Apr 16, 2021, 17:35:09	Online	Sync	Normal	548028-fcc600	172.18.103.9

Step 17 Repeat this procedure for each aggregation Switch pair in your network.

Example: Aggregation Switch Template

Aggregation Switch Template

Wired Access

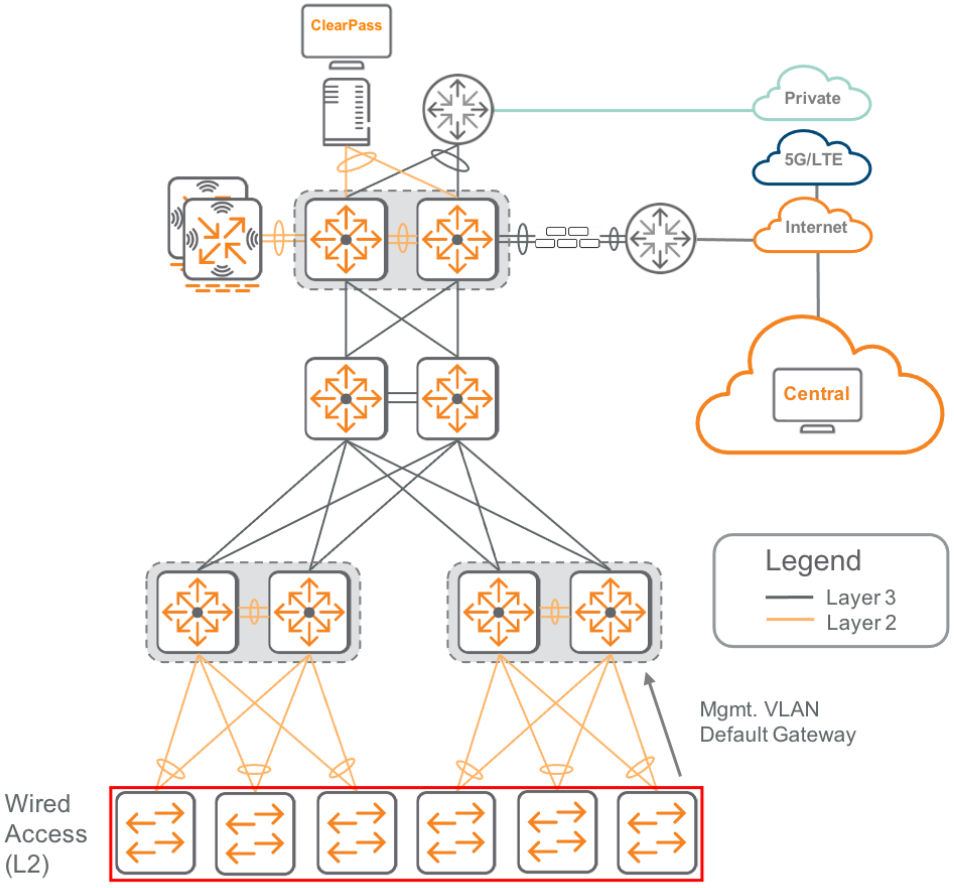
The access layer in this design provides Layer 2 connectivity to the network for wired and wireless devices. It plays an important role in protecting users, application resources, and the network itself from human error and malicious attacks. This protection includes verifying the devices are allowed on the network, making sure the devices cannot provide unauthorized services to end users, and preventing unauthorized devices from taking over the role of other devices on the network.

Configuring the Access with Template Groups

The access layer also provides services like PoE, QoS, and VLAN assignments in order to reduce operational requirements. To simplify the network as much as possible, the access Switches are Layer 2 and have a default gateway in their management VLAN for Central connectivity.

The following figure shows the access switches in the ESP Campus.

Wired Access



Configure Access Switch Stacking

This optional procedure is for switching platforms with VSF front plane stacking, like the Aruba 6200 and 6300 series. If you are not using a switch stack in this area of your network, skip this procedure.

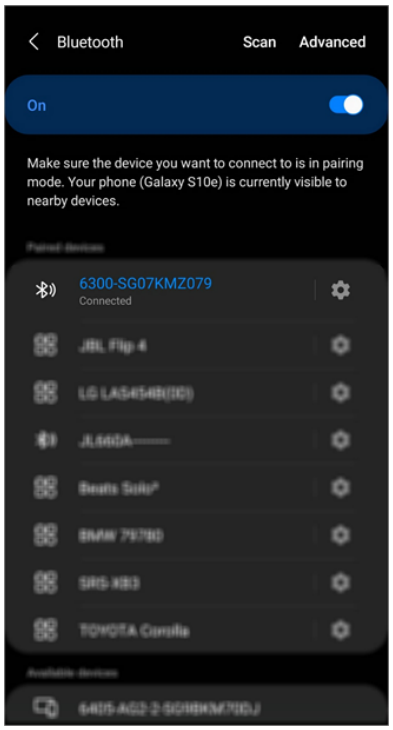
VSF stacking allows multiple access switches to be combined into one logical device increasing port density in the access closet. Combining multiple physical switches into one virtual switch allows easier management and configuration from a single IP address. Since stacking is disruptive, it should be done before applying additional configuration.

This procedure uses the Aruba CX mobile app to provision stacking and requires a supported Android or iOS device. To configure stacking using the CLI of the Switch, please visit the VSF Best Practices for Aruba CX 6300 Switch Series guide.

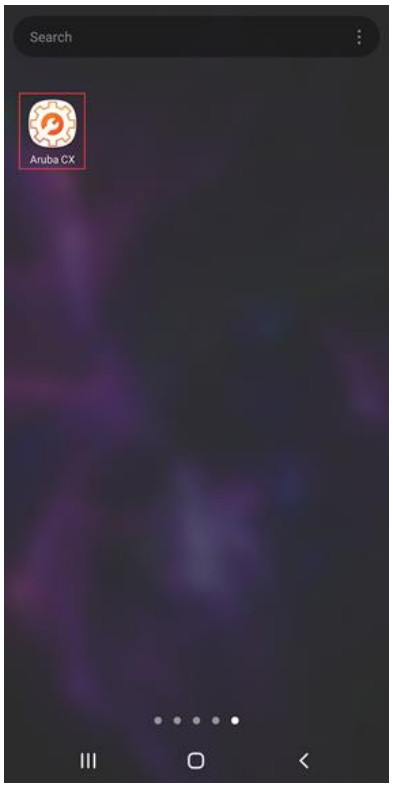
To start the provisioning process, power up and fully boot all members of the stack into their factory default state. Connect cables to all the ports used for the VSF links and plug the USB Bluetooth adapters into the front panel USB-A port on each switch member.

NOTE:
The USB Bluetooth adapter is purchased with the switch.

Step 1 Using your phone's Bluetooth menu, search for the serial number of the commander switch and then connect to it.

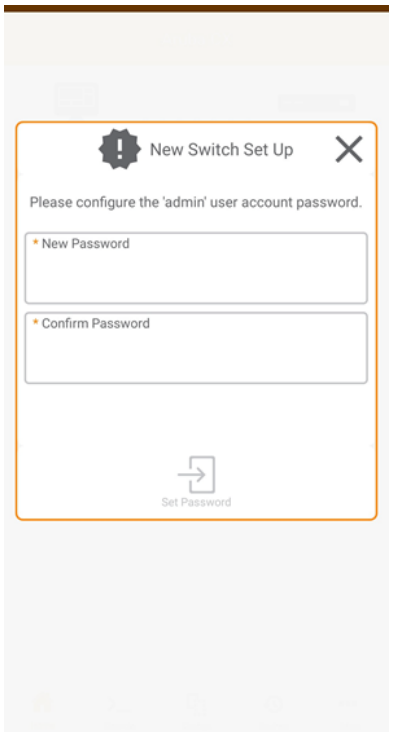


Step 2 On your phone, open the **Aruba CX** app.



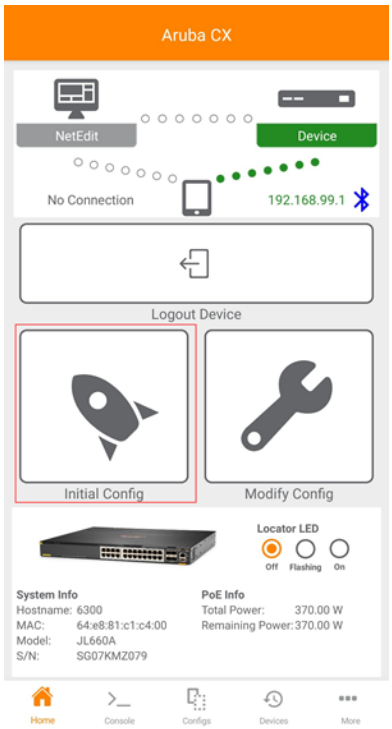
Step 3 On the New Switch Set Up screen, implement the following settings and then select **Set Password**.

- **New Password:** *password*
- **Confirm Password:** *password*



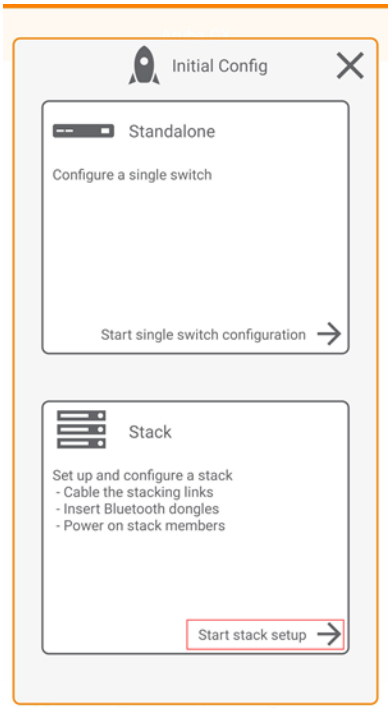
NOTE:
The initial admin user account password is overwritten in a later process by the admin password stored in the Central template. This is a temporary password used during setup.

Step 4 On the Home screen, select **Initial Config**.

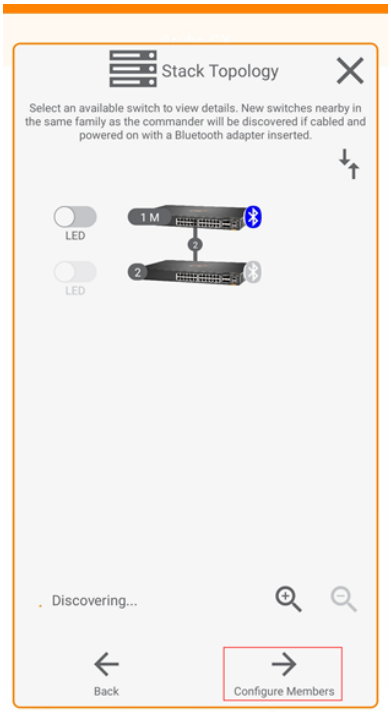


NOTE:
To confirm you are connected to the correct switch, select the Locator LED Flashing radio button and then look for the flashing blue light labeled **UID** on the front of the switch.

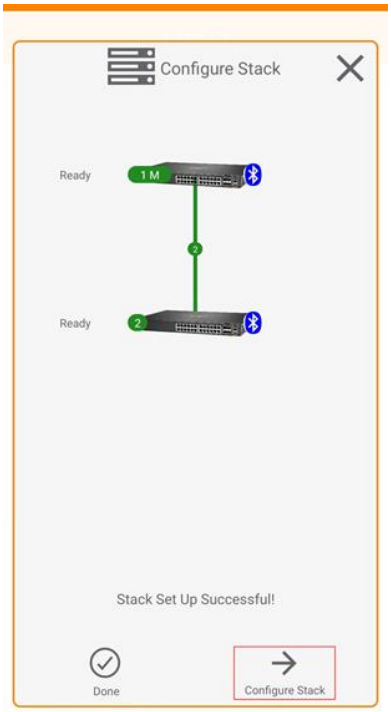
Step 5 On the Initial Config screen, select **Start stack setup**.



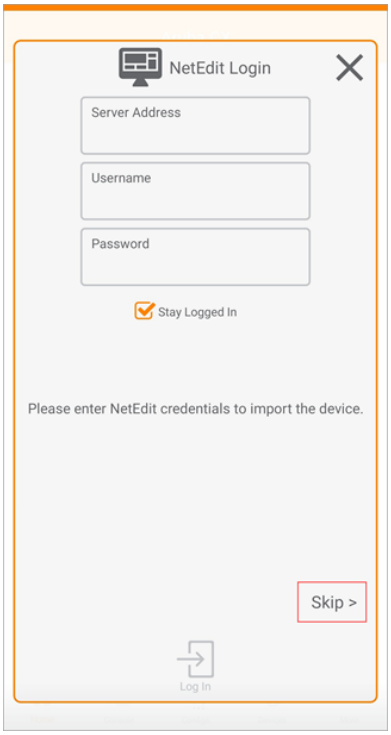
Step 6 On the Stack Topology screen, wait for the members to be discovered, and then click **Configure Members**.



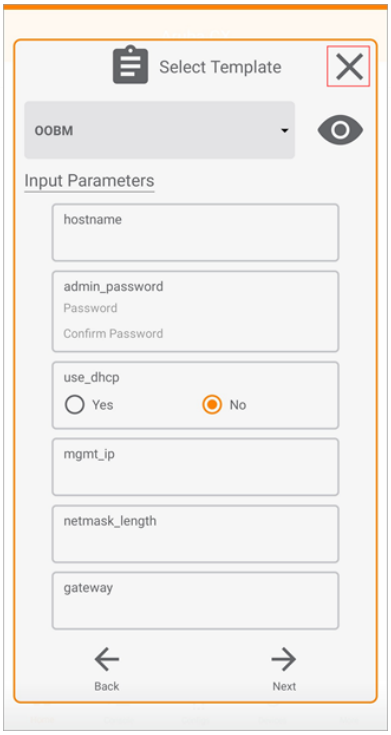
Step 7 On the Configure Stack screen, once the stack is complete, click **Configure Stack**.



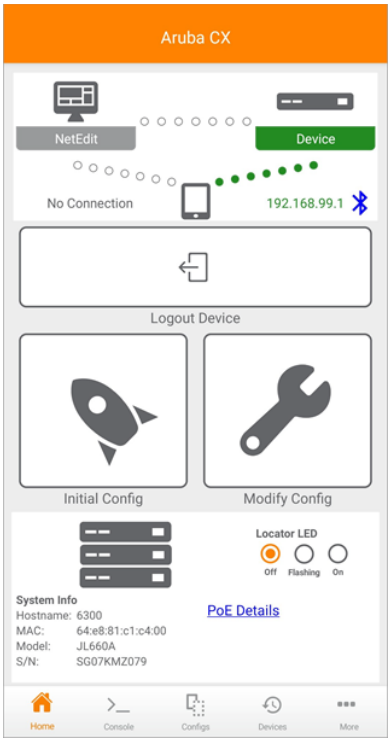
Step 8 On the NetEdit Login screen, click **Skip**.



Step 9 On the Select Template screen, in the top right, click the **X**.



Step 10 On the Home screen, confirm the switch stack is configured by the stack icon in the lower left.



Step 11 Repeat this procedure for each switch stack in the environment.

Configure the Access Base Features

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

On each access Switch or Switch stack, perform the following steps:

Step 1 Configure the Switch host name.

```
hostname Access-Switch
```

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.

```
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 will break the switch from the MOTD context. In this example, the delineator is the "$".

Step 4 Configure the NTP servers and timezone.

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

Step 5 Verify the NTP configuration with the **show ntp status** command.

There are several things to look for:

- 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.

```
6300M-AG1-AC5 # show ntp status
NTP Status Information

NTP                          : Enabled
NTP Authentication           : Disabled
NTP Server Connections       : Using the default VRF

System time                  : Fri Apr  2 01:11:14 PDT 2021
NTP uptime                   : 24 days, 9 hours, 8 minutes, 54 seconds

NTP Synchronization Information

NTP Server                   : 10.2.120.98 at stratum 3
Poll interval                : 1024 seconds
Time accuracy                : Within -0.002617 seconds
Reference time               : Fri Apr  2 2021  0:50:57.918 as per US/Pacific
```

Step 6 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.com
```

Step 7 Configure the TACACS servers with a plaintext key.

```
tacacs-server host 10.2.120.94 key Plaintext <key>
tacacs-server host 10.2.120.95 key Plaintext <key>
```

Step 8 Configure the TACACS server group. Create the server group and use the IP addresses from the TACACS server hosts configured previously.

- **Server group name:** *ClearPass*

```
aaa group server tacacs ClearPass
    server 10.2.120.94
  server 10.2.120.95
```

NOTE:
TACACS servers groups allow the Switch to fallback to a secondary server if the primary server is down.

Step 9 Configure AAA for the TACACS server group. The AAA commands point to the TACACS server group configured previously. Configure the start and stop time of each session and a fallback mechanism in case the TACACS server is down or unreachable.

```
aaa authentication login ssh group ClearPass local
aaa authentication login console group ClearPass local
aaa authorization commands default group  local ClearPass
aaa accounting all default start-stop group ClearPass local
aaa authentication allow-fail-through
```

NOTE:
Devices use TACACS for both console and SSH access with a fall back to local authentication. All devices should have a local backup account on the switch to allow access when the TACACS server is unreachable.

Step 10 Configure TACACS server tracking.

```
tacacs-server tracking user-name TrackUser plaintext <password>
```

NOTE:
The tracking account used with the TACACS server should only have permissions to log in and nothing else.

Step 11 Verify the TACACS server configuration with the **show tacacs-server statistics** command.

There are several things to look for:

- Round Trip Time
- Auth Start
- Auth Accepts
- Tracking Requests
- Tracking Responses

The non-zero values indicate the TACACS service is reachable by the Switch.

```
6300M-AG1-AC5(config)# show tacacs-server statistics
 Server Name     : 10.2.120.94
 Auth-Port       : 49
 VRF             : default
 Authentication Statistics
-------------------------------------------
 Round Trip Time(ms)       : 82
 Pending Requests          : 0
 Timeout                   : 0
 Unknown Types             : 0
 Packet Dropped            : 1
 Auth Start                : 25
 Auth challenge            : 2
 Auth Accepts              : 20
 Auth Rejects              : 4
 Auth reply malformed      : 0
 Tracking Requests         : 3
 Tracking Responses        : 5
...
```

Configure the Access VLANs

In order to provide client devices with network connectivity, the access switches must have the same VLANs as the aggregation switches. The access switches will also have an additional Layer 3 interface for the management VLAN and one for User-Based Tunnel (UBT) clients.

DHCP snooping stops DHCP starvation attacks and it also prevents rogue DHCP servers from servicing requests on your network. ARP inspection stops man-in-the-middle attacks caused by ARP cache poisoning.

IGMP snooping is designed to prevent 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. IGMP snooping must be enabled on the Layer 2 switches for Dynamic Multicast Optimization (DMO) to work.

DHCP snooping needs to be enabled globally, as well as under each VLAN to snoop DHCP packets. ARP inspection only needs to be enabled under the VLAN but will not take effect unless DHCP snooping is also enabled. Finally, IGMP snooping is enabled for IP multicast traffic.

Example: Access VLANs

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

On each access Switch, perform the following steps:

Step 1 Configure DHCP snooping globally.

```
dhcpv4-snooping
```

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

```
vlan 1
  dhcpv4-snooping
  arp inspection
  ip igmp snooping enable
vlan 2
  name ZTP_NATIVE
  dhcpv4-snooping
  arp inspection
  ip igmp snooping enable
...
vlan 15
  name MGMT
  dhcpv4-snooping
  arp inspection
  ip igmp snooping enable
vlan 4000
  name UBT_CLIENT
  dhcpv4-snooping
  arp inspection
  ip igmp snooping enable
```

CAUTION:
The access switch VLANs must match the aggregation switch VLANs to allow the access devices to reach their default gateway.

Step 3 Configure the Layer 3 interface VLAN. Configure a large MTU to match the aggregation switch.

```
interface vlan 2
  description ZTP_Native
  ip mtu 9198
  ip address 10.2.15.5/24
```

Step 4 Repeat the previous step for every VLAN on the switch. **Step 5** Configure the default route in the management VLAN. Add the static route for the active gateway IP address in VLAN 15.

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

NOTE:
The access Switch must have a default route in the management VLAN for reachability to network services like Central, TACACS, RADIUS, and NTP servers.

Step 7 Verify the DHCP Snooping and ARP inspection configurations with the **show dhcpv4-snooping statistics**, **show dhcpv4-snooping binding**, and **show arp inspection statistics vlan** commands.

There are a couple of things to look for:

- Packet-Type: server - Action: forward
- Packet-Type: client - Action: forward

The non-zero values indicate DHCP snooping is actively forwarding traffic from servers and clients.

```
6300M-AG1-AC5# show dhcpv4-snooping statistics

 Packet-Type  Action   Reason                          Count
 -----------  -------  ------------------------------  ---------
 server       forward  from trusted port               9
 client       forward  to trusted port                 11
 server       drop     received on untrusted port     0
 server       drop     unauthorized server            0
 client       drop     destination on untrusted port  0
 client       drop     untrusted option 82 field      0
...
```

```
6300M-AG1-AC5# show dhcpv4-snooping binding

  MacAddress         IP               VLAN  Interface  Time-Left
  -----------------  ---------------  ----  ---------  --------------------
  a0:36:9f:05:0a:c8  10.1.14.105      14   1/1/21     689577
```

```
6300M-AG1-AC5# show arp inspection statistics vlan 14

-------------------------------------------------------------------
VLAN   Name              Forwarded           Dropped
-------------------------------------------------------------------
 14    CRITICAL_AUTH     159                 321
-------------------------------------------------------------------
```

Configure RADIUS and UBT

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

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

RADIUS tracking is enabled to ensure the status of the client and server. The configuration will also leverage user roles for rejected clients and RADIUS failure scenarios. The configuration of RADIUS and user roles goes hand in hand with UBT, so this section also covers the UBT configuration.

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 UBT to tunnel traffic to the gateways. Define the UBT client VLAN and create the UBT zone in the default VRF. Connect to a pair of gateways for the primary and backup tunnels.

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

```
ubt-client-vlan 4000

ubt zone Aruba vrf default
  primary-controller ip 10.6.15.11
  backup-controller ip 10.6.15.12
  enable
```

Step 4 Configure local user roles. Create the user role and if the VLAN is tunneled, set the gateway zone, and gateway role. If the VLAN is not tunneled, set the authentication mode or the reauthorization period and the local VLAN.

```
port-access role BLDG-MGMT
    gateway-zone zone Aruba gateway-role EXAMPLE-BLDG-MGMT
port-access role GUEST
    gateway-zone zone Aruba gateway-role EXAMPLE-GUEST
port-access role ARUBA-AP
  auth-mode device-mode
  vlan access 15
port-access role CRITICAL_AUTH
  reauth-period 120
  vlan access 14
port-access role REJECT_AUTH
  reauth-period 120
  vlan access 13
```

NOTE:
Special-case local user roles, like Aruba-AP, Critical Auth, and Reject, are not tunneled back to the gateways.

Step 5 Configure AAA authentication on the access ports. Set the client limit, configure 802.1x, and MAC authentication, and set the authentication order. Set the critical role and the rejection role to use special case user roles with local VLANs. 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
```

NOTES:
EAPOL timeout: The amount of time the EAP request will wait before its considered a lost packet
Max EAPOL requests: The number of requests the interfaces can have at a time
Max retries: The number of times the switch will try to authenticate the device

Step 6 Verify the RADIUS configuration with the **show radius-server** command.

There are a couple of things to look for:

- Both servers are reachable without a "*" before their name
- The VRF is set to the default

These values indicate the RADIUS servers are reachable in the correct VRF.

```
6300M-AG1-AC5# show radius-server
Unreachable servers are preceded by *
******* Global RADIUS Configuration *******

Shared-Secret: None
Timeout: 5
Auth-Type: pap
Retries: 1
TLS Timeout: 5
Tracking Time Interval (seconds): 300
Tracking Retries: 1
Tracking User-name: radius-tracking-user
Tracking Password: None
Number of Servers: 2

-------------------------------------------------------------------
SERVER NAME                                | TLS  | PORT | VRF
-------------------------------------------------------------------
10.2.120.94                                |      | 1812 | default
10.2.120.95                                |      | 1812 | default
-------------------------------------------------------------------
```

Step 7 Verify the UBT configuration with the **show ubt state**, **show port-access clients**, and **show ubt users up** commands.

There are a couple of things to look for:

- The active and standby SAC’s are registered
- If you have active users, check the client status equals success and tunnels are activated without failures

These values indicate the UBT gateways are registered, and the clients are operational.

```
6300M-AG1-AC5# show ubt state

================================================================
Zone Aruba:
================================================================

Local Master Server (LMS) State:

LMS Type      IP Address    State               Role
----------------------------------------------------------------
Primary     : 10.6.15.11 ready_for_bootstrap operational_primary

Switch Anchor Controller (SAC) State:

              IP Address      MAC Address          State
-------------------------------------------------------------
Active      : 10.6.15.11      00:1a:1e:05:0e:70    registered
Standby     : 10.6.15.12      00:1a:1e:05:01:30    registered
```

```
6300M-AG1-AC5# show port-access clients

Port Access Clients

Status codes: d device-mode

------------------------------------------------------------------------------
  Port     MAC-Address       Onboarding     Status      Role
                             Method
------------------------------------------------------------------------------
  1/1/1    9c:8c:d8:c9:0e:60 mac-auth       Success     BLDG-MGMT
  1/1/23   00:1b:21:ad:1f:51                Success     CRITICAL_AUTH, Critical
```

```
6300M-AG1-AC5(config)# show ubt users up

================================================================
Displaying UBT Users of Zone: Aruba having Tunnel Status UP
================================================================
Downloaded user roles are preceded by *
Port    Mac-Address        Tunnel Status  Gateway-Role        Failure Reason
----------------------------------------------------------------------------
1/1/1   9c:8c:d8:c9:0e:60  activated      EXAMPLE-BLDG-MGMT   ---/---
```

Configure Device Profiles

Device profiles dynamically detect the APs, place them into the management VLA,N and identify the locally bridged VLANs.

NOTE:
This procedure can be skipped if ClearPass will be used to authenticate Aruba AP's.

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 15
  vlan trunk allowed 1-3,5-6,13-15
```

NOTE:
The Aruba-AP role identifies the AP's VLAN and what VLANs are bridged locally. It also sets the authentication mode for AP's to device mode which allows users connecting to the AP to be authenticated from the wireless captive portal rather than the switching infrastructure.

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 AP's and sets the system-description at the end as a catch all for future AP's.

Step 3 Configure the device profile. Create the profile, enable it, and 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
```

Step 4 Verify the device profile configuration with the **show port-access clients** and **show port-access device-profile all** commands.

There are a couple of things to look for:

- 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.

```
6300M-AG1-AC5# show port-access clients

Port Access Clients

Status codes: d device-mode

--------------------------------------------------------------------------------
  Port     MAC-Address       Onboarding     Status      Role
                             Method
--------------------------------------------------------------------------------
  1/1/1    9c:8c:d8:c9:0e:60 mac-auth       Success     BLDG-MGMT
d 1/1/2    bc:9f:e4:c3:3d:64 device-profile Success     ARUBA-AP
```

```
6300M-AG1-AC5# show port-access device-profile interface all
  Port 1/1/2, Neighbor-Mac  bc:9f:e4:c3:3d:64
    Profile Name:           : ARUBA_AP
    LLDP Group:             : AP-LLDP-GROUP
    CDP Group:              :
    MAC Group:              :
    Role:                   : ARUBA-AP
    State:                  : applied
    Failure Reason:         :
```

Configure Spanning Tree

Spanning tree is enabled globally on each access switch as a loop prevention mechanism. Supplemental features like admin-edge, root guard, BPDU guard, and TCN guard are enabled on each interface to ensure spanning tree runs effectively.

On each access switch, perform the following steps:

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

```
spanning-tree mode rpvst
spanning-tree
spanning-tree priority 0
spanning-tree vlan 1-3,5-6,13-15
```

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
```

Step 3 Configure loop protect. Enable loop protect on access ports to stop unwanted loops between access interfaces.

```
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 4 Repeat the previous two steps for each access port interface.

Step 5 Verify the spanning tree configuration with the **show spanning-tree summary root** and **show spanning-tree summary port** commands.

There are several things to look for:

- The STP status is enabled and the protocol is RPVST
- The root port is the uplink to the aggregation switch
- The access ports have the supplemental features enabled

These values indicate RPVST is enabled, and the supplemental features are configured.

```
6300M-AG2-AC2# show spanning-tree summary root
STP status            : Enabled
Protocol              : RPVST
System ID             : 64:e8:81:c5:a2:40

Root bridge for VLANs :
                                          Root Hello Max Fwd
VLAN     Priority Root ID                 cost  Time Age Dly    Root Port
-------- -------- ----------------- --------- ----- --- --- ------------
VLAN1        4096 00:00:10:00:06:01       800     2  20  15         lag1
VLAN2        4096 00:00:10:00:06:01       800     2  20  15         lag1
...
VLAN14       4096 00:00:10:00:06:01       800     2  20  15         lag1
VLAN15       4096 00:00:10:00:06:01       800     2  20  15         lag1
```

```
6300M-AG2-AC2# show spanning-tree summary port
STP status                      : Enabled
Protocol                        : RPVST
BPDU guard Timeout value        : None
BPDU guard enabled interfaces   : 1/1/1-1/1/24,2/1/4-2/1/24
BPDU filter enabled interfaces  : None
Root guard enabled interfaces   : 1/1/1-1/1/24,2/1/4-2/1/24
Loop guard enabled interfaces   : None
TCN guard enabled interfaces    : 1/1/1-1/1/24,2/1/4-2/1/24
RPVST filter enabled interfaces : None
RPVST guard enabled interfaces  : None

Interface count by state

VLAN                   Blocking Listening Learning Forwarding
---------------------- -------- --------- -------- ----------
VLAN1                        45         0        0          6
VLAN2                         6         0        0          5
...
VLAN14                        6         0        0          5
VLAN15                        6         0        0          5
---------------------- -------- --------- -------- ----------
Total =    8                 87         0        0         42
```

Configure Uplink Ports

The uplink ports use the link aggregation control protocol (LACP) to combine two or more physical ports into a single trunk interface for redundancy and increased capacity. By default, the uplink trunks use source and destination IP, port, and MAC addresses to load-balance traffic between the physical interfaces.

On each access switch, perform the following steps:

Step 1 Configure the LAG interface. Configure a large MTU to match the aggregation switch. Set the native VLAN and the allowed VLANs on the trunk. Enable LACP with active mode.

```
interface lag 1
  description Uplink_AGG
  ip mtu 9198
  no shutdown
  no routing
  vlan trunk native 1
  vlan trunk allowed 1-3,5-6,13-15
  lacp mode active
```

Step 2 Configure ARP inspection trust and DHCP snooping trust.

```
interface lag 1
  no shutdown
  no routing
  vlan trunk native 1
  vlan trunk allowed 1-3,5-6,13-15
  lacp mode active
  arp inspection trust
  dhcpv4-snooping trust
```

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

Step 3 Configure the uplink interfaces with the LAG from the previous step.

```
interface 1/1/49
  no shutdown
  lag 1

interface 1/1/50
  no shutdown
  lag 1
```

Step 4 Verify the LAG configuration with the **show lacp interfaces** command.

There are a couple of things to look for:

- The LAG state for Actor and Partner is ALFCND
- The forwarding state for Actor is up

These values indicate LACP is active, and traffic is forwarded.

```
6300M-AG2-AC2# show lacp interfaces

State abbreviations :
A - Active        P - Passive      F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync     O - OutofSync
C - Collecting    D - Distributing
X - State m/c expired              E - Default neighbor state

Actor details of all interfaces:
------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr Forwarding
           Name       Id    Pri                             Pri    Key  State
------------------------------------------------------------------------------
1/1/28     lag1       29    1     ALFNCD  64:e8:81:c5:a2:40 65534  1    up
2/1/28     lag1       93    1     ALFNCD  64:e8:81:c5:a2:40 65534  1    up

Partner details of all interfaces:
------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr
           Name       Id    Pri                             Pri    Key
------------------------------------------------------------------------------
1/1/28     lag1       1130  1     ALFNCD  00:00:10:00:06:01 65534  12
2/1/28     lag1       130   1     ALFNCD  00:00:10:00:06:01 65534  12
```

Import the Access Switches

Use this procedure to create template groups for the access switches and then import them into Central.

When importing access switches into Central, template groups are recommended due to the large number of switches with common configurations.

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

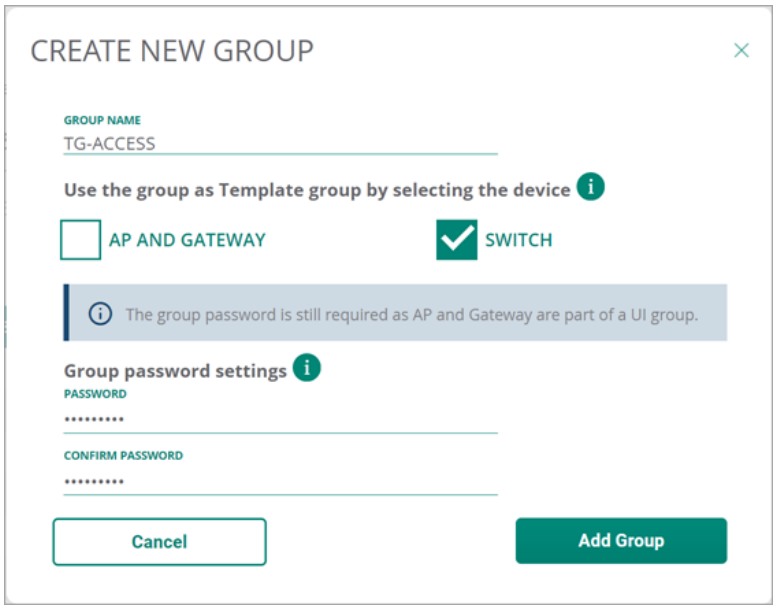
Step 2 On the Aruba Central Account Home page, launch the **Network Operations** app.

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

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

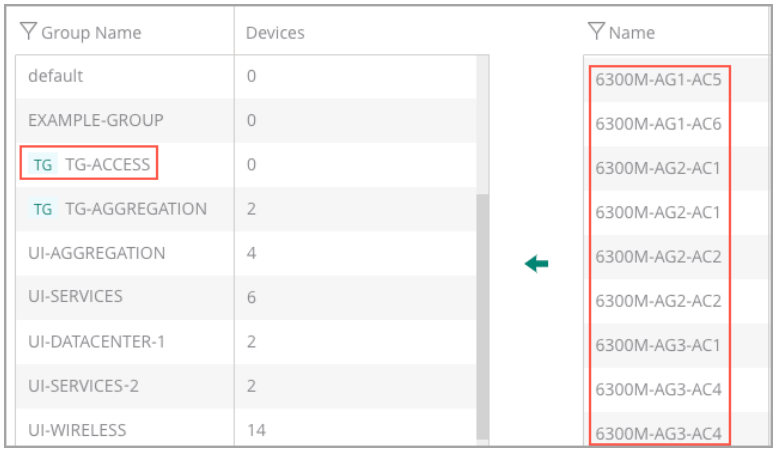
Step 5 On the Create New Group page, implement the following settings, and then click **Add Group**.

- **GROUP NAME:** *TG-Access*
- **SWITCH:** *checkmark*
- **PASSWORD:** *password*
- **CONFIRM PASSWORD:** *password*

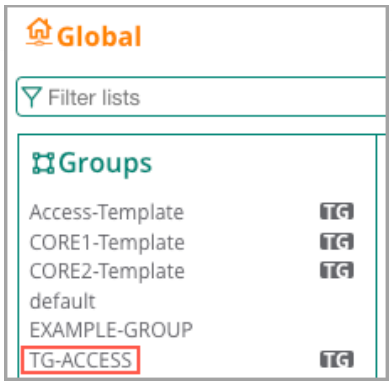


NOTE:
The password enables administrative access to the devices interface. This password is used as the login password for all the devices in the group, but it is not the enable password. The same password can be used across multiple groups.

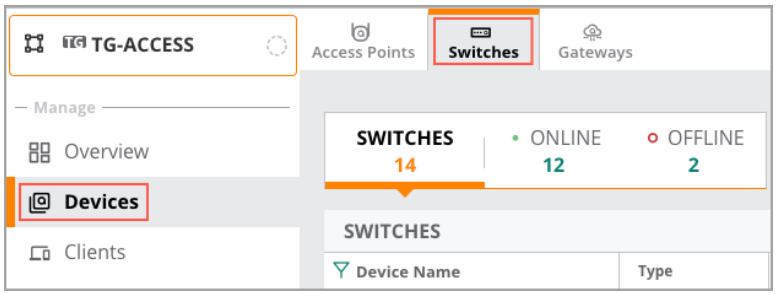
Step 6 On the Groups page, in the Manage Groups section, drag the access Switches from the right side to the template group on the left side.



Step 7 At the top left of the page, navigate to **Global > Groups**, and then from the Groups list, select **TG-ACCESS**.



Step 8 From the left menu, select **Devices**, and then on the tab menu bar, select **Switches**.

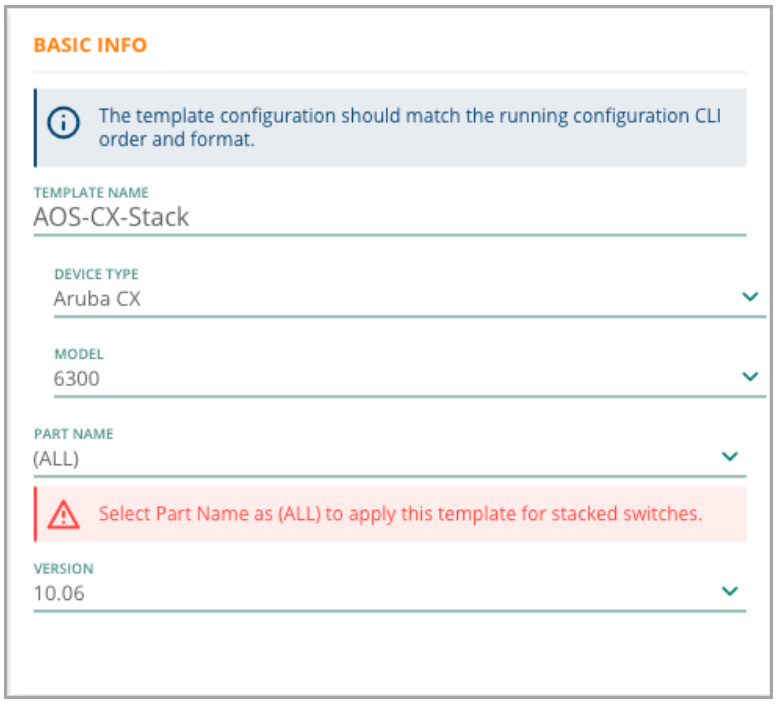


Step 9 On the Switches List page in the top right, click **Config**.

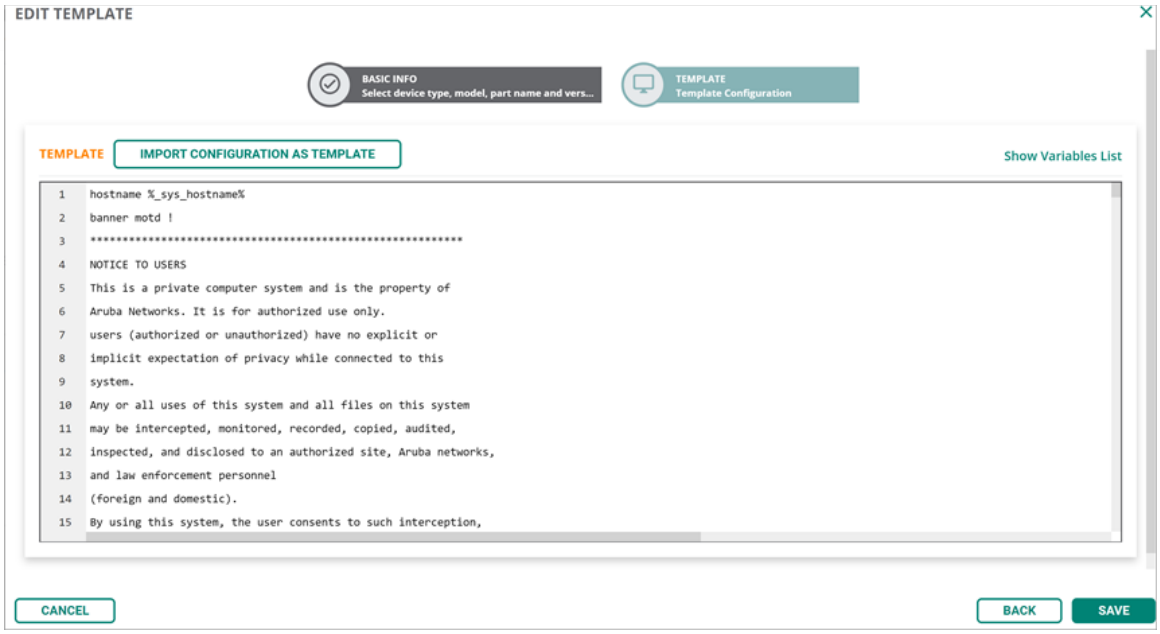
Step 10 On the Switches Template section in the top right, click the **+** symbol.

Step 11 On the Add Template popup in the Basic Info section, implement the following settings, and then click **Next**.

- **Template Name:** *AOS-CX-Stack*
- **Device Type:** *Aruba CX*
- **Model:** *6300*
- **Part Name:** *(ALL)*
- **Version:** *10.06*



Step 12 In the Edit Template section, paste the access configuration in the box, and then click **SAVE**.



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

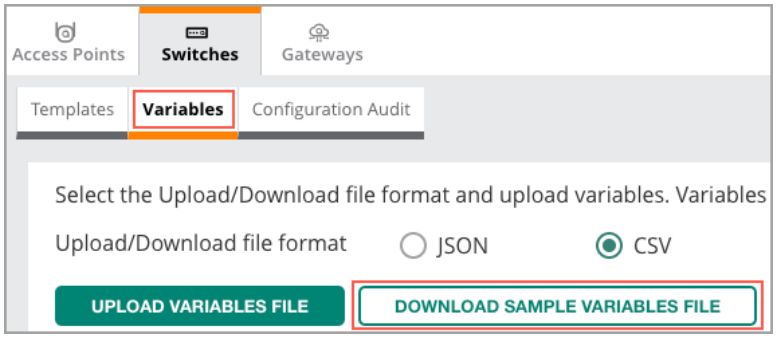
Example: Access Switch Template

Access Switch Template

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, and then click **DOWNLOAD SAMPLE VARIABLES FILES**.

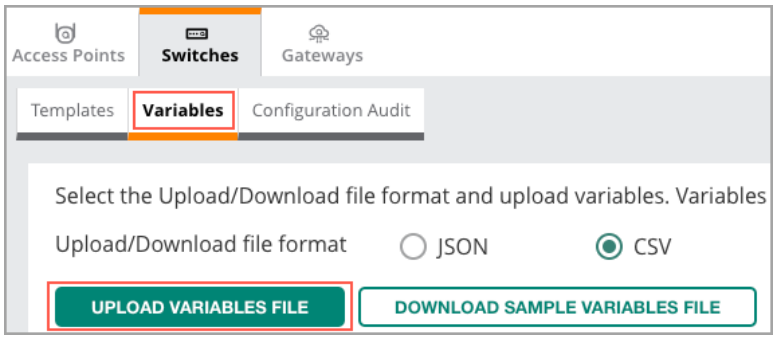


Step 2 Open the CSV file in your favorite editor, enter the proper value for each variable, and then **Save** the file to your computer.

_sys_serial	_sys_lan_mac	modified	_sys_hostname	IP_MGMT	MGMT_IP_GW	MGMT_VLAN_IP	_ip_default_route
SG07KMZ079	64:e8:81:c1:c4:00	y	6300M-AG2-AC1	172.16.10.13	172.16.10.1	10.1.15.13	10.1.15.1

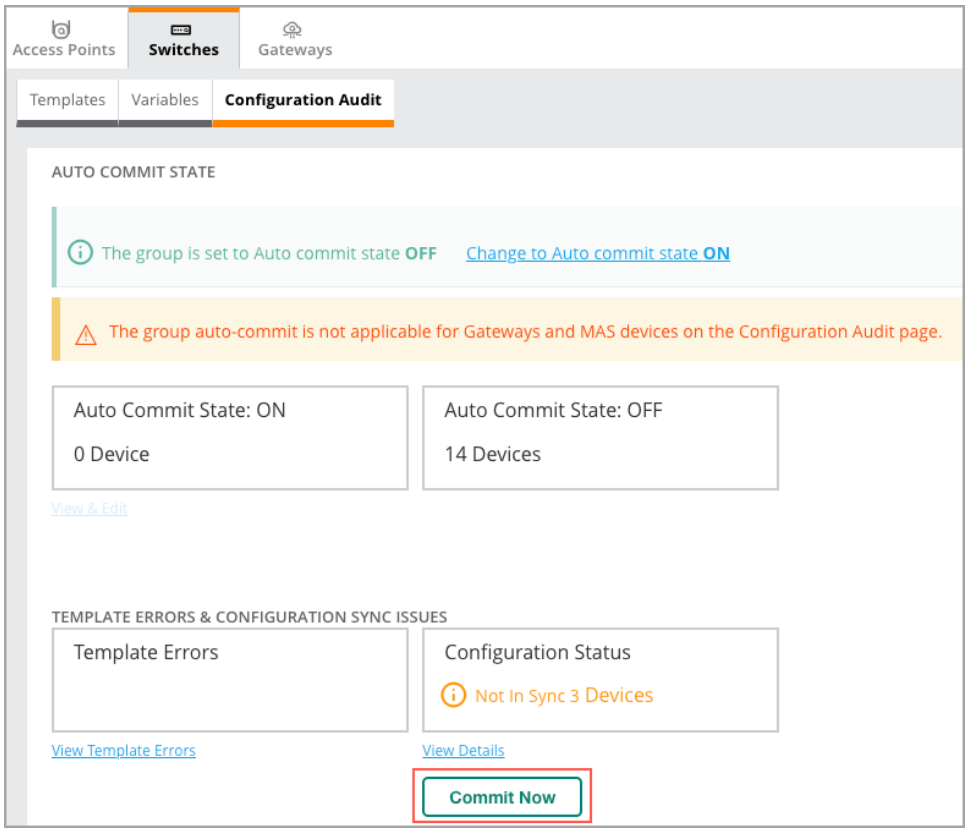
NOTE:
Change the **modified** column to **Y** for each device.

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

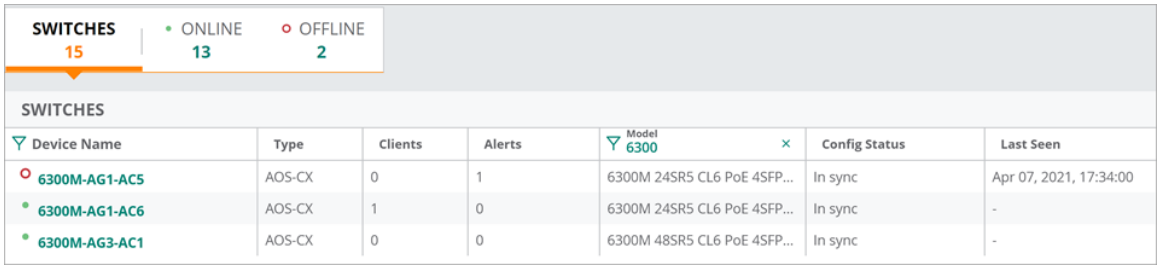


NOTE:
If the group is set to Auto Commit State: Off, the variables will not be pushed to the devices.

Step 4 If the group is set to auto commit off and you want to commit the changes immediately, navigate to **Devices > Switches > Config > Configuration Audit**, and then select **Commit Now**. If auto commit is on, skip this step.



Step 5 Navigate to **Devices > Switches > List** and verify the Switches are **In sync**.



Step 6 Repeat the two previous procedures for each access group.

Campus Wireless Connectivity

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

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

Configuring Group Settings for Wireless

Aruba Central uses a two-level hierarchy for configuration tasks. A device's final configuration is a result of configuration that is applied at the group level, along with configuration that is applied at a device level. Parameters added at the device level override the configuration performed at the group level. Aruba recommends performing the bulk of the configuration at the group level and only using device-level configurations when specific overrides are needed.

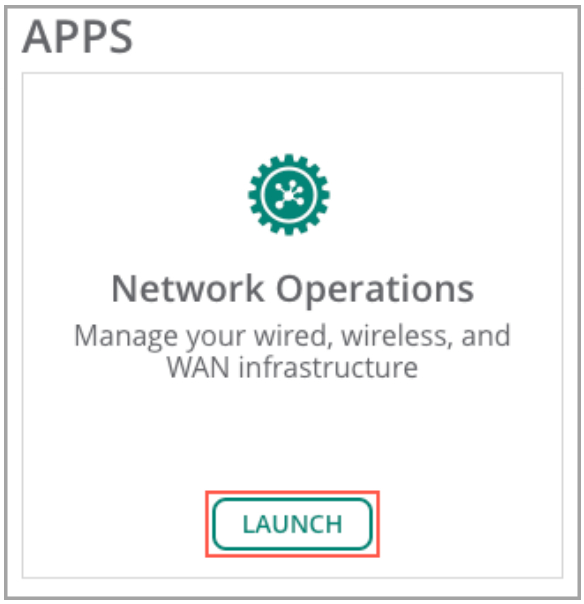
Configure AP Group Settings

Use this procedure to configure group settings for APs. An AP Group guarantees common settings are consistently applied across a group of APs in the network.

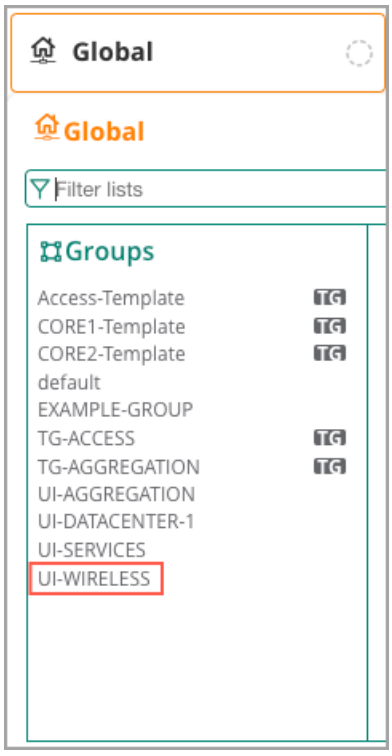
NOTE:
The best practice is to use the fewest groups necessary to provide logical organization for the network and consistent configuration between devices. Configuration cannot be shared between groups.

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

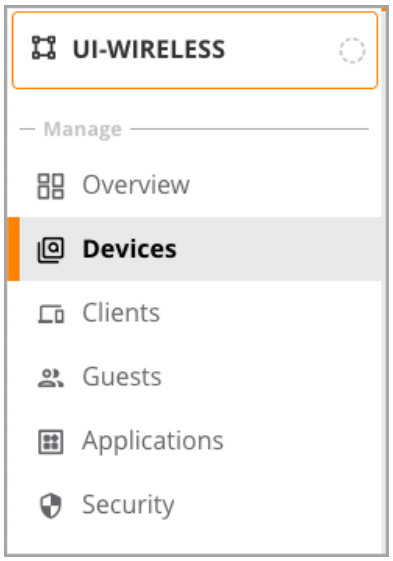
Step 2 On the Aruba Central Account Home page, launch the **Network Operations** app.



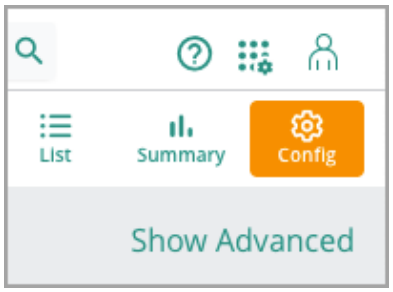
Step 3 In the filter drop-down list, select an AOS10 Group name. In this example, select **UI-WIRELESS**.



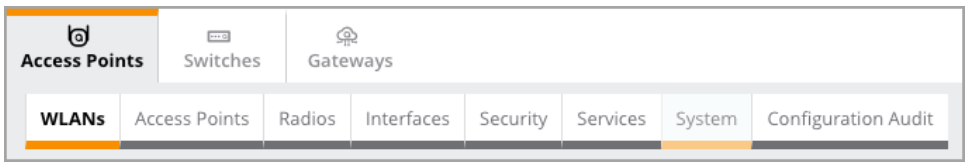
Step 4 From the left menu, select **Devices**.



Step 5 In the upper right of the Access Points page, select **Config**, and then select **Show Advanced**.

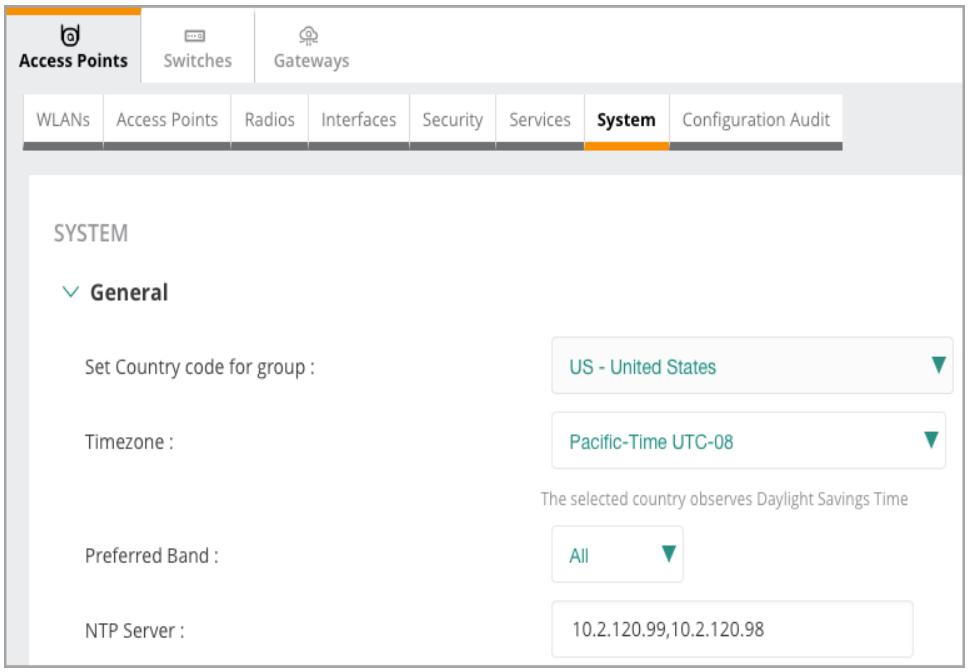


Step 6 On the Access Points page, select the **System** tab.



Step 7 On the System tab, implement the following settings, and then select **Save Settings**.

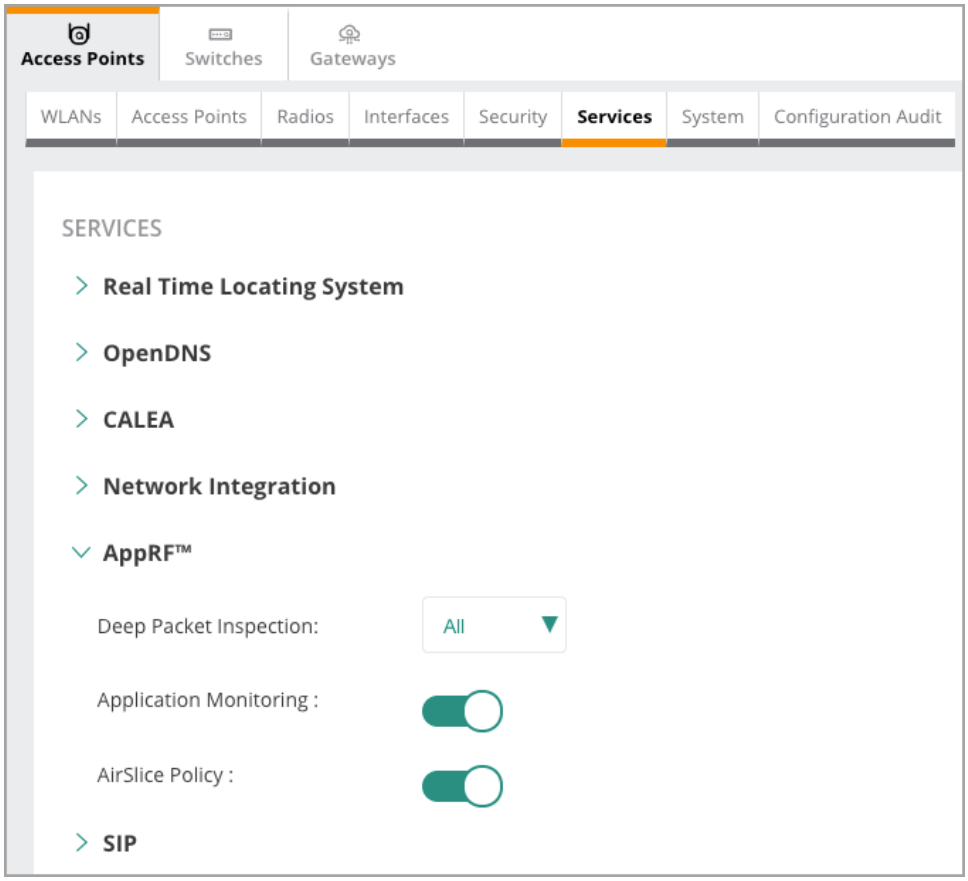
- **Set Country code for group:** *US - United States*
- **Timezone:** *Pacific-Time UTC-08*
- **Preferred Band:** *All*
- **NTP Server:** 10.2.120.99, 10.2.120.98



CAUTION:
Incorrect time synchronization within the network can lead to authentication errors.
NOTES:
All APs in the group must have the same country code, so you must create a group for each country code in the network. The country code must be set before a configuration is pushed to an AP.
An NTP server defined in the Group configuration takes precedence over NTP configured with DHCP.

Step 8 On the Access Points page, select the **Services** tab, expand the **AppRF** section, implement the following settings, and then select **Save Settings**.

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



NOTES:
Aruba AppRF is an application aware firewall running within the APs providing application visibility and control capabilities. APs with Deep Packet Inspection (DPI) enabled can inspect the data payload within packets to identify applications in use. DPI also allows the creation of rules to determine client access to applications and websites, as well as traffic shaping policies. For a complete overview of Aruba AppRF, refer to the appropriate version ArubaOS User Guide.
Occasionally Central features are released under Select Availability. If a documented feature does not appear in the Central application, contact an Aruba SE or Aruba TAC to request feature access.

Configure Gateway Group Settings

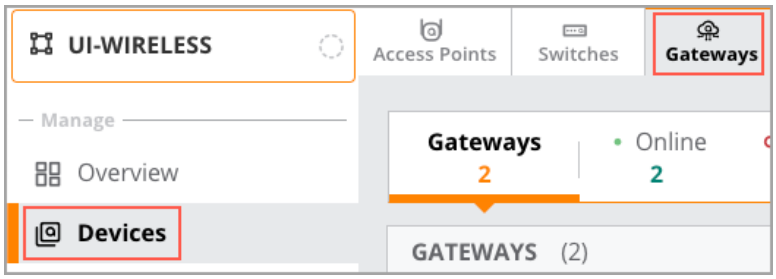
Use this procedure to configure group settings for Gateways. The best practice is to put APs and Gateways in the same group in order to simplify navigation between the two settings tabs when deploying the network.

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

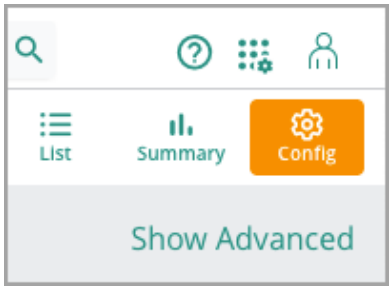
Step 2 On the Aruba Central Account Home page, launch the **Network Operations** app.

Step 3 In the filter drop-down list, select an AOS10 **Group** name.

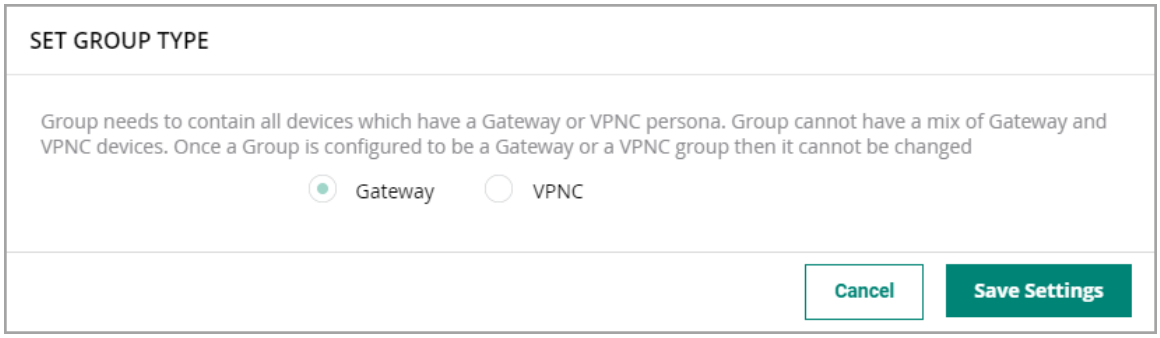
Step 4 From the left menu, select **Devices**, and then at the top, select **Gateways**.



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



Step 6 If this is the first time using the AOS10 group to configure a Gateway, the Set Group Type popup will appear. Select **Gateway** and click **Save Settings**.

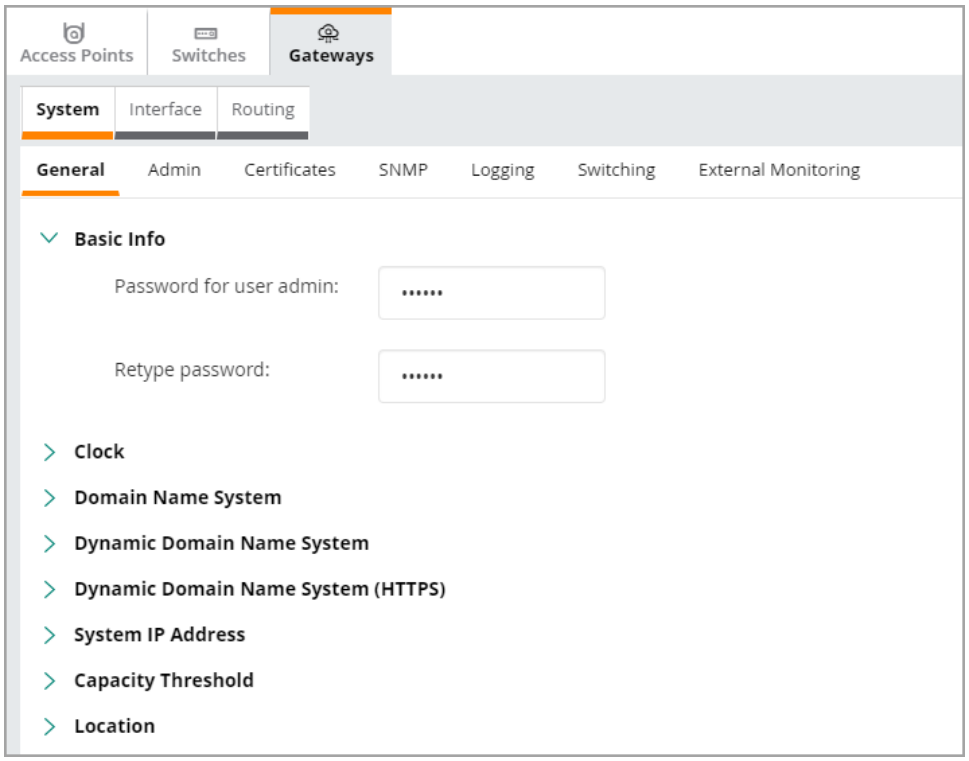


CAUTION:
If *Branch Gateway* is the only "Gateway" option, go back to the **Global > Organization > Groups** configuration page and convert the group to AOS10 before returning here to set the group type to Gateway. Do not select Branch Gateway or VPNC as they are only used for SD-Branch deployments and once the group type is set, it cannot be changed.

Step 7 Select the **System** tab and then the **General** tab.

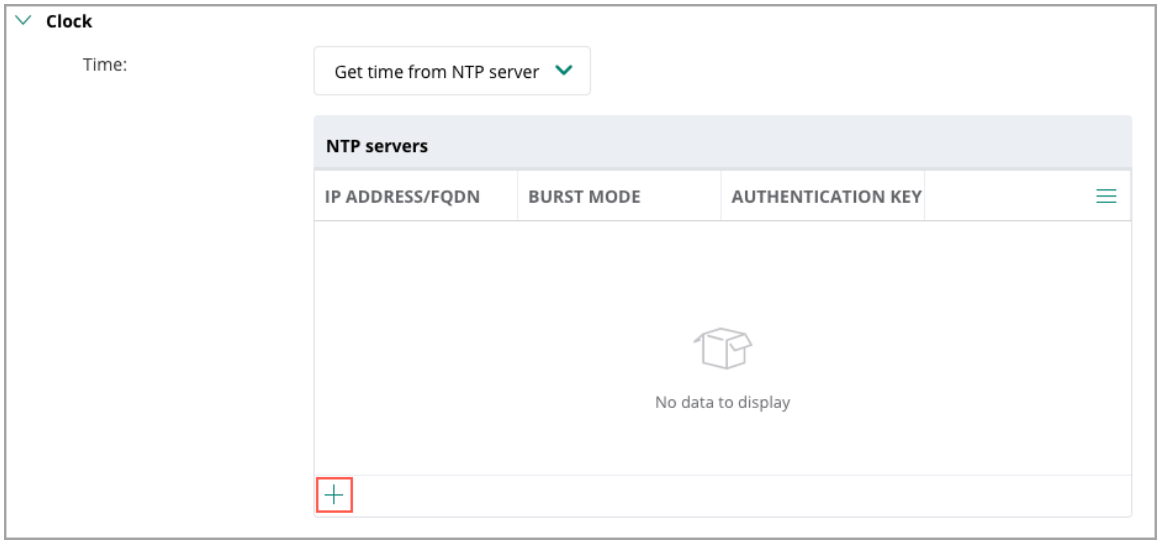
Step 8 In the **Basic Info** section, implement the following settings, and the click **Save Settings**.

- **Password for user admin:** *password*
- **Retype password:** *password*



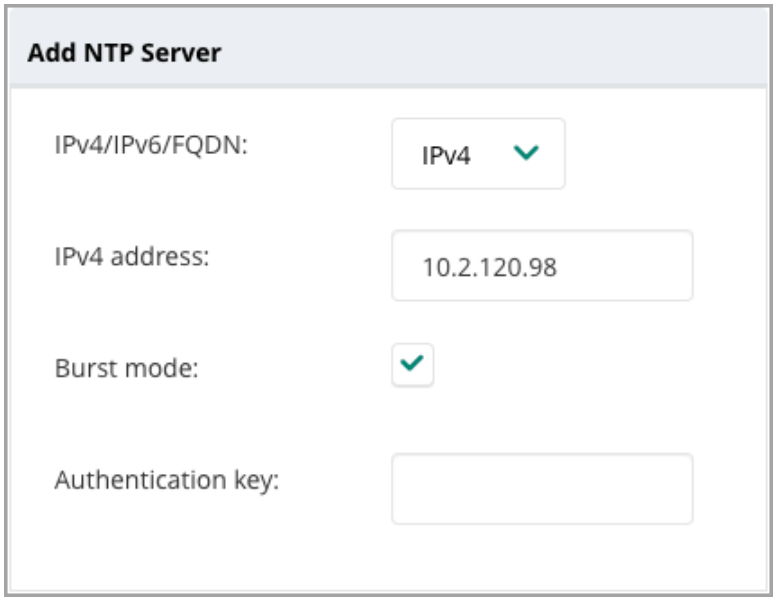
NOTE:
Configuration changes are not applied to a device until it has a System IP Address. This will be added later at the device level.

Step 9 Expand the **Clock** section and in the lower left corner of the **NTP servers** table, select the **+** sign.



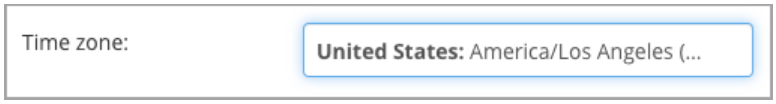
Step 10 On the **Add NTP Server** page, implement the following settings, and then click **Save Settings**.

- **IPv4/IPv6/FQDN:** *IPv4*
- **IPv4 address:** *10.2.120.98*
- **Burst mode:** *checkmark*



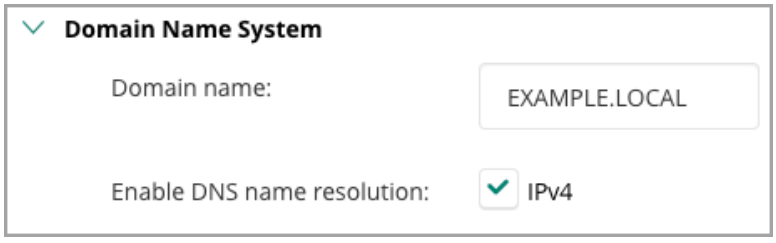
Step 11 Repeat the two previous steps to enter additional NTP servers.

Step 12 In the Clock section at the bottom, click **Choose a timezone**, select the timezone from the drop-down list, and then click **Save Settings**.

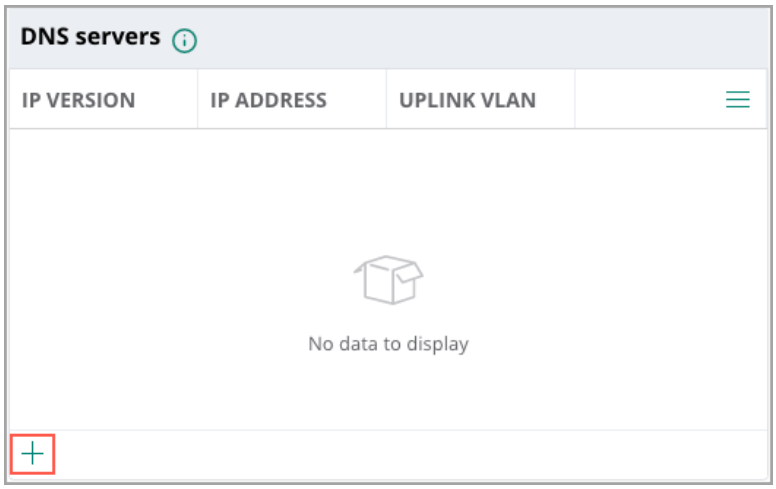


Step 13 Expand the **Domain Name System** section, implement the following settings, and then click **Save Settings**

- **Domain name:** *Example.Local*
- **Enable DNS name resolution:** *checkmark IPv4*

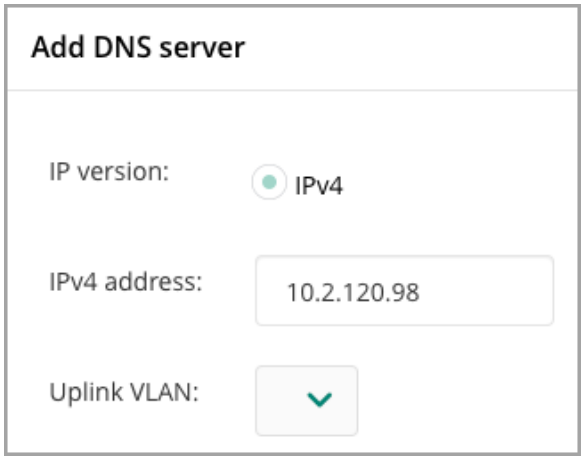


Step 14 In the lower left corner of the **DNS servers** table, select the **+** sign.



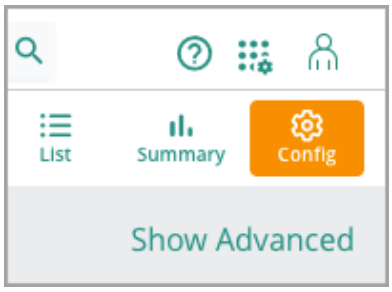
Step 15 On the Add DNS server page, implement the following setting, and then click **Save Settings**.

- **IPv4 address:** *10.2.120.98*



Step 16 Repeat the two previous steps to enter additional **DNS servers**.

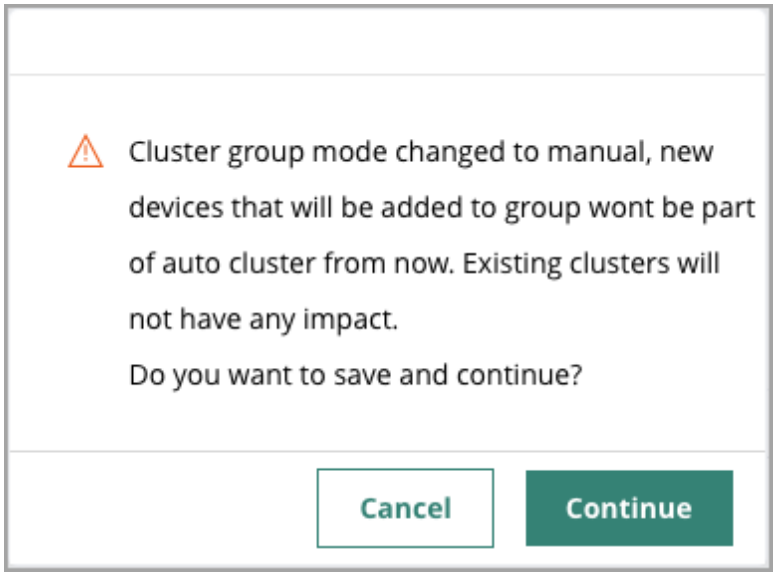
Step 17 In the upper right of the Gateways page, select **Show Advanced**.



Step 18 On the Gateways page, select the **High Availability** tab.

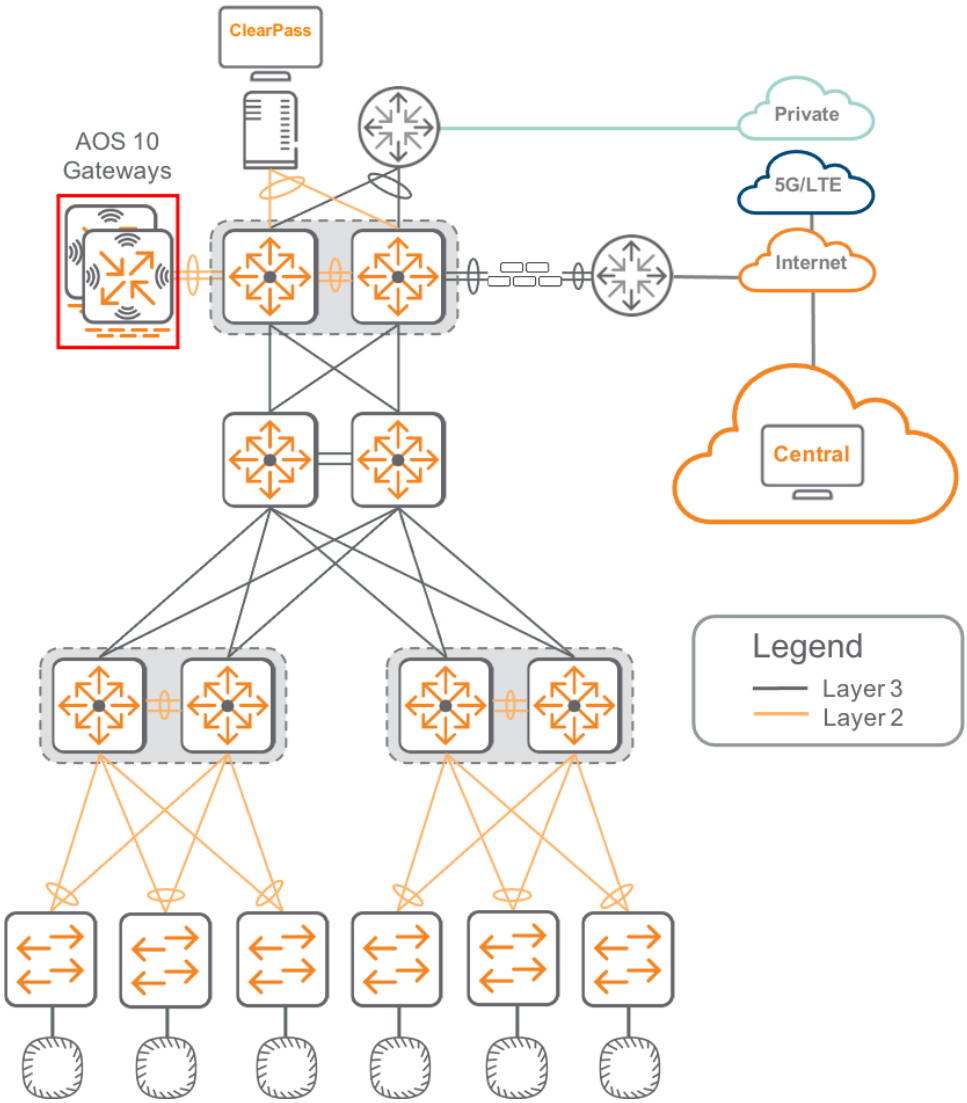
Step 19 In the Cluster mode section, disable **Automatic** clustering by moving the slider to the left.

Step 20 On the Cluster group mode popup, select **Continue**.



Configuring Gateway Devices

The ESP Campus for large networks includes a gateway cluster in the services aggregation layer. In this design, WLANs are tunneled to the gateways to take advantage of advanced policy enforcement and firewall capabilities available on that platform. Gateway clustering is implemented to ensure high availability and throughput.



This section describes how to deploy a gateway using Aruba Central and the Zero Touch Provisioning (ZTP) process. The information from the following table includes the VLANs and IP addresses used in the procedures below.

Example: IP addresses and VLAN ID

Name	IP address	Default gateway	VLAN ID	VLAN name	Gateway VRRP Address
7210-1	10.6.15.11/24	10.6.15.1	15	MGMT	10.6.15.13
7210-2	10.6.15.12/24	10.6.15.1	15	MGMT	10.6.15.14

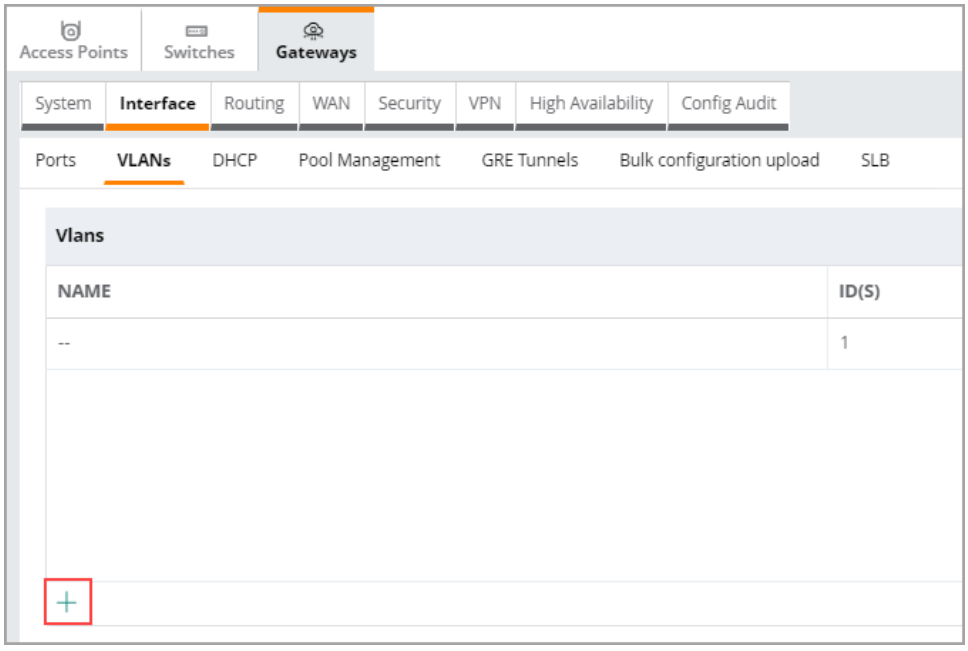
Configure Gateway VLANs

Use the following procedure to configure Gateway VLANs.

Example: VLANs for Gateways

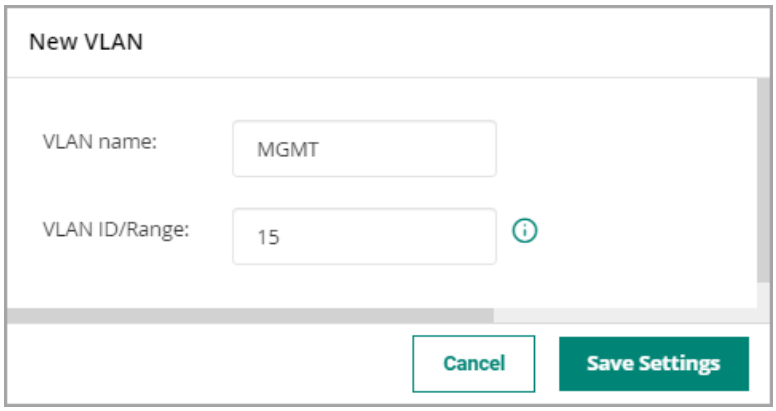
VLAN Name	VLAN ID
MGMT	15
EMPLOYEE	103
BLDG-MGMT	104
CAMERA	105
PRINTER	106
VISITOR	112
REJECT_AUTH	113
CRITICAL_AUTH	114
ZTP	4094
CAUTION:	
The Gateway VLANs need to be created prior to adding the port channels, so the Native VLAN and Allowed VLANs can be selected from the pull-down lists.	

Step 1 On the Gateways tab, select the **Interface** tab, select **VLANs** and then in the lower left, click the **+** sign.



Step 2 On the New VLAN popup, implement the following settings, and then select **Save Settings**.

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



NOTE:
Named VLANs facilitate policy consistency between sites.

Step 3 Repeat this procedure for each Gateway VLAN in the environment.

Enable Physical Interfaces

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

The ESP Campus supports zero-touch provisioning (ZTP) of Gateway devices. ZTP requires physical interface configuration to be performed for Gateways at the Group level. To simplify this configuration, the best practice is to standardize on a single Gateway model within each Group.

CAUTION:
If a Group level interface configuration is applied to a Gateway that does not have the specified physical interface, the Gateway will not be added to the Group. The unsupported interface will need to be removed from the Group configuration, if the Gateway must be added.

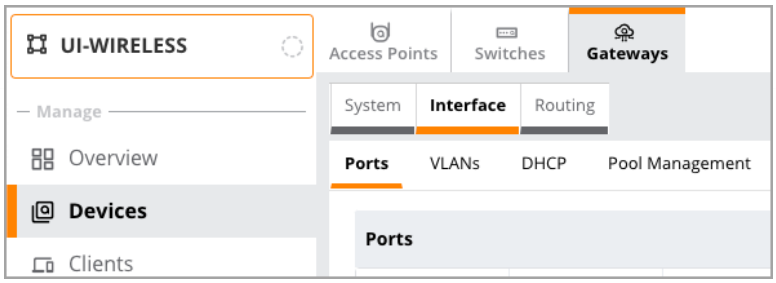
Step 1 Navigate to **Central** and login using administrator credentials.

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

Step 3 In the filter drop-down list, select an AOS10 **Group** name.

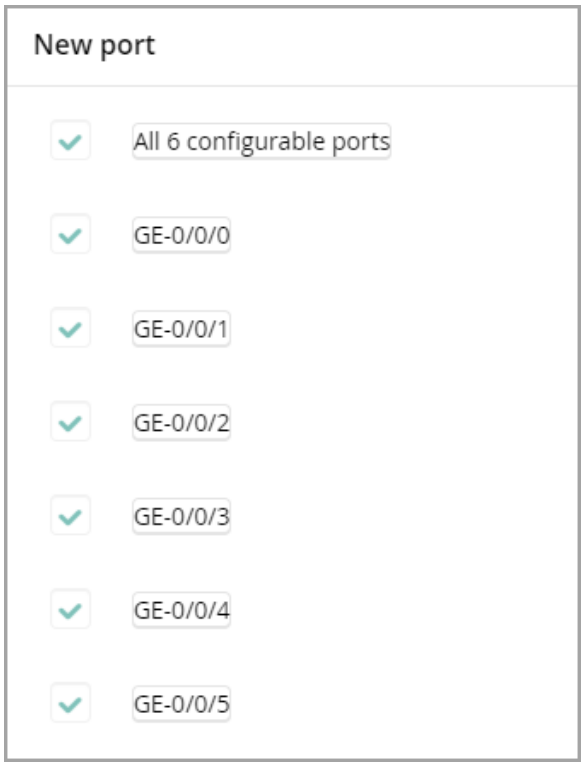
Step 4 From the left menu, select the **Devices** tab, select the **Gateways** tab and in the upper right, select **Config**.

Step 5 On the Gateways page, select the **Interface** tab, and then the **Ports** tab.



Step 6 At the bottom of the Ports table, click the **+** sign.

Step 7 On the New Port popup, select the checkbox next to the interface name, and then click **Save Settings**.



Configure Port Channels

Use the following procedure to configure Gateway port channels.

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

When a Gateway is deployed using ZTP it does not have an LACP configuration initially. To accommodate this during the provisioning process, LACP Fallback is enabled on the Switch. An example configuration for VSX MC-LAG is below:

```
interface lag 11 multi-chassis
    description 7210-1
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
    lacp fallback
!
interface lag 12 multi-chassis
    description 7210-2
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
    lacp fallback
```

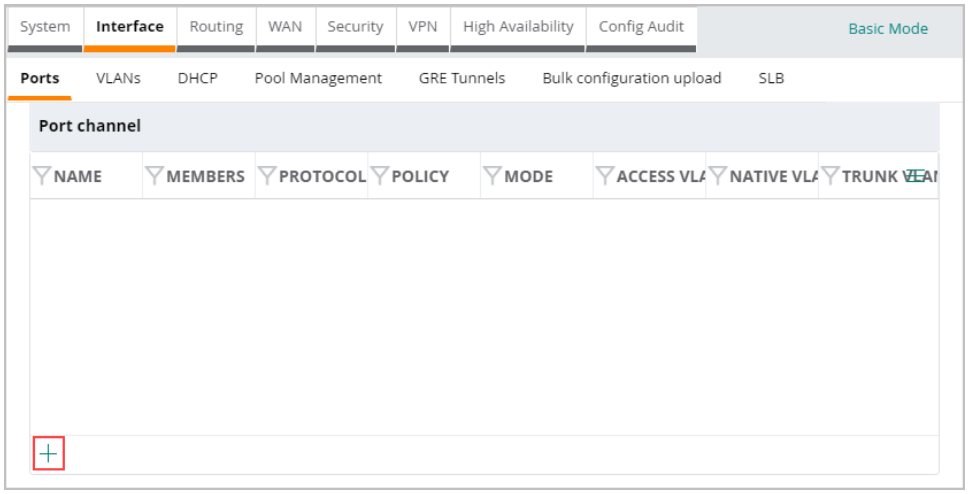
NOTES:
When LACP negotiation fails, LACP Fallback allows switch ports to function as standard access/trunk ports until LACP functions.
The above configuration snippet illustrates implementation of the LACP Fallback command in context. Refer to earlier sections of this guide for complete switch configuration.

Step 1 In the filter drop-down list, select an AOS10 **Group** name.

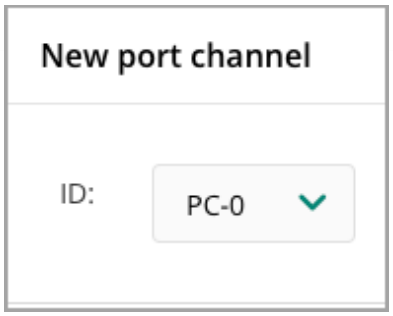
Step 2 From the left menu, select the **Devices** tab, select the **Gateways** tab and in the upper right, select **Config**.

Step 4 On the Gateways page, select the **Interface** tab, and then the **Ports** tab.

Step 5 From the Port Channel section, click the **+** sign.

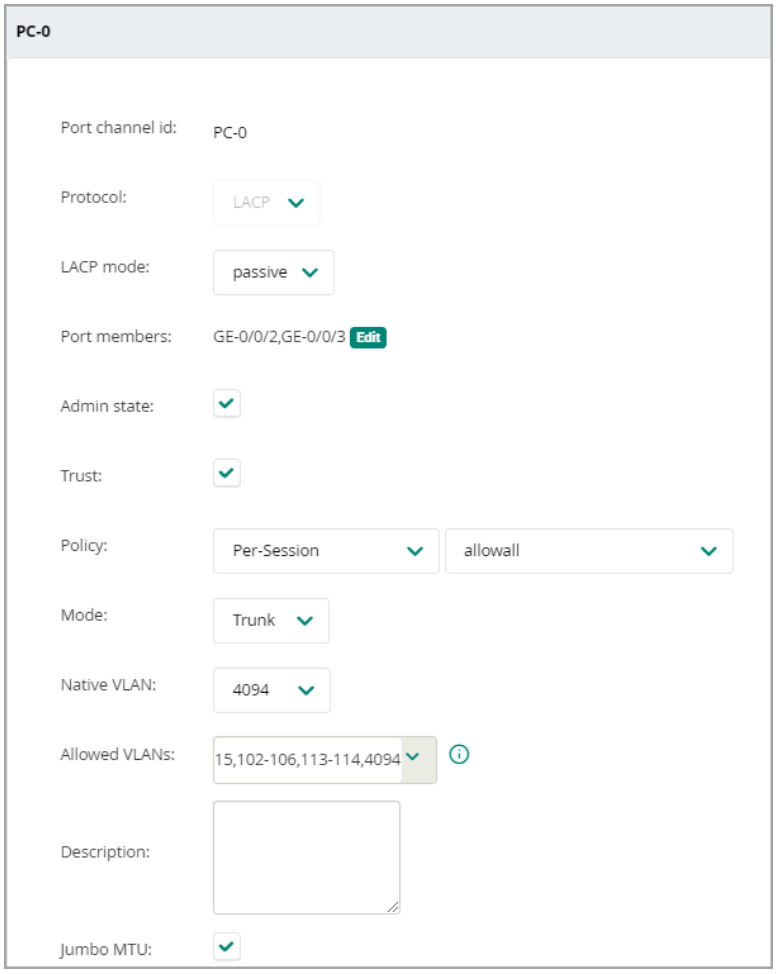


Step 5 On the New port channel popup, select the next available PC-*n* ID; in this example **PC-0**. Then click **Save Settings**.



Step 6 In the PC-*n* section, implement the following settings.

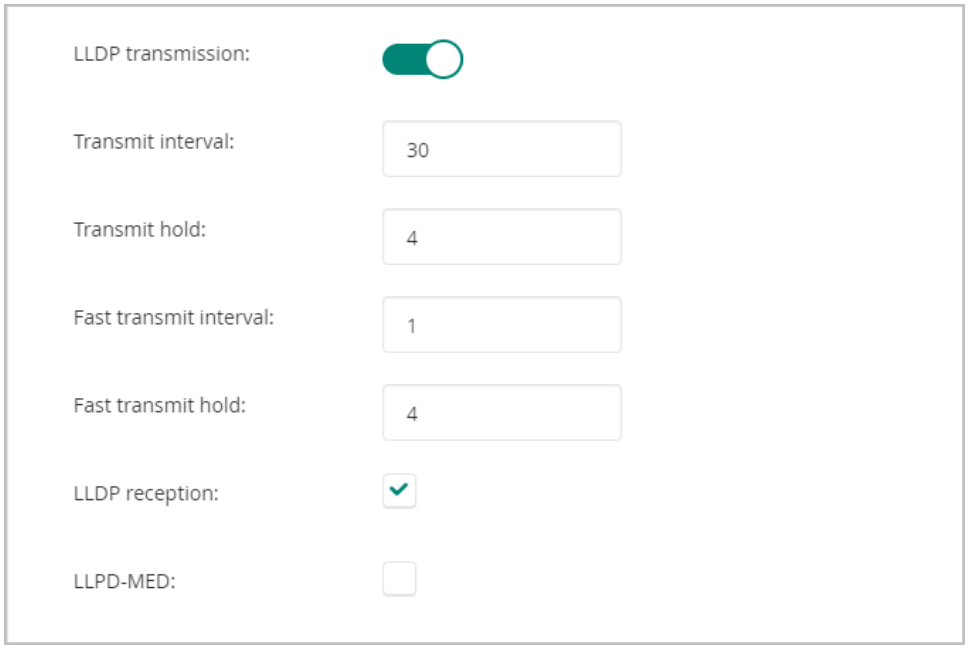
- **Protocol**: *LACP*
- **LACP Mode:** *Passive*
- **Port Members:** Click **Edit**, select port channel ports under **Available**, use the right arrow to move them to **Selected**, and then click **OK**.
- **Admin State:** *checkmark*
- **Trust:** *checkmark*
- **Policy:** *Leave empty*
- **Mode:** *Trunk*
- **Native VLAN:** *4094*
- **Allowed VLANS:** *15, 102-106,112-114,4094*
- **Jumbo MTU:** *checkmark*



NOTE:
The Allowed VLANs are a drop-down menu choice from the Gateway VLANs created in the Configure VLAN Interfaces procedure.

Step 7 At the bottom of the page, expand **Show advanced options**, implement the following settings, and then click **Save Settings**.

- **LLDP Transmission:** *Slide to right*
- **LLDP Reception:** *checkmark*



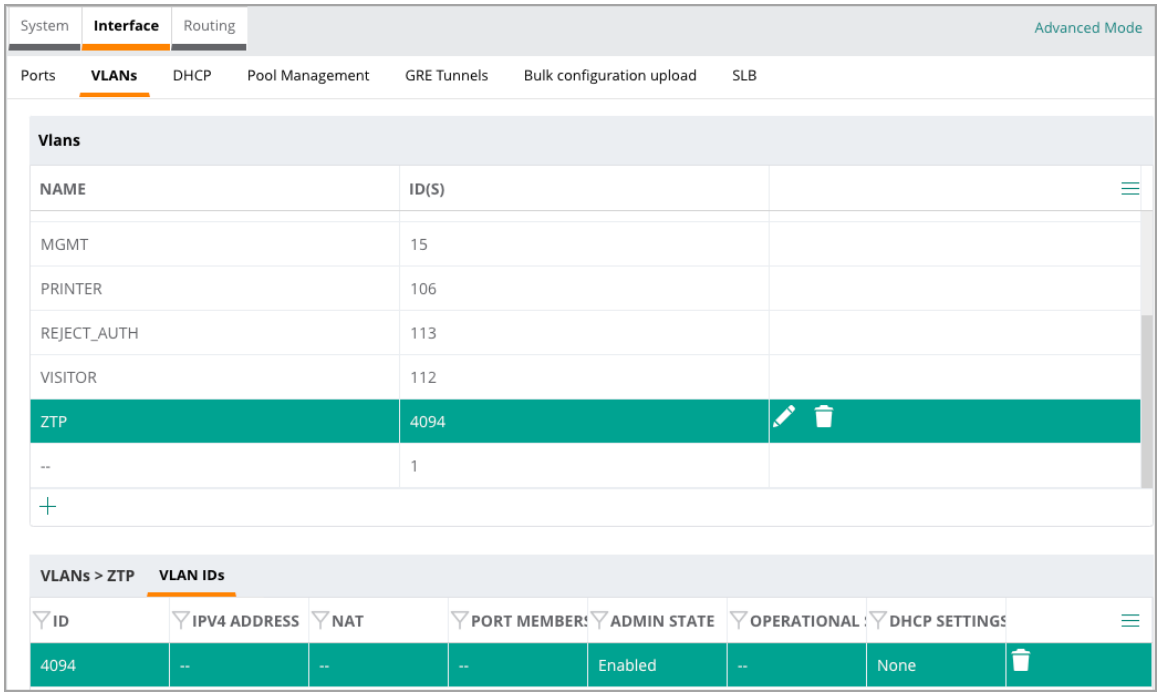
Configure the ZTP VLAN

Use the following procedure to disable VLAN 4094 on the Gateway physical interfaces.

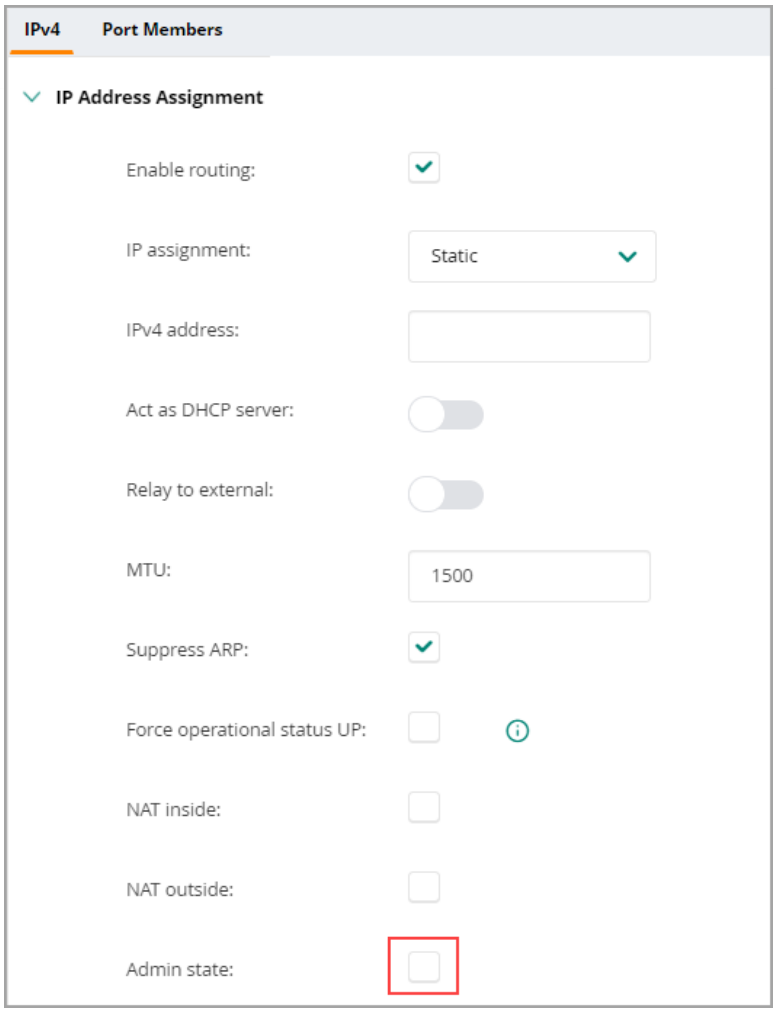
The Gateway has a factory configured native VLAN ID of 4094 on the interface used for making an initial connection to Central. However, a Gateway will not sync with Central until a system IP is assigned. This behavior allows for the configuration push which disables VLAN 4094 when the Gateway is assigned a system IP address.

Step 1 On the **Gateways** page, select the **Interface** tab, and then select the **VLANs** tab.

Step 2 Scroll down, select the row for **4094**, and then in the lower VLAN IDs section, click the **VLAN** row.



Step 3 On the IPv4 page, deselect the **Admin state:** check box, and then click **Save Settings**.



Configure the Default Gateway

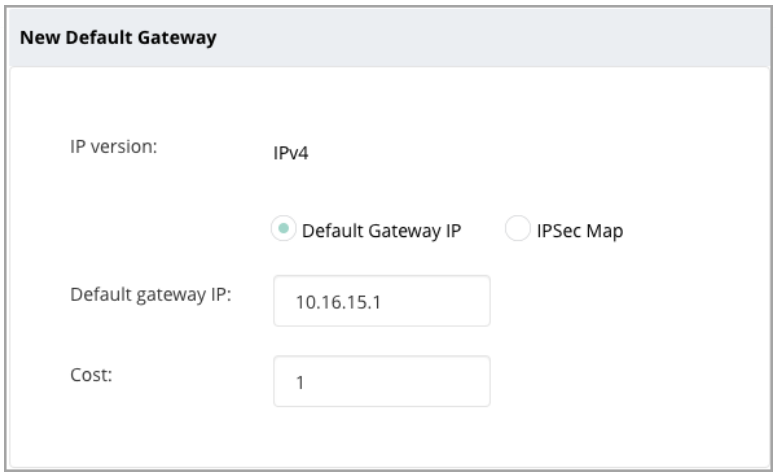
Use the following procedure to configure a default gateway on the Gateway device.

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

Step 2 Expand the **Static Default Gateway** section, and then at the bottom of the table, click the **+** sign.

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

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



Configure the Gateway Base Features

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

NOTE:
In the Aruba ESP Campus design, most Gateway configuration is entered at the Group level. An attempt to change a device property which is overridden at the Group level will be indicated in the Audit Trail.

Step 1 In the filter drop-down list, select an AOS10 **Group** name.

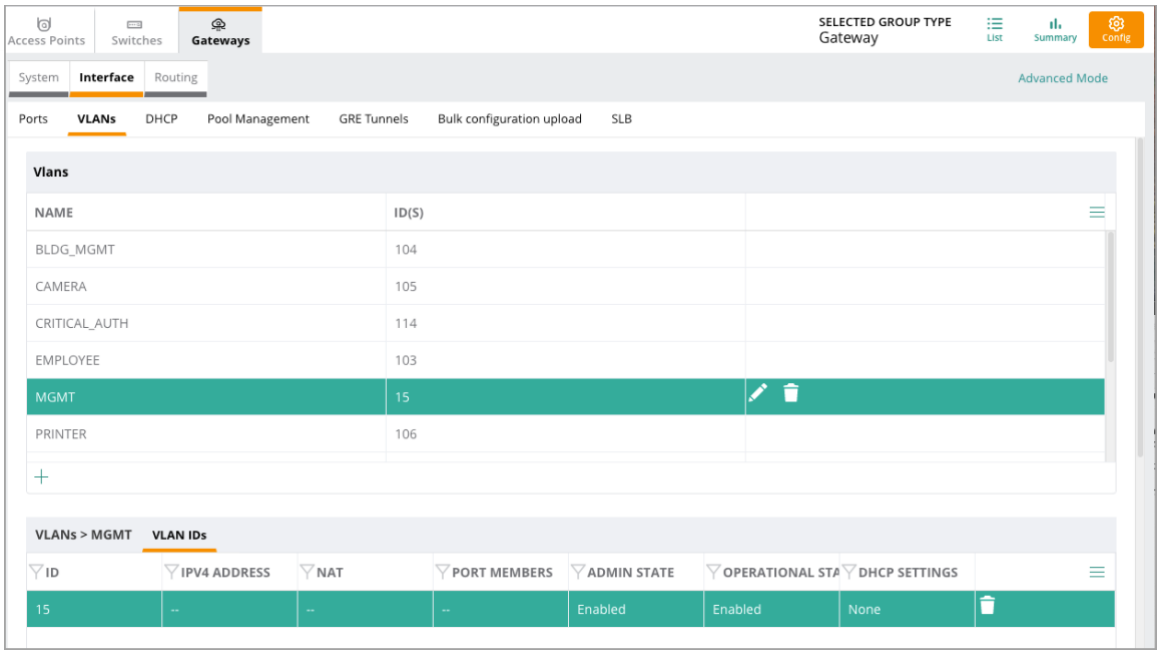
Step 2 From the left menu, select **Devices**, on the tab menu bar and then select **Gateways**.

Step 3 Select a new Gateway from the list.

NOTE:
An unnamed Gateway is listed with the system MAC address.

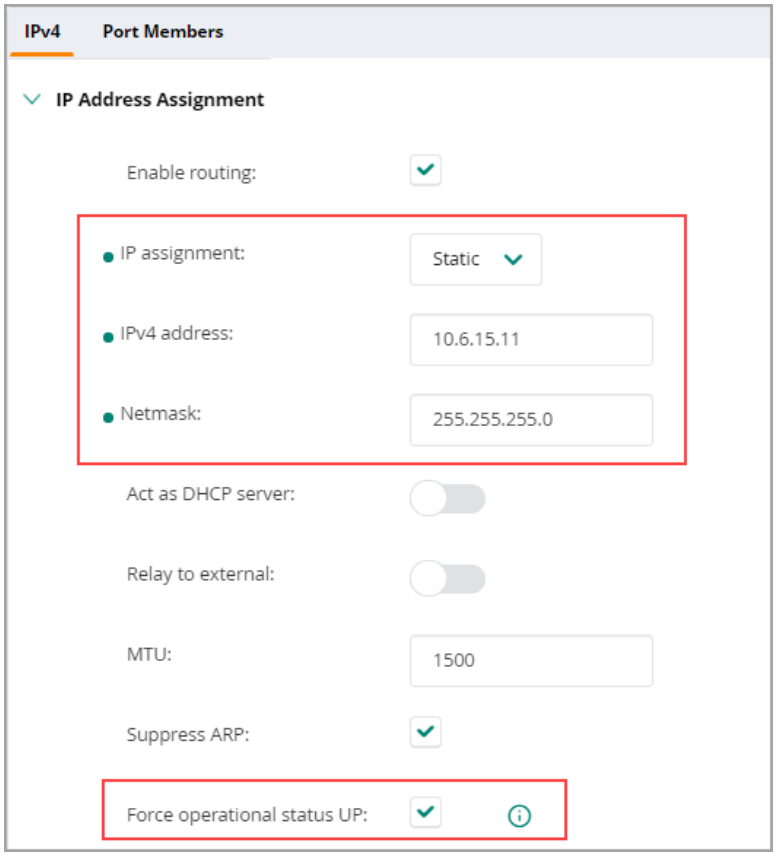
Step 4 From the left menu, select **Device**, select the **Interface** tab, and then the **VLANs** tab.

Step 5 On the VLANs table, select the **MGMT** VLAN, and then in the lower VLAN IDs section, click the **VLAN** row.



Step 6 Scroll down to the IP Address Assignment section, implement the following settings, and then click **Save Settings**:

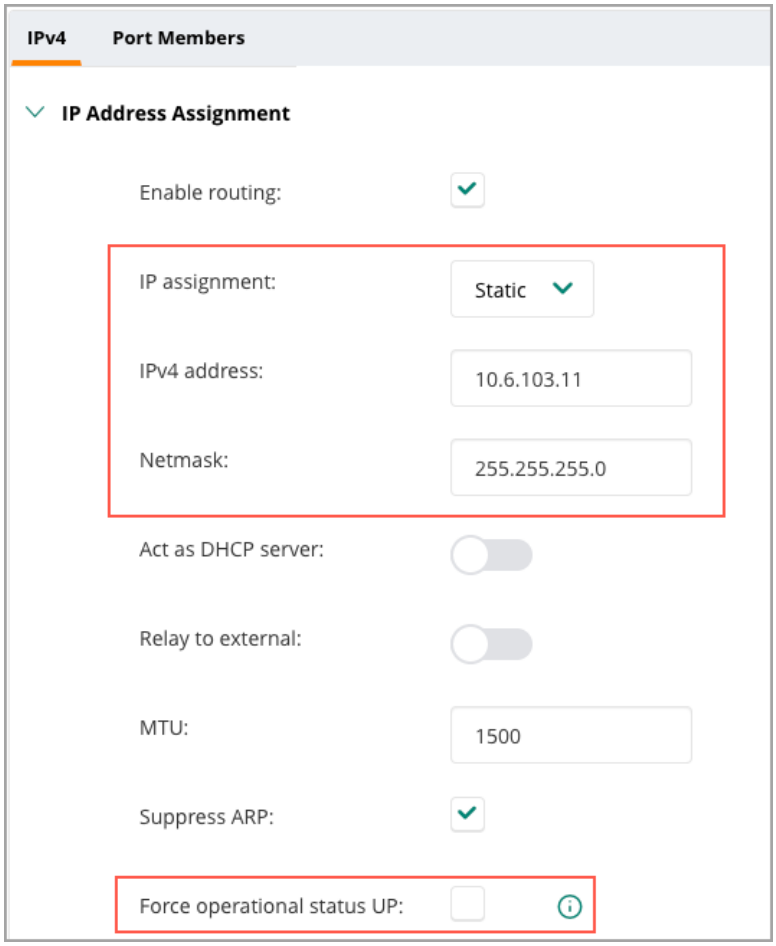
- **IP Assignment:** *Static*
- **IPv4 Address:** *10.6.15.11*
- **Netmask:** *255.255.255.0*
- **Force operational status UP:** *checkmark*



Step 7 On the Vlans table, select a different VLAN, and then in the lower VLAN IDs section, click the **VLAN** row.

Step 8 Scroll down to the IP Address Assignment section, implement the following settings, and then click **Save**:

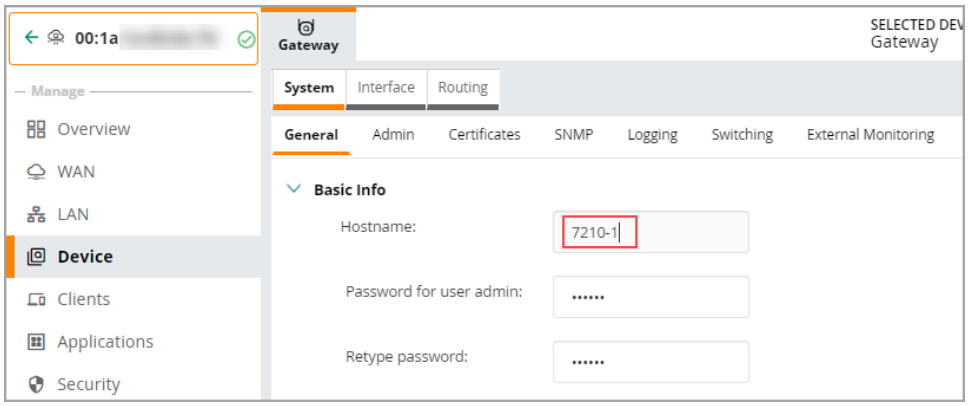
- **IP Assignment:** *Static*
- **IPv4 Address:** *10.6.103.11*
- **Netmask:** *255.255.255.0*
- **Force operational status UP:** *unchecked*



Step 9 Repeat the previous two steps for each additional VLAN in the environment.

Step 10 On the Gateway page, select the **System** tab, and then the **General** tab.

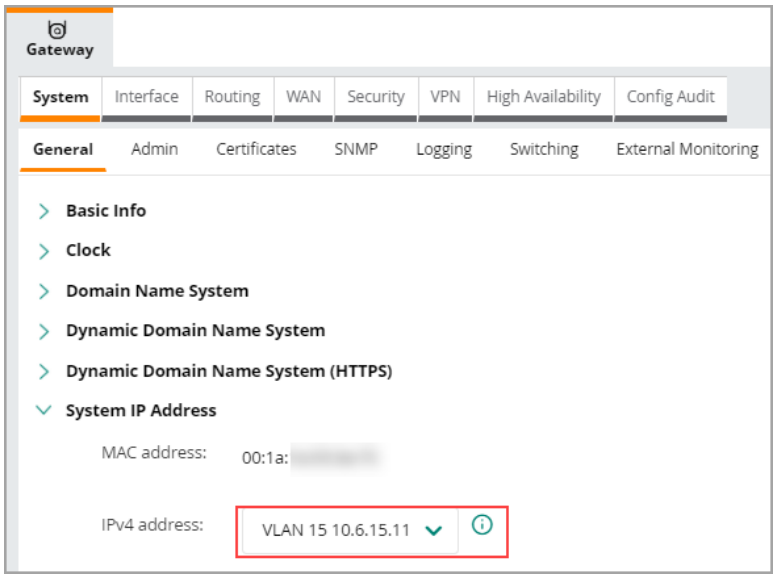
Step 11 In the Basic Info section, enter the **Hostname**, and then click **Save Settings**.



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

Step 12 Expand the System IP Address section, use the **IPv4 address** drop down menu to select the VLAN with the Force operational UP setting, and then click **Save**.

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



NOTE:
The Gateway will reboot and download its configuration once the System IP address is set. This may take some time and may require multiple reboots for all the configuration to be pushed. A status of what is happening can be found in the audit log. Once the configuration has been successfully pushed the Gateway will show a status of in-sync on the device summary page.

Step 13 Repeat this procedure for each new Gateway in the environment.

Configure Layer 2 Gateway Clustering

Use this procedure to configure Layer 2 Gateway clustering.

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

NOTE:
VRRP Addresses on Gateway cluster members are required for COA to work correctly. However, automatic cluster creation does not support COA.

Example: Gateway VRRP IP addresses and VLANs

Gateway	IP address	Multicast VLAN	VRRP IP address	VRRP VLAN
7210-1	10.6.15.11	15	10.6.15.13	15
7210-2	10.6.15.12	15	10.6.15.14	15

Step 1 In the filter drop-down list, select an AOS10 **Group** name.

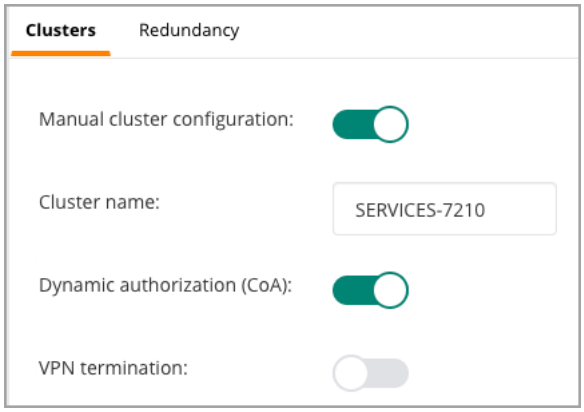
Step 2 From the left menu, select **Devices**, select the **Gateways** tab, and then in the top right, click **Config**.

Step 3 In the top right, select **Advanced Mode**, and then select the **High Availability** tab.

Step 4 Confirm the Cluster mode **Automatic** slider is to the left.

Step 5 At the bottom of the Clusters table, click the **+** sign and implement the following settings.

- **Manual cluster configuration:** *Slide to right*
- **Cluster name:** *SERVICES-7210*
- **Dynamic Authorization (COA):** *Slide to right*



Step 6 At the bottom of the **Gateways in Cluster** table, click the **+** sign and implement the following settings.

- **Gateway:** *7210-1*
- **VRRP IP:** *10.6.15.13*

Step 7 Click the **+** sign again and implement the following settings.

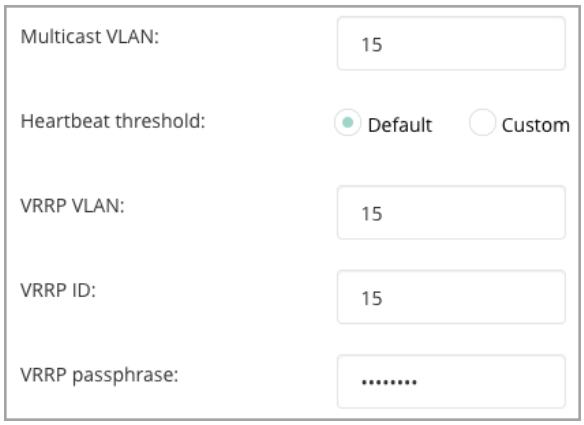
- **Gateway:** *7210-2*
- **VRRP IP:** *10.6.15.14*

Gateways in UI-WIRELESS Cluster

GATEWAY	VRRP IP
7210-2	10.6.15.14
7210-1	10.6.15.13

Step 8 Scroll down, implement the following settings, and then click **Save Settings**.

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



NOTE:
Cluster operations are disruptive to client traffic and should be done during a maintenance window.

Configuring Wireless Access

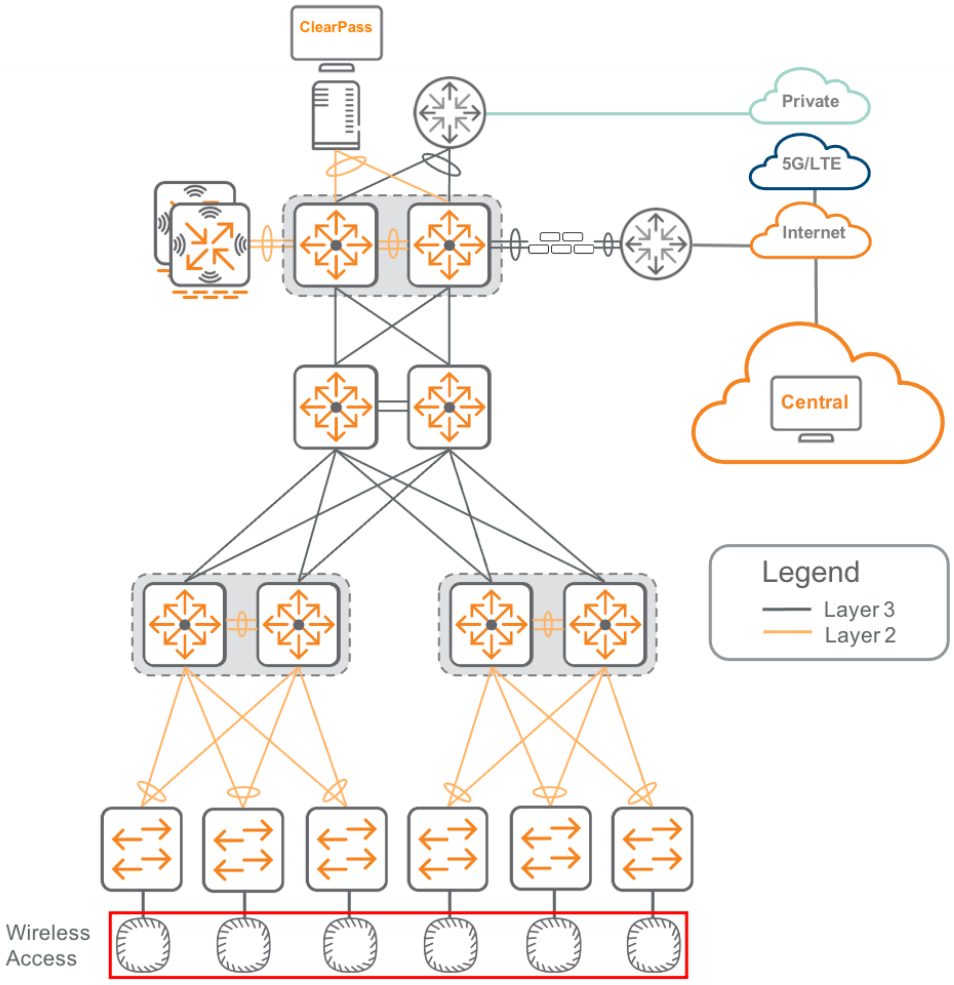
The primary function of the wireless access layer is to provide network connectivity anywhere on the campus for wireless devices. Wireless access must be secure, available, fault tolerant, and reliable to meet the demands of today's users.

To satisfy the requirements for wireless access in a variety of network designs, the Aruba ESP Campus supports two modes of switching traffic between wireless and wired networks. In bridged mode, the AP converts the 802.11 frame to an 802.3 Ethernet frame. In tunneled mode, the AP encapsulates the 802.11 frame in a GRE packet and tunnels the traffic to a Gateway device for decapsulation, additional inspection, and, if permitted, switching onto the correct VLAN.

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

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

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



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

Example: AP Access VLANs

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

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

Example: RADIUS servers

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

Configure the WPA3-Enterprise Wireless LAN

Use this procedure to configure a WPA3-Enterprise SSID.

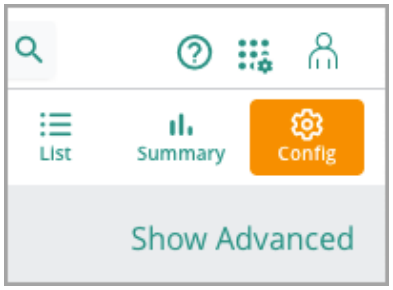
WPA3-Enterprise enables authentication using passwords or certificates to identify users and devices before they are granted access to the network. The wireless client authenticates against a RADIUS server using an EAP-TLS exchange, and the AP acts as a relay. Both the client and the RADIUS server use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

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

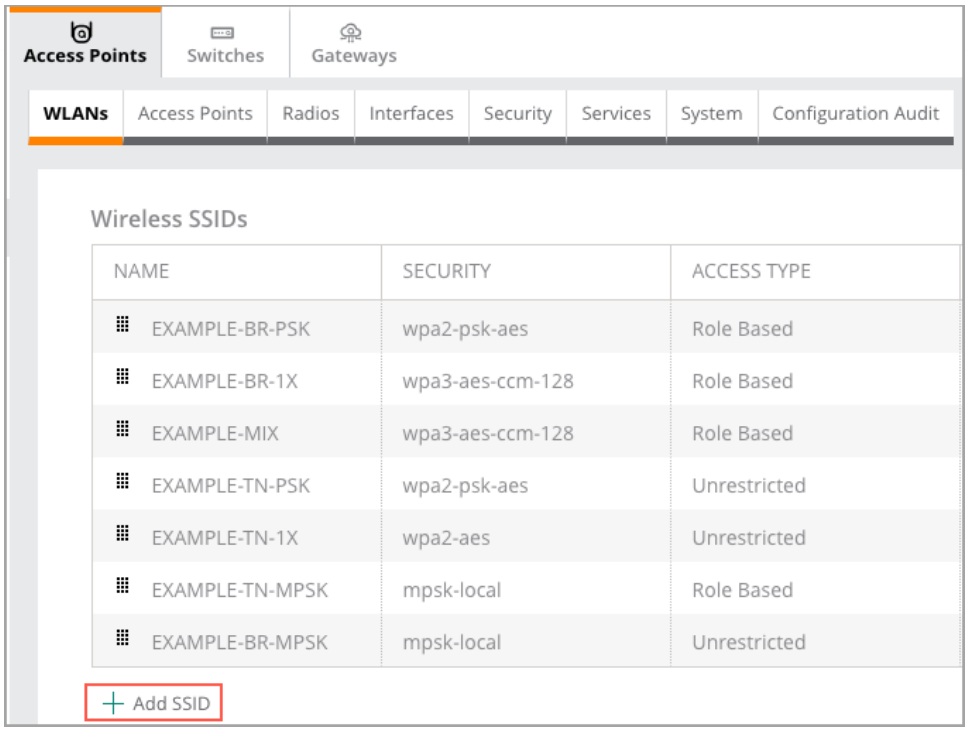
Step 2 On the Aruba Central Account Home page, launch the **Network Operations** app.

Step 3 In the filter drop-down list, select an AOS10 **Group** name, and then from the left menu, select **Devices**.

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

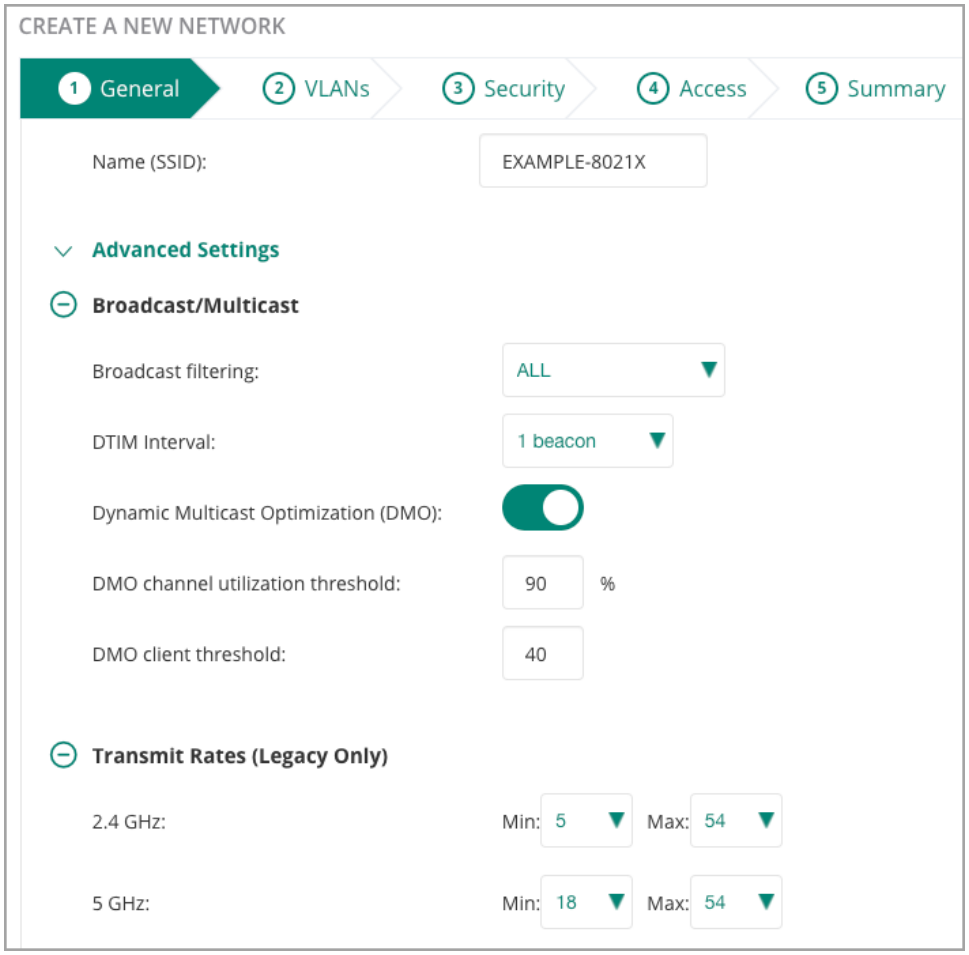


Step 5 From the Access Points page, select the WLANs tab, and then on the bottom left of the Wireless SSIDs table, click **+ Add SSID**.



Step 6 In the Create a New Network page on the General tab, expand **Advance Settings**, and then click the **+** sign to expand **Broadcast/Multicast**. **Step 7** Click the **+** sign to expand **Transmit Rates (Legacy Only)**, implement the following settings, and then click **Next**.

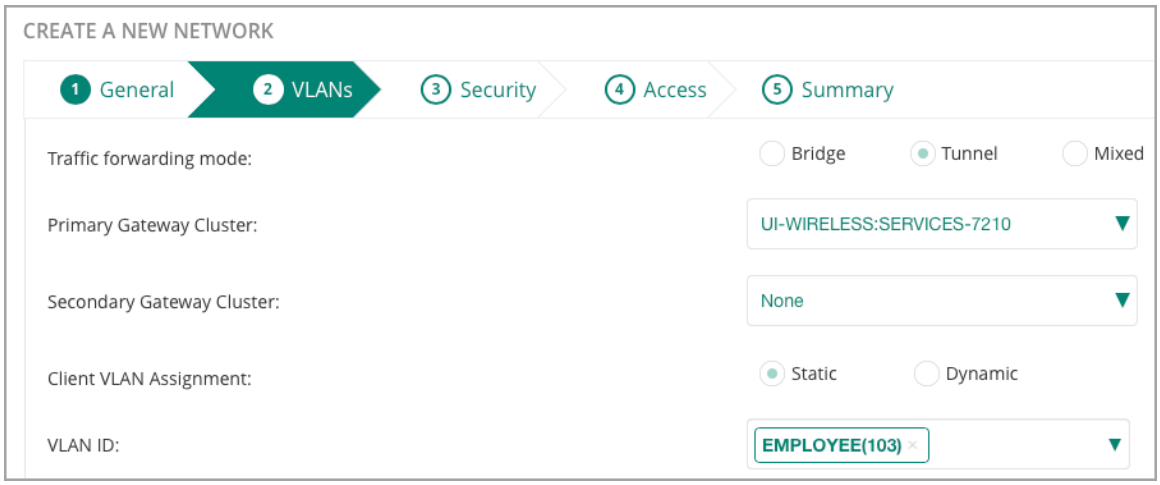
- **Name (SSID)**: *EXAMPLE-8021X*
- **Broadcast filtering:** *ALL*
- **Dynamic Multicast Optimization (DMO):** *Slide to the right*
- **DMO Client Threshold:** *40*
- **2.4 GHz: Min:** *5*
- **5 GHz: Min:** *18*



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

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

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



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

Step 9 On the Security tab, implement the following settings.

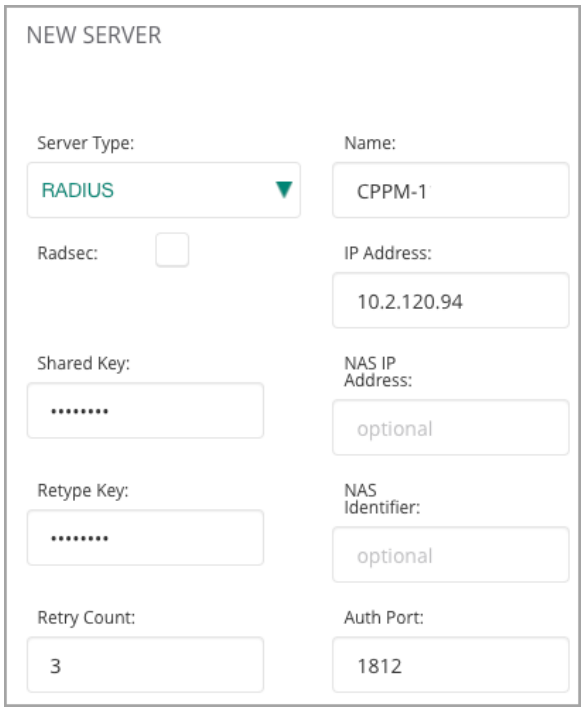
- **Security Level:** *Slide to Enterprise*
- **Key Management**: *WPA3 Enterprise (CMM 128)*

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

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

Step 11 In the New Server popup, implement the following settings, and then click **OK**.

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

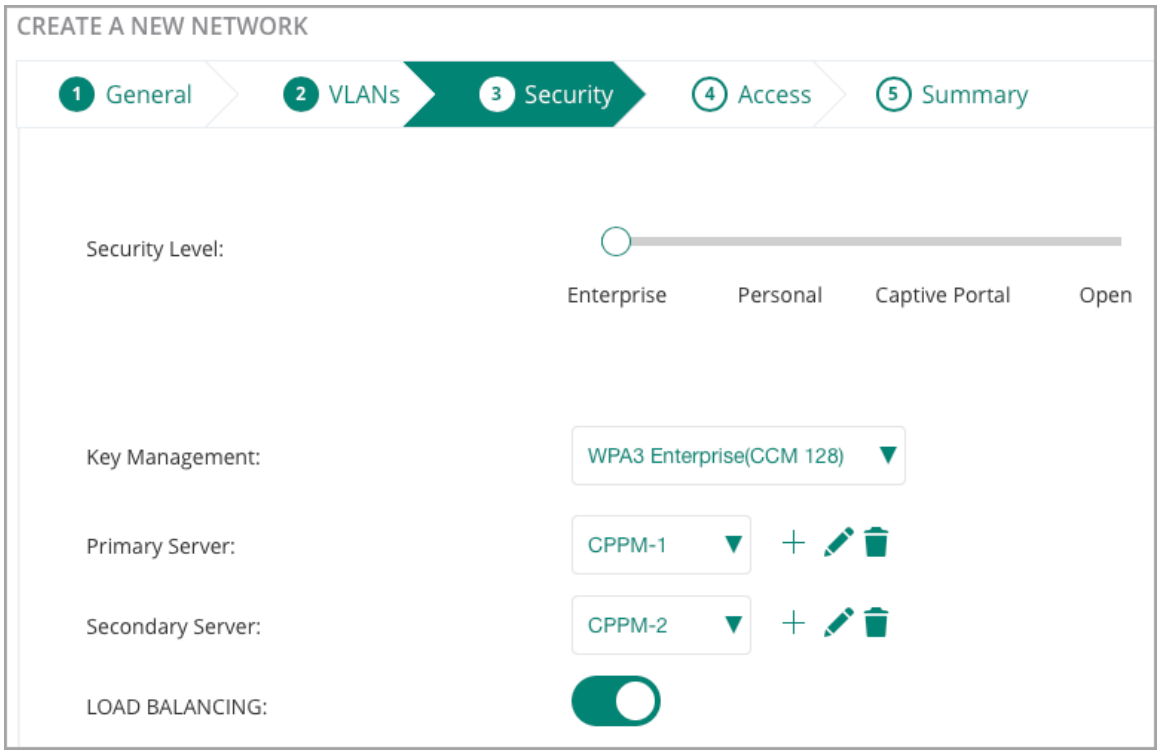


NOTE:
It is important to record the **Shared Key** created above for use when configuring ClearPass Policy Manager in the procedure below.

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

Step 13 On the Security tab, implement the following setting.

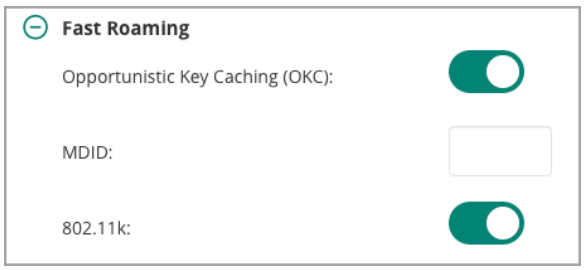
- **Load Balancing:** *Slide to the right*



NOTE:
The best practice is to deploy 2 RADIUS servers and enable load balancing.

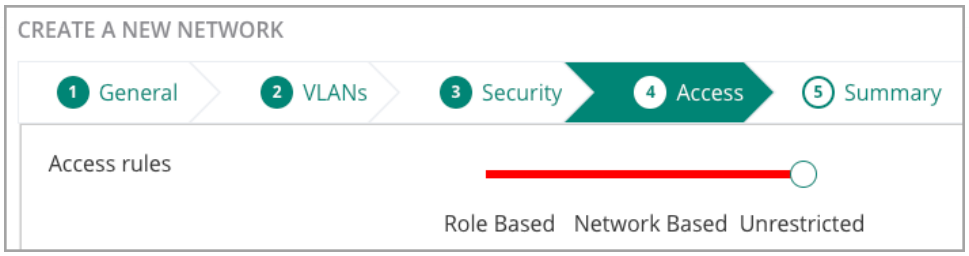
Step 14 On the Security tab, expand **Advanced Settings**, scroll down and click the **+** sign to expand **Fast Roaming**, implement the following settings, and then click **Next**.

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



Step 15 On the Access Tab, implement the following setting, and then click Next.

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



NOTE:
The restrictions for this type of SSID are done in the Gateway.

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

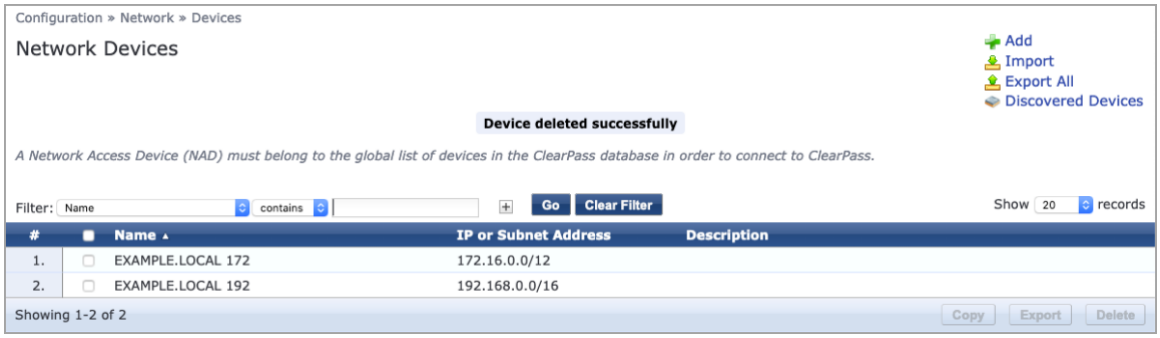
Configure ClearPass for the WPA3-Enterprise Wireless LAN

Use this procedure to configure ClearPass Policy Manager for the WPA3-Enterprise SSID.

Step 1 Browse to the ClearPass Policy Manager server, and login with administrator credentials.

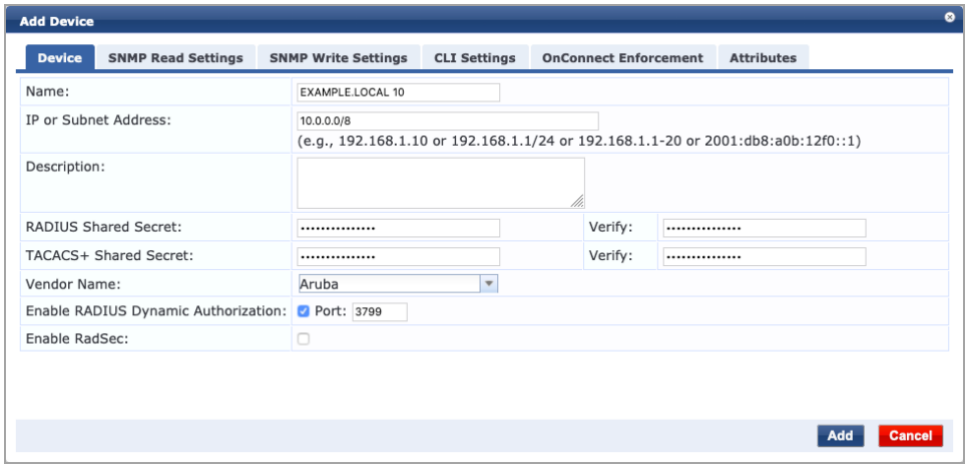
Step 2 From the left navigation menu, select **Configuration**, use the **+** sign to expand **Network**, and then select **Devices**.

Step 3 From the upper right of the Network Devices page, click **+Add**.



Step 4 On the Add Device page, implement the following settings, and then click **Add**.

- **Name:** *EXAMPLE.LOCAL 10*
- **IP or Subnet Address:** *10.0.0.0/8*
- **Description:** *<subnet description>*
- **Radius Shared Secret & Verify:** *RADIUS-SECRET*
- **TACACS Shared Secret & Verify:** *RADIUS-SECRET*
- **Vendor Name:** *Aruba (default)*
- **Enable RADIUS Dynamic Authorization:** *checkmark*
- **Port:** *3799 (default)*



Step 5 Repeat this procedure for additional ClearPass Policy Manager servers in the network.

Configure the Pre-Shared Key Wireless LAN

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

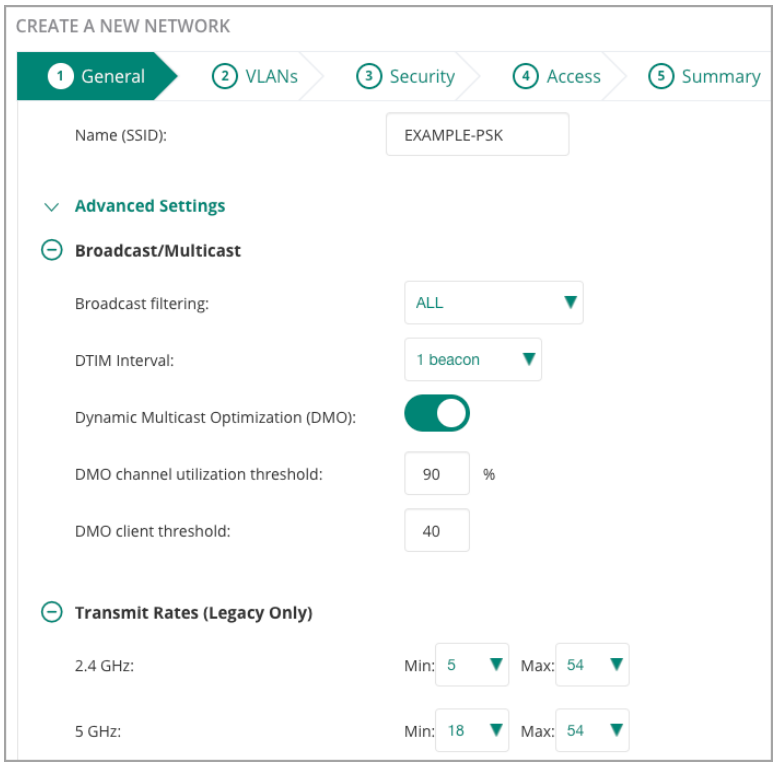
WPA3-Personal allows for authentication using a pre-shared key on a device that does not support 802.1x authentication.

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

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

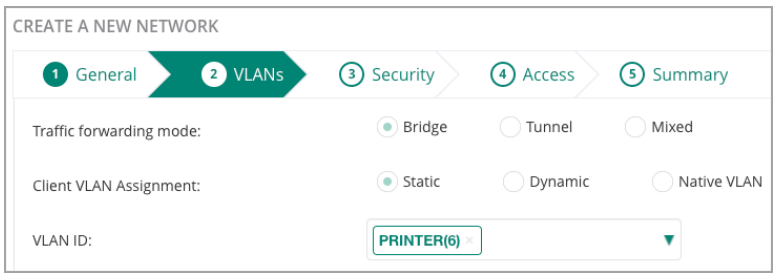
Step 3 Click the **+** sign to expand **Transmit Rates (Legacy Only)**, implement the following settings, and then click **Next**.

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



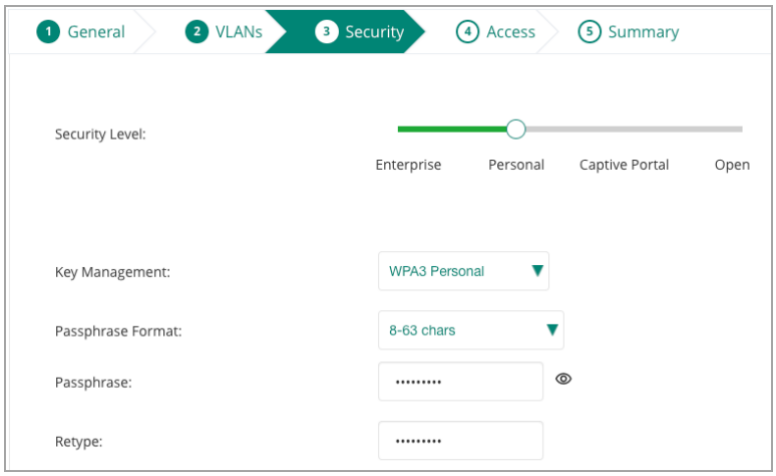
Step 4 On the VLANs tab, implement the following settings, and then click **Next**:

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



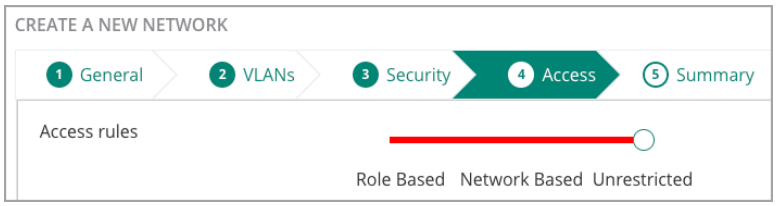
Step 5 On the Security tab, implement the following settings, and then click **Next**:

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



Step 6 On the Access Tab, implement the following setting, and then click Next.

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



NOTE:
The restrictions for this type of SSID are done in the Switch network.

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

Configure the Visitor Wireless LAN

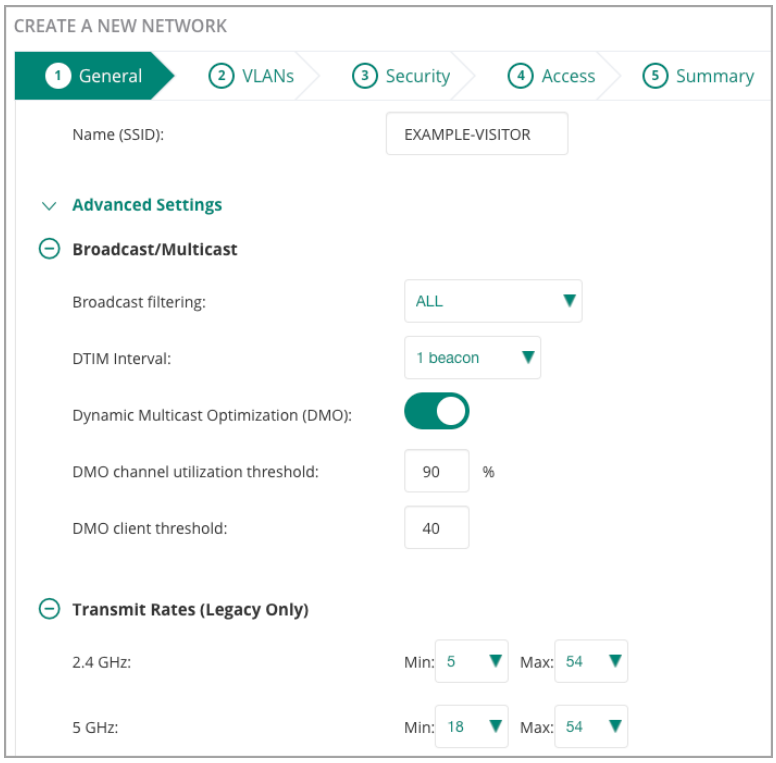
Use this procedure to configure a visitor SSID.

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

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

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

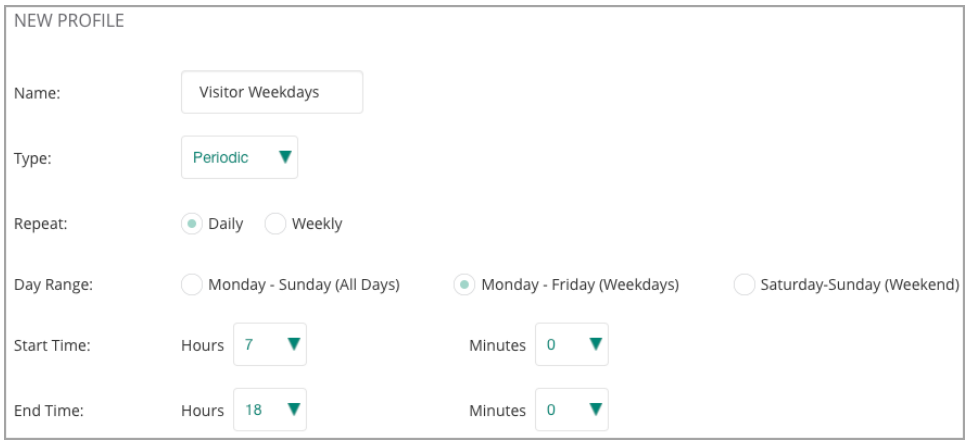
- **Name (SSID)**: *EXAMPLE-VISITOR*
- **Broadcast filtering:** *ALL*
- **Dynamic Multicast Optimization (DMO):** *Slide to the right*
- **DMO Client Threshold:** *40*
- **2.4 GHz: Min:** *5*
- **5 GHz: Min:** *18*



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

Step 5 In the New Profile popup, implement the following settings, and then click **Save**.

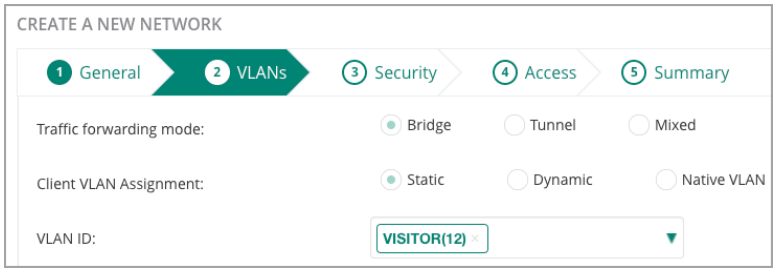
- **Name:** *Visitor Weekdays*
- **Type:** *Periodic*
- **Repeat:** *Daily*
- **Day Range:** *Monday - Friday (Weekdays)*
- **Start Time Hours:** *7* **Minutes:** *0*
- **End Time Hours:** *18* **Minutes:** *0*



Step 6 From the Time Range Profiles section in the Status drop-down list, find the newly created profile, select **Enabled**, and then at the bottom of the page, click **Next**.

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

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

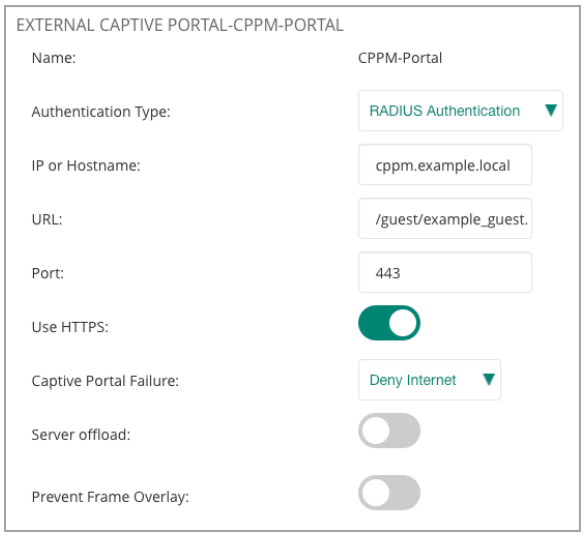


Step 8 On the Security tab, implement the following settings.

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

Step 9 In the Splash Page section, click the **+** sign next to **Captive Portal Profile**. **Step 6** In the External Captive Portal-New popup, implement the following settings, and then click **OK**.

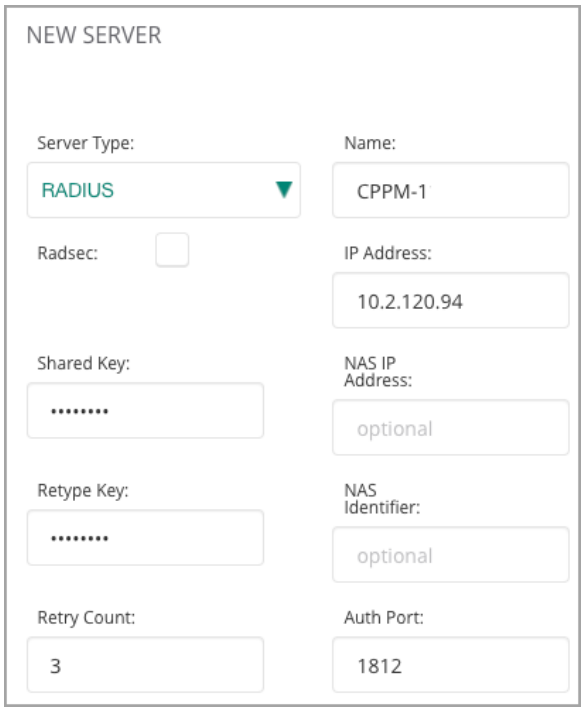
- **Name:** *CPPM-Portal*
- **Authentication Type:** *RADIUS Authentication*
- **IP or Hostname:** *cppm.example.local*
- **URL:** */guest/example_guest.php*
- **Port:** *443*
- **Redirect URL:** *http://www.arubanetworks.com*



Step 10 On the Security tab in the Splash Page section, click the **+** sign next to **Primary Server**.

Step 11 In the New Server popup, implement the following settings, and then click **OK**.

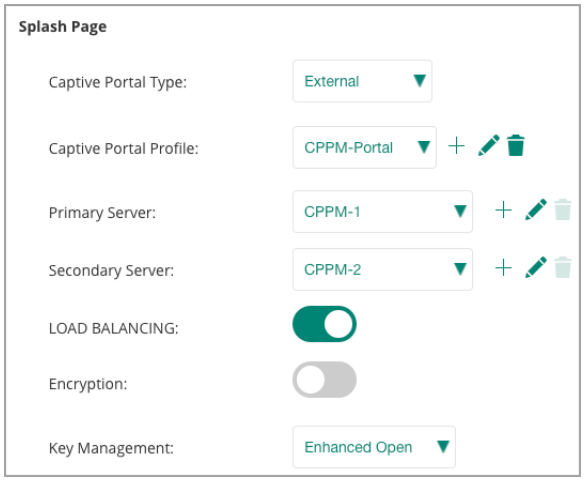
- **Server Type:** *RADIUS*
- **Name:** *CPPM-1*
- **IP Address:** *10.2.120.94*
- **Shared Key:** *shared key*
- **Retype Key:** *shared key*



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

Step 13 On the Security tab in the Splash Page section, implement the following settings, and then click **Next**.

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



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

Step 14 On the Access tab, move the slider to **Network Based**, select the **Allow any to all destinations** rule, and then click the **pencil** icon.

Step 15 In the Access Rules popup, implement the following settings, and then click **OK**.

- **Action:** *Deny*

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

Step 16 On the Access tab, select **+Add Rule**.

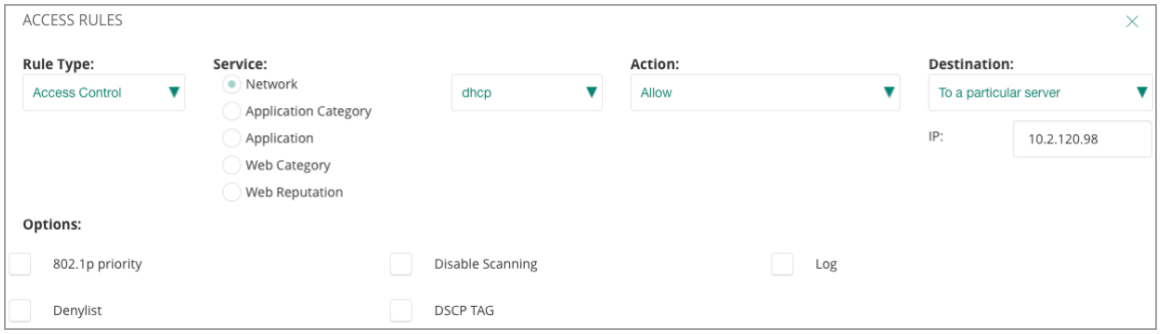
In most cases, the visitor only needs access to DHCP and DNS services, and HTTP/HTTPS access to all destinations on the Internet. Allow access to DHCP servers on the internal network and allow DNS to two well-known DNS servers. To prevent access to internal resources, add an exception network and mask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

Example: Access rules for visitors

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

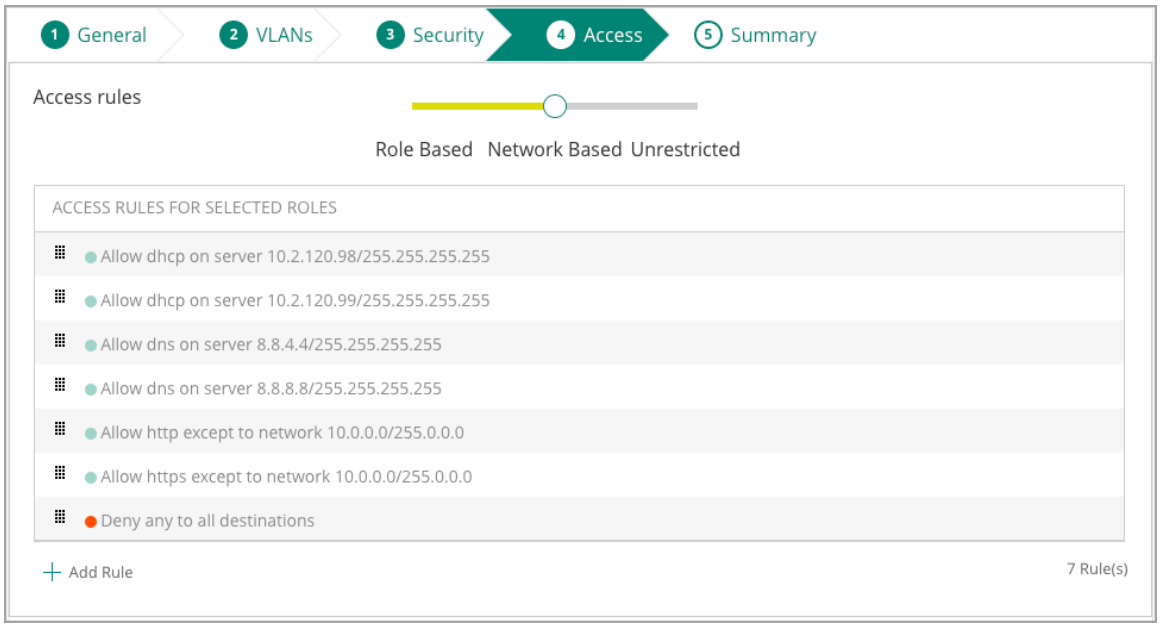
Step 17 In the Access Rules popup, implement the following settings, and then click **OK**.

- **Rule Type:** *Access Control*
- **Service:** *Network*
- **Service: Dropdown:** *dhcp*
- **Action:** *Allow*
- **Destination:** *To a particular server*
- **IP:** *10.2.120.98*
- **Options:** *none selected*



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

Step 18 Repeat the previous two steps to add all the rules in the table.



Step 19 On the Access tab, click **Next**.

Step 20 On the Summary tab, review the settings, and select **Finish**.

Campus Services

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

Configuring AI Insights

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

In this release the insights are classified under three categories:

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

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

Configuring AirMatch

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

Use this procedure to enable AirMatch for automated RF planning.

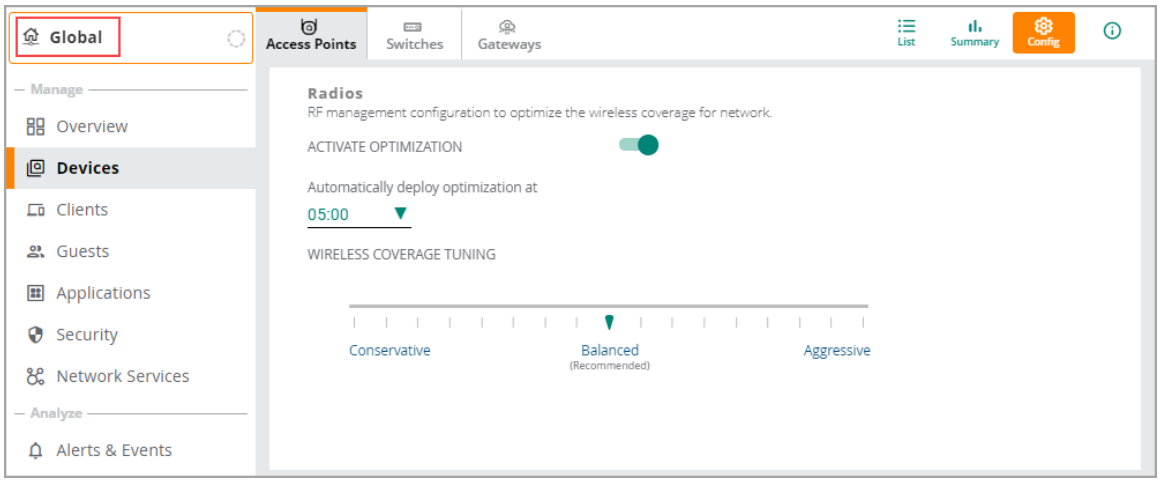
Step 1 On the Aruba Central Account Home page, launch the **Network Operations** app.

Step 2 In the filter drop-down list, select the **Global** filter.

Step 3 From the left menu, select **Devices**, select **Access Points**, and then, in the top right, select **Config**.

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

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



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

Configuring ClientMatch

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

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

Summary

The flow of information is a critical component to a well-run organization. The Aruba ESP Campus design provides a prescriptive solution, based on best practices and tested topologies. This allows you to build a robust network that accommodates your organization's requirements. Whether users are located at a large LAN location or at a smaller remote site, this design provides a consistent set of features and functionality for network access, which helps improve user satisfaction and productivity while reducing operational expense.

The ESP Campus design provides a consistent and scalable methodology of building your network, improving overall usable network bandwidth and resilience and making the Campus easier to deploy, maintain, and troubleshoot.

Validated Hardware and Software

The following hardware and software versions were validated for this guide. For compatibility, please upgrade to at least the versions listed below.

Wired Core

Product name	Software version
Aruba CX 8400	10.06.0113

Wired Aggregation

Product name	Software version
Aruba CX 8360	10.06.0113
Aruba CX 8325	10.06.0113
Aruba CX 8320	10.06.0113
Aruba CX 6400	10.06.0113

Wired Access

Product name	Software version
Aruba CX 6300M	10.06.0113
Aruba CX 6400	10.06.0113
Aruba 3810	16.10.0010
Aruba 2930M	16.10.0010

Wireless Gateways

Product name	Software version
Aruba 7200	10.2.0.1_79907

Wireless Access Points

Product name	Software version
Aruba AP 500	10.2.0.1_79907
Aruba AP 300	10.2.0.1_79907

Management and Orchestration

Product name	Software version
Aruba Central	2.5.3
Aruba ClearPass Policy Manager	6.9.2

What's New in This Version

The following changes were made since Aruba last published this guide:

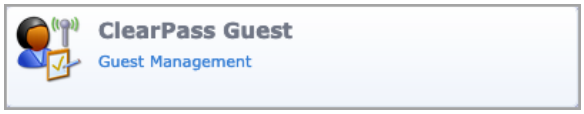
- This is a new guide

Appendix A: How to Find ClearPass Details for the Visitor WLAN

This section outlines the procedure to collect captive portal information and VRRP VIP information from ClearPass Policy Manager that is needed to configure Visitor WLAN.

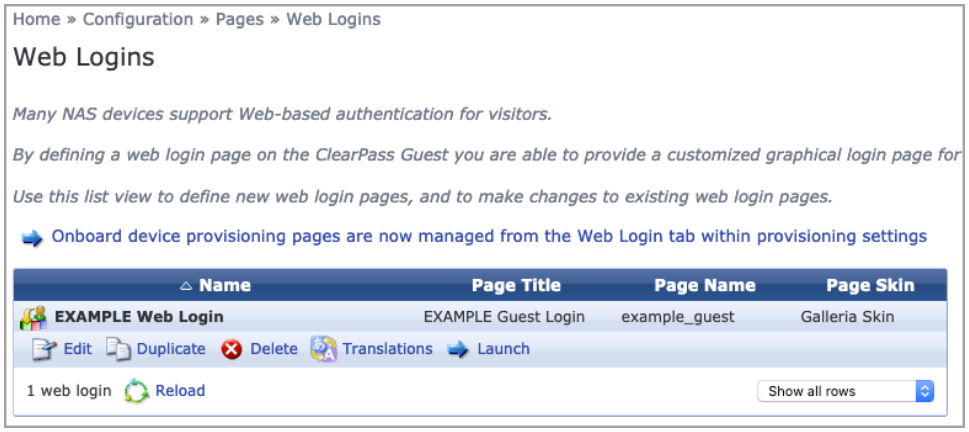
Find the Captive Portal Information

Step 1 Open a new browser tab, connect to one of the ClearPass servers, and login to ClearPass Guest with administrator credentials.



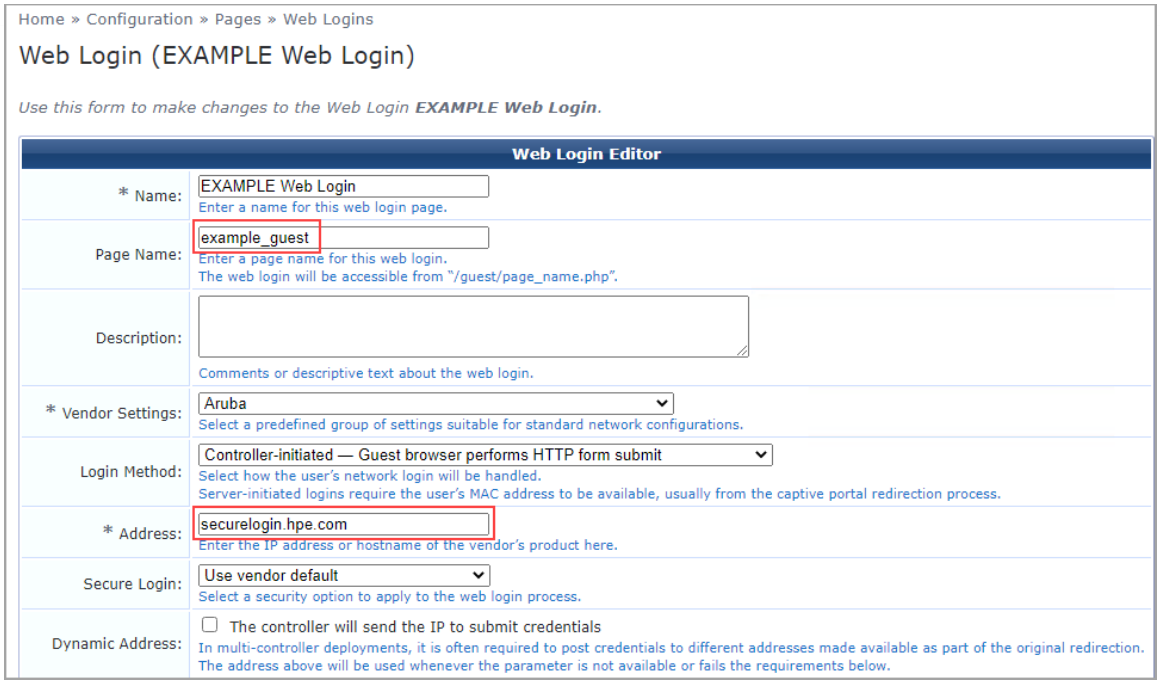
Step 2 From the left navigation menu, select **Configuration**, use the **+** sign to expand **Pages**, and then select **Web Logins**.

Step 3 Select the name of the already configured **Web Login** and then click **Edit**.



Step 4 Copy and store for later use the values found in **Page Name** and **Address**.

Step 5 Using the Menu at the up right, select **Logout**.



CAUTION:
Some legacy versions of AOS8 use a certificate with the name of securelogin.arubanetworks.com. All versions of AOS released since 2020 now use a certificate with the name securelogin.hpe.com. If this is a mixed environment where the legacy certificate is still in use, you may need to clone/duplicate the page to use another certificate. It is best practice to replace the certificate with a publicly signed one. If the certificate is replaced this issue is avoided but the **Address** in the web login will need to reflect the Common Name (CN) assigned to the certificate when it was issued.
NOTE:
This procedure uses the default certificate. It is best practice to replace the certificate with a publicly signed one. See the caution section above.

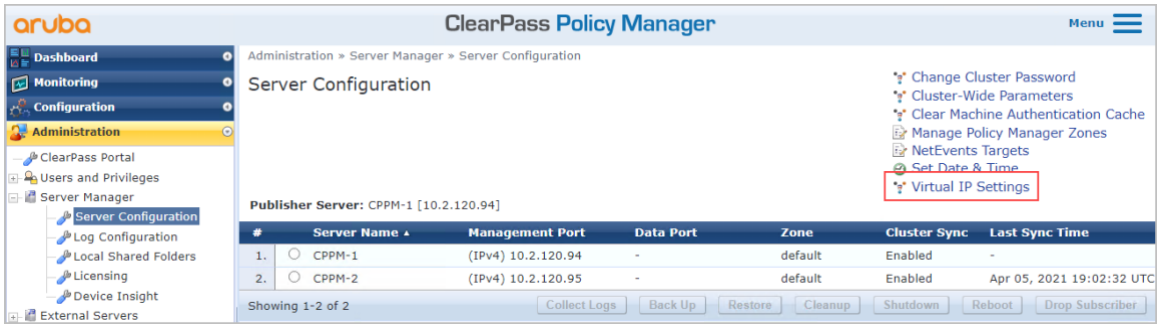
Find the ClearPass VRRP VIP

When following best practices and using more than one ClearPass Server for network authentication, the captive portal address or hostname in the WLAN **Access Policy** must be the VRRP address of the ClearPass servers. The following procedure shows how to find the VRRP address in ClearPass Policy Manager.

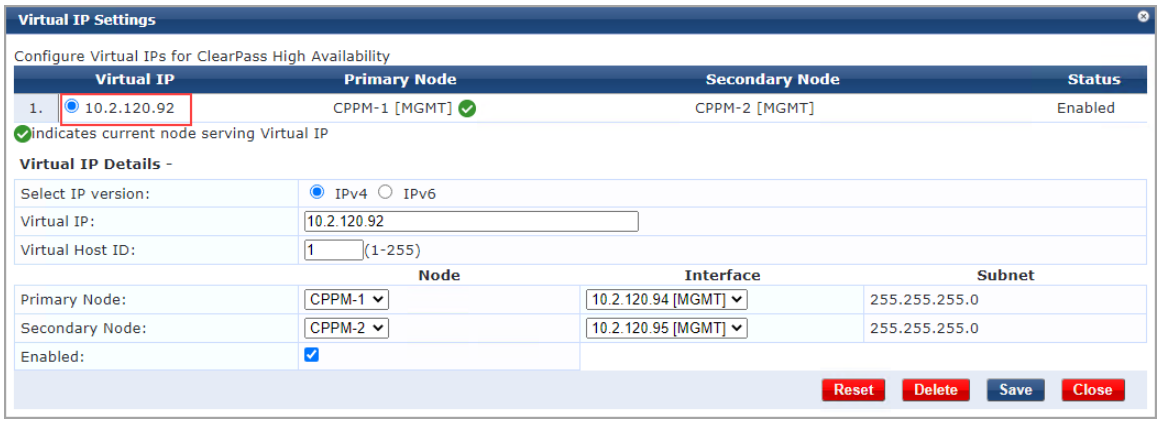
Step 1 Open a new browser tab, connect to one of the ClearPass servers, and login to ClearPass Policy Manager with administrator credentials.

Step 2 From the left navigation menu, select **Administration**, use the **+** sign to expand **Server Manager**, and then select **Server Configuration**.

Step 3 On the Server Configuration page in the top right, select **Virtual IP Settings**.



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



Step 5 Use *nsLookup* or other operating system specific mechanism to confirm that the above Virtual IP address has a resolvable host name and use the host name in the **Captive Portal Profile: IP or Hostname:** field when configuring a WLAN for captive portal authentication.